CRYPTOEXPERTS

WE INNOVATE TO SECURE YOUR BUSINESS

Offre de Stage - Internship Offer

Post-Quantum Anonymious Credentials

November 2025

Type of internship:	Master 2 / final-year engineering internship (6 months)
Field:	Cryptography
Company:	CryptoExperts
Workplace:	41 boulevard des Capucines, 75002 Paris
Period:	First semester of 2026

1 Company presentation

CryptoExperts is a private research lab providing R&D services in cryptography. The company has a team of experts from industry and academia, with PhDs in cryptography, and specialized in various fields. They include public key cryptography (both post- and pre-quantum), symmetric cryptography, efficient and secure implementations, security protocols and proofs, side-channel attacks, and security of embedded systems. CryptoExperts develops innovative cryptographic solutions for various applications, and offers security auditing, custom conception of cryptographic protocols and implementation of cryptographic libraries. The company is also very active in the field of scientific research in cryptography, producing every year several publications in the main conferences in the field, and taking part in various academic and industrial projects on advanced research issues (such as post-quantum cryptography, white-box cryptography, homomorphic encryption, proven security against physical attacks and zero-knowledge proofs).

2 Internship description

Anonymous credentials. Anonymous credential systems are cryptographic constructions that enable users to obtain and later prove possession of credentials issued by an authority, while preserving privacy. Such systems involve three main entities: an issuer, a user, and a verifier. The issuer provides the user with a credential attesting to certain attributes (e.g., age, membership, or qualification), the user stores this credential, and later interacts with a verifier to prove statements about these attributes without revealing unnecessary information. A well-designed anonymous credential (AC) system must ensure several security properties: *unforgeability* (only the issuer can produce valid credentials), *unlinkability* (different presentations of the same credential cannot be linked), and *selective disclosure* (only the required information is revealed when presenting a credential).

Anonymous credentials are gaining attention as a key privacy-enhancing technology for digital identity and access control. For instance, the Google Wallet supports privacy-preserving age verification [Goo23, Cry24]. Similarly, the upcoming European Digital Identity Wallet (EUDI Wallet) mandated by regulation in the EU calls for cryptographic support for selective attribute disclosure and unlinkability of presentations, indicating that anonymous credentials or similar constructs may form its backbone [Eur24, BBC+24].

From a construction viewpoint, most AC systems rely on digitally signed credentials combined with zero-knowledge proofs of knowledge. A general blueprint is the following:

1. Issuance: The user commits to their attributes m and requests a credential. The issuer signs these attributes $\sigma = \mathsf{Sign}_{\mathrm{sk}_I}(m)$ with their secret key sk_I, which might be done blindly. The credential is composed of the pair (m, σ).

2. Presentation: To prove possession of the credential, the user constructs a non-interactive zero-knowledge proof:

$$\pi = \mathsf{NIZK}\big(\exists\,(m,\sigma) : \mathsf{Ver}_{\mathrm{pk}_I}(m,\sigma) = 1 \ \wedge \ \Phi(m)\big)$$

where $\Phi(m)$ encodes what is disclosed. For instance, if m is a passport data, Φ could express "French citizen" or "age ≥ 18". By verifying π, the verifier is ensured that the user has a valid credential with attributes satisfying Φ.

Some signature schemes are specifically designed for anonymous credentials, offering efficient protocols for re-randomization or proof of knowledge, e.g., Camenisch–Lysyanskaya [CL03, CL04], BBS+ [BBS04, TZ23], or Pointcheval–Sanders [PS16] signatures. However, real-world deployments often prefer standardized signatures for interoperability and certification reasons. For instance, the Google Wallet uses ECDSA, a NIST-standardized signature scheme based on elliptic curves, and constructs ZK proofs tailored to this scheme [Fs24].

