Post Quantum Cryptography Research Lines in the Italian Center for Security and Rights in Cyberspace

Alessandro Barenghi[0000−0003−0840−6358] and Gerardo Pelosi[0000−0002−3812−5429]

Politecnico di Milano, Milano, 20133, Italy
{alessandro.barenghi, gerardo.pelosi}@polimi.it

Abstract. The Italian foundation for Security and Rights in Cyberspace (SERICS) is in charge of managing the current, broad range, research in a variety of computer security domains, ranging from strictly computer related aspects, such as OS and Virtualization security, to the development of new cryptographic techniques, up to tackling human, social and legal problems related to computer security and privacy. The SERICS project is founded by the Italian National Recovery and Resilience Plan (NRRP), which in turn receives funding from the EU - NextGenerationEU programme. The SERICS foundation is managing the STRIDE project, to tackle the aforementioned research challenges. In the context of the STRIDE projects, a cascade call was made to tackle specific aspects of the overall reseach challenges. The two-years AQuSDIT project, winner of the aforementioned cascade call, aims to tackle the current open problems in the digital identity realm, with a particular focus on resistance to quantum computer-based attacks, and ledger-based technologies for identification and supply chain tracking. In this context, the research activities at Politecnico di Milano focus on the design of post quantum cryptosystems, and their secure and efficient realization as hardware components, either in the form of full accelerators, or support to existing computing infrastructures. In the following, we will present an overview of the research activities of the 2-year AQuSDIT project, together with an outlook on the first research results which have been obtained by the group of participants from Politecnico di Milano.

Keywords: Computer security · Cryptography · Post quantum cryptography.

1 Introduction

The Italian SERICS Foundation [30] - Security and Rights in CyberSpace was established to be the entity implementing the extended partnerships among national research institutions and companies, to submit funding applications for the development of fundamental scientific research projects - under the Italian National Recovery and Resilience Plan (NRRP), Mission 4 “Education and Research” - Component 2 “From Research to Enterprise” - Investment 1.3, funded

by the European Union - NextGenerationEU [19]. The creation of the whole structure received an important organizational push from the Cybersecurity Italian National Lab, which in turn represents the coordination point of a network of 59 interconnected entities, which include the main Italian Universities, Research Institutes and Military Academies. The Cybersecurity Italian National Lab has played a key role in gathering the Italian cybersecurity community around the unique SERICS foundation structure that will be the recipient of funds for research in one of the most relevant fields of this century, that is cybersecurity. From an operative perspective, the SERICS foundation aggregates activities across ten different scientific fields, and it is organised according to a Hub and Spoke model. The Hub is meant to validate and manage the research programmes, whose activities will be led by the Spokes, which in turn include universities, research organizations and companies to build a synergy between the scientific communities and the industrial world. The 10 spokes are focused on 10 thematic areas of interest, which are: *Human, social and legal aspects*, *Misinformation and Fake News*, *Attacks and Defences*, *Operating Systems and Virtualization Security*, *Cryptography and Distributed Systems Security*, *Software and Platform Security*, *Infrastructure Security, Risk Management and Governance*, *Securing Digital Transformation*, *Data Governance and Protection*. The objectives of the projects developed by the partnerships in each spoke are focused on identifying key problems in computer and network security and privacy that cause societal harm, economic losses and hinder the adoption of smart city technologies. Each project consortium is the result of a planning action made by the SERICS foundation that led to the definition of a broad research agenda that as previously mentioned, encompasses technical, legal, and societal issues related to security and privacy and includes the best academic and industrial researchers with the expertise needed to make progress on these issues.

