Christoph Striecks
Senior Scientist
Cyber Security and Communication Technologies

Research interests

Secure Communication, Forward Security. Hybrid Key Exchanges

Employment

Senior Scientist
Cyber Security and Communication Technologies
AIT Austrian Institute of Technology GmbH
1 Jan 2026 → present

Research outputs

Assessment of provably secure hybrid authenticated key exchange for dual-use applications
Abelard, S., Vieira Giestinhas, J. A., Kahrobaei, D., Perret, L., Spiller, T. & Striecks, C., 11 Jun 2026, In: EPJ Quantum Technology. 13, 1, 24 p., 86.

Quantum-safe hybrid key exchanges with KEM-based authentication
Battarbee, C., Striecks, C., Perret, L., Ramacher, S. & Verhaeghe, K., 10 Nov 2025, In: EPJ Quantum Technology. 12, 1, 28 p., 128.

Versatile Quantum-Safe Hybrid Key Exchange and Its Application to MACsec
Saez de Buruga, J., Bugler, A., Brito, J. P., Martin, V. & Striecks, C., 4 Jul 2025, In: Journal of Optical Communications and Networking. 12, 1, 27 p., 84.

Malleable SNARKs and Their Applications
Chakraborty, S., Hofheinz, D., Langrehr, R. (Author and Speaker), Nielsen , J. B., Striecks, C. & Venturi , D., 27 Apr 2025, *Advances in Cryptology – EUROCRYPT 2025: 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4–8, 2025, Proceedings, Part IV.* Fehr, S. & Fouque, P.-A. (eds.). 1 ed. Vol. 15604. p. 184–213 29 p. (Lecture Notes in Computer Science; vol. 15604).

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, p. 799-822 33 p., 12.

(Inner-Product) Functional Encryption with Updatable Ciphertexts
Cini, V., Ramacher, S., Slamanig, D., Striecks, C. & Tairi, E., 2024, In: Journal of Cryptology. 37, 1, p. 1-32 40 p., 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. p. 220-250

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

Unique-Path Identity Based Encryption With Applications to Strongly Secure Messaging
Rösler, P. (Speaker), 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. (eds.). LNCS ed. Springer, Vol. 14008. p. 3-34 32 p. (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); vol. 14008 LNCS).

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

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

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, p. 13 1 p.

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

Guideline for Architectural Safety, Security and Privacy Implementations Using Design Patterns: SECREDAS Approach
Marko, N., Castella Triginer, J. M. (Speaker), 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. (eds.). Springer, p. 39-51 13 p.

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

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

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

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

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

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

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

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

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

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

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. (eds.). Springer, Vol. 526. p. 153-169 17 p.

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

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

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

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

Activities

Universidad Politécnica de Madrid (External organisation)
Striecks, C. (Examiner)
11 Sept 2026

Universidad Politécnica de Madrid (External organisation)
Striecks, C. (Examiner)
27 Jul 2026

Quantum-Safe Hybrid Authenticated Key Exchanges
Striecks, C. (Speaker, invited)
22 Jul 2026

On developing quantum-safe hybrid cryptographic standards
Striecks, C. (Speaker)
17 Jun 2026

Quantum-Safe Hybrid Authenticated Key Exchanges
Striecks, C. (Speaker, invited)
27 Feb 2026

Quantum-Safe Hybrid Technologies for the Public Sector
Striecks, C. (Speaker, invited)
5 Feb 2026

KPMG IMPULSE Podcast #134: Quantencomputing: Chancen und Herausforderungen dieser Technologie
Striecks, C. (Participant)
19 Jan 2026

External PhD Thesis Reviewer for Universidad Politécnica de Madrid
Striecks, C. (Other)
2026

External PhD Thesis Reviewer for Universidad Politécnica de Madrid
Striecks, C. (Other)
2026

Hybridization: securely combining PQC and Quantum Cryptography Components
Striecks, C. (Speaker, invited)
5 Sept 2025

Security Standardisation Research Conference 2025 (Event)
Striecks, C. (International Programme Committee - Member)
11 Aug 2025 → 5 Dec 2025

EPJ Quantum Technology (Journal)
Striecks, C. (Reviewer)
Aug 2025

On the Transition to Quantum-Safe Cryptography
Striecks, C. (Speaker, invited)
26 Jun 2025

Quantum-Safe Hybrid Cryptography Workshop (Event)
Perret , L. (International Programme Committee - Co-Chair) & Striecks, C. (International Programme Committee - Co-Chair)
25 Jun 2025

