Researcher Library

Matteo

February 5, 2026

1 Introduction

I want to make this a library of good refs/papers I have read/studied and a little about them so that I can find things simply and understand them. This document will require lot of work to bring up to speed, and will likely miss a lot of past readings, it will be continued overtime. This project was started on November 2025, hopefully will include descriptions of 100s of papers overtime, as I continue delving deeper into academic research.

Specifically refs useful for PhD, or other projects will be emphasized when the interest is less they will be reduced to a normal size.

Books to study deeply: Postquantum Cryptography of Bernstein [8], Foundations of Cryptography volumes 1&2 [23]

Contents

2 Cryptography

Science and practice of securing information

[3] check this for coding guidelines not a paper but interesting.

2.1 Computer Aided Crypto

- [4] *SoK: Computer-aided cryptography*: This systematization paper surveys and organizes the rapidly expanding field of computer-aided cryptography (CAC), which applies formal, machine-checked methods to the design, analysis, and implementation of cryptographic systems. Its central contribution is a cross-cutting taxonomy that unifies three major strands of CAC—design-level security (both symbolic and computational), functional correctness and efficiency, and implementation-level security against digital side-channels—and clarifies how each contributes to end-to-end assurance. The authors critically assess current capabilities, limitations, and trade-offs of dozens of tools along dimensions of accuracy, scope, trust, and usability, illustrating how CAC methods have enabled proofs of complex real-world protocols such as TLS 1.3 and the deployment of verified high-performance primitives in production libraries like HACL*. Through two detailed case studies, the paper highlights the challenges of combining heterogeneous verification results into unified guarantees and the lessons learned from formal participation in standards processes. Overall, it provides a consolidated foundation for understanding the state of CAC and outlines key research directions needed to scale formal cryptographic assurance to full systems.

  READ: 03/12/2025;

  Interesting papers to have a look: Very very important paper in understanding the SOTA 2 flavours of symbolic sec Trace properties and Equivalence properties; Computational properties along 2 arcs: game based/ simulation based & concrete/ asymmetric. Assymetric is prevailing but weaker than concrete same goes for game based and simulation respectively. All the tools for everything. Compiler optimizations danger for code. EasyCrypt/Jasmin. they advocate for more interplay between proof engineering research and cac; standard to implementation gap; hand written sec arguments and proofs often cannot be reasonably audited goes back to bernstein [7].

- [1] *Machine-checked proofs for cryptographic standards: Indifferentiability of sponge and secure high-assurance implementations of SHA-3* Good example of full verification of sha3 with highest guarantees according to SoK

- [38] *HACL*: A verified modern cryptographic library*
- [20] *A high-assurance evaluator for machine-checked secure multiparty computation* When interested in MPC verif

2.2 Mitigating attacks

- [32] *On configurable SCA countermeasures against single trace attacks for the NTT: A performance evaluation study over Kyber and Dilithium on the arm Cortex-M4*:

2.3 Searchable Encryption

- [37] *Practical techniques for searches on encrypted data* Foundation paper Symmetric Searchable encryption
- [13] *Public key encryption with keyword search* Same foundational paper this time asymmetric searchable encryption more like multiple can write one can read with the private key

2.4 Hybrid protocols and Key exchanges

All the muckle papers and qkd oracles paper I guess need to add the ref and descriptions but they are read

- [2] *Post-Quantum Ratcheting for Signal*
- [18] *Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange* This foundational paper introduces the HAKE (Hybrid Authenticated Key Exchange) framework, a formal security model designed to analyze protocols that combine classical, post-quantum (PQ), and Quantum Key Distribution (QKD) keying material. The authors propose “Muckle,” a specific instantiation of a hybrid protocol that achieves one-round-trip (1-RTT) key exchange. Crucially, Muckle relies on pre-shared keys (PSKs) for authentication to avoid the high overhead of post-quantum signatures, effectively leveraging the symmetric keys already inherent in QKD setups. The paper provides a rigorous security proof demonstrating that Muckle achieves forward security and post-compromise security, ensuring that the session remains secure even if some component keys (e.g., classical or QKD) are compromised, provided at least one source of entropy remains safe.

  READ: 01/11/2025;
  Seminal work establishing the HAKE framework; essential reading for hybrid KEX. Introduces the concept of ”defense-in-depth” for key exchange (combining Classical + PQ + QKD). Uses PSKs for auth, which

limits scalability but is highly efficient for static links. Models QKD abstractly as a shared random string (a simplification addressed in later papers like [25]). Strong security properties: Forward Secrecy (PFS) and Post-Compromise Security (PCS).

