Chapter 2
Authentication and Secret-Key Cryptology

2.1 Introduction

The transmission of information in a communication process faces various threats. These threats arise if during the transmission, the messages are at the mercy of unauthorized actions of an adversary, that is, if the channel used for the communication is insecure. Basically there are three attacks the communicants have to be aware of when using an information transmission system. An adversary might observe the communication and gain information about it, he might insert false messages or he might replace legally sent messages by false messages. The protection against the first attack is a question of *secrecy* and the protection against the latter two attacks is a question of *authenticity*.

The need to protect communication has been appreciated for thousands of years. It is not surprising that most of the historical examples arise from the battleground, where secrecy and authenticity of messages is directly related to a potential loss of life. But apart from those military applications, the fast development of information technology has led to a number of economical applications in our days. From electronic fund transfer in international banking networks to the transmission of private electronic mail, there are vast amounts of sensitive information routinely exchanged in computer networks that demand for protection.

From ancient times on up to now, the authenticity of documents or letters has been guaranteed by the usage of seals and handwritten signatures, which are difficult to imitate. In order to guarantee secrecy, people have used methods in which the very existence of a message is hidden. Those techniques are known as concealment systems, including, for instance, the usage of invisible ink or the microscopical reduction of messages to hide them in meaningless text. An historical example of such a concealment goes back to the Greeks. Learning that the Persian king Darius was about to attack Greece, a Greek living in Persia scratched a warning message on a wooden writing tablet, then covered the tablet with wax so that it looked like a fresh writing surface. He sent it to Sparta, where Gorgo, the wife of the Spartan king

© Springer International Publishing Switzerland 2016

A. Ahlswede et al. (eds.), *Hiding Data – Selected Topics*,
Foundations in Signal Processing, Communications
and Networking 12, DOI 10.1007/978-3-319-31515-7_2

Leonidas, guessed that the blank wax writing surface covered something important, scraped it off and discovered the message that enabled the Greeks to prepare for Darius' attack and to defeat him ([16], pp. 38).

We will not deal with such physical devices for information protection but discuss a different method known as encryption or cryptographic coding, which allows a mathematical treatment. The idea is to transform the messages before transmission in order to make them unintelligible and difficult to forge for an adversary. Perhaps one of the first who employed such a method was Julius Caesar when replacing in his correspondence each letter by its third successor (cyclically) in the Latin alphabet ([15], pp. 83). The general usage of such a cryptosystem can be imagined as follows. Sender and receiver agree upon one of several possible methods to transform the messages. Using this method the sender transforms an actual message and transmits the result over the insecure channel. The receiver, knowing which method was used by the sender, can invert the transformation and resolve the original message. The possible transformations are usually referred to as *keys* and the transformed messages sent over the insecure channel are referred to as *cryptograms*. Further, the transformation of the original message into the cryptogram done by the sender is called *encryption* and the opposite action by the receiver is called *decryption*.

The mathematical model to analyze secrecy systems of this type was introduced by Shannon [24] in 1949. His work on this subject is generally accepted as the starting point of the scientific era of cryptology. As indicated, cryptosystems have been used for more than 2000 years and they were thought to be secure if no one who had tried to break them, had succeeded. Shannon's theory made it possible to prove the security of cryptosystems and to give bounds on the amount of information, which has to be securely transmitted to achieve this provable security.

The problem of authenticity, when a cryptosystem is used, was treated much later than Shannon's development of a theory for secrecy systems. The systematic study of authentication problems is the work of G.J. Simmons [28]. Although he is not among the originators of the earliest publication [12] from 1974 on this subject, the authors of this paper already mentioned that Simmons drew their attention to the model considered ([12], pp. 406).

The successful usage of a cryptosystem of the described form is primarily based on the ability of the sender and the receiver to agree upon a key to be used for the encryption and to keep this key secret. Therefore one has to assume that they can use a secure channel to exchange the identity of that key. Systems of this type are called *secret-key cryptosystems*. One might object that if sender and receiver have a secure channel at their disposal, they could use it directly for the transmission of the messages, but it might be possible that the secure channel is only available at some time instance before the transmission of the messages. Furthermore the secure channel might be unsuitable for the transmission of the messages, for instance, if it has a capacity that is too small. Hence, the assumption that a secure channel is available can be justified in a lot of cases and, in particular, systems with a small number of keys compared to the number of messages are of practical interest.

An example of a secret-key cryptosystem is the DES (data encryption standard), which was developed at IBM around 1974 and adopted as a national standard for

the USA in 1977. It uses keys specified by binary strings of length 56 and encrypts using these keys messages given as binary strings of length 64 [7].

We will analyze both the authentication and the secrecy problem on a theoretical level, where we assume that the adversary has infinite computing power. In 1976 Diffie and Hellman [9] invented a new type of cryptosystems where a secure channel to exchange the key is no longer needed. Each participant has a publically available key and a secret private key. These so called *public-key cryptosystems* are mostly based on an intractability assumption on the adversaries ability to solve a certain computational problem, like the factorization of large composite integers or the evaluation of the discrete logarithm, and are in this way based on a bound on the computational power of the adversary. Those systems are beyond the scope of this section.

The present chapter is organized as follows. In Sect. 2.1 the models of secret-key cryptology and authentication are introduced. We start with the classical model of a secrecy system formulated by Shannon [24]. As a measure for the secrecy provided by such a system the entropy criterion and the opponent's error probability when decrypting will be introduced and a relation between these criteria will be derived. In order to analyze the authentication problem we extend the so far discussed model in such a way that the adversary is allowed to become an active wiretapper, which means that he has more influence on the communication channel. We introduce the two different actions an opponent can try in order to deceive the receiver, namely, the so called impersonation attack and the substitution attack and we define the corresponding success probabilities P_I and P_S, respectively.

Although the model of the classical secrecy system is extended, it is still possible to analyze the introduced criteria for secrecy. Especially the class of authentication systems with no secrecy at all is of interest for some applications.

Section 2.3 is concerned with the authentication problem. We begin with deriving some general bounds on P_I and P_S. The derivation of Simmons' bound for P_I leads to the definition of perfect authenticity. We will see that, in general, authenticity and secrecy are two independent attributes of a cryptosystem (Sect. 2.3.1).

Then we will analyze the special class of authentication systems without secrecy. We derive the bound on P_S in such a case, which was originally proved in [12] and in a more general form in [2]. We show that a certain generalization to a larger class of message sources is not possible and we derive from the proof given in [2] necessary and sufficient conditions that an authentication system achieves the lower bound on P_S (Sect. 2.3.2).

The problem of the maximal number of messages in an authentication system under certain constraints on the success probabilities of the opponent will be treated in the next section. We study the behavior of the maximal number of messages for large values of Kp^2, where K is the number of keys and p is an upper bound on the opponent's success probability. The problem is still not completely solved and we derive the known upper and lower bounds. A typical result is that $M \sim \exp(K \cdot f(p))$ where M is the number of messages and f is some positive function. The special shape of f is up to now not exactly known. The difference between the upper and

lower bounds for M consists (for small p) essentially of a factor of order $\log \frac{1}{p}$ in the exponent of the bounds (Sect. 2.3.3).

The observation that the receiver's decision problem to accept a received message or not, can be viewed as an hypothesis testing problem will lead to a simpler derivation of information-theoretic lower bounds on the opponent's success probability. This approach, which was made in [19], allows also to generalize the model in several directions (Sect. 2.3.4).

In Sect. 2.4 we start the analyzation of secrecy systems with the derivation of some upper bounds on the secrecy measured by the entropy criterion. This leads to Shannon's result that a necessary condition for perfect secrecy is that the number of keys is at least as big as the number of messages. Afterwards we introduce the notions of regular and canonical ciphers and derive a lower bound on the secrecy for every locally regular cipher (Sects. 2.4.1 and 2.4.2). Furthermore we give an explicit construction of a good locally regular cipher and derive various bounds for the secrecy of this cipher (Sect. 2.4.3). Finally we present an approach to extend the model with a source coder and a (private) randomizer (Sects. 2.4.4 and 2.4.5).

In Sect. 2.4 we shall take a closer look at public-key cryptology. In Shannon's original model of a cryptosystem it is assumed that the cryptanalyst has unlimited computational power and hence is able to decipher the cryptogram immediately, once he knows the key. Shannon already remarked that this assumption often is not realistic. In their pioneering paper "New Directions in Cryptography" Diffie and Hellman [9] introduced public-key cryptology. They presented a protocol using only one key, which is a one-way function. In order to encrypt and decrypt the message, sender i and receiver j have to rise a special value to the power a_i (resp. a_j). This can be done very fast by repeated squaring. In principle a_i and a_j are known to the cryptanalyst, since they are stored in a public directory. However, they are published in the form $b_i = w^{a_i}$ and $b_j = w^{a_j}$, where w is a primitive element in a finite field. In order to conclude from b_i to a_i, the cryptanalyst has to take the *discrete logarithm* $a_i = \log_w b_i$ and for this task up to now no efficient algorithm is known. So, the cryptanalyst has all the necessary information to obtain the original message, but he cannot do this in a reasonable amount of time. There are several advantages of public-key cryptology compared to secret-key cryptology:

(1) the existence of a secure channel is no longer required;
(2) communication is faster, since the key has not to be transmitted;
(3) most public-key protocols are extendable to multi-user systems;
(4) public-key protocols also can be designed for further purposes, such as verification of identity, digital signatures, etc.

Whereas in secret-key cryptology the mathematical tools mostly stem from Information Theory, in public-key cryptology we need some background in Complexity Theory (one-way functions, zero-knowledge proofs) and in Number Theory, since most of the protocols we shall present are based on the hardness of integer factorization. We shall only present the ideas and facts which are important to understand the protocols presented and refer the reader to standard literature in the respective sections.

2.2 Models and Notation

2.2.1 Secret-Key Cryptology

In this paragraph the models of secret-key cryptology and authentication will be introduced. In both models we have three actors, a *sender*, a *receiver* and an *opponent*. Sender and receiver act together against the opponent. The sender has to inform the receiver about the state of a message source, in presence of the opponent who has access to the communication channel. The two models differ mainly in the abilities and actions of the opponent.

The opponent reads what is transmitted by the sender. The aim of sender and receiver is to avoid that the opponent can obtain any information from the transmitted message. To this aim sender and receiver share a *secret key* which is not known to the opponent. The sender uses this key to encrypt the original message into a different message, the so called cryptogram. This cryptogram is transmitted over the insecure channel to the receiver who can reconstruct the original message using the key. As the opponent does not know the secret key he hopefully can do nothing useful with the cryptogram. Such a secrecy system is depicted in Fig. 2.1, later this model will be extended with a randomizer and a source coder.

For the components of this model the following notation is used:

- Message Source $(\mathcal{M}, P)$
  where $\mathcal{M} \triangleq \{1, \ldots, M\}$ is a set of M messages and P is a probability distribution on $\mathcal{M}$.

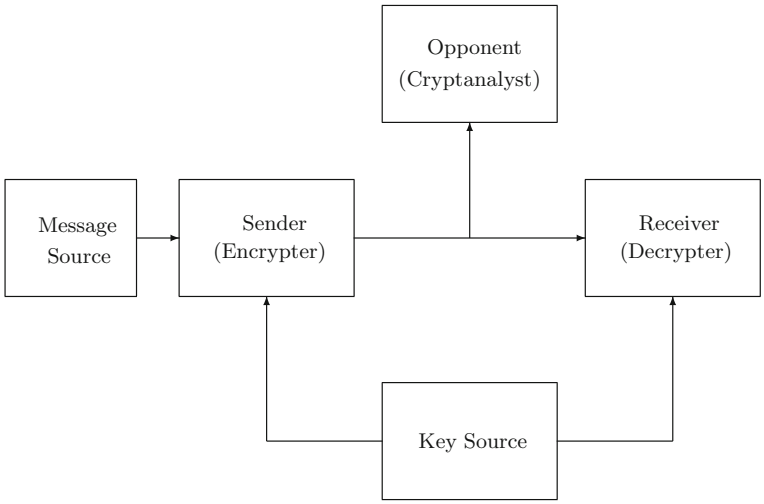


Fig. 2.1 A secret-key crypto system

- Key Source $(\mathcal{C}, Q)$
  where $\mathcal{C} \triangleq \{c_1, \ldots, c_K\}$ is a set of K keys and Q is a probability distribution on $\mathcal{C}$. Every key c_z is a mapping $c_z : \mathcal{M} \to \mathcal{M}'$ from the set of messages $\mathcal{M}$ to the set of cryptograms $\mathcal{M}'$, i.e., the sender encrypts the message $m \in \mathcal{M}$ into the cryptogram $c_z(m) \in \mathcal{M}'$, if the key with index z is used. In order to enable the receiver to reconstruct the original message we have to require

$$c_z(m_1) \neq c_z(m_2) \tag{2.2.1}$$

  for all $m_1, m_2 \in \mathcal{M},\ m_1 \neq m_2,\ z \in \{1, \ldots, K\}$.
  This implies that $|c_z(\mathcal{M})| = M$ for all $z \in \{1, \ldots, K\}$. When considering secrecy systems it is usually also assumed that $c_i(\mathcal{M}) = c_j(\mathcal{M})$ for all $i, j \in \{1, \ldots, K\}$ and therefore one can identify $\mathcal{M}$ and $\mathcal{M}'$ via isomorphy and regard the keys c_z as permutations on $\mathcal{M}$.
  The pair $(\mathcal{C}, Q)$ is also referred to as *cipher*.
- Random variables X, Y, Z
  It is often convenient to work with random variables for message, cryptogram and key rather then with the probability distributions P and Q itself, i.e.:
  Let X be a random variable with values in $\mathcal{M}$ and distribution $P_X = P$.
  Let Z be a random variable with values in $\{1, \ldots, K\}$ and distribution P_Z with $P_Z(z) = Q(c_z)$ for all $z \in \{1, \ldots, K\}$.
  Let Y be a random variable with values in $\mathcal{M}'(=\mathcal{M})$ and distribution P_Y, which is determined by the common distribution P_{XZ}. If not explicitly stated in another way, then we assume that the message and the key are generated by independent random experiments, i.e., $P_{XZ} = P_X P_Z$ and therefore

$$P_Y(m') = \sum_{m \in \mathcal{M}} P_X(m) \sum_{z : c_z(m) = m'} P_Z(z) \qquad \text{for all } m' \in \mathcal{M}. \tag{2.2.2}$$

In order to avoid trivialities we assume that we have more than one message ($M \geq 2$) and we will only deal with messages and keys that occur with strictly positive probability, otherwise they are irrelevant at all. We therefore assume that

$$P_X(m) > 0 \quad \text{and} \quad P_Z(z) > 0 \quad \text{for all } m \in \mathcal{M},\ z \in \{1, \ldots, K\}.$$

The triple $(X, Z, \mathcal{C})$ is referred to as *secrecy system*.

The Opponent's Knowledge

The secrecy provided by such a cryptosystem should be measured according to the fact that the value of the secret key can be kept unknown to the opponent but nothing more. This means it should not be assumed that one can prevent the opponent from getting information about other elements of the secrecy system. This is known as *Kerckhoffs' Principle*[1] in cryptology, which means that the opponent is assumed to

[1] First enunciated by A. Kerckhoffs (1835–1903) ([15], pp. 235).

know all details of the cryptosystem except for the value of the secret key, especially we also assume that the opponent has full knowledge about the probability distributions of messages and keys. Of course this worst-case assumption is quite pessimistic. Nevertheless in the long run it might not be too difficult for an opponent to get information about the design of the cryptosystem.

Measurements for Secrecy

We will introduce two measures for the secrecy provided by a cryptosystem of this type.

Entropy Criterion As the opponent reads the cryptogram $m' \in \mathcal{M}$ which is a realization of the random variable Y and tries to draw conclusions about the original message $m \in \mathcal{M}$ which is a realization of the random variable X, it is natural to use the average uncertainty about the state of the message source given the observation of the cryptogram. This is expressed by the conditional entropy

$$H(X|Y).$$

A 'very good' secrecy system will not decrease the uncertainty about X if Y is observed, i.e., $H(X|Y) = H(X)$. This leads to the following definition.

Definition 21 A secrecy system is perfect if X and Y are independent.

Cryptanalyst's Error Probability Beside the entropy criterion, already studied by Shannon [24], Ahlswede [1] considered as a measure for secrecy the cryptanalyst's error probability in deciding which message was sent.

Given a secrecy system by X, Z and $\mathcal{C}$ the probability of decrypting correctly is

$$\lambda_c(X, Z, \mathcal{C}) = \sum_{m' \in \mathcal{M}} \max_{m \in \mathcal{M}} P_{XY}(m, m'),$$

assuming that the cryptanalyst is using the maximum-likelihood decision rule, which is best possible. Therefore the opponent's error probability is

$$\lambda(X, Z, \mathcal{C}) = 1 - \lambda_c(X, Z, \mathcal{C}).$$

Lemma 4 *The two criteria for secrecy are not unrelated, namely for every secrecy system*

$$\lambda_c \geq 2^{-H(X|Y)}.$$

Proof

$$-\log \lambda_c = -\log \sum_{m' \in \mathcal{M}} \max_{m \in \mathcal{M}} P_{XY}(m, m')$$

$$\leq -\log \sum_{m' \in \mathcal{M}} \sum_{m \in \mathcal{M}} P_{X|Y}(m|m') P_{XY}(m, m')$$

$$\leq -\sum_{m' \in \mathcal{M}} \sum_{m \in \mathcal{M}} P_{XY}(m, m') \log P_{X|Y}(m|m')$$

$$= H(X|Y),$$

where the first inequality is due to the fact that the maximum is greater than the average of terms and the second one follows by application of Jensen's inequality for the $\cup$-convex function $-\log$. □

This lemma can be used to convert lower bounds on λ into lower bounds on $H(X|Y)$ and upper bounds on $H(X|Y)$ into upper bounds on λ.

Apart from the two measurements introduced so far, as a further criterion for secrecy Hellman [13] considered the average number of *spurious decipherments*.

2.2.2 Authentication

In general, authentication theory is concerned with providing evidence to the receiver of a message that it was sent by a specified and legitimate sender, even in presence of an opponent who can send fraudulent messages to the receiver or intercepts legally sent messages and replaces them by fraudulent ones.

In the model of secret-key cryptology the encryption with a secret key was done in order to guarantee secrecy, i.e., an opponent cannot decipher the cryptogram. In the model of authentication the encryption with a secret key is used to guarantee the authenticity of a transmitted message, which means that the encryption is done in such a way that the receiver recognizes if a fraudulent cryptogram was inserted by an opponent. So in this model the opponent is considered to be more powerful in the sense that he has more influence on the communication channel than before. The opponent can try two types of attacks:

- He can intercept a legally sent cryptogram and replace it by a different one.
  This is the so called *substitution attack*.
- He can send a fraudulent cryptogram to the receiver, even when no cryptogram was transmitted by the sender.
  This is the so called *impersonation attack*.

The opponent tries to deceive the receiver about the actual value of the random variable X. In the case of a successful substitution attack the receiver believes the random variable X to attain a value different from the true one. In the case of a successful impersonation attack the receiver believes the random variable X to attain some value but actually the message source has not generated a message. In both cases the aim of the opponent is to misinform the receiver about the state of the message source. (In fact this is the basic aim. For instance, it would be not very useful for a cheater to make his bank believe that on his account is a less amount of money than there actually is. Therefore one might think about more ambitious aims for the opponent. This will be treated in Sect. 2.3.4).

Such an authentication system is depicted in Figs. 2.2 and 2.3. In Fig. 2.2 a substitution attack is shown. In case of an impersonation attack the opponent simply sends a cryptogram to the receiver, sender and message source are thought to be inactive. Such a situation is shown in Fig. 2.3.

We will use the same notation for the components of this model as before:

- Message Source $(\mathcal{M}, P)$.
- Key Source $(\mathcal{C}, Q)$.
- Keys $c_z : \mathcal{M} \to \mathcal{M}',\ z \in \{1, \ldots, K\}$.
- Random Variables X, Y, Z for messages,cryptograms and keys, respectively.

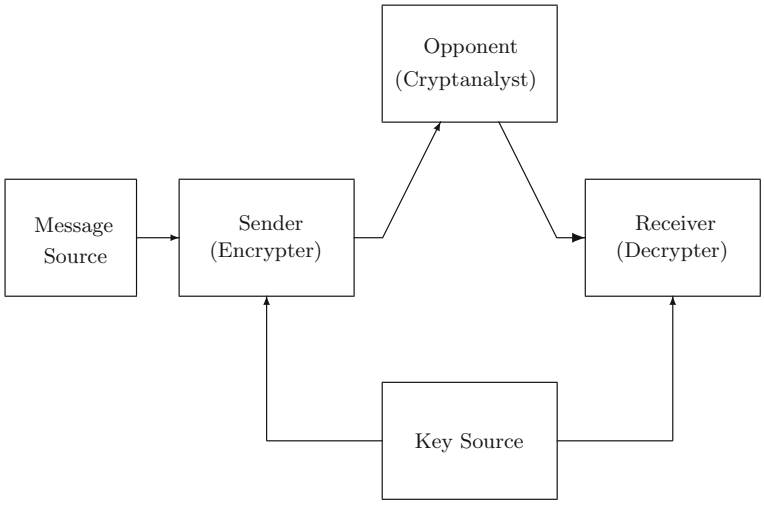
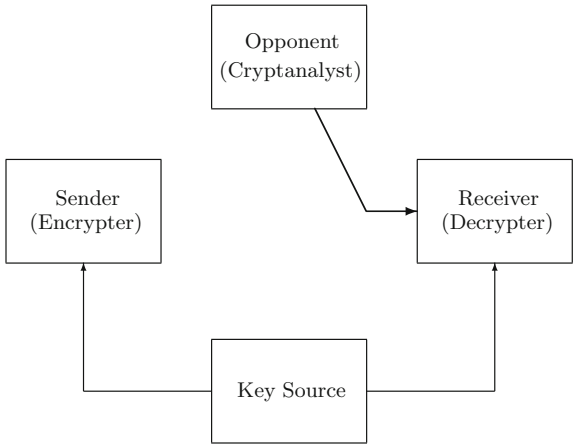


Fig. 2.2 A substitution attack

Fig. 2.3 An impersonation attack



In addition to this we need a random variable Y' for the cryptogram the opponent inserts. We use Y' for both cases of impersonation- and substitution attacks. To specify when the opponent is successful, we need the following definition.

Definition 22 A cryptogram $y \in \mathcal{M}'$ is valid under the key $c_z \in \mathcal{C}$ if y is in the range of c_z, i.e., $y \in c_z(\mathcal{M})$.

If the opponent inserts a cryptogram y', then the receiver does not detect the deception, if the cryptogram y' is valid under the secret key used by sender and receiver. On the other hand if y' is not valid under the secret key, then the receiver is sure that the cryptogram does not come from the sender and must have been inserted by the opponent.

Definition 23 The opponent is considered to be successful in each case if the receiver accepts the inserted y' as a valid cryptogram.

We call a probability distribution $P_{Y'}$ on $\mathcal{M}'$ an impersonation strategy and a family $\{P_{Y'|Y}(\cdot|y) : y \in \mathcal{M}'\}$ of conditional distributions on $\mathcal{M}'$ with $P_{Y'|Y}(y|y) = 0$ for all $y \in \mathcal{M}'$ a substitution strategy.

Let P_I and P_S denote the probabilities for the opponent using his optimal strategy to be successful in an impersonation attack and in a substitution attack, respectively.

Remark 8

1. Note that in a substitution attack we force the opponent to replace the intercepted cryptogram y by a *different* cryptogram y' because otherwise he would not misinform the receiver about the state of the message source.
2. In the model of secret-key cryptology it was assumed $\mathcal{M} = \mathcal{M}'$. Now this does not make sense any longer because it would imply that every cryptogram is valid under every key, therefore $P_I = P_S = 1$ and one cannot guarantee any authenticity of messages. Therefore we will allow in this context that $\mathcal{M}$ and $\mathcal{M}'$ are different sets with $|\mathcal{M}'| \geq |\mathcal{M}|$.

The triple $(X, Z, \mathcal{C})$ is referred to as *authentication system* or *authentication code*.

Such an authentication system can either provide no secrecy, i.e., $H(X|Y) = 0$, or it can provide some degree of secrecy, i.e., $H(X|Y) > 0$. Sometimes authentication codes without secrecy are called *cartesian* or *systematic* in the literature.

For this model of authentication we will keep the assumption of Section "The Opponent's Knowledge" that the opponent knows all details of the elements of the system except for the value of the secret key. In fact, Simmons [26, 27], who introduced this model, had a different notion. He thought of a game-theoretic authentication model. This means sender and receiver play against the opponent. In a game one needs to define the strategy sets of the players. Clearly the strategies for the opponent are the distributions introduced in Definition 23. The strategies of sender and receiver Simmons then defined as the possible distributions P_Z of the keys. Therefore he had to assume that the opponent does not know the key statistics. This approach has not further been developed in literature and we will keep Kerckhoffs' assumption, which means that also P_Z is fixed and known to the opponent.

Remark 9 In order to avoid confusion it should be noted that in a lot of papers concerning authentication theory (for example those of Simmons) a different notation is used. Messages are called source states, cryptograms are called messages and keys are called encoding rules.

2.3 Authentication

2.3.1 General Bounds and Perfectness

In Shannon's model of secret-key cryptology it was clear how to define the perfectness of the system. In the authentication model it is no longer obvious, when one can say that a system provides perfect authenticity. We will see that a complete protection against deception is impossible. Therefore we have to start with the analysis to what degree the opponent is able to deceive the receiver.

Hence, we try to give lower bounds on the probabilities P_I and P_S. It should be noted that there is no general relationship of the form $P_S \geq P_I$, as one might think at first sight because in a substitution attack the opponent has the additional information about a valid cryptogram. Recall that in a substitution attack the opponent is restricted to choose a cryptogram different from the original one, as he wants to misinform the receiver. The next example shows that this can lead to a situation with $P_S < P_I$.

Example 3 Let us define an authentication system as follows:

- Two messages, $\mathcal{M} \triangleq \{1, 2\}$, which occur each with probability $\frac{1}{2}$, i.e., $P_X(1) \triangleq P_X(2) \triangleq \frac{1}{2}$.
- 3 keys, $\mathcal{C} \triangleq \{c_1, c_2, c_3\}$, with $P_Z(z) \triangleq \frac{1}{3}$ for all $z \in \{1, 2, 3\}$.
- 3 possible cryptograms, $\mathcal{M}' \triangleq \{y_1, y_2, y_3\}$ and the encryption is done according to the following table.

	y_1	y_2	y_3
c_1	1	2	
c_2		1	2
c_3	2		1

For instance, the message 2 is encrypted using the key c_3 to the cryptogram y_1 or formally $c_3(2) = y_1$.

Clearly $P_I = \frac{2}{3}$, as $Pr(y_i \text{ valid}) = \frac{2}{3}$ for all $i \in \{1, 2, 3\}$.

But after having observed any valid cryptogram, the probability that a different one is also valid under the used key is always $\frac{1}{2}$.

Therefore $P_S = \frac{1}{2} < \frac{2}{3} = P_I$.

Combinatorial Bounds

Theorem 31 *For every authentication system*

$$P_I \geq \frac{M}{|\mathcal{M}'|} \quad \textit{and} \quad P_S \geq \frac{M-1}{|\mathcal{M}'|-1}.$$

Proof The statement immediately follows by consideration of the following impersonation strategy and substitution strategy, respectively.

- *Impersonation*: The opponent chooses $y \in \mathcal{M}'$ according to the uniform distribution, i.e., $P_{Y'}(y) = \frac{1}{|\mathcal{M}'|}$ for all $y \in \mathcal{M}'$.
- *Substitution*: Observing $y \in \mathcal{M}'$ the opponent chooses $y' \neq y$ according to the uniform distribution from $\mathcal{M}'\backslash\{y\}$, i.e., $P_{Y'|Y}(y'|y) = \frac{1}{|\mathcal{M}'|-1}$ for all $y' \neq y$.

As these strategies are not necessarily optimal, by calculation of the corresponding success probabilities we obtain lower bounds on P_I and P_S, namely

$$P_I \geq \sum_{z=1}^{K} P_Z(z) \frac{|c_z(\mathcal{M})|}{|\mathcal{M}'|} = \frac{M}{|\mathcal{M}'|}$$

and similarly

$$P_S \geq \sum_{z=1}^{K} P_Z(z) \frac{|c_z(\mathcal{M})|-1}{|\mathcal{M}'|-1} = \frac{M-1}{|\mathcal{M}'|-1},$$

where we used that $|c_z(\mathcal{M})| = M$, as c_z is injective. □

Remark 10
1. Note that in Example 3 the bounds hold with equality.
2. If we consider also randomized ciphers (i.e., some messages may be mapped to different cryptograms under the same key according to some probability distribution), then we have $|c_z(\mathcal{M})| \geq M$ and therefore equality in the bounds is only possible if the cipher is not randomized.
3. $P_I = 0$ or $P_S = 0$ is impossible (recall that $M \geq 2$).

Simmons' Bound

In this section we present the basic information-theoretic lower bound on P_I, first given by Simmons [26, 27].

Before this, note that one can get two rough bounds on P_I and P_S in terms of entropy simply by bounding the probabilities of guessing the key correctly (in case of a substitution attack after observing the cryptogram y). Doing this we get:

$$P_I \geq 2^{-H(Z)} \quad \text{and} \quad P_S \geq 2^{-H(Z|Y)}.$$

The derivation of this type of bounds is done in Sect. 2.3.4, where we will treat the bound on P_S in a more general context. The next theorem shows that it is possible to add $H(Z|Y)$ in the exponent of the bound for P_I.

Theorem 32 (Simmons) *For every authentication system*

$$P_I \geq 2^{-I(Y \wedge Z)}.$$

At first sight this bound may look somewhat strange, as it tells us that P_I can be made small only if the cryptogram gives away much information about the key. But recall that in an impersonation attack the opponent does not have access to a legally sent cryptogram. Furthermore one could interprete the bound from the receivers viewpoint. The receiver can only hope for a small P_I if his knowledge of the key gives him a lot information about the cryptogram.

The proof for Simmons' bound presented below was taken from Johannesson and Sgarro [14]. It is simpler than Simmons' original derivation and one easily sees how the bound can be strengthened.

Proof of the theorem. The best impersonation attack for the opponent is to choose a cryptogram $y \in \mathcal{M}'$ with maximal probability of validity, i.e.,

$$P_I = \max_{y \in \mathcal{M}'} \Pr(y \text{ valid}) = \max_{y \in \mathcal{M}'} \sum_{z:\phi(y,z)=1} P_Z(z), \tag{2.3.1}$$

where the function ϕ is defined as follows

$$\phi(y, z) \triangleq \begin{cases} 1, & \text{if } P_{YZ}(y, z) > 0 \\ 0, & \text{otherwise,} \end{cases}$$

i.e., $\phi(y, z)$ is equal to one exactly if y is a valid cryptogram under the key c_z.

Now we calculate $I(Y \wedge Z)$ and apply the log-sum inequality.

$$I(Y \wedge Z) = \sum_y P_Y(y) \sum_z P_{Z|Y}(z|y) \log \frac{P_{Z|Y}(z|y)}{P_Z(z)}.$$

We can restrict the summation to terms with $\phi(y, z) = 1$ (because only for these we have $P_{Z|Y}(z|y) > 0$) and apply the log-sum inequality. In this way we obtain

$$I(Y \wedge Z) = \sum_y P_Y(y) \sum_{z:\phi(y,z)=1} \phi(y,z) P_{Z|Y}(z|y) \log \frac{\phi(y,z) P_{Z|Y}(z|y)}{\phi(y,z) P_Z(z)}.$$

$$\geq \sum_y P_Y(y) \underbrace{\Big(\sum_{z:\phi(y,z)=1} \phi(y,z) P_{Z|Y}(z|y) \Big)}_{=1} \log \frac{\overbrace{\sum_{z:\phi(y,z)=1} \phi(y,z) P_{Z|Y}(z|y)}^{=1}}{\underbrace{\sum_{z:\phi(y,z)=1} \phi(y,z) P_Z(z)}_{\Pr(y \text{ valid})}}$$

$$= -\sum_y P_Y(y) \log \Pr(y \text{ valid}) \geq -\log \max_y \Pr(y \text{ valid}) = -\log P_I . \square$$

Corollary 1 *Necessary and sufficient conditions for equality in Simmons' bound are:*

1. $\Pr(y \text{ valid})$ *is constant in* y.
2. $\frac{P_Z(z) P_Y(y)}{P_{YZ}(y,z)}$ *is constant for all* (y,z) *with* $P_{YZ}(y,z) > 0$.

