The Freedom of Information and the Freedom to Edit

Degree programme: Master of Science in Engineering | Specialisation: Information and Communications Technologies
Thesis advisor: Prof. Dr. Reto Koenig
Expert: Dr. Stephan Krenn (Austrian Institute of Technology)

Classical digital signatures authenticate a message and ensure its integrity; however, a signed message may not subsequently be modified. As one of the main reasons for signing is the detection of modifications, why would it possibly be desirable to break this property on purpose? And if so, how? In fact, there are situations, for which this makes sense, and this is where Malleable Signature Schemes for Editing (MSSEs), which we will explore in this work, come into play.

Since almost exactly twenty years, redactable signature schemes are known as a cryptographic primitive, shortly followed by sanitizable signature schemes. Together, they constitute an important part of the broader family of MSSEs, for which active research is still ongoing. They both allow for the editing of parts of a signed message without invalidating the corresponding signature, though the possible kinds of modifications differ. Despite their long availability, MSSEs are not yet widely known and used in practice so far - we hope to contribute in changing this with our work.

A Novel Use Case

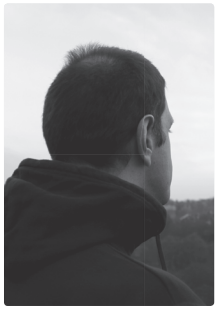
An important aspect for the dissemination of a technology are practical and accessible use cases. Often so far, the application of MSSEs has been considered for the domain of e-health, where their properties enable privacy-preserving, yet authenticated exchange of patient data for instance. In our work, we develop a novel use case for an entirely different domain, which we consider applicable to a broad range of scenarios: the editable signature of documents released in so-called freedom of information requests (FOIA). FOIAs have become an important mechanism for interacting with institutions of the public sector, and we think that the application of MSSEs may provide a large improvement to the processes involved.

A Practical and Efficient Implementation

A second, important part of our work consists of a practical and efficient implementation of a concrete MSSE construction, serving multiple purposes. First, it enables the demonstration of the FOIA use case to interested parties, while at the same time being flexible enough to also support different applications. Next, due to the simplicity of the underlying construction, as well as the compact and readable code base, it may readily be used as a tool for teaching MSSEs in applied cryptography courses. Finally, as the first available implementation of this specific construction, it also serves as framework for its practical validation and for further evaluation and research.

Contributing Back to the Cryptographic Community

This last aspect of our implementation leads us to our third and final contribution, which consists of supporting the research of the underlying construction. Here, we have contributed to the quest for a so-called secure enumeration algorithm, which is required for the construction to be secure. We have also provided initial performance figures, which help in comparing the approach taken with other MSSEs. Our concurrent contribution to the scientific paper being written at the time this work is being handed in, will continue, and we hope in the end to provide another interesting MSSE to the cryptographic community.



Pascal Mainini