Quantum-Safe Authenticated Key Exchanges: The Present and the Future of Hybrid Approaches
Striecks, C. (Speaker)
4 Jun 2025

The Hybrid State-of-Play: How to Securely Combine Quantum and Classical Key Establishment Technologies
Striecks, C. (Speaker) & Perret , L. (Author)
4 May 2025

The Hybrid State-of-Play: How to Securely Combine Quantum and Post-Quantum Technologies
Striecks, C. (Speaker)
30 Apr 2025

IEICE Transactions on Communications (Journal)
Striecks, C. (Reviewer)
1 Apr 2025 → 24 Jul 2025

Crypto 2025 (Event)
Striecks, C. (Reviewer)
26 Feb 2025 → 3 May 2025

The Hybrid Paradigm for Key Establishment: Quantum-Safe and Crypto-Agile Solutions
Striecks, C. (Speaker, invited)
25 Feb 2025

24th International Conference on Cryptology And Network Security (CANS 2025) (Event)
Striecks, C. (International Programme Committee - Member)
3 Feb 2025 → 14 Aug 2025

IEEE Transactions on Information Forensics and Security (Journal)
Striecks, C. (Reviewer)
9 Jan 2025 → 15 Apr 2025

Austrian QCI-CAT Project Overview and Architecture
Striecks, C. (Speaker)
13 Dec 2024

Don't Put All Your Key-Exchange Eggs in One Basket
Striecks, C. (Speaker, invited)
2 Dec 2024 → 6 Dec 2024

CERIS Workshop on Secure Communication
Striecks, C. (Speaker, invited)
24 Oct 2024

International Conference on Quantum Communications, Networking, and Computing (QCNC 2025) (Event)
Striecks, C. (International Programme Committee - Member)
11 Oct 2024 → 2 Apr 2025

Quantum-Secure Hybrid Key Exchanges: "Do Not Put All Your Eggs in One Basket"
Striecks, C. (Speaker, invited) & Perret , L. (Speaker, invited)
2 Oct 2024

PETRUS Webinars: Authentication
Striecks, C. (Speaker)
29 Aug 2024 → 10 Sept 2024

ACM Computing Surveys (Journal)
Striecks, C. (Reviewer)
29 Jul 2024 → 12 Sept 2024

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

Austrian Electrotechnical Association (OVE) (External organisation)
Striecks, C. (Member)
21 Feb 2024 → …

Hybride Schlüsselweiterleitung
Striecks, C. (Speaker, invited)
15 Feb 2024

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

Hybrid Authenticated Key Exchanges
Striecks, C. (Speaker)
11 Jan 2024

Austrian Standards (External organisation)
Striecks, C. (Member)
2024 → …

CANS 2024 : The International Conference on Cryptology and Network Security (Event)
Striecks, C. (International Programme Committee - Member)
2024

Crypto 2024 (Event)
Striecks, C. (Reviewer)
2024

European Committee for Standardization (CEN) (External organisation)
Striecks, C. (Member)
2024 → …

GI Sicherheit (Event)
Striecks, C. (International Programme Committee - Member)
2024

ICISSP 2025: 11th International Conference on Information Systems Security and Privacy (Event)
Striecks, C. (International Programme Committee - Member)
2024 → 2025

IEEE Standards Association (External organisation)
Striecks, C. (Member)
2024 → …

International Conference on Quantum Communications, Networking, and Computing (QCNC 2024) (Event)
Striecks, C. (International Programme Committee - Member)
2024

Security Standardisation Research Conference 2024 (Event)
Striecks, C. (International Programme Committee - Member)
2024

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

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

Shaping the Future of Quantum Computing & Post-Quantum Security
Striecks, C. (Speaker, invited)
19 Oct 2023

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

Muckle+: End-to-End Hybrid Authenticated Key Exchanges
Striecks, C. (Speaker, invited) & Ramacher, S. (Speaker)
3 May 2023

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

Hybrid Key Exchanges for End-to-End Security in Quantum-Safe Networks
Striecks, C. (Speaker, invited)
9 Feb 2023 → 10 Feb 2023

ARES Workshops 2023 (Event)
Striecks, C. (International Programme Committee - Member)
2023 → …

CANS 2023 : The International Conference on Cryptology and Network Security (Event)
Striecks, C. (International Programme Committee - Member)
2023

CCS '23: ACM SIGSAC Conference on Computer and Communications Security (Event)
Striecks, C. (Reviewer)
2023

ICISSP 2024: 11th International Conference on Information Systems Security and Privacy (Veranstaltung) (Event)
Striecks, C. (International Programme Committee - Member)
2023 → 2024