Proof The first condition follows from the last inequality in the proof and the condition for equality in the log-sum inequality is in our case:

$$P_{Z|Y}(z|y) \Pr(y \text{ valid}) = P_Z(z) \quad \text{for all } (y,z) \text{ with } \phi(y,z) = 1,$$

which is equivalent to condition 2. as we saw already that $\Pr(y \text{ valid})$ must be constant in y. □

Strengthening of Simmons' Bound

The first strengthening by Johannesson and Sgarro [14] is easily derived by the following observation. From Eq. (2.3.1) it is clear that $\Pr(y \text{ valid})$ and therefore also P_I is independent of the distribution P_X of messages, but the mutual information $I(Y \wedge Z)$ is not, in general. This implies that if we change our distribution P_X of messages to some $P_{\tilde{X}}$ in such a way that the function ϕ is kept unchanged, then we get a new value $2^{-I(\tilde{Y} \wedge Z)}$ which is also a bound for P_I in our original authentication system. Therefore we obtain a stronger bound in the following way.

Proposition 2 (Johannesson, Sgarro)

$$P_I \geq 2^{-\inf I(Y \wedge Z)},$$

where the infimum is taken over all distributions P_X *which leave* ϕ *unchanged.*

In the next example we show that this new bound can return values, which are strictly better than those of the former bound.

Example 4 Let us define an authentication system in the following way.

- Two messages, $\mathcal{M} \triangleq \{1, 2\}$ with $P_X(1) \triangleq p \leq \frac{1}{2}$ (w.l.o.g.).
- Four equiprobable keys, $\mathcal{C} \triangleq \{c_1, \ldots, c_4\}$ with $P_Z(z) \triangleq \frac{1}{4}$ for all $z \in \{1, \ldots, 4\}$.
- Four cryptograms, $\mathcal{M}' \triangleq \{y_1, \ldots, y_4\}$.

The encryption is shown in the table below.

	y_1	y_2	y_3	y_4
c_1	1	2		
c_2	2		1	
c_3		1		2
c_4			2	1

For this authentication system we have $P_I = \frac{1}{2}$ and $P_S = 1 - p \geq \frac{1}{2}$, which implies $P_D = 1 - p$.

$I(Y \wedge Z) = H(Y) - H(Y|Z) = \log 4 - h(p) = 2 - h(p)$, where h is the binary entropy, i.e., $h(p) \triangleq -p \log p - (1 - p) \log(1 - p)$. Therefore $2^{-I(Y \wedge Z)} = \frac{2^{h(p)}}{4} \leq \frac{1}{2}$ with equality exactly if $p = \frac{1}{2}$.

Hence, the strengthened bound for P_I is sharp and the old bound is not sharp for $p \neq \frac{1}{2}$.

We could strengthen the bound by observing that P_I is independent of P_X (if ϕ is kept unchanged). We can obtain a further strengthening by analyzing on what P_I depends. Again from Eq. (2.3.1) it is clear that P_I depends only on the (marginal) distribution of Z and on the function ϕ. Thus, given that these are kept fixed, both the message distribution and *any correlation of X and Z* are totally irrelevant. Therefore we get a new bound:

Theorem 33 (Johannesson, Sgarro)

$$P_I \geq 2^{-\inf I(Y \wedge Z)},$$

where now the infimum is taken over all (possibly dependent) random couples (X, Z) *such that*

1. *Z has the same marginal distribution as for the given system*
2. *the resulting function ϕ is the same as for the given system.*

Again this new bound can return values that are strictly better than those of the previously considered bounds, which is shown in the next example.

Example 5 Let us define an authentication system in the following way:

- Two messages, $\mathcal{M} \triangleq \{1, 2\}$ with $P_X(1) \triangleq p$.
- Two equiprobable keys, $\mathcal{C} \triangleq \{c_1, c_2\}$ with $P_Z(1) \triangleq P_Z(2) \triangleq \frac{1}{2}$.

- Three cryptograms $\mathcal{M}' \triangleq \{y_1, y_2, y_3\}$.

The encryption is done according to the following table.

	y_1	y_2	y_3
c_1	1	2	
c_2	2		1

For this authentication code we have $P_I = 1$, because $\Pr(y_1 \text{ valid}) = 1$ and $I(Y \wedge Z) = H(Y) - H(Y|Z) = 1 + \frac{1}{2}h(p) - h(p) = 1 - \frac{1}{2}h(p)$.

If we take $p = \frac{1}{2}$, then $I(Y \wedge Z)$ is minimized and we obtain the (old) bound $P_I \geq 2^{-\frac{1}{2}} = \frac{1}{\sqrt{2}}$, which is not sharp. Suppose now that X and Z are no longer independent and assume that X and Z return the same values with probability close to one (we cannot say with probability equal to 1 because this would change ϕ). Then with probability close to one $Y = y_1$ and therefore $I(Y \wedge Z) = H(Y) - H(Y|Z) \leq H(Y) \approx 0$. So the new bound gives the correct estimate $P_I = 1$ for the original system where X and Z are independent.

There are also nondegenerate examples ($P_I < 1$) with this effect (see [14]).

Perfectness

Up to now we derived lower bounds on P_I. With each of these lower bounds we obtain also a lower bound on the probability of deception P_D, which we define as $P_D \triangleq \max\{P_I, P_S\}$. For instance,

$$P_D \geq 2^{-I(Y \wedge Z)} \tag{2.3.2}$$

Simmons [26, 27] defined perfect authenticity to mean that equality holds in (2.3.2). In this case, he noted that *the information capacity of the transmitted cryptogram is used either to inform the receiver as to the state of the message source or else to confound the opponent*.

Definition 24 An authentication system is perfect if

$$P_D = 2^{-I(Y \wedge Z)}.$$

One could also think of perfect authenticity to mean that equality holds in (2.3.2), where instead of Simmons' bound the stronger bound on P_I from Theorem 33 is used on the right-hand side. However we will keep the original definition by Simmons. This was also done by Massey [18] who noted that the information that Y gives about Z, $I(Y \wedge Z)$, is a measure of how much of the secret key is used to provide authenticity. Therefore, if the stronger bound $2^{-\inf I(Y \wedge Z)}$ is greater than $2^{-I(Y \wedge Z)}$, then this indicates that the authentication system is wasting part of the information $I(Y \wedge Z)$ and therefore should not be called 'perfect'.

Remark 11 1. Note that we may have to call a system perfect although it provides no authenticity at all, i.e., $P_D = 1$. For instance, the "One-Time Pad" described in Example 7 provides perfect secrecy and Y and Z are independent. Therefore $P_D = 2^{-I(Y \wedge Z)} = 1$.

2. The authentication system of Example 4 provides for $p = \frac{1}{2}$ both perfect secrecy and perfect authenticity with $P_D = \frac{1}{2}$. For $p \neq \frac{1}{2}$ it still provides perfect secrecy but has no longer perfect authenticity. The next example shows an authentication system with perfect authenticity but without perfect secrecy. Therefore we can say that *in general* authenticity and secrecy are two independent attributes of a cryptographic system. Massey [18] says that this is a lesson that is too often forgotten in practice.

Example 6 Let us define an authentication system in the following way:

- Two messages $\mathcal{M} \triangleq \{1, 2\}$, with $P_X(1) \triangleq P_X(2) \triangleq \frac{1}{2}$.
- Four keys, $\mathcal{C} \triangleq \{c_1, \ldots, c_4\}$, which are chosen according to the uniform distribution.
- Four cryptograms $\mathcal{M}' \triangleq y_1, \ldots, y_4\}$.

The encryption is shown in the following table.

	y_1	y_2	y_3	y_4
c_1	1		2	
c_2	1			2
c_3		1	2	
c_4		1		2

For this authentication system we have $P_I = P_S = \frac{1}{2}$, $I(Y \wedge Z) = H(Y) - H(Y|Z) = \log 4 - \log 2 = 1$ and therefore $P_I = P_S = 2^{-I(Y \wedge Z)}$, which means that the system provides perfect authenticity but it is clearly not perfectly secret as $H(X|Y) = 0 \neq 1 = H(X)$.

A Bound on P_S

In this section we derive a bound on P_S presented in [23] which is based on Simmons' bound for P_I.

Definition 25 For every cryptogram $y \in \mathcal{M}'$ let $\mathcal{K}(y) \triangleq \{z \in \{1, \ldots, K\} : P_{Y,Z}(y, z) > 0\}$ be the set of key-indices such that y is a valid cryptogram under the corresponding keys.

Let $P_S(y)$ denote the probability of successful substitution after observing that $Y = y$.

If the opponent intercepts y and substitutes y' then his probability of success is $P_{Z|Y}(\mathcal{K}(y')|y)$. Therefore $P_S(y)$ can be written as

$$P_S(y) = \max_{y' \neq y} P_{Z|Y}(\mathcal{K}(y')|y). \tag{2.3.3}$$

We will now obtain a lower bound on $P_S = \sum_y P_Y(y)\, P_S(y)$ by bounding $P_S(y)$ below. Therefore let us define for every $y \in \mathcal{M}'$ random variables Y_y, with values in $\mathcal{M}'\backslash\{y\}$, and Z_y, with values in $\{1, \ldots, K\}$, as follows

$$P_{Z_y}(z) \triangleq P_{Z|Y}(z|y) \text{ and } P_{Y_y|Z_y}(y'|z) \triangleq \frac{P_{Y|Z}(y'|z)}{a_y(z)} \quad \text{for all } y' \neq y, \tag{2.3.4}$$

where $a_y(z) \triangleq \sum_{y' \neq y} P_{Y|Z}(y'|z)$ is the normalization constant such that $P_{Y_y|Z_y}(\cdot\,|z)$ is a probability distribution. Note that $a_y(z)$ is always greater 0 because $M \geq 2$ and there are M valid cryptograms for every key.

Although one cannot assure that there always exists an authentication system which induces this random couple (Y_y, Z_y), we can (formally) look at the corresponding probability of successful impersonation, since this only depends on the joint distribution of Y_y and Z_y (recall (2.3.1) and the definition of ϕ). We denote this probability by $P_I(y)$. Then from (2.3.1) it follows

$$P_I(y) = \max_{y' \neq y} P_{Z_y}(\mathcal{K}(y')) = \max_{y' \neq y} P_{Z|Y}(\mathcal{K}(y')|y) = P_S(y).$$

Hence, we can apply to $P_S(y)$ the lower bound from Theorem 32 and get

$$P_S(y) \geq 2^{-I(Y_y \wedge Z_y)}.$$

Therefore the next theorem is immediate.

Theorem 34 (Sgarro) *For every authentication code*

$$P_S \geq \sum_y P_Y(y)\, 2^{-I(Y_y \wedge Z_y)},$$

where Y_y and Z_y are defined in (2.3.4).

Remark 12 As already mentioned we can bound P_S by $2^{-H(Z|Y)}$ and given some value $y \in \mathcal{M}'$ we have $P_S(y) \geq 2^{-H(Z|Y=y)}$ (compare also Sect. 2.3.4). The bound just derived returns always values at least as good as this bound because by definition of Z_y we obtain

$$\begin{aligned} -I(Y_y \wedge Z_y) &= -H(Z_y) + H(Z_y|Y_y) \\ &= -H(Z|Y = y) + H(Z_y|Y_y) \geq -H(Z|Y = y). \end{aligned}$$

2.3.2 Authentication Codes Without Secrecy

Now we discuss authentication codes without secrecy, which means that the opponent knows the state of the message source after observing the correct cryptogram, i.e.,

$H(X|Y) = 0$. This applies to situations where secrecy is not required or can not be guaranteed (for instance if the opponent has full access to the message source) but the authenticity of messages is still desired.

Preliminaries

In those cases a convenient method of enciphering is the following. We consider only keys c_z which produce cryptograms y of the form

$$c_z(m) = y = (m, n),$$

where n is an extra symbol (string) dependent on m and z which is simply added to the clear message m. We can restrict ourselves, w.l.o.g., to this class of keys because if we are given an arbitrary set of K keys $\{c'_1, \ldots, c'_K\}$, we can define $c_z(m) \triangleq (m, c'_z(m))$ for all $z \in \{1, \ldots, K\},\ m \in \mathcal{M}$. This modification leads to a set of K keys $\{c_1, \ldots, c_K\}$ of the desired form and for the opponent the situation is as before since m was already uniquely determined by $c'_z(m)$.

Keys of this form have the property that for different messages the sets of possible cryptograms are always disjoint, i.e.,

$$c_i(m) \neq c_j(m') \quad \text{for all } i, j \in \{1, \ldots, K\},\ m, m' \in \mathcal{M},\ m \neq m'.$$

The second part n of such a cryptogram $y = (m, n)$ is the so called *authenticator* [12]. It is used by the receiver to check if he can accept the cryptogram as an authentic one. If the opponent is successful in an impersonation attack or in a substitution attack, respectively, he knows in addition to the general case also exactly to which message the receiver decrypts the fraudulent cryptogram.

For instance, in a substitution attack the opponent replaces the original cryptogram (m, n) by a fraudulent one (m', n') with $m' \neq m$. He will be successful if the secret key is also consistent with (m', n'), i.e., if $z \in \mathcal{K}((m', n'))$ (recall Definition 25) and $Z = z$. For ease of notation we will omit sometimes the brackets of (m, n). For instance, we write $\mathcal{K}(m, n) = \mathcal{K}((m, n))$ and for the success probability after observing the cryptogram $y = (m, n)$ we write $P_S(m, n)$ instead of $P_S((m, n))$ (recall Definition 25).

Note that for every message m the sets $\mathcal{K}(m, n)$ form a partition of $\{1, \ldots, K\}$, i.e., $\bigcup_n \mathcal{K}(m, n) = \{1, \ldots, K\}$ and the sets are disjoint.

We denote as $P_S(m', n', m, n)$ the probability of successful substitution of (m, n) with (m', n').

$$P_S(m', n', m, n) \triangleq \begin{cases} \frac{P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n'))}{P_Z(\mathcal{K}(m,n))}, & m' \neq m \\ 0, & m' = m. \end{cases} \tag{2.3.5}$$

For a chosen substitution strategy of the opponent $\{P_{Y'|Y}(\cdot\,|m, n) : (m, n) \in \mathcal{M}'\}$ (recall Definition 23) his success probability $P_{S,Y'}$ is given by

$$P_{S,Y'} \triangleq \sum_{m,n,m',n'} P_{Y'Y}(m',n',m,n)\, P_S(m',n',m,n). \tag{2.3.6}$$

From (2.3.5) and (2.3.6) it follows that an optimal strategy for the opponent is to select $(m^\star, n^\star)$ for given (m,n) such that

$$P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m^\star,n^\star)) = \max_{m' \neq m,\, n'} P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')), \tag{2.3.7}$$

i.e., an optimal strategy for the opponent is given by

$$P_{Y'|Y}(m',n'|m,n) = \begin{cases} 1, & \text{if } (m',n') = (m^\star,n^\star) \\ 0, & \text{otherwise,} \end{cases} \tag{2.3.8}$$

where $(m^\star, n^\star)$ is in each case the maximizer in (2.3.7) dependent on (m,n) (if $(m^\star,n^\star)$ is not unique, one can choose any of the maximizers).

We denote as $P_S(m)$ the probability of successful substitution if the message m occurs. Then with (2.3.5) and (2.3.8) it follows

$$\begin{aligned} P_S(m) &= \sum_n P_{Y|X}(m,n|m)\, P_S(m^\star,n^\star,m,n) \\ &= \sum_n P_Z(\mathcal{K}(m,n))\, P_S(m^\star,n^\star,m,n) = \sum_n P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m^\star,n^\star)), \end{aligned} \tag{2.3.9}$$

where $(m^\star, n^\star)$ is in each case the maximizer in (2.3.7) dependent on (m,n).

The Lower Bound on P_S in the Case of No Secrecy

The bound on P_S presented in Theorem 35 was first given by Gilbert, MacWilliams and Sloane and proved in [12] for the case of an equiprobable message distribution. It can be generalized to arbitrary distributions P_X with the property $P_X(m) \leq \frac{1}{2}$ for all $m \in \mathcal{M}$ as it was done by Bassalygo in [2]. We will present this derivation.

In order to get a lower estimate on P_S one can consider the following two strategies, which are not optimal in general. The strategies are described as follows. If the original cryptogram is (m,n) then in both strategies the message m', which shall be substituted for m, is chosen at random from the $M-1$ messages different from m (according to the uniform distribution). The two strategies differ only in the choice of n' given (m,n) and m'. In the first strategy n' is chosen with probability $\frac{P_S(m',n',m,n)}{\sum_{n''} P_S(m',n'',m,n)}$, i.e., the opponent uses as weights for the authenticators their success probabilities. In the second strategy n' is chosen optimal given (m,n) and m'.

To describe the strategies formally let Y_1' and Y_2' be the corresponding random variables for strategy 1 and 2, respectively. Then we define

$$P_{Y_1'|Y}(m',n'|m,n) \triangleq \frac{1}{M-1} \frac{P_S(m',n',m,n)}{\sum_{n''} P_S(m',n'',m,n)}$$

$$\text{and } P_{Y_2'|Y}(m', n'|m, n) \triangleq \begin{cases} \frac{1}{M-1}, & n' = n^\star \\ 0, & n' \neq n^\star, \end{cases}$$

where $n^\star$ is chosen for given m, n, m' in such a way that

$$P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n^\star)) = \max_{n'} P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n'))$$

(if $n^\star$ is not unique we choose any of the maximizers).

We denote as $P_{S,Y_1'}$ and $P_{S,Y_2'}$ the success probabilities for these strategies. It was shown in [12] that for equiprobable messages $P_S \geq P_{S,Y_2'} \geq 2^{-\frac{H(Z)}{2}} \geq \frac{1}{\sqrt{K}}$. To generalize this result for other distributions on $\mathcal{M}$ a lower bound on the sum of the probabilities of successful substitution of m with m' and m' with m for the first strategy, which is presented in the next lemma, is essential.

Definition 26 For any substitution strategy of the opponent and any two messages m and m' let $P_{S,Y'}(m', m)$ be the probability of successful substitution of message m with message m'.

Lemma 5 *For any two messages* $m, m' \in \mathcal{M},\ m \neq m'$

$$P_{S,Y_1'}(m', m) + P_{S,Y_1'}(m, m') \geq 2^{1-\frac{H(Z)}{2}}.$$

Proof Let $m, m' \in \mathcal{M},\ m \neq m'$. By (2.3.5) and the choice of Y_1' it follows that

$$\begin{aligned} P_{S,Y_1'}(m', m) &= \sum_n P_{Y|X}(m, n|m) \sum_{n'} \frac{P_S(m', n', m, n)}{\sum_{n''} P_S(m', n'', m, n)} P_S(m', n', m, n) \\ &= \sum_n P_Z(\mathcal{K}(m, n)) \sum_{n'} \frac{P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n'))^2}{P_Z(\mathcal{K}(m, n)) \sum_{n''} P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n''))} \\ &= \sum_{n,n'} \frac{P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n'))^2}{P_Z(\mathcal{K}(m, n))}, \end{aligned} \tag{2.3.10}$$

where we used in the last step that $\bigcup_{n''} \mathcal{K}(m', n'') = \{1, \ldots, K\}$ and the sets are disjoint.

Therefore,

$$P_{S,Y_1'}(m', m) + P_{S,Y_1'}(m, m')$$

$$= \sum_{n,n'} P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n'))^2 \left(\frac{1}{P_Z(\mathcal{K}(m, n))} + \frac{1}{P_Z(\mathcal{K}(m', n'))} \right).$$

As for every $a, b > 0$ $\frac{1}{a} + \frac{1}{b} \geq \frac{2}{\sqrt{ab}}$ (with equality iff $a = b$), we obtain

$$P_{S,Y_1'}(m', m) + P_{S,Y_1'}(m, m')$$

$$\geq 2 \sum_{n,n'} P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')) \frac{P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n'))}{\sqrt{P_Z(\mathcal{K}(m,n)) P_Z(\mathcal{K}(m',n'))}}.$$

Note that $\{1, \ldots, K\} = \bigcup_{n,n'} \mathcal{K}(m,n) \cap \mathcal{K}(m',n')$ and the sets are disjoint. Therefore $\sum_{n,n'} P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')) = 1$ and we can exploit the $\cap$-convexity of ln and get

$$\begin{aligned}
&\ln\left(P_{S,Y_1'}(m',m) + P_{S,Y_1'}(m,m')\right) \\
&\geq \ln 2 + \sum_{n,n'} P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')) \ln \frac{P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n'))}{\sqrt{P_Z(\mathcal{K}(m,n)) P_Z(\mathcal{K}(m',n'))}} \\
&= \ln 2 + \frac{1}{2} \sum_{n,n'} P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')) \ln P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')) \\
&\quad \underbrace{+ \frac{1}{2} \sum_{n,n'} P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')) \ln \frac{P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n'))}{P_Z(\mathcal{K}(m,n)) P_Z(\mathcal{K}(m',n'))}}_{\star} \\
&\geq \ln 2 + \frac{1}{2} \sum_{n,n'} P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')) \ln P_Z(\mathcal{K}(m,n) \cap \mathcal{K}(m',n')),
\end{aligned}$$

where we used in the last step that the term $\star$ is greater than or equal to 0, which follows from the inequality $\ln x \geq 1 - \frac{1}{x}$ (it can also be seen directly by the observation that the sum is up to a positive factor an I-divergence, which is always nonnegative).

Multiplying both sides of the inequality with $\log e$ and applying the grouping axiom of the entropy function yields the desired result.

$$\begin{aligned}
&\log\left(P_{S,Y_1'}(m',m) + P_{S,Y_1'}(m,m')\right) \\
&\geq \log 2 + \frac{1}{2} \sum_{z} P_Z(z) \log P_Z(z) = 1 - \frac{1}{2} H(Z).
\end{aligned}$$

□

Theorem 35 (Gilbert, Mac Williams, Sloane-Bassalygo) *If the distribution P_X satisfies $P_X(m) \leq \frac{1}{2}$ for all $m \in \mathcal{M}$, then*

$$P_S \geq 2^{-\frac{H(Z)}{2}} \geq \frac{1}{\sqrt{K}}.$$

Proof

$$P_S = \sum_{m\in\mathcal{M}} P_X(m)\, P_S(m) \geq \sum_{m\in\mathcal{M}} P_X(m) \max_{m'\neq m} P_{S,Y_1'}(m', m). \tag{2.3.11}$$

Let $q \triangleq \min_{m\in\mathcal{M}} \max_{m'\neq m} P_{S,Y_1'}(m', m)$.

If $q \geq 2^{-\frac{H(Z)}{2}}$, then we are done and, as we did not use any restriction on P_X in this case, the theorem is valid for any distribution P_X. So let us assume that $q < 2^{-\frac{H(Z)}{2}}$.

Let $m_0 \in \mathcal{M}$ be a message such that

$$q = \max_{m'\neq m_0} P_{S,Y_1'}(m', m_0)$$

and let $m \in \mathcal{M}$ be any message with $m \neq m_0$. Then from the definition of m_0 and Lemma 5 it follows that

$$q + \max_{m'\neq m} P_{S,Y_1'}(m', m) \geq P_{S,Y_1'}(m, m_0) + P_{S,Y_1'}(m_0, m) \tag{2.3.12}$$

$$\geq 2^{1-\frac{H(Z)}{2}}. \tag{2.3.13}$$

Hence, for all $m \in \mathcal{M}$ with $m \neq m_0$ we have

$$\max_{m'\neq m} P_{S,Y_1'}(m', m) \geq 2^{1-\frac{H(Z)}{2}} - q.$$

Together with (2.3.11) this implies

$$\begin{aligned} P_S &\geq P_X(m_0)\, q + (1 - P_X(m_0))(2^{1-\frac{H(Z)}{2}} - q) \\ &= (1 - P_X(m_0))2^{1-\frac{H(Z)}{2}} - q\underbrace{(1 - 2P_X(m_0))}_{\geq 0} \\ &\geq (1 - P_X(m_0))2^{1-\frac{H(Z)}{2}} - 2^{-\frac{H(Z)}{2}}(1 - 2P_X(m_0)) \\ &= 2^{1-\frac{H(Z)}{2}} - 2^{-\frac{H(Z)}{2}} = 2^{-\frac{H(Z)}{2}}. \end{aligned} \tag{2.3.14}$$

□

Impossibility of a Generalization

In this section we show that the constant $\frac{1}{2}$ in the assumptions of Theorem 35 is best possible, i.e., a generalization of the theorem in the form that the condition "$P_X(m) \leq \frac{1}{2}$ for all m" is weakened to "$P_X(m) \leq c$ for all m" where c is a constant $> \frac{1}{2}$ is not possible.

We need the following auxiliary result.

Lemma 6

$$\lim_{a\to\infty}\left(1+a-\sqrt{a^2+a}\right)=\frac{1}{2}$$

Proof

$$1+a-\sqrt{a^2+a}-\frac{1}{2}=\sqrt{a^2+a+\frac{1}{4}}-\sqrt{a^2+a}\geq 0$$

and on the other hand the $\cap$-convexity of the square-root function implies

$$\sqrt{a^2+a+\frac{1}{4}}-\sqrt{a^2+a}\leq\frac{1}{4}\,\frac{1}{2\sqrt{a^2+a}}.$$ □

Now let $a\in\mathbb{N}$. We define an authentication code with two messages, $\mathcal{M}\triangleq\{1,2\}$, and $K\triangleq a^2+a$ keys, which are chosen according to the uniform distribution.

The enciphering is defined by specifying the bundles $\mathcal{K}(m,n)$ in the following way:

$$\mathcal{K}(1,n)\triangleq\{(n-1)(a+1)+1,\ldots,n(a+1)\}$$

for all $n\in\{1,\ldots,a\}$ and

$$\mathcal{K}(2,n)\triangleq\{n,n+(a+1),n+2(a+1),\ldots,n+(a-1)(a+1)\}$$

for all $n\in\{1,\ldots,a+1\}$.

For the first message we have a bundles of cardinality $a+1$ and
for the second message we have $a+1$ bundles of cardinality a. Note that

$$|\mathcal{K}(1,n)\cap\mathcal{K}(2,n')|=|\{(n-1)(a+1)+n'\}|=1$$

for all $n\in\{1,\ldots,a\}$ and $n'\in\{1,\ldots,a+1\}$. Therefore we can easily calculate P_S. According to (2.3.9) we obtain

$$P_S(1)=\sum_{n=1}^{a}\frac{1}{K}=\frac{a}{a^2+a}=\frac{1}{a+1}$$

$$\text{and } P_S(2)=\sum_{n=1}^{a+1}\frac{1}{K}=\frac{a+1}{a^2+a}=\frac{1}{a}.$$

Let $c\triangleq P_X(1)$, then

$$P_S=c\frac{1}{a+1}+(1-c)\frac{1}{a}$$

and we have $P_S < \frac{1}{\sqrt{K}} = \frac{1}{\sqrt{a^2+a}}$, if $c\frac{1}{a+1} + (1-c)\frac{1}{a} < \frac{1}{\sqrt{a^2+a}}$ or equivalently

$$c > 1 + a - \sqrt{a^2 + a}.$$

Hence, with Lemma 6 we get that if $P_X(1) > \frac{1}{2}$, then for large enough a, we obtain $P_S < \frac{1}{\sqrt{K}}$.

Conditions for Equality

Now we concentrate on the case where P_Z is the uniform distribution. For this case necessary and sufficient conditions for the equality $P_S = \frac{1}{\sqrt{K}}$ were given in [12]. As there the bound was proved for equiprobable messages and the conditions were derived from that proof, we have to give a new proof which is based on our derivation on the bound on P_S. Therefore we will make use of two lemmas stated in [2].

Definition 27 For any message $m \in \mathcal{M}$ we denote by $\mathcal{N}(m) = \{n : (m, n) = c_z(m)$ for some $z \in \{1, \ldots, K\}\}$ the set of possible authenticators attached to message m.

Lemma 7 *For given P_Z and any two messages $m, m' \in \mathcal{M}$, $m \neq m'$*

$$P_{S,Y_1'}(m', m) \geq \frac{1}{|\mathcal{N}(m')|}.$$

Proof From the $\cup$-convexity of $x \mapsto x^2$ it follows that for any finite index set $\mathcal{I}$

$$\sum_{i \in \mathcal{I}} z_i^2 \geq \frac{1}{|\mathcal{I}|} \left(\sum_{i \in \mathcal{I}} z_i \right)^2, \tag{2.3.15}$$

with equality exactly if all z_i are equal. Applying this to (2.3.10) we obtain

$$\begin{aligned} P_{S,Y_1'}(m', m) &= \sum_{n \in \mathcal{N}(m)} \sum_{n' \in \mathcal{N}(m')} \frac{P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n'))^2}{P_Z(\mathcal{K}(m, n))} \\ &\geq \sum_{n \in \mathcal{N}(m)} \frac{1}{P_Z(\mathcal{K}(m, n))} \frac{1}{|\mathcal{N}(m')|} \left(\sum_{n' \in \mathcal{N}(m')} P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n')) \right)^2 \\ &= \sum_{n \in \mathcal{N}(m)} \frac{1}{|\mathcal{N}(m')|} P_Z(\mathcal{K}(m, n)) \\ &= \frac{1}{|\mathcal{N}(m')|}. \end{aligned}$$

□

Lemma 8 *If P_Z is the uniform distribution then for any two messages $m, m' \in \mathcal{M}$, with $m \neq m'$*

$$P_{S,Y_1'}(m', m) \geq \frac{|\mathcal{N}(m)|}{K}.$$

Proof

$$\begin{aligned} P_{S,Y_1'}(m', m) &= \sum_{n,n'} \frac{|\mathcal{K}(m, n) \cap \mathcal{K}(m', n')|^2}{K\,|\mathcal{K}(m, n)|} \\ &\geq \sum_{n} \sum_{n'} \frac{|\mathcal{K}(m, n) \cap \mathcal{K}(m', n')|}{K\,|\mathcal{K}(m, n)|} = \sum_{n \in \mathcal{N}(m)} \frac{1}{K} \\ &= \frac{|\mathcal{N}(m)|}{K}, \end{aligned}$$

with equality exactly if $|\mathcal{K}(m, n) \cap \mathcal{K}(m', n')| \leq 1$ for all n, n'. □

Now we can derive necessary and sufficient conditions that an authentication code achieves $P_S = \frac{1}{\sqrt{K}}$. These conditions are as follows:

1. $|\mathcal{N}(m)| = \sqrt{K}$ for all $m \in \mathcal{M}$.
2. $|\mathcal{K}(m, n) \cap \mathcal{K}(m', n')| = 1$ for all $m \neq m', n \in \mathcal{N}(m), n' \in \mathcal{N}(m')$.
3. $|\mathcal{K}(m, n)| = \sqrt{K}$ for all $m \in \mathcal{M},\ n \in \mathcal{N}(m)$.

Note that condition 1 and 2 imply condition 3 and therefore one could as well eliminate 3. from this list ($|\mathcal{K}(m, n)| = \sum_{n' \in \mathcal{N}(m')} |\mathcal{K}(m, n) \cap \mathcal{K}(m', n')| = \sum_{n' \in \mathcal{N}(m')} 1 = |\mathcal{N}(m')| = \sqrt{K}$).

Theorem 36 *Let P_Z be the uniform distribution. If conditions 1. and 2. are satisfied, then $P_S = \frac{1}{\sqrt{K}}$ and on the other hand if $P_S = \frac{1}{\sqrt{K}}$ and the assumption of Theorem 35 holds, then conditions 1. and 2. are satisfied.*

Proof First of all we show that condition 1. and 2. are sufficient. From (2.3.9) it follows that for every message $m \in \mathcal{M}$

$$\begin{aligned} P_S(m) &= \sum_{n} \sum_{\mathcal{K}(m,n) \cap \mathcal{K}(m^\star, n^\star)} \frac{1}{K} \\ &= |\mathcal{N}(m)|\,\frac{1}{K} = \frac{1}{\sqrt{K}}. \end{aligned}$$

Therefore also $P_S = \frac{1}{\sqrt{K}}$.

Now we show the necessity. Assume that $P_S = \frac{1}{\sqrt{K}}$.

Case 1: In the proof of Theorem 35 we have $q \geq \frac{1}{\sqrt{K}}$.

Then it follows

$$\max_{m' \neq m} P_{S,Y_1'}(m', m) = \frac{1}{\sqrt{K}} \qquad \text{for all } m \in \mathcal{M}.$$

Hence, for any $m' \neq m$ Lemma 7 implies

$$\frac{1}{\sqrt{K}} \geq P_{S,Y_1'}(m', m) \geq \frac{1}{|\mathcal{N}(m')|}.$$

Therefore $|\mathcal{N}(m)| \geq \frac{1}{\sqrt{K}}$ for all $m \in \mathcal{M}$ and Lemma 8 implies

$$\frac{1}{\sqrt{K}} = \max_{m' \neq m} P_{S,Y_1'}(m', m) \geq \frac{|\mathcal{N}(m)|}{K} \text{ for all } m \in \mathcal{M}.$$

Hence, we also have $|\mathcal{N}(m)| \leq \frac{1}{\sqrt{K}}$ for all $m \in \mathcal{M}$ and therefore $|\mathcal{N}(m)| = \frac{1}{\sqrt{K}}$ for all $m \in \mathcal{M}$. Furthermore Lemmas 7 and 8 hold with equality for every $m, m', m \neq m'$. Thus, the corresponding conditions for equality imply $|\mathcal{K}(m, n) \cap \mathcal{K}(m', n')| = 1$ for all $m \neq m', n \in \mathcal{N}(m), n' \in \mathcal{N}(m')$, which shows that conditions 1. and 2. are satisfied.

