On the Design and Security of Post-Quantum Aggregate Signatures

Turin, October 14, 2024

Candidate: Edoardo Signorini.
Supervisor: Prof. Danilo Bazzanella
Co-supervisor: Dott. Guglielmo Morgari

Abstract

Digital signatures are pivotal for ensuring the authenticity and integrity of digital communications, serving as the backbone of numerous cryptographic protocols and systems. However, the physical constraints of network communication pose challenges in the transmission of large number of signatures, including digital certificates in Public Key Infrastructures, routing protocols, and decentralized systems. The advent of quantum computing has heightened these challenges, given that post-quantum cryptographic schemes, like those proposed under NIST's standardization project, generally result in larger signature sizes.

Aggregate signatures represent a powerful cryptographic tool to reduce communication costs in protocols that require the verification of multiple signatures. In fact, this method can reduce the total amount of transmitted data by allowing multiple signers to combine their individual signatures on separate messages into a single aggregate signature. Since general forms of aggregations are difficult to achieve in practice, weaker variants can be considered. For instance, in a Sequential Aggregate Signature (SAS) scheme, signatures are combined in a specific sequence, allowing each subsequent signer to append their signature to an already aggregated one. Although sequential aggregation is more restrictive, it often suits contexts where order or hierarchy are inherent, thus continuing to be beneficial in practical applications. This thesis contributes primarily by exploring aggregate signatures under post-quantum assumptions, particularly focusing on signature schemes that are not based on structured lattices.

Our research delves into two main classes of digital signatures in the post-quantum setting. Firstly, we explore the generalization of SAS schemes to Hash-and-Sign signatures based on generic trapdoor functions. The simple structure of signatures within this paradigm appears to make them ideal candidates for sequential aggregation. However, early SAS proposals required the use of trapdoor permutation (e.g., RSA), while post-quantum trapdoor functions known so-far are not injective. Direct attempts at generalizing permutation-based schemes have been proposed, but they either lack formal security or require additional properties on the trapdoor function, which are typically not available for multivariate or code-based functions. We provide a comprehensive

analysis of existing models, discuss their limitations, and prove how direct extensions of original SAS schemes are not possible without additional properties. Then, we propose a novel construction of history-free SAS within the probabilistic Hash-and-Sign with retry paradigm, generalizing existing techniques to generic trapdoor functions. We prove the security of our scheme in the random oracle model, and we instantiate our construction with multivariate and code-based schemes.

Secondly, we investigate the potential of group action-based signatures within the Fiat-Shamir paradigm, proposing new techniques for signature aggregation. Group actions are emerging as a promising tool in post-quantum cryptography, and have been used to build several signature schemes, including some submitted to the recent NIST call for additional post-quantum signatures. We propose two novel aggregation methods for group action-based signatures: a sequential aggregate signature and an interactive aggregation scheme. Although provably secure sequential aggregation can be achieved, we show that the resulting compression is too small for practical applications. Therefore, we investigate a trade-off between aggregation capabilities and the need for interaction between signers. We then obtain an interactive aggregation scheme (or multi-signature), whose security can be reduced directly to the assumptions underlying the group action.