
# BROKERAGE AND MARKET PLATFORM FOR PERSONAL DATA

## *D4.1*
## *Progress report on cryptographic protocols for privacy-preserving data markets and SSI systems*

www.krakenh2020.eu

This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 871473

# D4.1
# Progress report on cryptographic protocols for privacy-preserving data markets and SSI systems

| | |
|---|---|
| **Grant agreement** | 871473 |
| **Work Package Leader** | TUG |
| **Author(s)** | Sebastian Ramacher (AIT), Karl Koch (TUG) |
| **Contributors** | Daniel Kales (TUG), Stefan More (TUG) |
| **Reviewer(s)** | Luigi Rizzo (ICERT), Juan Carlos Pérez Baún (Atos) |
| **Version** | Final |
| **Due Date** | 31/07/2021 |
| **Submission Date** | 27/07/2021 |
| **Dissemination Level** | Public |

**Release History**

| Version | Date | Description | Released by |
|---|---|---|---|
| v0.0 | 30/04/2021 | Initial version | Karl Koch (TUG) |
| v0.1 | 10/05/2021 | Contributing to T4.3 | Stefan More (TUG) |
| v0.2 | 26/05/2021 | Contributions to T4.2, T4.3, and Conclusion | Karl Koch (TUG) |
| v0.3 | 27/05/2021 | Contributing to Introduction | Karl Koch (TUG) |
| v0.4 | 28/05/2021 | Contributions to T4.1-T4.3 | Daniel Kales (TUG) |
| V0.5 | 28/05/2021 | Contributions to T4.1-T4.2 | Sebastian Ramacher (AIT) |
| v0.6 | 23/06/2021 | Contributions to T4.1, T4.2, and Conclusion | Sebastian Ramacher (AIT) |
| v0.7 -> v1.0 | 06/07/2021 | Contributions to T4.3, Conclusion, and Executive Summary; Minor adaptions in T4.1, T4.2, and Bibliography | Karl Koch (TUG) |
| v1.1 | 23/07/2021 | Baking in reviewers' feedback on T4.3, Conclusion, Bibliography & References, and general (meta) things; as well as parts of the feedback on Executive Summary | Karl Koch (TUG) |
| V1.2 | 26/07/2021 | Updates to executive summary, introduction; integration of reviewer feedback on T4.1 and T4.2; finalization of the deliverable | Sebastian Ramacher (AIT) |

# Table of Contents

# List of Acronyms

| Acronym | Description |
|---|---|
| CA | Consortium Agreement |
| WP | Work Package |
| MPC | Multi-Party Computation |
| SNARKs | Succinct Non-Interactive Arguments of Knowledge |
| GDPR | General Data Protection Regulation |
| FE | Functional Encryption |
| ZK-PoK | Zero-Knowledge Proof of Knowledge |
| ZKP | Zero-Knowledge Proof |
| SSI | Self-Sovereign Identity |
| NIST | National Institute of Standards and Technology |
| PQC | Post-Quantum Cryptography |
| IND-CCA2 | Indistinguishability under adaptive chosen ciphertext attacks |
| MQDSS | Multivariate Quadratic Digital Signature Scheme |
| AES | Advanced Encryption Standard |
| PKE | Public-key encryption |
| KEM | Key-encapsulation mechanism |
| HHK | Hofheinz, Hövelmanns, and Kiltz |
| FO | Fujisaki-Okamoto |
| (Q)ROM | (Quantum) Random Oracle Model |
| CPA | Chosen Plaintext Attack |
| CCA | Chosen Ciphertext Attack |
| IBE | Identity-Based Encryption |
| BFKEM | Bloom Filter KEM |
| 0-RTT | Zero Round-Trip Time |
| PE | Puncturable Encryption |
| DFPE | Dual-Form Puncturable Encryption |
| TLS | Transport Layer Security |
| SSH | Secure Shell Protocol |
| US | Updatable Signature |
| UMAC | Universal Message Authentication Code |
| PRF | Pseudorandom Function |
| RLWE | Ring Learning With Errors |
| SIS | Short Integer Solution |
| BLS | Boneh-Lynn-Shacham |
| SE | Simulation extractability |
| NIZK | Non-Interactive Zero Knowledge |
| CRS | Common Reference String |
| STARK | Succinct Transparent Argument of Knowledge |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| DID | Decentralized Identifier |

# List of Figures

# Executive Summary

The work in Work Package 4 (WP4) is mainly concerned with the cryptographic tools employed as part of KRAKEN. Within WP4, the focus lies on the cryptographic design and analysis, as well as efficient and secure implementations of thereof. This deliverable, D4.1 *Progress report on cryptographic protocols for privacy-preserving data markets and SSI systems*, describes the research efforts as conducted to build a privacy-preserving and authenticity-preserving KRAKEN architecture. The goal of this deliverable is to give a high-level overview of research results on cryptographic tools affecting the KRAKEN architecture. The final version of the report on research on cryptographic primitives, schemes and protocols will be released as D4.2 *Final research report on cryptographic protocols for privacy-preserving data markets and SSI systems* in May 2022.

The research results presented as part of D4.1 are motivated by the requirements and needs defined in other work packages. Specifically, work packages 2 (for the overall architecture), 5 (for the data marketplace) and 3 (for the self-sovereign identity aspects) and their deliverables D5.1 *Initial Pilot Marketplaces User Stories*, D3.1 *Self sovereign identity solution. First release*, D2.2 *Intermediate KRAKEN architecture,* and D2.4 *KRAKEN intermediate technical design* serve as main inputs for this deliverable. At the same time, the results of this deliverable influences design decisions that must be made regarding the architecture as well as features to be integrated in KRAKEN. Therefore, this deliverable will serve as inputs to the forthcoming deliverables D2.5 *KRAKEN final technical design*, D5.4 *Final KRAKEN marketplace integrated architecture document*, D3.2 *Self sovereign identity solution. Final release*, and D4.4 *Final implementation of cryptographic libraries*.

This report relates to Tasks 4.1 to 4.3 of WP4: Task 4.1 provides design and research in the area of end-to-end-secure data sharing; between, e.g., a data producer and a data consumer via a marketplace (like the one of KRAKEN). Task 4.2 provides design and research in the area of privacy-preserving as well as authenticity-preserving data analytics, of, e.g., many data producers for a (dedicated) data consumer, such that the consumer gets only the analysis result, and all that while the (KRAKEN) marketplace does not learn either the input data nor the result. Task 4.3 provides research and enhancement opportunities in the area of (KRAKEN's) cryptographic aspects of self-sovereign identity (SSI). Finally, we outline ongoing research and future work within these areas.

# 1 Introduction

## 1.1 Purpose of the document

KRAKEN is comprised of three core pillars: the self-sovereign identity (SSI) paradigm, the data marketplace, and cryptographic tools. The goal of Work Package 4 is to provide the cryptographic tools to support the functionality of the other two pillars. Cryptographic primitives, schemes and protocols are analyzed, developed and implemented to support the applications envisioned for the data marketplace as well as the cryptographic aspects of implementing SSI systems. Therefore, we focus on the cryptographic building blocks that are required to implement the functionalities, applications and use-cases of Work Package 3 and Work Package 5. One core aspect of the cryptographic tools is their privacy-preserving features which are required in all KRAKEN use-cases and applications.

