

ALLEGATO B

UNIVERSITÀ DEGLI STUDI DI MILANO

selezione pubblica per n. 1 posto/i di Ricercatore a tempo determinato in tenure track (RTT)

per il settore concorsuale 01/A2 - GEOMETRIA E ALGEBRA,

settore scientifico-disciplinare MAT/02 - ALGEBRA

presso il Dipartimento di Matematica Federigo Enriques,

(avviso bando pubblicato sulla G.U. 97 del 22/12/2023) Codice concorso 5468

Alessio Meneghetti **CURRICULUM VITAE**

INFORMAZIONI PERSONALI (NON INSERIRE INDIRIZZO PRIVATO E TELEFONO FISSO O CELLULARE)

COGNOME	MENEGHETTI
NOME	ALESSIO
DATA DI NASCITA	19/04/1986

TITOLI

TITOLO DI STUDIO

(indicare la Laurea conseguita inserendo titolo, Ateneo, data di conseguimento, ecc.)

Dottore Magistrale con lode in Matematica, Università di Trento, Dipartimento di Matematica, 20 Settembre 2013

TITOLO DI DOTTORE DI RICERCA O EQUIVALENTI, OVVERO, PER I SETTORI INTERESSATI, DEL DIPLOMA DI SPECIALIZZAZIONE MEDICA O EQUIVALENTE, CONSEGUITO IN ITALIA O ALL'ESTERO

(inserire titolo, ente, data di conseguimento, ecc.)

Dottore di Ricerca Cum Laude in Matematica, Università di Trento, Dipartimento di Matematica, 25 Gennaio 2017

CONTRATTI DI RICERCA, ASSEGNI DI RICERCA O EQUIVALENTI

(per ciascun contratto stipulato, inserire università/ente, data di inizio e fine, ecc.)

- Assegno di Ricerca, MAT/02, Dipartimento di Matematica, Università di Trento, 01 Luglio 2019 - 31 Dicembre 2021, Progetto Europeo PON "Distributed Ledgers for Secure Open Communities"
- Assegno di Ricerca, MAT/02, Dipartimento di Matematica, Università di Trento, 27 Giugno 2018 - 26 Giugno 2019
- Assegno di Ricerca, MAT/02, Dipartimento di Matematica, Università di Trento, 27 Giugno 2017 - 26 Giugno 2018

ATTIVITÀ DIDATTICA A LIVELLO UNIVERSITARIO IN ITALIA O ALL'ESTERO

(inserire periodo [gg/mm/aa inizio e fine], anno accademico, ateneo, corso laurea, numero ore, ecc.)

- Corso di Dottorato “Advances in Cryptography and Codes: Advanced algebraic and geometric methods for the construction of minimal codes” (course lecturer, 5 hours), Ph.D. School of Mathematics, SSD MAT/02, A.Y. 2022-2023
- Corso di Dottorato “The interplay between algebra and randomness in Cryptography (course lecturer, 30 hours), Ph.D. School of Mathematics, SSD MAT/02, A.Y. 2020-2021
- Corso Magistrale “Discrete Fourier Analysis” (course lecturer, 42 hours), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2021-2022
- Corso Magistrale “Discrete Fourier Analysis” (course lecturer, 42 hours), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2022-2023
- Corso Magistrale “Discrete Fourier Analysis” (course lecturer, 42 hours), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2023-2024
- Corso Magistrale “Coding Theory and Applications” (assistant), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2014-2015
- Corso Magistrale “Coding Theory and Applications” (assistant), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2018-2019
- Corso Magistrale “Coding Theory and Applications” (assistant), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2019-2020
- Corso Magistrale “Coding Theory and Applications” (assistant), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2020-2021
- Corso Magistrale “Advanced Coding Theory and Cryptography” (assistant), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2015-2016
- Corso Magistrale “Advanced Coding Theory and Cryptography” (assistant), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2018-2019
- Corso Magistrale “Advanced Coding Theory and Cryptography” (assistant), M.Sc. in Mathematics, SSD MAT/02, A.Y. 2019-2020
- Corso Magistrale “Statistics of Stochastic Processes” (assistant), M.Sc. in Mathematics, SSD MAT/06, A.Y. 2014-2015

Numero di Tesi di Dottorato correntemente sotto supervisione: 3

Numero di Tesi Magistrali seguite: 27

Numero di Tesi Triennali seguite: 1

DOCUMENTATA ATTIVITÀ DI FORMAZIONE O DI RICERCA PRESSO QUALIFICATI ISTITUTI ITALIANI O STRANIERI;

(inserire anno accademico, ente, corso, periodo, ecc.)

