
Quantum-Safe Internet (QSI)

Deliverable D6.6 & Deliverable D6.8

Deliverable: D6.6, **Deliverable Name:** International Conference Presentations.

Deliverable: D6.8, **Deliverable Name:** Publication in high-impact journals.

Work Package No: WP6

Due Date: 30/09/2026.

References: Grant Agreement of the Project.

Publications

Below, we include a list of the publications produced by the Doctoral Candidates (DCs) within the QSI project. We distribute them into journal papers that have been already published and/or accepted for publication, proceedings, journal papers that are currently under review, and conference papers that have been presented in conferences and workshops. The DCs are highlighted in bold and their name has moreover been underlined.

6.1 Journal Papers, published/accepted (Doctoral Candidates)

[1] **V. Mannalath**, A. Pathak: “Multiparty entanglement routing in quantum networks”, Phys. Rev. A 108, 062614 (2023). DOI: <https://doi.org/10.1103/PhysRevA.108.062614>

[2] **J. Rey-Dominguez**, A. Navarrete, P. van Loock, and M. Curty: “Hacking coherent-one-way quantum key distribution with present-day technology”, Quantum Sci. Technol. 9 035044 (2024). <https://doi.org/10.1088/2058-9565/ad4f0c>

[3] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, A. Valle, K. Tamaki, M. Curty, “Characterising higher-order phase correlations in gain-switched laser sources with application to quantum key distribution”, EPJ Quantum Technology, 12(1), 38, 2025. <https://doi.org/10.1140/epjqt/s40507-025-00340-7>

[4] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, D. Scalcon, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, **S. Juárez**, P. Rydlichowski, D. Vicinanza, G. Roberts, A. J. Shields, “Long-distance coherent quantum communications in deployed telecom networks”. Nature 640, 911–917 (2025). <https://doi.org/10.1038/s41586-025-08801-w>

- [5] B. Lopes da Costa, **M. R Bolaños**, R. Chaves, C. Narduzzi, M. Avesani, D. G. Marangon, A. Stanco, G. Vallone, P. Villoresi, Y. Omar, "Power-consumption back door in quantum key distribution", Phys. Rev. Applied 24, 054004, 2025. <https://doi.org/10.1103/f92x-c3zj>
- [6] **M. R. Bolaños**, D. Vogrig, P. Villoresi, G. Vallone and A. Stanco, "A Time-to-Digital Converter With Steady Calibration Through Single-Photon Detection," in IEEE Transactions on Instrumentation and Measurement 74, 1-9, 2025, Art no. 6510309, <https://doi.org/10.1109/TIM.2025.3601244>.
- [7] **L. Millet**, A. Boaron, R. Thew, G. Boso, "Influence of laser chirp and interferometer delay and imbalance on the performance of a time-bin BB84 quantum key distribution system", Appl. Phys. Lett. 127 (4): 044001, 2025. <https://doi.org/10.1063/5.0280232>
- [8] **A. Marcomini**, A. Mizutani, F. Grünenfelder, M. Curty, K. Tamaki, "Loss-tolerant quantum key distribution with detection efficiency mismatch", Quantum Science and Technology, 10(3), 035002, 2025. <https://doi.org/10.1088/2058-9565/adc8cc>
- [9] **V. Mannelath**, V. Zapatero, M. Curty, "Sharp Finite Statistics for Quantum Key Distribution", Physical Review Letters 135, 020803 (2025). <https://doi.org/10.1103/l735-x48g>
- [10] **V. Mannelath**, A. Pathak, Entanglement Routing and Bottlenecks in Grid Networks. Annalen der Physik 537, 2400316, 2025. <https://doi.org/10.1002/andp.202400316>
- [11] **S. Juárez**, **A. Marcomini**, M. Petrov, R. I. Woodward, T. J. Dowling, R. M. Stevenson, M. Curty, D. Rusca, "Reference-beam attacks against twin-field quantum key distribution using optical injection locking", Physical Review A, 113(3), 032613, 2026. <https://doi.org/10.1103/71m5-3c5n>
- [12] **S. Kumar**, **A. Marcomini**, L. Millet, T. Taher, A. Cavalié, R. Houlmann, D. Cabrerizo, G. Boso, M. Curty, R. Thew, B. Korzh, "Phase-correlation-free quantum key distribution source operating at gigahertz rates", APL Photonics 11, 081302, 2026. <https://doi.org/10.1063/5.0347954>
- [13] **V. Mannelath**, V. Zapatero, M. Curty, "Elementary Tail Bounds on the Hypergeometric Distribution", Communications in Statistics – Theory and Methods, 1–7 (2026). <https://doi.org/10.1080/03610926.2026.2676012>
- [14] E. Diamanti, A. B. Grilo, A. Innocenzi, P. Lefebvre, V. Yacoub, **Á. Yáñez**, "A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions", Quantum 10, 2124, 2026. <https://doi.org/10.22331/q-2026-06-01-2124>
- [15] **J. Rey-Domínguez**, M Razavi, "Rethinking quantum repeaters: balancing scalability, feasibility, and interoperability", Quantum Sci. Technol. 11, 045016, 2026. <https://doi.org/10.1088/2058-9565/ae9178>
- [16] **Á. Yáñez**, T. A. Hahn, J. Kochanowski, "Efficient Quantum Measurements: Computational Max- and Measured Rényi Divergences and Applications", in IEEE Transactions on Information Theory 72, no. 6, pp. 4085-4114, 2026, <https://doi.org/10.1109/TIT.2026.3680247>
- [17] A. B. Grilo, **Á. Yáñez**, "Quantum pseudoresources imply cryptography", IACR Communications in Cryptology 2, no. 4, Jan 08, 2026, <https://doi.org/10.62056/ahbngyl7s>.