For the data marketplace, KRAKEN envisions use-cases that are supported and partly enabled by the cryptographic protocols and schemes. Most importantly, cryptographic techniques such as secure multi-party computation and functional encryption – among others – enable us to build a data-analytics-as-a-service platform that tightly integrates into the data marketplace. Cryptography is also a key aspect to ensure end-to-end secure data transfer with fine-grained access control both in terms of confidentiality and authenticity which can be achieved by employing sophisticated encryption schemes such as proxy re-encryption, puncturable encryption, attribute-based encryption and others. For authenticity guarantees in both applications we require (group) signature schemes and zero-knowledge proofs. Both are also essential building blocks for SSI systems.

The purpose of this document is to give an overview of the research results obtained so far regarding the objectives set out for Work Package 4 and specifically on those covered by Tasks 4.1 to 4.3. The objectives focus on cryptographic tools for end-to-end secure data sharing, authenticity of data analytics via cryptographic means, and confidentiality of privacy-sensitive data while performing data analysis. The research topics are also driven by the requirements identified and derived in Work Package 5 (cf. D5.1 *Initial Pilot Marketplaces User Stories* [25]) and Work Package 3 (cf. D3.1 *Self sovereign identity solution. First release* [26]) and the architecture designed in Work Package 2 (cf. D2.2 *Intermediate KRAKEN architecture* [23] and D2.4 *KRAKEN intermediate technical design* [24]). The latter is highlighted by the LINDDUN analysis of the data marketplace architecture which helped us to fix and mitigate some risks which were identified as part of this analysis. Thus, the results of this deliverable directly influence KRAKEN's architecture and will thus serve as input for the forthcoming deliverables in Work Packages 2 and 4 (D2.5 *KRAKEN final technical design* and D5.4 *Final KRAKEN marketplace integrated architecture document*). The results on privacy aspects of SSI systems will serve as input for Work Package 3 (D3.2 *Self sovereign identity solution. Final release*). As this deliverable discusses cryptographic building blocks that will be integrated in KRAKEN, it also serves as input for future implementation efforts in Task 4.2 and is therefore input to its final deliverable, D4.4 *Final implementation of cryptographic libraries*.

We will give a short overview of the goals and the research conducted in each Task. In Sections 2, 3, and 4 we present a more in-depth discussion of the individual research results which have been published in peer-reviewed conference or workshop proceedings.

**T4.1 End-to-end secure data-sharing capabilities.** The secure sharing of data is at the core of a data marketplace. Participants want to share their data only with potential buyers, without the need to first upload it in the clear to the marketplace or any third party. To secure this process, we rely on both well-established cryptographic primitives for confidential and authentic data transfer, such as Transport Layer Security (TLS), and also advanced cryptographic primitives that allow the delegation of access rights to encrypted data, such as proxy re-encryption or attribute-based encryption. Part of the research carried out in Task 4.1 investigates long-term aspects of the security of TLS by designing and analyzing the security of post-quantum cryptographic primitives. Quantum computers pose a major threat to the current TLS infrastructure as all public-key encryption and signature schemes

currently used in TLS are vulnerable to attacks from powerful quantum computers. The second part of the research in Task 4.1 focuses on the design and security of advanced cryptographic primitives for data sharing. These new primitives can provide advanced features such as fine-grained access control and forward-secrecy that are not possible to achieve using the traditional cryptographic primitives used, for example, in TLS.

**T4.2 – Authenticity-preserving and privacy-preserving data analytics.** The secure implementation of a data analytics as a service platform as envisioned for the data marketplace has some challenging requirements regarding both privacy of user's data and the authenticity of the processed data. First, beyond the result of the performed data analytics that is obtained by the buyer, no party is allowed to learn or obtain any data that is processed by the overall system. This requirement implies that also the data processors are only allowed to work on encrypted or otherwise secured user data. Second, data owners should be able to verify the authenticity of the received results. Beyond the authenticity of the computation, authenticity guarantees are required to hold also with respect to the data source. Therefore, Task 4.2 focuses on the cryptographic tools including secure multiparty computation and non-interactive zero-knowledge proofs to achieve both features.

Our research focuses on design and the security of the overall architecture including all building blocks and their interaction to deploy such a platform. The results from the security analysis directly influenced the design proposed in WP2 to implement the data marketplace in WP5. Also, we are interested in reducing the trust requirements necessary to deploy non-interactive zero-knowledge proofs in practice.

**T4.3 – Cryptographic aspects of SSI systems.** Self-Sovereign Identity (SSI) systems aim to give the user control over their (digital) identity. However, even with SSI systems in place, additional privacy challenges for users exist. One such example is the selective showing of parts of your credentials (for example, only your age), without the need to show your full data to a potential verifier.

Based on the needs of Work Package 3, Task 4.3 focuses on the research of cryptographic tools for SSI systems. Our research deals with more advanced privacy aspects, such as the ability to delegate rights to your data to another party, the security and efficiency of a critical one-time setup phase in an existing SSI system to support revocation of credentials and the concrete efficiency of privacy-preserving credential showings using zero-knowledge proofs. As the involved cryptographic tools may incur a non-negligible performance penalty, also the performance of such systems and their building blocks are of concern. Thus, a goal is to reduce the costs of deploying privacy-preserving systems in practice by designing secure primitives that work particularly well together.

## 1.2 Structure of the document

The remainder of this document is organized as follows:

- Section 2 describes our contributions within **T4.1 - End-to-end secure data-sharing capabilities**,
- Section 3 describes our contributions within **T4.2 - Authenticity-preserving and privacy-preserving data analytics**,
- Section 4 describes our contributions within **T4.3 - Cryptographic aspects of SSI systems**, and
- Section 5 discusses ongoing research and outlines planned future work.

# 2 T4.1 - End-to-end secure data-sharing capabilities

One of the core goals that the KRAKEN data marketplace tries to achieve and implement is the secure transfer of any kind of data between users – data sellers and data buyers. In the context of a data marketplace, providing a system for end-to-end secure data sharing has to address unique challenges that arise from the marketplace's architecture (cf. D2.4 [24]). First of all, any data transfer between users must be end-to-end secured to reduce the risk of data leakage and legal liability on the side of the data market. In order to avoid potential legal issues when having plaintext access to users' data, the KRAKEN marketplace architecture was designed so that the operators of the KRAKEN marketplace itself never have access to plaintext users' data.

Feature-wise, KRAKEN does not require the owners of their data to be always online. Thereby any identifiable information including public keys or certificates of the buyers is not available when users register their data sets for sale on the marketplace. Hence, data sellers already need to prepare their data in a way that any buyer can access the bought data without having any direct interaction with the corresponding seller. Therefore, we build our data sharing system with more expressive tools than public-key encryption and investigate technologies such as proxy re-encryption, attributed-based and functional encryption that allows us to specify fine-grained access policies. These policies ideally support access by multiple different buyers without the need to produce distinct ciphertexts for every buyer.

