Seminar: Grundlagen der Kryptographie

Multiparty Computation und Sicherheit im Internet

Organizers: Thomas Aulbach, Thomas Baumgartner, Samed Düzlü,
Antoine Gansel, Prof. Dr. Juliane Krämer, Maximiliane Weishäupl

FIDS - Chair of Data Security and Cryptography
Version 1.1

Durch ihre Funktionsweise ist die Kommunikation im Internet vom Prinzip her zunächst unsicher. Kryptographische Methoden ermöglichen eine sichere digitale Infrastruktur, in der möglichst wenig auf bloßem Vertrauen gegenüber bestimmten Instanzen basiert.

In diesem Seminar werden wir verschiedene kryptographische Konzepte kennenlernen und sie im Zusammenhang eines *untrusted cloud* Szenarios in die Anwendung bringen. So werden wir sehen, wie die Kommunikation im Internet gesichert und authentifiziert wird und wie diese Sicherheit modelliert und mathematisch bewiesen wird. Als Anwendungsbeispiel werden wir ein Cloud Provider nehmen, zu welchem User eine sichere Verbindung aufbauen und welcher kritische Daten wie zum Beispiel Passwörter sicher speichern muss. Des Weiteren werden wir die Möglichkeit von sicheren Modifikationen von verschlüsselten Daten durch User direkt auf der Cloud studieren. Abschließend betrachten wir die Möglichkeit von sogenannten *code injections* und schließen daraus Kriterien für ProgrammiererInnen zur sicheren Implementierung von Web-Applikationen.

Terminänderungen. Die Termine am **15.05.** und **29.05.** fallen aus.

Die Vorträge 4 und 6 werden beide am **05.06.** präsentiert. Vortrag 7, der planmäßig am 05.06. stattfinden sollte, wird zusammen mit Vortrag 8 am **12.06.** präsentiert.

Lernziel. Die TeilnehmerInnen des Seminars werden nach der erfolgreichen Teilnahme ein fundiertes Wissen über grundlegende Konzepte der Kryptographie im Zusammenhang mit sicherer Kommunikation und Datenspeicherung im Internet erworben haben.

Prüfungsleistung. Die TeilnehmerInnen werden zu einem ausgewählten Thema einen **60 bis 75** minütigen Vortrag halten. Neben dem Vortrag ist des Weiteren eine Ausarbeitung anzufertigen, die jeweils zwei Wochen nach dem Vortragstermin abzugeben ist. Nur bei den ersten beiden Vorträgen wird die Frist um jeweils eine Woche verlängert. Die genauen Abgabedaten für die Vorträge ist in der Beschreibung unten angegeben.
Details zur Form der Ausarbeitung werden separat zur Verfügung gestellt. Es wird dabei keine Seitenvorgaben geben. Die Ausarbeitung soll den TeilnehmerInnen des Seminars die Möglichkeit bieten, den Inhalt des Vortrags nachzuvollziehen, selbst wenn sie an dem Termin nicht teilnehmen konnten.

Betreuung. Jede SeminarteilnehmerIn soll spätestens 4 Wochen vor dem eigenen Vortragstermin selbstständig ein Treffen mit der BetreuerIn vereinbaren, um Details bezüglich der Inhalte zu besprechen. Eine erste Version der Ausarbeitung ist bereits *eine Woche vor dem Vortrag* an die BetreuerIn zu senden und zu besprechen. Es wird erwartet, dass die StudentIn die BetreuerIn rechtzeitig, in der Regel per Mail, kontaktiert, um Treffen zu vereinbaren.

Vorbereitungstreffen und Verteilung der Themen. Wir werden ein Vorbereitungstreffen zum Ablauf des Seminars am 20. März 2024 um 14 Uhr (s.t.) im Seminarraum 607 in der Bajuwarenstraße 4 abhalten. Unter anderem werden wir dann die Vorträge an die interessierten StudentInnen aufteilen. Eine Anmeldung per Mail bei uns ist bis vor dem Termin möglich, wenn der Termin ansonsten nicht realisierbar ist. Spätere Anmeldungen werden nur berücksichtigt, falls nicht alle Termine vergeben werden.

