



Beyond post-quantum stereotypes

Antoine Gicquel & Benjamin Sepe

Hack.lu 2025

About us



Antoine Gicquel

Pentester / Security auditor
@bluesheeet.bsky.social



Benjamin Sepe

Pentester / Security auditor
@butanol.bsky.social

Table of Contents

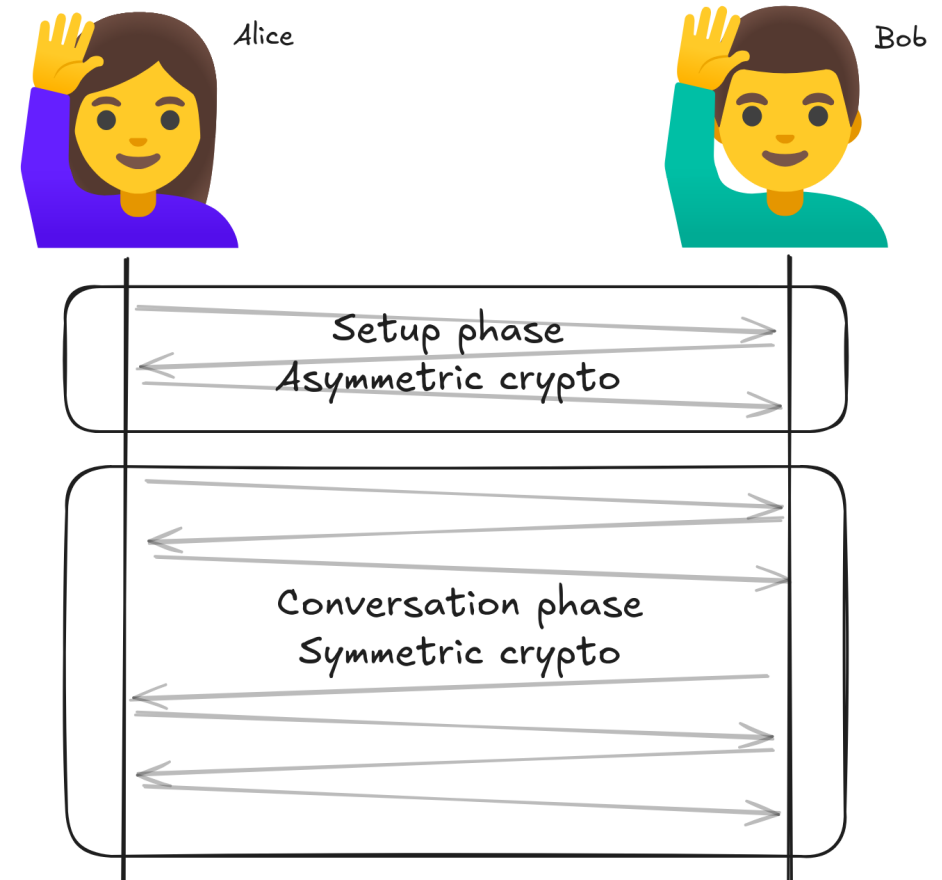


- **What does "secure" mean in cryptography?**
- **How do quantum computing affect the security of cryptographic algorithms?**
- **Upgrading your cryptography to post-quantum...**
- **... and auditing it!**