We are also concerned with the storage and protection of data over long timeframes, where potential advances in quantum computing threaten the security of existing and currently employed public-key cryptography. To prepare for this scenario, many standardization bodies initiated a selection process for cryptographic primitives providing post-quantum security, with the most prominent being the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) standardization project [1].

For end-to-end secure data sharing we focus on puncturable encryption (PE) which provides two interesting features: first, it allows us to build forward secure public-key encryption schemes. Thereby, we can ensure that encrypted data can stay secure even in the case of key compromise. Regardless of whether a key was leaked by accident or a user was actively attacked, forward security plays a critical role in particular if ciphertexts are stored for long time periods in the cloud. Beyond forward-secure public-key encryption, our work on PE in Section 2.4 also gives rise to forward-secure identity-based encryption. Thereby we are able to combine strong security properties with capabilities to delegate access rights. The work we present in Section 2.1 also considers PE for forward secure communication channels in the context of post-quantum cryptography.

In our work on post-quantum secure cryptography we are interested in two aspects: long term secure public-key encryption and digital signatures. The former is important for KRAKEN to ensure long-term security of stored data. While quantum computers are not powerful enough currently, more powerful ones may become a threat to data that is stored over long periods of time. Digital signature schemes also play a crucial role for authenticating users and authenticating data. Both factors are important for data sharing as otherwise the marketplace is unable to verify the identity of its users. They also enable data buyers to verify the authenticity of the data. In the context of public-key encryption schemes, we consider public-key encryption schemes that are currently submitted to the NIST PQC standardization project in Section 2.1. In particular, we are interested in generic transformations to obtain strong security guarantees (indistinguishability under adaptive chosen ciphertext attacks – IND-CCA2). The transformation we consider in this work is targeted towards constructions that start from post-quantum secure assumption which inherently have issues with decryption errors. For the signatures, we focused also on candidate schemes that are currently under consideration by NIST for standardization. In Section 2.2 we present an attack on Multivariate Quadratic Digital Signature Scheme (MQDSS), a digital signature scheme based on an assumption on multivariate equations, which

reduces the security level of the proposed parameter sets significantly. Furthermore, we proposed new variant of the Picnic signature scheme called Banquet (cf. 2.3). The new variant replaces LowMC which is a relatively young block cipher design with the well-established and standardized Advanced Encryption Standard (AES) block cipher. Thereby, we show that Picnic-style signatures are practically possible by only employing standardized symmetric-key primitives.

Within the upcoming sections, we present the precise research and outcome of these cryptographic aspects of data sharing:

- CCA-Secure (Puncturable) KEMs from Encryption With Non-Negligible Decryption Errors
- An Attack on Some Signatures Schemes Constructed From Five-Pass Identification Schemes
- Banquet: Short and Fast Signatures from AES
- Fine-Grained Forward Secrecy: Allow-List/Deny-List Encryption and Applications
- Updatable Signatures and Message Authentication Codes

## 2.1 CCA-Secure (Puncturable) KEMs from Encryption With Non-Negligible Decryption Errors

Public-key encryption (PKE) schemes or key-encapsulation mechanisms (KEMs) are fundamental cryptographic building blocks to realize secure communication protocols. In particular, PKE is essential for non-interactive end-to-end secure data exchange. There are several known transformations that generically turn weakly secure schemes (e.g., indistinguishability against chosen plaintext attacks) into strongly (i.e., indistinguishability against chosen ciphertext attacks) secure ones. While most of these transformations require the weakly secure scheme to provide perfect correctness, i.e., every well-formed ciphertext can be decrypted, Hofheinz, Hövelmanns, and Kiltz (HHK) [3] have recently shown that variants of the Fujisaki-Okamoto (FO) transform can work with schemes that have negligible correctness error in the (quantum) random oracle model ((Q)ROM). While many recent schemes in the NIST PQC use variants of these transformations, some of their Chosen Plaintext Attack (CPA)-secure versions even have a non-negligible correctness error and so do not satisfy the requirements to apply the techniques of HHK.

In this work, we study the setting of generically transforming PKE schemes with potentially large, i.e., non-negligible, correctness error to ones having negligible correctness error. In an asymptotic setting, this question was studied by Dwork, Naor and Reingold [4]. Our goal is to come up with practically efficient compilers in a concrete setting. First, we show how to generically transform weakly secure deterministic or randomized PKEs into Chosen Ciphertext Attack (CCA)-secure KEMs in the (Q)ROM using variants of the HHK techniques. This applies to essentially all candidates of the NIST PQC based on lattices and codes with non-negligible error. In our extensive analysis, we show that our techniques improve some of the code-based candidates. Second, we apply our techniques to identity-based encryption (IBE) schemes from lattices and codes with (non-)negligible correctness error. Thereby we generically achieve the first post-quantum secure Bloom Filter KEMs which were proposed by Derler et al. [2] and inherently have a non-negligible correctness error. BFKEMs are a building block to construct fully forward-secret zero round-trip time (0-RTT) key-exchange protocols.

**CCA-Secure (Puncturable) KEMs from Encryption with Non-Negligible Decryption Errors.** *Valerio Cini (AIT), Sebastian Ramacher (AIT), Daniel Slamanig (AIT), Christoph Striecks (AIT).* In: Moriai S., Wang H. (eds) Advances in Cryptology – ASIACRYPT 2020. ASIACRYPT 2020. Lecture Notes in Computer Science, vol 12491. Springer, Cham. Open access: https://eprint.iacr.org/2020/1548.

## 2.2 An Attack on Some Signatures Schemes Constructed From Five-Pass Identification Schemes

Many popular signature schemes are constructed by taking an interactive identification scheme and making it non-interactive by using the Fiat-Shamir transformation, a decade old standard technique. While the security of the Fiat-Shamir transformation is well understood for traditional 3-pass identification schemes (an identification scheme consisting of 3 messages in total), an increasing number of proposed signature schemes are instead built from 5-pass identification protocols. In this work, we investigate the concrete security of signature schemes build from 5-pass identification schemes. We show a generic attack that uses the nature of how parallel repetitions are used to boost the soundness of the identification scheme to cryptographic security levels by splitting the attack cost between the different phases of the identification scheme. While our attack reduces the concrete security of schemes, it still has exponential runtime and can be mitigated by increasing the number of internal parallel repetitions of the identification scheme.

We apply our attack to MQDSS, a second-round candidate in the current NIST post-quantum standardization project and show that a forgery for their proposed 128-bit parameter set can be produced with about 2^95 hash function calls. The designers acknowledged our attack and in turn increased the number of internal repetitions by about 40%, following our proposal. However, this change in turn reduced the performance of MQDSS and it did not advance into the third round of the NIST post-quantum standardization project, highlighting the practical impact of this work.

Finally, we generalize the attack and apply it to other schemes from the literature. The parameter sets of these schemes already have been updated to take our attack into account.

**An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes.** *Daniel Kales (TUG), Greg Zaverucha (external).* In: Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings. Open access: https://eprint.iacr.org/2020/837.