Case 2: $q < \frac{1}{\sqrt{K}}$.

Then in the proof of Theorem 35 for every $m \neq m_0$, (2.3.14) implies that equality holds in (2.3.12) and (2.3.13), i.e.,

$$\max_{m' \neq m_0} P_{S,Y_1'}(m', m_0) + \max_{m' \neq m} P_{S,Y_1'}(m', m)$$

$$= P_{S,Y_1'}(m, m_0) + P_{S,Y_1'}(m_0, m) = \frac{2}{\sqrt{K}}.$$

Then Lemma 7 implies $\frac{1}{\sqrt{K}} > q = P_{S,Y_1'}(m, m_0) \geq \frac{1}{|\mathcal{N}(m)|}$ or

$$|\mathcal{N}(m)| > \sqrt{K}$$

and Lemma 8 implies $\frac{1}{\sqrt{K}} > P_{S,Y_1'}(m, m_0) \geq \frac{|\mathcal{N}(m_0)|}{K}$ or

$$|\mathcal{N}(m_0)| < \sqrt{K}.$$

Together we have

$$|\mathcal{N}(m_0)| < |\mathcal{N}(m)|. \tag{2.3.16}$$

But note that for m and m_0 Lemma 5 holds with equality. For instance, the first inequality in the proof of this lemma must hold with equality and this means:

$$\text{If } \mathcal{K}(m_0, n) \cap \mathcal{K}(m, n') \neq \emptyset, \text{ then } |\mathcal{K}(m_0, n)| = |\mathcal{K}(m, n')|,$$

for all $m, n' \in \mathcal{N}(m), n \in \mathcal{N}(m_0)$.

As this is a contradiction to (2.3.16), we see that if $P_S = \frac{1}{\sqrt{K}}$, then $q \geq \frac{1}{\sqrt{K}}$ and therefore conditions 1. and 2. are necessarily satisfied. □

A Construction

We will come now to a construction which is taken from [12]. We will define an authentication code which achieves $P_S = \frac{1}{\sqrt{K}}$ (for certain values of K) and possesses the maximal possible number of messages under that constraint.

In order to see what is the maximal number of messages M, assume that we are given an authentication code with $P_S = \frac{1}{\sqrt{K}}$. Then we know that conditions 1. and 2. (and therefore also 3.) are satisfied. Now we list all unordered pairs of key-indices which are together in some bundle $\mathcal{K}(m, n)$, where $m \in \mathcal{M}, n \in \mathcal{N}(m)$. As we have M messages, $\sqrt{K}$ bundles for each message and $\sqrt{K}$ elements in each bundle, we get with this procedure $M\sqrt{K}\binom{\sqrt{K}}{2}$ pairs. Condition 2. implies that all these pairs are different and therefore their number must be less or equal the total number of unordered pairs of key-indices. This shows that

$$M\sqrt{K}\binom{\sqrt{K}}{2} \leq \binom{K}{2} \text{ or equivalently } M \leq \sqrt{K} + 1. \tag{2.3.17}$$

Our construction applies for the case that K is an even prime power. So, let us assume that $K = p^{2k}$ where p is prime and $k \in \mathbb{N}$. We make use of the projective plane constructed from $GF(q)$, where $q = p^k$. This has

- $q^2 + q + 1$ points
- $q^2 + q + 1$ lines
- $q + 1$ points on each line
- $q + 1$ lines through each point.

Recall that for every projective plane two different lines intersect in exactly one point and two different points uniquely determine a line, on which both points lie.

We select arbitrarily a line to play a special role. According to [12] we call this line the equator. The points on the equator represent the messages. All other points in the projective plane represent the keys ($K = q^2 + q + 1 - (q + 1) = q^2 = p^{2k}$). Then a message and a key uniquely determine a line through their representations in the projective plane. Therefore this line will stand for the cryptogram to which the message is encrypted using the key. From now on we will make no difference anymore between message, key, cryptogram and their representation in the projective plane.

This authentication system provides no secrecy as a cryptogram and the equator intersect in exactly one point, which is therefore the encrypted message.

In order to see if $P_S = \frac{1}{\sqrt{K}}$, we have to check if conditions 1. and 2. are satisfied:

1. As through the point m we have $q + 1$ lines of which one is the equator, it follows

$$|\mathcal{N}(m)| = q + 1 - 1 = q = \sqrt{K}.$$

2. Let $m \neq m'$, $n \in \mathcal{N}(m)$, $n' \in \mathcal{N}(m')$. The lines (m, n) and (m', n') are different (if not m and m' would lie on this line and therefore (m, n) and (m', n') would be the equator, which is impossible). Hence, there is exactly one intersection point of the lines (m, n) and (m', n') (which again cannot lie on the equator because $m \neq m'$) and we obtain

$$|\mathcal{K}(m, n) \cap \mathcal{K}(m', n')| = 1.$$

Therefore the authentication code satisfies conditions 1. and 2. and we have $P_S = \frac{1}{\sqrt{K}}$. Note that equality holds in (2.3.17),

$$M = q + 1 = \sqrt{K} + 1.$$

2.3.3 *Estimates on the Number of Messages Given the Success Probability of the Opponent*

In this section we ask how many messages can be included in an authentication code under some constraints on the success probabilities of the opponent. We saw in the last section that a first result for this sort of question was already given in [12]. In [3] Bassalygo and Burnashev considered the case of authentication codes without secrecy. These results will be presented in Section "The Number of Messages for Authentication Codes Without Secrecy Given the Probability of Deception". Recently they gave in [4] an approach for the problem under a slightly modified constraint by connecting it to the problem of identification and the problem of the maximal cardinality of pairwise separated measures in the L_1-metric. This approach includes also cases of authentication codes without secrecy. We present the results relevant for the authentication problem in the Section on "Pairwise Separated Measures".

The Number of Messages for Authentication Codes Without Secrecy Given the Probability of Deception

Definition 28 Let $P_S^{max} \triangleq \max_{m \in \mathcal{M}} P_S(m)$ denote the maximal probability of successful substitution.

Burnashev and Bassalygo [3] require for the authentication codes under consideration to have the property that P_S^{max} does not exceed some given (usually small) constant $p \geq 0$ and ask for the maximal number of messages under this constraint. This requirement can be justified because an authentication code with $P_S^{max} \leq p$ has

the property $P_D \leq p$ as well. Clearly, if $P_S^{max} \leq p$, then also $P_S \leq p$ but this holds for P_I as well, which is shown in the next theorem.

Theorem 37 *For any authentication code without secrecy*

$$P_S^{max} \geq P_I. \tag{2.3.18}$$

Proof Let $m_0 \in \mathcal{M}$ and $n_0 \in \mathcal{N}(m_0)$ such that (m_0, n_0) is an optimal choice for the impersonation attack, i.e.,

$$P_I = \Pr((m_0, n_0) \text{ valid}) = P_Z(\mathcal{K}(m_0, n_0)).$$

Now the idea is to bound for any $m \neq m_0$ the value of $P_S(m)$ below by choosing the strategy to substitute always (m_0, n_0). Let $m \in \mathcal{M},\ m \neq m_0$. Then with (2.3.9) it follows

$$P_S(m) \geq \sum_{n \in \mathcal{N}(m)} P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m_0, n_0)).$$

Therefore, as $\{\mathcal{K}(m, n) : n \in \mathcal{N}(m)\}$ is a partition of $\{1, \ldots, K\}$, we obtain

$$P_S(m) \geq P_Z(\mathcal{K}(m_0, n_0)) = P_I.$$

Hence, the statement follows from $P_S^{max} \geq P_S(m) \geq P_I$. □

Remark 13 We have seen in Example 3 that there are authentication codes (with secrecy) for which the statement (2.3.18) does not hold.

Corollary 2 *If for an authentication code without secrecy there exist* $m_0, m_1 \in \mathcal{M},\ m_0 \neq m_1$ *and* $n_0 \in \mathcal{N}(m_0),\ n_1 \in \mathcal{N}(m_1)$ *such that* $P_I = P_Z(\mathcal{K}(m_0, n_0)) = P_Z(\mathcal{K}(m_1, n_1))$*, i.e., if the optimal choice for an impersonation attack is not unique with respect to messages, then*

$$P_S \geq P_I.$$

Proof In this case it follows directly from the proof of Theorem 37 that for any $m \in \mathcal{M}$ we have that $P_S(m) \geq P_I$ and therefore $P_S = \sum_{m \in \mathcal{M}} P_X(m)\, P_S(m) \geq P_I$. □

Clearly P_S^{max} depends on the number of messages M, the definition of the K keys in $\mathcal{C}$ and the distribution P_Z, i.e., $P_S^{max} = P_S^{max}(M, \mathcal{C}, P_Z)$. If the parameters M, K and P_Z are given, then sender and receiver try to minimize P_S^{max} by using the K keys in the best possible way. Therefore it is natural to introduce the minimal achievable probability $p(M, K, P_Z)$ of successful substitution as

$$p(M, K, P_Z) \triangleq \min_{\mathcal{C}} P_S^{max}(M, \mathcal{C}, P_Z).$$

Now the question is how large can M be if K and P_Z are given and we require that $p(M, K, P_Z)$ does not exceed a given value p. The maximal M with this property will be denoted as

$$M(K, P_Z, p).$$

In other words if $M \leq M(K, P_Z, p)$, then there exists $\mathcal{C} = \{c_1, \ldots, c_K\}$ with P_S^{max} $(M, \mathcal{C}, P_Z) \leq p$.

If P_Z is the uniform distribution, $M(K, P_Z, p)$ will be denoted as

$$M_e(K, p).$$

As $P_S^{max} \geq \frac{1}{\sqrt{K}}$, we have to analyze the cases where $Kp^2 \geq 1$. We saw in Section "A Construction" that $M_e(K, \frac{1}{\sqrt{K}}) = \sqrt{K} + 1$, if K is an even prime power. Burnashev and Bassalygo studied in [3] the asymptotic behaviour of $M(K, P_Z, p)$ for large values of $K p^2$ and gave the following results.

Theorem 38 *For* $0 < p \leq \frac{1}{2}$ *the following inequality holds*

$$\log M_e(K, p) \geq \frac{K p^2}{8} + 2 \log p - 6.2\,.$$

Theorem 39 *For* $0 < p < 1$ *the following inequality holds*

$$\log M(K, P_Z, p) \leq 64\, K\, p^2 \log \frac{2}{p} + 2 \log K.$$

Derivation of the Lower Bound The lower bound will be proved by a construction. The idea is the following. For given $\mathcal{C}$, every message $m \in \mathcal{M}$ induces a partition of the set $\{1, \ldots, K\}$ into sets $\mathcal{K}(m, n)$, $n \in \mathcal{N}(m)$. If we have equiprobable keys, (2.3.9) implies that a "rather good" authentication code (with small P_S^{max}) must have the property that all the intersections of partition elements of the different partitions are sufficiently small.

$\mathcal{C}$ is completely determined by specifying partitions of $\{1, \ldots, K\}$ for each message. We do this by dividing the set $\{1, \ldots, K\}$ for every message $m \in \mathcal{M}$ into sets of cardinality a (the parameter a will be chosen later and we assume for the moment that $\frac{K}{a}$ is an integer). With this property each of our partitions has $\frac{K}{a}$ elements and we want to form the partitions additionally in such a way that the following condition is satisfied.

Any two elements of any two different partitions have no more than ap_0 *common elements.*

Here $0 < p_0 < p \leq \frac{1}{2}$ is a parameter, which will be chosen later. We will refer to these properties by saying that a collection of partitions satisfies the intersection property.

After adjusting the parameters we will have to show that our construction leads to an authentication code with the desired property $P_S^{max} \leq p$ but first of all, in order to get a bound on M we ask how many partitions of the described form we can find. Let $N(K, a)$ denote the number of all possible partitions of the set $\{1, \ldots, K\}$ into sets with a elements. Clearly, we have

$$N(K,a) = \frac{\binom{K}{a}\binom{K-a}{a}\cdots\binom{a}{a}}{\left(\frac{K}{a}\right)!}. \tag{2.3.19}$$

If M is the maximal number of partitions with the intersection property, then

$$N(K,a) \le M\,\frac{K}{a}\,N(K-a,a)\sum_{i=i_0}^{a}\binom{a}{i}\binom{K-a}{a-i}, \tag{2.3.20}$$

where i_0 is the smallest integer strictly greater than ap_0.

The validity of this inequality can be seen as follows. Take a maximal collection of partitions with the intersection property. The maximality implies that if we take any of the $N(K,a)$ partitions we find an element in it and an element of one of the partitions of our maximal collection such that they have more than ap_0 common elements. Therefore we can get any of the $N(K,a)$ partitions by a transformation of a partition of the maximal collection in the following way. First we choose one of the M partitions from which we choose one of its $\frac{K}{a}$ partition elements. From the a elements of this set we keep i in it ($i \ge i_0$) and exchange the remaining $a-i$ with some of the $K-a$ other elements. Then the other partition elements are formed from the $K-a$ remaining elements.

The right-hand side of the inequality (2.3.20) counts the number of such transformations.

From (2.3.20) we get a lower bound on M, which is

$$M \ge \frac{a\,N(K,a)}{K\,N(K-a,a)\sum_{i=i_0}^{a}\binom{a}{i}\binom{K-a}{a-i}} = \frac{a^2\binom{K}{a}}{K^2\sum_{i=i_0}^{a}\binom{a}{i}\binom{K-a}{a-i}}.$$

Now we use the following inequality which can easily be verified[2]

$$\frac{\binom{K-a}{a-i}}{\binom{K}{a}} \le \left(\frac{K-a}{K}\right)^{a-i}\left(\frac{a}{K-a}\right)^{i}$$

and we obtain

$$M \ge \frac{a^2}{K^2\sum_{i=i_0}^{a}\binom{a}{i}\left(\frac{K-a}{K}\right)^{a-i}\left(\frac{a}{K-a}\right)^{i}} = \frac{a^{2-a}(K-a)^a}{K^2\sum_{i=i_0}^{a}\binom{a}{i}\left(\frac{(K-a)^2}{aK}\right)^{a-i}}$$

2

$$\frac{\binom{K-a}{a-i}}{\binom{K}{a}} = \underbrace{\frac{K-a}{K}\cdots\frac{K-2a+i+1}{K-a+i+1}}_{a-i\text{ factors}}\underbrace{\frac{a}{K-a+i}\cdots\frac{a-i+1}{K-a+1}}_{i\text{ factors}} \le \left(\frac{K-a}{K}\right)^{a-i}\left(\frac{a}{K-a}\right)^{i}.$$

$$= \frac{a^{2-a}(K-a)^a}{K^2 \sum_{j=0}^{a-i_0} \binom{a}{j} \left(\frac{aK}{(K-a)^2}\right)^{-j}}.$$

Further we use the inequality

$$\sum_{j=0}^{b} \binom{a}{j} z^{-j} \le z^{-b} \exp\left(a\, h\left(\frac{b}{a}\right)\right) \text{ for } 0 < z \le \frac{a-b}{b},\ b \le a,$$

which holds because for any $0 < x \le 1$

$$\sum_{j=0}^{b} \binom{a}{j} z^{-j} \le \frac{1}{x^b} \sum_{j=0}^{b} \binom{a}{j} \left(\frac{x}{z}\right)^j \le \frac{1}{x^b} \sum_{j=0}^{a} \binom{a}{j} \left(\frac{x}{z}\right)^j = \frac{1}{x^b} \left(1 + \frac{x}{z}\right)^a$$

and with the substitution $x = \frac{bz}{a-b}$ we get

$$= \frac{1}{z^b} \left(\frac{a-b}{b}\right)^b \left(\frac{a}{a-b}\right)^a = \frac{1}{z^b} \exp(a\, h(\frac{b}{a})).$$

In our case the condition $z \le \frac{a-b}{b}$ turns out to be

$$\frac{aK}{(K-a)^2} \le \frac{i_0}{a-i_0}, \tag{2.3.21}$$

which we have to check after our choice of the parameters. If it holds we can bound M by

$$\begin{aligned} M &\ge \frac{a^{2-a} \left(\frac{(K-a)^2}{aK}\right)^{i_0-a} (K-a)^a}{K^2 \exp\left(a\, h\left(\frac{a-i_0}{a}\right)\right)} \\ &\ge \frac{a^{2-a} \left(\frac{(K-a)^2}{aK}\right)^{ap_0-a} (K-a)^a}{K^2 \exp\left(a\, h(p_0)\right)} \\ &= \frac{a^2}{K^2} \exp\left(a \underbrace{(1-2p_0)}_{\ge 0} \log \frac{K}{K-a} + ap_0 \log \frac{K}{a} - a\, h(p_0)\right) \\ &\ge \frac{a^2}{K^2} \exp\left(ap_0 \log \frac{Kp_0}{ae}\right), \end{aligned} \tag{2.3.22}$$

Now we pass to the general case, where K is not necessarily a multiple of a.

Let

$$p_0 \triangleq \frac{pe^2}{1+e^2} \quad \text{and} \quad a \triangleq \left\lceil \frac{pK}{1+e^2} \right\rceil.$$

Let $K_0 \le K$ be the largest integer divisible by a, i.e., $K_0 \triangleq \left\lfloor \frac{K}{a} \right\rfloor a$. Now we define $\mathcal{C}$ by choosing the partitions as follows. We select an arbitrary subset of $\{1, \ldots, K\}$ with $K - K_0$ elements to form a partition element for every partition. From the remaining K_0 elements of $\{1, \ldots, K\}$ we form a collection of partitions such that the intersection property holds.

First of all we show that the resulting authentication code possesses the desired property $P_S^{max} \le p$. Let $m \in \mathcal{M}$. Then

$$P_S(m) = \sum_n \frac{1}{K} \left| \mathcal{K}(m,n) \cap \mathcal{K}(m^\star, n^\star) \right| \le \frac{K - K_0}{K} + \frac{K_0}{a} \cdot \frac{ap_0}{K}.$$

By definition of K_0 we have $K - K_0 \le a - 1$ and therefore

$$P_S(m) \le \frac{a-1}{K} + \frac{K_0}{K} p_0 \le \frac{a-1}{K} + p_0 \le \frac{pK}{K(1+e^2)} + \frac{pe^2}{1+e^2} = p.$$

In order to apply our estimate for M we have to check if (2.3.21) is satisfied. W.l.o.g. we may assume that $pK > 70$ (see (2.3.25)). Then $a = \lceil \frac{p_0 K}{e^2} \rceil \le \frac{p_0 K}{e}$ and $\frac{K_0}{K} = \lfloor \frac{K}{a} \rfloor \frac{a}{K} \ge 1 - \frac{a}{K} \ge 1 - \frac{p_0}{e}$. Therefore

$$\frac{aK_0}{(K_0 - a)^2} \le \frac{\frac{p_0}{e}}{(\frac{K_0}{K} - \frac{p_0}{e})^2} \le \frac{\frac{p_0}{e}}{(1 - 2\frac{p_0}{e})^2} \le \frac{p_0}{1 - p_0} \le \frac{i_0}{a - i_0},$$

where we used that $p_0 \le \frac{1}{2}$ and $ap_0 \le i_0$. As (2.3.21) holds the number $M_e(K,p)$ must satisfy the last inequality for M, which is (2.3.22), with K replaced by K_0, i.e.,

$$\begin{aligned} M_e(K,p) &\ge \frac{a^2}{K_0^2} \exp\left(ap_0 \log \frac{K_0 p_0}{ae} \right) \\ &\ge \frac{p^2}{(1+e^2)^2} \exp\left(\frac{pK}{1+e^2} \cdot \frac{pe^2}{1+e^2} \log \frac{K_0 pe}{a(1+e^2)} \right) \\ &= \frac{p^2}{(1+e^2)^2} \exp\left(\frac{Kp^2e^2}{(1+e^2)^2} \log \frac{1}{z} \right), \end{aligned} \tag{2.3.23}$$

with $z \triangleq \frac{a(1+e^2)}{K_0 pe}$.

The value z satisfies the following inequalities

$$z = \frac{\left\lceil \frac{pK}{1+e^2} \right\rceil (1+e^2)}{K_0 pe} \geq \frac{K}{K_0 e} \geq \frac{1}{e}$$

and

$$\begin{aligned} z &\leq \frac{\left(\frac{pK}{1+e^2}+1\right)(1+e^2)}{K_0 pe} = \frac{1}{e} \cdot \frac{1+\frac{1+e^2}{pK}}{1-\frac{K-K_0}{K}} \\ &\leq \frac{1}{e} \cdot \frac{1+\frac{1+e^2}{pK}}{1-\frac{a-1}{K}} \leq \frac{1}{e} \cdot \frac{1+\frac{1+e^2}{pK}}{1-\frac{p}{1+e^2}}. \end{aligned}$$

Combining these two inequalities, yields

$$\frac{1}{e} \leq z \leq \frac{1}{e} \cdot \frac{1+\frac{1+e^2}{pK}}{1-\frac{p}{1+e^2}} \tag{2.3.24}$$

and as $\log \frac{1}{z}$ is monotonically decreasing in z, it attains its minimal value at the right-hand side of (2.3.24). Substituting this into (2.3.23) we get

$$M_e(K,p) \geq \frac{p^2}{(1+e^2)^2} \exp\left(\frac{Kp^2e^2}{(1+e^2)^2}(\log e)\left(1+\ln\frac{1-\frac{p}{1+e^2}}{1+\frac{1+e^2}{pK}}\right)\right).$$

Taking the logarithm on both sides of the inequality we get that if $pK > 70$ and $p \leq \frac{1}{2}$

$$\begin{aligned} \log M_e(K,p) &\geq 2\log p - \underbrace{2\log(1+e^2)}_{\approx 6.14} + Kp^2 \underbrace{\frac{e^2 \log e}{(1+e^2)^2}\left(1+\ln\frac{1-\frac{\frac{1}{2}}{1+e^2}}{1+\frac{1+e^2}{70}}\right)}_{\approx 0.12502} \\ &\geq \frac{Kp^2}{8} + 2\log p - 6.2. \end{aligned}$$

If $pK \leq 70$, the statement is trivial because in this case

$$\exp\left(\frac{Kp^2}{8} - 6.2\right)p^2 \leq \exp\left(\frac{70}{16} - 6.2\right) \leq 0.3. \tag{2.3.25}$$

Hence, the proof of Theorem 38 is complete.

Derivation of the Upper Bound First of all we will derive an upper bound for $M_e(K,p)$ and then generalize this bound to arbitrary key distributions P_Z.

Let us assume we are given an authentication code with $P_S^{max} \leq p$. As we have seen before every message $m \in \mathcal{M}$ induces a partition of $\{1, \ldots, K\}$ into sets $\mathcal{K}(m, n)$. Every such partition element must have a cardinality less than pK. Assume on the contrary that $|\mathcal{K}(m, n)| > pK$ for some $m \in \mathcal{M}, n \in \mathcal{N}(m)$. Then for any $m' \in \mathcal{M}$ with $m' \neq m$ we would have $P_S(m') \geq \sum_{n'} \frac{1}{K} |\mathcal{K}(m', n') \cap \mathcal{K}(m, n)| = \frac{1}{K} |\mathcal{K}(m, n)| > p$, which is a contradiction.

Moreover, there exists for every message $m \in \mathcal{M}$ a certain element $\mathcal{A}_m$ of the corresponding partition with the property that the cardinality of the intersection of $\mathcal{A}_m$ with any element of any other partition does not exceed $p|\mathcal{A}_m|$. This follows from the next lemma.

Lemma 9 *If for an authentication code without secrecy $P_S^{max} \leq p$, then for every $m \in \mathcal{M}$ there exists $n \in \mathcal{N}(m)$ with the property*

$$P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n')) \leq p\, P_Z(\mathcal{K}(m, n)) \qquad \text{for any } m' \neq m, n' \in \mathcal{N}(m').$$

Proof Assume on the contrary that for $m \in \mathcal{M}$ there exists no such $\mathcal{K}(m, n)$. This means that for every $n \in \mathcal{N}(m)$ there exists $m' \in \mathcal{M} \quad m' \neq m$ and $n' \in \mathcal{N}(m')$ such that $P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n')) > p\, P_Z(\mathcal{K}(m, n))$. Therefore we get by substituting (m, n) with (m', n') the desired contradiction $P_S(m) > \sum_n p\, P_Z(\mathcal{K}(m, n)) = p$. □

From the obtained set $\{\mathcal{A}_m : m \in \mathcal{M}\}$ we can take out a maximal subset $\{\mathcal{A}_{m_1}, \ldots, \mathcal{A}_{m_N}\}$ such that all the $\mathcal{A}_{m_i}$ have the same cardinality. We denote this cardinality by w. Then this subset has the following properties:

1. $|\mathcal{A}_{m_i}| = w \leq \lfloor pK \rfloor \quad$ for all $i = 1, \ldots, N$.
2. $|\mathcal{A}_{m_i} \cap \mathcal{A}_{m_j}| \leq \lfloor pw \rfloor \quad$ for all $i, j = 1, \ldots, N \quad i \neq j$.
3. $N \geq \frac{M}{pK}$.

Properties 1 and 2 are clear by construction of the set $\{\mathcal{A}_{m_1}, \ldots, \mathcal{A}_{m_N}\}$. Property 3 follows from the fact that all the sets $\mathcal{A}_m$ have cardinalities less than pK and the number of sets $\mathcal{A}_m$ with some same cardinality is less than N. Therefore $N \cdot pK \geq M$.

We can also give an upper bound for N, which is well known in coding theory and combinatorics (see the remark below) but we will give its derivation here. Let $l \triangleq \lfloor pw \rfloor$ and let $t > l$. Then property 2 implies that all possible subsets of the sets $\mathcal{A}_{m_1}, \ldots, \mathcal{A}_{m_N}$, which have t elements, are different. Therefore the total number of subsets obtained in this way is less than the total number of t-elementary subsets of $\{1, \ldots, K\}$, i.e., $N \cdot \binom{w}{t} \leq \binom{K}{t}$, or

$$N \leq \frac{\binom{K}{t}}{\binom{w}{t}} \qquad \text{for all } t > l.$$

As the right hand side attains its minimal value for $t = l + 1$ we obtain

$$N \leq \frac{K(K-1)\cdots(K-l)}{w(w-1)\cdots(w-l)}. \tag{2.3.26}$$

Remark 14 If we consider the characteristic vectors of the sets $\mathcal{A}_{m_i}$, then we obtain a constant weight code with weight w and Hamming distance between the codewords at least $2(w-l)$. The upper bound in (2.3.26) is nothing else than the Johnson bound (see [17], pp. 527) for the cardinality of such a code.

If we combine the two estimates for N ((2.3.26) and property 3.) we get an upper bound for M. As we do not know the concrete value of w we maximize over w.

$$\begin{aligned} M &\le pK \max_{1\le w\le pK} \frac{K(K-1)\cdots(K-l)}{w(w-1)\cdots(w-l)} \\ &\le pK \max_{1\le w\le pK} \frac{K}{w}\cdot\left(\frac{K-l}{w-l}\right)^{l} \\ &\le pK^2 \max_{1\le w\le pK} \left(\frac{K-pw}{w-pw}\right)^{pw} \\ &= pK^2 \exp\left(p \max_{1\le w\le pK} w\log\frac{K-pw}{w-pw}\right). \end{aligned}$$

The maximized function is $\cap$-convex in w and the first derivative is positive at $w = pK$ provided that $p \le 0.42$. Hence, in this case the function attains its maximum at $w = pK$. By substituting this into the last term we obtain the following Proposition.

Proposition 3 *If $p \le 0.42$, then the following inequality holds*

$$M_e(K,p) \le pK^2 \exp\left(Kp^2 \log\frac{1+p}{p}\right).$$

Now we would like to transform this result to the case of an arbitrary key distribution P_Z.

Definition 29 If P_Z is the uniform distribution then let

$$p_e(M,K) \triangleq p(M,K,P_Z)$$

and let $p(M,K)$ denote the minimal achievable probability of successful substitution for K keys and M messages, i.e.,

$$p(M,K) \triangleq \min_{P_Z} p(M,K,P_Z).$$

Lemma 10 *Let $\mathcal{K} \subset \{1,\ldots,K\}$ with $|\mathcal{K}| = N$. Then the following statements hold.*

(a)

$$p(M,K,P_Z) \ge P_Z(\mathcal{K})\, p(M,N).$$

(b) If P_Z satisfies also the condition $P_Z(z) \geq \beta$ for all $z \in \mathcal{K}$, then

$$p(M, K, P_Z) \geq \beta N \, p_e(M, N).$$

Proof We start with (a). Recall that

$$p(M, K, P_Z) = \min_{\mathcal{C}} P_S^{max}(M, \mathcal{C}, P_Z). \tag{2.3.27}$$

Let $\mathcal{C}$ be a minimizer in (2.3.27). Then for all $m \in \mathcal{M}$ it follows

$$p(M, K, P_Z) \geq P_S(m) \geq \sum_n P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n'))$$

where $m' = m'(m, n) \neq m$ and $n' = n'(m, n)$ are chosen according to some not necessarily optimal decision rule. Hence,

$$p(M, K, P_Z) \geq P_Z(\mathcal{K}) \sum_n \frac{P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n') \cap \mathcal{K})}{P_Z(\mathcal{K})}$$

Let $\mathcal{C}' \subset \mathcal{C}$ be the subset of keys with index in $\mathcal{K}$. If we take for $m'(m, n)$ and $n'(m, n)$ the opponents's optimal decision rule for the authentication code, where the keys are chosen from $\mathcal{C}'$ according to the distribution $\frac{P_Z(\cdot)}{P_Z(\mathcal{K})}$, then we can conclude from the last inequality and the definition of $p(M, N)$ that

$$\begin{aligned} p(M, K, P_Z) &\geq P_Z(\mathcal{K}) \, P_S^{max}(M, \mathcal{C}', \frac{P_Z(\cdot)}{P_Z(\mathcal{K})}) \\ &\geq P_Z(\mathcal{K}) \, p(M, N, \frac{P_Z(\cdot)}{P_Z(\mathcal{K})}) \geq P_Z(\mathcal{K}) \, p(M, N), \end{aligned}$$

which completes the proof of (a).

Now we prove (b). Let $\mathcal{C}$ be a minimizer in (2.3.27) again. Then

$$\begin{aligned} p(M, K, P_Z) = P_S^{max}(M, \mathcal{C}, P_Z) &\geq \max_{m \in \mathcal{M}} \sum_n P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n')) \\ &\geq \max_{m \in \mathcal{M}} \sum_n P_Z(\mathcal{K}(m, n) \cap \mathcal{K}(m', n') \cap \mathcal{K}) \\ &\geq \beta N \max_{m \in \mathcal{M}} \sum_n \frac{|\mathcal{K}(m, n) \cap \mathcal{K}(m', n') \cap \mathcal{K}|}{N} \end{aligned}$$

and if $m'(m, n)$ and $n'(m, n)$ are chosen such that the last expression is maximized, then we obtain

$$p(M, K, P_Z) \geq \beta N p_e(M, N). \qquad \square$$

In order to prove Theorem 39 we will derive a sequence of upper bounds for $M(K, P_Z, p)$ and in the limit we get the bound of the theorem.

Let us start with the following result.

Proposition 4 *The following statements hold.*

(a) If $M \geq 2^K$ then $p(M, K) = 1$.
(b) If $0 < p < 1$ then for arbitrary P_Z

$$\lfloor \log M(K, P_Z, p) \rfloor \leq Kp.$$

Proof Let $M \geq 2^K$ and suppose $P_S(m) \leq p$ for all $m \in \mathcal{M}$ and some $p \leq 1$. In order to prove (a) we have to show that $p = 1$.

We know from Lemma 9 that for every $m \in \mathcal{M}$ there exists an element $\mathcal{A}_m$ of the corresponding partition with $P_Z(\mathcal{A}_m \cap \mathcal{K}(m', n')) \leq p P_Z(\mathcal{A}_m)$ for any $m' \neq m$ and $n' \in \mathcal{N}(m')$.

In particular we have

$$P_Z(\mathcal{A}_m \cap \mathcal{A}_{m'}) \leq p P_Z(\mathcal{A}_m) \qquad \text{for all } m' \neq m.$$

As there are $2^K - 1$ nonempty subsets of $\{1, \ldots, K\}$ and as $M > 2^K - 1$ we can find $m' \neq m$ with $\mathcal{A}_m = \mathcal{A}_{m'}$. If $p < 1$, then it follows

$$P_Z(\mathcal{A}_m) = P_Z(\mathcal{A}_m \cap \mathcal{A}_{m'}) \leq p P_Z(\mathcal{A}_m) < P_Z(\mathcal{A}_m)$$

which is a contradiction and therefore necessarily $p = 1$.