- [18] Y. S. Lo, A. H. Brzosko, P. R. Smith, R. I. Woodward, D. G. Marangon, J. F. Dynes, **S. Juárez**, T. K. Paraíso, R. M. Stevenson, A. J. Shields, "Phase-randomized laser pulse generation at 10 GHz for quantum photonic applications", APL Photonics 11 (8), 086111, 2026. <https://doi.org/10.1063/5.0321309>
- [19] **M. R. Bolaños**, E. Rossi, F. Berra, A. De Toni, I. Karakosta-Amarantidou, D. C. Lawo, C. Agnesi, M. Avesani, A. Stanco, F. Vedovato, P. Villoresi, G. Vallone, "GHz-rate polarization-based QKD system for fiber and free-space applications," Optica Quantum 4, 389-396, 2026. <https://doi.org/10.1364/OPTICAQ.596140>
- [20] F. Berra, **M. R. Bolaños**, A. De Toni, K. Vijayadharan, C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, G. Vallone, "General model and modulation strategies for Sagnac-based encoders", Phys. Rev. Research 8, 033069, 2026. <https://doi.org/10.1103/q2sy-sw7h>
- [21] A. Bernardi, M. Clementi, M. Bacchi, **M. R. Bolaños**, S. Congia, F. Garrisi, A. Martellosio, M. Passoni, A. Wrobel, C. Agnesi, G. Vallone, P. Villoresi, F. A. Sabbatoli, M. Galli, D. Bajoni, "Gigahertz-rate thin-film lithium niobate receiver for time-bin quantum communication", Light Sci Appl 15, 237, 2026. <https://doi.org/10.1038/s41377-026-02306-5>
- [22] K. Vijayadharan, **M. R. Bolaños**, M. Avesani, G. Vallone, P. Villoresi, C. Agnesi, "A Sagnac-based arbitrary time-bin state encoder for quantum communication applications", EPJ Quantum Technology 12:129, 2025. <https://doi.org/10.1140/epjqt/s40507-025-00428-0>

