Christoph Striecks
Scientist
Security & Communication Technologies
E-Mail: christoph.striecks@ait.ac.at

Forschungsgebiete

Kryptographische Bausteine, Sichere Kommunikation, Vorwärtssicherheit, Hybride Schlüsselaustauschverfahren

Organisationszugehörigkeiten

Scientist
Security & Communication Technologies

1 Jan. 2016 → 31 Dez. 2099

Publikationen

Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting
Hofheinz, D., Koch, J. & Striecks, C., 29 Feb. 2024, in: Journal of Cryptology. 37, 2, S. 799-822 33 S., 12.

(Inner-Product) Functional Encryption with Updatable Ciphertexts
Cini, V., Ramacher, S., Slamanig, D., Striecks, C. & Tairi, E., 15 Dez. 2023, in: Journal of Cryptology. 37, 1, S. 1-32 40 S., 8.

Revisiting Updatable Encryption: Controlled Forward Security, Constructions and a Puncturable Perspective
Slamanig, D. & Striecks, C., 27 Nov. 2023, *Theory of Cryptography Conference: TCC 2023.* Vol. 14370. S. 220-250

Muckle+: End-to-End Hybrid Authenticated Key Exchanges
Bruckner, S. P., Ramacher, S. & Striecks, C., 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).

Unique-Path Identity Based Encryption With Applications to Strongly Secure Messaging
Rösler, P., Slamanig, D. & Striecks, C., 16 Apr. 2023, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques.* Bertino, E., Gao, W., Steffen, B. & Yung, M. (Hrsg.). LNCS Aufl. Springer, Vol. 14008. S. 3-34 32 S. (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Band 14008 LNCS).

Optimizing 0-RTT Key Exchange with Full Forward Security
Göth, C., Ramacher, S., 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

Logarithmic-Size (Linkable) Threshold Ring Signatures in the Plain Model
Haque, A., Krenn, S., Slamanig, D. & Striecks, C., 2022, *25th International Conference on Practice and Theory of Public-Key Cryptography - PKC 2022.* LNCS Aufl. Springer, Vol. 13178. S. 437-467 31 S.

Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange
Derler, D., Gellert, K., Jager, T., Slamanig, D. & Striecks, C., 2021, in: Journal of Cryptology. 34, S. 13 1 S.

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

Guideline for Architectural Safety, Security and Privacy Implementations Using Design Patterns: SECREDAS Approach
Marko, N., Castella Triginer, J. M., Striecks, C., Braun, T., Schwarz, R., Marksteiner, S., Vasenev, A., Kemmerich, J., Hamazaryan, H., Shan, L. & Loiseaux, C., 2021, *SAFECOMP 2021: Computer Safety, Reliability, and Security. SAFECOMP 2021 Workshops.* Habli, I., Sujan, M., Gerasimou, S., Schoitsch, E. & Bitsch, F. (Hrsg.). Springer, S. 39-51 13 S.

Updatable Signatures and Message Authentication Codes
Cini, V., 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.

Versatile and Sustainable Timed-Release Encryption and Sequential Time-Lock Puzzles
Chvojka, P., Jager, T., Slamanig, D. & Striecks, C., 2021, *26th European Symposium on Research in Computer Security - ESORICS 2021.* Springer, S. 64-85 22 S.

CCA Secure (Puncturable) KEMs from Encryption With Non-Negligible Decryption Errors
Cini, V., 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.

Collecting and Classifying Security and Privacy Design Patterns for Connected Vehicles: SECREDAS Approach
Marko, N., Vasenev, A. & Striecks, C., 2020, *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops.* Springer, S. 36-53 18 S.

Privacy-Preserving Incentive Systems with Highly Efficient Point-Collection
Bobolz, J., Eidens, F., Krenn, S., Slamanig, D. & Striecks, C., 2020, *15th ACM ASIA Conference on Computer and Communications Security - ACM ASIACCS 2020.* S. 319-333 15 S.

Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based
Derler, D., Samelin, K., Slamanig, D. & Striecks, C., 2019, *26th Annual Network and Distributed System Security Symposium, NDSS 2019.* 1 S.

Practical Group-Signatures with Privacy-Friendly Openings
Krenn, S., Samelin, K. & Striecks, C., 2019, *Availability, Reliability and Security - ARES 2019.* S. 1-10 10 S.

Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange
Derler, D., Jager, T., Slamanig, D. & Striecks, C., 2018, *37th Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2018.* Springer, S. 425-455 31 S.

