Geplante Abschlussarbeitsthemen

Sommersemester 2018

12.03.2018

Anbei finden Sie die geplanten Abschlussarbeitsthemen für den Sommersemester 2018.

Um sich für eine Abschlussarbeit zu bewerben, schreiben Sie mir bitte eine Email einschließlich bis

03.04.2018,

die insbesondere die folgenden Informationen beinhaltet:

Subjekt der Email: Vorname + Nachname + Name des ausgewählten Themas

1. Titel des ausgewählten Themas
2. Matrikelnummer
3. Telefonnummer
4. Studiengang
5. Vollzeit/Teilzeit
6. Fehlende Leistungsnachweise (Erbringung geplant am)
7. Fehlende Fachprüfungen
8. Relevante Fachprüfungen und Leistungsnachweise für gewähltes Thema
9. Vorheriges Studium
10. Kurze Begründung für die Auswahl des Themas

Wenn Sie sich mehrere Themen bewerben, schreiben Sie bitte jeweils eine separate Email.

Nach einer ersten Auswahl bekommen die ausgewählten Studierenden die Übertragung des Themas (eventuell erst nach einem diesbezüglichen Telefongespräch), welches sie bearbeiten, und innerhalb von 4 Wochen ein Exposé bezüglich Grundlagen, Herangehensweise und Zeitplanung erstellen können.

Bei Akzeptanz des Exposés erfolgt die Anmeldung der Abschlussarbeit beim Prüfungsamt, ansonsten wird das Thema an eine/n andere/n Kanditatin/Kandidaten vergeben.

Energie-Effiziente und Verzögerungsbewusste Authentifizierung für drahtlose Systeme im Internet der Dinge

Bachelorarbeit Informatik/Wirtschaftsinformatik, oder
Masterarbeit Praktische Informatik

12.03.2018

Viele neue innovativen Anwendungen wie Smart-City, Smart-Home, unbemannte Fahrzeuge (Drohnen) und digitale Medizin erfordern neue effiziente Authentifizierungsmechanismen, die einerseits ein gewisses Verzögerungsbewusstsein (delay-awareness) nachweisen, aber andererseits auch eine enorme Energie-Effizienz benötigen. Dabei stellt insbesondere die effiziente Implementierung und Untersuchung geeigneter sicherer digitalen Signaturen eine große Herausforderung dar.

Ziel dieser Abschlußarbeit ist es,

- die relativ neu vorgeschlagenen Methoden in [1], [2] mit verschiedenen Schlüsselgrößen zu erarbeiten und implementieren,
- die Ergebnisse mit der Literatur zu vergleichen und evaluieren,
- eventuell ein Verbesserungsvorschlag näher zu untersuchen, implementieren, und evaluieren.

Referenzen

[1] M. O. Ozmen und A. A. Yavuz. *Low-Cost Standard Public Key Cryptography Services for Wireless IoT Systems*, IoT S&P '17 Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, 65–70, 2017.

[2] M. O. Ozmen, R. Behnia, und A. A. Yavuz. *Compact Energy and Delay-aware Authentication*, Cryptology ePrint Archive, https://eprint.iacr.org/2018/028.

Effiziente Klient-Puzzles gegen DoS-Angriffe mit Hilfe modularer Exponentiation

Bachelorarbeit Informatik

12.03.2018

Klient-Puzzles werden als eine effektive Gegenmaßnahme gegen Denial-of-Service Angriffe (Dos-Angriffe) in der Netzwerksicherheit benutzt. Dabei ist es enorm wichtig, dass einerseits die Puzzles nicht parallelisierbar bleiben, andererseits aber auch sie die besondere Eigenschaft besitzen, dass die Verifizierung dieser Puzzles sehr effizient verwirklicht werden kann. Eine Möglichkeit bei der Realisierung der Klient-Puzzles gegen DoS-Angriffe besteht darin, mittels der Zusammenwirkung der Exponentiation in Restklassenringen mit dem RSA-Kryptosystem, ein für die Puzzle-Erzeugung und Verifizierung effizientes Verfahren zu entwickeln [1].

