Sebastian Ramacher
Senior Scientist
Security & Communication Technologies

Organisationszugehörigkeiten

Senior Scientist
Security & Communication Technologies
1 Jan. 2024 → present

Graz University of Technology
Österreich
1 März 2015 → 31 Juli 2019

Publikationen

QCI-CAT: Making Austria Quantum Secure
Ramacher, S. (Vortragende:r), Kos, M. & Hübel, H., 5 Dez. 2024. 1 S.

One Tree to Rule Them All: Optimizing GGM Trees and OWFs for Post-Quantum Signatures
Baum, C., Beullens, W., Mukherjee, S. (Autor:in und Vortragende:r), Orsini, E., Ramacher, S., Rechberger, C., Roy, L. & Scholl, P., Dez. 2024, *Advances in Cryptology – ASIACRYPT 2024: 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9–13, 2024, Proceedings, Part I.* Chung, K.-M. & Sasaki, Y. (Hrsg.). Springer, Vol. 15484. S. 463–493 (ASIACRYPT: International Conference on the Theory and Application of Cryptology and Information Security).

QKD4GOV: Sicherung von Behördendaten mittels quanten-sicherer Kryptographie
Hübel, H. (Autor:in und Vortragende:r), Kos, M., Ramacher, S. & Kutschera, F., 11 Nov. 2024. 1 S.

Circuit-Succinct Universally-Composable NIZKs with Updatable CRS
Abdolmaleki, B., Glaeser, N. (Autor:in und Vortragende:r), Ramacher, S. & Slamanig, D., 2024, *2024 IEEE 37th Computer Security Foundations Symposium (CSF).* S. 527 - 542

(Inner-Product) Functional Encryption with Updatable Ciphertexts
Cini, V., Ramacher, S., Slamanig, D., Striecks, C. & Tairi, E., 2024, in: Journal of Cryptology. 37, 1, S. 1-32 40 S., 8.

OPRFs from Isogenies: Designs and Analysis
Heimberger, L. (Autor:in und Vortragende:r), Hennerbichler, T., Meisingseth, F., Ramacher, S. & Rechberger, C., 2024, *ASIA CCS '24: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security.* S. 575 - 588

Pure Rust implementation of the post-quantum secure digital signature scheme FAEST
Ramacher, S. (Entwickler:in), 2024

QCI-CAT: Making Austria Quantum Secure
Kos, M. (Vortragende:r), Ramacher, S. & Hübel, H., 2024. 1 S.

Key Management Systems for Large-Scale Quantum Key Distribution Networks
James, P., Laschet, S., Ramacher, S. (Vortragende:r) & Torresetti, L., 29 Aug. 2023, *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security.* S. 1-9 9 S. 126. (ACM International Conference Proceeding Series).

Quantum-resistant End-to-End Secure Messaging and Email Communication
Döberl, C., Eibner, W., Gärtner, S., Kos, M., Kutschera, F. & Ramacher, S. (Vortragende:r), 29 Aug. 2023, *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security.* S. 1-8 8 S. 125. (ACM International Conference Proceeding Series).

Muckle+: End-to-End Hybrid Authenticated Key Exchanges
Bruckner, S. P., Ramacher, S. & Striecks, C. (Vortragende:r), Aug. 2023, *PQCrypto 2023: Post-Quantum Cryptography.* Johansson, T. & Smith-Tone, D. (Hrsg.). 1 Aufl. Springer, S. 601–633 (Lecture Notes in Computer Science; Band 14154).

Outsourced Computations Maintaining Confidentiality and Authenticity
Krenn, S., Lorünser, T., Ramacher, S. & Wohner, F., 28 Apr. 2023, in: ERCIM News. 133, S. 17-18 2 S.

FAEST reference implementation
Ramacher, S. (Entwickler:in) & Mukherjee, S. (Entwickler:in), 2023

Optimizing 0-RTT Key Exchange with Full Forward Security
Göth, C., Ramacher, S. (Vortragende:r), Slamanig, D., Striecks, C., Tairi, E. & Zikulnig, A., 2023, *CCSW '23: Proceedings of the 2023 on Cloud Computing Security Workshop.* Regazzoni, F. & Fournaris, A. (Hrsg.). S. 55-68

Extending Expressive Access Policies with Privacy Features
More, S., Ramacher, S., Alber, L. & Herzl, M., 2022, *2022 IEEE 21th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) .* S. 1-9

KRAKEN: A Privacy-Preserving Data Market for Authentic Data
Koch, K., Krenn, S., Marc, T., More, S. & Ramacher, S. (Vortragende:r), 2022, *DE '22: Proceedings of the 1st International Workshop on Data Economy.* Laoutaris, N. & Mellia, M. (Hrsg.). S. 15-20 6 S.

KRAKEN: a secure, trusted, regulatory compliance and privacy-preserving data sharing platform
Gabrielli, S., Krenn, S., Pellegrino, D., Perez Braun, J. C., Pérez Berganza, P., Ramacher, S. & Vandevelde, W., 2022, *Data Spaces.* Curry, E., Scerri, S. & Tuikka, T. (Hrsg.). Springer, S. 107-130 24 S.