In particular, Spoke 5 is primarily concerned with research activities in the domains of cryptography and distributed system security. Given the vastness of these domains and the necessity of identifying concrete objectives aimed at obtaining long-term results of high technological value and possible impact on the country, the activities of this spoke recognize the necessity of coexistence of two distinct yet interrelated souls. Among the subtopics *(i)* cryptographic primitives and protocols, *(ii)* foundational cryptography and cryptanalysis, *(iii)* post-quantum cryptography, *(iv)* digital identity, authentication, and accountability, and *(v)* distributed ledgers and blockchain, the two main directions are the continuous search for advancing the knowledge in all the fields mentioned above and the plan to apply this investigative approach to applied research goals with low- and medium-term societal impacts. Such an objective is pursued by implementing a single unifying project, named STRIDE - *Secure and TRaceable Identities in Distributed Environments*, focused on the notion of digital identification and tracing, with an emphasis on unconventional perspectives. STRIDE project as well as the EU funded projects pursued by other spokes received the needed financial support from the European Commission with the funding mechanism named “Financial Support for Third Parties (FSTP)”, which has been envisioned

to distribute 80% of the public funding, received by the subject in charge of pursuing the research activities in the first place, through issuing further open calls to the end of creating a domino effect, where funding flows from one EC funded project to another, enlarging effectively the set of relevant competencies contributing to the digital innovation. However, the performance of the activities pursued in the projects selected with a cascade call is critically evaluated, with a keen focus on deliverables and the successful achievement of Key Performance Indicators (KPIs). In response to the cascade call issued by SERICS-Spoke 5, a Consortium composed by 10 Italian Universities (Politecnico di Milano, Università di Camerino, Università dell'Insubria, Università di Perugia, Università di Pisa, Università Politecnica delle Marche, Università di Trento, Università di Reggio Calabria, Università di Palermo, Università di Roma 3), gathering competencies in mathematics, physics, computer science, computer engineering, telecommunications and law, proposed to pursue the research activities related to post quantum cryptographic techniques and technologies that realize one of the pillars of the 2-year project (2024–2025) named AQuSDIT - *Advanced and Quantum-safe Solutions for Digital Identity and digital Tracing.*

2 AQuSDIT Project

Cryptography is a fundamental discipline for safeguarding the integrity and confidentiality of data in a multitude of contexts, including critical infrastructure, business applications, and personal data management. The availability of modern and robust cryptographic tools is also crucial for the competitiveness and attractiveness of Italian companies and institutions. Moreover, cryptography is now a pivotal component in the functioning of public administration, defense, and social security. Despite their continued use, traditional cryptographic tools are becoming inadequate to address modern challenges such as the need to protect data at rest (secure storage), the need to protect data in transit (secure communication), and the need to protect data in use (secure computation). These challenges are to be considered in combination with the technological advancements in quantum computing and decentralized systems, calling for substantial investment in research, development, and education to enable the medium- and long-term design and implementation of robust cryptographic tools that can be used as building blocks for protecting data in cyberspace. Cryptography is also at the basis of modern decentralized infrastructures, which are commonly referred to as blockchains. These technologies, which originated with the introduction of cryptocurrencies, are now widespread and can be applied in a wide variety of contexts: supply chain tracking, electronic voting, and certification of artworks. Cryptographic primitives and protocols provide the foundation for the security and immutability of such digital infrastructures. Consequently, they must be adapted and modernized to withstand new threats, including those posed by quantum computing. This project aims to strengthen the national community through the development, validation, and implementation of cryptographic tools and innovative blockchain technologies to address the above challenges, with par-

ticular reference to digital identity and digital traceability applications.
The research will be structured along two main lines:

(1) The design, analysis, and experimental validation of new cryptographic primitives and protocols capable of withstanding quantum computer-based attacks for application in digital identity systems.
(2) The design, analysis, and experimental validation of new methods based on distributed ledger technologies for digital identification of things or people and for traceability of products and processes.