Ziel dieser Bachelorarbeit ist es,

- den in [1] eingeführten Algorithmus näher zu analysieren und implementieren,
- die Sicherheit der Ergebnisse im Falle der Existenz mehrerer Benutzer nach [2] zu analysieren,
- gegebenenfalls ein Verbesserungsvorschlag zu implementieren und evaluieren.

Referenzen

[1] G. O. Karame und S. Čapkun. *Low-Cost Client Puzzles Based on Modular Exponentiation*, ESORICS 2010, LNCS 6345, pp. 679–697, 2010.

[2] D. Stebila, L. Kuppusamy, J. Rangasamy, C. Boyd, und Juan Gonzalez Nieto. *Stronger Difficulty Notions for Client Puzzles and Denial-of-Service-Resistant Protocols*, CT-RSA 2011, LNCS 6558, 284–301, 2011.

Widerrufbare (revocable) identitätsbasierte Verschlüsselung mit Hilfe eines Cloud-Servers

Bachelorarbeit Informatik/Wirtschaftsinformatik, oder
Masterarbeit Praktische Informatik/Informatik

12.03.2018

Im Gegensatz zu den PKI-basierten (public key infrastructure) Systemen, stellt die effiziente Widerrufung der Schlüssel von böswilligen und nicht mehr registrierten Benutzer in identitätsbasierter Verschlüsselung eine große Herausforderung dar. Einige Lösungen setzen einen vertrauenswürdigen interaktiven Server voraus, welche im gewisser Sinne mit der Grundidee der identitätsbasierter Verschlüsselung widersprechen, weil die identitätsbasierte Verschlüsselung (unter anderem) auch das Hauptziel hat, eine wesentlich effizientere Infrastruktur als die PKI-basierten traditionellen Mechanismen anzubieten.

Neulich werden alternative Methoden durch den Einsatz eines cloud-basierten halbvertrauenswürdigen Schlüssel-Update-Servers verwirklicht [1], [2], die die bilinearen Abbildungen (Paarungen) als Grundfunktionen benutzen.

Ziel dieser Abschlußarbeit ist es,

- die Verfahren in [1] und [2] näher zu analysieren,
- die Verfahren in [1] und [2] zu implementieren und die Effizienz dieser Verfahren miteinander zu vergleichen,
- gegebenenfalls ein Mechanismus zu implementieren, der mit einem nichtvertrauenswürdigen Schlüssel-Update-Server die widerrufbare identitätsbasierte Verschlüsselung verwirklicht.

Referenzen

[1] Y. Ren, N. Ding, X. Zhang, H. Lu, und D. Gu . *Identity-Based Encryption with Verifiable Outsourced Revocation*, The Computer Journal (59) No. 11, 1659–1668, 2016.

[2] X. Jia, N. Kumar, K. K. Raymond Choo, D. He. *Efficient revocable ID-based encryption with cloud revocation server*, International Journal of Communication Systems (31), Issue 1, 1–15, 2018.

Das Schlüsselaustauschverfahren mittels Isogenien supersingulärer elliptischer Kurven

Masterarbeit Mathematik/Informatik

12.03.2018

Verwirklichung der Schutzziele wie die Vertraulichkeit und die Authentizität bei digitalen Infrastrukturen beruht meist auf die derzeit im Einsatz befindenen Public-Key-Kryptosysteme, dessen Sicherheit wesentlich auf die Schwierigkeit des Faktorisierungsproblems (*wie die RSA-Verschlüsselung/Signaturen*) oder des diskreten Logarithmus Problems (DLP) (*wie ECDSA und der Schlüsselaustausch von Diffie-Hellman*) basieren. Bekanntlich gelten die Quanten-Algorithmen eine herausfordernde Bedrohung für die Sicherheit dieser Verfahren, da sich sowohl das Faktorisierungsproblem als auch das DLP mit Hilfe von Quanten-Algorithmen in polynomieller Zeit lösen lassen.
Post-Quanten-Kryptographie bezieht sich daher auf die Untersuchung mathematischer Probleme nebst den darauf basierenden neuen kryptographischen Verfahren, die sich mit Hilfe von Quantencomputern nicht effizienter als die klassische Computer-Architekturen lösen lassen. Durch die Ersetzung des DLP mit dem so genanten **IP-Problem** (d.h. *Isogenien zwischen supersingulären elliptischen Kurven über endlichen Körpern zu finden*), erhält man ein solches Problem, weil das IP-Problem sich zur Zeit mit Quantencomputern nicht besser als die exponentielle Zeit in der Länge des Schlüssels lösen läßt. Mit Hilfe vom IP-Problem wurde ein relativ neues sehr effizientes Schlüsselaustauchverfahren (SIDH) konstruiert [1, 2].