Engineering Cryptography for Security and Privacy in the Cloud
Krenn, S., Lorünser, T. & Striecks, C., 2018, in: ERCIM News. 113, S. 53-55 3 S.

Revisiting Proxy Re-encryption: Forward Secrecy, Improved Security, and Applications
Derler, D., Krenn, S., Lorünser, T., Ramacher, S., Slamanig, D. & Striecks, C., 2018, *21st IACR International Conference on Practice and Theory of Public-Key Cryptography - PKC 2018.* Springer, S. 219-250 32 S.

Secure and Privacy-Friendly Storage and Data Processing in the Cloud
Chiaro, P., Fischer-Hübner, S., Groß, T., Krenn, S., Lorünser, T., Martínez Garcí, A. I., Migliavacca, A., Rannenberg, K., Slamanig, D., Striecks, C. & Zanini, A., 2018, *Privacy and Identity Management. The Smart Revolution.* Hansen, M., Kosta, E., Nai-Fovino, I. & Fischer-Hübner, S. (Hrsg.). Springer, Vol. 526. S. 153-169 17 S.

Agile Cryptographic Solutions for the Cloud
Lorünser, T., Krenn, S., Striecks, C. & Länger, T., 2017, in: e&i elektrotechnik und informationstechnik. 134, 7, S. 364-369 6 S.

Batch-verifiable Secret Sharing with Unconditional Privacy
Krenn, S., Lorünser, T. & Striecks, C., 2017, *ICISSP 2017.* S. 303-311 9 S.

Opportunities and Challenges of CREDENTIAL - Towards a Metadata-Privacy Respecting Identity Provider
Karegar, F., Striecks, C., Krenn, S., Hörandner, F., Lorünser, T. & Fischer-Hübner, S., 2016, *Privacy and Identity Management 2016.* Springer, S. 76-91 16 S.

Towards Attribute-Based Credentials in the Cloud
Krenn, S., Lorünser, T., Salzer, A. & Striecks, C., 2016, *Cryptology and Network Security - CANS 2017.* Capkun, S. & Chow, S. S. M. (Hrsg.). Springer, S. 166-187 22 S.

Confined Guessing: New Signatures From Standard Assumptions
Böhl, F., Hofheinz, D., Jager, T., Koch, J. & Striecks, C., 2015, in: Journal of Cryptology. 28, S. 176–208

Identity-Based Encryption with (Almost) Tight Security in the Multi-instance, Multi-ciphertext Setting
Hofheinz, D., Koch, J. & Striecks, C., 2015, *18th IACR International Conference on Practice and Theory in Public-Key Cryptography - PKC 2015.* Springer, Vol. 9020. S. 799–822

On Cryptographic Building Blocks and Transformations
Striecks, C., 2015, 129 S.

A Generic View on Trace-and-Revoke Broadcast Encryption Schemes
Hofheinz, D. & Striecks, C., 2014, *Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014.* Springer, Vol. 8366. S. 48-63

Practical Signatures from Standard Assumptions
Böhl, F., Hofheinz, D., Jager, T., Koch, J., Seo, J. H. & Striecks, C., 2013, *32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2013.* Springer, Vol. 7881. S. 461-485

Programmable Hash Functions in the Multilinear Setting
Freire, E. S. V., Hofheinz, D., Paterson, K. G. & Striecks, C., 2013, *Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference Santa Barbara, CA, USA, August 2013, Proceedings Part1.* Springer, Vol. 8042. S. 513-530

Aktivitäten

Don’t Put All Your Key-Exchange Eggs in One Basket: Where Classical Crypto Meets Quantum
Striecks, C. (Vortragender)
5 Juni 2024

Austrian Electrotechnical Association (OVE) (Externe Organisation)
Striecks, C. (Mitglied)
21 Feb. 2024 → …

Exploring Cutting-Edge Architecture Developments for QKD Networks
Striecks, C. (Vortragender)
25 Jan. 2024

ASI - Austrian Standards International (Externe Organisation)
Striecks, C. (Mitglied des Nationalen Komitees)
2024 → …

CANS 2024 : The International Conference on Cryptology and Network Security (Veranstaltung)
Striecks, C. (Gutachter:in)
2024

CEN - European Committee for Standardization (Externe Organisation)
Striecks, C. (Mitglied)
2024 → …

Crypto 2024 (Veranstaltung)
Striecks, C. (Gutachter:in)
2024

GI Sicherheit (Veranstaltung)
Striecks, C. (Gutachter:in)
2024

ICISSP 2025: 11th International Conference on Information Systems Security and Privacy (Veranstaltung)
Striecks, C. (Gutachter:in)
2024 → …