2.1 Originality, methodology, and organization

The research activity will address some open challenges that are recognized to be of significant interest by the national and international scientific community. Such challenges include:

- The definition and validation of new asymmetric cryptographic primitives, with a particular focus on digital signatures. The aim is to develop primitives that are capable of withstanding quantum computer-based attacks and achieve higher levels of security and efficiency than those currently available in the state of the art. This will be achieved aiming at reducing the size of digital signatures and the size of the corresponding public verification keys.
- The definition and validation of new zero-knowledge identification protocols (ZK-IDs) that offer resistance to quantum computer-based attacks and achieve better performance than those currently available in the state of the art, in terms of key size and amount of information transmitted, is also a key objective.
- The definition and validation of functional encryption methods that enable the disclosure of secret data functions in a concise and publicly verifiable manner, with numerous applications in the areas of distributed systems, blockchain, and distributed ledger technologies.
- The definition of new decentralized protocols and systems, based on blockchain and distributed ledger technologies, to overcome the fragmentation of existing state of the art solutions and define common and scientifically validated approaches for use in applications for digital identity and traceability of products and processes.
- The study and definition of techniques for attacking cryptographic primitives and protocols that provide the foundations for decentralized systems, with a particular interest being taken into systems for self-sovereign identity, electronic voting, digital currency and traceability.
- The study of new models and solutions for advanced blockchain-based applications that support traceability, transparency, verifiability and accountability, possibly based on paradigms of self-sovereign identity.
- The analysis of protocols to reconcile privacy and identification needs in distributed applications (including those based on location and proximity), possibly based on models of self-sovereign identity and zero-knowledge proof.

- The definition of methods and protocols for action identification (supply chain, notarization, process tracking) possibly based on smart contracts with automatic synthesis and security verifiable.
- The definition of smart contract specification techniques and new model-driven approaches for design, execution and auditing of business processes on blockchain platforms.

The methodology that will be adopted in addressing the research challenges described above will be strictly bound to the scientific method, and aimed at producing reliable and verifiable knowledge advancement. It will start from the analysis of existing models and the development of new models for the solutions, algorithms and protocols under study, while defining which key performance indicators (KPIs) are suitable to characterize them. Typical information engineering methodologies will be used to design new solutions and improve existing ones, as well as to implement the new solutions for experimental validation. The scientific activity and its findings will be documented in scientific papers proposed for publication in proceedings of national and international conferences and workshops and in scientific journals of international relevance. Scientific publications resulting from the project activities will be made available in open access, and following the principles of the San Francisco Declaration on Research Assessment (DORA).

Organization. Two main research lines on "Quantum-safe cryptographic primitives and protocols for digital identity" (RL1) and "Advanced digital identification and tracing and distributed ledger technologies" (RL2) will be pursued by the consortium members, maintaining four milestones, at months 4, 8, 19 and 24, to provide detailed deliverables and artifacts. The research activities of RL1 will aim to achieve the following objectives.

- RL1.O1. Design and implement post-quantum digital signature and cryptographic systems and public key cryptography based on lattices and codes, as per the STRIDE call on lattices and code-based, with or without homomorphic properties. This will be done taking into account their computational and engineering security as well as hardware and software tradeoffs in their practical implementation.
- RL1.O2. Design code-based techniques for blockchain security.
- RL1.O3. Design of functional and post-quantum cryptography, and realization of related hardware support.
- RL1.O4. Design and implementation of secure (quantum-safe) cryptographic mechanisms for distributed systems. This includes advanced cryptographic primitives (e.g., homomorphic/functional cryptography.) cryptography), multiparty computation security, and the design of new cryptographic primitives.

The research activities of RL2 will aim to achieve the following objectives.

- RL2.O1. New models and solutions for advanced blockchain-based applications supporting traceability, transparency, auditability, and accountability, possibly based on self-sovereign-identity paradigms. Protocols to rec-

oncile privacy and identification needs in distributed applications (including location-based and proximity-based), possibly based on self-sovereign-identity models and zero-knowledge proofs. Legal aspects should also be addressed concerning both digital identity and privacy.
- RL2.O2. Methods and protocols for action identification (supply chain, notarization, process tracing) possibly based on smart contracts with automatic synthesis and verifiable security.
- RL2.O3. Study of methodologies for secure smart contracts: secure design, runtime enforcement techniques, innovative off-chain models and protocols that enable the secure and efficient execution of smart contracts.
- RL2.O4. Study of multiple blockchain platforms and generation of related smart contracts. Model-driven techniques for the design, development, and execution of business process-based applications should be adopted.