Vorkenntnisse. Die Teilnahme an dem Seminar braucht nur die grundlegenden Kenntnisse der Mathematik, die im ersten Semester des Informatik Studiengangs erlernt wurden.

Literatur. In der Beschreibung der Vorträge geben wir Hinweise zu Quellen, die zur Vorbereitung der Präsentation und der Ausarbeitung hilfreich sind. Darüber hinaus können weitere Quellen aus der eigenen Recherche zur Bearbeitung herangezogen werden. Falls der freie Zugang zu Quellen nicht möglich ist, kontaktiert uns gerne.

Bemerkung. Interessierte Personen können als ZuhörerInnen am Seminar teilnehmen, ohne einen Vortrag zu halten.

Themenverzeichnis

1 Symmetrische Kryptographie

Betreuer. Thomas Baumgartner
Datum. 17.04.2024
Frist für die Abgabe der Ausarbeitung. 08.05.2024
Vorgetragen von A.W.

Symmetrische Kryptographie ist ein grundlegendes Sicherheitskonzept, das durch die Verwendung desselben Schlüssels für Verschlüsselung und Entschlüsselung die Vertraulichkeit von Daten gewährleistet.

Inhalt. Gib als Einstieg einen historischen Überblick zur Entstehung der Kryptographie. Erläutere anhand des Beispiels der Cäsar Chiffre die allgemeine Definition eines symmetrischen Verschlüsselungssystems. Gehe kurz darauf ein, dass man Texte mittels Zahlenkodierung als Zahlenfolgen auffassen kann. Erkläre, welche Eigenschaften für die Sicherheit eines symmetrischen Verschlüsselungssystems wichtig sind. Gib anschließend mindestens zwei weitere Beispiele für symmetrische Verschlüsselungsverfahren und erkläre, welche Eigenschaften diese im Hinblick auf die Sicherheit erfüllen und welche Angriffsmöglichkeiten es gibt.

Literatur.

[**KL07**] Katz und Lindell. *Introduction to Modern Cryptography.*

[**Ros21**] Rosulek. *The Joy of Cryptography.*

2 Public-Key Kryptographie I: Definition und erstes Beispiel

Betreuer. Samed Düzlü
Datum. 24.04.2024
Frist für die Abgabe der Ausarbeitung. 15.05.2024
Vorgetragen von M.K.

In diesem Vortrag wird public-key bzw. asymmetrische Kryptographie als Gegenstück zu symmetrischer Kryptographie eingeführt. Sie ist ein fundamentaler Zweig der Kryptographie, auf der die gesamte Sicherheit der digitalen Kommunikation basiert. In diesem Vortrag werden die Probleme erläutert, die public-key Kryptographie motivieren und anschließend die Konzepte asymmetrische Verschlüsselung und Key-Exchange eingeführt. Der Vortrag schließt mit einem klassischen Beispielverfahren zum Schlüsselaustausch ab.

Inhalt. Erläutere die Notwendigkeit von asymmetrischer Kryptographie, selbst wenn zwei Parteien mit einem gemeinsamen Schlüssel sicher kommunizieren können, wie im ersten Vortrag dargelegt wurde. Definiere die Konzepte *Schlüsselaustausch/Key Exchange* und *Public-Key Encryption*. Zeige, dass man mit konstantem Aufwand jeweils aus einem Schlüsselaustauschverfahren eine Public-Key Encryption und andersrum konstruieren kann. Beschreibe use-cases für die beiden Konzepte. Erkläre das Schlüsselaustauschverfahren von Merkle, cf. [Mer78].

Literatur.

[**Buc02**] Buchmann. *Introduction to Cryptography.*

[**Buc16**] Buchmann. *Einführung in die Kryptographie.*

[**KL07**] Katz und Lindell. *Introduction to Modern Cryptography.*

[**Ros21**] Rosulek. *The Joy of Cryptography.*

[**Mer78**] Merkle. “Secure Communications over Insecure Channels”.