- [5] *Quantum-safe hybrid key exchanges with KEM-based authentication*: This work proposes "Muckle#," an evolution of the Muckle family designed to improve efficiency in large-scale networks where digital signatures are too bandwidth-heavy and PSKs are not scalable. Instead of using signatures (like Muckle+) or PSKs (like Muckle), Muckle# utilizes post-quantum Key Encapsulation Mechanisms (KEMs) for implicit authentication, inspired by the KEMTLS protocol. The authors extend the HAKE framework to support this mode of authentication and provide a security proof showing that Muckle# maintains the robust security properties of its predecessors—such as forward and post-compromise security—while significantly reducing communication overhead compared to signature-based variants.

  READ: 01/11/2025;
  Optimizes efficiency by removing heavy PQ signatures; uses KEMs for authentication (implicit auth). Follows the KEMTLS design philosophy but adapted for the hybrid QKD setting. Addresses the scalability issues of Muckle (no PSKs needed) without the bandwidth cost of Muckle+. Requires a PKI for KEM keys, which is non-standard but efficient. Critical for constrained environments requiring quantum safety.

- [14] *Muckle+: End-to-end hybrid authenticated key exchanges*: Addressing the scalability limitations of the original Muckle protocol's reliance on pre-shared keys, this paper introduces "Muckle+." This variant replaces PSK-based authentication with post-quantum digital signatures, making it suitable for dynamic, large-scale networks where establishing pairwise PSKs is infeasible. The authors adapt the HAKE framework to model this public-key setting and provide a formal security proof. The paper demonstrates that replacing PSKs with signatures is non-trivial in the hybrid setting but achievable, thereby offering a protocol that retains strong hybrid security guarantees (forward and post-compromise security) while enabling the flexibility of a Public Key Infrastructure (PKI).

  READ: 01/11/2025;
  First HAKE protocol to integrate standard PKI (Digital Signatures) for scalability. Enables dynamic networks (unlike original Muckle's static PSK requirement). Highlights the complexity of proving security when swapping PSKs for Signatures in hybrid models. Trade-off: Higher bandwidth usage (PQ signatures are large) vs. better scalability. Direct predecessor to VMuckle; essential for understanding the move to PKI.

- [16] *Versatile quantum-safe hybrid key exchange and its application to MACsec*: This paper presents "VMuckle" (Versatile Muckle), a flexible

HAKE protocol designed to bridge the gap between small and large-scale deployments by supporting both PSK and digital signature-based authentication methods adaptively. A major contribution of this work is the practical integration of VMuckle into the Media Access Control Security (MACsec) standard (IEEE 802.1AE) to replace the classical 802.1X authentication. This integration provides a quantum-safe root of trust for Layer 2 network security. The authors provide a security analysis within the HAKE framework and demonstrate via implementation that VMuckle is a viable, standards-compliant path toward quantum-resistant Ethernet security.

READ: 01/11/2025;
Highly applied paper: Bridges theory (HAKE) and practice (MACsec/IEEE 802.1AE). "Versatile" means it supports *both* PSK (efficient) and PKI (scalable) modes. Replaces legacy 802.1X auth with quantum-safe hybrid keys. Includes concrete implementation and performance benchmarks. Crucial for real-world deployment of hybrid security in Layer 2 networks.

- [25] *QKD Oracles for Authenticated Key Exchange*: This theoretical paper critically examines how Quantum Key Distribution (QKD) is modeled in cryptographic security proofs. The authors identify a significant gap in existing literature: improper handling of QKD Key IDs can lead to "Dependent-Key attacks" that break protocol security. To resolve this, they introduce a rigorous "QKD Oracle" model that closely mirrors the standard ETSI GS QKD 014 interface used in real-world hardware. By integrating this oracle into the established CK+ security model, they provide a formal methodology for proving the security of protocols that combine QKD with classical AKE. They validate this model by proving the security of a novel hybrid protocol that combines a triple-KEM handshake with QKD, ensuring it preserves the information-theoretic security properties of the quantum link.

  READ: 01/11/2025;
  Theory-heavy; critiques and improves the abstract QKD models used in Muckle/Muckle+. Identifies "Dependent-Key attacks" caused by poor Key ID handling in proofs. Aligns cryptographic models with real-world ETSI hardware standards. Proposes a Triple-KEM + QKD handshake. Must-read for correctness in security proofs involving QKD interfaces.