In order to prove (b) let $\mathcal{K} \subset \{1, \ldots, K\}$ be the subset with the $\lfloor \log M \rfloor$ most probable key-indices. Then we apply part (a) of Lemma 10 and get

$$p(M, K, P_Z) \geq P_Z(\mathcal{K})\, p(M, \lfloor \log M \rfloor).$$

By the choice of $\mathcal{K}$ it follows that $P_Z(\mathcal{K}) \geq \frac{\lfloor \log M \rfloor}{K}$ and we have already proved in (a) that $p(M, \lfloor \log M \rfloor) = 1$. Therefore

$$\lfloor \log M \rfloor \leq K\, p(M, K, P_Z). \qquad \square$$

In the sequel we only have to consider the case $p < \frac{1}{4}$ because for $p \geq \frac{1}{4}$ the bound in Proposition 4 (b) is stronger than the bound of Theorem 39 (for $p \geq \frac{1}{4}$ it holds that $64Kp^2 \log \frac{2}{p} + 2 \log K \geq 64Kp^2 \geq 16Kp \geq Kp$).

We assume the keys to be enumerated such that

$$P_Z(1) \geq \cdots \geq P_Z(K).$$

Then necessarily $P_Z(1) < \frac{1}{4}$ because otherwise $P_S^{max} \geq \frac{1}{4}$ and therefore $p \geq \frac{1}{4}$.

Let $\mathcal{K} \subset \{1, \ldots, K\}$ be the maximal subset consisting of the first N key-indices such that $P_Z(\mathcal{K}) \leq \frac{1}{2}$.

Then clearly $P_Z(\mathcal{K}) > \frac{1}{4}$ and $P_Z(z) \geq \frac{1}{2K}$ for all $z \in \mathcal{K}$ (assume on the contrary that $P_Z(N) < \frac{1}{2K}$ then $P_Z(z) < \frac{1}{2K}$ for all $z \geq N$ and therefore $P_Z(\mathcal{K}) > 1 - (K - N)\frac{1}{2K} > \frac{1}{2}$, which is a contradiction).

We now apply Lemma 10 (a) and get $p \geq p(M, K, P_Z) \geq P_Z(\mathcal{K})\, p(M, N) \geq \frac{p(M,N)}{4}$ and therefore

$$p(M, N) \leq 4p < 1. \tag{2.3.28}$$

From part (b) of Lemma 10 we get $p \geq \frac{1}{2K} N\, p_e(M, N)$ or

$$p_e(M, N) \leq \frac{2Kp}{N}. \tag{2.3.29}$$

Combining (2.3.28) and Proposition 4 (b) we see that M must satisfy the inequality

$$\log M \leq 4pN + 1 \leq 4pN \log \frac{2}{p} + 2 \log K. \tag{2.3.30}$$

Combining (2.3.29) and the bound of Proposition 3 we get

$$\begin{aligned} \log M &\leq \log M_e(N, p_e(M, N)) \\ &\leq \log M_e(N, \frac{2Kp}{N}) \leq \frac{4K^2p^2}{N} \log \frac{2}{p} + 2 \log K, \end{aligned} \tag{2.3.31}$$

where we have to assume that $\frac{2Kp}{N} \leq 0.42$ in order to apply Proposition 3 but otherwise $4pN \leq 64Kp^2$ and therefore the bound in (2.3.30) would be sharper then the bound of Theorem 39.

Combining (2.3.30) and (2.3.31) yields

$$\begin{aligned} \log M &\leq 4p \min\{N, \frac{K^2p}{N}\} \log \frac{2}{p} + 2 \log K \\ &\leq 4Kp^{\frac{3}{2}} \log \frac{2}{p} + 2 \log K, \end{aligned} \tag{2.3.32}$$

where the last inequality can be verified as follows: if $N \leq \frac{K^2p}{N}$, then $N \leq Kp^{\frac{1}{2}}$ and if $\frac{K^2p}{N} < N$, then $\frac{K}{N} < \frac{1}{\sqrt{p}}$ and therefore $\frac{K^2p}{N} \leq Kp^{\frac{1}{2}}$.

So we have obtained from the bound Kp the stronger bound (for sufficiently small p) $4Kp^{\frac{3}{2}} \log \frac{2}{p} + 2 \log K$. We now repeat the procedure using instead of the bound Kp the new bound, i.e., we combine the inequalities

$$\log M \leq 4N(4p)^{\frac{3}{2}} \log \frac{2}{p} + 2 \log K$$

and

$$\log M \leq 4 \frac{K^2 p^2}{N} \log \frac{2}{p} + 2 \log K \leq 8 \frac{K^2 p^2}{N} \log \frac{2}{p} + 2 \log K$$

to

$$\begin{aligned} \log M &\leq (4p)^{\frac{3}{2}} 4 \min\{N, \frac{K^2 p^{2-\frac{3}{2}}}{N}\} \log \frac{2}{p} + 2 \log K \\ &\leq 16 K p^{\frac{7}{4}} \log \frac{2}{p} + 2 \log K. \end{aligned}$$

Generally, if after the nth step we have the inequality

$$\log M \leq C_n K p^{\alpha_n} \log \frac{2}{p} + 2 \log K$$

then in the $(n+1)$th step we obtain the same type of inequality with coefficients C_{n+1} and α_{n+1} that satisfy

$$C_{n+1}^2 = 64 C_n \quad \text{and} \quad \alpha_{n+1} = 1 + \frac{\alpha_n}{2}.$$

(Note that in the $(n+1)$th step the inequality $\log M \leq 4 \frac{K^2 p^2}{N} \log \frac{2}{p} + 2 \log K$ has to be weakened to $\log M \leq \beta_{n+1} \frac{K^2 p^2}{N} \log \frac{2}{p} + 2 \log K$ with $\beta_{n+1} \triangleq \frac{64}{4^{\alpha_n}} \geq 4$ to adjust the min term in the right way.)

As $\lim_{n \to \infty} \alpha_n = 2$ and $\lim_{n \to \infty} C_n = 64$ we obtain that $M(K, P_Z, p)$ must satisfy the inequality

$$\log M(K, P_Z, p) \leq 64 K p^2 \log \frac{2}{p} + 2 \log K,$$

which completes the proof of Theorem 39.

Remark 15

1. For small p the principal difference of the upper and the lower bound consists of an additional factor of order $\ln \frac{1}{p}$. Burnashev and Bassalygo [3, 4] say that they do not know which of the bounds can be improved.
2. The estimates on the number $M(K, P_Z, p)$ should certainly depend on the distribution P_Z. Burnashev and Bassalygo [3] conjectured that this dependence is as follows

$$C_1 + C_2 p^2 \exp(H(Z)) < \log M(K, P_Z, p) < C_3 + C_4 p^2 \log \frac{1}{p} \exp(H(Z))$$

where $C_1, \ldots, C_4$ are constants.

Pairwise Separated Measures

Now we will return to the general case and no longer restrict ourselves to the class of authentication codes without secrecy. If we consider the problem of the last section, then the lower bound we gave there remains valid as we have only enlarged our possibilities to build authentication codes. The problem how the secrecy provided by an authentication code attaches the answer to the question of the maximal number of messages given the probability of deception has not been treated rigorously. In this section the constraint on the success probability of the opponent, which has to be fulfilled by the authentication codes, is sharpened compared to the last section. This will allow us to use as an upper bound for the maximal number of messages the maximal number of pairwise separated measures.

Definition 30 Let $\mathcal{K} \triangleq \{1, \ldots, K\}$ and $\mu_1, \ldots, \mu_M$ be probability measures on $\mathcal{K}$. Further let p be a constant with $0 \leq p \leq 1$. The L_1-norm of a function $\mu : \mathcal{K} \to \mathbb{R}$ is

$$||\mu|| \triangleq \sum_{z \in \mathcal{K}} |\mu(z)|.$$

The set $\{\mu_i : i = 1, \ldots, M\}$ is called p-pairwise separated if

$$||\mu_i - \mu_j|| \geq 2(1 - p)$$

for any $i, j = 1, \ldots, M \quad i \neq j$.

When working with the L_1 distance of probability measures the following identity is useful.

Lemma 11 *For two probability measures μ and ν on $\mathcal{K}$*

$$||\mu - \nu|| = 2\left(1 - \sum_{z \in \mathcal{K}} \min\{\mu(z), \nu(z)\}\right).$$

Proof

$$\begin{aligned}
||\mu - \nu|| &= \sum_{z:\mu(z) \geq \nu(z)} (\mu(z) - \nu(z)) + \sum_{z:\nu(z) > \mu(z)} (\nu(z) - \mu(z)) \\
&= \sum_{z:\mu(z) \geq \nu(z)} \mu(z) + \sum_{z:\nu(z) > \mu(z)} \nu(z) - \sum_{z \in \mathcal{K}} \min\{\mu(z), \nu(z)\} \\
&= \sum_{z \in \mathcal{K}} \mu(z) + \sum_{z \in \mathcal{K}} \nu(z) - 2 \sum_{z \in \mathcal{K}} \min\{\mu(z), \nu(z)\} = 2 - 2 \sum_{z \in \mathcal{K}} \min\{\mu(z), \nu(z)\}. \quad \square
\end{aligned}$$

Definition 31 For a given constant $0 \leq p < 1$ we denote by $M_{sep}(K, p)$ the maximal cardinality of a set of p-pairwise separated probability measures on $\mathcal{K}$.

In [6] the following inequality for the value $M_{sep}(K, p)$ was proved

$$M_{sep}(K, p) \leq \left(\frac{2}{1-p}\right)^{K-1}. \tag{2.3.33}$$

The main analytical result in [4] consists of an improvement of this bound for small p, which makes it valuable for the problem of the maximal number of messages in an authentication code.

Theorem 40 (Burnashev and Bassalygo) *For any* $0 < p < 1$ *the following inequality holds*

$$M_{sep}(K, p) \leq K + \frac{1}{p^2} + \frac{1}{2p^2} \exp\left(\frac{p^2 K}{(1-\sqrt{p})^3} \log \frac{2e}{p^2}\right).$$

In order to prove Theorem 40 we need the following Lemma.

Lemma 12 *Let* $\{\mu_1, \ldots, \mu_M\}$ *be a set of* δ*-pairwise separated probability measures on* $\mathcal{K}$ *and let* $\mathcal{K}_i \triangleq \{z \in \mathcal{K} : \mu_i(z) > 0\}$ *be the support of* μ_i *for any* $i = 1, \ldots, M$. *Then the following statements hold.*

(a) If $\max\{\mu_i(z) : z \in \mathcal{K}, i = 1, \ldots, M\} \leq \mu$, *then*

$$M \leq \frac{(1-\delta)\mu K}{1-\delta\mu K}, \qquad \textit{provided that } 1 - \delta\mu K > 0.$$

(b) If $\mu_i(z) \geq \mu \geq \frac{\delta}{K}$ *for all* $z \in \mathcal{K}_i$ *and all* $i = 1, \ldots, M$, *then*

$$M \leq \frac{(1-\delta)\mu K}{2\delta} \exp\left(\frac{\delta}{\mu} \log \frac{2e\mu K}{\delta(1-\delta)}\right).$$

Proof We start with (a). As $\{\mu_1, \ldots, \mu_M\}$ is δ-pairwise separated it follows that

$$\sum_{i=1}^{M} \sum_{j=1}^{M} ||\mu_i - \mu_j|| \geq 2(1-\delta)M(M-1). \tag{2.3.34}$$

Now we bound this sum from above using the identity of Lemma 11 and the inequality $\min\{\mu_i(z), \mu_j(z)\} \geq \frac{\mu_i(z)\mu_j(z)}{\mu}$, which holds by the assumption made in (a).

$$\sum_{i=1}^{M}\sum_{j=1}^{M}||\mu_i-\mu_j|| \le 2\left(M^2-\frac{1}{\mu}\sum_{i=1}^{M}\sum_{j=1}^{M}\sum_{z\in\mathcal{K}}\mu_i(z)\mu_j(z)\right)$$
$$= 2\left(M^2-\frac{1}{\mu}\sum_{z\in\mathcal{K}}\left(\sum_{i=1}^{M}\mu_i(z)\right)^2\right)$$
$$\le 2\left(M^2-\frac{1}{\mu K}\left(\sum_{z\in\mathcal{K}}\sum_{i=1}^{M}\mu_i(z)\right)^2\right) = 2M^2\left(1-\frac{1}{\mu K}\right), \tag{2.3.35}$$

where we applied (2.3.15) to get the last inequality. Combining (2.3.34) and (2.3.35) leads to

$$\left(\frac{1-\delta\mu K}{\mu K}\right)M \le (1-\delta)$$

and this proves (a).

Now we prove (b). As $\{\mu_1,\ldots,\mu_M\}$ is δ-pairwise separated and the assumption made in (b) implies that $\mu \le \min\{\mu_i(z),\mu_j(z)\}$ for all $z\in\mathcal{K}_i\cap\mathcal{K}_j$ it follows that for $i\ne j$

$$|\mathcal{K}_i\cap\mathcal{K}_j|\cdot\mu \le \sum_{z\in\mathcal{K}}\min\{\mu_i(z),\mu_j(z)\} \le \delta.$$

Therefore $|\mathcal{K}_i\cap\mathcal{K}_j| \le \left\lfloor\frac{\delta}{\mu}\right\rfloor$ for $i\ne j$. Let $T \triangleq \left\lfloor\frac{\delta}{\mu}\right\rfloor$. This implies that the number of measures μ_i with $|\mathcal{K}_i|>T$ does not exceed $\binom{K}{T+1}$ (otherwise there would be two measures μ_i and μ_j $(i\ne j)$ with $|\mathcal{K}_i\cap\mathcal{K}_j|\ge T+1$) and clearly the number of measures μ_i with $|\mathcal{K}_i|\le T$ does not exceed $\binom{K}{T}M_{sep}(T,\delta)$. Therefore

$$M \le \binom{K}{T+1}+\binom{K}{T}M_{sep}(T,\delta) \le \frac{K}{T}\binom{K}{T}M_{sep}(T,\delta).$$

Using the bound given in (2.3.33) for the value $M_{sep}(T,\delta)$ and the inequality $\binom{n}{k}\le\left(\frac{ne}{k}\right)^k$, which can be verified using Stirling's formula,[3] we obtain

$$M \le \frac{K}{T}\left(\frac{Ke}{T}\right)^T\left(\frac{2}{1-\delta}\right)^{T-1} = \frac{(1-\delta)K}{2T}\exp\left(T\log\left(\frac{2Ke}{(1-\delta)T}\right)\right)$$

[3] $\binom{n}{k} \le \left(\frac{n}{k}\right)^k\left(1+\frac{k}{n-k}\right)^{n-k}e^{\frac{1}{12n}-\frac{1}{12k+1}-\frac{1}{12(n-k)+1}+\frac{1}{2}\ln\left(\frac{n}{2\pi k(n-k)}\right)}$
$\le \left(\frac{ne}{k}\right)^k e^{\frac{1}{2n}-\frac{1}{6n+1}+\frac{1}{2}\ln\left(\frac{n}{2\pi(n-1)}\right)} \le \left(\frac{ne}{k}\right)^k$.

$$\leq \frac{(1-\delta)\mu K}{2\delta} \exp\left(\frac{\delta}{\mu} \log\left(\frac{2e\mu K}{\delta(1-\delta)}\right)\right). \qquad \square$$

Proof of the theorem. Let $\{\mu_1, \ldots, \mu_M\}$ be a set of p-pairwise separated probability measures on $\mathcal{K}$. It contains not more than K measures μ_i with $\max_z \mu_i(z) > p$ because otherwise there would be some $i \neq j$ and a z with $\min\{\mu_i(z), \mu_j(z)\} > p$, which implies $||\mu_i - \mu_j|| < 2(1-p)$. Therefore below we assume that all the measures μ_i satisfy $\max_z \mu_i(z) \leq p$ and derive for that case an upper bound to which we have to add K in the end.

Fix now parameters μ and ϵ such that $0 < p < \epsilon < 1$ and $0 < \mu$ (the parameters will be chosen later) and let $\mathcal{K}_i(\mu) \triangleq \{z \in \mathcal{K} : \mu_i(z) \geq \mu\}$. First we upper bound the number M_1 of measures μ_i with $\mu_i(\mathcal{K}_i^c(\mu)) \geq 1 - \epsilon$. We may assume that these measures are $\mu_1, \ldots, \mu_{M_1}$ and introduce on their basis new probability measures ν_i with supports $\mathcal{K}_i^c(\mu)$ in the following way.

$$\nu_i(z) \triangleq \frac{\mu_i(z)}{\mu_i(\mathcal{K}_i^c(\mu))} \qquad \text{for all } z \in \mathcal{K}_i^c(\mu) \text{ and } i = 1, \ldots, M_1.$$

For these measures we obtain the following relation.

$$||\nu_i - \nu_j|| \geq 2\left(1 - \sum_{z \in \mathcal{K}_i^c(\mu) \cap \mathcal{K}_j^c(\mu)} \frac{\min\{\mu_i(z), \mu_j(z)\}}{1-\epsilon}\right) \geq 2\left(1 - \frac{p}{1-\epsilon}\right)$$

for all $i, j = 1 \ldots, M_1,\ i \neq j$. Furthermore

$$\max_{z \in \mathcal{K}} \nu_i(z) < \frac{\mu}{\mu_i(\mathcal{K}_i^c(\mu))} \leq \frac{\mu}{1-\epsilon} \qquad \text{for all } i = 1, \ldots, M_1.$$

Thus we can apply Lemma 12 (a) to bound M_1.

$$M_1 \leq \frac{(1 - \frac{p}{1-\epsilon})\frac{\mu}{1-\epsilon} K}{1 - \frac{p}{1-\epsilon}\frac{\mu}{1-\epsilon} K} = \frac{(1-\epsilon-p)\mu K}{(1-\epsilon)^2 - p\mu K} \leq \frac{\mu K}{(1-\epsilon)^2 - p\mu K}, \tag{2.3.36}$$

provided that

$$(1-\epsilon)^2 - p\mu K > 0. \tag{2.3.37}$$

Now we consider the remaining $M_2 = M - M_1$ measures μ_i with $\mu_i(\mathcal{K}_i(\mu)) \geq \epsilon$. As all the values $\mu_i(z)$ do not exceed p there exists in every set $\mathcal{K}_i(\mu)$ a subset $\mathcal{K}_i'(\mu)$ such that $\epsilon \leq \mu_i(\mathcal{K}_i(\mu)) \leq \epsilon + p$. We introduce new probability measures σ_i with supports $\mathcal{K}_i'(\mu)$ in the following way.

$$\sigma_i(z) \triangleq \frac{\mu_i(z)}{\mu_i(\mathcal{K}_i'(\mu))} \qquad \text{for all } z \in \mathcal{K}_i'(\mu) \text{ and } i = M_1 + 1, \ldots, M.$$

For these measure we obtain the following relation.

$$||\sigma_i - \sigma_j|| \geq 2\left(1 - \sum_{z \in \mathcal{K}_i'(\mu) \cap \mathcal{K}_j'(\mu)} \frac{\min\{\mu_i(z), \mu_j(z)\}}{\epsilon}\right) \geq 2\left(1 - \frac{p}{\epsilon}\right)$$

for all $i, j = M_1 + 1, \ldots, M \quad i \neq j$. Furthermore

$$\sigma_i(z) \geq \frac{\mu}{\epsilon + p} \qquad \text{for all } z \in \mathcal{K}_i'(\mu) \text{ and } i = M_1 + 1, \ldots, M.$$

Thus we can apply Lemma 12 (b) to bound M_2.

$$\begin{aligned} M_2 &\leq \frac{(1 - \frac{p}{\epsilon})\frac{\mu}{\epsilon+p}K}{2\frac{p}{\epsilon}} \exp\left(\frac{\frac{p}{\epsilon}}{\frac{\mu}{\epsilon+p}} \log \frac{2e\frac{\mu}{\epsilon+p}K}{\frac{p}{\epsilon}(1 - \frac{p}{\epsilon})}\right) \\ &\leq \frac{\mu K}{2p} \exp\left(\frac{p(p+\epsilon)}{\mu\epsilon} \log \frac{2e\mu K\epsilon}{p(\epsilon - \frac{p^2}{\epsilon})}\right) \\ &\leq \frac{\mu K}{2p} \exp\left(\frac{p(p+\epsilon)}{\mu\epsilon} \log \frac{2e\mu K\epsilon}{p(\epsilon - p)}\right), \end{aligned} \tag{2.3.38}$$

provided that the assumption made in Lemma 12 (b) holds, which is in this case

$$\frac{\mu}{\epsilon + p} \geq \frac{p}{\epsilon K}. \tag{2.3.39}$$

We choose the parameters ϵ and μ as follows

$$\epsilon \triangleq \sqrt{p} \text{ and } \mu \triangleq \frac{(1 - \sqrt{p})^3(1 + \sqrt{p})}{pK}.$$

Then clearly $0 < p < \epsilon < 1$ and $0 < \mu$.

Furthermore we have to check for this choice of parameters that (2.3.37) and (2.3.39) hold. (2.3.37) holds as

$$(1 - \epsilon)^2 - p\mu K = (1 - \sqrt{p})^2 - (1 - \sqrt{p})^3(1 + \sqrt{p}) = (1 - \sqrt{p})^2 p > 0$$

and (2.3.39) holds, provided that $p \le \frac{1}{4}$ because then

$$\frac{\mu}{\epsilon + p} = \frac{(1-p)(1-\sqrt{p})^2}{pK(p+\sqrt{p})} \ge \frac{(1-\frac{1}{4})(1-\sqrt{\frac{1}{4}})^2}{\frac{1}{4}K(\frac{1}{4}+\sqrt{\frac{1}{4}})} \ge \frac{1}{K} \ge \frac{\sqrt{p}}{K} = \frac{p}{\epsilon K}.$$

Hence, if $p \le \frac{1}{4}$ we get from (2.3.36) and (2.3.38) that

$$\begin{aligned} M &\le K + M_1 + M_2 \\ &\le K + \frac{1-p}{p^2} + \frac{(1-\sqrt{p})^3(1+\sqrt{p})}{2p^2} \exp\left(\frac{Kp^2}{(1-\sqrt{p})^3} \log \frac{2e(1-\sqrt{p})(1-p)}{p^2}\right) \\ &\le K + \frac{1}{p^2} + \frac{1}{2p^2} \exp\left(\frac{Kp^2}{(1-\sqrt{p})^3} \log \frac{2e}{p^2}\right) \end{aligned}$$

If $\frac{1}{4} < p < 1$, then the last bound is weaker than (2.3.33), as we have the factor $\frac{p^2}{(1-\sqrt{p})^3}$ in the exponent. This completes the proof of Theorem 40. □

Now we will require that the authentication codes satisfy the condition

$$P_S^\star \triangleq \max_{y \in \mathcal{M}'} P_S(y) \le p \tag{2.3.40}$$

for some given constant $p > 0$, i.e., (recall Definition 25 and (2.3.3)) that for any cryptogram $y \in \mathcal{M}'$ the probability of a successful substitution with any cryptogram $y' \in \mathcal{M}'$, $y' \ne y$, does not exceed p.

In the case of an authentication code without secrecy we have $P_S^{max} \le P_S^\star$. Therefore the requirement made in (2.3.40) is stronger than $P_S^{max} \le p$ and we have $P_D \le p$ if (2.3.40) holds. However the deficiency of this approach is that, in general (for authentication codes with some degree of secrecy), we cannot assure $P_D \le p$ if (2.3.40) holds, which can be seen in Example 3 again.

Definition 32 For any $0 < p < 1$ let $M^\star(K, p)$ denote the maximal number of messages in an authentication code with K keys such that $P_S^\star \le p$.

The next lemma enables us to use as an upper bound for $M^\star(K, p)$ upper bounds for the maximal cardinality of a set of pairwise separated probability measures.

Lemma 13 *Let $0 < p < 1$. If $P_S^\star \le p$ for an authentication code, then the set $\{P_{Z|Y}(\cdot|y) : y \in \mathcal{M}'\}$ of probability measures on the set $\{1, \dots, K\}$ is p-pairwise separated.*

Proof Let $y, y' \in \mathcal{M}'$, $y \ne y'$. According to Definition 25 the support of $P_{Z|Y}(\cdot|y')$ is $\mathcal{K}(y')$. As $P_S(y) \le p$ it follows from (2.3.3) that

$$P_{Z|Y}(\mathcal{K}(y')|y) \le p \tag{2.3.41}$$

Using Lemma 11 and (2.3.41) we obtain

$$\begin{aligned} ||P_{Z|Y}(\cdot|y) - P_{Z|Y}(\cdot|y')|| &= 2\left(1 - \sum_{z=1}^{K} \min\{P_{Z|Y}(z|y), P_{Z|Y}(z|y')\}\right) \\ &= 2\left(1 - \sum_{z\in\mathcal{K}(y')} \min\{P_{Z|Y}(z|y), P_{Z|Y}(z|y')\}\right) \\ &\geq 2\left(1 - P_{Z|Y}(\mathcal{K}(y')|y)\right) \geq 2(1-p). \end{aligned}$$

□

With this notion the next theorem is immediate.

Theorem 41 *For any* $0 < p < 1$ *the following inequality holds*

$$M^{\star}(K,p) \leq K + \frac{1}{p^2} + \frac{1}{2p^2} \exp\left(\frac{p^2 K}{(1-\sqrt{p})^3} \log \frac{2e}{p^2}\right).$$

Proof The statement follows directly from the previous Lemma, the bound on the cardinality of a set of pairwise separated measures given in Theorem 40 and the fact that for any authentication code $M \leq |\mathcal{M}'|$. □

Remark 16

1. We exploited the fact that an authentication code induces a probability distribution P_{ZY} on the set $\{1,\ldots,K\} \times \mathcal{M}'$ such that the measure of the support of $P_{Z|Y}(\cdot|y')$ under $P_{Z|Y}(\cdot|y)$ is less than p for any $y' \neq y$. For the moment let us denote such a configuration as a $(|\mathcal{M}'|, K, p)$-configuration. Burnashev and Bassalygo [4] looked abstractly on such configurations, i.e., where not necessarily the probability distribution is induced by some cipher and a message source, and denoted as $M_{aut,1}(K,p)$ the maximal M such that there exists a (M,K,p)-configuration. Furthermore they denoted as $M_{aut,2}(K,p)$ the maximal number of messages in a generalized authentication code (where keys and messages are not necessarily generated independently) such that $P_S^{\star} \leq p$. Clearly, $M_{aut,1}(K,p) \leq M_{aut,2}(K,p)$, because we can define for an optimal (M,K,p)-configuration the encryption by $c_z(m) = m$ for all $z = 1,\ldots,K$. On the other hand we saw already that an authentication code with $P_S^{\star} \leq p$ induces a $(|\mathcal{M}'|, K, p)$-configuration (this is also true if messages and keys are no longer chosen independently). As for any authentication code we have $M \leq |\mathcal{M}'|$ it follows $M_{aut,2}(K,p) \leq M_{aut,1}(K,p)$. Therefore the values $M_{aut,1}(K,p)$ and $M_{aut,2}(K,p)$ coincide.
2. In [4] the value $M_{aut,1}(K,p)$ was bounded by $M^{sep}(K,2p)$ but it is also possible to bound it directly by $M^{sep}(K,p)$ similarly to the derivation of Lemma 13 and Theorem 41. This gives a better result as $M^{sep}(K,p) \leq M^{sep}(K,2p)$.

2.3.4 Authentication as an Hypothesis Testing Problem

In this paragraph we present an elegant approach by Maurer [19] to give information-theoretic lower bounds on the success probabilities of the opponent in a generalized model. The key point is the interpretation of the receiver's decision whether the received cryptogram is authentic or not as a decision for one of two hypotheses.

Generalizations

We generalize the model in the following ways.

- The sender wants to inform the receiver about a sequence of messages produced by a source at some time instances. We denote by $X_1, X_2, \ldots, X_i, \ldots$ the random variables for those messages.
- Each message is encrypted separately to some cryptogram. We denote by Y_1, $Y_2, \ldots, Y_i, \ldots$ the corresponding random variables. The cryptogram sent at time i depends on the secret key, the message produced at time i and possibly also on the previous messages. Therefore in this context a key c_z can be described as a mapping $c_z : \bigcup_{i=1}^{\infty} \mathcal{M}^i \longrightarrow \mathcal{M}'$ such that $y_i = c_z(m_1, \ldots, m_i)$.
- We assume that the receiver is synchronized, i.e., he knows the message number i. In order to enable the receiver to decrypt correctly we have to assume that the message m_i produced at time i is uniquely determined by the previous messages $m_1, \ldots, m_{i-1}$ and cryptograms $y_1, \ldots, y_i$ and the secret key. Therefore, by induction, m_i is uniquely determined by $m_1, \ldots, m_{i-1}, y_i$ and the secret key (also by $y_1, \ldots, y_i$ and the secret key itself). In other words we require that for all $i \in \mathbb{N}$ and all $m_1, \ldots, m_i, m_i' \in \mathcal{M}$ with $m_i \neq m_i'$ we have $c_z(m_1, \ldots, m_i) \neq c_z(m_1, \ldots, m_{i-1}, m_i')$ for all $z \in \{1, \ldots, K\}$.
- The opponent can choose between impersonation and substitution. In an *impersonation attack at time i* he waits until he has seen the first $i-1$ cryptograms $y_1, \ldots, y_{i-1}$, which he lets pass unchanged to the receiver and then sends a fraudulent cryptogram y_i'. We denote by Y_i' the corresponding random variable. In a *substitution attack at time i* the opponent lets pass the first $i-1$ cryptograms $y_1, \ldots, y_{i-1}$, intercepts y_i and replaces it by a different cryptogram y_i'.
- Up to now the receiver has accepted a cryptogram as authentic if and only if it is consistent with the secret key. Now we will allow, at least for purposes of calculation, the receiver to reject a valid cryptogram with some probability. This generalization is important because it establishes the link to the standard hypothesis testing scenario.

We will also refine our notion when the opponent is considered to be successful in an impersonation attack and substitution attack, respectively. Suppose the receiver accepted the fraudulent cryptogram y_i' as a valid cryptogram. Then he decodes $y_1, \ldots, y_{i-1}, y_i'$ to some message m_i'. We distinguish now three cases. The opponent is considered to be successful when

(a) the receiver accepts the fraudulent cryptogram y_i' as a valid cryptogram (this is the case we considered so far).

(b) the receiver accepts the fraudulent cryptogram y_i' as a valid cryptogram and the message m_i' is known to the opponent. In other words the opponent is only considered to be successful if he also guesses the message m_i' correctly.
(c) the receiver accepts the fraudulent cryptogram y_i' as a valid cryptogram and the message m_i' was chosen by the opponent before. Of course this type of attack depends on the particular value m_i'.

Note that in an authentication code without secrecy case (a) and (b) coincide as the cryptograms uniquely determine the message and therefore the opponent will always guess correctly.

Definition 33 We distinguish the three described cases by denoting the corresponding attacks as impersonation attack and substitution attack of type (a), (b) and (c), respectively. We denote the success probabilities for the opponent using an optimal strategy for an attack of the type (a), (b) and (c) by

$$P_{I,i}^a, P_{I,i}^b \text{ and } P_{I,i,m_i'}^c,$$

for an impersonation attack at time i, respectively, and by

$$P_{S,i}^a, P_{S,i}^b \text{ and } P_{S,i,m_i'}^c,$$

for a substitution attack at time i, respectively.

For a particular observed sequence $y_1, \ldots, y_{i-1}$ of cryptograms and, in case of a substitution attack also for a fixed intercepted cryptogram y_i, we denote the corresponding success probabilities by

$$P_{I,i}^a(y_1, \ldots, y_{i-1}), P_{I,i}^b(y_1, \ldots, y_{i-1}) \text{ and } P_{I,i}^c(y_1, \ldots, y_{i-1}),$$

respectively, for an impersonation attack at time i and by

$$P_{S,i}^a(y_1, \ldots, y_i), P_{S,i}^b(y_1, \ldots, y_i) \text{ and } P_{S,i,m_i'}^c(y_1, \ldots, y_i),$$

respectively, for a substitution attack at time i.

With this notion, for instance, $P_{I,i}^a$ is the expected value of $P_{I,i}^a(y_1, \ldots, y_{i-1})$, i.e.,

$$P_{I,i}^a = \sum_{(y_1,\ldots,y_{i-1})} P_{Y_1 \ldots Y_{i-1}}(y_1, \ldots, y_{i-1}) P_{I,i}^a(y_1, \ldots, y_{i-1}).$$

Some Results on Hypothesis Testing

We collect some results of the theory of hypothesis testing. Suppose we have to decide which of two hypotheses, H_0 or H_1, is true and we know from some random experiment the outcome of a random variable U with values in some set $\mathcal{U}$. The distribution of U depends on which of the two hypotheses is true. Under H_0 let U

be distributed according to P and under H_1 let U be distributed according to Q. A decision rule assigns to each possible value $u \in \mathcal{U}$ one of the two hypotheses. Therefore a decision rule may be viewed as a partition of $\mathcal{U}$ into two sets $\mathcal{U}_0$ and $\mathcal{U}_1$ such that we vote for H_0 if $U \in \mathcal{U}_0$ and vote for H_1 otherwise. There are two types of possible errors that may occur when making a decision. Accepting hypothesis H_1 when actually H_0 is true is called an error of the first kind and we will typically denote the probability of this event by α. Accepting hypothesis H_0 when actually H_1 is true is called an error of the second kind and we will typically denote the probability of this event by β. The optimal decision rule is given by the Neyman–Pearson Theorem which states that, for a given maximal tolerable probability β of an error of the second kind, α can be minimized by assuming hypothesis H_0 if and only if

$$\log \frac{P(u)}{Q(u)} \geq T \tag{2.3.42}$$

for some threshold T (see for instance [5]).