3 Public-Key Kryptographie II: RSA und Diffie-Hellman

Betreuer. Samed Düzlü
Datum. 08.05.2024

Frist für die Abgabe der Ausarbeitung. 22.05.2024
Vorgetragen von *offen.*

In diesem Vortrag werden wir die bis heute am häufigsten benutzten public-key Verfahren studieren. Sie basieren auf der Arithmetik ganzer Zahlen, die wir zuerst wiederholen werden.

Inhalt. Wiederhole die grundlegende Arithmetik für die Einführung von dem Faktorisierungsproblem und dem diskreten Logarithmus. Beschreibe das RSA Verfahren und den Diffie-Hellman Key-Exchange. Zeige, dass die Sicherheit der Verfahren jeweils auf die obigen Probleme zurückzuführen sind. Die formalen Definitionen von Sicherheit werden erst im nächsten Vortrag erklärt. Hier werden wir nur eine intuitive Definition von Sicherheit benutzen. Erkläre ohne Details zu gehen, dass die Probleme bis heute schwierig zu lösen sind, wenn nur klassische Computer benutzt werden, jedoch theoretisch mit Quantum Computer gebrochen werden können.

Literatur.

[Buc02] Buchmann. *Introduction to Cryptography.*

[Buc16] Buchmann. *Einführung in die Kryptographie.*

[KL07] Katz und Lindell. *Introduction to Modern Cryptography.*

[HPS08] Hoffstein, Pipher und Silverman. *An Introduction to Mathematical Cryptography.*

[Ros21] Rosulek. *The Joy of Cryptography.*

4 Public-Key Kryptographie III: Sicherheitsbegriffe

Betreuer. Thomas Aulbach
Datum. 05.06.2024
Gastvortrag von Dr. Patrick Struck

Nachdem wir in den letzten beiden Vorträgen gelernt haben, was public-key Kryptographie ist und Instantiierungen von entsprechenden Protokollen gesehen haben, wollen wir die theoretischen Sicherheitsaspekte in diesem Vortrag erlernen.

Inhalt. Führe das Konzept von *computational security* ein. Dieser steht im Gegensatz zu theoretischer Sicherheit, die stärker, aber für die Praxis zu restriktiv ist. Definiere die Sicherheitsbegriffe CPA und CCA. Zeige, dass man aus einer CPA sicheren public-key Encryption, ein CCA sicheres Schlüsselaustauschverfahren konstruieren kann.

Literatur.

[Buc02] Buchmann. *Introduction to Cryptography.*

[Buc16] Buchmann. *Einführung in die Kryptographie.*

[KL07] Katz und Lindell. *Introduction to Modern Cryptography.*

[Ros21] Rosulek. *The Joy of Cryptography.*

[Lip14] Lippert. *The Fujisaki-Okamoto Transformation.*

5 Hash Funktionen I

Betreuer. Thomas Aulbach
Datum. 22.05.2024
Frist für die Abgabe der Ausarbeitung. 05.06.2024
Vorgetragen von C.R.

Hash-Funktionen spielen eine zentrale Rolle in der Schlüsselverwaltung der Kryptographie. Ihr Hauptzweck besteht darin, Daten jeglicher Größe in eine feste und eindeutige Zeichenkette, den sogenannten Hash-Wert, umzuwandeln.

Inhalt. Starte mit der Definition von Hash Funktionen und motiviere diese. Erkläre den Unterschied zwischen schwacher und starker Kollisionsresistenz. Erläutere den Unterschied hinsichtlich der Sicherheit gegenüber Angriffen anhand des Geburtstagsparadoxons. Erkläre zum Schluss die Merkle-Damgård Konstruktion zur Entwicklung kollisionsresistenter Hash Funktionen.

Literatur.

[Mac21] Macharia. "Cryptographic Hash Functions".