Fine-Grained Forward Secrecy: Allow-List/Deny-List Encryption and Applications
Derler, D., Ramacher, S. (Vortragende:r), Slamanig, D. & Striecks, C., 2021, *25th International Conference on Financial Cryptography and Data Security - FC 2021.* Springer, S. 499-519 21 S.

Issuer-Hiding Attribute-Based Credentials
Bobolz, J., Eidens, F., Krenn, S. (Vortragende:r), Ramacher, S. & Samelin, K., 2021, *20th International Conference on Cryptology And Network Security - CANS 2021.* Springer, S. 158-178 21 S.

KRAKEN - Brokerage and Market Platform for Personal data
Ramacher, S., Abraham, A. & Perez Braun, J. C., 2021, in: ERCIM News. 126, S. 16-17 2 S.

Multi-Party Revocation in Sovrin: Performance through Distributed Trust
Helminger, L., Kales, D., Ramacher, S. (Vortragende:r) & Walch, R., 2021, *CT-RSA 2021: Topics in Cryptology - CT-RSA 2021.* Springer, S. 527-551 25 S.

Privacy-Preserving Analytics for Data Markets Using MPC
Koch, K., Krenn, S., Pellegrino, D. & Ramacher, S., 2021, *IFIP Advances in Information and Communication Technology.* Springer Science and Business Media Deutschland GmbH, S. 226-246 21 S. (IFIP Advances in Information and Communication Technology; Band 619 IFIP).

Privacy-Preserving Authenticated Key Exchange: Stronger Privacy and Generic Constructions
Ramacher, S., Slamanig, D. & Weninger, A. (Vortragende:r), 2021, *26th European Symposium on Research in Computer Security - ESORICS 2021.* Springer, S. 676-696 21 S.

Privacy-Preserving eID Derivation to Self-Sovereign Identity Systems with Offline Revocation
Abraham, A., Koch, K., More, S., Ramacher, S. (Vortragende:r) & Stopar, M., 2021, *20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021, Shenyang, China, October 20-22, 2021.* S. 506-513 8 S.

Steering Drivers of Change: Maximising Benefits of Trustworthy IoT
Veledar, O. (Vortragende:r), Armengaud, E., Happ Botler, L., Damjanovic-Behrendt, V., Derler, C., Jaksic, S., Krammer, L., Lettner, C., Macher, G., Merksteiner, S., Martin, A. J., Matschnig, M., Priller, P., Ramacher, S., Römer, K. U., Schmittner, C., Tiefnig, C., Vallant, H., Weiskirchner, H. & Drobics, M., 2021, *28th European Conference, EuroSPI 2021, Krems, Austria, September 1-3, 2021, Proceedings.* Springer Nature, 11 S.

Updatable Signatures and Message Authentication Codes
Cini, V. (Vortragende:r), Ramacher, S., Slamanig, D., Striecks, C. & Tairi, E., 2021, *24th International Conference on Practice and Theory of Public-Key Cryptography - PKC 2021.* Springer, S. 691-723 33 S.

CCA Secure (Puncturable) KEMs from Encryption With Non-Negligible Decryption Errors
Cini, V. (Vortragende:r), Ramacher, S., Slamanig, D. & Striecks, C., 2020, *26th Annual International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2020.* Springer, S. 1-32 32 S.

Efficient FPGA Implementations of LowMC and Picnic
Kales, D., Ramacher, S., Rechberger, C., Walch, R. (Vortragende:r) & Werner, M., 2020, *Topics in Cryptology - CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24-28, 2020, Proceedings.* Springer, S. 417-441 25 S.

Lift-and-Shift: Obtaining Simulation Extractable Subversion and Updatable SNARKs Generically
Abdolmaleki, B. (Vortragende:r), Ramacher, S. & Slamanig, D., 2020, *27th ACM Conference on Computer and Communications Security - ACM CCS 2020.* S. 1987-2005 19 S.

Privacy-preserving Analytics for Data Merkets using MPC
Koch, K., Krenn, S., Pellegrino, D. (Vortragende:r) & Ramacher, S., 2020, *Privacy and Identity Management. Privacy and Identity 2020. IFIP Advances in Information and Communication Technology.* Springer, S. 226-246 21 S.

Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems
Abraham, A. (Vortragende:r), Hörandner, F., Omolola, O. & Ramacher, S., 2020, *Information and Communications Security. ICICS 2019.* Zhou , J., Luo , X., Shen , Q. & Xu , Z. (Hrsg.). Springer, Vol. 11999. S. 307-323 16 S. (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)).

Selective end-to-end data-sharing in the cloud
Hörandner, F., Ramacher, S. & Roth, S., 2020, in: Journal of Banking and Financial Technology. 4, S. 139-157 19 S.

Short-lived Forward-Secure Delegation for TLS
Ramacher, S. (Vortragende:r), Alber, L. & More, S., 2020, *Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop.* S. 119-132 14 S.