Periodo di ricerca presso il LIRMM - Laboratoire d'informatique, de robotique et de microélectronique de Montpellier, Montpellier, Gennaio 2026-Marzo 2016, gruppo di ricerca ECO - Exact Computing, con Dr.ssa Eleonora Guerrini

DOCUMENTATA ATTIVITÀ IN CAMPO CLINICO

(indicare, data, durata, ruolo, ente presso il quale si è prestata attività assistenziale, ecc.)

REALIZZAZIONE DI ATTIVITÀ PROGETTUALE

(indicare, data, progetto, ecc.)

Progetti Europei:

- Post-Quantum Cryptography for decentralised systems, 2022-presente
PON 2014-2020 Ricerca ed Innovazione, “Contratti di Ricerca su tematiche dell’Innovazione”
Responsabile Scientifico Locale Prof. M. Sala (MAT/02)
Purpose: design of cryptographic protocols resistant against quantum threats, in particular for decentralised systems dealing with sensitive data.
- Distributed Ledgers for secure open communities (SecureOpenNets), 2019-2021
PON 2014-2020 Ricerca ed Innovazione
Responsabile Scientifico Locale Prof. M. Sala (MAT/02)
Partnership: Alkemy Tech srl, Poste Italiane SpA, OKT Srl, BV Tech SpA, Consiglio Nazionale delle Ricerche, SUBCOM srl, University of Trento, University of Calabria, Mediterranean University of Reggio Calabria
Purpose: design of cryptographically secure blockchain-based protocols for secure management of sensitive data, with focus on the compliance to GDPR.
Role: design of protocols for data integrity verification, analysis of consensus protocols, analysis of methods for blockchain scalability, study of cryptographic primitives for sensitive data management.

Progetti Nazionali e Locali:

- Istituto di Scienze della Sicurezza dell’Università degli Studi di Trento (ISSTN) 2018-2019
University of Trento
Responsabile Scientifico Locale Prof. M. Sala (MAT/02)
Purpose: research on security-related topics to enhance territorial development.
Role: research on digital security from an algebraic point of view, analysis of blockchain-based protocols, cryptography and coding theory.
- On silicon quantum optics for quantum computing and secure communications (SiQuro) 2013-2016
Bando Grandi Progetti 2012, Autonomous Province of Trento
Responsabile Scientifico Locale Prof. M. Sala (MAT/02)
Partnership: University of Trento, Fondazione Bruno Kessler (FBK), Center for Materials and Microsystems (CMM), Istituto Nazionale di Ottica (INO-CNR), ETH Zürich, III-V lab, AdvanSiD, TELS
Purpose: research and development of silicon-based quantum random number generators.
Role: statistical analysis of random bit-sequences for cryptographically-secure applications; estimation of the entropy rate of QRNGs prototypes through stochastic modelling; research on entropy extractors and their link to the theory of Boolean functions and methods from coding Theory.

Conti-Terzi e progetti aziendali:

- Sharding-based Consensus Algorithms for Distributed Ledgers, 2021
Purpose: analysis of consensus algorithms and their adaption to scalable blockchains.
Role: design and security analysis of consensus mechanisms.
- Cryptographic design of blockchain platforms, 2019-2021
Purpose: design of blockchain-based protocols capable of managing data from IoT devices.
Role: development of new consensus algorithms for sharding-based blockchain platforms.
- Post-Quantum Digital Signatures for blockchain platforms, 2019-2021
Purpose: analysis of post-quantum digital signatures to determine security parameters compatible with blockchain-based protocols.
Role: study and analysis of the security of multivariate-based post-quantum digital signatures.
- Threshold multi-signatures with offline recovery parties, 2019
Purpose: design of new cryptographically secure protocols of (t, n) -Threshold MultiSig, where the key-generation algorithm itself requires the participation of t among n players.
Role: adaptation of ECDSA and EdDSA multisig variants to allow offline participants during the key-generation phase.
- A first assessment of Takamaka blockchain platform, 2019
Purpose: analysis and implementation of cryptographic primitives for blockchain platforms.
Role: analysis of the vulnerabilities of cryptographic primitives in decentralised applications.

