Understanding Covercrypt and Exploring Its Potential to Meet ETSI TS 104 015

Santosh Pandit

London, 5 April 2025

Contents

Background

I had promised my readers to write a separate feature on Covercrypt.

Call it serendipity - Chloé Hébant, a cryptographer and co-author of the paper "*Security Analysis of Covercrypt: A Quantum-Safe Hybrid Key Encapsulation Mechanism for Hidden Access Policies*", shared their work with me. Since the paper is packed with technical details (and I'd rather not lose my followers who dislike complex stuff), I'm here to break it down in simpler terms.

Important Disclaimer: All opinions and any mistakes are mine, neither Chloé's nor my employer's.

What is Covercrypt?

Covercrypt is a Key Encapsulation Mechanism (KEM) designed to securely share session keys using public-key cryptography with fine-grained access control. It's a hybrid system combining two protections:

- **Pre-quantum security** via Elliptic Curve Diffie-Hellman (ECDH), effective against current computers but vulnerable to quantum attacks.
- **Post-quantum security** via ML-KEM, a lattice-based method resistant to quantum computers.

This double-layered approach ensures that if one part fails - e.g., ECDH due to a quantum breakthrough - ML-KEM keeps your data secure. It also lets you encrypt data with specific rules (e.g., user roles or clearance levels) embedded in a hidden access policy for enhanced privacy.

What Does the Research Paper Establish?

Key Features

The paper highlights some standout features:

Hidden Access Policies: You can encrypt data with rules - like "only Marketing staff with top clearance" - and those rules stay secret in the encrypted file. This keeps prying eyes from figuring out who's allowed to see it.

Dual Security: By blending pre-quantum (ECDH) and post-quantum (ML-KEM) methods, Covercrypt protects against both today's threats and tomorrow's quantum risks.

Speed: Older post-quantum systems took hundreds of milliseconds to seconds, but Covercrypt encrypts in 0.271–0.794 ms and decrypts in 0.508–4.36 ms, depending on policy size, making it practical for many uses.

Traceability: It has a feature to spot if someone misuses a decryption key, helping to track down anyone breaking the rules.

How It Works

Here’s the process in a nutshell:

Setup: The system starts by defining rights (like departments or clearance levels) and creating master keys.

Key Generation: Users get their own secret keys tied to their specific rights.

Encryption: A session key is encapsulated with a hidden policy, ensuring only authorised users can retrieve it.

Decryption: If your rights match the policy, your secret key retrieves the session key to unlock the data.

The paper backs this up with formal proof, showing that the keys stay secret, and the access rules remain hidden, based on well-tested cryptographic ideas.

Performance and Practicality

Covercrypt is built in Rust, and its open-source code proves its speed. Encryption time scales linearly with policy size, and decryption ranges from 0.5–4.36 ms depending on the number of rights. Compared to GPSW (encryption 4.8–7.2 ms, decryption ~3.9 ms), Covercrypt is faster and balances security with practicality.

Authors' Conclusion

The researchers see Covercrypt as a smart, future-ready tool. Its mix of pre- and post-quantum security, fast performance, hidden policies, and traceability make it a great fit for industries dealing with sensitive data. With quantum computing on the horizon, Covercrypt could be a solid stepping stone to keep information safe.

My Perspective from an ETSI TS Perspective

High Bar

The ETSI Technical Specification sets a high bar for encryption systems, focusing on security, privacy, and readiness for quantum threats. Here's how Covercrypt stacks up:

Security: Its hybrid design - mixing pre- and post-quantum methods - fits ETSI's need for protection against current and future risks. The paper's formal proofs show it keeps keys and policies secure, which aligns with ETSI's strict standards.

Privacy: Hiding access policies is a big win for ETSI's privacy goals. It ensures no one can tell who's allowed to see the data just by looking at the encrypted file.

Speed: ETSI prioritises practicality, and Covercrypt's encryption (0.271–0.794 ms) and decryption (0.5–4.36 ms) times outperform older systems, making it a strong candidate.

Areas Needing Work

Traceability: Covercrypt can track key misuse, which is great for accountability. But CISO/DPO might want more detail on how this works in practice - can an independent party check it without breaking privacy rules? A question for ETSI consideration: should a 'Chief Auditor' role be standardised in ABE systems for oversight?