Refreshers

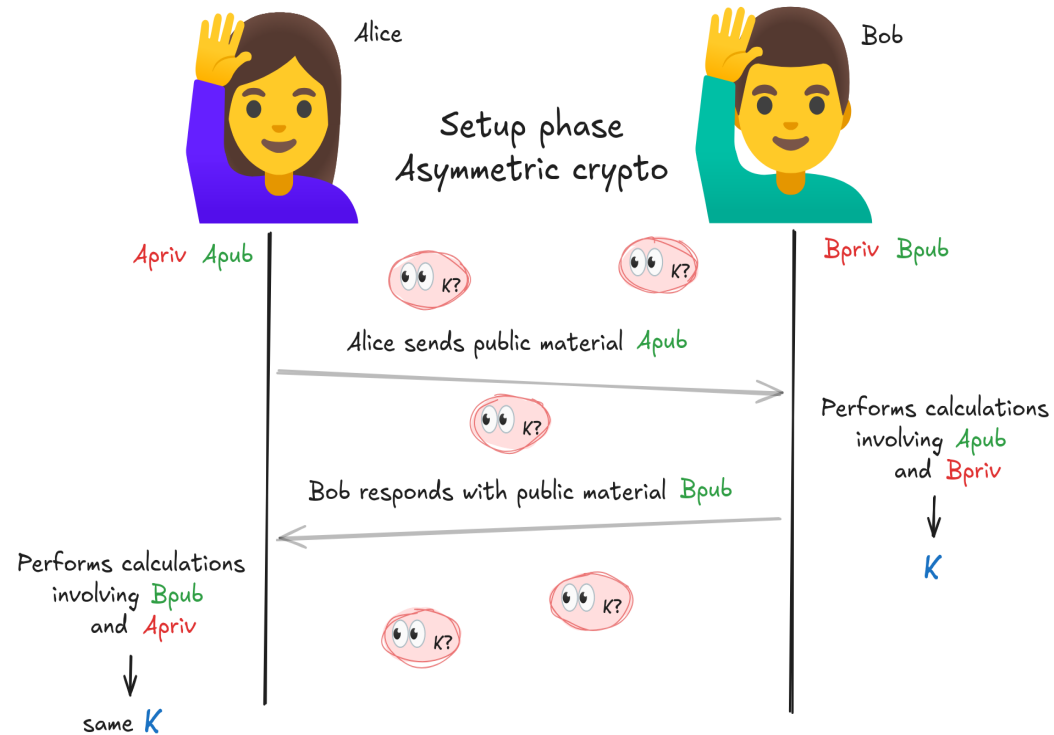
Modern crypto 101

- **A simple goal:** to enable Alice 🧑 and Bob 🧑 to have a secure conversation
- **A smart combination of two paradigms**
 - **Asymmetric (Public-Key) Cryptography:** For the initial setup
 - **Symmetric Cryptography:** For the actual conversation