- Digital Notary Double-Blockchain, 2017

Purpose: study of new cryptographically secure protocols for management and integrity verification of data on blockchain.

Role: design of notarisation protocols and security analyses.

- An application of insertion/deletion codes to electronic payments, 2014

Purpose: security analysis and research on new methods for safe management of credentials in electronic payment services.

Role: analysis of the DTMF channel and design of codes for data protection against errors, insertions and deletions.

ORGANIZZAZIONE, DIREZIONE E COORDINAMENTO DI GRUPPI DI RICERCA NAZIONALI E INTERNAZIONALI, O PARTECIPAZIONE AGLI STESSI

(per ciascuna voce inserire anno, ruolo, gruppo di ricerca, ecc.)

- Partecipazione e organizzazione al gruppo di ricerca “Crittografia e Codici”, 2020-present, Unione Matematica Italiana, Research Group for Coding and Cryptography
- Membro del gruppo gruppo GNSAGA, 2019-present, Istituto Nazionale di Alta Matematica “Francesco Severi” (INDAM), Group for Algebraic and Geometric Structures and their Applications, Section Algebraic Structures and Combinatorial Geometry
- Membro dell’associazione De Componendis Cifris, 2018-present, National Association for Cryptography
- Membro del gruppo di ricerca CryptoLabTN, 2013-present, Laboratory for Industrial Mathematics and Cryptography, Dep. of Mathematics, University of Trento

TITOLARITÀ DI BREVETTI

(per ciascun brevetto, inserire autori, titolo, tipologia, numero brevetto, ecc.)

- [1] V. Di Nicola, M. Sala, A. Meneghetti, and R. Longo, “Method and apparatus for a blockchain-agnostic safe multi-signature digital asset management”, Publication number 20210158444, May 2021.
- [2] N. Massari, F. Acerbi, G. Fontana, D. Stoppa, N. Zorzi, L. Pavesi, M. Sala, A. Meneghetti, L. Gasparini, Z. Bisadi, et al., “Improved random number generator, in particular improved true random number generator”, US Patent App. 16/334,332, Jul. 2019.

ATTIVITÀ DI RELATORE A CONGRESSI E CONVEGNI NAZIONALI E INTERNAZIONALI

(inserire titolo congresso/convegno, data, ecc.)

- Cutting the GRASS: Threshold GRoup Action Signature Schemes, 06-09 May 2024, M. Battagliola, G. Borin, A. Meneghetti, E. Persichetti, Accepted at The Cryptographers’ Track at RSA Conference, San Francisco, California, USA
- LETSS sign together: Linear Equivalence Threshold Signature Scheme, 22-23 April 2023, M. Battagliola, G. Borin, A. Meneghetti, International Workshop on Code-Based Cryptography (CBCrypto 2023), Lyon, France
- (Invited Speaker) Threshold Signatures with Offline Participants, 27-28 May 2021, CryptO Conference 2021, Torino, Italy
- Characterisation of the parameters of MWS codes according to their spread, 22-25 September 2020, A. Meneghetti, W. Kadir, SEquences and Their Applications 2020 (SETA2020), Saint-Petersburg, Russia
- (Invited Speaker) A formula on the weight distribution of codes, 10 October 2019, 1st Workshop on Algebra for Cryptography (A4C2019), L’Aquila, Italy

- A survey on efficient parallelization of blockchain-based smart contracts (poster), 22 February 2019, A. Meneghetti, T. Parise, M. Sala, D. Taufer, 3rd Workshop on Trusted Smart Contracts (WTSC19), Saint Kitts, Saint Kitts and Nevis
- Two-tier blockchain timestamped notarization with incremental security, 12 February 2019, 2nd Distributed Ledger Technology Workshop (DLT19), Pisa, Italy
- Blockchain per processi aziendali in una grande azienda, 17 December 2018, CifrisChain 2018, Rome, Italy
- A two-level distributed ledger for data integrity verification, 3 May 2018, A. Ottaviano Quintavalle, A. Meneghetti, M. Sala, Euregio Blockchain Conference, Bolzano, Italy
- Security proofs for some protocols based on blockchain technology, 1 February 2018, M. Sala, A. Meneghetti
1st Distributed Ledger Technology Workshop (DLT18), Perugia, Italy
- On the Griesmer bound for nonlinear systematic codes (poster), 15-19 June 2015, Effective Methods in Algebraic Geometry 2015 (MEGA2015), Trento, Italy
- On the Griesmer bound for nonlinear codes, 13-17 April 2015, 9th International Workshop on Coding and Cryptography 2015 (WCC 2015), Paris, France
- An application of insertion/deletion codes to electronic payments, 22 December 2014, Quinto workshop di crittografia (BunnyTN 2014), Trento, Italy
- Algebraic Post-Processing for Physical RNGs (poster), 14-18 April 2014, IEEE European School of Information Theory (ESIT 2014), Tallinn, Estonia