International Conference on Quantum Communications, Networking, and Computing (QCNC 2024) (Veranstaltung)
Striecks, C. (Gutachter:in)
2024

Hybrid Authenticated Key Exchanges
Striecks, C. (Vortragender)
17 Nov. 2023

QCI-CAT: Austrian Quantum Communication Infrastructure
Striecks, C. (Vortragender)
19 Okt. 2023

Shaping the Future of Quantum Computing & Post-Quantum Security
Striecks, C. (Vortragender, eingeladen)
19 Okt. 2023

The 22nd International Conference on Cryptology and Network Security (CANS) (Veranstaltung)
Striecks, C. (International Programme Committee - Member)
13 Juli 2023 → 10 Aug. 2023

Muckle+: End-to-End Hybrid Authenticated Key Exchanges
Striecks, C. (Vortragender)
16 Juni 2023

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

Hybrid Key Exchanges for End-to-End Security in Quantum-Safe Networks
Striecks, C. (Vortragender, eingeladen)

9 Feb. 2023 → 10 Feb. 2023

CCS '23: ACM SIGSAC Conference on Computer and Communications Security (Veranstaltung)
Striecks, C. (Gutachter:in)
2023

Efficient Puncturable Encryption – From Bloom Filters to Forward Security
Striecks, C. (Vortragender, eingeladen)
9 Dez. 2022

International Conference on Practice and Theory of Public Key Cryptography (PKC) 2023 (Veranstaltung)
Striecks, C. (Gutachter:in)
1 Nov. 2022 → 25 Jan. 2023

EUROCRYPT 2023 (Veranstaltung)
Striecks, C. (Gutachter:in)
6 Okt. 2022 → 31 Jan. 2023

Efficient Puncturable Encryption – From Bloom Filters to Forward Security
Striecks, C. (Vortragender, eingeladen)
21 Sept. 2022

Product Security for Cross Domain Reliable Dependable Automated Systems (SECREDAS)
Schoitsch, E. (Vortragender) & Striecks, C. (Autor)
1 Juni 2022 → 2 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

Security Standardisation Research Conference 2023 (Veranstaltung)
Striecks, C. (International Programme Committee - Member)
12 Jan. 2022 → 9 Feb. 2023

Towards Functional Encryption in the Quantum-Safe Setting and Standardization Efforts
Striecks, C. (Vortragender)
18 Feb. 2021 → 19 Feb. 2021

Redactable Blockchains
Slamanig, D. (Vortragender) & Striecks, C. (Vortragender)
14 Jan. 2021

Europäische Standards für das IoT - Security-, Safety-, und Privacy-by-Design
Striecks, C. (Vortragender, eingeladen) & Schmittner, C. (Vortragender, eingeladen)
4 Nov. 2020

Attribute Based Encryption for Strong Access Control
Striecks, C. (Vortragender, eingeladen)
11 Juni 2020

Quantum-Safe (Hierarchical) Identity-Based Encryption
Striecks, C. (Vortragender, eingeladen)
11 Juni 2020

Advanced (Public-Key) Encryption
Striecks, C. (Vortragender, eingeladen)
28 Jan. 2020

Attribute-Based Encryption for Strong Access Control
Striecks, C. (Vortragender)
19 Sept. 2019

Next Generation Cryptography
Striecks, C. (Vortragender, eingeladen) & Slamanig, D. (Vortragender)
22 März 2019

Advanced (Public-Key) Encryption
Striecks, C. (Vortragender, eingeladen)
22 Jan. 2019

Attribute Based Encryption for Access Control and Personal Data Protection
Ambrosini, F. (Vortragender) & Striecks, C. (Vortragender)
23 Okt. 2018

Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange
Striecks, C. (Vortragender, eingeladen)
18 Okt. 2018

Advanced Public-Key Cryptography Mechanisms for the IoT
Striecks, C. (Vortragender)
25 Sept. 2018

Attribute-based Encryption
Striecks, C. (Vortragender)
11 Sept. 2018 → 12 Sept. 2018

Trust in Chained Blocks
Striecks, C. (Vortragender)
5 Sept. 2018

Attribute-based Encryption - Data Access Control in the IoT: a Newly Standardized Mechanism
Striecks, C. (Vortragender)
11 Juni 2018 → 15 Juni 2018

Confined guessing: a reduction strategy to obtain new signatures from standard assumptions
Striecks, C. (Vortragender)
Sept. 2015

Programmable Hash Functions in the Multilinear Setting
Striecks, C. (Vortragender)
1 Jan. 2014