6.2 Proceedings (Doctoral Candidates)

- [1] N. Alnahawi, K. Hövelmanns, A. Hülsing, **S. Ritsch**, "Towards post-quantum secure PAKE-A tight security proof for OCAKE in the BPR model", In: Kohlweiss, M., Di Pietro, R., Beresford, A. (eds) Cryptology and Network Security. CANS 2024. Lecture Notes in Computer Science, vol 14906. Springer, Singapore. https://doi.org/10.1007/978-981-97-8016-7_9
- [2] C. Majenz, **F. Sisinni**, "Provable Security Against Decryption Failure Attacks from LWE", in: Reyzin, L., Stebila, D. (eds) Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol 14921. Springer, Cham. (2024). https://doi.org/10.1007/978-3-031-68379-4_14
- [3] A. May, **M. Ostuzzi**, (2025). Multiple Group Action Dlogs With(out) Precomputation. In: Jager, T., Pan, J. (eds) Public-Key Cryptography – PKC 2025. PKC 2025. Lecture Notes in Computer Science, vol 15676. Springer, Cham. https://doi.org/10.1007/978-3-031-91826-1_12
- [4] **J. Rey-Domínguez**, M. Razavi, "Quantum key distribution over an encoded repeater chain with sequential swapping," 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Nara, Japan, 2025, pp. 323-330, <https://doi.org/10.1109/QCNC64685.2025.00058>.
- [5] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, D. Scalcon, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, **S. Juárez**, P. Rydlichowski, D. Vicinanza, G. Roberts, A. J. Shields. "Twin-field QKD over a deployed optical network enabled by long-range phase locking and semiconductor detectors", Proc. SPIE 13391, Quantum Computing, Communication, and Simulation V, 133910I (19 Mar 2025); <https://doi.org/10.1117/12.3043348>

- [6] K. Hövelmanns, A. Hülsing, C. Majenz, **F. Sisinni**, “(Un) breakable Curses-Re-encryption in the Fujisaki-Okamoto Transform”, In: Fehr, S., Fouque, PA. (eds) Advances in Cryptology – EUROCRYPT 2025. EUROCRYPT 2025. Lecture Notes in Computer Science, vol 15602. Springer, Cham. https://doi.org/10.1007/978-3-031-91124-8_9
- [7] Y. S. Lo, A. H. Brzosko, P. R. Smith, R. I. Woodward, D. G. Marangon, J. F. Dynes, **S. Juárez**, T. K. Paraíso, R. M. Stevenson, A. J. Shields, "10 GHz Phase-Randomized Light Source for Quantum Photonic Applications," 2026 Optical Fiber Communications Conference and Exhibition (OFC), Los Angeles, CA, USA, 2026, pp. 1-3. Electronic ISBN:978-1-957171-54-8