CONSEGUIMENTO DI PREMI E RICONOSCIMENTI NAZIONALI E INTERNAZIONALI PER ATTIVITÀ DI RICERCA
(inserire premio, data, ente organizzatore, ecc.)

POSSESSO DEL DIPLOMA DI SPECIALIZZAZIONE EUROPEA RICONOSCIUTO DA BOARD INTERNAZIONALI
(relativamente a quei settori concorsuali nei quali è prevista)
(indicare diploma, data di conseguimento, ecc.)

TITOLI DI CUI ALL'ARTICOLO 24 COMMA 3 LETTERA A) E B) DELLA LEGGE 30 DICEMBRE 2010, N. 240
(indicare se contratto di tipologia A o B, Ateneo, data di decorrenza e fine contratto, ecc.)

Ricercatore a tempo determinato, legge 240/2010, art. 24 lettera A), SSD MAT/02, Dipartimento di Matematica, Università di Trento, data di decorrenza 01 Gennaio 2022 - data di fine contratto 31 Dicembre 2024, Progetto Europeo PON "Sviluppo di protocolli crittografici resistenti ad attacchi di tipo quantistico, in particolare per sistemi decentralizzati di gestione di informazioni sensibili"

PRODUZIONE SCIENTIFICA

PUBBLICAZIONI SCIENTIFICHE

(per ciascuna pubblicazione indicare: nomi degli autori, titolo completo, casa editrice, data e luogo di pubblicazione, codice ISBN, ISSN, DOI o altro equivalente)

Journal Papers

- [1] M. Battagliola, R. Longo, A. Meneghetti, and M. Sala, "Provably unforgeable threshold EdDSA with an offline participant and trustless setup", Mediterranean Journal of Mathematics, no. 20, p. 253, 2023. DOI <https://doi.org/10.1007/s00009-023-02452-9>
- [2] G. Cavicchioni and A. Meneghetti, "The weight distribution of codes over finite chain rings", Linear

Algebra and its Applications, vol. 675, pp. 90-105, 2023. DOI

<https://doi.org/10.1016/j.laa.2023.06.015>

[3] A. Meneghetti, A. Pellegrini, and M. Sala, "On the equivalence of two post-quantum cryptographic families", *Annali di Matematica Pura ed Applicata* (1923 -), no. 202, pp. 967-991, 2023. DOI <https://doi.org/10.1007/s10231-022-01267-x>

[4] M. Battagliola, R. Longo, A. Meneghetti, and M. Sala, "Threshold ECDSA with an offline recovery party", *Mediterranean Journal of Mathematics*, vol. 19, no. 4, 2022. DOI <https://doi.org/10.1007/s00009-021-01886-3>

[5] G. D'Alconzo, A. Meneghetti, and P. Piasenti, "Security issues of CFS-like digital signature algorithms", Accepted for publication in *Journal of Discrete Mathematical Sciences & Cryptography*, 2022, preprint: <https://arxiv.org/abs/2112.00429>.