2.5 Proofs

- [36] *Sequences of games: a tool for taming complexity in security proofs* Foundational paper on proofs

- [6] *he security of triple encryption and a framework for code-based game-playing proofs* Also foundational game based proof paper

- [28] *How to simulate it–a tutorial on the simulation proof technique* Simulation based proof foundational paper harder than game based essential for symbolic

2.6 Thresholds

- Threshold KEM paper [27]

3 Cryptanalysis

Art and science of "cracking" encryption without knowing the secret key

- [9] *CryptAttackTester: high-assurance attack analysis*: The central contribution of this report is the introduction of the Crypt Attack Tester (CAT), a software framework designed to bring high assurance and rigor to the quantitative analysis of cryptographic attack costs. Historically, security-level claims often contain errors due to ambiguities or untested assumptions. CAT addresses this by enforcing complete, formal definitions of the attack algorithm, the underlying model of computation, and the cost metric. By systematically simulating attacks on small-scale inputs and comparing the observed cost and success probability directly against the analytical predictions, CAT provides auditable evidence that the security-level claims are correct and fully defined. This process, demonstrated through detailed case studies on AES-128 brute-force search and various Information Set Decoding (ISD) algorithms for McEliece, catches errors that slipped past informal testing and provides concrete, validated cost predictions for cryptographic sizes, such as the median cost of AES-128 key search being under $2^{141.89}$ bit operations.

  Papers using CAT: [12, 10, 21, 31]

  READ: 11/26/2025;

  Most significant and concrete example of a framework built to achieve the goals of formalizing cryptanalysis. Machine checkable validation via simulation rather than formal proofs.

  CAT enforces a complete definition of the attack algorithm, the underlying model of computation (a Boolean circuit model), the cost metric (bit operations), and the formulas for cost and success probability. This rigorous specification is the necessary first step for any formal verification effort.

  The core innovation is using a simulator to automatically check if the predicted cost and predicted success probability match the observed cost and probability from running the formalized circuit on small-scale inputs. This step is a high-assurance substitute for a formal proof, testing the consistency between the analytical formulas and the algorithm's actual behavior in the specified model.

Proof assistant: Prove that Algorithm → Prediction CAT's Approach: Test that Algorithm $\rightleftharpoons$ Prediction

- [24] The fragility of AES-GCM authentication algorithm interesting example of failure that could be avoided with CAC
- [15] Some bug I want to checkout in OSSL perhaps not
- [30] Hardware Implementation of Stealthy and Lightweight Backdoor for CRYSTALS-Kyber: The paper introduces a kleptographic backdoor for the NIST-standardized KEM CRYSTALS-Kyber and demonstrates its feasibility in hardware. Instead of using conventional hardware Trojan triggers and payloads, the attack leverages asymmetric cryptography to embed a hidden setup directly into the key-generation process.

  Two constructions are presented. The first uses Curve25519 to encrypt the user's secret seed, while the second improves latency by using static ECC values together with AES-256. The key innovation is achieving practical undetectability: by modifying the Central Binomial Distribution and adding a compensation term to the public key, the altered error distribution remains statistically indistinguishable from that of standard Kyber.

  The implemented backdoor adds only about 2% area overhead (283 LUTs) and increases latency by roughly 4%, allowing it to pass performance evaluations and Known Answer Tests even in debug mode. Overall, the work shows how hybrid cryptosystems can serve as a covert channel for attackers to recover user secrets if hardware IP is not fully verified.

  READ: 22/12/2025;
  Key Takeaway: This is the first hardware realization of a kleptographic attack on post-quantum cryptography, demonstrating that even standardized algorithms can be subverted when randomness or hardware design is manipulated.

4 Formal Methods

Mathematics to specify, design, and verify systems — particularly software and hardware.

- [7] *Papers with computer-checked proofs*: This report challenges the widespread assumption that including computer-checked proofs with mathematical papers is prohibitively expensive and time-consuming. The author, Daniel J. Bernstein, argues for a "single-stage" process where the paper presenting a new theorem also includes its formal verification. Drawing on four of his own case studies—where he produced thousands of lines of checked proofs in just a few weeks per paper —he demonstrates that this practice is affordable with modern proof assistants. The main takeaway is that line counts are a ”terribly misleading” metric for effort , and that mathematicians should adopt this single-stage process to improve efficiency, catch their own errors early , and reduce the correctness-checking burden on referees.

READ: 11/11/2025;
Interesting but little novelty or scientific interest; Use: Framing importance of computer aided/gap

5 Mathematics

The abstract study of numbers, structure, and probability, serving as the theoretical foundation for cryptographic security definitions.