- [8] **S. Juárez**, A. Marcomini, M. Petrov, R. I. Woodward, T. J. Dowling, R. M. Stevenson, M. Curty, and D. Rusca, "Implementation Security of Twin-Field Quantum Key Distribution using Optical Injection Locking," in CLEO 2026, Technical Digest Series (Optica Publishing Group, 2026), paper JTU.187. https://doi.org/10.1364/CLEO_AT.2026.JTU.187
- [9] A. H. Brzosko, Y. S. Lo, P. R. Smith, R. I. Woodward, D. G. Marangon, J. F. Dynes, **S. Juárez**, T. K. Paraíso, R. M. Stevenson, and A. J. Shields, "Overcoming the Phase Diffusion Limit in a Semiconductor Laser-based QRNG," in CLEO 2026, Technical Digest Series (Optica Publishing Group, 2026), paper FM3A.2. https://doi.org/10.1364/CLEO_FS.2026.FM3A.2
- [10] A. H. Brzosko, Y. S. Lo, P. R. Smith, R. I. Woodward, D. G. Marangon, J. F. Dynes, **S. Juárez**, T. K. Paraíso, R. M. Stevenson, and A. J. Shields, "Phase Randomization of DFB Laser Pulses Beyond the Diffusion Limit," in Quantum diamond Conference and Exhibition, Technical Digest Series (Optica Publishing Group, 2026), paper QTu3A.2. ISBN: 978-1-957171-61-6
- [11] **S. Juárez**, **A. Marcomini**, M. Petrov, R. I. Woodward, T. J. Dowling, R. M. Stevenson, M. Curty, and D. Rusca, "Reference Beam Attacks against Twin-Field Quantum Key Distribution using Optical Injection Locking," in Quantum 2.0 Conference and Exhibition, Technical Digest Series (Optica Publishing Group, 2026), paper QTu4C.7.
- [12] A. Bernardi, M. Clementi, M. Bacchi, **M. R. Bolaños**, S. Congia, F. Garrisi, A. Martellosio, M. Passoni, A. Wrobel, C. Agnesi, G. Vallone, P. Villoresi, F. A. Sabattoli, M. Galli, and D. Bajoni, "Thin-Film Lithium Niobate Receiver for Time-Bin Quantum Communication," in CLEO 2026, Technical Digest Series (Optica Publishing Group, 2026), paper FTH1B.7. https://doi.org/10.1364/CLEO_FS.2026.FTH1B.7
- [13] M. Giacomini, J. M. Traktenberg, **M. R. Bolaños**, G. Di Sciullo, T. Hayashi, C. Antonelli, G. Vallone, P. Villoresi, C. Agnesi, "Demonstration of a Cross-Encoded RFI QKD system in a field-deployed multi-core fiber," 2026 Optical Fiber Communications Conference and Exhibition (OFC), Los Angeles, CA, USA, 2026, pp. 1-3. ISBN: 978-1-957171-54-8
- [14] A. May, **M. Ostuzzi**, H. Ressler (2026). Just Guess: Improved (Quantum) Algorithm for the Underdetermined MQ Problem. In: Daemen, J., Thomé, E. (eds) Advances in Cryptology – EUROCRYPT 2026. EUROCRYPT 2026. Lecture Notes in Computer Science, vol 16544. Springer, Cham. https://doi.org/10.1007/978-3-032-25327-9_12