Modern crypto 101

Key Exchange

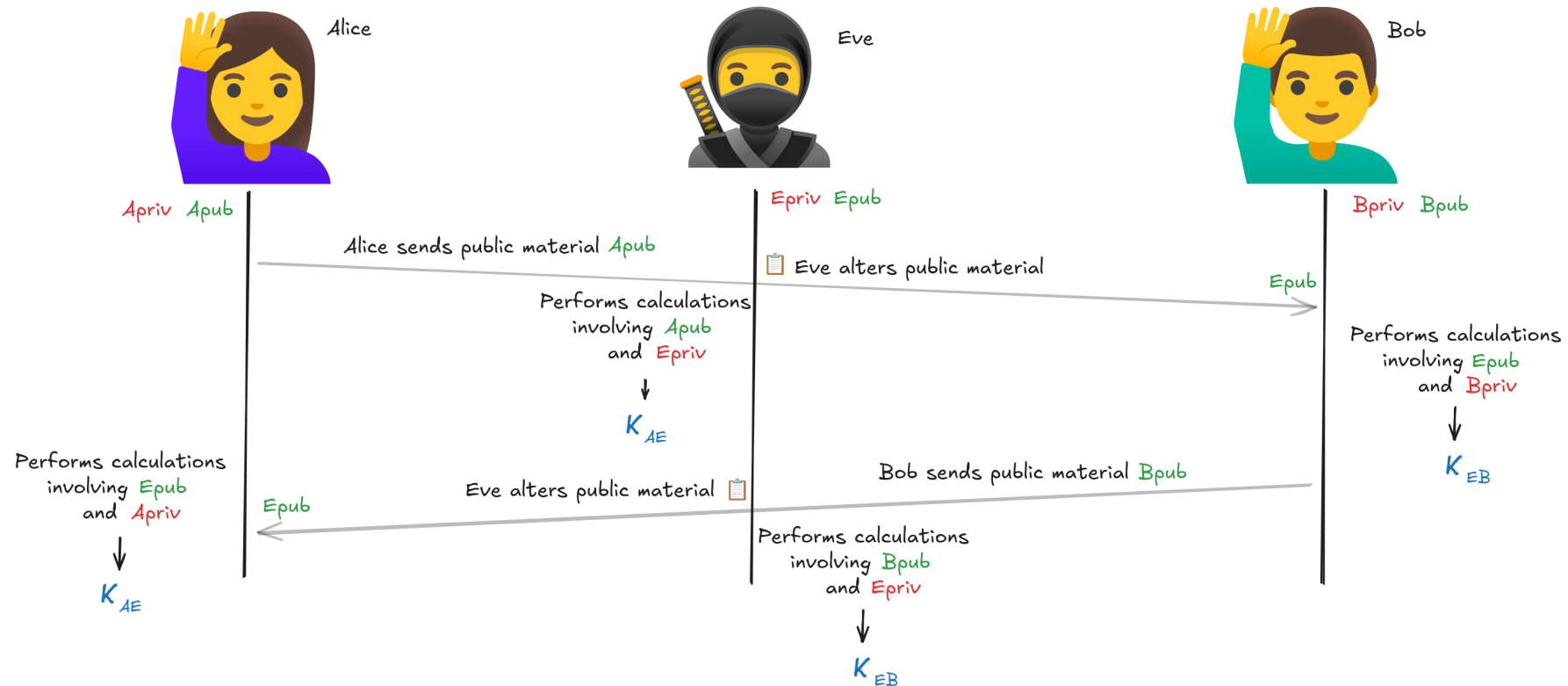


- **Securely agree on a shared secret key** thanks to asymmetric crypto
- **Over the untrusted internet**
