OUKA
The University of Osaka
Institutional Knowledge Archive

Title	Isogeny-Based Multi- and Proxy Signatures, and a Private Tracing Protocol Based on Multi-Signatures
Author(s)	De Goyon, Mathieu
Citation	大阪大学, 2026, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/105281
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

様式３

論　文　内　容　の　要　旨

氏　名　（DE GOYON Mathieu）	
論文題名	Isogeny-Based Multi- and Proxy Signatures, and a Private Tracing Protocol Based on Multi-Signatures (同種写像ベースの多重署名，代理署名と多重署名に基づくプライベート追跡プロトコル)

論文内容の要旨

The potential development of large-scale quantum computers has raised serious concerns about the security of classical cryptographic systems. In response, the field of post-quantum cryptography has emerged to design cryptographic schemes that remain secure even against quantum adversaries. Isogeny-based cryptography is the most recent addition to post-quantum cryptography and started garnering attention in the 2010s.
Digital signature schemes are a fundamental part of public key cryptography, providing authenticity, integrity, and non-repudiation for digital messages. They are essential for secure communication, software updates, electronic transactions, and virtually all systems requiring trust and verification. Although the traditional digital signature scheme consists only of a single prover and verifier, numerous variants have been developed over the years to address specific needs, such as multi-signatures, ring signatures, group signatures, and proxy signatures. These variants extend the functionality of traditional signatures to support more complex security models in real-world applications, such as contact tracing.
As isogeny-based cryptography is a relatively young research field, many commonly used cryptographic primitives, such as variants of signature schemes, have not yet been fully developed or widely implemented. This leaves room for exploration and optimization in designing secure and efficient isogeny-based alternatives, while taking advantage of its strength with its small keys and signature compared to other post-quantum based constructions such as lattice.

Multi-signature schemes have been extensively studied for decades and form a well-established area of research in cryptography. These schemes enable a group of users to collaboratively generate a single, compact signature on a shared message, ensuring that all designated parties have approved the content. Their efficiency and security properties make them particularly valuable in applications such as blockchain transactions and distributed systems. Active security in multi-signature schemes requires the signature to be unforgeable even in the worst-case scenario, where malicious signers would collude to generate a multi-signature in a group with a single honest signer. Our first contribution is to propose an actively secure isogeny-based multi-signature scheme.

Proxy signature schemes have been the subject of extensive research over the years, offering cryptographic solutions for secure delegation of signing authority. These schemes allows an original signer to designate a proxy signer to generate signatures on their behalf, within the limitations imposed by the original signer. Such mechanisms are particularly useful in settings like secure communications, delegated access control, and corporate approval systems where it is essential for operations to continue even in the absence of the designated signer. Proxy signatures are required to be unforgeable even if either the original or the proxy signer is malicious, which is commonly referred to as the existential unforgeability under chosen message attack and chosen warrant attack. Some security models with more stringent requirements, such as existential unforgeability under chosen

message attack with proxy key exposition (EUF-CMA-PKE), require the proxy signature to be unforgeable even if the proxy signing key are leaked. Our second contribution is to propose two proxy signatures satisfying both models using isogeny-based cryptography.

Contact tracing applications have become a crucial tool in managing public health during pandemics, relying on digital protocols to identify and notify individuals exposed to infectious diseases. These systems must balance effective tracking with strong privacy guarantees, ensuring that users' identities remain confidential. At the same time, it is essential that they reflect accurately the situation on the ground. To achieve this, advanced cryptographic techniques, such as ring signatures and multi-signatures, can be employed, making contact tracing a promising real-world application for these variant signature schemes. Our third contribution is to propose a contact tracing application which correctly reflects the interactions between patients and their close contacts while preserving the privacy of its users.

The work of this dissertation is divided into studies about isogeny-based multi-signatures, isogeny-based proxy signatures, and efficient multi-party contact tracing protocols.

- A proposal of an actively secure isogeny-based multi-signature that uses zero-knowledge proofs and commitments to guarantee the existential unforgeability of the signature.
- A proposal of two isogeny-based proxy signature protocols guaranteeing existential unforgeability in the case of a corrupted original or proxy signer, one designed to remain secure even in the event of proxy key leakage, and another constructed under the assumption that the proxy key remains secret.
- A proposal of a contact tracing protocol using ID-based ring signatures and multi-signatures to accurately reflect the interactions between users in an efficient way while preserving their privacy.

