Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Seminar: **Secure Computation**
Dennis Hofheinz, Alexander Koch, Lisa Kohl, Matthias Nagel, Jiaxin Pan

Seminarprogramm

1. Vortrag: Sicherheitsmodell (9.5., Betreuer: Alexander Koch)

([HL10] S. 19 - 29, 46 - 48) Im ersten Vortrag soll sichere Zwei-Parteien-Berechnung noch einmal motiviert und definiert werden. Hierbei soll zunächst auf Sicherheit gegen passive und anschließend auf Sicherheit gegen aktive Angreifer eingegangen werden. An einem Beispiel soll erklärt werden, warum Sicherheit gegen aktive Angreifer nicht unbedingt Sicherheit gegen passive Angreifer impliziert und wie die Definition von passiver Sicherheit erweitert werden kann um dies zu umgehen. Schließlich soll besprochen werden, warum die Sicherheit im beschriebenen Modell schon Sicherheit unter sequenzieller Komposition impliziert.

2. Vortrag: Vorbereitung Yao's Protokoll (16.5., Betreuer: Matthias Nagel)

([HL10] S. 53 - 66) Der zweite Vortrag soll auf Yao's Protokoll vorbereiten. Dazu soll zunächst ein Überblick gegeben und schließlich als Grundlagen „Special" Private Key Encryption und die Garbled-Circuits-Konstruktion erklärt werden. Falls noch Zeit bleibt, kann in diesem Vortrag (in Absprache mit dem 3. Vortrag) noch auf Oblivious Transfer näher eingegangen werden.

3. Vortrag: Yao's Protokoll (passive Angreifer) (23.5., Betreuer: Matthias Nagel)

([HL10] S. 62, 67 - 80) In diesem Vortrag soll Yao's Zwei-Parteien-Protokoll erklärt und als sicher bewiesen werden. Dazu muss (sofern noch nicht im 2. Vortrag geschehen) zunächst Oblivious Transfer kurz motiviert und definiert werden. Das Protokoll selbst soll möglichst anschaulich beschrieben und die wesentlichen Teile des Sicherheitsbeweises skizziert werden. Schließlich sollte kurz auf die Effizienz eingegangen werden.

4. Vortrag: Yao's Protokoll (aktive Angreifer) - Teil I (30.5., Betreuer: Alexander Koch)

([HL10] S. 81 - 92, 106 - 107) Ziel des vierten Vortrages ist es Yao's Protokoll so zu erweitern, dass Sicherheit gegen aktive Angreifer erreicht wird. Dazu sollte zunächst eine High-Level Idee des Protokolls gegeben und schließlich das Protokoll selbst beschrieben und kurz auf die Effizienz eingegangen werden. Ein notwendiger Baustein hierfür sind Commitments, die im Laufe des Vortrages definiert werden sollen.

5. Vortrag: Yao's Protokoll (aktive Angreifer) - Teil II (6.6., Betreuer: Lisa Kohl)

([HL10] S. 93 - 105) Im fünften Vortrag soll der Beweis der Sicherheit gegen aktive Angreifer ergänzt werden. Hierzu werden die Parteien separat betrachtet. Wichtig ist, dass die wesentlichen Teile des Beweises erklärt werden und eine Intuition für die jeweiligen Beweisschritte gegeben wird.

6. Vortrag: Sigma-Protokolle (13.6., Betreuer: Lisa Kohl)

([HL10] S. 147 - 160) Im sechsten Vortrag sollen Σ-Protokolle motiviert und definiert werden. Für den weiteren Verlauf des Seminars soll die Sprache der Diffie-Hellman Tupel definiert und ein Σ-Protokoll für diese Sprache angegeben werden. Weiter soll auf Proofs of Knowledge eingegangen werden. Falls noch Zeit bleibt können Σ-Protokolle für ODER-Beweise erklärt werden.

7. Vortrag: Zero-Knowledge (20.6., Betreuer: Lisa Kohl)

([HL10] S. 160 - 175) Aufbauend auf den vorherigen Vortrag soll im siebten Vortrag erläutert werden, wie aus Σ-Protokollen effiziente Zero-Knowledge Protokolle konstruiert werden können. Als Grundlage sollen Pederson-Commitments definiert werden. Weiter soll erklärt werden, wie das erreichte Zero-Knowledge Protokoll so abgewandelt werden kann, dass ein Zero-Knowledge Proof of Knowledge entsteht.

