Kolloquium zu aktuellen Themen der Kryptographie

am 3.9. 2020

- **9:00** Prof. Dr. Steffen Reith (Hochschule RheinMain):
  (Kryptographische) Open Source Hardware

- **10:00** Alan Meckel (Uni Wü):
  Elliptische Kurven und die Berechnung von Quadratwurzeln mod p

- **11:00** Benedikt Müller (Uni Wü):
  Edwards-Kurven und ihre Anwendung in paarungsbasierter Kryptographie

- **13:00** Michael Meyer (Hochschule RheinMain):
  Threshold Schemes from Isogeny Assumptions

- **14:00** Fabio Campos (Hochschule RheinMain):
  Trouble at the CSIDH: Protecting CSIDH with Dummy Operations against Fault Injection Attacks

- **15:00** Thomas Aulbach (Uni Wü):
  Isogeny-based cryptography – B-SIDH and the quest for primes in smooth sandwiches

- **16:00** Philipp Muth (TU Darmstadt):
  (Somewhat) efficient Computation on Secret Shared Data

Abstracts

Prof. Dr. Steffen Reith (Hochschule RheinMain):
(Kryptographische) Open Source Hardware

Alan Meckel (Uni Wü):
Elliptische Kurven und die Berechnung von Quadratwurzeln mod p

Elliptische Kurven über endlichen Körpern stellen eines der grundlegendsten Konzepte der modernen Kryptographie dar.

Ich möchte Ihnen einen Überblick über meine Methoden vermitteln, eine Einführung in elliptische Kurven über endlichen Körpern geben und das Konzept von Schoof's Algorithmus in Grundzügen darstellen.

Wir erarbeiten ausgehend von einem anschaulichen Ansatz die Anzahl der Punkte auf einer elliptischen Kurve über einem endlichen Primkörper mit Charakteristik $p > 3$. Die Zielsetzung ist hier die asymptotische Laufzeit dieses Algorithmus zu bestimmen, dabei werden effiziente Methoden zur Bestimmung von Quadratwurzeln in endlichen Körpern erläutert. Da dieses Vorgehen asymptotisch nicht effizient ist, wird Schoof's Algorithmus als Alternative motiviert. Dieser bestimmt die Anzahl der Punkte einer elliptischen Kurve über einem endlichen Körper in polynomialer Laufzeit, was ihn zu einer bahnbrechenden Entdeckung macht.

Benedikt Müller (Uni Wü):
Edwards-Kurven und ihre Anwendung in paarungsbasierter Kryptographie

Elliptische Kurven sind in der Kryptographie beliebt, um Gruppen zu realisieren, in denen diskrete Logarithmen schwer zu berechnen sein sollen. In meiner Bachelorarbeit habe ich untersucht, ob sich Edwards-Kurven, spezielle, höchst effiziente elliptische Kurven, zum Einsatz in paarungsbasierter Kryptographie eignen. In solchen Protokollen werden Gruppen verwendet, über denen zusätzlich eine effizient zu berechnende bilineare Abbildung, auch Paarung (engl. Pairing) genannt, existiert. Spannende Vertreter der paarungsbasierten Kryptographie sind zum Beispiel zk-SNARKs, kurze nicht-interaktive Zero-Knowledge-Beweise. Die Frage, ob und wie effizient sich Paarungen über Edwards-Kurven realisieren lassen, bietet tiefe

Einblicke in die Theorie elliptischer Kurven. Interessanterweise spielt die geometrische Anschauung des Additionsgesetzes in Edwards-Kurven eine entscheidende Rolle.

Michael Meyer (Hochschule RheinMain):
Threshold Schemes from Isogeny Assumptions

We initiate the study of threshold schemes based on the Hard Homogeneous Spaces (HHS) framework of Couveignes. Quantum-resistant HHS based on supersingular isogeny graphs have recently become usable thanks to the record class group precomputation performed for the signature scheme CSI-FiSh. Using the HHS equivalent of the technique of Shamir's secret sharing in the exponents, we adapt isogeny based schemes to the threshold setting. In particular we present threshold versions of the CSIDH public key encryption, and the CSI-FiSh signature schemes

---

Fabio Campos (Hochschule RheinMain):
Trouble at the CSIDH: Protecting CSIDH with Dummy Operations against Fault Injection Attacks

The isogeny-based scheme CSIDH is a promising candidate for quantum-resistant static-static key exchanges with very small public keys, but is inherently difficult to implement in constant time.In the current literature, there are two directions for constant-time implementations: algorithms containing dummy computations and dummy-free algorithms. While the dummy-free implementations come with a 2x slowdown, they offer by design more resistance against fault attacks. In this work, we evaluate how practical fault injection attacks are on the constant-time implementations containing dummy calculations. We present three different fault attacker models, evaluate them on a ChipWhisperer board, and present countermeasures.

Thomas Aulbach (Uni Wü):
Isogeny-based cryptography – B-SIDH and the quest for primes in smooth sandwiches

B-SIDH is a variation of the more famous isogeny based cryptosystem SIDH introduced by De Feo and Jao in 2011. It works also with the torsion of the twist of the elliptic curves and therefore, may lift the restriction on the form of the primes $p = 2^e 3^f 1$, which is typical for SIDH.

We briefly introduce the SIDH protocol and the main technicalities that prove its correctness. We illustrate the important adaption that allows to choose isogenies from the twist of the elliptic curves, when working with projective XZ-only Montgomery coordinates. The degrees of these isogenies correspond to factors of the group order of the twist $p1$. This facilitates the usage of new prime classes in the B-SIDH setting and we present search methods for those, following a recent work by Costello.

Philipp Muth (TU Darmstadt):
(Somewhat) efficient Computation on Secret Shared Data

Die Menge an personenbezogenen Informationen, die über jeden Einzelnen von uns auf täglicher Basis erhoben werden, ist in den letzten Jahren dramatisch angestiegen und tut dies auch weiter. Während Teile dieser Informationen, wie zum Beispiel präferierte Speiseeissorten, keines besonderen Schutzes bedürfen, muss die Vertraulichkeit anderer Teile umso stärker forciert werden. Dies kann beispielsweise per Secret Sharing Algorithmen geschehen. Einerseits garantiert Secret Sharing unbedingte Vertraulichkeit solange nicht eine authorisierte Menge an Beteiligten korrumpiert wird. Andererseits sind Berechnungen auf den Daten entweder ineffizient oder hebeln die Vertraulichkeit aus. Wir behandeln einen effizienten Ansatz für Berechnungen auf geteilten Daten ohne diese rekonstruieren zu müssen, der gleichzeitig die Korrektheit der Berechnung sicherstellt.