## 2.3 Banquet: Short and Fast Signatures from AES

Existing post-quantum signatures can be based on different hardness assumptions such as lattice problems, code-based cryptography, or the hardness of solving multivariate quadratic equation systems. A very conservative choice is to build signatures only from symmetric-key primitives such as block ciphers and hash functions. These constructions include Picnic and SPHINCS+ [20], both candidates in the ongoing NIST PQC project.

Picnic is built using the novel approach of proving knowledge of a block cipher secret key for a given public plaintext-ciphertext pair and the internal complexity of the used block cipher is the main factor in the final size of the signature. Picnic therefore uses LowMC internally, a relatively recent design which is optimized for evaluations in contexts such as the used proof system. LowMC provides performance improvements of up to 5x when compared to using standard primitives such as AES, however as a tradeoff, LowMC has not received the 20 years of combined cryptanalysis that AES has.

In our work, we propose a Picnic-style signature scheme based around AES instead of LowMC. We build on previous work, BBQ [21], and improve on their ideas by proposing a new proof system that works well with the internal structure of the AES Sbox (and the field inversion contained therein). This results in signatures from conservative and standardized primitives that approach Picnic's signature sizes with lower performance or can match Picnic's performance at the cost of larger signatures. In comparison to previous AES-based signatures, we improve on the current state-of-the-art (BBQ) by a factor of more than 2 in signature size and provide an open-source implementation.

**Banquet: Short and Fast Signatures from AES.** *Carsten Baum (external), Cyprien Delpech de Saint Guilhem (external), Daniel Kales (TUG), Emmanuela Orsini (external), Peter Scholl (external), Greg*

*Zaverucha (external).* In: Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I. Open access: https://eprint.iacr.org/2021/068.

## 2.4 Fine-Grained Forward Secrecy: Allow-List/Deny-List Encryption and Applications

Forward secrecy is an important feature for modern cryptographic systems and is widely used in secure messaging such as Signal and WhatsApp as well as in common Internet protocols such as Transport Layer Security (TLS), IPSec, WireGuard or Secure Shell Protocol (SSH). The benefit of forward secrecy is that the damage in case of key-leakage is mitigated. Forward-secret encryption schemes provide security of past ciphertexts even if a secret key leaks, which is interesting in settings where cryptographic keys often reside in memory for quite a long time and could be extracted by an adversary, e.g., in cloud computing. The recent concept of PE [5] provides a versatile generalization of forward-secret encryption: it allows to puncture secret keys with respect to ciphertexts to prevent the future decryption of these ciphertexts.

We introduce the abstraction of allow-list/deny-list encryption schemes and classify different types of PE schemes using this abstraction. Based on our classification, we identify and close a gap in existing work by introducing a novel variant of PE which we dub Dual-Form Puncturable Encryption (DFPE). DFPE significantly enhances and, in particular, generalizes previous variants of PE by allowing an interleaved application of allow- and deny-list operations.

We present a construction of DFPE in prime-order bilinear groups, discuss a direct application of DPFE for enhancing security guarantees within Cloudflare's Geo Key Manager, and show its generic use to construct forward-secret IBE and forward-secure digital signatures.

**Fine-Grained Forward Secrecy: Allow-List/Deny-List Encryption and Applications.** *David Derler (external), Sebastian Ramacher (AIT), Daniel Slamanig (AIT), Christoph Striecks (AIT).* In: Financial Cryptography and Data Security. FC 2021. Lecture Notes in Computer Science, Springer, Cham. 2021 (to appear). Open access: https://eprint.iacr.org/2019/912.

## 2.5 Updatable Signatures and Message Authentication Codes

Cryptographic objects with updating capabilities have been proposed by Bellare, Goldreich and Goldwasser [15] under the umbrella of incremental cryptography. They have recently seen increased interest, motivated by theoretical questions [10] as well as concrete practical motivations [11], [12], [13]. In this work, the form of updatability we are particularly interested in is that primitives are key-updatable and allow to update old cryptographic objects, e.g., signatures or message authentication codes, from the old key to the updated key at the same time without requiring full access to the new key (i.e., only via a so-called update token).

Inspired by the rigorous study of updatable encryption by Lehmann and Tackmann [11] and Boyd et al. [14], we introduce a definitional framework for updatable signatures (USs) and universal message authentication codes (UMACs). We discuss several applications demonstrating that such primitives can be useful in practical applications, especially around key rotation in various domains, as well as serve as building blocks in other cryptographic schemes. We then turn to constructions and our focus is on ones that are secure and practically efficient. In particular, we provide generic constructions from key-homomorphic primitives (signatures and Pseudorandom Functions (PRFs)) as well as direct constructions. This allows us to instantiate these primitives from various assumptions such as Decisional Diffie-Hellman or Computational Diffie-Hellman (latter in bilinear groups), or the Ring Learning With Errors ((R)LWE) and the Short Integer Solution (SIS) assumptions. As an example, we

obtain highly practical US schemes from Boneh-Lynn-Shacham (BLS) signatures or UMAC schemes from the Naor-Pinkas-Reingold PRF.

**Updatable Signatures and Message Authentication Codes.** *Valerio Cini (AIT), Sebastian Ramacher (AIT), Daniel Slamanig (AIT), Christoph Striecks (AIT), Erkan Tairi (external).* In: Garay J.A. (eds) Public-Key Cryptography – PKC 2021. PKC 2021. Lecture Notes in Computer Science, vol 12710. Springer, Cham. 2021. Open access: https://eprint.iacr.org/2021/365.

# 3 T4.2 - Authenticity-preserving and privacy-preserving data analytics

Besides end-to-end secure data exchange, the second cryptographic core component of KRAKEN's data marketplace also includes an analytics service where buyers do not obtain access to the users' plain data, but only to, say, statistical evaluations performed on top of that data. As with the data sharing capabilities, the goal is to ensure that neither the marketplace nor any of the computing nodes that perform the computations have access to the user's plaintext data. Hence, as part of T4.2 we are interested in cryptographic concepts that enable us to build a (potentially distributed) system for computing on encrypted or otherwise protected data. For KRAKEN, we proposed an architecture that builds on secure multi-party computation (cf. D2.4 [24], Figure 1).