Post-quantum transition. The advent of quantum computing poses a fundamental threat to classical public-key cryptography, as quantum algorithms such as Shor's algorithm efficiently solve the integer factorization and discrete logarithm problems, thereby compromising schemes like RSA and ECDSA. To address this, the cryptographic community is transitioning toward *post-quantum cryptography* (PQC). The National Institute of Standards and Technology (NIST) has been leading an international standardization effort [Nat], culminating in the selection of two key-encapsulation mechanisms (ML-KEM, a.k.a. CRYSTALS-Kyber, and HQC) and three digital signature algorithms: ML-DSA (also known as CRYSTALS-Dilithium [LDK+20]), SLH-DSA (also known as SPHINCS+ [HBD+20]), and FN-DSA (also known as Falcon [PFH+20]).

In parallel, recent advances in post-quantum zero-knowledge proofs (ZKPs) provide promising building blocks for privacy-preserving systems. Protocols relying exclusively on symmetric primitives –particularly hash functions– offer both post-quantum security and practical efficiency. Notably, constructions such as Ligero [AHIV17, AHIV23] and their recent optimizations [FR25b, FR25a] achieve a favorable balance between proof size, prover and verifier complexity, while enabling their application to a wide range of cryptographic protocols.

2.1 Objectives

The objective of this internship is to design and implement a post-quantum anonymous credential system combining standardized post-quantum signatures with hash-based zero-knowledge proofs for selective disclosure. The work will follow four main stages:

1. **Literature review.** The intern will begin with a survey of the state of the art to get familiar with the concepts of anonymous credential systems and zero-knowledge proofs. They will specifically focus on recent hash-based ZK protocols [AHIV23, FR25b, FR25a].

2. **Design of a post-quantum AC system.** The core of the internship will focus on the design of an anonymous credential construction based on standardized post-quantum signatures and hash-based ZKPs. Specifically, we will explore the application of these

ZKPs to prove knowledge of PQC signatures and selective disclosure of attributes. We will primarily focus on ML-DSA (CRYSTALS-Dilithium) as the underlying signature scheme, but we may also investigate extensions using SLH-DSA (SPHINCS+) or FN-DSA (Falcon) if time permits.

3. **Prototype implementation.** A prototype of the proposed post-quantum anonymous credential system will be implemented in a suitable programming language (e.g., C, C++, or Rust). The goal is to benchmark the performance of the main components –credential issuance, selective disclosure proof generation, and verification– under realistic parameters. The evaluation will include both computational cost and proof size, allowing comparison with existing classical AC systems and with theoretical expectations.

4. **Application to EUDI Wallet.** In the final stage, we will investigate how the designed post-quantum anonymous credential system could be adapted to the context of the EUDI Wallet. This includes identifying the relevant interface and privacy requirements from the Architecture and Reference Framework (ARF) [Eur24] and assessing how our construction can satisfy these requirements or be integrated into the EUDI ecosystem.

The expected outcome of the internship is a proof-of-concept implementation and an accompanying technical report describing the design and experimental results. Depending on progress, the results may form the basis for a research publication or further development within the host laboratory.

3 Candidates

This internship offer is for a Master student who has a taste for cryptography and applied research. The candidate will have to demonstrate a solid background in mathematics and/or computer science with a specialization in cryptography. The technical background required for this internship combines skills in algebra (finite fields, polynomials, etc.) and in programming. The candidate will have to demonstrate autonomy and dynamism. A good level of English shall also be considered as a plus. After a first interview, selected candidates will be given a challenge to carry out at home before a second technical interview.

4 Internship conditions

The intern will be supervised by Thibauld Feneuil and Matthieu Rivain, researchers in cryptography. The internship duration is 6 months and can start anytime in 2026. The candidate will have an office in our open space in CryptoExperts' premises located in Paris (41 boulevard des Capucines, 75002 Paris). The location allows an interesting emulation among our team composed of researchers, PhD students and other interns. Remote work is also possible most of the time. The company offers many advantages (1 week holiday for

interns, flexible hours, restaurant vouchers, public transport refund). The intern is also an integral part of the team and is invited to any social event of the company.

