
Abstract

- **Name:** Meers
- **First Name:** Jonas
- **Title:** Isogeny Based Cryptography: Design and Attacks

Cryptography is everywhere. It secures online communication, bank transactions, and private messaging on a daily basis. Public key cryptography plays a central role in this context, enabling two parties to exchange a secret even if they have never interacted before. However, with large-scale quantum computers becoming available, it is only a matter of time before most public key protocols become obsolete due to Shor’s algorithm.

Isogeny-based cryptography is one of the many approaches to achieving post-quantum security. It builds on the hardness of finding an isogeny between two supersingular elliptic curves, which appears to be too complex of a problem even for a quantum computer. However, this added complexity is also reflected in many other aspects of isogenies.

One notable example is the design of isogeny-based protocols. In particular, more advanced protocols are much harder to construct from isogenies than their pre-quantum counterparts. Since many real-world applications rely on these protocols, it is necessary to explore how to make them post-quantum secure using isogenies.

Furthermore, since isogenies are a relatively young field of research, there are many unexplored areas in its cryptanalysis. Particularly, this concerns leakage attacks on isogeny-based protocols where an adversary is given (parts of) internal values that may enable an efficient attack. Once a protocol is deployed in the real world, these attacks become a real threat and need to be researched in advance.

In this context, this thesis advances the state of the art in two areas:

- **Isogeny-Based Protocol Design:** We give novel constructions for three advanced cryptographic primitives based on isogenies: Updatable Encryption, Authenticated Key Encapsulation and Non-Interactive Timed Commitments. Compared to previous works, our constructions improve in at least one of the following areas: security, efficiency or compactness.
- **Cryptanalysis of Isogenies:** We develop several leakage attacks on isogeny-based key exchanges and signature schemes. Furthermore, we show that some isogeny-based schemes feature an inherent leakage resilience.

Zusammenfassung

- **Name:** Meers
- **Vorname:** Jonas
- **Titel:** Isogeny Based Cryptography: Design and Attacks

Kryptografie ist allgegenwärtig. Sie sichert täglich unsere Online-Kommunikation, Banktransaktionen und privaten Nachrichten. Die Public-Key-Kryptografie spielt in diesem Zusammenhang eine zentrale Rolle, da sie es zwei Parteien ermöglicht, ein Geheimnis auszutauschen, auch wenn sie zuvor noch nie miteinander interagiert haben. Mit der Verfügbarkeit großer Quantencomputer ist es jedoch nur eine Frage der Zeit, bis die meisten Public-Key-Protokolle aufgrund von Shor's Algorithmus obsolet werden.

Die isogeniebasierte Kryptografie ist einer von vielen Ansätzen, um Post-Quanten-Sicherheit zu erreichen. Sie baut auf der Schwierigkeit auf, eine Isogenie zwischen zwei supersingulären elliptischen Kurven zu finden, was selbst für einen Quantencomputer ein zu komplexes Problem zu sein scheint. Diese zusätzliche Komplexität spiegelt sich jedoch auch in vielen anderen Aspekten von Isogenien wider.

Ein wichtiges Beispiel ist das Design von isogeniebasierten Protokollen. Vor allem fortgeschrittenere Protokolle sind viel schwieriger mit Isogenien zu konstruieren als ihre Prä-Quanten-Pendants. Da viele reale Anwendungen auf diesen Protokollen basieren, muss untersucht werden, wie sie mit Hilfe von Isogenien post-quantensicher gemacht werden können.

Da Isogenien ein relativ junges Forschungsgebiet sind, gibt es außerdem viele unerforschte Bereiche in ihrer Kryptoanalyse. Dies betrifft insbesondere Leakage-Angriffe auf isogeniebasierte Protokolle, bei denen ein Angreifer (Teile von) internen Werten erhält, die einen effizienten Angriff ermöglichen könnten. Sobald ein Protokoll in der Praxis eingesetzt wird, stellen diese Angriffe eine echte Bedrohung dar und müssen im Voraus untersucht werden.

In diesem Zusammenhang entwickelt diese Arbeit den Stand der Technik in den folgenden zwei Bereichen weiter:

- **Isogenie-basiertes Protokoll-Design:** Wir stellen neuartige Konstruktionen für drei fortschrittliche kryptografische Primitive auf Basis von Isogenien vor: Updatable Encryption, Authenticated Key Encapsulation und Non-Interactive Timed Commitments. Im Vergleich zu früheren Arbeiten bieten unsere Konstruktionen Verbesserungen in mindestens einem der folgenden Bereiche: Sicherheit, Effizienz oder Kompaktheit.
- **Kryptoanalyse von Isogenien:** Wir entwickeln mehrere Leakage-Angriffe auf isogeniebasierte Schlüsselaustausch- und Signaturschemata. Darüber hinaus zeigen wir, dass einige isogeniebasierte Schemata eine inhärente Leakage-Resilienz aufweisen.