6.3 Journal Papers, under review (Doctoral Candidates)

- [1] D. J. Bernstein, J. Cottaar, E. Di Giandomenico, K. Hövelmanns, A. Hülsing, M. Kudinov, T. Lange, M. Mahzoun, M. Meijers, A. Pellegrini, A. Ravagnani, **S. Ritsch**, S. Schäge, T. Tang, M. Trimoska, M. Vorstermans, F. J. Weber, “Report on evaluation of KpqC Round-2 candidates”, Cryptology ePrint Archive <https://cr.yp.to/papers/kpqc-20241226.pdf>
- [2] C. Majenz, **F. Sisinni**, “Provable decryption failure security for practical lattice-based PKE”, Cryptology ePrint Archive Paper 2025/1997. <https://ia.cr/2025/1997>
- [3] J. Janneck, J. Meers, **M. Ostuzzi**, D. Riepel, “Snake mackerel: An isogeny-based AKEM leveraging randomness reuse”, Cryptology ePrint Archive Paper 2025/1474. <https://ia.cr/2025/1474>
- [4] **A. Marcomini**, P. J. Vetter, T. Calarco, F. Motzoi, F. Jelezko, M. M. Müller, “Gate optimization via efficient two-qubit benchmarking for NV centers in diamond”, preprint: arXiv:2603.08581, 2026. <https://doi.org/10.48550/arXiv.2603.08581>
- [5] **Á. Yálguez**, N. Avidan, J. Kochanowski, T. A. Hahn, “Accessible Quantum Correlations Under Complexity Constraints”, arXiv preprint arXiv:2604.15540, 2026. <https://doi.org/10.48550/arXiv.2604.15540>
- [6] M. S. Winnel, **S. Juárez**, C. Perumangatt, T. Paraiso, R. M. Stevenson, “All-photonic quantum key distribution beyond the single-repeater bound”, arXiv preprint arXiv:2604.16174, 2026. <https://doi.org/10.48550/arXiv.2604.16174>
- [7] G. Currás-Lorenzo, M. Pereira, **A. Marcomini**, K. Tamaki, M. Curty, “Security of decoy-state quantum key distribution with correlated bit-and-basis encoders”, preprint: arXiv:2605.11767, 2026. <https://doi.org/10.48550/arXiv.2605.11767>
- [8] **V. Mannalath**, V. Zapatero, M. Curty, “Finite-key feasibility of geostationary quantum key distribution”, arXiv preprint arXiv:2605.29706, 2026. <https://doi.org/10.48550/arXiv.2605.29706>
- [9] **L. Millet**, B. Korzh, R. Thew, G. Boso, “Analytical Model of Clock Drift in Quantum Key Distribution and a Simple Synchronization Algorithm”, arXiv preprint arXiv:2605.26705, 2026. <https://doi.org/10.48550/arXiv.2605.26705>
- [10] M. Sabatini, T. Bertapelle, A. Peri, G. Gualandi, **M. R. Bolaños**, Y. Piétri, G. Corrielli, P. Villaresi, G. Vallone, R. Osellame, A. Tavakoli, M. Avesani, “Efficient Energy-Constrained Semi-Device-Independent QRNG with an Integrated Heterodyne Receiver”, arXiv preprint arXiv:2606.23231, 2026. <https://doi.org/10.48550/arXiv.2606.23231>
- [11] **V. Mannalath**, V. Zapatero, K. Tamaki, M. Curty, “Quantum Key Distribution Beyond Stationary Channels”, arXiv preprint arXiv:2607.17690, 2026. <https://doi.org/10.48550/arXiv.2607.17690>
- [12] Y.-H. Huang, A. Hülsing, V. Maram, **S. Ritsch**, A. Saha, “Feistel Tools: Reprogramming and Query-Recording for QRPs”, Cryptology ePrint Archive Paper 2026/146. <https://ia.cr/2026/146>
- [13] K. Hövelmanns, A. Hülsing, M. Kudinov, **S. Ritsch**, “CAKE requires programming-on the provable post-quantum security of (O) CAKE”, Cryptology ePrint Archive Paper 2025/458. <https://ia.cr/2025/458>

[14] **M. Ostuzzi**, “Pseudo-Oil Subspaces and the Geometry of Underdetermined MQ Problems”, Cryptology ePrint Archive Paper 2026/1122. <https://ia.cr/2026/1122>

6.4 Conference papers, presented/accepted (Doctoral Candidates)

[1] **V. Mannalath**, “Multiparty Entanglement Routing in Quantum Networks”, Quantum Technologies for Young Researchers Workshop held at Instituto de Química Física Blas Cabrera (IQF-CSIC) in Madrid from 4-7th July, 2023.

[2] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, M. Curty, “Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD”, 13th international conference on quantum cryptography (QCRYPT2023), University of Maryland, USA, 14-18 August, 2023.

[3] F. Berra, **M. R. Bolaños**, C. Agnesi, M. Avesani, A. Stanco, G. Vallone, P. Villaresi, “Quantum Key Distribution at 1 GHz and time-tagging system development”, 108a Reunión Anual de la Asociación de Física Argentina, 19-22 September, 2023.

[4] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, M. Curty, “Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD”, “Primera Reunión Nacional del Plan Complementario de Comunicaciones Cuánticas”, Universidad Politécnica de Madrid (Spain), 19-21 September, 2023.

[5] F. Berra, C. Agnesi, I. Karakosta-Amarantidou, M. Avesani, **M. R. Bolaños**, A. De Toni, A. Stanco, F. Picciariello, F. Vedovato, N. Laurenti, P. Villaresi, G. Vallone, “High speed source for satellite quantum key distribution”. IAC2023, Baku, Azerbaijan, 1-7 October 2023.

[6] A. Innocenzi, V. Yacoub, **Á. Yáñez**, P. Lefebvre, A. B. Grilo, E. Diamanti, “Experimental implementation of Simulation secure Quantum Oblivious Transfer”, 1st Colloquium GdR TeQ “Quantum Technologies”, University of Montpellier, France, 22-24 November 2023.