[CIC13] Chandramouli, Iorga und Chokhani. "Cryptographic Key Management Issues & Challenges in Cloud Services".

6 Zertifikate: Digitale Signaturen

Betreuerin. Juliane Krämer
Datum. **05.06.2024**
Frist für die Abgabe der Ausarbeitung. 19.06.2024
Vorgetragen von S.B.

Eines der wichtigsten Ziele von Kryptographie ist die Authentizität, also die Sicherheit, dass Nachrichten oder Daten unverändert von der vorgesehenen Quelle stammen. Für diese Eigenschaft spielen digitale Signaturen eine zentrale Rolle. Ein Anwendungsbereich sind Zertifikate, mit denen unter anderem sichere Verbindungen zu Web-Seiten aufgebaut werden können.

Inhalt. Motiviere den Einsatz von digitalen Signaturen anhand von Beispielen (Software-Verteilung, E-Mail-Authentifizierung, Zertifikate) und hebe Authentizität als relevantes Ziel in der Kryptographie hervor. Definiere digitale Signaturen und führe den Sicherheitsbegriff *existential unforgeability under a chosen message attack* (EUF-CMA) ein. Gehe auch kurz auf *strong existential unforgeability* (SUF-CMA) und *non-repudiation* als weitere Sicherheitseigenschaften ein.

Literatur.

[BS23] Boneh und Shoup. *A Graduate Course in Applied Cryptography.* – Section 13.

[Gre] Green. *EUF-CMA and SUF-CMA.*

7 Zertifikate: Konstruktion digitaler Signaturen

Betreuerin. Maxi Weishäupl
Datum. **12.06.2024**
Frist für die Abgabe der Ausarbeitung. 26.06.2024
Vorgetragen von T.H.

In diesem Vortrag werden wir konkrete Konstruktionen von Signaturverfahren kennenlernen.

Inhalt. Erläutere am Beispiel von RSA Signaturen wie aus Trapdoor Funktionen Signaturverfahren konstruiert werden können. Erkläre warum 'textbook' RSA Signaturen nicht sicher sind und wie sie sicher gemacht werden können (Hashed RSA Signaturen). Führe das Hash-and-Sign Paradigma ein und erkläre wie damit der Nachrichtenraum einer bestehenden Signatur vergrößert werden kann. Beschreibe wie mit Hilfe von Lamport Signaturen aus einer One-way Funktion ein sicheres Signaturverfahren gebaut werden kann. Diskutiere Vor-und Nachteile der beiden vorgestellten Ansätze.

Literatur.

[BS23] Boneh und Shoup. *A Graduate Course in Applied Cryptography.* – Sections 13.2, 13.3, 14.

[Ros21] Rosulek. *The Joy of Cryptography.* – Section 13.3.

8 Hash Funktionen II: Password Management

Betreuer. Thomas Baumgartner
Datum. 12.06.2024
Frist für die Abgabe der Ausarbeitung. 26.06.2024
Vorgetragen von F.O.

Das Passwortmanagement mit Hashfunktionen bezieht sich auf die Verwendung von kryptografischen Hashfunktionen, um Passwörter sicher zu speichern.

Inhalt. Dieser Vortrag soll aufbauend auf Vortrag 5 die Anwendung von Hashfunktionen auf die Speicherung von Passwörtern erläutert werden. Wiederhole zunächst die wichtigsten Eigenschaften einer kryptographischen Hashfunktion und motiviere die Anwendung von Hashfunktionen bei der Speicherung von Passwörtern. Erkläre in diesem Kontext die Begriffe *Hashing* und *Salting* und gib Beispiele für mögliche Angriffe auf diese Verfahren.

Literatur.

[Mac21] Macharia. "Cryptographic Hash Functions".

[CIC13] Chandramouli, Iorga und Chokhani. "Cryptographic Key Management Issues & Challenges in Cloud Services".