8. Vortrag: Oblivious Transfer - Teil I (27.6., Betreuer: Jiaxin Pan)

([HL10] S. 42-46, 177 - 188) Beginnend mit dem achten Vortrag soll näher auf Oblivious Transfer Protokolle eingegangen werden, die einen wichtigen Baustein bei der Konstruktion von sicheren Protokollen darstellen. Zunächst müssen die grundlegenden Sicherheitsbegriffe definiert werden. Anschließend soll ein effizientes Oblivious Transfer Protokoll basierend auf DDH erläutert werden, das lediglich die Privatheit der Eingaben (bzw. einem Teil der Eingaben) garantiert. Falls genug Zeit ist, kann außerdem ein Protokoll basierend auf homomorpher Verschlüsselung erklärt werden. Schließlich soll ein Oblivious Transfer Protokoll mit einseitiger Simulation angegeben werden.

9. Vortrag: Oblivious Transfer - Teil II (4.7., Betreuer: Jiaxin Pan)

([HL10] S. 188 - 202) Im neunten Vortrag soll zunächst die Erweiterung zu vollständiger Simulation motiviert werden, indem erklärt wird, warum das im vorherigen Vortrag vorgestellte Protokoll nicht vollständiger simuliert werden kann. Schließlich soll ein Oblivious Transfer Protokoll erläutert werden, das diesen Sicherheitsbegriff erfüllt. Falls noch Zeit bleibt, kann auf Batch Oblivious Transfer und ein weiteres Oblivious Transfer Protokoll, das im Batch-Modus effizienter ist, eingegangen werden.

10. Vortrag: Das GMW Protokoll (11.7., Betreuer: Matthias Nagel)

([GMW87], [Gol01], [HL10] S. 11 - 13) Ziel des zehnten Vortrages ist es die GMW Konstruktion zu erklären. Dazu soll zunächst ein Protokoll vorgestellt werden, dass jede probabilistische Polynomialzeit Zwei-Parteien Funktionalität passiv sicher auswertet. Anschließend soll der GMW-Compiler erklärt werden, der jedes passiv sichere Protokoll in ein aktiv sicheres Protokoll umwandelt.

11. Vortrag: Secret Sharing und BGW - Teil I (18.7., Betreuer: Jiaxin Pan)

([AL17] Kap. 3 - 4, [CDN15] Kap. 3) Zum Abschluss des Seminars soll Mehrparteienberechnung beruhend auf der Secret-Sharing-Methode vorgestellt werden. Dazu behandeln die letzten beiden Vorträge das BGW Protokoll. Die Motivation des BGW Protokolls besteht darin, informationstheoretisch sichere Mehrparteienberechnung (ohne Annahmen) zu erhalten. Der elfte Vortrag erläutert das Secret-Sharing-Schema und die benötigten Eigenschaften, um das passiv sichere BGW Protokoll zu erhalten.

12. Vortrag: Secret Sharing und BGW - Teil II (25.7., Betreuer: Jiaxin Pan)

([AL17] Kap. 5 - 7) In Teil II soll informationstheoretisch sichere Mehrparteienberechnung in der Anwesenheit von aktiven Angreifern betrachtet werden. Zuerst erläutert der Vortrag das Verifiable-Secret-Sharing (VSS) Protokoll, das bivariate Polynome verwendet. Danach wird ein Überblick des BGW Protokolls mit Sicherheit gegen aktive Angreifer präsentiert.

Am Ende sollen die im Seminar behandelten Ansätze zur sicheren Mehrparteienberechnung kurz bezüglich ihrer Effizienz gegenübergestellt werden, und auf Vor- und Nachteile in verschiedenen Anwendungsszenarien eingegangen werden.

Literatur

[AL17] Gilad Asharov and Yehuda Lindell. A full proof of the BGW protocol for perfectly secure multiparty computation. *Journal of Cryptology*, 30(1):58–151, 2017.

[CDN15] Ronald Cramer, Ivan Bjerre Damgaard, and Jesper Buus Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, New York, NY, USA, 1st edition, 2015.

[GMW87] Shafi Goldwasser, Silvio Micali, and Avi Wigderson. How to play any mental game, or a completeness theorem for protocols with an honest majority. In *Proc. of the Nienteenth Annual ACM STOC*, volume 87, pages 218–229, 1987.

[Gol01] Oded Goldreich. *The Foundations of Cryptography – Volume 1, Basic Techniques*. Cambridge University Press, 2001.

[HL10] Carmit Hazay and Yehuda Lindell. *Efficient Secure Two-Party Protocols: Techniques and Constructions*. Springer-Verlag New York, Inc., New York, NY, USA, 1st edition, 2010.