[6] A. Flamini, R. Longo, and A. Meneghetti, "Cob: A leaderless protocol for parallel byzantine agreement in incomplete networks", *Distributed and Parallel Databases*, pp. 1-38, 2022. DOI <https://doi.org/10.1007/s10619-022-07410-0>

[7] A. Flamini, R. Longo, and A. Meneghetti, "Multidimensional byzantine agreement in a synchronous setting", *Applicable Algebra in Engineering, Communication and Computing*, 2022. DOI <https://doi.org/10.1007/s00200-022-00548-5>

[8] R. Longo, C. Mascia, A. Meneghetti, G. Santilli, and G. Tognolini, "Adaptable cryptographic primitives in blockchains via smart contracts", *Cryptography*, vol. 6, no. 3, p. 32, 2022. DOI <https://doi.org/10.3390/cryptography6030032>

[9] A. Meneghetti, M. Pellegrini, and M. Sala, "A formula on the weight distribution of linear codes with applications to AMDS codes", *Finite Fields and Their Applications*, vol. 77, p. 101 933, 2022. DOI <https://doi.org/10.1016/j.ffa.2021.101933>

[10] A. Meneghetti, M. Sala, and D. Taufer, "A new ECDLP-based PoW model", *Mathematics*, vol. 8, no. 8, p. 1344, 2020. DOI <https://doi.org/10.3390/math8081344>

[11] A. Meneghetti, M. Sala, and D. Taufer, "A survey on PoW-based consensus", *Annals of Emerging Technologies in Computing (AETiC)*, pp. 2516-0281, 2020. DOI: 10.33166/AETiC.2020.01.002

[12] R. Aragona and A. Meneghetti, "Type-preserving matrices and security of block ciphers", *Advances in Mathematics of Communications*, vol. 13, no. 2, p. 235, 2019. Doi: 10.3934/amc.2019016

[13] A. Meneghetti, T. Parise, M. Sala, and D. Taufer, "A survey on efficient parallelization of blockchain-based smart contracts", *Annals of Emerging Technologies in Computing (AETiC)*, vol. 3, no. 5, pp. 9-16, 2019. DOI: 10.33166/AETiC.2019.05.002

[14] A. Meneghetti, A. O. Quintavalle, M. Sala, and A. Tomasi, "Two-tier blockchain timestamped notarization with incremental security", *Annals of Emerging Technologies in Computing (AETiC)*, pp. 2516-0281, 2019. DOI: 10.33166/AETiC.2019.05.004

[15] H. Xu, N. Massari, L. Gasparini, A. Meneghetti, and A. Tomasi, "A SPAD-based random number generator pixel based on the arrival time of photons", *Integration*, vol. 64, pp. 22-28, 2019. <https://doi.org/10.1016/j.vlsi.2018.05.009>

[16] A. Tomasi, A. Meneghetti, N. Massari, L. Gasparini, D. Rucatti, and H. Xu, "Model, validation, and characterization of a robust quantum random number generator based on photon arrival time comparison", *Journal of Lightwave Technology*, vol. 36, no. 18, pp. 3843-3854, 2018. DOI 10.1109/JLT.2018.2829210

[17] A. Tomasi, A. Meneghetti, and M. Sala, "Code generator matrices as RNG conditioners", *Finite Fields and Their Applications*, vol. 47, pp. 46-63, 2017. DOI <https://doi.org/10.1016/j.ffa.2017.05.005>

[18] Z. Bisadi, A. Meneghetti, A. Tomasi, A. Tengattini, G. Fontana, G. Pucker, P. Bettotti, M. Sala, and L. Pavesi, "Generation of high quality random numbers via an all-silicon-based approach", *physica status solidi (a)*, vol. 213, no. 12, pp. 3186-3193, 2016. DOI <https://doi.org/10.1002/pssa.201600298>

[19] E. Guerrini, A. Meneghetti, and M. Sala, "On optimal nonlinear systematic codes", *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3103-3112, 2016. DOI: 10.1109/TIT.2016.2553142

Proceedings

[1] M. Battagliola, G. Borin, A. Meneghetti, and E. Persichetti, "Cutting the GRASS: Threshold GRoup Action Signature Schemes", in *CT-RSA proceedings*, to be published by Springer in its LNCS series (accepted at The Cryptographers' Track at RSA Conference, San Francisco, California), preprint: <https://eprint.iacr.org/2020/023.pdf>, 2024.

[2] M. Battagliola, A. Galli, R. Longo, and A. Meneghetti, "A provably-unforgeable threshold Schnorr signature with an offline recovery party", in *DLT2022 at Itasec 2022, CEUR Workshop Proceedings*,

2022. ISSN 16130073

[3] A. Flamini, R. Longo, and A. Meneghetti, "Cob: A consensus layer enabling sustainable sharding-based consensus protocols", in *Proceedings of DLT2022 at Itasec 2022, CEUR Workshop Proceedings*, 2022. ISSN 16130073

[4] A. Meneghetti and W. K. Kadir, "Characterisation of the parameters of maximum weight spectrum codes according to their spread", in *SETA 2020*,

<https://seta-2020.org/assets/files/program/paper/paper-13.pdf>, 2020.