Efficient Puncturable Encryption – From Bloom Filters to Forward Security
Striecks, C. (Speaker, invited)
9 Dec 2022

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

EUROCRYPT 2023 (Event)
Striecks, C. (Reviewer)
6 Oct 2022 → 31 Jan 2023

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

Product Security for Cross Domain Reliable Dependable Automated Systems (SECREDAS)
Schoitsch, E. (Speaker) & Striecks, C. (Author)
1 Jun 2022 → 2 Jun 2022

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

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

43rd IEEE Symposium on Security and Privacy (Event)
Striecks, C. (Reviewer)
2022

49th EATCS ICALP 2022 (Event)
Striecks, C. (Reviewer)
2022

ARES Workshops 2022 (Event)
Striecks, C. (International Programme Committee - Member)
2022

ASIACRYPT 2022 (Event)
Striecks, C. (Reviewer)
2022

CANS 2022 : The International Conference on Cryptology and Network Security (Event)
Striecks, C. (International Programme Committee - Member)
2022

CCS '22: ACM SIGSAC Conference on Computer and Communications Security (Event)
Striecks, C. (Reviewer)
2022

Crypto 2022 (Event)
Striecks, C. (Reviewer)
2022

Designs, Codes, and Cryptography (Journal)
Striecks, C. (Reviewer)
2022

ETSI - European Telecommunications Standards Institute (External organisation)
Striecks, C. (Member)
2022 → …

IEEE Transactions on Dependable and Secure Computing (Journal)
Striecks, C. (Reviewer)
2022

IEEE Transactions on Information Forensics and Security (Journal)
Striecks, C. (Reviewer)
2022

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

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

Asiacrypt 2021 (Event)
Striecks, C. (Reviewer)
2021

Eurocrypt 2022 (Event)
Striecks, C. (Reviewer)
2021 → 2022

GI Sicherheit 2022 (Event)
Striecks, C. (International Programme Committee - Member)
2021 → 2022

IEEE Transactions on Dependable and Secure Computing (Journal)
Striecks, C. (Reviewer)
2021

USENIX Security '21 (Event)
Striecks, C. (Reviewer)
2021

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

Attribute Based Encryption for Strong Access Control
Striecks, C. (Speaker, invited)
11 Jun 2020

Quantum-Safe (Hierarchical) Identity-Based Encryption
Striecks, C. (Speaker, invited)
11 Jun 2020

Advanced (Public-Key) Encryption
Striecks, C. (Speaker, invited)
28 Jan 2020

15th IFIP Summer School on Privacy and Identity Management 2020 (Event)
Striecks, C. (Conference Committee - Member)
2020

ARES Workshops 2020 (Event)
Striecks, C. (International Programme Committee - Member)
2020

CCS '20: ACM SIGSAC Conference on Computer and Communications Security (Event)
Striecks, C. (Reviewer)
2020

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

Next Generation Cryptography
Striecks, C. (Speaker, invited) & Slamanig, D. (Speaker)
22 Mar 2019

Advanced (Public-Key) Encryption
Striecks, C. (Speaker, invited)
22 Jan 2019

14th IFIP Summer School on Privacy and Identity Management 2019 (Event)
Striecks, C. (Conference Committee - Member)
2019

Crypto 2019 (Event)
Striecks, C. (Reviewer)
2019

GI Sicherheit 2020 (Event)
Striecks, C. (International Programme Committee - Member)
2019 → 2020

IMA International Conference on Cryptography and Coding (Event)
Striecks, C. (International Programme Committee - Member)
2019

International Conference on Practice and Theory of Public Key Cryptography (PKC) 2020 (Event)
Striecks, C. (Reviewer)
2019 → 2020

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

Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange
Striecks, C. (Speaker, invited)
18 Oct 2018

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

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

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

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

ETSI - European Telecommunications Standards Institute (External organisation)
Striecks, C. (Expert)
6 Mar 2017 → 9 Feb 2018

International Conference on Practice and Theory of Public Key Cryptography (PKC) 2018 (Event)
Striecks, C. (Reviewer)
2017 → 2018

ASIACRYPT 2016 (Event)
Striecks, C. (Reviewer)
2016

International Conference on Practice and Theory of Public Key Cryptography (PKC) 2016 (Event)
Striecks, C. (Reviewer)
2016

International Conference on Practice and Theory of Public Key Cryptography (PKC) 2017 (Event)
Striecks, C. (Reviewer)
2016 → 2017

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

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