Research Statement

Jonas von der Heyden

My research is concerned with the application of cryptography to real-world use cases. Thanks to the rapid development in both theoretical and applied cryptography, techniques that were considered to be of purely theoretical interest a decade ago are now at the threshold of practical feasibility or beyond. At the same time, there has only been a muted adoption of advanced cryptographic techniques such as multi-party computation (MPC) or fully homomorphic encryption (FHE) "in the wild". I believe that in order to realize the untapped potential of these primitives, we need to assume an interdisciplinary lens. Instead of thinking in cryptographic primitives, we should, once in a while, start with a problem from another discipline (e.g. electrical engineering or history) and investigate whether it can be solved by means from our cryptographic toolkit. By shifting my perspective to that of the problem domain—or, ideally, of the end user—I aim to unlock the power of advanced cryptography for impact in the real world.

Past and current research

The main thrust of my doctoral dissertation is the design and implementation of advanced cryptographic protocols for applications involving resource-constrained (IoT) devices, such as passports and smart meters. Among others, my past research includes the following:

Post-quantum authentication of passports The *Extended Access Control* (EAC) protocol is a cryptographic standard mandated by ICAO for the authentication of passports and the protection of sensitive data such as fingerprints. The protocol assumes the hardness of the discrete log, and since passports are typically valid for 10 years, the adoption of post-quantum secure primitives is an urgent objective. In our work [FvdHM+23], we show how to replace the Diffie-Hellman key exchange with post-quantum secure KEMs while maintaining compatibility with the standard. We also give an efficient implementation of the protocol for passport-embedded smart cards, showing the practical feasibility of lattice-based KEMs in real-world applications. In this work, my contributions include the design of the novel protocol, contributions to the implementation, and the authoring of the majority of the manuscript.

Privacy-preserving smart grids Smart grids optimize our energy distribution, and help to alleviate climate change by allowing for the efficient integration of renewables into the electricity grid. Unfortunately they also require fine-grained usage measurements, which leak sensitive private information such as household occupancy, daily routine and even which movies are being watched. In our work [vdHSB+25] we use MPC to implement one of the most complex algorithms used in smart grids, *power flow analysis*, in a privacy-preserving manner such that no household has to reveal sensitive information. In the implementation, we overcome two main challenges. Firstly, we give an efficient MPC implementation for resource-constrained smart meters. Secondly, we provide optimizations that reduce the number of required communication rounds and thereby mitigate the effects of high-latency connections between smart meters. My contributions include the design and implementation of the entire privacy-preserving MPC solution and the authoring of all cryptography-related sections of the paper.

Revisiting rerandomizable garbling schemes Motivated by our experiences in the smart grid project, we explore techniques that ease the adoption of advanced MPC protocols in real-world settings, namely outsourced MPC (addressing performance constraints) with constant round complexity (addressing

network latency). The YOSO-like MPC protocol SCALES [AHKP22], which is based on rerandomizable garbling schemes (RGS), offers outsourcing under a dishonest majority and with constant-round complexity. Unfortunately, due to its use of BHHO [BHHO08] as a building block, it is extremely inefficient. In our work (accepted at Crypto '25), we replace BHHO by a novel key-and-message homomorphic encryption (KMHE) scheme and improve space and runtime complexity of RGS by four to five orders of magnitude, making SCALES practically feasible for simple circuits. Moreover, we are currently working on a lattice-based RGS implementation. My primary contributions include participating in the ideation of the novel KMHE scheme, validating security proofs, conducting performance benchmarks, and authoring a comprehensive technical overview.

Future objectives

In my future research, I plan to continue working on the utilization of advanced cryptography to solve real-world and interdisciplinary problems. Among others, this entails finding innovative solutions to mitigate limitations around high-latency networks and resource-constrained devices, e.g. on IoT devices. Potential projects include:

Privacy-preserving decentralized control systems for smart grids Decentralized control for smart grids [KHW+25] enables a network of prosumers to manage their electricity grid in a distributed manner without centralized coordination. Besides the somewhat intangible benefit of increased independence from a grid operator, decentralized control also provides better resilience and allows for cheaper energy due to eligibility for take-or-pay tariffs. As in smart grids with centralized control, exchanging fine-grained usage measurements in the clear would reveal sensitive information. Therefore, implementing decentralized control in a privacy-preserving manner is an important research problem.