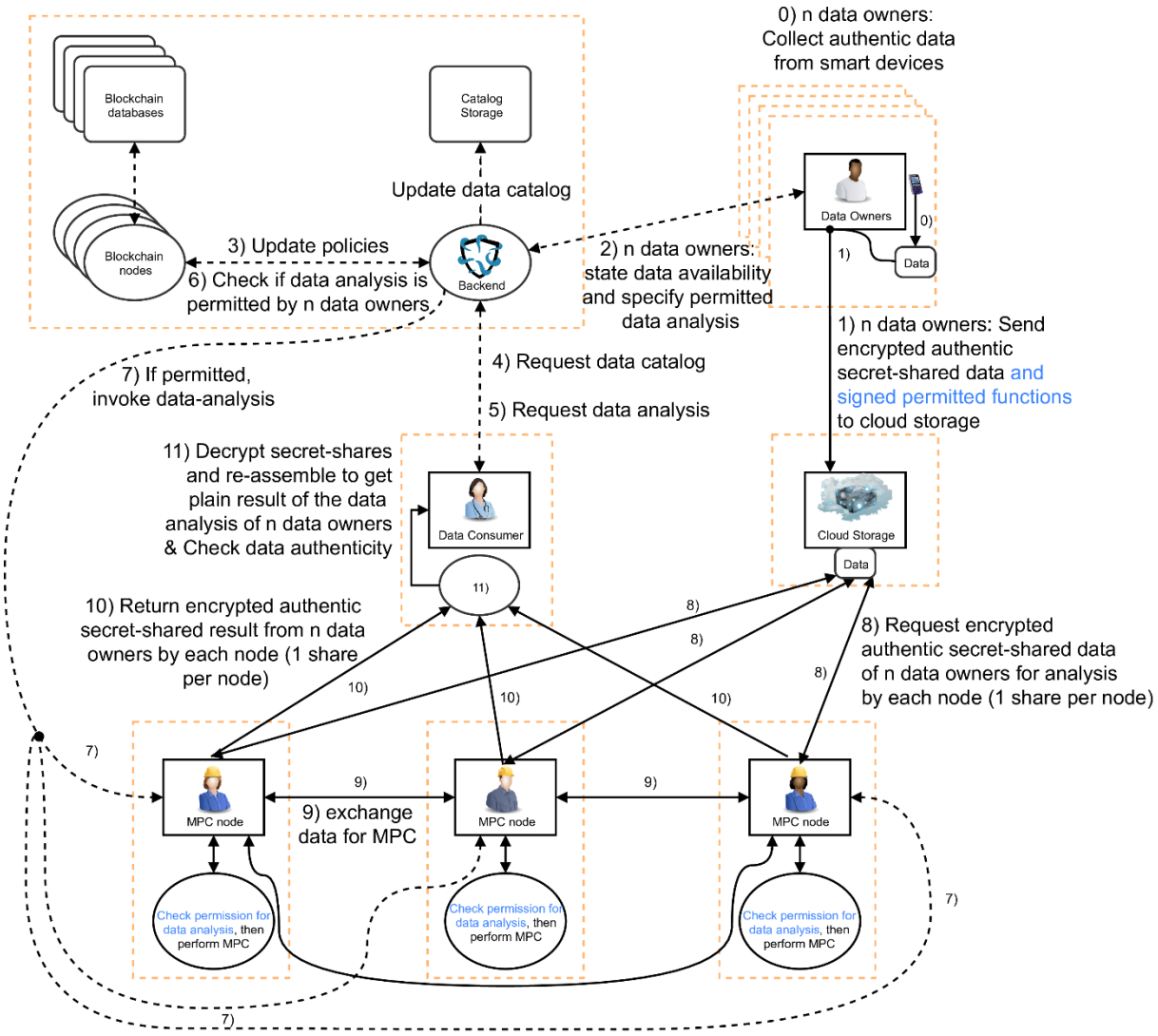


**Figure 1: Architecture for privacy-preserving analytics in a data marketplace.**

The system is composed of the KRAKEN backend which handles user registration, listing of data offerings, and payments. Storage for data is provided by user-defined cloud storage services. Once users join the system, they can upload their data in register in the KRAKEN backend. If a customer buys an analysis on the data, the backend triggers the computation on the Multi-Party Computation (MPC) nodes, which then send the results directly to the consumer. All cryptographic primitives and protocols required for processing data on the nodes in a privacy-preserving way are of interest for this task.

In addition to confidentiality of the processed data, authenticity of data and computation throughout the whole architecture is also a major concern. While MPC protocols already provide a level of authenticity guarantees as long as enough parties perform their computations honestly, these guarantees are not enough for the use in the data marketplace. In particular, the goal of the KRAKEN architecture is to ensure an authenticity chain from the initial set of data to the data buyer. To that end, KRAKEN employs group signatures together with non-interactive zero-knowledge proofs, and in particular succinct variants in the form of zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs), to provide this authenticity chain.

Our first work (Section 3.1) focuses on the architecture to support the privacy-preserving data processing workflow of the KRAKEN platform. Starting from the initial architecture that was designed as part Work Package 2 (cf. D2.4 [24]), we performed a security analysis based on the LINDDUN framework [22]. By performing this analysis, we were able to discover certain risks that were mitigated in an updated version of the architecture.

Regarding the use of zk-SNARKs, note that they honestly generate common reference strings by trusted third parties. As the goal of the architecture is to reduce the required trust in any of the participating parties, we want to avoid the introduction of an additional trusted party. Hence, we investigate variants of zk-SNARKs with subversion-resistance, i.e., even if the common reference string is subverted, the soundness or zero-knowledge properties hold, and with updatability, i.e. the common reference string can be updated such that one can be sure that no single party holds trapdoors that could break soundness or zero-knowledge. We present the results on generic compilers to obtain subversion and updatable zk-SNARKs in Section 0. Thereby we can design a system without relying on a trusted third party to ensure authenticity for all computations and data processed via the KRAKEN marketplace.

Within the upcoming sections, we present the precise research and outcome of these cryptographic aspects of data analysis:

- Privacy-preserving Analytics for Data Markets using MPC
- Lift-and-Shift: Obtaining Simulation Extractable Subversion and Updatable SNARKs

## 3.1 Privacy-preserving Analytics for Data Markets using MPC

*"Data markets have the potential to foster new data-driven applications and help growing data-driven businesses. When building and deploying such markets in practice, regulations such as the European Union's General Data Protection Regulation (GDPR) impose constraints and restrictions on these markets especially when dealing with personal or privacy-sensitive data."* - [17] (this paper). Also in KRAKEN we deal with personal data, and the protection of this personal data is very important from a security as well as a privacy point of view; (1) to keep the users' security and privacy intact and, furthermore, (2) to be GDPR-compliant.

In KRAKEN we leverage Functional Encryption (FE) and Multi-Party Computation (MPC) to enable privacy-preserving data analytics. Users encrypt (FE) or secret-share and then encrypt (MPC) their data before uploading it to an (external) cloud. To ensure the data-origin's authenticity, we leverage Group Signatures. Group signatures have the (nice) property, that users can authenticate their data by signing it and yet they stay anonymous within the group. Only a kind of "opening authority", like a judge, could identify a user, e.g. in a dispute during a lawsuit. On the other hand, if this is an issue, the group's "master key" could be, e.g., thrown away or only used via MPC. A data buyer only gets the analytics' result, yet it is still possible to verify the data-origin's authenticity and if the correct function has been applied. This verification is achieved by leveraging zero-knowledge proofs of knowledge, which is further explained, e.g., in Section 4.3. Moreover, with our solution, the KRAKEN marketplace does not learn about the users' data nor the analytics' result in the MPC case.