Feistel Structures for MPC, and More
Albrecht, M. R., Grassi, L. (Vortragende:r), Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A. & Schofnegger, M., 2019, *Computer Security – ESORICS 2019.* Vol. 11736. S. 151–171 20 S. (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)).

Aktivitäten

SECPID: 6th Workshop on Security, Privacy, and Identity Management in the Cloud (Veranstaltung)
Krenn, S. (International Programme Committee - Member), Ramacher, S. (International Programme Committee - Co-Chair) & Kos, M. (Conference Committee - Member)

30 Apr. 2025 → 14 Aug. 2025

QCI-CAT Project Overview
Ramacher, S. (Vortragender)
5 Dez. 2024

International Conference on Quantum Communications, Networking, and Computing (QCNC 2025) (Veranstaltung)
Ramacher, S. (International Programme Committee - Member)
1 Dez. 2024 → 20 Jan. 2025

28th IACR International Conference on Practice and Theory of Public-Key Cryptography - PKC 2025 (Veranstaltung)
Ramacher, S. (International Programme Committee - Member)
16 Okt. 2024 → 5 Feb. 2025

Coordinate the first deployment of national EuroQCI projects and prepare the large scale QKD testing and certification infrastructure
Ramacher, S. (Vortragender)
4 Sept. 2024

QCI-CAT Project Overview
Ramacher, S. (Vortragender)
4 Sept. 2024

Hybrid post quantum cryptography and quantum key distribution, applications and national test beds
Ramacher, S. (Vortragender, eingeladen)
4 Juni 2024

International Conference on Quantum Communications, Networking, and Computing (QCNC 2024) (Veranstaltung)
Ramacher, S. (International Programme Committee - Member)
6 Apr. 2024 → 8 Mai 2024

Hybrid Cryptographic Protocols and Applications
Ramacher, S. (Vortragender)
27 Feb. 2024

Coordinate the first deployment of national EuroQCI projects and prepare the large-scale QKD testing and certification infrastructure
Ramacher, S. (Vortragender)
26 Feb. 2024

QCI-CAT Project Overview
Ramacher, S. (Vortragender)
26 Feb. 2024

QCI Days Vienna 2024 (Veranstaltung)
Hübel, H. (Conference Committee - Member), Kos, M. (Conference Committee - Member), Ramacher, S. (Conference Committee - Member) & Seifert, E. (Conference Committee - Member)
24 Jan. 2024 → 26 Jan. 2024

Quanten-resistente Kryptographie für sichere Kommunikation
Ramacher, S. (Vortragender)
24 Jan. 2024

Muckle+: End-to-End Authenticated Key Exchanges
Ramacher, S. (Vortragender)

10 Jan. 2024

Post-Quantum Cryptography
Krenn, S. (Vortragender) & Ramacher, S. (Vortragender)
1 Dez. 2023 → 26 Jan. 2024

Muckle+: End-to-End Hybrid Authenticated Key Exchanges
Striecks, C. (Vortragender, eingeladen) & Ramacher, S. (Vortragender)
3 Mai 2023

Hybrid Authenticated Key Exchanges: Status-Quo, Novel Constructions, and Applications to Long-Range Quantum-Safe Networks
Striecks, C. (Vortragender), Ramacher, S. (Autor), Perret , L. (Autor) & Bruckner, S. P. (Autor)
12 Feb. 2023 → 15 Feb. 2023

Inscrypt 2023 - The 19th International Conference on Information Security and Cryptology (Veranstaltung)
Ramacher, S. (International Programme Committee - Member)
2023

Hybrid Key Exchanges for End-to-End Security
Ramacher, S. (Vortragender, eingeladen)
14 Dez. 2022 → 15 Dez. 2022

Key Management for QKD: From a Single Link to a Network
Ramacher, S. (Vortragender, eingeladen)
12 Sept. 2022

Understanding Maturity of Data Spaces: KRAKEN SSI and Crypto solutions to data spaces
Ramacher, S. (Vortragender, eingeladen) & Perez Braun, J. C. (Vortragender, eingeladen)
19 Mai 2022 → 9 Juni 2022

Puncturable Encryption - A Fine-Grained Approach to Forward-Secure Encryption and More
Striecks, C. (Vortragender), Ramacher, S. (Autor) & Slamanig, D. (Autor)
13 Apr. 2022 → 15 Apr. 2022

KRAKEN. User engagement with privacy-preserving data sharing platforms: challenges and opportunities
Ramacher, S. (Vortragender, eingeladen), Gabrielli, S. (Autor, eingeladen), Palomares, A. (Autor, eingeladen), Perez Braun, J. C. (Autor, eingeladen), Presa, J. (Autor, eingeladen) & Zaccagnini, D. (Autor, eingeladen)
29 Nov. 2021 → 3 Dez. 2021

SoK: Lifting Transformations for Simulation Extractable Subversion and Updatable SNARKs
Abdolmaleki, B. (Vortragender), Ramacher, S. (Autor) & Slamanig, D. (Autor)
20 Apr. 2020 → 21 Mai 2020