5 Internship Conditions

The intern will be supervised by Thibauld Feneuil and Matthieu Rivain, researchers in cryptography. The internship duration is 6 months and can start anytime in 2026. The candidate will have an office in our open space in CryptoExperts' premises located in Paris (41 boulevard des Capucines, 75002 Paris). The location allows an interesting emulation among our team composed of researchers, PhD students and other interns. Remote work is also possible most of the time. The company offers many advantages (1 week holiday for interns, flexible hours, restaurant vouchers, public transport refund). The intern is also an integral part of the team and is invited to any social event of the company. The monthly stipend is 1801.80 gross.

6 Contact

To apply for this internship offer, please send your resume to Matthieu Rivain and Thibauld Feneuil at

matthieu.rivain@cryptoexperts.com
thibauld.feneuil@cryptoexperts.com

References

[AHIV17] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight sublinear arguments without a trusted setup. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 2087–2104. ACM Press, October / November 2017.

[AHIV23] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: lightweight sublinear arguments without a trusted setup. *DCC*, 91(11):3379–3424, 2023.

[BBC+24] Carsten Baum, Olivier Blazy, Jan Camenisch, Jaap-Henk Hoepman, Eysa Lee, Anja Lehmann, Anna Lysyanskaya, René Mayrhofer, Hart Montgomery, Ngoc Khanh Nguyen, Bart Preneel, Abhi shelat, Daniel Slamanig, Stefano Tessaro, Søren Eller Thomsen, and Carmela Troncoso. Cryptographers' feedback on the eu digital identity's arf. Technical report, June 2024. Preprint, version 1.0, available at https://files.dyne.org/dynebolic/?file=eudi%2Fcryptographers-feedback-june2024.pdf.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, Berlin, Heidelberg, August 2004.

[CL03] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02*, volume 2576 of *LNCS*, pages 268–289. Springer, Berlin, Heidelberg, September 2003.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 56–72. Springer, Berlin, Heidelberg, August 2004.

[Cry24] Cryptopolitan. Google wallet introduces zero-knowledge proofs for age verification. https://www.cryptopolitan.com/google-wallet-introduces-zk-proofs/, 2024.

[Eur24] European Digital Identity Wallet Cooperation Group. European digital identity wallet – architecture and reference framework (arf) version 1.4.0. Technical report, European Digital Identity Wallet (EUDIW) Cooperation Group, 2024. Version 1.4.0, available at https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/.

[FR25a] Thibauld Feneuil and Matthieu Rivain. Smallwood: Hash-based polynomial commitments and zero-knowledge arguments for relatively small instances. *IACR Cryptol. ePrint Arch.*, page 1085, 2025.

[FR25b] Thibauld Feneuil and Matthieu Rivain. Threshold computation in the head: Improved framework for post-quantum signatures and zero-knowledge arguments. *J. Cryptol.*, 38(3):28, 2025.

[Fs24] Matteo Frigo and abhi shelat. Anonymous credentials from ECDSA. Cryptology ePrint Archive, Report 2024/2010, 2024.

[Goo23] Google. How google wallet keeps your digital id private and secure. https://blog.google/products/google-pay/google-wallet-digital-id-privacy-security/, 2023.

[HBD+20] Andreas Hülsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS$^+$. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[LDK+20] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[Nat] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization process. Technical report. Overview available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[PFH+20] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[PS16] David Pointcheval and Olivier Sanders. Short randomizable signatures. In Kazue Sako, editor, *CT-RSA 2016*, volume 9610 of *LNCS*, pages 111–126. Springer, Cham, February / March 2016.

[TZ23] Stefano Tessaro and Chenzhi Zhu. Revisiting BBS signatures. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 691–721. Springer, Cham, April 2023.