9 MPC: Sicherheitsbegriffe

Betreuer. Antoine Gansel
Datum. 19.06.2024
Frist für die Abgabe der Ausarbeitung. 03.07.2024
Vorgetragen von *offen.*

In *Multi-Party Computation* (MPC) ist das Ziel, dass mehrere Parteien, die jeweils geheime Informationen haben, eine gemeinsame Funktion berechnen wollen, ohne Informationen über ihre geheimen Daten preiszugeben. In diesem Vortrag lernen wir, wie sichere MPC Protokolle modelliert werden.

Inhalt. Definiere die zwei wichtigsten Sicherheitsmodelle, das *semi-honest* Modell und das *malicious* Modell, und erkläre die Unterschiede der beiden Modelle. Erkläre dabei das Simulationsparadigma. Zeige, dass Sicherheit im malicious Modell die Sicherheit im semi-honest Modell impliziert.

Literatur.

[Lin16] Lindell. *How To Simulate It - A Tutorial on the Simulation Proof Technique.*

[Gol09] Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications* – Sections 7.2, 7.4.3.

[LWZ11] Laur, Willemson und Zhang. *Round-efficient Oblivious Database Manipulation.*

10 MPC: Zero-Knowledge Proofs

Betreuerin. Maxi Weishäupl
Datum. 26.06.2024
Frist für die Abgabe der Ausarbeitung. 10.07.2024
Vorgetragen von C.F.

Zero-Knowledge Proofs sind Protokolle mit zwei Parteien, von welchen eine der Parteien eine geheime Information hat, und die Parteien so kommunizieren, dass die Partei mit der geheimen Information die andere Partei überzeugt, dass sie das Geheimnis kennt, ohne Information über dieses Geheimnis zu verraten.

Inhalt. Definiere Zero-Knowledge Protokolle und gehe hierbei besonders auf die drei Eigenschaften Completeness, Soundness und Zero-Knowledge ein. Stelle den Zero-Knowledge Beweis für das Graph-3-Coloring Problem vor. Führe dafür Commitment Schemes ein und erkläre ihre Rolle im Beweis. Diskutieren zuletzt die Anwendung von Zero-Knowledge Proofs im Kontext von Multi-Party Computation.

Literatur.

[Goy18] Goyal. *Lecture 21: Zero-Knowledge Proofs III.*

[Goy20] Goyal. *Lecture Notes: Introduction to Cryptography.* – Section 12.

[Gol09] Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications.* – Sections 7.4.2, 7.5.4.

[Gre14] Green. *Zero Knowledge Proofs: An illustrated primer.*

[Gre17] Green. *Zero Knowledge Proofs: An illustrated primer, Part 2.*

[LWZ11] Laur, Willemson und Zhang. *Round-efficient Oblivious Database Manipulation.*

11 MPC: Secret Sharing

Betreuerin. Juliane Krämer
Datum. 03.07.2024
Frist für die Abgabe der Ausarbeitung. 17.07.2024
Vorgetragen von P.J.

Secret-sharing ist eine Methode, mit der ein Dealer verschiedenen Parteien shares zuteilt, sodass ein gemeinsames Geheimnis nur durch Zusammenführen der shares bestimmter autorisierter Teilmengen der Parteien rekonstruiert werden kann. In diesem Vortrag lernen wir Konstruktionen und Anwendungsbeispiele von secret-sharing.

Inhalt. Zunächst soll das Konzept von secret-sharing definiert werden. Insbesondere sollen die Eigenschaften correctness und perfect privacy eingeführt werden. Anhand des secret-sharing Verfahrens von Shamir soll das Konzept beispielhaft illustriert werden. Anschließend wollen wir möglichst diverse Anwendungssituationen von secret-sharing kennenlernen, z.B. Byzantine consensus von Rabin, oder

Literatur. *Sources for the talk. (The speakers may choose other sources if they like.)*

[Bei11] Beimel. “Secret-Sharing Schemes: A Survey”.

[Sha79] Shamir. “How to Share a Secret”.

[Ros21] Rosulek. *The Joy of Cryptography.*

[Aro] Arora. *Notes on Rabin’s algorithm for Byzantine Generals Problem.*

[Rab83] Rabin. “Randomized byzantine generals”.

