## Contents

3.4 Non-interactive Argument Based Approaches .................................... 18
  3.4.1 Pinocchio: Nearly Practical Verifiable Computation .......................... 19
  3.4.2 Geppetto: Versatile Verifiable Computation ...................................... 19
  3.4.3 SNARKs for C: Verifying Program Executions
      Succinctly and in Zero Knowledge ................................................. 20
  3.4.4 Succinct Non-interactive Zero Knowledge for a
      von Neumann Architecture ......................................................... 20
  3.4.5 Buffet: Efficient RAM and Control Flow in
      Verifiable Outsourced Computation ............................................. 20
  3.4.6 ADSNARK: Nearly Practical and
      Privacy-Preserving Proofs on Authenticated Data ............................ 20
  3.4.7 Block Programs: Improving Efficiency of
      Verifiable Computation for Circuits with
      Repeated Substructures .............................................................. 21

References .................................................................................. 21

4 Verifiable Computing from Fully Homomorphic Encryption ............... 23
  4.1 Definitions for Fully Homomorphic Encryption ................................. 23
  4.2 Verifiable Computing Schemes Based on FHE ................................. 24
      4.2.1 Non-interactive Verifiable Computing:
          Outsourcing Computation to Untrusted Workers ......................... 24
      4.2.2 Improved Delegation of Computation Using Fully
          Homomorphic Encryption ......................................................... 25

References .................................................................................. 25

5 Homomorphic Authenticators ......................................................... 27
  5.1 Definitions for Homomorphic Authenticators ....................................... 27
  5.2 Verifiable Computing Schemes Based on MACs ................................. 30
      5.2.1 Verifiable Delegation of Computation on
          Outsourced Data ..................................................................... 30
      5.2.2 Generalized Homomorphic MACs with Efficient
          Verification ............................................................................ 30
      5.2.3 Efficiently Verifiable Computation on Encrypted Data ............... 31
  5.3 Signature Based Verifiable Computing on Linear Functions ............. 31
      5.3.1 Programmable Hash Functions Go
          Private: Constructions and Applications to
          (Homomorphic) Signatures with Shorter Public Keys .................. 31
  5.4 Signature Based Verifiable Computing for Polynomial Functions ....... 32
      5.4.1 Homomorphic Signatures with Efficient
          Verification for Polynomial Functions ....................................... 32
      5.4.2 Algebraic (Trapdoor) One-Way Functions and
          Their Applications ................................................................. 32
  5.5 Signature Based Verifiable Computing Using
      Homomorphic Encryption ............................................................ 33

References .................................................................................. 34
Privately and Publicly Verifiable Computing Techniques
A Survey
Demirel, D.; Schabhüser, L.; Buchmann, J.
2017, XII, 64 p., Softcover
ISBN: 978-3-319-53797-9