- **Follow-up messages can be encrypted with K**

Modern crypto 101

Trust

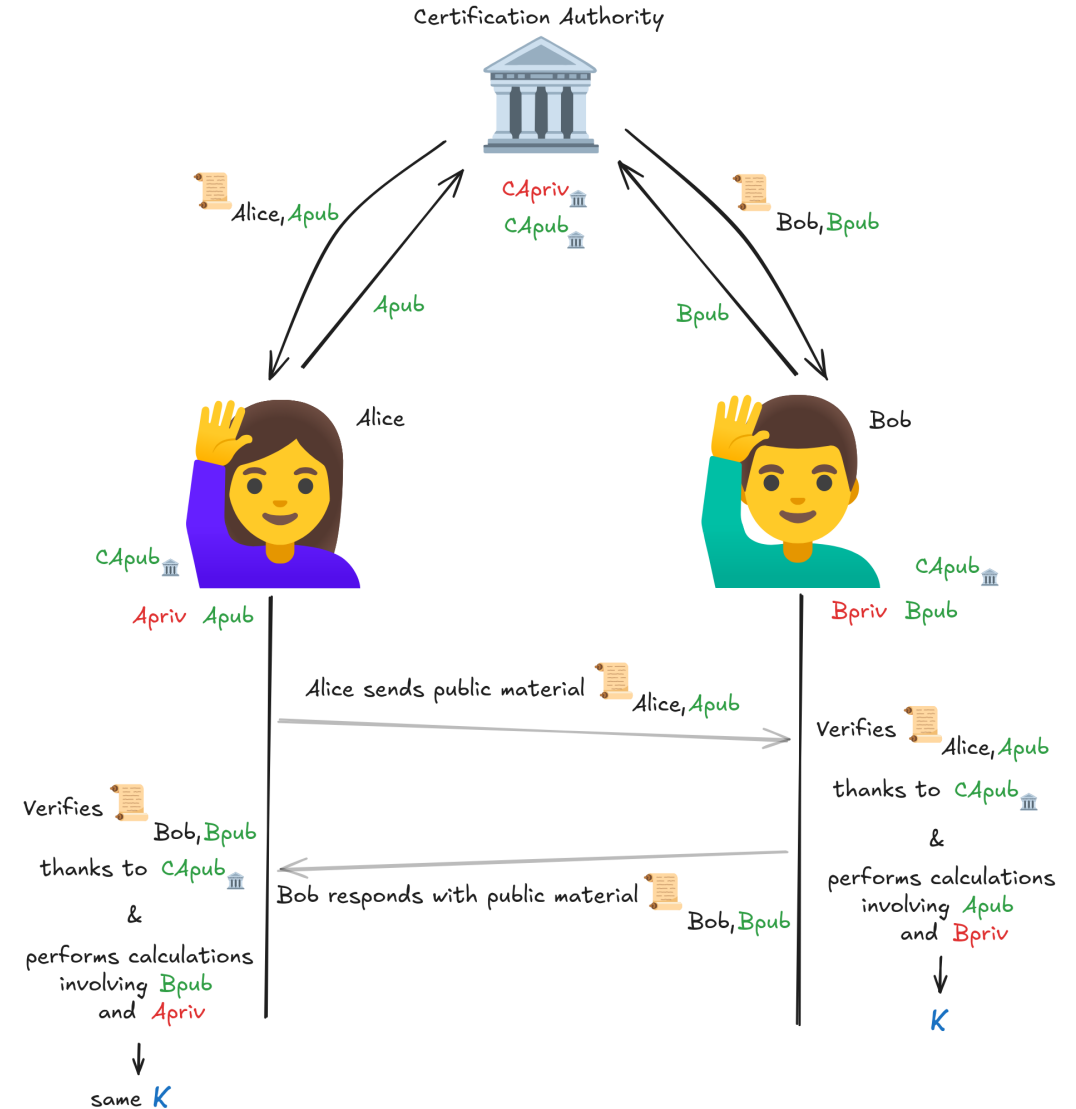
How can Alice trust Bob's public key?