Note that only the existence of T, but not its specific value is given by the theorem. The term on the left-hand side of (2.3.42) is called the log-likelihood ratio. The expected value of the log-likelihood ratio with respect to P is the I-divergence

$$D(P||Q) = \sum_{u \in \mathcal{U}} P(u) \log \frac{P(u)}{Q(u)},$$

which is nonnegative and equal to zero exactly if the two distributions P and Q are identical.

The I-divergence and the error probabilities in an hypothesis test of the described form are related at follows.

Lemma 14 *The probabilities α and β of an error of the first and second kind, respectively, satisfy*

$$d(\alpha, \beta) \leq D(P||Q),$$

where $d(\alpha, \beta) \triangleq \alpha \log \frac{\alpha}{1-\beta} + (1-\alpha) \log \frac{1-\alpha}{\beta}$.

In particular, for $\alpha = 0$ we have

$$\beta \geq 2^{-D(P||Q)}.$$

Proof Let $\{\mathcal{U}_0, \mathcal{U}_1\}$ be the partition of $\mathcal{U}$ induced by the used decision rule. Then

$$\alpha = \sum_{u \in \mathcal{U}_1} P(u) \quad \text{and} \quad \beta = \sum_{u \in \mathcal{U}_0} Q(u).$$

Therefore

$$d(\alpha,\beta)=\left(\sum_{u\in\mathcal{U}_1}P(u)\right)\log\frac{\sum_{u\in\mathcal{U}_1}P(u)}{\sum_{u\in\mathcal{U}_1}Q(u)}+\left(\sum_{u\in\mathcal{U}_0}P(u)\right)\log\frac{\sum_{u\in\mathcal{U}_0}P(u)}{\sum_{u\in\mathcal{U}_0}Q(u)}$$

$$\leq\sum_{u\in\mathcal{U}_1}P(u)\log\frac{P(u)}{Q(u)}+\sum_{u\in\mathcal{U}_0}P(u)\log\frac{P(u)}{Q(u)}=D(P||Q),$$

where we applied the log-sum inequality. □

Later we will deal with the case where the random variable U is given as a random couple $U=(S,T)$, the distribution P will be the actual joint distribution P_{ST} and the distribution Q will be the product of the marginal distributions P_SP_T. In that case the I-divergence $D(P||Q)$ turns out to be the mutual information $I(S\wedge T)$.

$$\begin{aligned}D(P||Q)&=\sum_{s,t}P_{ST}(s,t)\log\frac{P_{ST}(s,t)}{P_S(s)P_T(t)}\\&=H(S)+H(T)-H(S,T)=H(S)-H(S|T)=I(S\wedge T).\end{aligned}$$

Suppose now that the distributions P and Q depend on the value v of an additional random variable V with values in $\mathcal{V}$, which is known to the testing person, i.e., we have a collection of pairs (P_v,Q_v) of conditional distributions each pair occurring with probability $P_V(v)$. The decision rule may depend on the value v of V and for each $v\in\mathcal{V}$ we denote by $\alpha(v)$ and $\beta(v)$ the probabilities of an error of the first and second kind, respectively, given that $V=v$.

Lemma 15 *The average probabilities of an error of the first and second kind given by*

$$\alpha\triangleq\sum_{v\in\mathcal{V}}P_V(v)\alpha(v)\quad\textit{and}\quad\beta\triangleq\sum_{v\in\mathcal{V}}P_V(v)\beta(v),$$

respectively, satisfy

$$d(\alpha,\beta)\leq\sum_{v\in\mathcal{V}}P_V(v)D(P_v||Q_v).$$

Proof As the function d is $\cup$-convex we can apply Jensen's inequality and get

$$d(\alpha,\beta)\leq\sum_{v\in\mathcal{V}}P_V(v)d(\alpha(v),\beta(v)).$$

Lemma 14 implies that for every $v\in\mathcal{V}$

$$d(\alpha(v),\beta(v))\leq D(P_v||Q_v)$$

and this completes the proof. □

We may go another step further. Lemma 15 holds of course also for distributions conditioned on the event that a further random variable W takes on a particular value w known to the testing person, i.e., for pairs $(P_{v,w}, Q_{v,w})$ of distributions. We denote by $\alpha(v, w)$ and $\beta(v, w)$ the two error probabilities. The following corollary follows directly from Lemma 15.

Corollary 3 *The average probabilities (over $\mathcal{V}$) of an error of the first and second kind given by*

$$\alpha(w) \triangleq \sum_{v\in\mathcal{V}} P_V(v)\alpha(v, w) \quad \textit{and} \quad \beta(w) \triangleq \sum_{v\in\mathcal{V}} P_V(v)\beta(v, w),$$

respectively, satisfy

$$d(\alpha(w), \beta(w)) \leq \sum_{v\in\mathcal{V}} P_V(v)D(P_{v,w}||Q_{v,w}).$$

Let us look again at the special case where $U = (S, T)$ and the distributions $P_v = P_{ST|V}(\cdot\,|v)$ and $Q_v = P_{S|V}(\cdot\,|v)P_{T|V}(\cdot\,|v)$ depend on the value of the random variable V. Then the expression on the right-hand side in the statement of Lemma 15 becomes

$$\sum_{v\in\mathcal{V}} P_V(v)D(P_v||Q_v) = \sum_{v\in\mathcal{V}} P_V(v)\, I(S \wedge T|V = v) = I(S \wedge T|V).$$

Similarly if $P_{v,w} = P_{ST|VW}(\cdot\,|v, w)$ and $Q_{v,w} = P_{S|VW}(\cdot\,|v, w)P_{T|VW}(\cdot\,|v, w)$ then the right-hand side in Corollary 3 becomes

$$\begin{aligned}\sum_{v\in\mathcal{V}} P_V(v)D(P_{v,w}||Q_{v,w}) &= \sum_{v\in\mathcal{V}} P_V(v)\, I(S \wedge T|V = v, W = w)\\ &= I(S \wedge T|V, W = w).\end{aligned}$$

The Receivers Hypothesis Testing Problems

Let us now describe how we can make these methods applicable to the authentication problem.

Basically the receiver is faced with the following two hypotheses:

H_0—the received cryptogram is authentic.

H_1—the received cryptogram has been inserted by the opponent.

The two probabilities α and β of an error of the first and second kind, respectively, become:

α—probability of rejecting a valid cryptogram.

β—probability of accepting a fraudulent cryptogram.

Note that the behavior of the receiver considered so far implies $\alpha = 0$.

Let us consider an impersonation attack of the type (a) at time i. The receiver and the opponent have seen the first $i-1$ cryptograms $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$. Let us denote by $\bar{Y}_i$ the random variable for the ith cryptogram (under H_0 we have $\bar{Y}_i = Y_i$ and under H_1 we have $\bar{Y}_i = Y_i'$). The receiver knows the secret key, i.e., he knows the value of Z. Given the value of the random couple $(\bar{Y}_i, Z)$ the receiver has to decide which of the two hypotheses is true. If H_0 is true then $(\bar{Y}_i, Z)$ is distributed according to

$$P_{Y_i Z|Y_1 \ldots Y_{i-1}}(\cdot\,|y_1, \ldots, y_{i-1}). \tag{2.3.43}$$

The opponent chooses the fraudulent cryptogram y_i' depending on $y_1, \ldots, y_{i-1}$ but without further knowledge about the value of Z. Therefore, if H_1 is true, then $(\bar{Y}_i, Z)$ is distributed according to

$$P_{Y_i'|Y_1 \ldots Y_{i-1}}(\cdot\,|y_1, \ldots, y_{i-1}) P_{Z|Y_1 \ldots Y_{i-1}}(\cdot\,|y_1, \ldots, y_{i-1}). \tag{2.3.44}$$

One possible but generally not optimal impersonation strategy for the opponent would be to select y_i' according to the actual distribution of Y_i given $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$, i.e., he chooses

$$P_{Y_i'|Y_1 \ldots Y_{i-1}}(\cdot\,|y_1, \ldots, y_{i-1}) = P_{Y_i|Y_1 \ldots Y_{i-1}}(\cdot\,|y_1, \ldots, y_{i-1}). \tag{2.3.45}$$

Now we can derive the following theorem.

Theorem 42 *For every authentication system*

$$P_{I,i}^a(y_1, \ldots, y_{i-1}) \geq 2^{-I(Y_i \wedge Z|Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1})}$$

and

$$P_{I,i}^a \geq 2^{-I(Y_i \wedge Z|Y_1, \ldots, Y_{i-1})}. \tag{2.3.46}$$

Proof Let $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$ be given. Suppose the opponent chooses his impersonation strategy according to (2.3.45). Let us denote by $P_{I,Y'}(y_1, \ldots, y_{i-1})$ his success probability when following this strategy and by $P_{I,Y'}$ the corresponding average success probability. Suppose the receiver selects some decision rule giving him $\alpha(y_1, \ldots, y_{i-1})$ as the probability of rejecting a valid cryptogram and $\beta(y_1, \ldots, y_{i-1})$ as the probability of accepting a fraudulent cryptogram.

Then Lemma 14 implies

$$d(\alpha(y_1, \ldots, y_{i-1}), \beta(y_1, \ldots, y_{i-1})) \leq I(Y_i \wedge Z|Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}).$$

Denoting by α and β the corresponding average error probability we get from Lemma 15

$$d(\alpha, \beta) \leq I(Y_i \wedge Z|Y_1, \ldots, Y_{i-1}).$$

Selecting the decision rule for the receiver as before which means that he accepts the cryptogram exactly if it is consistent with the secret key and the previous $i-1$ cryptograms we get $\alpha(y_1,\ldots,y_{i-1})=0$ and $\beta(y_1,\ldots,y_{i-1})=P_{I,Y'}(y_1,\ldots,y_{i-1})$. This implies

$$P_{I,Y'}(y_1,\ldots,y_{i-1}) \geq 2^{-I(Y_i\wedge Z|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1})}$$

and

$$P_{I,Y'} \geq 2^{-I(Y_i\wedge Z|Y_1,\ldots,Y_{i-1})}.$$

Therefore we obtain from

$$P^a_{I,i}(y_1,\ldots,y_{i-1}) \geq P_{I,Y'}(y_1,\ldots,y_{i-1}) \text{ and } P^a_{I,i} \geq P_{I,Y'}$$

the desired result. □

Remark 17 Note that in the case when $i=1$, (2.3.46) is Simmons' bound of Theorem 32.

Let us analyze an impersonation attack of type (b) at time i, i.e., the opponent is only considered to be successful if he also guesses the message to which the receiver decodes the fraudulent cryptogram to correctly. Now a strategy for the opponent consists of a distribution $P_{X'_iY'_i|Y_1,\ldots,Y_{i-1}}(\cdot|y_1,\ldots,y_{i-1})$ where the value of Y'_i is the fraudulent cryptogram and the value of X'_i is the message the opponent guesses. Consider now the 'fictive' hypothesis testing scenario, where in addition to values of the random variables $\bar{Y}_i$ and Z the receiver also gets a value of $\bar{X}_i$, which is under hypothesis H_0 equal to X_i and under H_1 equal to X'_i. This means that if H_0 is true than the receiver is told the correct message and if H_1 is true the receiver is told the message the opponent guesses. One possible but generally not optimal impersonation strategy for the opponent would be to select the pair (m'_i, y'_i) according to the actual distribution of (X_i, Y_i) given $Y_1=y_1,\ldots,Y_{i-1}=y_{i-1}$, i.e., he chooses

$$P_{X'_iY'_i|Y_1\ldots Y_{i-1}}(\cdot|y_1,\ldots,y_{i-1}) = P_{X_iY_i|Y_1\ldots Y_{i-1}}(\cdot|y_1,\ldots,y_{i-1}). \tag{2.3.47}$$

Then it follows that if H_0 is true then $(\bar{X}_i, \bar{Y}_i, Z)$ is distributed according to

$$P_{X_iY_iZ|Y_1\ldots Y_{i-1}}(\cdot|y_1,\ldots,y_{i-1})$$

and if H_1 is true then $(\bar{X}_i, \bar{Y}_i, Z)$ is distributed according to

$$P_{X_iY_i|Y_1\ldots Y_{i-1}}(\cdot|y_1,\ldots,y_{i-1})P_{Z|Y_1\ldots Y_{i-1}}(\cdot|y_1,\ldots,y_{i-1}).$$

Now we can derive the following theorem.

Theorem 43 *For every authentication system*

$$P^b_{I,i}(y_1,\ldots,y_{i-1}) \geq 2^{-I(X_iY_i\wedge Z|Y_1=y_1,\ldots,Y_{i-1}=y_{i-1})}$$

and

$$P_{I,i}^{b} \geq 2^{-I(X_iY_i \wedge Z|Y_1,\ldots,Y_{i-1})}.$$

Proof Let $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$ be given. Suppose the opponent chooses his impersonation strategy according to (2.3.47). Let us denote by $P_{I,Y'}(y_1, \ldots, y_{i-1})$ his success probability when following this strategy and by $P_{I,Y'}$ the corresponding average success probability. Suppose the receiver selects some decision rule giving him $\alpha(y_1, \ldots, y_{i-1})$ as the probability of an error of the first kind and $\beta(y_1, \ldots, y_{i-1})$ as the probability of an error of the second kind in the above described hypothesis testing scenario. Then Lemmas 14 and 15 imply

$$d(\alpha(y_1, \ldots, y_{i-1}), \beta(y_1, \ldots, y_{i-1})) \leq I(X_iY_i \wedge Z|Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1})$$

and

$$d(\alpha, \beta) \leq I(X_iY_i \wedge Z|Y_1, \ldots, Y_{i-1})$$

for the average error probabilities α and β.

Now suppose the receiver selects the decision rule in such a way that he votes for H_0 exactly if the value of $\bar{Y}_i$ is a valid cryptogram under the secret key and he would decode it to the message given by $\bar{X}_i$.

Then we get $\alpha(y_1, \ldots, y_{i-1}) = \alpha = 0$, $\beta(y_1, \ldots, y_{i-1}) = P_{I,Y'}(y_1, \ldots, y_{i-1})$ and $\beta = P_{I,Y'}$. As $P_{I,i}^{b}(y_1, \ldots, y_{i-1}) \geq P_{I,Y'}(y_1, \ldots, y_{i-1})$ and $P_{I,i}^{b} \geq P_{I,Y'}$, we obtain the desired result. □

Let us analyze an impersonation attack of type (c), when the opponent is only considered to be successful if the receiver accepts the fraudulent cryptogram and decodes it to some message, which was chosen by the opponent. Let this message be $m_i' \in \mathcal{M}$. We consider the following 'fictive' hypothesis testing scenario. Suppose $Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}$ are given and the message source produces at time i the message m_i', i.e., $X_i = m_i'$. Let us assume the receiver knows this. As in case (a) the receiver now sees some value of the random couple $(\bar{Y}_i, Z)$ and has to decide if the cryptogram he got is authentic or not. Again we may consider a generally not optimal impersonation strategy for the opponent given by

$$P_{Y_i'|Y_1\ldots Y_{i-1}}(\cdot\,|y_1, \ldots, y_{i-1}) = P_{Y_i|Y_1\ldots Y_{i-1}X_i}(\cdot\,|y_1, \ldots, y_{i-1}, m_i'). \tag{2.3.48}$$

If H_0 is true than $(\bar{Y}_i, Z)$ is distributed according to

$$P_{Y_iZ|Y_1\ldots Y_{i-1}X_i}(\cdot\,|y_1, \ldots, y_{i-1}, m_i')$$

and if H_1 is true then $(\bar{Y}_i, Z)$ is distributed according to

$$P_{Y_i|Y_1\ldots Y_{i-1}X_i}(\cdot\,|y_1, \ldots, y_{i-1}, m_i')P_{Z|Y_1\ldots Y_{i-1}}(\cdot\,|y_1, \ldots, y_{i-1}),$$

which is (as Z and X_i are independent) the same as

$$P_{Y_i|Y_1\dots Y_{i-1}X_i}(\cdot\,|y_1,\dots,y_{i-1},m_i')P_{Z|Y_1\dots Y_{i-1}X_i}(\cdot\,|y_1,\dots,y_{i-1},m_i')$$

With this the following conclusion is no more difficult.

Theorem 44 *For every authentication system*

$$P_{I,i}^c(y_1,\dots,y_{i-1}) \geq 2^{-I(Y_i\wedge Z|Y_1=y_1,\dots,Y_{i-1}=y_{i-1},X_i=m_i')}$$

and

$$P_{I,i}^c \geq 2^{-I(Y_i\wedge Z|Y_1,\dots,Y_{i-1},X_i=m_i')}.$$

Proof We proceed analogously to the proofs of the Theorems 42 and 43 using instead of Lemma 15 the Corollary 3 for the above described hypothesis test. Then the desired result is obtained for the receiver's decision rule to accept H_0 exactly if the observed cryptogram is valid under the secret key and would be decoded to m_i'. □

For the substitution attacks of the three described forms (a), (b) and (c), respectively, we can derive a lower bound on the success probability simply by giving a lower bound on the opponent's probability to guess the correct value of Z because, when guessing the secret key correctly, the opponent can launch any of the described attacks.

Let S be a random variable with values in some finite set $\mathcal{S}$. The probability to guess a value of S correctly knowing only P_S is $\max_{s\in\mathcal{S}} P_S(s)$. As the entropy of S is the expected value of $-\log P_S(S)$ we obtain

$$-\log\left(\max_{s\in\mathcal{S}} P_S(s)\right) = \min_{s\in\mathcal{S}}\left(-\log P_S(s)\right) \leq H(S)$$

and therefore

$$\max_{s\in\mathcal{S}} P_S(s) \geq 2^{-H(S)}.$$

Knowing in addition the value of a further random variable T we get by applying Jensen's inequality that the (average) probability of guessing S correctly is bounded by

$$\sum_t P_T(t)2^{-H(S|T=t)} \geq 2^{-H(S|T)}.$$

This applies to our situation in the following way.

Theorem 45 *For every authentication system*

$$P_{S,i}^a(y_1,\dots,y_i) \geq 2^{-H(Z|Y_1=y_1,\dots,Y_i=y_i)}$$

and

$$P^a_{S,i} \geq 2^{-H(Z|Y_1,\ldots,Y_i)}.$$

These bounds also hold for the types (b) and (c) of substitution attacks.

Proof In a substitution attack at time i the opponent knows a sequence of values of $Y_1, \ldots, Y_i$ and therefore the result follows from the previously made remarks. □

We can combine the bounds derived for impersonation attacks and substitution attacks in the following way.

Theorem 46 *For every authentication system*

$$\max\{P^a_{I,1}, \ldots, P^a_{I,n}, P^a_{S,n}\} \geq 2^{-\frac{H(Z)}{n+1}} \quad \textit{for all} \quad n \in \mathbb{N}.$$

Proof Recall that

$$\begin{aligned}
&\sum_{i=1}^{n} I(Y_i \wedge Z|Y_1 \ldots Y_{i-1}) \\
&\quad = \Big(H(Z) - H(Z|Y_1)\Big) + \Big(H(Z|Y_1) - H(Z|Y_1Y_2)\Big) + \cdots \\
&\qquad \cdots + \Big(H(Z|Y_1 \ldots Y_{n-1}) - H(Z|Y_1 \ldots Y_n)\Big) \\
&\quad = H(Z) - H(Z|Y_1 \ldots Y_n) = I(Y_1 \ldots Y_n \wedge Z).
\end{aligned}$$

(Sometimes this is called "Chain Rule of Mutual Information".)

Applying the bound of Theorem 42 for $P^a_{I,i}$ and the bound of Theorem 45 for $P^a_{S,n}$ we obtain that

$$-\sum_{i=1}^{n} \log P^a_{I,i} - \log P^a_{S,n} \leq \sum_{i=1}^{n} I(Y_i \wedge Z|Y_1 \ldots Y_{i-1}) + H(Z|Y_1 \ldots Y_n) = H(Z)$$

and therefore

$$\begin{aligned}
&-\log\big(\max\{P^a_{I,1}, \ldots, P^a_{I,n}, P^a_{S,n}\}\big) \\
&\leq -\log\left(\frac{1}{n+1}\left(\sum_{i=1}^{n} P^a_{I,1} + P^a_{S,n}\right)\right) \leq \frac{H(Z)}{n+1},
\end{aligned}$$

where we used the fact that $-\log$ is a monotonically decreasing and $\cup$-convex function. □

Remark 18 The last result can be interpreted as follows. If an authentication system is used to authenticate n messages the opponent can choose the type of attack that gives him the highest success probability. For a cipher of a given size (measured in terms of the entropy $H(Z)$) Theorem 46 states that the achievable authenticity for n messages corresponds at most to the difficulty of guessing the secret key of a cipher whose size is $n+1$ times smaller than the size of the actual cipher.

2.4 Secret-Key Cryptology

The information-theoretic approach to secret-key cryptology was introduced by Shannon [24] as already mentioned. The problems of these "classical" secrecy systems were further discussed in papers by Ahlswede [1] and Hellman [13]. In this section we concentrate on some new results and approaches of Shtarkov [25] concerning the following problems.

1. Evaluation or estimation of $H(X|Y)$ for a given cipher $(\mathcal{C}, Q)$ and different distributions P_X. This is meaningful for incomplete information on the distribution P_X and/or different constraints on the choice of the cipher.
2. Determination of the optimal (or close to optimal) cipher, if the number of keys and the message distribution is given.

Furthermore the model is extended with a source coder and a randomizer.

2.4.1 Preliminaries

Conditions for Perfectness and Upper Bounds for Secrecy

We start with the derivation of some general upper bounds for the secrecy measured by the opponent's average uncertainty about the message after observing the cryptogram. These are combined in the next theorem.

Theorem 47 *For every secrecy system*

$$\begin{aligned} H(X|Y) &\le \min\{H(X), H(Z|Y)\} \le \min\{H(X), H(Z)\} \\ &\le \min\{H(X), \log K\} \le \log K. \end{aligned} \tag{2.4.1}$$

Proof The statement immediately follows if we can show $H(X|Y) \le H(Z|Y)$. Recall that cryptogram and key determine the message, i.e., $H(X|Y,Z) = 0$ and therefore

$$H(X|Y) \le H(X,Z|Y) = H(X|Y,Z) + H(Z|Y) = H(Z|Y). \qquad \square$$

Keeping this in mind we can derive necessary conditions for the perfectness of a cipher.

Theorem 48 *If a secrecy system is perfect, then*

$$H(Z) \geq H(X).$$

Proof Recall that a secrecy system is said to be perfect, if the random variables for the message and the cryptogram are independent, i.e., $H(X) = H(X|Y)$. Combining this with (2.4.1) yields the desired result. □

Theorem 49 *If a secrecy system is perfect, then*

$$K \geq M.$$

Proof Recall that we have assumed all messages and keys to occur with probability strictly greater than 0. Therefore the fact that X and Y are independent implies for any $y \in \mathcal{M}$

$$P_{X|Y}(m|y) = P_X(m) \text{ for all } m \in \mathcal{M}.$$

Hence, for every $m \in \mathcal{M}$ there exists at least one key $z \in \{1, \ldots, K\}$ such that $m = c_z^{-1}(y)$. As the keys are injective this implies $K \geq |\mathcal{M}|$. □

These are quite pessimistic results, which tell us that perfect secrecy requires that the uncertainty about the key must be at least as big as the uncertainty about the message and that the secrecy system must contain more keys than messages.

Example 7 We show that it is possible to guarantee perfect secrecy with $K = M$ keys. Let

$$c_z(m) \triangleq (m + z) \bmod M \quad \text{for all } m, z \in \{1, \ldots, M\}$$

and let the keys be equiprobable, i.e., $P_Z(z) \triangleq \frac{1}{M}$ for all $z \in \{1, \ldots, M\}$.

This cipher has the property that for every message $m \in \mathcal{M}$ and every cryptogram $y \in \mathcal{M}$ there exists exactly one key c_z with $c_z(m) = y$ and therefore we immediately get that $P_{X|Y}(m|y) = P_X(m)$. Hence, $H(X|Y) = H(X)$, which means that the secrecy system is perfect. Moreover it is perfect independent of the kind of distribution P_X and one can speak therefore of a robustly perfect cipher. Note that if $K = M$, then every regular and canonical cipher (what will be defined in the next section) has the here described properties.

The idea to use of $K = M$ keys in such a way that a message and a cryptogram is consistent with exactly one key was first developed by G.S. Vernam in 1926 ([18], pp. 7). He enciphered messages given as binary strings by adding binary strings of the same length componentwise modulo 2, that is, in the Vernam cipher each single message bit is enciphered with a new randomly chosen key bit. As the key bits are used only one time those systems are called *One-Time Systems* (or *One-Time Pads* in some contexts). They are only used for transmission of highly confidential information because of the large number of keys.

Regular and Canonical Ciphers

Usually we will restrict ourselves to ciphers where the keys are equiprobable.

Definition 34 A cipher $(\mathcal{C}, Q)$ is canonical, if Q is the uniform distribution.

From now on we will *always* assume ciphers to be canonical. This restriction is usually done [1, 13, 24, 25] and it does not seem to be severe but this has not been proved.

Definition 35 A cipher $(\mathcal{C}, Q)$ is regular, if $|\{c_z^{-1}(y) \,:\, z \in \{1, \ldots, K\}\}| = K$ for any cryptogram $y \in \mathcal{M}$.

Now suppose we are given a number $S \in \mathbb{N}$ and two partitions $\mathcal{X} = \{\mathcal{X}_i : i = 1, \ldots, S\}$ and $\mathcal{Y} = \{\mathcal{Y}_i : i = 1, \ldots, S\}$ of the set $\mathcal{M}$.

Definition 36 A cipher $(\mathcal{C}, Q)$ is locally regular (with respect to $(\mathcal{X}, \mathcal{Y})$) if:

1. $|\mathcal{X}_i| = |\mathcal{Y}_i|$ for all $i \in \{1, \ldots, S\}$.
2. $c_z(\mathcal{X}_i) \subset \mathcal{Y}_i$ for all $z \in \{1, \ldots, K\},\ i \in \{1, \ldots, S\}$.
3. $(\mathcal{C}, Q)$ is a regular cipher.

Remark 19 By definition every locally regular cipher is regular and every regular cipher is locally regular at least with respect to the trivial partitions $(\mathcal{X}, \mathcal{Y})$ which consist only of the set $\mathcal{M}$.

Using "random ciphers" Shannon [24] gave the following lower bound on $H(X|Y)$ (under the additional AEP hypothesis on the message source).

$$H(X|Y) \geq \log K + H(X) - \log M.$$

With our notion of regular ciphers, we get this bound for every regular cipher and without any assumption on the message source $(\mathcal{M}, P_X)$, just by observing that $H(Y|X) = \log K$ in those situations and therefore

$$\begin{aligned} H(X|Y) &= H(X, Y) - H(Y) \\ &= H(Y|X) + H(X) - H(Y) = \log K + H(X) - H(Y). \\ &\geq \log K + H(X) - \log M \end{aligned} \tag{2.4.2}$$

If $H(X) = \log M$, i.e., if the source is compressed, then the bound is tight but for general X it is rather poor. In the Sect. 2.4.3 we give a better bound by evaluating $H(X|Y)$ for a certain cipher. Ahlswede considers in [1] the class of message sources $(\mathcal{M}, P_X)$ with $H(X) \geq H_0$ for some constant $0 \leq H_0 \leq \log M$. Then (2.4.2) obviously implies for any such source

$$H(X|Y) \geq \log K + H_0 - \log M. \tag{2.4.3}$$

This bound reflects a robustified model, where one drops the assumption that sender and receiver know the message statistics. The opponent is still granted to know it exactly but sender and receiver only have to know a lower bound on the entropy of the source. In [1] it was also shown that the bound (2.4.3) is essentially best possible for this class of sources.

2.4.2 The Lower Bound for Locally Regular Ciphers

We now derive the fundamental result of Shtarkov in [25], where he gives a lower bound on $H(X|Y)$ for any locally regular cipher, which uses as information about the message statistics the relation of the greatest to the smallest probability of the messages in each of the sets $\mathcal{X}_i$ (recall Definition 36). Essential for the derivation of this bound is the Schur-concavity of the entropy function.

Lemma 16 *Let P and Q be two probability distributions on $\{1, \ldots, K\}$ with $P(1) \geq \cdots \geq P(K)$ and $Q(1) \geq \cdots \geq Q(K)$. Furthermore let $P(1) = Q(1)$ and $P(K) = Q(K)$. If P has the property that all the probabilities $P(i)$ are equal to $P(1)$ or $P(K)$, i.e., if there exists an $n \in \{1, \ldots, K-1\}$ with $P(1) = \cdots = P(n)$ and $P(n+1) = \cdots = P(K)$, then*

$$H(P) \leq H(Q).$$

Proof The statement follows from the Schur-concavity of the entropy function, if we can show that P Schur-dominates Q, i.e., if

$$\sum_{i=1}^{j} P(i) \geq \sum_{i=1}^{j} Q(i) \qquad \text{for all } j \in \{1, \ldots, K\}.$$

Let $j \in \{1, \ldots, K\}$.

Case 1: $j \leq n$, then

$$\sum_{i=1}^{j} P(i) = j\,P(1) = j\,Q(1) \geq \sum_{i=1}^{j} Q(i).$$

Case 2: $j > n$, then

$$\sum_{i=1}^{j} P(i) = 1 - \sum_{i=j+1}^{K} P(i) = 1 - (K-j)\,P(K) = 1 - (K-j)\,Q(K)$$

$$\geq 1 - \sum_{i=j+1}^{K} Q(i) = \sum_{i=1}^{j} Q(i).\square$$

□

Theorem 50 (Shtarkov) *Let* $(\mathcal{C}, Q)$ *be a locally regular cipher with respect to* $(\mathcal{X}, \mathcal{Y})$. *Let*

$$\rho_i \triangleq \frac{\max\limits_{m\in\mathcal{X}_i} P_X(m)}{\min\limits_{m\in\mathcal{X}_i} P_X(m)} \quad \textit{for all} \quad i = 1, \ldots, S. \tag{2.4.4}$$

Then

$$H(X|Y) \geq \log K - (\log e) \sum_{i=1}^{S} P_i\, \delta(\rho_i), \tag{2.4.5}$$

where

$$P_i \triangleq \sum_{m\in\mathcal{X}_i} P_X(m)$$

and

$$\delta : [1, \infty[\to \mathbb{R}$$

$$\delta(1) \triangleq 0$$

$$\delta(\rho) \triangleq \begin{cases} \ln(\rho - 1) - \ln\ln\rho - 1 + \frac{\ln\rho}{\rho-1}, & 1 < \rho \leq T \\ \ln\left(\frac{\rho K}{\rho+K-1}\right) - \frac{K-1}{\rho+K-1}\ln\rho, & \rho > T \end{cases} \tag{2.4.6}$$

and $T = T(K)$ *is the greatest solution of the equation*

$$(T\,\ln T - T + 1)\,K = (T-1)^2 \tag{2.4.7}$$

Proof $\delta'(\rho) = \frac{(\rho\ln\rho+1-\rho)(\rho-1-\ln(\rho))}{\rho\ln\rho(\rho-1)^2} \geq 0, \quad \text{if } 1 < \rho < T(K).$

$\delta'(\rho) = \frac{(K-1)\ln\rho}{(K+\rho-1)^2} \geq 0, \quad \text{if } T(K) < \rho.$

Hence, as the function δ is continuous we see that it is monotonically increasing. From the local regularity of the cipher follows that

$$\begin{aligned} H(X|Y) &= \sum_{y\in\mathcal{M}} P_Y(y)\, H(X|Y=y) = \sum_{i=1}^{S}\sum_{y\in\mathcal{Y}_i} P_Y(y) H(X|Y=y) \\ &\geq \sum_{i=1}^{S} P_i \min_{y\in\mathcal{Y}_i} H(X|Y=y). \end{aligned}$$

Thus we are done if we can show that for any $i \in \{1, \ldots, S\}$

$$H(X|Y=y) \geq \log K - (\log e)\delta(\rho_i) \qquad \text{for all } y \in \mathcal{Y}_i. \tag{2.4.8}$$

because this implies (2.4.5). So let $i \in \{1, \ldots, S\}$ and $y \in \mathcal{Y}_i$.

Case 1: $\rho_i = 1$.

In this case all messages in $\mathcal{X}_i$ are equiprobable and therefore for any $m \in \mathcal{X}_i$ $P_{X|Y}(m|y) = \frac{1}{K}$ provided that $P_{X|Y}(m|y) > 0$.

This implies $H(X|Y = y) = \log K$ and as $\delta(\rho_i)$ is defined to be 0 in this case the estimate (2.4.8) holds.

Case 2: $\rho_i > 1$.

Let

$$\rho_i(y) \triangleq \frac{\max\limits_{m \in \mathcal{X}_i} P_{X|Y}(m|y)}{\min\limits_{m \in \mathcal{X}_i} P_{X|Y}(m|y)},$$

where the minimum is taken only over terms strictly greater than 0.