Ziel dieser Abschlußarbeit ist es,

- die mathematischen Methoden für SIDH näher zu untersuchen [1],
- die grundlegenden Hardprobleme und deren Beziehung zum IP-Problem zu erläutern [2],
- *eventuell* die Aspekte der Implementierung und der Effizienz vom SIDH für die verschiedenen Sicherheitsstufen (d.h. variierende Schlüssellänge) zu analysieren.

Referenzen

[1] L. De Feo. *Mathematics of Isogeny Based Cryptography*, https://arxiv.org/pdf/1711.04062.pdf, 2017.

[2] D. Jao und L. De Feo. *Towards Quantum-Resistant cryptosystems from supersingular elliptic curve isogenies*, Post-Quantum Cryptography, volume 7071, of Lecture Notes in Computer Science, 19–34, Springer, 2011.

Attributenbasierte Signaturverfahren mit Hilfe von sicherem und verifizierbarem Delegieren

Masterarbeit Informatik

12.03.2018

Atttributenbasierte Signaturen (ABS) ermöglichen eine feinkörnige (fine-grained) kryptographische Zugriffskontrolle über die Identifikationsinformationen um die gewünschten Nachrichten mittels eines attributengöherigen privaten Schlüssels zu signieren. Insbesondere erhält man mit den Attributen, die einer bestimmten Aussage genügen, ein privatheitsbewahrendes Signaturverfahren, welches das Schutzziel *Anonymität* der einzelnen Benutzer verwirklicht.

Obwohl viele effiziente ABS in der Literatur vorgeschlagen wurden, ist das eine große Herausforderung, ABS in resourcen-beschränkten Anwendungen wie die RFID-Karten, Smart-Karten, und/oder Sensoren zu bewerkstelligen, da die Berechnungskosten der ABS leider linear mit der Länge der Aussagenformel wächst. Um ein effizienteres ABS realisieren zu können, wurden daher neulich zwei Verfahren entwickelt [1], welche, im Falle der Existenz eines halbvertrauenswürdigen Cloud-Service-Anbieters (S-CSP), die entsprechenden Berechnungskosten der signierenden Benutzer erheblich reduzieren. Der S-CSP berechnet dabei die sogenannten Halbsignaturen, welche danach von Benutzer mit einem attributengöherigen privaten Schlüssel voll signiert werden. Leider ist bei diesen beiden Verfahren (in [1]) nicht auszuschließen, dass ein nicht-vertrauenswürdiger S-CSP die Benutzer täuschen, und somit falsche Halbsignaturen liefern kann.

Ziel dieser Masterarbeit ist es,

- die beiden Verfahren in [1] mit verschiedenen Sicherheitsstufen (Schlüssellänge) zu implementieren,
- eine verifizierbare (eventuell mit großer Wahrscheinlichkeit) Version des ABS zu untersuchen bzw. implementieren,
- die Ergebnisse in einer konkreten Anwendung zu vergleichen und evaluieren.

Referenzen

[1] X. Chen, J. Li, X. Huang, Ji. Li, Y. Xiang, und D. S. Wong. *Secure Outsourced Attribute-Based Signatures*, IEEE Transactions on Parallel and Distributed Systems (25), No. 12, 3285–3294, December 2014.