[7] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, A. Valle, K. Tamaki, M. Curty, “Security of Decoy-State QKD with Phase Correlations in Gain-Switched Lasers”. IX Workshop do Programa de Doutorado Interuniversitário em Laser, Fotónica e Visão, Universidade de Vigo, Spain (2023).

[8] **M. R. Bolaños**, D. Vogrig, P. Villaresi, G. Vallone, A. Stanco. “FPGA-based time-to-digital converter for Quantum Key Distribution with Continuous Calibration”, Optica Quantum 2.0 Conference and Exhibition, Rotterdam, Netherlands, 23-27 June 2024.

[9] **J. Rey-Domínguez**, A. Lawey and M. Razavi, “Quantum key distribution over connectionless quantum repeater networks”, White Rose QIST workshop 2024, York, United Kingdom, 11-12 July 2024.

[10] **A. Marcomini**, G. Currás-Lorenzo, D. Rusca, M. Curty, “Security of decoy-state QKD with higher-order phase correlations in gain-switched lasers”, XXXIX Reunión Bienal de la Real Sociedad Española de Física, School of Engineering of Gipuzkoa, San Sebastián (Spain), 15-19 July, 2024.

[11] V. Zapatero, **V. Mannalath**, M. Curty, “A refined statistical bound for QKD security analyses”, XXXIX Reunión Biental de la Real Sociedad Española de Física, School of Engineering of Gipuzkoa, San Sebastián (Spain), 15-19 July 2024.

[12] **A. Marcomini**, Fadri Grünenfelder, G. Currás-Lorenzo, A. Valle, K. Tamaki, H. Zbinden, M. Curty, D. Rusca, “Experimental characterisation of second-order phase correlations in gain-switched laser sources for decoy-state QKD”, 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September, 2024.

[13] **V. Mannalath**, V. Zapatero, M. Curty, “Quantum key distribution with small data block sizes”, 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[14] **M. R. Bolaños**, et al. “An auto-calibrated time-to-digital converter for Quantum Communication”, 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[15] B. Lopes da Costa, **M. R. Bolaños**, R. Chaves, C. Narduzzi, M. Avesani, D. G. Marangon, A. Stanco, G. Vallone, P. Villaresi and Y. Omar, “Quantum Backdoor - Performing Electronic Side-Channel Analysis on QKD System”, 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[16] A. Innocenzi, V. Yacoub, **Á. Yáñgüez**, P. Lefebvre, A. B. Grilo, E. Diamanti, “Experimental implementation of Simulation secure Quantum Oblivious Transfer”, 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[17] **J. Rey-Domínguez**, A. Lawey and M. Razavi, “Quantum key distribution over connectionless quantum repeater networks”, 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[18] E. Diamanti, A. B. Grilo, A. Innocenzi, P. Lefebvre, V. Yacoub, **Á. Yáñgüez**, “A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions”, 14th international conference on quantum cryptography (QCRYPT2024), Vigo, Spain, 2-6 September 2024.

[19] E. Diamanti, A. B. Grilo, A. Innocenzi, P. Lefebvre, V. Yacoub, **Á. Yáñgüez**, “A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions”, YQIS Conference, Paris, France, 4-8 November 2024.

[20] A. Innocenzi, V. Yacoub, **Á. Yáñgüez**, P. Lefebvre, A. B. Grilo, E. Diamanti, “Experimental implementation of quantum oblivious transfer from one-way functions”, 2nd Colloquium GdR TeQ “Quantum Technologies”, Sorbonne Université, France, 13-15 November 2024.

[21] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, **S. Juárez**, P. Rydlichowski, D. Vicinanza, G. Roberts, A. J. Shields, “Coherent Quantum Key Distribution Across National Scale Telecommunication Infrastructure”, Single Photon Workshop 2024, Edinburgh, Scotland (UK) November 20, 2024.