[CCD88] Chaum, Crépeau und Damgård. “Multiparty Unconditionally Secure Protocols (Extended Abstract)”.

12 MPC: Homorphic Encryptions

Betreuer. Antoine Gansel
Datum. 10.07.2024
Frist für die Abgabe der Ausarbeitung. 24.07.2024
Vorgetragen von M.Me.

Beim Speichern von sicherheitskritischen Daten in einer untrusted cloud ist es wichtig, die Daten vorher zu verschlüsseln. In dem Fall ist es praktisch die Möglichkeit zu haben, die verschlüsselten Daten zu modifizieren, ohne sie vorher herunterladen, entschlüsseln, modifizieren, verschlüsseln und wieder hochladen zu müssen. Dies kann mit sogenannter *homomorphic encryption* (HE) realisiert werden.

Inhalt. Definiere die drei Arten (partially, somewhat und fully) HE und erkläre den Unterschied zwischen diesen. Gib eine Intuition für die Bootstrapping Operation. Am Ende des Vortrags soll klar sein, warum es sicher ist, HE in einem untrusted cloud Kontext zu benutzen.

Literatur.

[Aca+17] Acar u. a. *A Survey on Homomorphic Encryption Schemes: Theory and Implementation.*

[LB13] Lagendijk und Barni. "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation".

13 Code Injections

Betreuer. Antoine Gansel
Datum. 17.07.2024
Frist für die Abgabe der Ausarbeitung. 31.07.2024
Vorgetragen von A.S.

Menschen denken oft, dass Cybersicherheit die exklusive Arbeit von Cybersicherheitsexperten ist. Es ist jedoch wichtig, dass selbst theoretisch sichere Protokolle korrekt umgesetzt werden, damit die Sicherheit von Software gewährleistet ist. In diesem Vortrag werden wir einen Überblick über mögliche Sicherheitslücken bekommen, die auf Entwicklungsebene entstehen können. Außerdem werden wir sehen, wie diese Lücken entdeckt/erkannt werden können.

Achtung. Code Injections sind nicht legal und die Techniken dürfen nicht ohne Erlaubnis gegen Web-Seiten benutzt werden.

Inhalt. Präsentiere die verschiedenen *Code Injection* Angriffe und erkläre, wie man diese anwenden kann, um geheime Informationen herauszufinden. Erläutere Best Practices und Methoden, um Sicherheitslücken zu entdecken (z.B. *Taint Analysis*). Benutze WebGoat um Code Injections zu demonstrieren. Befolge dazu die Anleitung auf der OWASP Web-Seite. Beachte, dass wenn WebGoat läuft, eine Backdoor durch Bots/Hacker genutzt werden könnte. Deshalb wird geraten, dass WebGoat Programm nur zu starten, wenn *keine* Verbindung zum Internet hergestellt ist.

Literatur. *Sources for the talk. (The speakers may choose other sources if they like.)*

[RL12] Ray und Ligatti. "Defining code-injection attacks".

[Com17] Computerphile, *Running an SQL Injection Attack - Computerphile — youtube.com.*

[Lia22] Liang Yang. *Cross-Site Scripting (XSS) Explained And Demonstrated By A Pro Hacker! — youtube.com.*

14 Post-Quantum Kryptographie

Betreuerin. Maximiliane Weishäupl
Datum. 17.07.2024
Frist für die Abgabe der Ausarbeitung. 31.07.2024
Vorgetragen von J.O.

Post-Quantum Kryptographie bezeichnet jene Kryptographie, die Sicherheit gegenüber Angriffen mit Quantencomputern verspricht.

