Efficient Secure Two-party Protocols

Accuracy;152 4.3.3;5.3 Efficiency of the Protocol;154 5;Part III Specific Constructions;155 5.1;Chapter 6 Sigma Protocols and Efficient Zero-Knowledge1;157 5.1.1;6.1 An Example;157 5.1.2;6.2 Definitions and Properties;159 5.1.3;6.3 Proofs of Knowledge;163 5.1.4;6.4 Proving Compound Statements;168 5.1.5;6.5 Zero-Knowledge from S-Protocols;170 5.1.5.1;6.5.1 The Basic Zero-Knowledge Construction;171 5.1.5.2;6.5.2 Zero-Knowledge Proofs of Knowledge;174 5.1.5.3;6.5.3 The ZKPOK Ideal Functionality;177 5.1.6;6.6 Efficient Commitment Schemes from S-Protocols;183 5.1.7;6.7 Summary;185 5.2;Chapter 7 Oblivious Transfer and Applications;186 5.2.1;7.1 Notational Conventions for Protocols;187 5.2.2;7.2 Oblivious Transfer Privacy Only;187 5.2.2.1;7.2.1 A Protocol Based on the DDH Assumption;187 5.2.2.2;7.2.2 A Protocol from Homomorphic Encryption;191 5.2.3;7.3 Oblivious Transfer One-Sided Simulation;194 5.2.4;7.4 Oblivious Transfer Full Simulation;197 5.2.4.1;7.4.1 1-out-of-2 Oblivious Transfer;197 5.2.4.2;7.4.2 Batch Oblivious Transfer;205 5.2.5;7.5 Another Oblivious Transfer Full Simulation;210 5.2.6;7.6 Secure Pseudorandom Function Evaluation;211 5.2.6.1;7.6.1 Pseudorandom Function Privacy Only;212 5.2.6.2;7.6.2 Pseudorandom Function Full Simulation;218 5.2.6.3;7.6.3 Covert and One-Sided Simulation;220 5.2.6.4;7.6.4 Batch Pseudorandom Function Evaluation;221 5.3;Chapter 8 The kth-Ranked Element;222 5.3.1;8.1 Backgro EAN/ISBN : 9783642143038 Publisher(s): Springer, Berlin Discussed keywords: Computersicherheit, Protokoll Format: ePub/PDF Author(s): Hazay, Carmit - Lindell, Yehuda

Probleme Im Internationalen Klimaschutz Am Beispiel Des Kyoto-Protokolls - Hendrik Utler

Protokoll GelÃ¤ndepraktikum Lotharpfad Im Grindenschwarzwald: Praktikumstag 04.07.2008 - Sebastian GrÃ¤f

Sammlung Von Versuchsprotokollen FÃ¼r Die Bereiche Gasbrennschneiden, Montageroboter, FÃ¼gen-Stabelektrode, Pneumatisches Handling, Schraubverfahren - Nadja Lachmund

Quantitative Und Qualitative GÃ¼terkontrolle DurchfÃ¼hren, Eingangsdaten Erfassen Und Fehlerprotokolle Erstellen (Unterweisung Fachkraft FÃ¼r Lagerwirtsc - Eric Bahle

Protokollierung Im Projekt CASSAC - Thomas Beer

MP3 Protokoll - Chapter 1