3 Activities at Politecnico di Milano and Preliminary Results

The research activities of the group of participants from Politecnico di Milano will be focused entirely on the topics included in RL1 - "Quantum-safe cryptographic primitives and protocols for digital identity".

Motivation and State of the Art. The advent of large-scale quantum computing has the potential to compromise the security of digital identities due to its ability to circumvent the cryptographic algorithms that currently underpin secure communication and digital identity systems. The main risks are:

(i) Compromising Digital Certificates: digital certificates play a pivotal role in binding digital identities to the means of verifying validating the signatures made by them, and allowing them to entertain confidential communications. For a quantum computer-enabled attacker it would be trivial to obtain the private signing key corresponding to a RSA or ECDSA public verification key contained in a certificate, in turn allowing her to impersonate the subject of the certificate itself. Similarly, if the certificate is binding an identity to a public encryption key, the attacker would be able to retrieve the corresponding private decryption key, jeopardizing secure communications.

(ii) The *store now, decrypt later threat*: The potential exists for quantum computers to decrypt encrypted data that was intercepted in the past. If an attacker stores encrypted communication until a quantum computer is available, they could use quantum algorithms to decrypt the information. This puts previously intercepted data at risk of being exposed.

(iii) Identity Theft and Fraud: Quantum computing can enable attackers to break the encryption protecting personal information like passwords and credit card numbers. This could lead to identity theft, fraud, and unauthorized access to personal accounts or systems.

Several industry standards are currently being developed and evaluated for post-quantum cryptography. Although the field is still evolving, there are some of the

major standardization organizations and initiatives that are actively contributing to the development of industry standards for post-quantum cryptography. Their efforts aim to provide new guidelines, new algorithms, and updated protocols that will ensure the security of digital systems and communications in the presence of powerful quantum computers. The research and development of post-quantum cryptography are currently witnessing the creation of several national and industry standards. The US National Institute of Standards and Technology (NIST) has been leading a standardization process for post-quantum cryptography, started in late 2016, to evaluate and select quantum-resistant cryptographic algorithms [25]. The initiative evolved over four rounds of public scrutiny and selection among the candidates, discarding either the ones affected by cryptanalytic breaks, or the ones which exhibit worse performance figures (execution times, or size of the signatures/ciphertexts). Upon closure of the third round, NIST has selected four algorithms which it will standardize as a result of the Post-Quantum Cryptography (PQC) Standardization Process: CRYSTALS–Kyber, along with three digital signature schemes: CRYSTALS–Dilithium, FALCON, and SPHINCS$^+$. The standardization process is continuing with a fourth round, involving alternate candidates for encryption schemes, as the only selected one after the third round relies on problems related to finding the closest vector in a finite dimensional lattice. The decision to have a fourth round was taken with the intent of standardizing alternatives to CRYSTALS-Kyber relying on alternative computationally hard problems, such as the ones coming from coding theory. Finally, we note that the International Organization for Standardization (ISO) has established a working group, ISO/IEC JTC 1/SC 27/WG 2, dedicated to the standardization of quantum-resistant cryptographic algorithms.

Code-based Cryptosystem Design. The research on the design of cryptosystems based on computationally hard problems coming from coding theory is currently tackled from different directions at Politecnico di Milano.

The first one involves quantifying the amount of cryptanalytic efforts required to solve computationally hard problems on which post-quantum cryptosystems are built. Indeed, while the computational complexity of the best current solvers for the *syndrome decoding problem* on random codes, currently one of the most popular candidates to build code-based cryptosystems, is exponential in the number of errors, finite regime estimates provide the means to match the security margin provided by symmetric ciphers without the need of sacrificing performance in the designed cryptosystem. In this direction, the estimation of the finite-regime, concrete quantum cryptanalytic effort required to break code based cryptosystems, started from the design of a quantum algorithm to speed up a combinatorial search taking place in Lee and Brickell's Information Set Decoding [23] (ISD) cryptanalytic technique [27]. This work lead to the acceleration of a full ISD algorithm (namely, the one devised by Prange) in [26,28,29]. Further investigations have lead to a complete description of a quantum walk approach to solve the subset sum problem [6], a key component to design a quantum circuit for the currently most advanced ISD techniques, such as the ones proposed by Both and May in [17]. These investigations allow to provide