[22] **M. R. Bolaños** et al., “Encoding arbitrary d-dimensional time-bin states”, XIII Quantum Foundations, Cordoba, Argentina, 25-27 November 2024.

[23] **A. Marcomini**, “Towards a Unified Security Proof for Prepare-and-Measure Quantum Key

Distribution” Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[24] **Á. Yángüez**, “Quantum pseudo-resources imply cryptography”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[25] **V. Mannelath**, “Tight Statistical Bounds for Quantum Key Distribution” Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[26] **S. Juárez**, “Constructing Stable Optical Links for Coherent Quantum Communications”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[27] **S. Ritsch**, “The hunt for Post-Quantum Password Authenticated Key Exchange”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[28] **G. Muuss**, “Connections between Complexity Theory and Cryptographic Memory-Hard functions”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[29] **F. Sisinni**, “(Un)breakable curses-re-encryption in the Fujisaki-Okamoto transform”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[30] **J. Rey-Domínguez**, “Hop-by-hop long-distance quantum key distribution with error detection”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[31] **M. R. Bolaños** et al., “Resource-efficient encoder for arbitrary time-bin state generation”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[32] **S. Kumar**, “Photonic Integrated Circuits for Scalable and Secure Quantum Key Distribution”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[33] **L. Millet**, “Impact of Interferometers Mismatch and Laser Chirp on the Performance of a Time Bin BB84 quantum Key Distribution System”, Quantum-Safe Internet workshop, Technical University of Denmark, Copenhagen (Denmark), 12-15 May 2025.

[34] **Á. Yángüez**, A. B. Grilo, “Quantum pseudoresources imply cryptography”, 15th international conference on quantum cryptography (QCRYPT2025), Sanya, Hainan, China, 25-29 August 2025.

[35] **A. Marcomini**, A. Mizutani, F. Grünenfelder, M. Curty, K. Tamaki, “Security of loss-tolerant QKD with source and receiver imperfections”, 15th international conference on quantum cryptography (QCRYPT2025), Sanya, Hainan, China, 25-29 August 2025.

[36] **V. Mannelath**, V. Zapatero, M. Curty, “Sharp finite statistics for quantum key distribution”, 15th international conference on quantum cryptography (QCRYPT2025), Sanya, Hainan, China, 25-29 August 2025.

- [37] **J. Rey-Domínguez**, M. Razavi, “Hop-by-hop long-distance quantum key distribution with error detection”, 15th international conference on quantum cryptography (QCRYPT2025), Sanya, Hainan, China, 25-29 August 2025.
- [38] **S. Juárez**, “Constructing Stable Optical Links for Coherent Quantum Communications”, Okinawa School in Physics: From quantum key distribution to the quantum internet (OSP2025), Okinawa, Japan, September 21, 2025 - October 3, 2025
- [39] **A. Marcomini**, A. Mizutani, F. Grünenfelder, M. Curty, K. Tamaki, “Loss-Tolerant Quantum Key Distribution with Detection Efficiency Mismatch”. X Workshop do Programa de Doutorado Interuniversitário em Laser, Fotônica e Visão, Universidade de Vigo, Spain (2025).
- [40] **A. Marcomini**, **S. Juárez**, M. Petrov, R. I. Woodward, T. J. Dowling, R. M. Stevenson, M. Curty, D. Rusca, “Implementation Security of TF-QKD: Fast Intensity Modulation of the Reference Light Attack and Countermeasures”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.
- [41] **S. Ritsch**, Y.-H. Huang, A. Huelsing, V. Maram, A. Saha, “Quantum-Secure Classical Protocols: Reprogramming Permutations for Tight(er) Proofs”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.
- [42] **J. Rey-Domínguez**, M. Razavi, “Rethinking Quantum Repeaters: Balancing Scalability, Feasibility, and Interoperability”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.
- [43] **S. Juárez**, **A. Marcomini**, M. Petrov, R. I. Woodward, T. J. Dowling, R. M. Stevenson, M. Curty, D. Rusca, “Implementation Security of TF-QKD: Trojan-Wavelength In the Reference Light Attacks and Countermeasures”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.
- [44] **V. Mannalath**, “Concentration bounds and satellite QKD”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.
- [45] **L. Millet**, R. Thew, B. Korzh, G. Boso, “A simple clock synchronization algorithm for time-bin quantum key distribution”, Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.
- [46] **A. Yáñez**, E. Diamanti, A. Grilo, A. Innocenzi, V. Yacoub, P. Lefebvre, “A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.
- [47] **M. R. Bolaños** et al., “GHz-rate polarization-based QKD system for fiber and satellite applications”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.