If for $m, m' \in \mathcal{X}_i$ $P_{X|Y}(m|y) > 0$ and $P_{X|Y}(m'|y) > 0$, then the local regularity of the cipher implies that $\frac{P_{X|Y}(m|y)}{P_{X|Y}(m'|y)} = \frac{P_X(m)\frac{1}{K}}{P_X(m')\frac{1}{K}} = \frac{P_X(m)}{P_X(m')}$. If all these conditional probabilities would be greater than 0, then we would have $\rho_i(y) = \rho_i$, but if $|\mathcal{X}_i| > K$ then some of the conditional probabilities are equal to 0 and therefore we get $\rho_i(y) \leq \rho_i$, in general. If we take into account that δ is monotonically increasing then we see that it suffices to show (2.4.8) with ρ_i replaced with $\rho_i(y)$. In order to get this lower estimate we ask for what probability distribution $P_{X|Y}(\cdot|y)$ the entropy $H(X|Y = y)$ is minimal if ρ_i is given.

Let c_i denote the smallest probability of such a distribution (then $\rho_i\, c_i$ is the largest) then we know from Lemma 16 a lower bound on the entropy given by the entropy of the distribution with n_i values equal to $\rho_i\, c_i$ and $K - n_i$ values equal to c_i, which is

$$-\, n_i\, \rho_i\, c_i \log \rho_i\, c_i - (K - n_i) c_i \log c_i, \tag{2.4.9}$$

where n_i is determined by the equation $n_i\, \rho_i\, c_i + (K - n_i)\, c_i = 1$ and therefore

$$n_i = \frac{1 - K\, c_i}{c_i\, (\rho_i - 1)}. \tag{2.4.10}$$

If we substitute (2.4.10) into (2.4.9), we can minimize over c_i. The first and second derivative of (2.4.9) with respect to c_i are

$$\frac{1}{\ln 2}\left(\frac{\rho_i\, K}{\rho_i - 1} \ln \rho_i - \frac{1}{c_i}\right)$$

and

$$\frac{1}{c_i^2\, \ln 2} > 0.$$

In this way we obtain that (2.4.9) is minimal for $c_i^\star$ and $n_i^\star$, where

$$c_i^\star = \frac{\rho_i - 1}{K\, \rho_i \ln \rho_i} \text{ and } n_i^\star = K \frac{\rho_i \ln \rho_i - \rho_i + 1}{(\rho_i - 1)^2}.$$

If we substitute these values in (2.4.9), then we get as a lower bound for $H(X|Y=y)$ the bound in (2.4.8), where δ is defined by the first expression in (2.4.6).

Now notice that we have $n_i \geq 1$ as an additional restriction. So if $n_i^\star < 1$, which is the case if $\rho_i > T(K)$, then we get a sharper lower bound by taking $n_i^\star = 1$ and correspondingly $c_i^\star = \frac{1}{\rho_i + K - 1}$. Substituting these terms into (2.4.9) we obtain again the bound (2.4.8) now with δ defined in the second expression of (2.4.6). □

Corollary 4 *Let*

$$\rho \triangleq \frac{\max\limits_{m \in \mathcal{M}} P_X(m)}{\min\limits_{m \in \mathcal{M}} P_X(m)}. \tag{2.4.11}$$

With the assumptions of Theorem 50 it follows

$$\begin{aligned} H(X|Y) &\geq \log K - (\log e)\, \delta(\max_{1 \leq i \leq S} \rho_i) \\ &\geq \log K - (\log e)\, \delta(\rho). \end{aligned} \tag{2.4.12}$$

Proof The bounds follow from (2.4.5), $\rho_i \leq \rho$ for all $i \in \{1, \ldots, S\}$ and the fact that the function δ is monotonically increasing. □

Remark 20

1. Equation (2.4.7) has always the solution $T = 1$. For $K \geq 3$ there exists exactly one other solution greater 1.
2. The lower bound on $H(X|Y)$ is always nontrivial, in the sense that the term in (2.4.12) is always nonnegative because we have seen that it is a value of the entropy function.

2.4.3 A Simple Cipher

Suppose that the probabilities $P_X(m)$ are ordered in such a way that

$$P_X(1) \geq \cdots \geq P_X(M). \tag{2.4.13}$$

Furthermore let $K \leq M$. We consider now the problem of constructing a good cipher if the distribution P_X and the number of keys K is given. A natural approach to the solution of this problem was given by Ahlswede [1], who defined a locally regular cipher with respect to $(\mathcal{X}, \mathcal{Y})$ with

$$\mathcal{X} \triangleq \{\mathcal{X}_i : i = 1, \ldots, S\} \text{ and } \mathcal{Y} \triangleq \{\mathcal{Y}_i : i = 1, \ldots, S\},$$

where $S \triangleq \left\lfloor \frac{M}{K} \right\rfloor$,

$$\mathcal{X}_i \triangleq \mathcal{Y}_i \triangleq \{(i-1)\,K + 1, \ldots, i\,K\} \qquad i = 1, \ldots, S-1$$

$$\text{and } \mathcal{X}_S \triangleq \mathcal{Y}_S \triangleq \{(S-1)K+1, \ldots, M\}.$$

Let $(\mathcal{C}, Q)$ be any locally regular cipher with respect to $(\mathcal{X}, \mathcal{Y})$.

It is clear that this choice of the cipher provides the minimal or close to the minimal values of the ρ_i and therefore yields the maximal or close to maximal estimate of $H(X|Y)$ in (2.4.5). Recall that for an regular cipher $H(X|Y) = \log K + H(X) - H(Y)$. Therefore the optimal choice of the cipher is it to minimize $H(Y)$. P_Y is a "smoothed" version of P_X. For the construction above almost equiprobable messages are put together in the sets $\mathcal{X}_i$ and the resulting P_Y is the corresponding "step approximation" of P_X. Hence, it is clear that the above choice of the partitions tries to minimize the action of the smoothing and therefore should be the best or close to the best one.

But before analyzing $H(X|Y)$ for this cipher let us take a look at the other secrecy criterion introduced in Section "Measurements for Secrecy" of Sect. 2.2. We proved in Theorem 1 that the cryptanalyst's error probability λ satisfies

$$\frac{K-1}{K}(1 - P_X(1)) \leq \lambda \leq (1 - P_X(1)). \tag{2.4.14}$$

It was shown in [1] that if M is a multiple of K and $P_X(m) \leq \frac{1}{K}$ for all $m \in \mathcal{M}$, then for the described cipher

$$H(X|Y) \geq \log K - 1. \tag{2.4.15}$$

Using Lemma 4 and (2.4.14) we can prove that this holds also if M is not a multiple of K.

Theorem 51 *For the cipher $(\mathcal{C}, Q)$ described above*

$$H(X|Y) \geq \log K - \log\Big((K-1)P_X(1) + 1\Big). \tag{2.4.16}$$

Proof From Lemma 4 it follows that $H(X|Y) \geq -\log \lambda_c = -\log(1-\lambda)$ and with (2.4.14) we obtain

$$H(X|Y) \geq -\log\Big(1 - \frac{K-1}{K}(1 - P_X(1))\Big) = \log K - \log\Big((K-1)P_X(1) + 1\Big).$$

□

Corollary 5 *If $P_X(1) \leq \frac{1}{K}$ then for the cipher $(\mathcal{C}, Q)$*

$$H(X|Y) \geq \log K - 1.$$

Proof If $P_X(1) \leq \frac{1}{K}$, then we get from (2.4.16)

$$H(X|Y) \geq \log K - \log\left(2 - \frac{1}{K}\right) \geq \log K - 1. \qquad \square$$

Shtarkov [25] derives the following lower bound for this cipher.

Theorem 52 *If M is a multiple of K then for the cipher $(\mathcal{C}, Q)$ described above*

$$H(X|Y) \geq \log K - \frac{K}{2}(\log e)\Big(P_X(1) - P_X(M)\Big). \tag{2.4.17}$$

Proof Let $m \in \mathcal{X}_i$ and $y \in \mathcal{Y}_i$ for some $i \in \{1, \ldots, S\}$. By construction of the cipher it follows that

$$P_{X|Y}(m|y) = \frac{P_{X,Y}(m, y)}{P_Y(y)} = \frac{\frac{1}{K}P_X(m)}{\sum_{m\in\mathcal{X}_i} P_X(m)\frac{1}{K}} = \frac{P_X(m)}{P_i},$$

with $P_i \triangleq \sum_{m\in\mathcal{X}_i} P_X(m)$. Note that for $m \in \mathcal{X}_i$ $P_{X|Y}(m|y)$ is independent of $y \in \mathcal{Y}_i$. Hence, we know from Lemma 16 that for given $y \in \mathcal{Y}_i$ that $H(X|Y = y)$ is minimal if P_X is concentrated on two values in $\mathcal{X}_i$. In order to get a lower bound on $H(X|Y)$ we may therefore assume that for all $i \in \{1, \ldots, S\}$ there exist numbers $n_i \in \{1, \ldots, K - 1\}$ with the property

$$\alpha_i \triangleq P_X(K(i-1)+1) = \cdots = P_X(K(i-1)+n_i)$$

and

$$\beta_i \triangleq P_X(K(i-1)+n_i+1) = \cdots = P_X(K\,i).$$

Then (2.4.13) implies that

$$\alpha_1 \geq \beta_1 \geq \alpha_2 \geq \beta_2 \geq \cdots \geq \alpha_S \geq \beta_S$$

and $P_i = n_i\,\alpha_i + (K - n_i)\beta_i$. With these preliminaries we calculate now $H(X|Y)$.

$$H(X|Y) = \sum_{i=1}^{S}\sum_{y\in\mathcal{Y}_i} P_Y(y)H(X|Y=y)$$

$$= -\sum_{i=1}^{S} P_i \sum_{m\in\mathcal{X}_i} \frac{P_X(m)}{P_i}\log\frac{P_X(m)}{P_i}$$

$$= -\sum_{i=1}^{S} n_i\,\alpha_i \log \frac{\alpha_i}{P_i} + (K - n_i)\beta_i \log \frac{\beta_i}{P_i}$$

$$= \sum_{i=1}^{S} -P_i \log \frac{\alpha_i + \beta_i}{P_i} - n_i\,\alpha_i \log \frac{\alpha_i}{\alpha_i + \beta_i} - (K - n_i)\beta_i \log \frac{\beta_i}{\alpha_i + \beta_i}$$

$$= \sum_{i=1}^{S} -P_i \log \frac{\alpha_i + \beta_i}{2\,P_i} - n_i\,\alpha_i \log \frac{2\,\alpha_i}{\alpha_i + \beta_i} - (K - n_i)\beta_i \log \frac{2\,\beta_i}{\alpha_i + \beta_i}$$

$$= \log K + \sum_{i=1}^{S} -P_i \log \frac{K(\alpha_i + \beta_i)}{2\,P_i} - n_i\,\alpha_i \log \frac{2\,\alpha_i}{\alpha_i + \beta_i} - (K - n_i)\beta_i \log \frac{2\,\beta_i}{\alpha_i + \beta_i}.$$

Now we use the inequality $-\ln x \geq 1 - x$ and obtain

$$H(X|Y) \geq \log K - (\log e)\frac{K}{2} \sum_{i=1}^{S} \frac{(\alpha_i - \beta_i)^2}{\alpha_i + \beta_i}.$$

Recall that $\alpha_i \geq \beta_i \geq \alpha_{i+1} \geq 0$ and therefore

$$H(X|Y) \geq \log K - (\log e)\frac{K}{2}\left(\sum_{i=1}^{S-1}(\alpha_i - \alpha_{i+1})\frac{\alpha_i - \beta_i}{\alpha_i + \beta_i} + (\alpha_S - \beta_S)\frac{\alpha_S - \beta_S}{\alpha_S + \beta_S}\right)$$

$$\geq \log K - (\log e)\frac{K}{2}\left(\sum_{i=1}^{S-1}(\alpha_i - \alpha_{i+1}) + \alpha_S - \beta_S\right)$$

$$= \log K - (\log e)\frac{K}{2}(\alpha_1 - \beta_S) = \log K - (\log e)\frac{K}{2}\Big(P_X(1) - P_X(M)\Big). \quad \square$$

Remark 21

1. If $P_X(m) \leq \frac{1}{K}$ for all $m \in \mathcal{M}$, then (2.4.15) is improved to

$$H(X|Y) \geq \log K - \frac{1}{2}(\log e)K\frac{1}{K} = \log K - \frac{1}{2}\log e \approx \log K - 0.72\,.$$

2. If P_X is the uniform distribution, then it follows $H(X|Y) \geq \log K$ and therefore $H(X|Y) = \log K$.
3. The bound in (2.4.5) is ≥ 0 exactly if $P_X(1) - P_X(M) \leq \frac{2\ln K}{K}$. Therefore it may happen that this bound is weaker than the bound of Theorem 50.
4. In order to construct the described cipher it is not necessary that sender and receiver know the message distribution P_X exactly. They (only) have to know

the information about the ordering of messages according to probability which is needed to form the partitions $\mathcal{X}$ and $\mathcal{Y}$.

2.4.4 Data Compression

We would like to analyze the effects of data compression in a cryptographic system. In all our previous considerations a message was an element of some set of other messages which occur with some probabilities. We have not been interested in the description of the messages. In a lot of applications the messages are given as a sequence of letters over a finite alphabet and we will assume that these sequences are produced by a source. This allows to install a source coder before using a cipher. The idea behind this is to remove the redundancy that helps a cryptanalyst.

Before we proceed we need some definitions to formalize the described scenario.

Preliminaries

In the sequel let $\mathcal{A} \triangleq \{0, \ldots, a-1\}$ for some $a \in \mathbb{N}$ with $a \geq 2$.

Definition 37 We call the set $\mathcal{A}$ an alphabet. An element of $\mathcal{A}$ is referred to as a letter and an element of $\mathcal{A}^n$ is called a word (of length n over $\mathcal{A}$). We denote the set of all words (over $\mathcal{A}$) by

$$\mathcal{A}^\star \triangleq \bigcup_{n=0}^{\infty} \mathcal{A}^n.$$

For a word $u \in \mathcal{A}^\star$ we denote by $l(u)$ its length.

Remark 22 Note that also the word with length 0 belongs to $\mathcal{A}^\star$. This is called the empty word.

We define the concatenation of two words and the prefix property.

Definition 38 Let $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_m) \in \mathcal{A}^\star$ be two words. We denote by

$$uv \triangleq (u_1, \ldots, u_n, v_1, \ldots, v_m)$$

their concatenation.

We say that u is a prefix of v if their exists a $w \in \mathcal{A}^\star$ such that $uw = v$ and we write in this case $u \preccurlyeq v$. We say that a set of words $\mathcal{W} \subset \mathcal{A}^\star$ has the prefix property (or shortly is a prefix set) if no element of $\mathcal{W}$ is prefix of another element, i.e., $u \preccurlyeq v$ for two elements $u, v \in \mathcal{W}$ necessarily implies $u = v$.

Remark 23 A well known fact is that a prefix set $\mathcal{W}$ satisfies the Kraft inequality, which is

$$\sum_{u \in \mathcal{W}} a^{-l(u)} \leq 1.$$

(See, for instance, [5], pp. 41.)

We would like to describe the output of a source which is a sequence of letters as a sequence of elements of a prefix set. Therefore the next definition is important.

Definition 39 We call a set $\mathcal{W} \subset \mathcal{A}^\star$ complete if for all $v \in \mathcal{A}^\star$ there exists a $u \in \mathcal{W}$ with $u \preccurlyeq v$ or $v \preccurlyeq u$.

This implies that given a complete set $\mathcal{W}$ we can find for any word $v \in \mathcal{A}^\star$ words $u_1, \ldots, u_n \in \mathcal{W}$ such that

$$v \preccurlyeq u_1 \ldots u_n \text{ and } u_1 \ldots u_{n-1} \preccurlyeq v. \tag{2.4.18}$$

If $\mathcal{W}$ is in addition a prefix set than this decomposition of v is unique except, maybe, for the last word u_n.

Remark 24 A complete prefix set has $i(a-1)+1$ elements (for some $i \in \mathbb{N}_0$) and a prefix set is complete exactly if we have equality in the Kraft inequality ([5], pp. 41).

Definition 40 For some finite set $\mathcal{V}$ we call a mapping $\phi : \mathcal{V} \to \mathcal{A}^\star$ a code. The words $\phi(v),\ v \in \mathcal{V}$, are called codewords.

A code ϕ is said to be uniquely decodable if every word in $\mathcal{A}^\star$ has at most one representation as a sequence of code words, i.e., if the mapping

$$\Phi : \bigcup_{n=1}^{\infty} \mathcal{V}^n \to \mathcal{A}^\star \text{ defined by } \Phi(v_1, \ldots, v_n) \triangleq \phi(v_1)\phi(v_2)\ldots\phi(v_n)$$

is injective.

A code is called a prefix code if the set of codewords is a prefix set.

Remark 25 Every prefix code is uniquely decodable. The opposite is not true but if a uniquely decodable code is given, then it is always possible to find a prefix code with the same codeword lengths (see for instance [5], pp. 51).

Definition 41 A (discrete) source over the alphabet $\mathcal{A}$ is a sequence $(U_n)_{n=1}^{\infty}$ of random variables with values in $\mathcal{A}$.

A source is called stationary if $P_{U_1 \ldots U_n}(u_1, \ldots, u_n) = P_{U_m \ldots U_{n+m-1}}(u_1, \ldots, u_n)$ for all $n, m \in \mathbb{N}$, i.e., if the joint distribution of $(U_m, \ldots, U_{n+m-1})$ does not depend on m (for all $n \in \mathbb{N}$).

Remark 26 A special case of a stationary source is the so called discrete memoryless source where the random variables are independent and identically distributed.

Definition 42 If for a given source $\lim_{n\to\infty} \frac{1}{n} H(U_1 \dots U_n)$ exists then this limit is called the entropy rate of the source.

Remark 27 For a stationary source $\frac{1}{n} H(U_1 \dots U_n)$ is nonincreasing in n and therefore the entropy rate always exist (see, for instance, [8], pp. 65).

The Extension of the Model with a Source Coder

Let $\mathcal{A} \triangleq \{0, \dots, a-1\}$ and $\mathcal{B} \triangleq \{0, \dots, b-1\}$, where $a, b \in \mathbb{N}$ with $a, b \geq 2$, be two alphabets. Suppose now that the messages to be securely transmitted consist of sequences over the alphabet $\mathcal{A}$, which are generated by a source $(U_n)_{n=0}^{\infty}$. The transmission of this source output to the receiver is implemented in three steps.

1. **Source Coding**
   The output of the source is encoded in the following way. Let $\mathcal{V} \subset \mathcal{A}^\star$ be a complete prefix set. According to [25] the elements of the set $\mathcal{V}$ are referred to as 'segments'. With these segments the output of the source is decomposed, i.e., any word $u \in \mathcal{A}^\star$ is split into a sequence of segments from $\mathcal{V}$.

   $$\underbrace{u_1, u_2, \dots, u_{l(v_1)}}_{v_1 \in \mathcal{V}}, \underbrace{u_{l(v_1)+1}, \dots, u_{l(v_1)+l(v_2)}}_{v_2 \in \mathcal{V}}, \dots$$

   Then using a uniquely decodable code $\phi : \mathcal{V} \to \mathcal{B}^\star$ every segment $v \in \mathcal{V}$ is replaced by its codeword $\phi(v)$ over $\mathcal{B}$.
   Thus the source coding allows to transform the sequence of letters from $\mathcal{A}$ into a sequence of letters from $\mathcal{B}$ ruled by a modified probability law.
2. **Encryption**
   The sequence of letters from $\mathcal{B}$ is encrypted in the following way. We take a set $\mathcal{M} \subset \mathcal{B}^\star$ such that we can decompose every possible sequence of letters over $\mathcal{B}$ generated by the encoding procedure and the source into elements from $\mathcal{M}$ (of course it always suffices to choose a complete set $\mathcal{M}$, usually, the set of words over $\mathcal{B}$ with a fixed length n is taken for $\mathcal{M}$, i.e., $\mathcal{M} = \mathcal{B}^n$). Then the elements of $\mathcal{M}$ are encrypted with a cipher $(\mathcal{C}, \mathcal{Q})$ in the usual way. This means the encoded sequence of letters of $\mathcal{B}$ is decomposed into a sequence of elements from $\mathcal{M}$ and each of this elements is encrypted with a secret key $c_z \in \mathcal{C}$ known to the sender and the receiver. Again we will refer to the elements of $\mathcal{M}$ as messages although it has to be remembered that these are only encoded versions of the original messages.
3. **Decryption**
   The receiver can reconstruct the original source output as $c_z : \mathcal{M} \to \mathcal{M}$ is bijective and ϕ is uniquely decodable.

Remark 28 We make Kerckhoffs' assumption (see Section "The Opponent's Knowledge" in Sect. 2.2) that the only thing the opponent does not know about the described

secrecy system is which of the keys is used by sender and receiver. In particular this means that the opponent knows the method how the source is encoded by means of the set of segments $\mathcal{V}$ and the code ϕ.

The described secrecy system is shown schematically in Fig. 2.4. We would like to define a random variable X with values in $\mathcal{M}$ whose distribution is induced by the source and the coding procedure and for the cryptograms a random variable Y with values in $\mathcal{M}$ whose distribution is induced as usual by $\mathcal{C}$ and the distributions of X and Z. (Note that in some cases the distribution of X may not be well defined because the probability that message $m \in \mathcal{M}$ occurs may be dependent upon the point of occurrence of m in the sequence of letters from $\mathcal{B}$ produced by the source and the coding method. Later we will be in a context where this problem does not occur.) Then in [25] the security of such a secrecy system is measured by

$$H(X|Y).$$

In the sequel we restrict ourselves to stationary sources. We say that the source coding is absent if $\mathcal{A} = \mathcal{B}$ and $\mathcal{V} = \mathcal{M} = \mathcal{A}^n$ for some $n \in \mathbb{N}$. If the source coding is absent and the number of keys K satisfies

$$\log K \geq c\, H(X) = c\, H(U_1 \dots U_n), \tag{2.4.19}$$

for some constant $c > 1$ then from Remark 27 it follows that

$$\log K - H(X|Y) \geq \log K - H(X) \geq (c-1)H(X) \geq (c-1)\, n\, H_\infty, \tag{2.4.20}$$

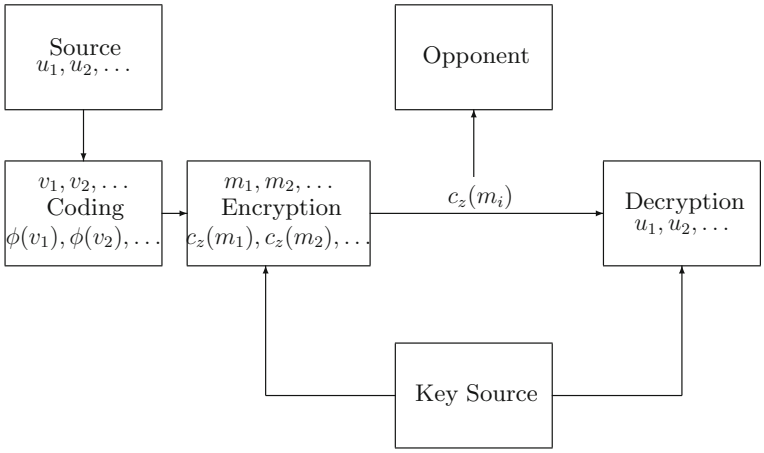


Fig. 2.4 A secrecy system with a source coder

where $H_\infty \triangleq \lim_{n\to\infty} \frac{1}{n} H(U_1 \dots U_n)$ is the entropy rate of the stationary source. It follows from (2.4.20) that if n tends to infinity the difference between $\log K$ and $H(X|Y)$ tends to infinity. It has to be remembered that "n tends to infinity" means according to (2.4.19) that the number of keys K and the number of messages $M \triangleq |\mathcal{M}|\ (= a^n)$ grow in such a way that

$$K \geq \exp(cnH_\infty) = M^{\frac{cH_\infty}{\log a}}.$$

We will see in the next section that the source coding allows to bound the difference $\log K - H(X|Y)$ above by a constant, which is independent of n. Therefore the source coding seems to be reasonable at least for numbers of keys K satisfying (2.4.19) and also the other cases require a special analysis.

If we use a cipher, which is locally regular with respect to $(\mathcal{X}, \mathcal{Y})$, then, in order to get a large value of $H(X|Y)$, we should use a source coding procedure such that the resulting distribution P_X is as uniform as possible within each of the sets $\mathcal{X}_i$, but quite different for different $\mathcal{X}_i$. This criterion has not been treated so far and Shtarkov [25] says that *in general the redundancy cannot characterize the efficiency of the source coding for the information protection.*

In the way we introduced the source coding the segments $v \in \mathcal{V}$ may have different lengths and also the codewords $\phi(v)$ may have different lengths. Then we speak of a variable-to-variable length coding. Beside the above mentioned problem that the distribution of X may not be well defined also the analysis of the value $H(X|Y)$ encounter some difficulties in this case because a given message $m \in \mathcal{M}$ may begin with a suffix of different codewords of ϕ or end with the prefix of different codewords of ϕ.

These problems do not arise if we consider the variable-to-fixed length coding procedure of the next section.

Variable-to-Fixed Length Coding

We now use codes ϕ such that all the codewords $\phi(v)$ have the same length. If we take $n \in \mathbb{N}$ for the length, then ϕ has the property that

$$\phi(\mathcal{V}) \subset \mathcal{B}^n.$$

We take

$$\mathcal{M} \triangleq \phi(\mathcal{V}).$$

Then $M = |\mathcal{V}|$ and the distribution of X is given by $P_X(m) = P_{U_1 \dots U_{l(v)}}(v)$ for $m \in \mathcal{M}$ and $v \in \mathcal{V}$ with $\phi(v) = m$.

A minimization of the average description length of the source output in the context of variable-to-fixed length coding means, as the length of the codewords is given, that one has to maximize the average length of the segments (in contrast to the minimization of the average codeword length in fixed-to-variable length coding). The solution to this problem under the constraints that the number of segments $|\mathcal{V}|$ is

given and that the set of segments has to be complete is known as Tunstall's method of coding which is a recursively defined procedure (of course the number of segments must be of the in Remark 24 described form because otherwise one cannot find a complete prefix set with this cardinality).

Tunstall's Method of Coding Define complete prefix sets $\mathcal{V}_i \subset \mathcal{A}^\star$ in the following way. Let

$$\mathcal{V}_1 \triangleq \mathcal{A}, \tag{2.4.21}$$

i.e., we take for $\mathcal{V}_1$ the set of all one letter words. If $\mathcal{V}_i$ ($i \in \mathbb{N}$) is already defined then let

$$\mathcal{V}_{i+1} \triangleq \mathcal{V}_i \backslash \{v_i^\star\} \cup \{v_i^\star u : u \in \mathcal{A}\}, \tag{2.4.22}$$

where $v_i^\star \in \mathcal{V}_i$ is chosen such that $P_{U_1 \ldots U_{l(v_i^\star)}}(v_i^\star) = \max_{v \in \mathcal{V}} P_{U_1 \ldots U_{l(v)}}(v)$ (if the choice of $v_i^\star$ is not unique we take any such element). Thus $\mathcal{V}_{i+1}$ is constructed by appending to the most probable element in $\mathcal{V}_i$ one letter in all possible ways.

Clearly, by construction $\mathcal{V}_i$ is a complete prefix set with $|\mathcal{V}_i| = i(a-1)+1$. The associated variable-to-fixed length code is a mapping $\phi_i : \mathcal{V}_i \to \mathcal{B}^n$, which is injective and $n \triangleq \lceil \log_b(i(a-1)+1) \rceil$ is the minimal possible codeword length.

The proof for the optimality of Tunstall's method of coding can be found in ([30], see also [11], pp. 418). For our purposes we need only the following property of the sets $\mathcal{V}_i$. Let V_i be a random variable with values in $\mathcal{V}_i$ and distribution $P_{V_i}(v) \triangleq P_{U_1 \ldots U_{l(v)}}(v)$ for any $v \in \mathcal{V}_i$.

Lemma 17 *Let $(U_n)_{n=0}^\infty$ be a discrete memoryless source and let $\mathcal{V}_i$ be constructed according to (2.4.21) and (2.4.22) for some $i \in \mathbb{N}$. Then*

$$\frac{\max_{v \in \mathcal{V}_i} P_{V_i}(v)}{\min_{v \in \mathcal{V}_i} P_{V_i}(v)} \leq \frac{1}{\min_{u \in \mathcal{A}} P_{U_1}(u)}, \tag{2.4.23}$$

where the minima are taken only over terms greater than zero.

Proof Clearly the statement holds for $i = 1$ because

$$\frac{\max_{u \in \mathcal{A}} P_{U_1}(u)}{\min_{u \in \mathcal{A}} P_{U_1}(u)} \leq \frac{1}{\min_{u \in \mathcal{A}} P_{U_1}(u)}.$$

Suppose now that the lemma is proved for $i \in \mathbb{N}$. From (2.4.22) follows that

$$\max_{v \in \mathcal{V}_{i+1}} P_{V_{i+1}}(v) \leq \max_{v \in \mathcal{V}_i} P_{V_i}(v).$$

This implies that if $\min_{v \in \mathcal{V}_{i+1}} P_{V_{i+1}}(v) = \min_{v \in \mathcal{V}_i} P_{V_i}(v)$ the statement holds also for $i+1$. Therefore we may assume that there exists an $u \in \mathcal{A}$ such that $P_{V_{i+1}}(v_i^\star u) = \min_{v \in \mathcal{V}_{i+1}} P_{V_{i+1}}(v)$. But then it follows

$$\frac{\max\limits_{v\in\mathcal{V}_{i+1}} P_{V_{i+1}}(v)}{\min\limits_{v\in\mathcal{V}_{i+1}} P_{V_{i+1}}(v)} \le \frac{P_{V_i}(v_i^\star)}{P_{V_{i+1}}(v_i^\star u)} = \frac{1}{P_{U_1}(u)} \le \frac{1}{\min\limits_{u\in\mathcal{A}} P_{U_1}(u)}.$$ □

Remark 29 It is easy to generalize Lemma 17 (and therefore also the next theorem) to Markovian sources. In these cases the minimum on the right-hand side of (2.4.23) has to be taken over the transition probabilities ([11], pp. 423).

Theorem 53 *Let $(U_n)_{n=0}^{\infty}$ be a discrete memoryless source. Let $\mathcal{V}_i$ and ϕ_i be given by Tunstall's method of coding. Then for any regular cipher $(\mathcal{C}, Q)$*

$$\log K - H(X|Y) \le (\log e)\,\delta\Big(\frac{1}{\min\limits_{u\in\mathcal{A}} P_{U_1}(u)}\Big),$$

where δ is the function defined in (2.4.6).

Proof The statement follows by combining Corollary 4 and Lemma 17. Lemma 17 implies that in (2.4.11) we get

$$\rho \le \frac{1}{\min\limits_{u\in\mathcal{A}} P_{U_1}(u)}$$

and therefore, as the function δ is monotonically increasing, the estimate in (2.4.12) implies that

$$H(X|Y) \ge \log K - (\log e)\,\delta\Big(\frac{1}{\min\limits_{u\in\mathcal{A}} P_{U_1}(u)}\Big).$$ □

Note that we have bounded the difference $\log K - H(X|Y)$ by a constant, which does not depend on M and K for any regular cipher.

Next we consider a simple example, which is taken from [25]. Suppose we are given a binary memoryless source, i.e., $\mathcal{A} \triangleq \{0, 1\}$ and the random variables U_i are independent and identically distributed. Let $P_{U_i}(0) \triangleq \frac{59}{64}$ and $P_{U_i}(1) \triangleq \frac{5}{64}$ for all $i \in \mathbb{N}$. We take 64 segments and messages, respectively, i.e., $|\mathcal{V}| \triangleq M \triangleq 64$ and as we take also a binary coding alphabet $\mathcal{B} \triangleq \{0, 1\}$ the lengths of the codewords is 6 and $\mathcal{M} = \mathcal{A}^6$. We consider two possible choices of the set of segments $\mathcal{V}$.

(a) *Absence of Source Coding*
Let $\mathcal{V} \triangleq \mathcal{A}^6$.

(b) *Optimal Variable-to-Fixed Length Coding for the given Source*
Let $\mathcal{V} \triangleq \mathcal{V}_{63}$, i.e., $\mathcal{V}$ is constructed by Tunstall's method for the given source. Then $\mathcal{V}$ contains the following segments:

$$0^i10^j1 \quad \text{and} \quad 0^i10^{6-i}, \quad \text{for } i = 0, 1, 2 \quad j = 0, 1, \ldots, 5 - i,$$

$$0^i10^j1 \quad \text{and} \quad 0^i10^{7-i}, \quad \text{for } i = 3, 4, 5, 6 \quad j = 0, 1, \ldots, 6 - i,$$

$$0^i1, \quad \text{for } i = 7, 8, \ldots, 37$$

$$\text{and } 0^{38},$$

where we denote by $u^i \triangleq \underbrace{(u, \ldots, u)}_{i-\text{times}}$ the word of length i with letters all equal to u ($u \in \mathcal{A}$).