Inhalt. Beschreibe die Konsequenzen, die der Einsatz von leistungsfähigen Quanten-Computern auf einen Großteil der aktuell verwendeten Kryptographie hätte. Gehe hierbei auf die Algorithmen von Shor und Grover ein. Führe Post-Quantum (PQ) Kryptographie als einen Ansatz ein, mit welchem versucht wird sichere Kommunikation auch unter Angriffen mit Quanten Computern zu gewährleisten. Stelle die fünf Familien (Gitter-, Code-, Isogien- und Hash-basierte sowie Multivariate Kryptographie) der PQ-Kryptographie vor. Beschreibe zuletzt an Hand der NIST Standardisierungsprozesse wie PQ-Kryptographie in die Anwendung gebracht werden soll.

Literatur. *Sources for the talk. (The speakers may choose other sources if they like.)*

[BL17] Bernstein und Lange. “Post-quantum cryptography”.

[BBD09] Bernstein, Buchmann und Dahmen. *Post-Quantum Cryptography.*

[NIS] NIST. *Post-Quantum Cryptography.*

[Ver23] Veritasium. *How Quantum Computers Break The Internet... Starting Now — youtube.com.*

Literatur

[Aca+17] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac und Mauro Conti. *A Survey on Homomorphic Encryption Schemes: Theory and Implementation*. 2017. arXiv: 1704.03578 [cs.CR] (siehe S. 8).

[Aro] Sanjeev Arora. *Notes on Rabin's algorithm for Byzantine Generals Problem*. URL: https://allquantor.at/blockchainbib/pdf/rabin1983randomized.pdf (siehe S. 7).

[BBD09] Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. *Post-Quantum Cryptography*. 2009. ISBN: 978-3-540-88701-0. URL: https://link.springer.com/book/10.1007/978-3-540-88702-7 (siehe S. 9).

[Bei11] Amos Beimel. "Secret-Sharing Schemes: A Survey". In: *Coding and Cryptology - Third International Workshop, IWCC 2011*. 2011 (siehe S. 7).

[BL17] Daniel J. Bernstein und Tanja Lange. "Post-quantum cryptography". In: *Nat.* 549.7671 (2017), S. 188–194. DOI: 10.1038/NATURE23461. URL: https://doi.org/10.1038/nature23461 (siehe S. 9).

[BS23] Dan Boneh und Victor Shoup. *A Graduate Course in Applied Cryptography*. Draft 0.6, http://toc.cryptobook.us/. 2023 (siehe S. 5).

[Buc02] Johannes Buchmann. *Introduction to Cryptography*. 2002. ISBN: 0-387-95034-6 (siehe S. 3, 4).

[Buc16] Johannes Buchmann. *Einführung in die Kryptographie*. 6. Auflage. Springer, 2016. ISBN: 978-3-642-39774-5. DOI: 10.1007/978-3-642-39775-2 (siehe S. 3, 4).

[CCD88] David Chaum, Claude Crépeau und Ivan Damgård. "Multiparty Unconditionally Secure Protocols (Extended Abstract)". In: *ACM Symposium on Theory of Computing*. ACM, 1988. URL: https://doi.org/10.1145/62212.62214 (siehe S. 7).

[CIC13] Ramaswamy Chandramouli, Michaela Iorga und Santosh Chokhani. "Cryptographic Key Management Issues & Challenges in Cloud Services". In: 2013. URL: https://api.semanticscholar.org/CorpusID:26249307 (siehe S. 5, 6).

[Com17] Computerphile. *Running an SQL Injection Attack - Computerphile — youtube.com*. https://www.youtube.com/watch?v=ciNHn38EyRc. 2017 (siehe S. 8).

[Gol09] odded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. 1st. USA: Cambridge University Press, 2009. ISBN: 052111991X (siehe S. 6, 7).

[Goy18] Vipul Goyal. *Lecture 21: Zero-Knowledge Proofs III*. https://www.cs.cmu.edu/~goyal/s18/15503/scribe_notes/lecture21.pdf. 2018 (siehe S. 7).

[Goy20] Vipul Goyal. *Lecture Notes: Introduction to Cryptography*. https://www.cs.cmu.edu/~goyal/15356/. 2020 (siehe S. 7).

[Gre] Matthew Green. *EUF-CMA and SUF-CMA*. https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/ (siehe S. 5).