[48] **F. Sisinni**, C. Majenz, “Provable decryption failure security for practical lattice-based PKE”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.

[49] **G. Muuss**, “Query bounds are inherent for the security of memory-hard functions”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.

[50] **M. Ostuzzi**, “Algorithms for the Underdetermined MQ problem”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.

[51] **S. Kumar, A. Marcomini, L. Millet**, T. Taher, R. Houlmann, D. Cabrerizo, G. Boso, R. Thew, B. Korzh, “GHz-Rate Phase-Randomized Time-Bin QKD Source Based on a SLED Platform”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.

[52] B. Korzh, **S. Kumar, A. Marcomini**, T. Taher, **L. Millet**, “Narrowing security gaps and boosting qubit rates in quantum communication”, International Conference on Quantum Communication and Security, DIM QuantIP, Université Sorbonne Paris Nord, France, 10-20 March 2026.

[53] **J. Rey-Domínguez**, K. Azuma and M. Razavi, “Design considerations for sequential quantum repeaters with error detection”, 5th Workshop for Quantum Repeater and Networks (WQRN5), Singapore, 27-29 April, 2026.

[54] **S. Juárez** et al., “Reference-beam attacks against TF-QKD using optical injection locking” Authentication for Quantum Networks, King's College London, London, UK. 1-2 June 2026.

[55] **A. Marcomini, S. Juárez**, M. Petrov, R. I. Woodward, T. J. Dowling, R. M. Stevenson, M. Curty, D. Rusca, “On the Implementation Security of Twin-Field Quantum Key Distribution using Optical Injection Locking”. XI Workshop do Programa de Doutorado Interuniversitário em Láser, Fotónica e Visión, Universidade de Vigo, Spain (2026).

[56] **S. Kumar, A. Marcomini, L. Millet**, T. Taher, R. Houlmann, D. Cabrerizo, G. Boso, M. Curty, R. Thew, B. Korzh, “GHz-Rate Phase-Randomized Decoy state Time-Bin QKD Source Based on a SLED Platform”, 16th international conference on quantum cryptography (QCRYPT2026), Ottawa, Canada, 24-28 August 2026.

[57] A. Brzosko, Y. Lo, P. Smith, T. Paraiso, **S. Juárez**, J. Dynes, R. Woodward, M. Stevenson, A. Shields, “Overcoming the Phase Diffusion Limit in a Semiconductor Laser-based QRNG”, 16th international conference on quantum cryptography (QCRYPT2026), Ottawa, Canada, 24-28 August 2026.

[58] **S. Juárez, A. Marcomini**, M. Petrov, R. Woodward, T. Dowling, R. Stevenson, M. Curty, D. Rusca, “Reference-beam attacks against OIL-based Twin-Field QKD”, 16th international conference on quantum cryptography (QCRYPT2026), Ottawa, Canada, 24-28 August 2026.

[59] **J. Rey-Domínguez**, M. Razavi, “Quantum repeaters with error detection and sequential entanglement swapping”, 16th international conference on quantum cryptography (QCRYPT2026), Ottawa, Canada, 24-28 August 2026.

[60] L. Millet, B. Korzh, R. Thew, G. Boso, “Clock synchronization in time-bin quantum key distribution derived from a model of detection statistics under clock drift”, 16th international conference on quantum cryptography (QCRYPT2026), Ottawa, Canada, 24-28 August 2026.