Privacy-preserving learning on IoT devices Wearables and other IoT devices often use and train machine learning models. While privacy-preserving neural networks are mostly not practical for use on resource-constrained devices, there exist somewhat efficient privacy-preserving solutions for learning problems such as k-means, logistic- and linear regression. Moreover, simplified models with targeted privacy mechanisms might be a practical workaround to deal with limitations of IoT devices. For example, Bos et al. [BCIV17] show that privacy-preserving forecasting based on the group method of data handling can be efficient enough for use on smart meters. Considering the sensitivity of the information generated by (potentially health-related) wearables, efficient privacy-preserving learning algorithms on resource-constrained IoT devices with intermittent connectivity are an important research problem.

Study of historical ciphers While virtually all historical encryption schemes, such as homophonic substitution ciphers, are considered to be broken, the actual decryption of historical secret letters remains non-trivial. This is mostly because we do not have enough encrypted material to extract sufficient statistical information about the ciphertext, but it might also be due to the use of codes ("nomenclatures") or encryption errors. Therefore, interdisciplinary cooperation is essential: cryptographers contribute semi-automated tools for cryptanalysis, while historians provide the necessary contextual knowledge and proficiency in historic languages to aid decryption. I supervised the bachelor theses of three computer science students who, in collaboration with history researchers at the University of Wuppertal, pursued this approach, leading to the decryption of a Renaissance-era letter from Cosimo de' Medici to Francesco Sforza. Decipherments of such historical secret letters reveal diplomatic secrets of the medieval and Renaissance periods, offering a glimpse into the private correspondence of important historic figures and prompting reassessments in historical research.

Censorship-resistance via YOSO ("you only speak once") protocols Most technological solutions to protect privacy against nation-state adversaries (such as E2EE instant-messaging) are run by a centralized entity (e.g. the Signal foundation) and could be disabled by a dictator who corrupts the entity, or simply blocks its IP-address(es). To protect against this threat, mechanisms of censorship-resistance are required. Firstly, the application code needs to be open-source. Secondly, we need

techniques to enable unblockable (potentially P2P) communication based on weak assumptions (e.g. continued existence of the internet). In YOSO protocols, participants appear spontaneously, speak only once and then disappear, hence blocking their IP-address is futile. A line of research ([GHK+21, AHKP22], our submission to Crypto '25) has shown that YOSO-MPC is practical for simple circuits. Another feature that makes YOSO attractive for censorship-resistance is that it does not require pre-existing secure point-to-point channels. Therefore it is natural to ask: Is it practically feasible to run censorship-resistant privacy-preserving applications by replacing a centralized server with ephemeral participants using YOSO-like protocols?

References

[AHKP22] Anasuya Acharya, Carmit Hazay, Vladimir Kolesnikov, and Manoj Prabhakaran. SCALES - MPC with small clients and larger ephemeral servers. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography - 20th International Conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, Proceedings, Part II*, volume 13748 of *Lecture Notes in Computer Science*, pages 502–531. Springer, 2022.

[BCIV17] Joppe W. Bos, Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling. In Marc Joye and Abderrahmane Nitaj, editors, *Progress in Cryptology - AFRICACRYPT 2017 - 9th International Conference on Cryptology in Africa, Dakar, Senegal, May 24-26, 2017, Proceedings*, volume 10239 of *Lecture Notes in Computer Science*, pages 184–201, 2017.

[BHHO08] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In David A. Wagner, editor, *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 108–125. Springer, 2008.

[FvdHM+23] Marc Fischlin, Jonas von der Heyden, Marian Margraf, Frank Morgner, Andreas Wallner, and Holger Bock. Post-quantum security for the extended access control protocol. In Felix Günther and Julia Hesse, editors, *Security Standardisation Research - 8th International Conference, SSR 2023, Lyon, France, April 22-23, 2023, Proceedings*, volume 13895 of *Lecture Notes in Computer Science*, pages 22–52. Springer, 2023.

[GHK+21] Craig Gentry, Shai Halevi, Hugo Krawczyk, Bernardo Magri, Jesper Buus Nielsen, Tal Rabin, and Sophia Yakoubov. YOSO: you only speak once - secure MPC with stateless ephemeral roles. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II*, volume 12826 of *Lecture Notes in Computer Science*, pages 64–93. Springer, 2021.

[KHW+25] Maximilian Kilthau, Vincent Henkel, Lukas Peter Wagner, Felix Gehlhoff, and Alexander Fay. A decentralized optimization approach for scalable agent-based energy dispatch and congestion management. *Applied Energy*, 377:124606, 2025.

[vdHSB+25] Jonas von der Heyden, Nils Schlüter, Philipp Binfet, Martin Asman, Markus Zdrallek, Tibor Jager, and Moritz Schulze Darup. Privacy-preserving power flow analysis via secure multi-party computation. *IEEE Trans. Smart Grid*, 16(1):344–355, 2025.