For these two choices of the segments we take the cipher of Sect. 2.4.3 with $\mathrm{K} = 2, 4, 8, \ldots, 64$ keys. The calculated values of $H(X|Y)$ are presented in Table 2.1. The values in row (c) will be treated in Sect. 2.4.5. Now we can take a look at the performance of the bounds we derived in Theorems 50 and 52. Let us first look at the case (a) when the source coding is absent. The values that the bound in (2.4.5) returns and the deviation from the actual value of $H(X|Y)$ are shown in the Table 2.2. The estimates are good for $K < 8$ because then $\rho_1 = 11.8$ and many of the values ρ_i are equal to 1 since in the blocks of length K often occur words with the same number of zeros. The bound in (2.4.17) degenerates in case (a), as $P_X(0^6) - P_X(1^6) = 0.614$ is very large.

For the case (b) we consider the simpler bound in (2.4.12) and the bound in (2.4.17). The values of these bounds and the deviation to $H(X|Y)$ are shown in Table 2.3. Already the simpler bound in (2.4.12) returns values that are approximately not more than 1 bit away from $H(X|Y)$. The bound in (2.4.17) becomes worse with increasing K but as the difference of the probabilities of the most probable segments 0^i10^{6-i} $(i = 0, 1, 2)$ and the most unlikely segment $0^i10^{6-i}1$ $(i = 3, 4, 5, 6)$ is only 0.044 it beats the bound (2.4.12) for all K up to 32.

Table 2.1 Calculated values of $H(X|Y)/H(V|Y)$

$\log K$	1	2	3	4	5	6
(a)	0.563	1.217	1.901	2.137	2.334	2.373
(b)	0.999	1.997	2.987	3.961	4.802	5.407
(c)	0.156	0.254	0.340	0.389	0.393	0.396

Table 2.2 Performance of the bound in (2.4.5) for (a)

$\log K$	1	2	3	4	5	6
Bound in (2.4.5)	0.563	1.105	0.563	0.913	0.225	1.842
Difference to $H(X\|Y)$	≈ 0	0.112	1.338	1.224	2.109	0.532

Table 2.3 Performance of the bounds in (2.4.12) and (2.4.17) for (b)

$\log K$	1	2	3	4	5	6
Bound in (2.4.12)	0.375	1.375	1.921	2.921	3.921	4.921
Difference to $H(X\|Y)$	0.624	0.322	1.066	1.04	0.881	0.486
Bound in (2.4.17)	0.936	1.872	2.745	3.49	3.98	3.959
Difference to $H(X\|Y)$	0.063	0.125	0.242	0.471	0.822	1.448

2.4.5 Randomization

An old cryptographic method is the usage of randomized ciphers known as multiple-substitution ciphers or homophonic ciphers. The idea is the substitution of highly probable words by randomly chosen representatives. For instance in a typical English text the letter e appears with the highest frequency. If the letters e are randomly substituted by different symbols all representing the e, then the new text over this larger alphabet may have a more balanced frequency distribution of letters and therefore an enciphering of this modified text can increase the secrecy.

We will extend our model of Sect. 2.4.4 in the following way. Let V be a random variable for the occurrence of the segments, i.e., V has values in $\mathcal{V}$ and the distribution is given by $P_V(v) \triangleq P_{U_1 \ldots U_{l(v)}}(v)$ for all $v \in \mathcal{V}$. We assume that with each occurrence of a segment $v \in \mathcal{V}$ the sender gets to know the value of an additional random variable R with values in some finite set $\mathcal{R}$. In general R and V are not independent. We make the encoding dependent upon the value of R, i.e., we replace the code $\phi : \mathcal{V} \to \mathcal{B}^\star$ by a code $\phi : \mathcal{V} \times \mathcal{R} \to \mathcal{B}^\star$ such that the decoding of a sequence over $\mathcal{B}$ is unique with respect to v. The rest of the model is as treated before. The receiver knowing the secret key can reconstruct the output of the source.

The introduction of the randomization results of course in an enlargement of the codeword lengths (if we take them all equal as before) compared to an absence of the randomization. Therefore we are dealing with to different approaches to increase the secrecy. The first is the elimination of redundancy by means of an effective source coding and the second is the randomization, which can be regarded as a special form of source coding increasing the description length and the redundancy. These approaches seem to be contradictory in principle. However, sometimes this contradiction can be eliminated.

We restrict ourselves again to a variable-to-fixed length encoding. This means we assume

$$\phi(\mathcal{V} \times \mathcal{R}) \subset \mathcal{B}^n \qquad \text{for some } n \in \mathbb{N}$$

and we define

$$\mathcal{M} \triangleq \phi(\mathcal{V} \times \mathcal{R}).$$

Furthermore let

$$\mathcal{M}(v) \triangleq \{m \in \mathcal{M} : m = \phi(v, r),\ r \in \mathcal{R}\} \subset \mathcal{M} \quad \text{for any } v \in \mathcal{V}$$

be the set of all possible messages if the segment v occurs. The decoding is unique with respect to v if the sets $\mathcal{M}(v),\ v \in \mathcal{V}$, are disjoint. Then it follows for the number of messages that

$$M = |\mathcal{M}| = \sum_{v \in \mathcal{V}} |\mathcal{M}(v)| \geq |\mathcal{V}|.$$

Shtarkov [25] notes that in this context the above mentioned contradiction can be eliminated rather simply. The secrecy of such a cryptosystem is related to the value $H(V|Y)$ rather than to the value of $H(X|Y)$ because a message $m \in \mathcal{M}$ is only an auxiliary description for some segment $v \in \mathcal{V}$ and therefore for a part of the original output sequence of the source. Without randomization, i.e., if we consider the secrecy system with the variable-to-fixed length coding scheme of the last section we have

$$H(X|Y) = H(V|Y),$$

but with the introduction of the randomization these values become different and we are interested in the behaviour of $H(V|Y)$. We would like to investigate, if the randomization allows to increase $H(V|Y)$. The inequality $H(V|Y) \leq H(V)$ gives an obvious upper bound and we know from Example 7 that this bound can be achieved *without* randomization if we are allowed to use $K = |\mathcal{V}|$ keys. With randomization the analogous bounds to (2.4.1) hold which is shown by

$$H(V|Y) \leq H(VZ|Y) = H(Z|VY) + \underbrace{H(V|ZY)}_{=0}$$

$$= H(Z|VY) \leq H(Z) \leq \log K.$$

This shows that also with randomization a necessary condition for $H(V) = H(V|Y)$ is that $H(Z) \geq H(V)$.

Under what conditions the randomization allows that the value of $H(V|Y)$ reaches the upper bound $\log K$ is treated in the next theorem.

Theorem 54 *If*

$$K \max_{v \in \mathcal{V}} |\mathcal{M}(v)| \leq M, \tag{2.4.24}$$

then there exists a regular cipher $(\mathcal{C}, Q)$ *with* K *keys such that*

$$H(V|Y) = H(X|Y).$$

If condition (2.4.24) does not hold then for any cipher $(\mathcal{C}, Q)$ with K keys

$$H(V|Y) < H(X|Y) \leq \log K.$$

Proof From the grouping axiom of the entropy function it follows that

$$H(X|Y=y) = H(V|Y=y) + \sum_{v\in\mathcal{V}} P_{V|Y}(v|y)H(P_v),$$

where P_v is the distribution on $\mathcal{M}(v)$ given by $P_v(m) \triangleq \frac{P_{X|Y}(m|y)}{\sum_{m'\in\mathcal{M}(v)} P_{X|Y}(m'|y)}$. Therefore in general we have $H(V|Y=y) \leq H(X|Y=y)$ with equality exactly if for every $v \in \mathcal{V}$ and $y \in \mathcal{M}$ with $P_{V|Y}(v|y) > 0$, there exist only one $m \in \mathcal{M}(v)$ with $P_{X|Y}(m|y) > 0$.

Now let us enumerate the segments, the messages and the cryptograms

$$v_1, \ldots, v_{|\mathcal{V}|} \in \mathcal{V} \quad m_0, \ldots, m_{M-1} \in \mathcal{M} \quad y_0, \ldots, y_{M-1} \in \mathcal{M}.$$

The enumeration of segments and cryptograms is arbitrary. The messages should be enumerated such that the first messages are those of the set $\mathcal{M}(v_1)$, the next are in $\mathcal{M}(v_2)$ and so on. More precisely the following condition has to be satisfied.

$$\mathcal{M}(v_i) = \{m_j \in \mathcal{M} : \eta(i-1) \leq j < \eta(i)\} \quad \text{for all } i = 1, \ldots, |\mathcal{V}|,$$

where

$$\eta(i) \triangleq \sum_{l=1}^{i} |\mathcal{M}(v_l)|$$

for all $i = 0, \ldots, |\mathcal{V}|$ (with the convention that $\sum_{l=1}^{0} \cdots = 0$).

Let $(\mathcal{C}, Q)$ be any regular cipher with K keys such that a message m_j is mapped to the K different cryptograms y_n with

$$n \in \{(K(j-1)+0) \bmod M, (K(j-1)+1) \bmod M, \ldots, (Kj-1) \bmod M\}.$$

Thus for every $v \in \mathcal{V}$ the messages $m \in \mathcal{M}(v)$ are mapped onto $|\mathcal{M}(v)|$ consecutive (modulo M) cryptograms. Therefore (2.4.24) implies that for every $y \in \mathcal{M}$ the set $\{c_z^{-1}(y) \in \mathcal{M} : z = 1, \ldots, K\}$ contains at most one message of every set $\mathcal{M}(v)$. Therefore $H(V|Y) = H(X|Y)$ and the first statement is proved.

On the other hand if (2.4.24) does not hold then for the segment $v \in \mathcal{V}$ with maximal $|\mathcal{M}(v)|$ there exists for any cipher with K keys a cryptogram $y \in \mathcal{M}$ such

that the set $\{c_z^{-1}(y) \in \mathcal{M}\ z = 1, \ldots, K\}$ contains at least two different messages belonging both to $\mathcal{M}(v)$. Therefore we have for this cryptogram

$$H(V|Y = y) < H(X|Y = y)$$

and this proves the second statement. □

If $P_V(v) < \frac{1}{M}$, then it follows for $m \in \mathcal{M}(v)$ that $P_X(m) \leq P_V(v) < \frac{1}{M}$. Therefore only if the minimal nonnegative probability $P_V(v)$ of a segment is not less than $\frac{1}{M}$ it may be possible to get a uniformly distributed random variable X on $\mathcal{M}$. In this case, when M is large enough such that $\min_{v \in \mathcal{V}} P_V(v) \geq \frac{1}{M}$, it suffices to choose the sizes of $\mathcal{M}(v)$ such that $|\mathcal{M}(v)| = M P_V(v)$ for all $v \in \mathcal{V}$ and the random variable R such that for any $v \in \mathcal{V}$ there are $|\mathcal{M}(v)|$ values in $\mathcal{R}$ such that $P_{R|V}(r|v)$ is equal to $\frac{1}{|\mathcal{M}(v)|}$ and for the remaining values in $\mathcal{R}$ $P_{R|V}(r|v)$ is equal to 0 (if $MP_V(v)$ is not an integer, then it is only possible to get an approximate uniform distribution P_X). In this way we obtain $P_X(m) = \frac{P_V(v)}{|\mathcal{M}(v)|} = \frac{1}{M}$ for all $m \in \mathcal{M}(v)$.

Then any regular cipher guarantees $H(X|Y) = \log K$ but Theorem 54 tells us that $H(V|Y) < \log K$ if the condition (2.4.24) is not fulfilled. If (2.4.24) holds then $H(V|Y) = \log K$ for the cipher introduced in the proof of Theorem 54. From condition (2.4.24) follows in the described case

$$K \leq \frac{1}{\max_{v \in \mathcal{V}} P_V(v)} \leq \frac{M}{\rho(\mathcal{V})},$$

where $\rho(\mathcal{V}) \triangleq \frac{\max_{v \in \mathcal{V}} P_V(v)}{\min_{v \in \mathcal{V}} P_V(v)}$.

Shtarkov [25] concludes that the equality $H(V|Y) = \log K$ can be attained at the expense of an increase in M and hence, of implementation complexity. Therefore he compares the results achievable with and without randomization under the same complexity, i.e., for the same values of K and M.

Consider the following example where the letters in the output of a discrete memoryless source are splitted.

Suppose that the probabilities for the occurrence of all letters $u \in \mathcal{A}$ can be written as

$$P_{U_1}(u) = \gamma_u b^{-\omega} \quad \text{for some } \omega, \gamma_u \in \mathbb{N} \text{ with } 0 < \gamma_u < b^{\omega}.$$

(Recall that b is the size of the alphabet $\mathcal{B}$.) Then we can partition the set $\mathcal{B}^{\omega}$ of words of length ω over $\mathcal{B}$ into $a = |\mathcal{A}|$ disjoint sets $\mathcal{B}_u^{\omega}$, $u \in \mathcal{A}$, with $|\mathcal{B}_u^{\omega}| = \gamma_u$ (recall that $\sum_{u \in \mathcal{A}} \gamma_u b^{-\omega} = 1$). Given the letter $u \in \mathcal{A}$ as source output then we may replace it by any element of $\mathcal{B}_u^{\omega}$ with probability $\frac{1}{\gamma_u}$. We can do this independently n times ($n \in \mathbb{N}$) and define in this way the code

$$\phi : \mathcal{A}^n \times \mathcal{R} \to \mathcal{B}^{n\omega},$$

where we chose $\mathcal{V} \triangleq \mathcal{A}^n$ and $\mathcal{M} \triangleq \mathcal{B}^{n\omega}$.

By construction X has a uniform distribution on the set $\mathcal{M}$. Furthermore the resulting source over the alphabet $\mathcal{B}$ has independent and identically distributed random variables.

The source treated in the example at the end of the Section "Variable-to-Fixed Length Coding" of Sect. 2.4.4 allows such a form of randomization. In that case we have $\omega = 6$, $\gamma_0 = 59$ and $\gamma_1 = 5$. To get the same complexity as for the cases without randomization we should take the same values for M and K. As $M = 64$ we can only take $\mathcal{V} = \mathcal{A}$, i.e., $n = 1$. The values of $H(V|Y)$ for the cipher introduced in the proof of Theorem 54 are presented in Table 2.1 in the row (c). We see in any column of the table, i.e., for fixed K, that (under the same complexity) the randomization reduces the secrecy compared to an absence of the source coding and even more to the variable-to-fixed length coding.

Shtarkov [25] concludes that on the whole, one can reasonably believe, that the efficiency of the randomization has been overestimated but that there are no reasons to reject this approach completely.

2.5 Public-Key Cryptology

2.5.1 Introduction

In secret-key cryptology the cryptanalyst's task was to find out which of the possible keys $c_1, \ldots, c_K$ was used to encrypt the message. It was assumed that sender and receiver could agree on this key by communicating over a "secure" channel to which the cryptanalyst had no access. This assumption is often not realistic. In computer networks, for example, all users share the same net and there usually is no possibility to transmit messages over some private wire to which only the two communicating parties have access. Even if such a secure channel would exist, there is a further disadvantage of secret-key cryptology. Recall from the previous chapter that in order to really protect a message from being decrypted the amount of key space has to be as big as the amount of message space. So if we want to protect a message of length n bits, say, we have to transmit another n bits as the key. This, of course, will slow down the transmission of the message by a factor 2.

In their paper "New directions in cryptography" Diffie and Hellman [9] introduced the first public-key protocol, based on the discrete logarithm. In public-key cryptology communication over a secure channel is no longer necessary. There is only one key $c : \mathcal{M} \to \mathcal{M}$. We now drop the assumption that the cryptanalyst has unlimited computational power. It was already pointed out by Shannon in his pioneering paper that the complexity of encoding and decoding might be considered and Diffie and Hellman finally introduced the concept of a *one-way function*, i.e., a function, which is easy to evaluate but hard to invert. We shall later precise this notion. So if we use a one-way function as key c, then the encoding, i.e., the evaluation of $c(m)$ can be done rather fast, but in order to decrypt the transmitted message the cryptanalyst has

to apply the inverse function c^{-1} to recover the original message $m = c^{-1}\big(c(m)\big)$ which is a task of much higher complexity and cannot be done in reasonable time. We shall present the protocol of Diffie and Hellman in order to get more insight.

The Diffie–Hellman Algorithm

(1) Person i chooses some $a_i \in \{1, 2, \ldots, p-1\}$ and stores the value $b_i = w^{a_i}$ in a public directory, accessible to everybody. p here is a large prime number and w some primitive element, i.e., the order of p in $GF(p)$ is $p-1$.
(2) If Persons i and j want to communicate, they calculate their common key

$$k_{ij} = b_i^{a_j} = w^{a_i \cdot a_j} = w^{a_j \cdot a_i} = b_j^{a_i} = k_{ji}$$

and encrypt and decrypt their message using this common key.
(3) In order to break the key, a third person has to know one of the numbers

$$a_i = \log_w b_i, a_j = \log_w b_j$$

(where $\log_w$ is the discrete logarithm to the base w in $\mathbb{Z}_p$).

The algorithm is already presented in such a form that it is clear how it will work in a multiuser system, e.g., in a computer network. Observe that there is only one key for communication between Persons i and j. For instance, they could split their message into blocks of length $\lceil \log_2 p \rceil$ and add k_{ij} to each of these blocks. If p is large enough, a third person will not be able to decipher the text. Additionally, every other user in the system has all the necessary information to calculate k_{ij}. He knows p and w and he also can deduce a_i and a_j from b_i and b_j, since $a_i \mapsto w^{a_i}$ is one-to-one.

However, in order to obtain a_i or a_j, a third person has to apply the discrete logarithm $\log_w b_i$ or $\log_w b_j$, which is a computationally hard task. The best known algorithm takes $O(\sqrt{p})$ steps. In contrast, Persons i and j have to exponentiate in order to obtain k_{ij}. This can be done in $O(\log p)$ steps using repeated squaring. The function $f(x) = w^x$ (in $GF(p)$) had been conjectured by Diffie and Hellman [9] to be a one-way function. Later Hellman and Pohlig [21] found that additionally $p-1$ must have a large prime factor.

Diffie and Hellman also introduced the concept of a *trapdoor one-way function*. This is a collection of functions $\{f_k\}_k$ with the properties that

(i) in knowledge of k there exist fast algorithms for the evaluation of f_k and f_k^{-1}.
(ii) when k is not known, then for almost all y it is hard to find the x with $f_k(x) = y$, even if the encoding procedure is known.

Diffie and Hellman did not give an example for a trapdoor one-way function. This was later done by Rivest, Shamir and Adleman. We shall now present the Rivest–Shamir–Adleman [22] (RSA) cryptosystem. The RSA-system is widely used today. The (conjectured) trapdoor one-way function here is obtained making use of the hardness of integer factorization.

The RSA—Public Key Cryptosystem

(1) Each person k selects two "large" prime numbers p and q and forms the product $n \triangleq p \cdot q$.
(2) Further, each person selects (at random) a "large" number d with the property that the greatest common divisor $gcd\ \big(d, (p-1)\cdot(q-1)\big) = 1$ and then computes its multiplicative inverse e, hence $e \cdot d \equiv 1 \mod (p-1)\cdot(q-1)$.
(3) The numbers e and n are published in a public directory.
(4) If another person wants to submit a message x to Person k, he encrypts it using the encoding functions

$$E_k(x) = x^e \mod n (=: y).$$

Person k can easily decrypt y by application of the decoding function

$$D_k(y) = y^d \mod n\big(= (x^e)^d = x^{e\cdot d} = x \mod n\big).$$

Again, it is obvious that the RSA-system is already constructed for multi-user networks. Since e and n are stored in a public directory, every other person can encrypt messages directed to Person k using the key E_k. Decoding is done very fast using the number d, which is only known to Person k. Anybody else has to find the prime factor p and q of n in order to obtain d. Now, there exist quite fast algorithms to find even large prime numbers, whereas factorization is a very hard computational task. This has not been proved, but under the assumption that there is a significant gap between the complexity of prime number generation and factorization a collection of functions $(E_k)_k$ as used in the RSA-system is a trapdoor one-way function.

Most of the cryptosystems we shall introduce in this chapter are based on the hardness of factorization. We shall discuss this in Sect. 2.5.3, where some prime number tests and the basic ideas of the best known factorization algorithms are presented. First, we need some background in elementary number theory, which is given in Sect. 2.5.2.

We introduced a one-way function as a function which is "easy" to evaluate but "hard" to invert. This is rather a heuristic approach and we did not say yet what we mean by easy and hard. We do not want to discuss this here, since it requires some background in Complexity Theory. However, we shall at least give the idea for those who are familiar with the notions. "f is easy to evaluate" means that there exists a probabilistic polynomial-time algorithm (Turing machine) that on input x outputs $f(x)$). "Hard to invert" analogously means that for all probabilistic polynomial-time algorithms A the probability that A finds the inverse for a given y is negligibly small.

The function presented in the Diffie–Hellman and RSA-cryptosystems have been conjectured to be one-way functions. However, this has not been proved. It is not even known if one-way functions exist at all. Computer Scientists say that the existence of a one-way function seems to be a stronger assumption than the famous $P \neq NP$, although it is widely believed that one-way functions exists.

Although the discrete logarithm and encoding functions based on integer factorization are often used in practice, from a theoretical point of view they are not quite satisfactory examples. It has not been shown that the inversion is really as hard as suggested. The only thing we know is that up to now the fastest known algorithms for the computation of the discrete logarithm and for integer factorization are much slower than repeated squaring (for exponentiation) and the best prime number tests, respectively. We shall discuss this briefly in Sect. 2.5.3 (factorization) and Sect. 2.5.4 (discrete logarithm).

On the other hand, there exist problems which are provably hard if we assume that $P \neq NP$, the NP-complete problems. Using an NP-complete problem as basic tool for the construction of an encoding (one-way) function might yield a cryptosystem which is secure—at least if we assume that $P \neq NP$. However most of the attempts to construct a cryptosystem based on some NP-complete problem, so far, have not been very satisfactory. We shall illustrate the difficulties which may arise, when the knapsack problem is used to encrypt messages, in Sect. 2.5.5.

In the two cryptosystems introduced by Diffie and Hellman, as in Shannon's model of secret-key cryptology, a message is encrypted in order to protect it against the cryptanalysts attempts to obtain the information contained in this message. In electronic communication further forms of protection may be required. We already saw in the chapter on authentication that the cryptanalyst could also have the possibility to replace a message. In order to prove the authenticity of a message, this message is often equipped with a signature—some extra bits of information, which prove to the receiver that the message really originated from the sender who encrypted it. There exist several public-key cryptosystems for digital signatures. Further, for many purposes it is required that a participant of a system has to prove his identity in order to get access. Think, e.g., of a password you have to enter in order to login into the computer or of a secret code for the credit card. If the person who has to verify the identity does not obtain any further information, the identity proof is said to be a zero-knowledge proof.

Digital signatures, identity proofs and further situations, for which public-key cryptosystems have been developed, will be discussed in Sect. 2.5.6.

2.5.2 Number Theory

In this section we shall present those results and facts from Number Theory which are important to understand the algorithms in the subsequent sections. We assume that the reader is familiar with basic notions such as prime number, greatest common divisor, congruences, group, ring, field, etc.

Euclidean Algorithm

The Euclidean algorithm yields the greatest common divisor of two natural numbers $a > b$, which we shall denote by $gcd(a, b)$. It proceeds as follows:

In the first step we divide the numbers a and b with remainder, i.e., we find non-negative integers t_0 and r_1 with $a = t_0 \cdot b + r_1$, where $0 \leq r_1 < b$. This procedure is repeated with b and r_1 to obtain numbers t_1 and r_2 with $b = t_1 \cdot r_1 + r_2$ and $0 \leq r_2 < r_1$. We continue with r_1 and r_2 until we finally find an r_m such that $r_{m-1} = t_m \cdot r_m + 0$ (since $0 < r_m < \cdots < r_2 < r_1 < b < a$, this algorithm really needs a finite number of m iterations).

Proposition 5 *The number r_m is the greatest common divisor $gcd(a, b)$.*

Proof We have to show that r_m divides a and b and that r_m is the largest number with this property. Since $r_{m-1} = t_m \cdot r_m$, r_m divides r_{m-1}. Of course, then r_m divides $r_{m-2} = t_{m-1} \cdot r_{m-1} + r_m = (t_m \cdot t_{m-1} + 1) \cdot r_m$. Inductively, r_m divides $r_{i-2} = t_{i-1} \cdot r_{i-1} + r_i$, since r_m is divisor of r_{i-1} and r_i, and hence r_m divides b and a. In order to show that r_m is really the greatest common divisor of a and b, we shall see that any d which divides a as well as b also has to divide r_m. To see this observe that d must divide $r_1 = t_0 b - a$, hence $r_2 = t_1 \cdot r_1 - b$ and finally (by induction) $r_m = t_{m-1} \cdot r_{m-1} - r_{m-2}$.

Proposition 6 *The greatest common divisor $gcd(a, b)$ can be written as $gcd(a, b) = u \cdot a + v \cdot b$ for some integers $u, v \in \mathbb{Z}$.*

Proof With $u_1 = 1$ and $v_1 = -t_0$ we have $r_1 = a - t_0 b = u_1 a + v_1 b$. Now assume that for some $u_k, v_k \in \mathbb{Z}$ it is $r_k = u_k a + v_k b$ $(k \leq m - 1)$. Then

$$\begin{aligned} r_{k+1} &= r_{k-1} - t_k r_k = u_{k-1} a + v_{k-1} b - t_k (u_k a + v_k b) \\ &= (u_{k-1} - t_k \cdot r_k) a + (v_{k-1} - t_k \cdot r_k) b, \end{aligned} \tag{2.5.1}$$

and hence

$$u_{k+1} = u_{k-1} - t_k r_k, v_{k+1} = v_{k-1} - t_k \cdot r_k \in \mathbb{Z}.$$

With $u \triangleq u_m$ and $v \triangleq v_m$ the Proposition is proved. For a speed analysis of the Euclidean algorithm, recall that the Fibonacci numbers $\{F_n\}_{n=0}^{\infty}$ are defined by the recurrence $F_n = F_{n-1} + F_{n-2}$ with initial values $F_0 = 0$, $F_1 = 1$. It can be shown that $F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n + \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$, especially, it turns out that $F_n \geq \left(\frac{1+\sqrt{5}}{2} \right)^{n-2}$. The proof is left as an exercise to the reader.

Proposition 7 (Lamé) *For positive integers $a > b$ the number of iterations to compute the greatest common divisor $gcd(a, b)$ via the Euclidean algorithm is at most $\lfloor \log_s a \rfloor - 2$, where $s = \frac{1+\sqrt{5}}{2}$.*

Proof For all $i = 1, \ldots, m$ it is $r_{i-2} = t_{i-1} \cdot r_{i-1} + r_i \geq r_{i-1} + r_i$ (since $t_{i-1} \geq 1$ and with the convention $r_{-1} \triangleq a$, $r_0 \triangleq b$). Since $\{r_i\}_i$ is a decreasing integer sequence with $r_m = gcd(a, b) \geq 1$, we see that $r_{i-2} \geq r_{i-1} + r_i$ must be larger than the $(i - m)$th Fibonacci number from which Proposition 3 follows. With Proposition 7 the Euclidean algorithm is a fast way to determine the greatest common divisor $gcd(a, b)$ of two non-negative integers a and b. It takes about $O(\log a)$ steps. The performance of the Euclidean algorithm can still be improved. Stein introduced a variant in which

we get rid off the division with remainder, which is replaced by divisions by 2. This can be done much faster by processors.

In the design of cryptographic protocols the Euclidean algorithm is used to find the inverse of a given number $d \in \mathbb{Z}_n$. To see this, observe that d is invertible in $\mathbb{Z}_n$ if $gcd(d, n) = 1$. With Proposition 6 this means that $1 = u \cdot d + v \cdot n \equiv u \cdot d (\text{mod } n)$ and hence $u = d^{-1}$ in $\mathbb{Z}_n$.

Repeated Squaring

The reason for the speed in the encoding and decoding function of the Diffie–Hellman and of the RSA cryptosystems is that the determination of the inverse in $\mathbb{Z}_n$ and exponentiation can be done very fast. The inverse element is found using the Euclidean algorithm in $O(\log n)$ computation steps. We shall now present the repeated squaring algorithm, which computes the nth power of a given number in $O(\log n)$ steps.

Let

$$n = \sum_{i=0}^{t} a_i 2^i, a_i \in \{0, 1\}, t = \lfloor \log_2 n \rfloor$$

be the binary representation of n. Then

$$x^n = x^{a_0 + a_1 2 + \cdots + a_t 2^t} = x^{a_0} \cdot (x^2)^{a_1} \cdot (x^4)^{a_2} \cdot \cdots \cdot (x^{2^t})^{a_t}$$

with this product representation, it is clear what to do. Starting with x, we obtain $x, x^2, x^4, \ldots, x^{2^t}$ by repeated squaring. This takes in total $t = \lfloor \log n \rfloor$ multiplications. Further, after each squaring, we look if the coefficient a_i is 0 or 1.

If $a_i = 0$ then x^{2^i} does not contribute to the product, if $a_i = 1$ then x^{2^i} occurs as a factor to the product $x^n = \prod_{\substack{i=1 \\ a_i=1}}^{t} x^{2^i}$.

So, to obtain x^n as product of the squares $(x^{2^i})_{i=1}^{t}$ we need at most another $t = \lfloor \log n \rfloor$ multiplications, such that the total number of multiplications is smaller than $2\lfloor \log n \rfloor$.

Euler's Totient Function

We denote by

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \exists y \in \mathbb{Z}_n \text{ such that } x \cdot y = 1\}$$

where multiplication is performed modulo n.

It can easily be verified that $\mathbb{Z}_n^*$ is a group. The order (number of elements) of $\mathbb{Z}_n^*$ is denoted by $\varphi(n)$. φ is called *Euler's totient function*. The proof of the following properties is left as an exercise to the reader.

Proposition 8 *Euler's φ-function has the following properties.*

(a) *For all $x \in \mathbb{Z}_n^*$ it is $x^{\varphi(n)} \equiv 1 \mod n$*
(b) $\sum_{d|n} \varphi(d) = n$

(c) For a prime power p^e, $e \in \mathbb{N}$, it is $\varphi(p^e) = p^{e-1}(p-1)$
(d) φ is multiplicative, i.e., $\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$ if $gcd(n_1, n_2) = 1$
(e) $\varphi(n) = n \cdot \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$

If p is a prime number, then by (c) $\varphi(p) = p - 1$ and if $u = p \cdot q$ is the product of the different primes, then $\varphi(n) = (p-1) \cdot (q-1)$ by (e). Since by (a) $x^{\varphi(n)} \equiv 1 \mod n$, the condition $e \cdot d \equiv 1 \mod (p-1) \cdot (q-1)$ in Step 2 of the RSA-cryptosystem now becomes clear.

When p is a prime number it can be shown that the multiplicative group $\mathbb{Z}_p^*$ is cyclic, i.e., $\mathbb{Z}_p^* = \{1, x, x^2, x^3, \ldots, x^{p-1}\}$ is generated by some element x. We denote such an element as *primitive root*.

Proposition 9 *Let p be a prime number. In $\mathbb{Z}_p^*$ there are exactly $\varphi(p-1)$ primitive roots.*

Little Fermat

Fermat's "Little" Theorem is the central tool in the prime number tests we shall present in the next section.

Theorem 55 (Little Fermat) *Let p be a prime number. Then for any integer $x \in \mathbb{Z}$ not divisible by p*

$$x^{p-1} \equiv 1 \mod p.$$

Proof For any $y \in \mathbb{Z}$

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \equiv x^p + y^p \mod p,$$

since $\binom{p}{k} \equiv 0 \mod p$ for $k = 1, \ldots, p-1$. So, especially $(x+1)^p \equiv x^p + 1 \mod p$.

By induction it is now clear that for all $x \in \mathbb{Z}$

$$x^p \equiv x \mod p$$

since with $x^p \equiv x \mod p$, also $(x+1)^p \equiv x^p + 1 \equiv x + 1 \mod p$. This is equivalent to

$$x(x^{p-1} - 1) \equiv 0 \mod p$$

and since by the assumption $x \not\equiv 0 \mod p$, Fermat's Little Theorem is proved.

Quadratic Residues

A number $x \in \mathbb{Z}_p^*$, p prime, is a *quadratic residue*, if there exists some $y \in \mathbb{Z}_p^*$ such that $y^2 \equiv x \mod p$. For $p = 7$ the quadratic residues in $\mathbb{Z}_p$ are 1, 2 and 4, whereas

3, 5 and 6 are non-residues. As this example suggests half of the elements in $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ are quadratic residues, more exactly

Proposition 10 *The squares in $\mathbb{Z}_p^*$ are a subgroup of $\mathbb{Z}_p^*$ with $\frac{p-1}{2}$ elements.*

Proof With $x^2 \cdot y^2 = (x \cdot y)^2$ and $(x^{-1})^2 \cdot x^2 = 1$ it is easy to verify that the squares form a subgroup. Since $\mathbb{Z}_p^*$ is cyclic it can be written as $\mathbb{Z}_p^* = \{1, w, w^2, \ldots, w^{p-1}\}$ for the generator w. Squares can only have an even exponent and indeed $|\{1, w^2, w^4, \ldots, (w^{\frac{p-1}{2}})^2\}| = \frac{p-1}{2}$.