reliable parameters (e.g., key sizes) for post-quantum cryptosystems, as closed-formulas to determine the quantum gate count of a cryptanalytic approach can be employed in an automated parameter space exploration, following the approach employed during the design of LEDACrypt [10,11]. A further improvement point for post-quantum encryption algorithms, such as LEDACrypt and the current fourth round candidate BIKE is represented by accurate estimates of the decryption failure rate, due to a decoding failure in the underlying bit flipping decoder. Decoding failures have a direct impact on the security, revealing information on the private key being employed in the decryption procedure. At Politecnico di Milano, recent advancements on providing accurate and reliable estimates for the decoding failure rate of bit flipping decoders [1] allow for improvements up to 30% in keysize with respect to the best previous bounds [12]. A different direction being pursued in Politecnico di Milano is the design of post quantum signature schemes, relying on the Fiat-Shamir transformation [20] to turn instances of a zero-knowledge interactive identification protocol into digital signatures. Indeed, such an approach allows to use instances of a problem which is computationally hard also for a quantum computer, where the problem instance itself becomes the public verification key of the signature scheme, while its solution represents the private signature key. The framework provides a way to prove, non interactively, the knowledge of the private signature key to anyone willing to verify the signature, without revealing provably anything but the fact that the signer knows the private key. The key generation process, given the intractability of the computational problem, starts by randomly sampling the private key (i.e., the problem solution) and then constructing a problem around it. In this direction, Politecnico di Milano is currently active in two signature schemes, LESS [8] and CROSS [9], both relying on the Fiat-Shamir transformation, and two separate, coding theory related hard problems, namely linear code equivalence for LESS, and restricted syndrome decoding for CROSS. The linear code equivalence problem employed in LESS allows greater flexibility in building signature schemes with richer features [14], while the NP-complete nature of the restricted syndrome decoding problem provides sound guarantees on the impracticality of a polynomial time solver [13].

Code-based Cryptosystem Engineering. Post quantum cryptosystem engineering requires both to design implementations which provide good resource-performance tradeoffs, and to provide protection against implementation attacks, among which, a prime threat is represented by *side channel attacks*. Post quantum cryptosystems, both code-based ones and lattice-based ones require efficient arithmetic operations among matrices (e.g., matrix- vector multiplications). However, it is a very common choice, in order to improve the computation speed of the cryptosystems, to select matrices with a particular property, i.e., block circulant matrices. Block circulant matrices are built splitting a rectangular matrix in square equally sized blocks. Each square block is in turn a square matrix that is fully defined by its first row, as all other rows are obtained from cyclic shifts of the first row itself. It can be proven that such matrices are isomorphic to the one of the remainders of polynomials with coefficients taken over

the same field as the matrix elements, divided by $x^n - 1$, where n is the length of the side of the square matrix. Properties similar to the ones of block circulant matrices can also be obtained considering directly polynomial rings modulo $x^n + 1$, which behave, arithmetically speaking, in a similar fashion.

At Politecnico di Milano, these facts were exploited to the design unified polynomial multipliers [3,5] supporting multiple lattice-based cryptosystems, in particular, different NTRU variants [22,18] and CRYSTALS-Kyber. The research efforts in designing hardware implementations of post quantum cryptosystems lead to the development of a complete hardware accelerator [2] for the NTRU cryptosystem proposal to the NIST standardization effort [18]. While not being selected for standardization, NTRU is explicitly considered by NIST a sound alternative to CRYSTALS-Kyber, in case the patent issues surrounding Kyber are a hindrance to its deployment. A further research direction pursued at Politecnico di Milano is the one of implementing code-based post quantum cryptosystems. The efforts in this direction have lead to the design of a full cryptographic accelerator for the HQC cryptosystem [4,7]. HQC [24], currently one of the three remaining candidates for the fourth round of NIST's standardization effort, is one of the few existing cryptosystems that has a direct security reduction to a computationally hard problem, in the regime where the parameters of the cryptosystem are selected. Furthermore, its efficient arithmetic choice (binary polynomials) allow for compact and high performing implementations.