Real-World Performance: The speed looks good on paper, but practitioners will likely want proof it holds up on different devices, like smartphones or IoT gadgets, especially under tough conditions like streaming or OTA updates.

Flexible Access: Covercrypt lets you update access rules without re-encrypting data, which is handy. For 'Top Secret' data, more evidence is needed to ensure long-term security after repeated rule updates.

In short, Covercrypt has a lot going for it - strong security, great privacy, and solid performance. But to fully meet ETSI's standards, we'd need more testing and clarity on traceability, device performance, and long-term flexibility.

My Perspective from an Application Perspective

Getting to ETSI's standard won't be a walk in the park - it'll take some creative thinking, as I've noted in my earlier posts. The standard prioritises outcomes, and Covercrypt advances this with its security and efficiency. I'm itching to test it in my lab.

Here's what I'll be checking for in Covercrypt and other solutions:

Smooth Hybrid Setup: Combining pre- and post-quantum methods is smart, but it needs to work seamlessly with existing systems without adding new weak spots.

Managing Hidden Policies: Hiding access rules boosts privacy, but it could get tricky if different organisations use different setups. We need to make sure it's practical across the board.

Traceability Balance: Tracking misuse is useful, but it can't clash with privacy laws. I'll be asking: can a third party verify it without causing issues?

Speed in Action: The efficiency claims are exciting, but I want to see how it performs on real devices - think IoT or smartphones - especially under heavy use like streaming.

Secure Updates: Changing access rules without re-encrypting is a bonus, but it has to stay rock-solid. If I were a hacker, I'd target that feature, so we need to ensure it's tough to crack.

This should give you a clear picture. Next up, I'll be putting Covercrypt through its paces. Meanwhile, the hunt for even better solutions goes on.

References

1. ETSI Technical Specification 104 015: Announcement is here. TS is here.
2. My first post (LinkedIn post here)
3. What is Attributed Based Encryption (Article here and paper is here).
4. Security Analysis of Covercrypt: “A Quantum-Safe Hybrid Key Encapsulation Mechanism for Hidden Access Policies”, Théophile Brézot, Chloé Hébant et al, source: link here)

Key Terms Explained

ABE (Attribute-Based Encryption): A type of encryption where access to data depends on specific user attributes, like job role or security clearance, rather than just a single key.

Covercrypt: A modern encryption tool that locks secret keys with hidden rules about who can unlock them. It combines old-school (pre-quantum) and future-proof (post-quantum) security to protect data now and against quantum computers later.

ECDH (Elliptic Curve Diffie-Hellman): A method to securely share secret keys using maths based on elliptic curves. It's strong against today's computers but could be cracked by quantum computers in the future.

Encryption: The process of scrambling data or keys so only authorised people can read them.

ETSI (European Telecommunications Standards Institute): A group that sets technical standards for things like encryption. ETSI TS 104 015 is their rulebook for quantum-safe key-sharing systems like Covercrypt.

ETSI TS 104 015: A technical standard from ETSI that outlines how to build secure, privacy-focused, quantum-ready key-sharing systems.

Hybrid System: A setup that mixes two different methods - in Covercrypt's case, pre-quantum (ECDH) and post-quantum (ML-KEM) security - to stay safe even if one method fails.

IoT (Internet of Things): Everyday devices, like smart thermostats or cameras, connected to the internet.

KEM (Key Encapsulation Mechanism): A way to lock up a secret key (called a session key) so only the right person can unlock it.

ML-KEM (Module-Lattice-Based Key Encapsulation Mechanism): A post-quantum encryption method based on tricky lattice maths. It's designed to resist attacks from quantum computers.

OTA (Over-the-Air) Updates: Sending software updates wirelessly, like to a phone or car.

Post-Quantum Security: Protection designed to stay safe even when powerful quantum computers exist.

Pre-Quantum Security: Protection that works well against today's computers but might not against quantum ones.

Quantum Computer: A super-powerful future computer that could break some older encryption methods (like ECDH) using quantum physics.

Rust: A programming language known for being fast and secure.

Session Key: A temporary secret code used to lock and unlock data.

Traceability: The ability to track if someone misuses a key, like sharing it when they shouldn't.