[Gre14] Matthew Green. *Zero Knowledge Proofs: An illustrated primer*. https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/. 2014 (siehe S. 7).

[Gre17] Matthew Green. *Zero Knowledge Proofs: An illustrated primer, Part 2*. https://blog.cryptographyengineering.com/2017/01/21/zero-knowledge-proofs-an-illustrated-primer-part-2/. 2017 (siehe S. 7).

[HPS08] Jeffrey Hoffstein, Jill Pipher und J.H. Silverman. *An Introduction to Mathematical Cryptography*. Springer Publishing Company, Incorporated, 2008. ISBN: 0387779930 (siehe S. 4).

[KL07] Jonathan Katz und Yehuda Lindell. *Introduction to Modern Cryptography*. 2007. ISBN: 978-1-58488-551-1. URL: http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf (siehe S. 3, 4).

[LB13] R L Lagendijk und M Barni. "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation". In: *IEEE Signal Process. Mag.* (2013). URL: https://homepage.tudelft.nl/c7c8y/SSP/privacyprotectedsignalprocessing.pdf (siehe S. 8).

[Lia22] Loi Liang Yang. *Cross-Site Scripting (XSS) Explained And Demonstrated By A Pro Hacker! — youtube.com*. https://www.youtube.com/watch?v=PPzn4K2ZjfY. 2022 (siehe S. 8).

[Lin16] Yehuda Lindell. *How To Simulate It - A Tutorial on the Simulation Proof Technique*. Cryptology ePrint Archive, Paper 2016/046. https://eprint.iacr.org/2016/046. 2016. URL: https://eprint.iacr.org/2016/046 (siehe S. 6).

[Lip14] Jan Lippert. *The Fujisaki-Okamoto Transformation*. 2014. URL: https://cs.uni-paderborn.de/fileadmin-eim/informatik/fg/cuk/Lehre/Abschlussarbeiten/Bachelorarbeiten/2014/BA_Lippert_FOT_final.pdf (siehe S. 4).

[LWZ11] Sven Laur, Jan Willemson und Bingsheng Zhang. *Round-efficient Oblivious Database Manipulation*. Cryptology ePrint Archive, Paper 2011/429. https://eprint.iacr.org/2011/429. 2011. URL: https://eprint.iacr.org/2011/429 (siehe S. 6, 7).

[Mac21] Wahome Macharia. "Cryptographic Hash Functions". In: (Mai 2021) (siehe S. 5, 6).

[Mer78] Ralph C. Merkle. "Secure Communications over Insecure Channels". In: *Commun. ACM* (1978). DOI: 10.1145/359460.359473. URL: http://doi.acm.org/10.1145/359460.359473 (siehe S. 3).

[NIS] NIST. *Post-Quantum Cryptography*. https://csrc.nist.gov/projects/post-quantum-cryptography (siehe S. 9).

[Rab83] Michael O. Rabin. "Randomized byzantine generals". In: *Symposium on Foundations of Computer Science*. 1983. DOI: 10.1109/SFCS.1983.48 (siehe S. 7).

[RL12] Donald Ray und Jay Ligatti. "Defining code-injection attacks". In: *Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. POPL '12. Philadelphia, PA, USA: Association for Computing Machinery, 2012, S. 179–190. ISBN: 9781450310833. DOI: 10.1145/2103656.2103678. URL: https://doi.org/10.1145/2103656.2103678 (siehe S. 8).

[Ros21] Mike Rosulek. *The Joy of Cryptography*. https://joyofcryptography.com/. 2021 (siehe S. 3–5, 7).

[Sha79] Adi Shamir. "How to Share a Secret". In: *Commun. ACM* (1979). URL: https://doi.org/10.1145/359168.359176 (siehe S. 7).

[Ver23] Veritasium. *How Quantum Computers Break The Internet... Starting Now — youtube.com*. https://www.youtube.com/watch?v=-UrdExQW0cs&ab_channel=Veritasium. 2023 (siehe S. 9).