*"In this paper, we present a candidate architecture for a privacy-preserving personal data market, relying on cryptographic primitives such as multi-party computation (MPC) capable of performing privacy-preserving computations on the data. Besides specifying the architecture of such a data market, we also present a privacy-risk analysis of the market following the LINDDUN methodology."* - [17] (this paper). Figure 2 gives an overview of KRAKEN's entities and crypto components for the data-analytics-via-MPC case including the concrete choice of cryptographic building blocks and their interaction. Figure 1 gives an overview of KRAKEN's entities and data flows of the MPC case; from data gathering to data-analytic results.

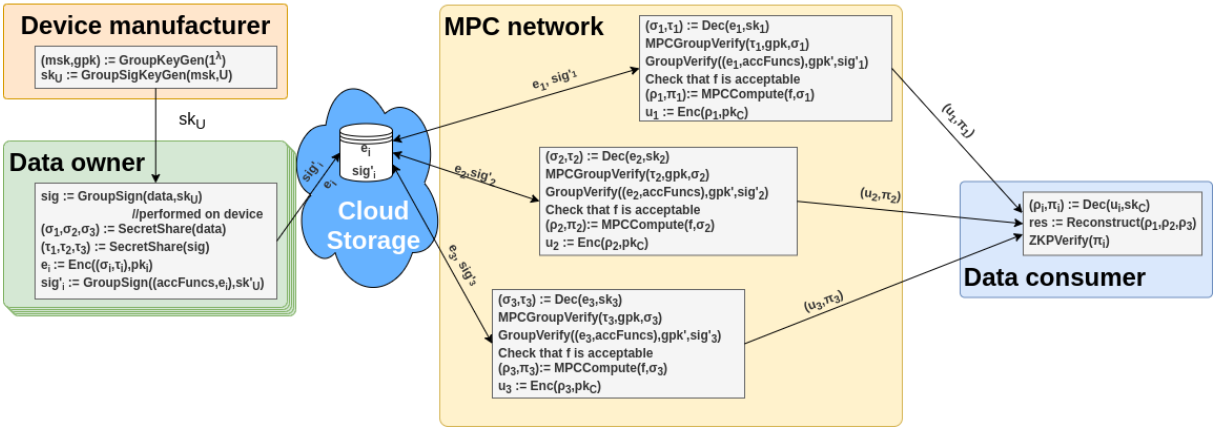


**Figure 2: Overview of KRAKEN's entities and crypto components for the data-analytics-via-MPC case [KKPR].**

**Privacy-Preserving Analytics for Data Markets Using MPC.** *Karl Koch (TUG), Stephan Krenn (AIT), Donato Pellegrino (TX), Sebastian Ramacher (AIT).* In: Friedewald M., Schiffner S., Krenn S. (eds) Privacy and Identity Management. Privacy and Identity 2020. IFIP Advances in Information and Communication Technology, vol 619. Springer, Cham. Open access: https://arxiv.org/abs/2103.03739.

## 3.2 Lift-and-Shift: Obtaining Simulation Extractable Subversion and Updatable SNARKs

Zero-knowledge proofs and in particular succinct non-interactive zero-knowledge proofs (so called zk-SNARKs) are getting increasingly used in real-world applications, with cryptocurrencies being the prime example. Simulation extractability (SE) is a strong security notion for zk-SNARKs which informally ensures non-malleability of proofs. The high importance of this property is underpinned by various attacks against the malleability of cryptographic primitives in the past [6]. Another problematic issue for the practical use of zk-SNARKs is the requirement of a fully trusted setup, as especially for large-scale decentralized applications because finding a trusted party that runs the setup is practically impossible or requires large-scale ceremonies including many different parties to set up the parameters [7]. Quite recently, the study of approaches to relax or even remove the trust in the setup procedure has been initiated [8]. This line of research introduced subversion-resistant und updatable Non-Interactive Zero Knowledges (NIZKs) (and zk-SNARKs). For subversion resistance, one considers subversion soundness, i.e., soundness holds even if the Common Reference String (CRS) is subverted, and subversion zero-knowledge, i.e., zero-knowledge holds even if the CRS is subverted. Note however, that it is impossible for both notions to holds simultaneously. For updatable NIZKs the approach is different. There the idea is that it is possible to update the CRS such that knowledge of trapdoors with respect to an old CRS will not help in breaking soundness or zero-knowledge of the new CRS. So far SE-SNARKs that are subversion-resistant or updatable are only constructed in an ad-hoc manner and no generic techniques are available.

We are interested in generic techniques for constructing updatable and subversion-resistant SE-SNARKs. Therefore, we firstly revisit the only available lifting technique due to Kosba et al. [9] (called COCO) to generically obtain SE-SNARKs. By exploring the design space of many recently proposed SNARK- and succinct transparent argument of knowledge (STARK)-friendly symmetric-key primitives we thereby achieve significant improvements in the prover computation and proof size. Unfortunately, the COCO framework as well as our improved version (called OCOCO) is not compatible with updatable SNARKs. Consequently, we propose a novel generic lifting transformation called LAMASSU. It is built using different underlying ideas compared to COCO (and OCOCO). In contrast, it only requires key-homomorphic signatures (which allow to shift keys) covering well studied schemes such as Schnorr or Elliptic Curve Digital Signature Algorithm (ECDSA). This makes LAMASSU highly interesting, as by using the novel concept of so-called updatable signatures, we can prove that LAMASSU preserves the subversion and in particular updatable properties of the underlying zk-SNARK. This makes LAMASSU the first technique to also generically obtain SE subversion and updatable SNARKs. As its performance compares favorably to OCOCO, LAMASSU is an attractive alternative that in contrast to COCO is only based on well-established cryptographic assumptions.

**Lift-and-Shift: Obtaining Simulation Extractable Subversion and Updatable SNARKs Generically.** *Behzad Abdolmaleki (external), Sebastian Ramacher (AIT), Daniel Slamanig (AIT).* In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). Association for Computing Machinery, New York, NY, USA, 2020. Open access: https://eprint.iacr.org/2020/062.

# 4 T4.3 - Cryptographic aspects of SSI systems

The third component of KRAKEN's cryptographic landscape concerns the cryptographic parts of KRAKEN's self-sovereign identity (SSI) system. As WP3 is mainly focused on SSI, T4.3 is in close collaboration with WP3 and supports with the (research-oriented) cryptographic parts of SSI.

One practical, as well as research, aspect is in the area of the data producers' data management. Imagine a data producer does not want to deal with the KRAKEN marketplace her/himself. Instead, a data producer might want to delegate the rights of the data management to a data union, which assembles data from many producers and then provides this data, e.g., as a bundle via the KRAKEN marketplace to potential data consumers.

Another interesting aspect is in the area of revocation within an SSI system, such as Sovrin [19] and others such as EBSI/eSSIF [28]. Revocation is a relevant concept whenever someone might be first within a certain group, such as an employee, and then, is not part of this group anymore. For revocation within Sovrin, usually the information about created trapdoors need to be destroyed, and techniques such as Multi-Party Computation (MPC) open up an interesting opportunity for improvement. Because within MPC, the generated trapdoors can be generated by all participating parties (usually also called nodes), and then each node has only one share of the trapdoor. Hence, the trapdoors do not need to be destroyed and allow faster revocation processes. And when choosing the respective underlying MPC protocol, it can be ensured that the trapdoor does not leak even if all nodes but one cooperate.