In order to characterize, if a given $x \in \mathbb{Z}_p^*, p > 2$, is a quadratic residue the *Legendre symbol* $\left(\frac{x}{p}\right)$ is introduced, defined by

$$\left(\frac{x}{p}\right) = \begin{cases} +1, & \text{if } x \text{ is quadratic residue} \\ -1, & \text{else.} \end{cases}$$

The Legendre symbol defines a homomorphism from $\mathbb{Z}_p^*$ into $\{1, -1\}$, since $\left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right) = \left(\frac{x \cdot y}{p}\right)$.

The Legendre symbol can be evaluated very fast using the following result.

Proposition 11 (Euler's lemma) *Let $p > 2$ be an odd prime number and $x \in \mathbb{Z}_p^*$. Then*

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p.$$

Proof By Fermat's Theorem the elements of $\mathbb{Z}_p^*$ are just the roots of the polynomial

$$z^{p-1} - 1 = (z^{\frac{p-1}{2}} - 1)(z^{\frac{p-1}{2}} + 1).$$

If x is a quadratic residue, then $x = y^2$ for some y and $x^{\frac{p-1}{2}} = y^{p-1} = 1$ by Fermat's Theorem.

If x is not a quadratic residue, then x must be a root of $(z^{\frac{p-1}{2}} + 1)$ (since there are exactly $\frac{p-1}{2}$ quadratic residues), hence $x^{\frac{p-1}{2}} = -1$.

With Euler's Lemma it is now easy to determine, whether a given $x \in \mathbb{Z}_p^*$ is a quadratic residue or not, just use repeated squaring to compute $x^{\frac{p-1}{2}}$.

We make use of this fact in order to present a fast probabilistic algorithm which finds a quadratic non-residue: Choose at random an $x \in \mathbb{Z}_p^*$ and compute $x^{\frac{p-1}{2}}$. If $x^{\frac{p-1}{2}} = -1$ we are done. Since exactly half of the elements in $\mathbb{Z}_p^*$ are quadratic non-residues, the probability that $x^{\frac{p-1}{2}} = -1$ is exactly $\frac{1}{2}$. So, on the average, after two attempts we are done. Note, that there is no deterministic algorithm known, which finds a quadratic non-residue this fast.

Once we know that x is a quadratic residue, we want to take the square root, i.e., to find a y with $y^2 = x$ in $\mathbb{Z}_p^*$ (of course with y also $p - y$ is square of x).

Proposition 12 *If x is quadratic residue modulo p and $\frac{p-1}{2}$ is odd, then*

$$y = x^{\frac{p+1}{4}}$$

and $p - y$ are the two square roots of x.

The proof is left as an exercise to the reader. Observe, that again we can apply repeated squaring in order to obtain a square root, if $\frac{p-1}{2}$ is odd. If this is not the case, there also exist fast algorithms, which solve this task. We do not want to discuss this here.

In cryptographic applications we are also interested in taking square roots in the ring $\mathbb{Z}_n$, when n is not a prime especially when $n = p \cdot q$ is the product of exactly two prime factors.

Proposition 13 *If $n = p \cdot q$, where p and q are distinct odd prime numbers, then there are exactly $\frac{(p-1)\cdot(q-1)}{4}$ quadratic residues in $\mathbb{Z}_n^*$, each of which has four distinct square roots.*

As an example consider $n = 15$. Here $\mathbb{Z}_n^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and $x^2 = 1$ for $x = 1, 4, 11, 14$, whereas $x^2 = 4$ for $x = 2, 7, 8, 13$.

Let $n = p \cdot q$ as before and let y be a quadratic residue in $\mathbb{Z}_n^*$. Then x_1 and x_2 are said to be *essentially different square roots* of y if $x_1 \neq x_2$ and $x_1 \neq n - x_2$. So, for $n = 15$ in the above example 1 and 4 are essentially different square roots of 1, whereas 1 and 14 are not essentially different.

From the following proposition we can conclude that taking square roots in $\mathbb{Z}_n$, $n = p_1 \cdot p_2$ and factoring n are computationally equivalent tasks, in the sense that once one task is solved the other can be done with little extra effort.

Proposition 14 *If $n = p \cdot q$, where p and q are distinct odd primes and if x_1 and x_2 are essentially different square roots of some quadratic residue in $\mathbb{Z}_n^*$, then either*

$$gcd(x_1 + x_2, n) = p \;\; or \;\; gcd(x_1 + x_2, n) = q.$$

Proof Since x_1 and x_2 are square roots of the same element in $\mathbb{Z}_n^*$, $x_1^2 - x_2^2 \equiv 0 \mod n$ and hence $(x_1 - x_2)(x_1 + x_2) = t \cdot n = t \cdot p \cdot q$ for some integer t. Since x_1 and x_2 are essentially different, $n = p \cdot q$ cannot divide $x_1 - x_2$ or $x_1 + x_2$. So p divides one factor, either $(x_1 - x_2)$ or $(x_1 + x_2)$ and q divides the other one but not both, and hence either p or q (but not both) must divide $x_1 + x_2$.

With Proposition 14 it is clear that once we found two essentially different square roots, we can easily factor $n = p \cdot q$ using the Euclidean Algorithm. With the Chinese Remainder Theorem it can, on the other hand, be shown that if the prime factors p and q are known, then all four square roots of a quadratic residue can be found very fast. So taking square roots in $\mathbb{Z}_n$ and factoring $n = p \cdot q$ are of about the same computational complexity.

2.5.3 Prime Number Tests and Factorization Algorithms

Little Fermat, Pseudoprimes and Carmichael Numbers

The simplest way to factorize a given integer $n \in \mathbb{N}$ is to divide n by all numbers smaller than n. Indeed, we only have to check all numbers $m < \sqrt{n}$, since if $n = n_1 \cdot n_2$ is a product of two integers $n_1, n_2 > 1$, then one of the factors n_1 and n_2 must be smaller than $\sqrt{n}$. If none of these integers is a divisor of n, then n must be a prime. Hence with $O(\sqrt{n})$ computation steps we can determine if n is prime or not. Moreover, if n is not a prime, the above *trial division* algorithm will yield a prime factor.

We shall see in this section that the performance of factorization algorithms has not essentially been improved, whereas there are fast algorithms (at least probabilistic algorithms) known that determine if a number n is prime within running time $O(\log n)$.[4] This gap is exploited in the RSA cryptosystem.

The prime number tests are based on the Little Fermat, which states that if p is prime for all $b \in \mathbb{Z}_p^* = \{1, \ldots, p-1\}$

$$b^{p-1} \equiv 1 \mod p.$$

So the Little Fermat yields a criterion for primality of an integer n which does not give any information about the prime factors of n. Just take a *base* $b \in \{1, \ldots, n-1\}$ and check if $b^{n-1} \equiv 1 \mod n$. If this is not the case, then n cannot be prime. However, this "Fermat test" does not always work, since if n is not a prime there might exist bases b which pass the Fermat test. For instance $2^{340} \equiv 1 \mod 341$ but $3^{340} \equiv 54 \mod 341$.

We say in this case that n is *pseudoprime* to the base b. Even worse is, that there exist *Carmichael numbers*, which are pseudoprimes to every base b relatively prime to n (i.e., $gcd(b, n) = 1$). For instance $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. The Fermat test can be executed in $O(\log n)$ steps using repeated squaring. So, if we must only apply this to a small fraction of bases $b \in \{1, \ldots, n-1\}$ in order to determine if n is prime, then we would have found a fast prime number test. Unfortunately it is not known if there are only finitely many Carmichael numbers, such that the Fermat test has to be executed for all bases.

[4] Remark by the editors: This statement is not up to date, because in the paper "M. Agrawal, N. Kayal, and N. Saxena, "PRIMES is in P", Annals of Mathematics, Vol. 160, No. 2, 781–793, 2004, the authors proved the asymptotic time complexity of the algorithm to be $\tilde{O}(\log^{12}(n))$. In other words, the algorithm takes less time than the twelfth power of the number of digits in n times a polylogarithmic (in the number of digits) factor. However, the upper bound proved in the paper was rather loose; indeed, a widely held conjecture about the distribution of the Sophie Germain primes would, if true, immediately cut the worst case down to $\tilde{O}(\log^6(n))$.

Probabilistic Prime Number Tests

Miller improved the Fermat test as follows. He proved that if n is prime and $n-1 = r \cdot 2^k$, where r is odd and hence 2^k the highest power of 2 dividing n, then for every $b \in \{1, \ldots, n-1\}$

$$b^r \equiv 1 \mod n \text{ or } b^{r \cdot 2^i} \equiv -1 \mod n \text{ for some } i \in \{1, \ldots, k-1\}.$$

Again, if some base b does not pass the Miller test, then n must be a composite number. For the Miller test there is no analogon to the Carmichael numbers. More exactly, if n is an odd composite number, then the fraction of integers $b \in \{1, \ldots, n\}$ which do not pass the Miller test is greater than $\frac{3}{4}$. This means that the probability that a randomly chosen $b \in \{1, \ldots, n-1\}$ passes the test is smaller than $\frac{1}{4}$. If we choose t bases independently at random than the probability that all t numbers pass the Miller test for a composite number is smaller than $\frac{1}{4^t}$. If for a given n we find t randomly chosen numbers that pass the test, we say that p is a *probable prime*. We just described the probabilistic prime number test due to Rabin, which for a given degree of accuracy has running time $O(\log n)$. Note that the Miller test would yield a deterministic $O(\log^3 n)$ prime number test, if the generalized Riemann hypothesis would hold. In this case, for a composite number n, one would find a base b which does not pass the Miller test in the interval $\{2, 3, \ldots, c \cdot \log^2 n\}$, where c is some universal constant not dependent on n. Hence the test would only have to be executed for the elements in this range.

Deterministic Prime Number Tests

The best known deterministic prime number tests[5] are based on factoring numbers related to the number n which has to be tested for primality. This is surprising, since we know that factoring is a hard task. However, the choice of the numbers which have to be factored is decisive.

Theorem 56 (Pocklington) *For an integer $n > 1$ let s be a divisor of $n-1$. Suppose there is an integer b satisfying*

$$b^{n-1} \equiv 1 \mod n$$

$$gcd(b^{\frac{n-1}{q}} - 1, n) = 1 \text{ for each prime } q \text{ dividing } s.$$

Then for every prime factor p of n it is $p \equiv 1 \mod s$, and if $s > \sqrt{n} - 1$, then n is prime.

Pocklington's theorem yields a probabilistic prime number test analogous to the Rabin test, by random selection of several bases b for which the condition in the theorem is checked. There are similar tests using factors of $n+1, n^2+1, n^2+n+1$ or n^2-n+1. Note that a test based on Pocklington's theorem can only be fast if the

[5] See the Remark in the previous footnote.

factorization of s is easy, i.e., s only has small prime factors. If, e.g., $n-1 = s_1 \cdot s_2$ where s_1 and s_2 are primes of about the same size, the test will be very slow. However the fastest prime number tests are based on similar arguments.

In the Jacobi-sum-test, the number s which is used for the single checks is no longer required to be a factor of $n-1$, any product $s > \sqrt{n}$ can be used. So we can try to find an $s > \sqrt{n}$ which is the product $s = q_1 \dots q_r$ with the property that the least common multiple $t = \ell cm\{q_1 - 1, \dots, q_r - 1\}$ is small, i.e., the $q_i - 1$ have many factors in common. Odlyzko and Pomerance have shown that there is a positive constant c such that for every $n > e^e$ there exists an integer $t < (\log n)^{c \cdot \log\log\log n}$ such that the corresponding $s > \sqrt{n}$. Because a similar lower bound on t can be derived, it follows that the trial division step of this primality test requires slightly more than polynomially many steps, namely $(\log n)^{O(\log\log\log n)}$.

Another approach to overcome the difficulties in finding an appropriate number s is taken in the primality tests based on elliptic curves. Note that in the condition of Pocklington's theorem the number s is a divisor of $n-1$ which is the order of the group $\mathbb{Z}_n^*$ if n is prime. Now to each prime p several groups over different elliptic curves are constructed. The group orders by a theorem of Hasse are between $p + 1 - 2\sqrt{p}$ and $p + 1 + 2\sqrt{p}$. Moreover, they are almost uniformly distributed in the interval $\{p + 1 - \sqrt{p}, \dots, p + 1 + \sqrt{p}\}$.

Now the groups are selected at random with the hope to find a group order T with a divisor s having a nice form.

Factorization Algorithms

The best factorization algorithms are rather slow compared to the best primality test. However, they show that in the construction of the RSA-cryptosystem and other schemes based on the hardness of factorization, one has to be very careful with the appropriate choice of the product $n = p \cdot q$.

In cryptographic applications, $n = p \cdot q$ is usually chosen as the product of two primes of about the same size $p \approx q$. In this case, one should first try the quadratic sieve method due to Pomerance. Lenstra developed a factorization algorithm based on elliptic curves. All these tests are not rigorously analyzed theoretically. However their performance in practice is good.

One should also take into account that a possible parallelization of a factorization algorithm might close the gap to primality tests a little bit. The RSA-129 (where the number n is a 129 digit number) was broken by factoring n using massive parallelization. The task was distributed worldwide via the Internet. A message encrypted with RSA-129 was presented in Scientific American 1977 as a "new kind of cipher that would take millions of years to break".

2.5.4 The Discrete Logarithm

Using repeated squaring $b = w^a$, $a \in \{0, \dots, n\}$ can be evaluated in $O(\log n)$ steps. The fastest known algorithm to find the discrete logarithm $a = \log_w b$ for a given b

(in an arbitrary multiplicative group) is due to Shanks. It has running time $O(\sqrt{n} \cdot \log \sqrt{n})$. The disadvantage is the enormous amount of storage space. However there are algorithms known, which are almost as fast and use less storage.

Shanks' algorithm consists of three stages.

(1) Select some $d \sim \sqrt{n}$. By Euclid's Algorithm there exist numbers Q and r such that $a = Qd + r$. The choice of d guarantees that all numbers involved (Q, d, r) have size not greater than $O(\sqrt{n})$.
(2) Make a table with entries $(x, \log_w x)$ for $\log_w x = 0, 1, \ldots, d-1$ and sort this table on x.
(3) It is $b = w^a = w^{Qd+r}$ and hence $b(w^{-d})^Q = b(w^{n-d})^Q = w^r$. Now for $Q = 0, 1, 2, \ldots$ compute $b(w^{n-d})^Q$ and compare the result with the entries in the table. Stop, when the result is equal to some x in the table. Then $r = \log_w x$ and $a = Qd + r$.

The most time-consuming task in this algorithm is the sorting of $O\sqrt{n}$ elements in the table in Step 2. This can be done using one of the best sorting procedures in time $O(\sqrt{n} \log \sqrt{n})$.

Note that taking logarithms can be done faster, when n is a composite number. In the Diffie–Hellman scheme this is the case, since $n = p - 1$, where p is prime. In order to keep the gap to the exponentiation algorithm large, n must then have a large prime factor. If this is not the case, $f(x) = w^x$ in $GF(p)$ is not a one-way function.

2.5.5 Knapsack Cryptosystems

We shall in this section discuss cryptosystems based on the knapsack problem. The knapsack problem is NP-complete and hence from a theoretical point of view such cryptosystems are quite attractive, since they are provably hard, as pointed out in the Introduction. However, in practice most of these cryptosystems have been broken.

The knapsack problem states as follows. For a given set of positive integers $a_1, \ldots, a_n$ and s, determine if there is a subset of $\{a_1, \ldots, a_n\}$ such that the sum of the a_i's in this subset is exactly s. In other words, do there exist variables $x_1, \ldots, x_n \in \{0, 1\}$ such that

$$\sum_{i=1}^{n} x_i a_i = s.$$

The number s may be interpreted as the capacity of a knapsack. If the a_i's are the weights of certain goods, the question is, if it is possible to find a collection of these goods which exactly fills the knapsack.

If such a collection exists, the subset of the a_i's can be guessed and it is easy to verify that $\sum_{i=1}^{n} x_i a_i = s$ in linear time (using at most n additions). Hence there exists a non-deterministic algorithm which solves the knapsack problem in polynomial time.

A simple deterministic algorithm is to check all possible 2^n subsets for the condition. Of course, this takes an exponential number of steps. This naive way has not essentially been improved. The best known algorithm takes about $2^{\frac{n}{2}}$ operations. The idea is to form all sums

$$S_1 = \left\{ \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} x_i a_i, x_i \in \{0,1\} \right\}, \; S_2 = \left\{ \sum_{i=\lfloor \frac{n}{2} \rfloor + 1}^{n} x_i a_i, x_i \in \{0,1\} \right\},$$

sort each of the sets S_1 and S_2 and then try to find a common element. If such a common element exists,

$$\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} x_i a_i = s - \sum_{i=\lfloor \frac{n}{2} \rfloor + 1}^{n} x_i a_i \quad \text{and hence} \quad \sum_{i=1}^{n} x_i a_i = s.$$

Like in Shanks' algorithm for the evaluation of the discrete logarithm, the speedup has to be paid with an enormous amount of storage space.

In a knapsack cryptosystem, a message $(x_1, \ldots, x_n) \in \{0,1\}^n$ is encoded as

$$s = \sum_{i=1}^{n} a_i x_i$$

where the weights $\{a_1, \ldots, a_n\}$ are stored in a public directory. The cryptanalyst then knows the $a_1, \ldots, a_n$ from the public directory and the message s he intercepted. So he has all the necessary information to decode the cryptogram. However, in order to do so, he has to solve an NP-complete problem.

The problem is that also the receiver has to solve the knapsack problem. Without any additional information his task is as hard as the cryptanalyst's. To overcome this difficulty, we first consider knapsacks of a certain structure which are easy to attack. Namely, it is required that the coefficients $a_1, \ldots, a_n$ form a *superincreasing* sequence, i.e., for all $i = 2, \ldots, n$

$$a_i > \sum_{j=1}^{i-1} a_j.$$

A knapsack problem based on a superincreasing sequence can be solved inductively very fast. It is $x_n = 1$ exactly if $s > \sum_{i=1}^{n-1} a_i$. So after having determined x_n we are left with the smaller knapsack problem $s - x_n a_n = \sum_{i=1}^{n-1} x_i a_i$.

All public-key cryptosystems based on the knapsack problem use such a superincreasing sequence $b_1, \ldots, b_n$, say, of coefficients. Of course, these coefficients can-

not be published, since the cryptanalyst could easily decode the cryptogram in this case. The idea is to transform the superincreasing sequence $b_1, \ldots, b_n$ to a sequence $a_1, \ldots, a_n$ from which the cryptanalyst does not benefit. The a_i's are published and the message $(x_1, \ldots, x_n)$ is encoded as $s = \sum x_i \cdot a_i$ using the public key. The cryptanalyst, hence, still has to solve a hard problem. The receiver, who can reconstruct the superincreasing sequence $b_1, \ldots, b_n$, only has to solve an easy knapsack problem.

Merkle and Hellman [20] introduced the first knapsack cryptosystem. We shall now present the transformation they used.

The system consists of

(1) a superincreasing sequence $b_1, \ldots, b_n$ with
$b_1 \approx 2^n$, $b_i > \sum_{j=1}^{i-1} b_j$ for $i = 2, \ldots, n$, $b_n \approx 2^{2n}$,
(2) two positive integers, M and W such that
$M > \sum_{i=1}^{n} b_i$, $gcd(M, W) = 1$,
(3) a permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

The superincreasing sequence $b_1, \ldots, b_n$ is transformed in two steps to a sequence $a_1, \ldots, a_n$ of coefficients by

(a) $a'_i \equiv b_i \cdot W \mod M$
(b) $a_i = a'_{\pi(i)}$.

So first the b_i's are multiplied by W modulo M. Observe that $a'_i = 0$ cannot occur, since $gcd(M, W) = 1$ and $M > b_i$ for all i. Then the so obtained numbers are shuffled using the permutation π. The sequence $a_1, \ldots, a_n$ is the public key. A message $(x_1, \ldots, x_n) \in \{0, 1\}^n$ is hence encrypted as $s = \sum_{i=1}^{n} x_i a_i$.

The receiver has some information, which is not available to the cryptanalyst. Namely he knows the numbers M and W from which he can conclude to the superincreasing sequence $b_1, \ldots, b_n$ as follows. He computes

$$\begin{aligned} C &\equiv s \cdot W^{-1} \mod M \\ &\equiv \sum_{i=1}^{n} x_i a_i W^{-1} \mod M \equiv \sum_{i=1}^{n} x_i a'_i W^{-1} \mod M \\ &\equiv \sum_{i=1}^{n} x_i b_{\pi(i)} \mod M \end{aligned}$$

by the encoding rules. So multiplication modulo M of the cryptogram s with W^{-1} leaves a knapsack based on a superincreasing sequence and this is an easy computational task for the receiver.

There also exists a refined version of the Merkle–Hellman system, where instead of the numbers (M, W) a sequence (M_k, W_k) is used to transform the superincreasing sequence iteratively. The Merkle–Hellman system has been broken by the following

approach. By the encoding prescription it is $a_i \equiv b_{\pi(i)} W \mod M$ and hence $b_{\pi(i)} \equiv a_i W^{-1} \mod M$. So for some integer k_i it is $a_i W^{-1} - k_i M = b_{\pi(i)}$ and hence

$$\frac{W^{-1}}{M} - \frac{k_i}{a_i} = \frac{b_{\pi(i)}}{a_i M}.$$

This means that the quotients $\frac{k_i}{a_i}$ are close to $\frac{W^{-1}}{M}$, since M is large compared to the first b_i's, at least.

Shamir used this close approximation to obtain numbers W' and M' with $\frac{(W')^1}{M'}$ close to $\frac{W^{-1}}{M}$ from which a superincreasing sequence similar to $b_1, \ldots, b_n$ is obtained. Another attack using Diophantine approximation is due to Lenstra.

2.5.6 *Further Cryptographic Protocols*

As pointed out in the introduction, in multiuser computer-networks cryptographic protocols are needed not only for protecting a message from being deciphered. We already learned about Simmon's theory of authentication, where a message is protected from being replaced. This is often done by a *digital signature*. Further applications of cryptography are *proofs of identity*. For instance, you have to enter a code before using a credit card or a password is needed in order to login to a computer. Identity proofs are often required to be *zero-knowledge* interactive proofs, i.e., the verifier should obtain no more information from the prover except information that the verifier could produce alone, even if the verifier cheats.

Proof of Identity

The following interactive protocol for a proof of identity is due to Omura. It is based on the discrete logarithm. First, each user of a multiuser system chooses some x (from a finite field) and puts $y = w^x$ in a public directory. It is assumed that each user has a copy of this directory. The protocol then proceeds in three rounds of communication.

(1) The first message $M_1 = a$ sent by the person who wants to prove his identity is the index a of his position in the public directory.
(2) The verifier selects some number r and transmits in the second round the message $M_2 = w^r$.
(3) The prover rises M_2 to the power x_a (he has a copy of the public directory) and transmits $M_3 = M_2^{x_a} = w^{r \cdot x_a}$.
(4) Finally, the verifier computes $y_a^r = w^{x_a \cdot r}$ and compares the result with the last message M_3.

Observe that this is not a zero-knowledge proof of identity since the verifier may cheat by sending $M_2 = r$ (not the power w^r) as second message. In this case he learns $M_3 = r^{x_A}$ which he could not calculate himself (However, he still has to take the discrete logarithm to conclude to x_a, which is a difficult task. So this information does not help him so much).

We shall later on present a zero-knowledge proof of identity using quadratic residues. First we shall illustrate the idea by a method for executing a fair random experiment interactively (due to Rabin).

Coin-Flipping by Telephone

Two persons want to execute a fair random experiment. They are only connected by telephone and do not trust each other. So they have to simulate a coin-flipping by telephone. The simulation is based on the factorization of an integer $n = p \cdot q$, a product of two large primes formed by Person 1. Since factorization is a hard task, Person 2 is not able to find the prime factors. In the course of the protocol Person 1 now will give some information about the number n, which will allow Person 2 to factor n with probability $\frac{1}{2}$. So "head" just means that Person 2 can factor n, whereas "tail" corresponds to the event that Person 2 cannot factor n. The protocol proceeds as follows.

(1) As first message $M_1 = n$, Person 1 sends the number $n = p \cdot q$.
(2) Person 2 selects an element $x \in \mathbb{Z}_n^*$ and transmits as second message $M_2 = x^2$.
(3) Person 1 computes a square root y of M_2 and sends this as message $M_3 = y$.
(4) If now $y = x$ or $-x$ in $\mathbb{Z}_n^*$ Person 2 can factor n (cf. Sect. 2). Else, he cannot factor n. Observe that if he can factor n, he can also prove this to anyone.

The idea of finding a square root that allows to factor a composite number n with probability $\frac{1}{2}$ is also used in the following zero-knowledge proof of identity due to Fiat and Shamir (1986).

Fiat–Shamir Zero-Knowledge Proof of Identity

It is assumed that $n = p \cdot q$ is a product of two large prime factors which is publicly known. Further each user selects an element $x \in \mathbb{Z}_n^*$ and stores x^2 next to the index of his name in a public directory. Again the protocol consists of three rounds.

(1) First, Person 1 selects at random an element $r \in \mathbb{Z}_n^*$ and transmits as first message $M_1 = (a, r^2)$ the index of his name a and r^2.
(2) Person 2 randomly chooses a binary digit $b \in \{0, 1\}$ which he transmits as message $M_2 = b$.
(3) Person 1 sends the third message $M_3 = \begin{cases} r, & \text{if } b = 0 \\ r \cdot x_a, & \text{if } b = 1. \end{cases}$
(4) If $b = 0$, Person 2 checks that $M_3^2 = r^2$, which was sent in the first message. If $b = 1$, Person 2 checks that $M_3^2 = r^2 \cdot x_a^2$.

Why is this protocol a zero-knowledge proof. Observe that since $(r \cdot x_a) \cdot r^{-1} = x_a$, Person 1 can know both possible values for the third message M_3 only if he knows the secret x_a. Hence, the probability that a third person not knowing x_a is deceiving Person 2, is less than or equal to $\frac{1}{2}$. On the other hand, Person 2 does not obtain any further information. The number r was chosen at random, so the only thing transmitted from Person 1 to Person 2 in the course of the protocol is a random number (either r or $r \cdot x_1$) and its square. This could be generated by Person 2 himself.

Observe that, contrasting to the first proof-of-identity protocol presented, here the only message from Person 2 to Person 1 is a random number, such that it is not possible to cheat for him. By repetition of the Fiat–Shamir protocol k times, say, (giving Person 1 k secrets), the probability that a third person, who does not know these secrets, deceives, is smaller than 2^{-k} and can hence be made arbitrarily small by the appropriate choice of k.

Another well-known zero-knowledge protocol for a proof of identity is based on the graph-isomorphism problem, i.e., on the decision if two graphs are isomorphic. As the knapsack problem, the graph-isomorphism problem is NP-complete and hence the zero-knowledge protocol in this case is based on a provably hard problem. The Fiat–Shamir protocol, as the RSA-system depends on the hardness of factorization.

Digital Signatures

A signature is attached to a message in order to identify the producer of this message. Signatures may be *implicit* or *explicit*. An implicit signature is used when the message is written in a way that no one else can imitate. An example for an implicit signature is the encryption of a message with a secret key, since it is very improbable that a randomly chosen string will be accepted as a valid plain-text. However, the opponent could replace the cryptogram by an older valid cryptogram. In order to avoid such an attack, messages are usually equipped with a time stamp.

We will rather be concerned with explicit signatures. In this case the message has an inseparable mark attached that no one else can imitate.

Further, signatures may be *private* or *public*. In order to discover a private signature, one has to share a secret with the author of the message (for instance, the secret-key example of an implicit signature is also private). A public signature can be identified by anybody else.

Explicit signatures are often obtained using hashing functions. Reversible two-key cryptosystems automatically yield implicit public signatures.

In electronic banking *blind signatures* are important, i.e., the signer does not know what message he is signing but can later certify whether a message was signed by him or not.

A detailed discussion on digital signatures will be carried out in Chap. 4. An overview is given in the book [29].

References

1. R. Ahlswede, Remarks on Shannon's secrecy systems. Prob. Control Inf. Theory **11**(4), 301–318 (1982)
2. L.A. Bassalygo, Lower bounds for the probability of successful substitution of messages. Prob. Inf. Trans. **29**(2), 194–198 (1993)
3. L.A. Bassalygo, M.V. Burnashev, Estimate for the maximal number of messages for a given probability of successful deception. Probl. Inf. Trans. **30**(2), 129–134 (1994)
4. L.A. Bassalygo, M.V. Burnashev, Authentication, identification and pairwise separated measures. Problemy Peredachi Informacii (in Russian) **32**(1), 41–47 (1996)

5. R.E. Blahut, *Principles and Practice of Information Theory* (Addison-Wesley, Boston, 1987)
6. M.V. Burnashev, S. Verdu, Measures separated in L_1-metrics and ID-codes. Probl. Inf. Trans. **30**(3), 3–14 (1994)
7. D. Coppersmith, The data encryption standard (DES) and its strength against attacks. IBM J. Res. Dev. **38**(3), 243–250 (1994)
8. I. Csiszar, J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems* (Academic Press, Cambridge, 1981)
9. W. Diffie, M.E. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
10. W. Feller, *An Introduction to Probability Theory and Its Applications*, 3rd edn. (Wiley, New York, 1968)
11. B. Fitingof, Z. Waksman, Fused trees and some new approaches to source coding. IEEE Trans. Inform. Theory **34**(3), 417–424 (1988)
12. E.N. Gilbert, F.J. Mac Williams, N.J.A. Sloane, Codes which detect deception. Bell Syst. Tech. J. **53**(3), 405–424 (1974)
13. M.E. Hellman, An extension of the shannon theory approach to cryptography. IEEE Trans. Inform. Theory **23**(3), 289–294 (1977)
14. R. Johannesson, A. Sgarro, Strengthening Simmons' bound on impersonation. IEEE Trans. Inform. Theory **37**(4), (1991)
15. D. Kahn, *The Codebreakers* (Mac Millan, New York, 1967)
16. D. Kahn, Modern cryptology. Sci. Am. 38–46 (1966)
17. F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes* (North-Holland, Amsterdam, 1977)
18. J.L. Massey, An introduction to contemporary cryptology, in *Contemporary Cryptology—the Science of Information Integrity*, ed. by G.J. Simmons (IEEE Press, New Jersey, 1992), pp. 1–39
19. U. Maurer, A unified and generalized treatment of authentication theory, in *Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science (STACS '96)*, Lecture Notes in Computer Science (Springer, Heidelberg, 1996), pp. 387–398
20. R.C. Merkle, M.E. Hellman, Hiding information and signatures in trapdoor knapsacks, Secure communications and asymmetric cryptosystems, 197-215, in *AAAS Selected Symposium Series* (Westview, Boulder, 1982)
21. S. Pohlig, M. Hellman, An improved algorithm for computing logarithms in GF(p) and its cryptographic significance. IEEE Trans. Inform. Theory **24** (1978)
22. R. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**, 120–126 (1978)
23. A. Sgarro, Informational divergence bounds for authentication codes, advances in *Cryptology—Eurocrypt '89*, Lecture Notes in Computer Science (Springer, Heidelberg, 1990)
24. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
25. Yu.M. Shtarkov, Some information-theoretic problems of discrete data protection. Prob. Inf. Trans. **30**(2), 135–144 (1994)
26. G.J. Simmons, Message authentication: a game on hypergraphs. Congressus Numerantium **45**, 161–192 (1984)
27. G.J. Simmons, Authentication theory/coding theory, advances in cryptology, in *Proceedings of the CRYPTO 84*, Lecture Notes in Computer Science, ed. by G.R. Blakley, D. Chaum (Springer, Heidelberg, 1985), pp. 411–431
28. G.J. Simmons, A survey of information authentication, in *Contemporary Cryptology—the Science of Information Integrity*, ed. by G.J. Simmons (IEEE Press, New Jersey, 1992), pp. 379–419
29. D.R. Stinson, *Cryptography—Theory and Practice, Discrete Mathematics and its Applications*, 3rd edn. (Chapman and Hall, London, 2006) (CRC, Florida)
30. B.P. Tunstall, Synthesis of Noiseless Compression Codes, Ph.D. Thesis, Georgia Institute of Technology, Atlanta, 1967

http://www.springer.com/978-3-319-31513-3

Hiding Data - Selected Topics
Rudolf Ahlswede's Lectures on Information Theory 3
Ahlswede, R. - Ahlswede, A.; Althöfer, I.; Deppe, C.; Tamm, U. (Eds.)
2016, XIV, 356 p. 17 illus. in color., Hardcover
ISBN: 978-3-319-31513-3