The sound engineering of post quantum cryptosystems also requires to tackle the issue of side channel attacks. This class of techniques exploits the measurement of physical parameters from a cryptosystem implementation, such as power consumption, electromagnetic radiations and computation time, to extract information from the computation itself. Typically the attacker attempts to deduce either the value of an encrypted message, or a private key, regardless of whether it is a signature or decryption key, from side channel information. A further step forward with respect to the aforementioned approach is to induce errors in the computation of a cryptographic primitive. While these errors will likely result in an unusable result (e.g., a mangled ciphertext, or an incorrect signature), the attacker may be able to derive useful information by either comparing the result with the corresponding correct one, or inferring information on the private key from the erroneous values. Such side channel attack techniques, known as fault attacks, have steadily proven to be extremely effective in disrupting the security guarantees of pre- and post-quantum cryptosystems alike [15,21,31]. In this direction, the research activity at Politecnico di Milano is tackling the study of the effectiveness of fault attacks against post-quantum cryptosystems, with a special focus on signature schemes [16]. Indeed, signature schemes built with the Fiat-Shamir transform start from a zero knowledge interactive identification scheme, which in principle, provides no information whatsoever to the attacker, when run interactively. However, the introduction of faults in the computation of the corresponding signature scheme may lead to the disclosure of the private key, or allow the splicing of a valid signature from its legitimate message, making the attacker able to reuse the said signature on a different document [16].

4 Concluding Remarks

Advancing the state of the art in computer security requires to tackle a variety of challenges, among which, the ones related to providing quantum computing resistant alternatives to current asymmetric cryptographic primitives. In this work, we described the current research directions of the Politecnico di Milano group, highlighting the research efforts in designing and engineering secure and efficient post quantum cryptosystems.

Acknowledgements. This work was supported in part by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

References

1. Annechini, A., Barenghi, A., Pelosi, G.: Bit-flipping Decoder Failure Rate Estimation for (v,w)-regular Codes. In: IEEE International Symposium on Information Theory, ISIT 2024, July 7–12, Athens, Greece, 2024. pp. 1–6. IEEE (2024)
2. Antognazza, F., Barenghi, A., Pelosi, G., Susella, R.: A Flexible ASIC-Oriented Design for a Full NTRU Accelerator. In: Takahashi, A. (ed.) Proceedings of the 28th Asia and South Pacific Design Automation Conference, ASPDAC 2023, Tokyo, Japan, January 16-19, 2023. pp. 591–597. ACM (2023), https://doi.org/10.1145/3566097.3567916
3. Antognazza, F., Barenghi, A., Pelosi, G., Susella, R.: An Efficient Unified Architecture for Polynomial Multiplications in Lattice-Based Cryptoschemes. In: Mori, P., Lenzini, G., Furnell, S. (eds.) Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, February 22-24, 2023. pp. 81–88. SciTePress (2023), https://doi.org/10.5220/0011654200003405
4. Antognazza, F., Barenghi, A., Pelosi, G., Susella, R.: A High Efficiency Hardware Design for the Post-Quantum KEM HQC. In: IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2024, Washington, DC, USA, May 6-9, 2024. pp. 431–441. IEEE (2024), https://dx.doi.org/10.1109/host55342.2024.10545409
5. Antognazza, F., Barenghi, A., Pelosi, G., Susella, R.: Performance and Efficiency Exploration of Hardware Polynomial Multipliers for Post-Quantum Lattice-Based Cryptosystems. SN Comput. Sci. **5**(2), 212 (2024), https://doi.org/10.1007/s42979-023-02547-w
6. Antognazza, F., Barenghi, A., Pelosi, G., Susella, R.: Poster: A versatile and unified hqc hardware accelerator. In: 61st ACM/IEEE Design Automation Conference (DAC '24), June 23–27, 2024, San Francisco, CA, USA. ACM (2024), https://doi.org/10.1145/3649329.3657337
7. Antognazza, F., Barenghi, A., Pelosi, G., Susella, R.: Poster: A versatile and unified hqc hardware accelerator. In: 5th ACNS Workshop on Secure Cryptographic Implementation (SCI 2024) - n Martin Andreoni (Editor) Applied Cryptography and Network Security Workshops. ACNS 2024 Satellite Workshops, AIBlock, AIHWS, AIoTS, SCI, AAC, SiMLA, LLE, and CIMSS. Lecture Notes in Computer Science, vol. 14586–14587. Springer (2024), https://doi.org/10.1007/BFb0054868
8. Baldi, M., Barenghi, A., Beckwith, L., Biasse, J.F., Esser, A., Gaj, K., Mohajerani, K., Pelosi, G., Persichetti, E., Saarinen, M., Santini, P., Wallace, R.: Linear Equivalence Signature Scheme. https://www.less-project.com/

