

Efficient Secure Two-party Protocols

[DOWNLOAD HERE](#)

1;Preface;6 2;Contents;10 3;Part I Introduction and Definitions;13 3.1;Chapter 1 Introduction;15 3.1.1;1.1 Secure Multiparty Computation Background;15 3.1.2;1.2 The GMW Protocol for Secure Computation;23 3.1.3;1.3 A Roadmap to the Book;25 3.1.3.1;1.3.1 Part I Introduction and Definitions;25 3.1.3.2;1.3.2 Part II General Constructions;27 3.1.3.3;1.3.3 Part III Specific Constructions;29 3.2;Chapter 2 Definitions;31 3.2.1;2.1 Preliminaries;31 3.2.2;2.2 Security in the Presence of Semi-honest Adversaries;32 3.2.3;2.3 Security in the Presence of Malicious Adversaries;35 3.2.3.1;2.3.1 The Definition;36 3.2.3.2;2.3.2 Extension to Reactive Functionalities;37 3.2.3.3;2.3.3 Malicious Versus Semi-honest Adversaries;38 3.2.4;2.4 Security in the Presence of Covert Adversaries;42 3.2.4.1;2.4.1 Motivation;42 3.2.4.2;2.4.2 The Actual Definition;45 3.2.4.3;2.4.3 Cheating and Aborting;47 3.2.4.4;2.4.4 Relations Between Security Models;48 3.2.4.5;2.5 Restricted Versus General Functionalities;50 3.2.4.5.1;2.5.1 Deterministic Functionalities;51 3.2.4.5.2;2.5.2 Single-Output Functionalities;51 3.2.4.5.3;2.5.3 Non-reactive Functionalities;53 3.2.4.6;2.6 Non-simulation-Based Definitions;54 3.2.4.6.1;2.6.1 Privacy Only;54 3.2.4.6.2;2.6.2 One-Sided Simulatability;57 3.2.4.7;2.7 Sequential Composition Simulation-Based Definitions;58 4;Part II General Constructions;62 4.1;Chapter 3 Semi-honest Adversaries;64 4.1.1;3.1 An Overview of the Protocol;64 4.1.2;3.2 Tools;68 4.1.2.1;3.2.1 "Special" Private-Key Encryption;68 4.1.2.2;3.2.2 Oblivious Transfer;72 4.1.3;3.3 The Garbled-Circuit Construction;74 4.1.4;3.4 Yao's Two-Party Protocol;77 4.1.5;3.5 Efficiency of the Protocol;89 4.2;Chapter 4 Malicious Adversaries;92 4.2.1;4.1 An Overview of the Protocol;92 4.2.1.1;4.1.1 High-Level Protocol Description;93 4.2.1.2;4.1.2 Checks for Correctness and Consistency;95 4.2.2;4.2 The Protocol;100 4.2.3;4.3 Proof of Security;104 4.2.3.1;4.3.1 Security Against a Malicious P1;104 4.2.3.2;4.3.2 Security Against a Malicious P2;110 4.2.4;4.4 Efficient Implementation of the Different Primitives;116 4.2.5;4.5 Efficiency of the Protocol;117 4.2.6;4.6 Suggestions for Further Reading;118 4.3;Chapter 5 Covert Adversaries;120 4.3.1;5.1 Oblivious Transfer;120 4.3.1.1;5.1.1 The Basic Protocol;122 4.3.1.2;5.1.2 Extensions;130 4.3.2;5.2 Secure Two-Party Computation;132 4.3.2.1;5.2.1 Overview of the Protocol;133 4.3.2.2;5.2.2 The Protocol for Two-Party Computation;135 4.3.2.3;5.2.3 Non-halting Detection

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

[DOWNLOAD HERE](#)

Similar manuals:

[Exkursionsprotokoll Vom 29.März 2003. Fr her Standen Wir Auf Zwei Beinen - Heute Sind Wir Tausendf ler: Heute Sind Wir Tausendf ler - Silke Gerlach](#)

[WTO/GATS - Das Vierte Protokoll: Das Vierte Protokoll - Andreas Vossenkuhl](#)

[Das Montrealer Protokoll Zum Schutz Der Ozonschicht Und Dessen Bewertung - Melanie Kubens](#)

[Das Protokoll Von Kyoto - Thomas Hissel](#)

[Exkursionsprotokoll Nationalpark Eifel - Marie-Louise Victoria Heiling](#)

[Erkundungsprotokoll: Perspektivlosigkeit Handelsschule: Auswirkung Auf Die Motivation Der Sch ler - Ina Meinschaefer](#)

[Probleme Im Internationalen Klimaschutz Am Beispiel Des Kyoto-Protokolls - Hendrik Utler](#)

[Protokoll Geländepraktikum Lotharpfad Im Grindenschwarzwald: Praktikumstag 04.07.2008 - Sebastian Gräß](#)

[Sammlung Von Versuchsprotokollen Für Die Bereiche Gasbrennschneiden, Montageroboter, Fliegen-Stabelektrode, Pneumatisches Handling, Schraubverfahren - Nadja Lachmund](#)

[Quantitative Und Qualitative Güterkontrolle Durchführen, Eingangsdaten Erfassen Und Fehlerprotokolle Erstellen \(Unterweisung Fachkraft Für Lagerwirtsch - Eric Bahle](#)

[Protokollierung Im Projekt CASSAC - Thomas Beer](#)

[MP3 Protokoll - Chapter 1](#)