The first study is composed of the first isogeny-based multi-signature scheme by extending the isogeny-based signature scheme CSI-SharK to the multi-party setting. Our scheme is proven unforgeable in the random oracle model under the MT-GAIP and C_{k-1}-VPwAI assumptions. To achieve security, a new proof system based on zero-knowledge proof and commitments is proposed by modifying the piecewise verifiable proof system proposed in the Distributed Key Generation protocol CSI-RASHI.
The second study is composed of two isogeny-based proxy signature protocols, ¥PKE{} and ¥CWA, based on CSI-SharK. Both are proven unforgeable under the MT-GAIP and C_{k-1}-VPwAI assumptions in the quantum random oracle model and considers chosen message attacks (corrupted original signer) and chosen warrant attacks (corrupted proxy signer), but only the former considers the risk of proxy key leakage.
The third study is composed of a privacy-preserving contact tracing application that accurately represents the interaction of its users, such as the number of participants. It is achieved by using the contact tracing protocol proposed by Liu et al and adapt it to the multi-party setting by incorporating a multi-signature as a proof of the meeting and a ring signature as a way to alert the close contacts while preserving the patient's privacy.
To summarize, the first two studies adapt a variant signature scheme, i.e., a multi-signature and a proxy signature, to the isogeny-based setting, while the third study proposes a potential application of such variant schemes.
The multi-signature scheme from the first study can be integrated into the third study's contact tracing protocol by replacing it, although the protocol would need to be adjusted to compensate for the lack of ID-based ring signatures in isogeny-based cryptography.

様式 7

論文審査の結果の要旨及び担当者

氏　名　（DE GOYON Mathieu）			
論文審査担当者	（職）		氏　名
	主 査	教授	宮地 充子
	副 査	教授	滝根 哲哉
	副 査	教授	丸田 章博
	副 査	教授	田中 雄一
	副 査	教授	落合 秀樹
	副 査	教授	清水 昌平
	副 査	教授	駒谷 和範
	副 査	講師	樽谷 優弥
	副 査	教授	鈴木 幸太郎（豊橋技術科学大学）

論文審査の結果の要旨

Digital signatures are a fundamental technology in the digital society, ensuring the authenticity, integrity, and non-repudiation of digital messages. Over the years, numerous specialized digital signatures have been developed to address specific needs. Among them, multi-signatures and proxy signatures have attracted the most attention. This dissertation focuses on these two specialized digital signatures—multi-signatures and proxy signatures—as well as their applications and provides the following contributions.

Multi-signatures are designed for scenarios in which a group of signers jointly produce a single compact signature on a common message. Originally introduced in 1983, multi-signatures have gained renewed importance in the post-quantum era. Existing post-quantum multi-signature research has primarily focused on lattice-based constructions, which tend to suffer from large key and signature sizes. In contrast, isogeny-based cryptography offers smaller key and signature sizes, but no isogeny-based multi-signature scheme had been proposed before. This dissertation presents the first isogeny-based multi-signature scheme, along with a new proof system required to achieve active security. Since all post-quantum multi-signatures have been limited to lattice-based constructions, this isogeny-based approach represents a significant contribution to the diversification and advancement of post-quantum cryptography.

Proxy signatures allow an original signer to delegate its signing rights to a proxy signer. They are useful in scenarios such as e-commerce, distributed systems, or corporate operations where actions must continue in the absence of the original signer. As with multi-signatures, post-quantum proxy signatures have become important. In the isogeny-based setting, the existing CSI-PS signature—built upon the SeaSign signature—suffers from slow signing and key generation, as well as large keys and signatures. Moreover, CSI-PS provides security only under the existential unforgeability under chosen message attack (EUF-CMA) model. Although a generic proxy signature construction exists, it fails to achieve misuse prevention and verifiability. To address these shortcomings, this thesis first formalizes the security properties of proxy signatures, explicitly capturing attacks related to misuse and verifiability. Based on this new formalization, two isogeny-based proxy signature schemes are proposed, both built upon the CSI-SharK signature. The first scheme achieves EUF-CMA-CWA (existential unforgeability under chosen message and chosen warrant attacks), while the second achieves

EUF-CMA-PKE (existential unforgeability under chosen message attack and proxy key exposure). The CWA scheme is faster, more compact, and more secure than CSI-PS, while also satisfying the new security properties. The PKE scheme, though slower, provides stronger security guarantees under a stricter model.

The final part of this research explores an application in contact tracing, a crucial technology during the COVID-19 pandemic. Contact tracing protocols aim to identify and alert potentially infected individuals while preserving user privacy and preventing false alerts. Most existing protocols rely on short-term identifiers and only consider pairwise interactions, which does not fully reflect real-world group encounters. To overcome this limitation, this thesis proposes a multi-party contact tracing protocol that leverages multi-signatures to prove group meetings and uses an ID-based ring signature as the alert mechanism. This ensures that only government-authorized patients can issue alerts, maintaining both reliability and privacy.

In summary, this dissertation presents novel isogeny-based multi-signature and proxy signature schemes, along with a practical application demonstrating their utility. It introduces the first isogeny-based multi-signature, enhances isogeny-based proxy signatures with new formal definitions and stronger security, and applies multi-signatures to privacy-preserving contact tracing. These contributions advance two essential cryptographic technologies that underpin the trust and authenticity of digital communications. The research not only deepens the theoretical foundation of post-quantum cryptography but also provides tangible evidence of how these technologies can transform our digital society. Therefore, this work makes a significant contribution to the field of information security and engineering and stands as a valuable doctoral dissertation.