Furthermore, within SSI systems it might be required to prove, e.g., a hash's pre-image in zero knowledge. First, it might seem natural to choose one of the "standard" hash functions, like SHA-256, for such a zero-knowledge proof (ZKP). However, as it turns out, these "standard" hash functions do not perform that well in a ZKP. Thus, this heralds the dawn of a new era: the design and creation of ZKP-friendly hash functions, which, in turn, offer practical performance when an SSI system needs, e.g., a ZKP for a hash's pre-image. Within KRAKEN, this is relevant when we want to perform such a ZKP in KRAKEN's SSI system, e.g. to prove that a user knows indeed the input to a certain identity document (where, for instance, only a hash is shown).

Within the upcoming sections, we present the precise research and outcome of these cryptographic SSI aspects:

- Short-Lived Forward-Secure Delegation for TLS
- Multi-Party Revocation in Sovrin: Performance through Distributed Trust
- Poseidon: A New Hash Function for Zero-Knowledge Proof Systems

## 4.1 Short-Lived Forward-Secure Delegation for TLS

Delegations are an important concept in many trust management systems, enabling more flexible authorization mechanisms than static access control. Delegations are also an integral part of many real-world processes in government and industry, so supporting delegations is crucial for systems used to digitalize those processes. One simple example for a delegation in the context of KRAKEN is if the subject of some data-set wants to enable another entity to manage or share these data. Doing this on the KRAKEN marketplace requires that the other entity (delegate) can use an SSI credential to act on behalf of the delegator.

When a delegate acts on behalf of a delegator, they have to authenticate themselves as the delegator to access some restricted resources. In some use cases this can be realized by issuing a credential to the delegate which authorizes her/him to represent the delegator – requiring modifications to the VC verification logic to support those special credentials. Other use cases require that the delegate has access to the secret key of the delegator's Decentralized Identifier (DID), which represents a security issue. To curb this problem, multiple workarounds exist to realize a delegation of the authentication.

In this paper, we present a solution that works without authorization-credentials, renders key sharing unnecessary and reduces the need for workarounds. By adapting identity-based signatures to this setting, our solution offers short-lived delegations. Additionally, by enabling forward-security, existing delegations remain valid even if the delegator's secret key leaks. To demonstrate the scheme's feasibility, we provide an implementation of the scheme. We furthermore show the scheme's versatility by discussing an integration into a TLS stack. We also evaluate the performance of the scheme's implementation, concluding that an efficient implementation incurs less overhead than a typical network round trip.

**Short-Lived Forward-Secure Delegation for TLS.** *Lukas Alber (TUG), Stefan More (TUG), Sebastian Ramacher (AIT).* In CCSW'20: Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop, Virtual, November 2020. Open access: https://arxiv.org/abs/2009.02137.

## 4.2 Multi-Party Revocation in Sovrin: Performance through Distributed Trust

Cryptographic accumulators are a common building block in identity systems, e.g., to accumulate all allowed identifiers into a central value called the *accumulator*. Parties can then prove that their identity is included in this accumulator using zero-knowledge techniques to show that they indeed belong to some specific group.

Cryptographic accumulators providing constant-size accumulation values are traditionally built using trapdoor functions, such as ones based on RSA or bilinear pairings. However, these trapdoors have some practical considerations that must be kept in mind when used. First, the trapdoor value used during the initial setup must be destroyed and not be known to any party after that point, otherwise the security of the system is not guaranteed. Second, without the knowledge of the secret trapdoor, many operations in the accumulator algorithms are much more expensive to compute. This puts some limits on the size of the sets that are accumulated in practice, where operations on large sets can take hours.

To fix both issues, we propose using our Multi-Party Linear-Secret-Shared Accumulators. They use multiple independent parties to generate the trapdoor secret in a secret-shared form, solving the issue of requiring a trusted party to set up the public parameters. Even further, instead of forgetting the secret trapdoor information, the parties can work together in the online phase to compute operations on the accumulator using the secret-shared trapdoor information from the setup phase. This allows the accumulation of large sets while still offering practical performance.

**Multi-Party Revocation in Sovrin: Performance through Distributed Trust.** *Lukas Helminger (TUG), Daniel Kales (TUG), Sebastian Ramacher (AIT), Roman Walch (TUG).* In: Topics in Cryptology - CT-RSA 2021 - The Cryptographers' Track at the RSA Conference 2021, San Francisco, CA, USA, May 17-20, 2021, Proceedings. Open access: https://eprint.iacr.org/2020/724.

## 4.3 Poseidon: A New Hash Function for Zero-Knowledge Proof Systems

In the KRAKEN architecture, which is also envisioned by the paper [17] in T4.2 (Section 3.1), data consumers only get the analysis result, and yet they are able to verify the data-origin's authenticity. Furthermore, they also want to verify if the correct function on the data has been applied. For the verification of both data-origin's authenticity and the correct function, among other things, zero-knowledge proofs of knowledge (ZK-PoK) are leveraged, specifically succinct non-interactive arguments of knowledge (SNARKs). Another use case for ZK-PoKs is the proof of the knowledge of a hash's preimage.

*"A zero-knowledge proof of knowledge (ZK-PoK) is a two party protocol between a prover and a verifier, which achieves two intuitively contradictory goals: it allows the prover to convince the verifier that she knows a secret piece of information, while at the same time revealing no further information than what*

*is already revealed by the claim itself."* - [17] Thus, e.g., for the hash's preimage, we are able to prove the knowledge of the preimage without actually showing it to the verifier. The verifier only gets the hash and the ZK proof. The proof of a hash's preimage is used, e.g., for identity proofs based on an identity assertion from a legal authority [18]. Whereas "traditional" standardized hash functions, such as SHA-256, are very efficient for creating a hash in a "traditional" setting, those hash functions are not well suited for, e.g., a ZK proof of a hash's preimage. This new requirement heralds the dawn of a new era in (modern/current) cryptography: ZK-friendly hash functions. Or as also said by this paper: *"The area of practical computational integrity proof systems, like SNARKs, STARKs, Bulletproofs, is seeing a very dynamic development with several constructions having appeared recently with improved properties and relaxed setup requirements. Many use cases of such systems involve, often as their most expensive part, proving the knowledge of a preimage under a certain cryptographic hash function, which is expressed as a circuit over a large prime field. A notable example is a zero-knowledge proof of coin ownership in the Zcash cryptocurrency, where the inadequacy of the SHA-256 hash function for such a circuit caused a huge computational penalty."* [16].

*"In this paper, we present a modular framework and concrete instances of cryptographic hash functions which work natively with GF(p) objects. Our hash function Poseidon uses up to 8x fewer constraints per message bit than Pedersen Hash. Our construction is not only expressed compactly as a circuit but can also be tailored for various proof systems using specially crafted polynomials, thus bringing another boost in performance. We demonstrate this by implementing a 1-out-of-a-billion membership proof with Merkle trees in less than a second by using Bulletproofs."* - [16] (this paper). Furthermore, our developed ZK-friendly hash function, Poseidon, is used in a proposal for a modern privacy-preserving eID and self-sovereign identity system. This proposal is ongoing research and part of our future work (cf. Section 5.1).