[5] A. Meneghetti, M. Sala, and D. Taufer, "A note on an ECDLP-based PoW model", in *DLT@ITASEC*, 2020. ISSN 16130073

[6] N. Massari, L. Gasparini, M. Perenzoni, G. Pucker, A. Tomasi, Z. Bisadi, A. Meneghetti, and L. Pavesi, "A compact TDC-based quantum random number generator", in *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, IEEE, 2019, pp. 815-818. DOI 10.1109/ICECS46596.2019.8964941

[7] A. Meneghetti, A. O. Quintavalle, M. Sala, and A. Tomasi, "Two-tier blockchain timestamped notarization with incremental security", in *CEUR Workshop Proceedings*, Vol. 2334, 2019, pp. 32-42. ISSN 16130073

[8] M. Nicola, L. Gasparini, A. Meneghetti, and A. Tomasi, "A SPAD-based random number generator pixel based on the arrival time of photons", in *2017 New Generation of CAS (NGCAS)*, IEEE, 2017, pp. 213-216. DOI 10.1109/NGCAS.2017.27

[9] N. Massari, L. Gasparini, A. Tomasi, A. Meneghetti, H. Xu, D. Perenzoni, G. Morgari, and D. Stoppa, "A 16×16 pixels SPAD-based 128 – M b/s quantum random number generator with –74dB light rejection ratio and –6.7ppm/°C bias sensitivity on temperature", in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, IEEE, 2016, pp. 292-293. DOI 10.1109/ISSCC.2016.7418022

[10] E. Bellini and A. Meneghetti, "On the Griesmer bound for nonlinear codes", in *Proceedings of WCC*, 2015.

[11] Z. Bisadi, A. Meneghetti, G. Fontana, G. Pucker, P. Bettotti, and L. Pavesi, "Quantum random number generator based on silicon nanocrystals led", in *Integrated Photonics: Materials, Devices, and Applications III*, International Society for Optics and Photonics, vol. 9520, 2015, p. 952 004. DOI 10.1117/12.2179027

[12] Z. Bisadi, A. Meneghetti, A. Tomasi, G. Fontana, A. Tengattini, P. Bettotti, G. Pucker, M. Sala, and L. Pavesi, "A post-processing free si nanocrystals based quantum random number generator", in *European Quantum Electronics Conference*, Optical Society of America, 2015, EA P 32. ISSN 21622701

[13] N. Massari, L. Gasparini, A. Tomasi, A. Meneghetti, D. Perenzoni, and D. Stoppa, "A low bias variation SPAD-based pixel for a quantum random generator", in *Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*, International Society for Optics and Photonics, vol. 9648, 2015, p. 964 813. DOI 10.1117/12.2195086

[14] A. Meneghetti, G. Boato, and F. G. De Natale, "Improved image copyright protection scheme exploiting visual cryptography in wavelet domain", in *Image Processing: Algorithms and Systems XI*, International Society for Optics and Photonics, vol. 8655, 2013, p. 865 504. DOI 10.1117/12.2005070

[15] D. Stucki, S. Burri, E. Charbon, C. Chunnillall, A. Meneghetti, and F. Regazzoni, "Towards a high-speed quantum random number generator", in *Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X*, International Society for Optics and Photonics, vol. 8899, 2013, 88990R DOI 10.1117/12.2029287

Books, Chapters and Contributions in Books

[1] N. Di Chiano, R. Longo, A. Meneghetti, and G. Santilli, "A survey on NIST PQ signatures", in *cryptOrino 2021*, ser. *Collectio Cipharrum*, Aracne, 2023, pp. 61-86. ISBN 979-12-218-0831-5 (cartaceo) 979-12-218-0832-2 (pdf)

[2] A. Meneghetti, P. Peterlongo, and M. Sala, "Encoding in the DTMF channel for two-channel authentication", in *Physical and Data-Link Security Techniques for Future Communication Systems*, Springer, 2016, pp. 205-212. DOI <https://doi.org/10.1007/978-3-319-23609-4>

Data

18/01/2024

Luogo

Trento