TO READ: [11], orgiginal shor paper [34, 35]

5.1 Probability Theory

- [33] *Some Notions of Entropy for Cryptography*: This survey clarifies the various definitions of entropy used in modern cryptography, distinguishing them from classical Shannon entropy. It focuses on min-entropy (measuring the probability of the most likely guess) and collision entropy, which are critical for key derivation and randomness extraction. The paper also explores computational analogues (like HILL and Yao entropy), which quantify randomness from the perspective of a computationally bounded adversary, demonstrating why high Shannon entropy alone does not guarantee security against brute-force attacks.

  READ: 04/02/2026;
  Essential theoretical reference; establishes why “randomness” in crypto is distinct from information content. It provides the mathematical justification for why we use min-entropy rather than Shannon entropy to measure password or key strength.

6 Computer Architechture

Structural design and organization of computer systems, hardware components, and instruction sets.

- [17] *SoK: Instruction Set Extensions for Cryptographers* very interesting for any lightweight constrained systems and iot

- [22] *No security without time protection: We need a new hardware-software contract*

6.1 Microarchitectural Side-Channel Attacks

- [29] Meltdown: Reading kernel memory from user space attacks relevant also why TEEs can be good
- [26] Spectre attacks: Exploiting speculative execution

6.2 Trusted Computing

- [19] *Towards Quantum-Resistant Trusted Computing: Architectures for Post-Quantum Integrity Verification Techniques*: This paper addresses the urgent migration of Trusted Computing primitives—specifically Secure Boot and Remote Attestation—to Post-Quantum Cryptography (PQC). The authors evaluate NIST standards, recommending Stateful Hash-Based Signatures (e.g., XMSS, LMS) for firmware integrity due to their conservative security guarantees, while suggesting Lattice-Based algorithms (ML-DSA) for runtime attestation. The work proposes a dual transition architecture: a Firmware TPM (fTPM) solution for ARM TrustZone and a hybrid kernel-level wrapper for legacy x86 systems to add PQ security to classical TPM quotes.

  READ: 04/02/2026;
  the architectural proposal is flawed. The x86 hybrid solution relies on a kernel driver to wrap quotes; this design fails if a quantum attacker is already present in the OS, as they can subvert the driver and forge the PQ wrapper. Furthermore, the paper omits the critical initialization phase of the TEEs (TrustZone/fTPM), simply assuming an immutable Core Root of Trust exists without explaining how the secure environment is safely bootstrapped.

7 Information Security

Protection of information systems and data from unauthorized access, use, or destruction.

8 Operating System

Management of hardware resources and provision of common services for computer programs.

9 Network

Interconnection of computing devices for the exchange of data and shared resources.

References

[1] José Bacelar Almeida, Cécile Baritel-Ruet, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Alley Stoughton, and Pierre-Yves Strub. Machine-checked proofs for cryptographic standards: Indifferentiability of sponge and secure high-assurance implementations of sha-3. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1607–1622, 2019.

[2] Benedikt Auerbach, Yevgeniy Dodis, Daniel Jost, Shuichi Katsumata, Thomas Prest, and Rolfe Schmidt. Post-quantum ratcheting for signal. 2025.

[3] Jean-Philippe Aumasson. Guidelines for low-level cryptography software. `https://github.com/veorq/cryptocoding`.

[4] Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno. Sok: Computer-aided cryptography. In *2021 IEEE symposium on security and privacy (SP)*, pages 777–795. IEEE, 2021.

[5] Christopher Battarbee, Christoph Striecks, Ludovic Perret, Sebastian Ramacher, and Kevin Verhaeghe. Quantum-safe hybrid key exchanges with kem-based authentication. *EPJ Quantum Technology*, 12(1):128, 2025.

[6] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 409–426. Springer, 2006.

[7] Daniel J Bernstein. Papers with computer-checked proofs.

[8] Daniel J Bernstein. Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1846–1847. Springer, 2025.

[9] Daniel J Bernstein and Tung Chou. Cryptattacktester: high-assurance attack analysis. In *Annual International Cryptology Conference*, pages 141–182. Springer, 2024.

[10] Daniel J Bernstein and Tanja Lange. Safe curves for elliptic-curve cryptography. *Information Security in a Connected World: Celebrating the Life and Work of Ed Dawson*, pages 124–191, 2025.

[11] Daniel J Bernstein and Bo-Yin Yang. Fast constant-time gcd computation and modular inversion. *IACR transactions on cryptographic hardware and embedded systems*, pages 340–398, 2019.

[12] Sreyosi Bhattacharyya and Palash Sarkar. Concrete time/memory trade-offs in generalised stern's isd algorithm. In *International Conference on Cryptology in India*, pages 307–328. Springer, 2023.