**Poseidon: A New Hash Function for Zero-Knowledge Proof Systems**. *Lorenzo Grassi (external), Dmitry Khovratovich (external), Christian Rechberger (TUG), Arnab Roy (external), Markus Schofnegger (TUG)*. In: 30th USENIX Security Symposium (USENIX Security 2021). Open access: https://eprint.iacr.org/2019/458.

# 5 Conclusion

Within T4.1, T4.2, and T4.3 we worked on the design- and research-oriented part of KRAKEN's cryptographic landscape. T4.1 provided design and research in the area of end-to-end-secure data sharing; between, e.g., a data producer and a data consumer via a marketplace (like the one of KRAKEN). T4.2 provided design and research in the area of privacy-preserving as well as authenticity-preserving data analytics, of, e.g., many data producers for a (dedicated) data consumer, such that the consumer gets only the analysis result, and all that while the (KRAKEN) marketplace does not learn either the input data nor the result. T4.3 provided research and enhancement opportunities in the area of (KRAKEN's) cryptographic aspects of SSI.

## 5.1 Ongoing Research & Future Work

The data marketplace architecture opens up a wide range of research opportunities in multiple directions: ensuring authenticity of the (processed) data in each step of the data flow requires compatible choices of cryptographic schemes to be efficient. While we can build our architecture with SNARKs and NIZKs for generic statements, the nature of the involved statements can render these proofs expensive. When we instantiate the involved fields, groups, etc. compatible, i.e. as it was done with the Jubjub curve on top of BLS12-381 based SNARKs [27], we expect to receive better performance figures. Furthermore, we have so far mostly investigated an MPC-based instantiation of the data marketplace. In a next step, also authenticity- and privacy-preserving instantiations based on functional encryption are of interest.

Also, the deployment of a self-sovereign identity (SSI) system as part KRAKEN's user management, leads to new research opportunities. Ongoing work focuses on a privacy-preserving eID and SSI system. In this area we want to increase the privacy of users during identity assertions towards a service provider. The main idea is to (1) have the same "quality" of the identity assertion as it would come directly from a legal entity, while (2) being able to show only the attributes really needed by the corresponding service provider. Furthermore, we want to reduce the availability of any other potentially privacy risks in SSI systems. For example, if the issuer is known to a verification or service provider, hidden attributes such as state of residence may be leaked via the issuer if certain issuers are only used for residents for certain state, district, and so on. On top of that, we are interested in improving the performance of all parts of an SSI system by employing novel primitives such as Poseidon within zero-knowledge proofs.

# 6 Bibliography & References

[1] https://csrc.nist.gov/projects/post-quantum-cryptography/ (accessed on July 2021).

[2] David Derler, Tibor Jager, Daniel Slamanig, Christoph Striecks: Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange. EUROCRYPT 2018.

[3] Dennis Hofheinz, Kathrin Hövelmanns, Eike Kultz: A Modular Analysis of the Fujisaki-Okamoto Transformation. TCC 2017.

[4] Cynthia Dwork, Moni Naor, Omer Reingold: Immunizing Encryption Schemes from Decryption Errors. EUROCRYPT 2004.

[5] Matthew D. Green, Ian Miers: Forward Secure Asynchronous Messaging from Puncturable Encryption. IEEE S&P 2015.

[6] https://www.coindesk.com/study-finds-mt-gox-lost-386-bitcoins-due-transaction-malleability (accessed on July 2021).

[7] Sean Bowe, Ariel Gabizon, Matthew D. Green: A Multi-Party Protocol for Constructing the Public Parameters of the Pinoccio zk-SNARK. FC 2018 Workshops.

[8] Mihir Bellare, Georg Fuchsbauer, Alessandra Scaufro: NIZKs with an untrusted CRS: Security in the face of parameter subversion. ASIACRYPT 2016

[9] Ahmed Kosba, Zhichao Zhao, Andrew Miller, Yi Qian, Hubert Chan, Charalampos Papamanthou, Rafael Pass, Abhi Sehlat, Elaine Shi: COCO: A Framework for Building Composable Zero-Knowledge Proofs. ePrint 2015/1093

[10] Prabhanjan Ananth, Aloni Cohen, Abhishek Jain: Cryptography with Updates. EUROCRYPT 2017

[11] Anja Lehmann, Björn Tackmann: Updatable Encryption with Post-Compromise Security. EUROCRYPT 2018

[12] Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, Ian Miers: Updatable and Universal Common Reference Strings with Applications to zk-SNARKs.

[13] Michael Klooß, Anja Lehmann, Andy Rupp: (R)CCA Secure Updatable Encryption with Integrity Protection. EUROCRYPT 2019

[14] Colin Boyd, Gareth T. Davies, Kristian Gjøsteen, Yao Jiang: Fast and Secure Updatable Encryption. CRYPTO 2020

[15] Mihir Bellare, Oded Goldreich, Shafi Goldwasser: Incremental Cryptography: The Case of Hashing and Signing. CRYPTO 1994

[16] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, Markus Schofnegger: Poseidon: A new hash function for zero-knowledge proof systems. 30th USENIX Security Symposium, 2021.

[17] Karl Koch, Stephan Krenn, Donato Pellegrino, Sebastian Ramacher: Privacy-preserving Analytics for Data Markets using MPC. IFIP International Summer School on Privacy and Identity Management, 2020.

[18] Andreas Abraham, Felix Hörandner, Olamide Omolola, Sebastian Ramacher: Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems. International Conference on Information and Communications Security (ICICS), 2019.

[19] https://sovrin.org/ (accessed on July 2021).

[20] Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, Peter Schwabe: The SPHINCS+ Signature Framework. CCS 2019

[21] Cyprien Delpech de Saint Guilhem, Lauren De Meyer, Emmanuela Orsini, Nigel P. Smart: BBQ: Using AES in Picnic Signatures. SAC 2019

[22] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, Wouter Joosen: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir. Eng. 16(1): 3-32 (2011)

[23] KRAKEN Consortium: D2.2 Intermediate KRAKEN architecture. 2020

[24] KRAKEN Consortium: D2.4 KRAKEN intermediate technical design. 2020

[25] KRAKEN Consortium: D5.1 Initial Pilot Marketplaces User Stories. 2020

[26] KRAKEN Consortium: D3.1 Self sovereign identity solution. First Release. 2021

[27] https://z.cash/technology/jubjub/ (accessed on July 2021)

[28] https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/1.3.2.+Data+modelling+ESSIF+v2 (accessed on July 2021)


Atos

FONDAZIONE BRUNO KESSLER

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

sic

LYNKEUS
STRATEGY CONSULTING | BLOCKCHAIN & SMART CONTRACTS | DATA ANALYTICS

XLAB

TX

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

IAIK TU Graz

InfoCert
TINEXTA GROUP

@KrakenH2020

Kraken H2020

**www.krakenh2020.eu**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871473