9. Baldi, M., Barenghi, A., Bitzer, S., Karl, P., Manganiello, F., Pavoni, A., Pelosi, G., Santini, P., Schupp, J., Slaughter, F., Wachter-Zeh, A., Weger, V.: Codes and Restricted Objects Signature Scheme. https://www.cross-crypto.com/
10. Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., Santini, P.: LEDAkem: A Post-quantum Key Encapsulation Mechanism Based on QC-LDPC Codes. In: Lange, T., Steinwandt, R. (eds.) Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. Lecture Notes in Computer Science, vol. 10786, pp. 3–24. Springer (2018), https://doi.org/10.1007/978-3-319-79063-3_1
11. Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., Santini, P.: LEDAcrypt: QC-LDPC Code-Based Cryptosystems with Bounded Decryption Failure Rate. In: Baldi, M., Persichetti, E., Santini, P. (eds.) Code-Based Cryptography - 7th International Workshop, CBC 2019, Darmstadt, Germany, May 18-19, 2019, Revised Selected Papers. Lecture Notes in Computer Science, vol. 11666, pp. 11–43. Springer (2019), https://doi.org/10.1007/978-3-030-25922-8_2
12. Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., Santini, P.: Performance Bounds for QC-MDPC Codes Decoders. In: Wachter-Zeh, A., Bartz, H., Liva, G. (eds.) Code-Based Cryptography - 9th International Workshop, CBCrypto 2021, Munich, Germany, June 21-22, 2021 Revised Selected Papers. Lecture Notes in Computer Science, vol. 13150, pp. 95–122. Springer (2021), https://doi.org/10.1007/978-3-030-98365-9_6
13. Baldi, M., Bitzer, S., Pavoni, A., Santini, P., Wachter-Zeh, A., Weger, V.: Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem. In: Tang, Q., Teague, V. (eds.) Public-Key Cryptography - PKC 2024 - 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15-17, 2024, Proceedings, Part II. Lecture Notes in Computer Science, vol. 14602, pp. 243–274. Springer (2024), https://doi.org/10.1007/978-3-031-57722-2_8
14. Barenghi, A., Biasse, J., Persichetti, E., Santini, P.: On the computational hardness of the code equivalence problem in cryptography. Adv. Math. Commun. **17**(1), 23–55 (2023), https://doi.org/10.3934/amc.2022064
15. Barenghi, A., Breveglieri, L., Koren, I., Naccache, D.: Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. Proc. IEEE **100**(11), 3056–3076 (2012), https://doi.org/10.1109/JPROC.2012.2188769
16. Barenghi, A., Pelosi, G.: Fault Attacks Friendliness of Post-quantum Cryptosystems. In: Workshop on Fault Detection and Tolerance in Cryptography, FDTC 2023, Prague, Czech Republic, September 10, 2023. p. 1. IEEE (2023), https://doi.org/10.1109/FDTC60478.2023.00006
17. Both, L., May, A.: Decoding Linear Codes with High Error Rate and Its Impact for LPN Security. In: Lange, T., Steinwandt, R. (eds.) Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. Lecture Notes in Computer Science, vol. 10786, pp. 25–46. Springer (2018), https://doi.org/10.1007/978-3-319-79063-3_2
18. Chen, C., Danba, O., Hoffstein, J., Hülsing, A., Rijneveld, J., Saito, T., Schanck, J.M., Schwabe, P., Whyte, W., Xagawa, K., Yamakawa, T., Zhang, Z.: NTRU - A submission to the NIST post-quantum standardization effort. https://www.cross-crypto.com/
19. European Commission: NextGenerationEU - more than a recovery plan. https://next-generation-eu.europa.eu/index_en (2021)
20. Feige, U., Fiat, A., Shamir, A.: Zero-Knowledge Proofs of Identity. J. Cryptol. **1**(2), 77–94 (1988), https://doi.org/10.1007/BF02351717