[13] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques*, pages 506–522. Springer, 2004.

[14] Sonja Bruckner, Sebastian Ramacher, and Christoph Striecks. : End-to-end hybrid authenticated key exchanges. In *International Conference on Post-Quantum Cryptography*, pages 601–633. Springer, 2023.

[15] Billy B Brumley, Manuel Barbosa, Dan Page, and Frederik Vercauteren. Practical realisation and elimination of an ecc-related software bug attack. In *Cryptographers' Track at the RSA Conference*, pages 171–186. Springer, 2012.

[16] Jaime S Buruaga, Augustine Bugler, Juan P Brito, Vicente Martin, and Christoph Striecks. Versatile quantum-safe hybrid key exchange and its application to macsec. *EPJ Quantum Technology*, 12(1):84, 2025.

[17] Hao Cheng, Johann Großschädl, Ben Marshall, Daniel Page, and Markku-Juhani O Saarinen. Sok: Instruction set extensions for cryptographers. *Cryptology ePrint Archive*, 2024.

[18] Benjamin Dowling, Torben Brandt Hansen, and Kenneth G Paterson. Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange. In *International Conference on Post-Quantum Cryptography*, pages 483–502. Springer, 2020.

[19] Grazia D'Onghia and Antonio Lioy. Towards quantum-resistant trusted computing: Architectures for post-quantum integrity verification techniques. In *2025 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE, 2025.

[20] Karim Eldefrawy and Vitor Pereira. A high-assurance evaluator for machine-checked secure multiparty computation. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 851–868, 2019.

[21] Andre Esser, Javier Verbel, Floyd Zweydinger, and Emanuele Bellini. Sok: Cryptographicestimators–a software library for cryptographic hardness estimation. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 560–574, 2024.

[22] Qian Ge, Yuval Yarom, and Gernot Heiser. No security without time protection: We need a new hardware-software contract. In *Proceedings of the 9th Asia-Pacific Workshop on Systems*, pages 1–9, 2018.

[23] Oded Goldreich. *Foundations of cryptography: volume 2, basic applications*, volume 2. Cambridge university press, 2001.

[24] Shay Gueron and Vlad Krasnov. The fragility of aes-gcm authentication algorithm. In *2014 11th International Conference on Information Technology: New Generations*, pages 333–337. IEEE, 2014.

[25] Kathrin Hövelmanns, Daan Planken, Christian Schaffner, and Sebastian R Verschoor. Qkd oracles for authenticated key exchange. *arXiv preprint arXiv:2509.12478*, 2025.

[26] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, et al. Spectre attacks: Exploiting speculative execution. *Communications of the ACM*, 63(7):93–101, 2020.

[27] Oleksandra Lapiha and Thomas Prest. A lattice-based ind-cca threshold kem from the bchk+ transform. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 461–494. Springer, 2025.

[28] Yehuda Lindell. How to simulate it–a tutorial on the simulation proof technique. *Tutorials on the Foundations of Cryptography: Dedicated to Oded Goldreich*, pages 277–346, 2017.

[29] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, et al. Meltdown: Reading kernel memory from user space. *Communications of the ACM*, 63(6):46–56, 2020.

[30] Suraj Mandal, Prasanna Ravi, M Dhilipkumar, Debapriya Basu Roy, and Anupam Chattopadhyay. Hardware implementation of stealthy and lightweight backdoor for crystals-kyber. *Cryptology ePrint Archive*, 2025.

[31] Shintaro Narisada, Shusaku Uemura, Hiroki Okada, Hiroki Furue, Yusuke Aikawa, and Kazuhide Fukushima. Solving mceliece-1409 in one day—cryptanalysis with the improved bjmm algorithm. In *International Conference on Information Security*, pages 3–23. Springer, 2024.

[32] Prasanna Ravi, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay. On configurable sca countermeasures against single trace attacks for the ntt: A performance evaluation study over kyber and dilithium on the arm cortex-m4. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pages 123–146. Springer, 2020.

[33] Leonid Reyzin. Some notions of entropy for cryptography: (invited talk). In *International Conference on Information Theoretic Security*, pages 138–142. Springer, 2011.

[34] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[35] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[36] Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *cryptology eprint archive*, 2004.

[37] Dawn Xiaoding Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *Proceeding 2000 IEEE symposium on security and privacy. S&P 2000*, pages 44–55. IEEE, 2000.

[38] Jean-Karim Zinzindohoué, Karthikeyan Bhargavan, Jonathan Protzenko, and Benjamin Beurdouche. Hacl*: A verified modern cryptographic library. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1789–1806, 2017.