21. Genêt, A.: On Protecting SPHINCS+ Against Fault Attacks. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2023**(2), 80–114 (2023), https://doi.org/10.46586/tches.v2023.i2.80-114
22. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. In: Buhler, J. (ed.) Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1423, pp. 267–288. Springer (1998), https://doi.org/10.1007/BFb0054868
23. Lee, P.J., Brickell, E.F.: An Observation on the Security of McEliece's Public-Key Cryptosystem. In: Günther, C.G. (ed.) Advances in Cryptology - EUROCRYPT '88, Workshop on the Theory and Application of of Cryptographic Techniques, Davos, Switzerland, May 25-27, 1988, Proceedings. Lecture Notes in Computer Science, vol. 330, pp. 275–280. Springer (1988), https://doi.org/10.1007/3-540-45961-8_25
24. Melchor, C.A., Blazy, O., Deneuville, J., Gaborit, P., Zémor, G.: Efficient Encryption From Random Quasi-Cyclic Codes. IEEE Trans. Inf. Theory **64**(5), 3927–3943 (2018), https://doi.org/10.1109/TIT.2018.2804444
25. National Institute of Standards and Technology: Post-Quantum Cryptography Standardization Initiative. https://csrc.nist.gov/projects/post-quantum-cryptography
26. Perriello, S., Barenghi, A., Pelosi, G.: A Complete Quantum Circuit to Solve the Information Set Decoding Problem. In: Müller, H.A., Byrd, G., Culhane, C., Humble, T.S. (eds.) IEEE International Conference on Quantum Computing and Engineering, QCE 2021, Broomfield, CO, USA, October 17-22, 2021. pp. 366–377. IEEE (2021), https://doi.org/10.1109/QCE52317.2021.00056
27. Perriello, S., Barenghi, A., Pelosi, G.: A Quantum Circuit to Speed-Up the Cryptanalysis of Code-Based Cryptosystems. In: García-Alfaro, J., Li, S., Poovendran, R., Debar, H., Yung, M. (eds.) Security and Privacy in Communication Networks - 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6-9, 2021, Proceedings, Part II. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 399, pp. 458–474. Springer (2021), https://doi.org/10.1007/978-3-030-90022-9_25
28. Perriello, S., Barenghi, A., Pelosi, G.: Improving the Efficiency of Quantum Circuits for Information Set Decoding. ACM Transactions on Quantum Computing (Jul 2023), https://doi.org/10.1145/3607256
29. Perriello, S., Barenghi, A., Pelosi, G.: Quantum circuit design for the lee-brickell based information set decoding. In: 5th ACNS Workshop on Secure Cryptographic Implementation (SCI 2024) - n Martin Andreoni (Editor) Applied Cryptography and Network Security Workshops. ACNS 2024 Satellite Workshops, AIBlock, AIHWS, AIoTS, SCI, AAC, SiMLA, LLE, and CIMSS. Lecture Notes in Computer Science, vol. 14586–14587. Springer (2024), https://doi.org/10.1007/BFb0054868
30. SERICS Foundation: SERICS - Security and Rights in CyberSpace. https://serics.eu (2022)
31. Ulitzsch, V.Q., Marzougui, S., Bagia, A., Tibouchi, M., Seifert, J.: Loop Aborts Strike Back: Defeating Fault Countermeasures in Lattice Signatures with ILP. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2023**(4), 367–392 (2023), https://doi.org/10.46586/tches.v2023.i4.367-392