Modern crypto 101

Certificates and signatures

- **Signature from a trusted Certificate Authority (CA)**
- It links a public key to an identity (Bob)
- Alice verifies the CA's signature thanks to a pre-trusted CA public key



Modern crypto 101

Security

- **Communications mainly rely on 3 primitives**
 - Signing data
 - Establishing a shared secret
 - Encrypting with symmetric algorithms
- **Security = difficulty for an attacker to falsify or decrypt information**
- **Difficulty = number of computational operations**
- **Good security: $>2^{100}$ operations**, impractical even in the next few decades
- **Example: AES-128**, symmetric scheme, best attack is bruteforcing the key, 2^{128} op.

A quantum threat to security

Quantum Computing vs. Crypto

- **Based on new principles:** Uses **qubits** instead of *classical* bits
- **Superposition:** Wave function, probability to read **0** / **1** for each bit
- **Entanglement:** Qubits can be linked, their states correlated
- Quantum computers can solve certain problems exponentially faster

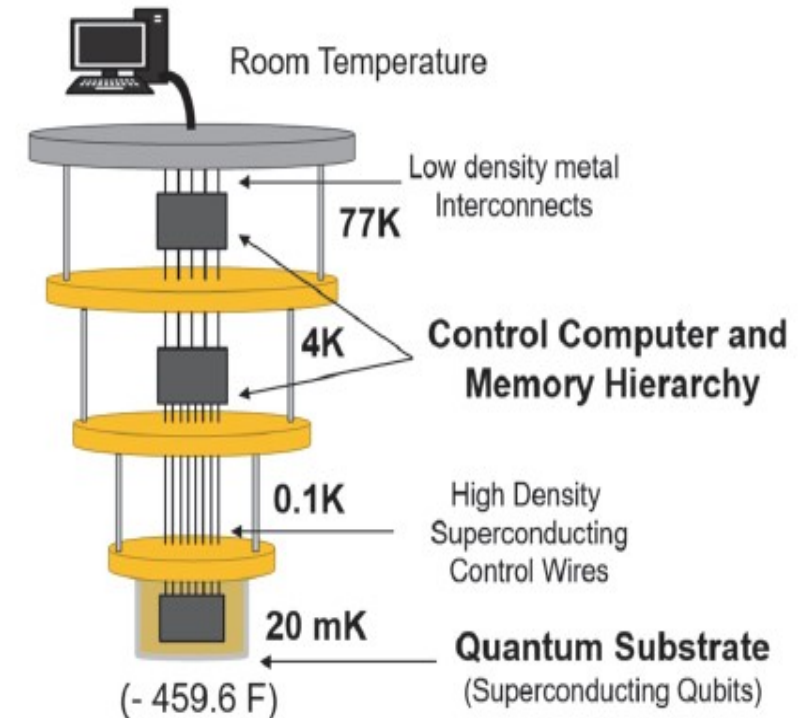


Image source: <https://attend.ieee.org/qc-dcep/purpose/>

Quantum Computing vs. Crypto

- **Shor's Algorithm:** finding periods in any function (n^3)
 - Breaks integer factorisation & discrete log
 - Asymmetric crypto in danger
 - **Example:** factoring a 2048-bit integer
 - Classical: 2^{112} operations → **secure** ✓
 - Quantum: 2048^3 ($\sim 2^{33}$) operations → **insecure** ✗
- **Grover's algorithm:** enhancing brute force, quadratic speedup ($2^n \rightarrow 2^{n/2}$)¹
 - Symmetric crypto in danger
 - **Example:** AES-128
 - Quantum: $\sim 2^{64}$ operations → **insecure** ✗
 - AES-256 stays secure vs. quantum computer, $\sim 2^{128}$ operations → **secure** ✓

1: <https://davidbkemp.github.io/animated-qubits/grover.html>

The impacts on our secure channel

So, what breaks in our Alice and Bob setup?

- **Key exchange (DH, ECC): broken! ❌**
 - Shor's algorithm solves their underlying math problems
- **Digital signatures (RSA, ECDSA): broken! ❌**
 - Also vulnerable to Shor. Certificates can be forged
- **Symmetric encryption (AES): weakened! ⚠️**
 - Grover's algorithm halves the effective key length
 - *Use AES-256 instead of AES-128*

Upgrading to post-quantum...

Upgrading to post-quantum

- **Need to find new math problems** that are hard for both classical and quantum computers
 - **Lattice-based problems:** ML-KEM, ML-DSA, Falcon, ...
 - **Code-based problems:** BIKE, HQC
 - **Hash-based problems:** SLH-DSA, XMSS
 - **Multivariate Quadratic polynomial equations:** UOV
 - ...
- **These algorithms run on classical computers**
 - Post-quantum is **not** quantum

Upgrading to post-quantum

Hybridization

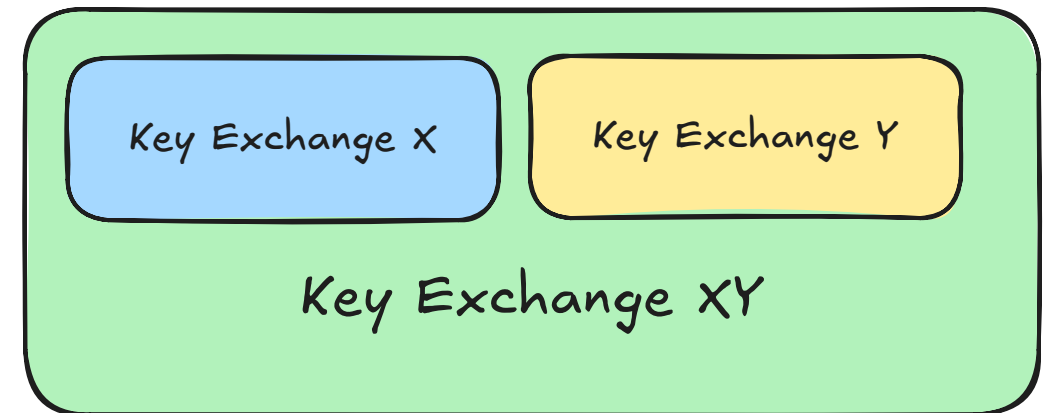
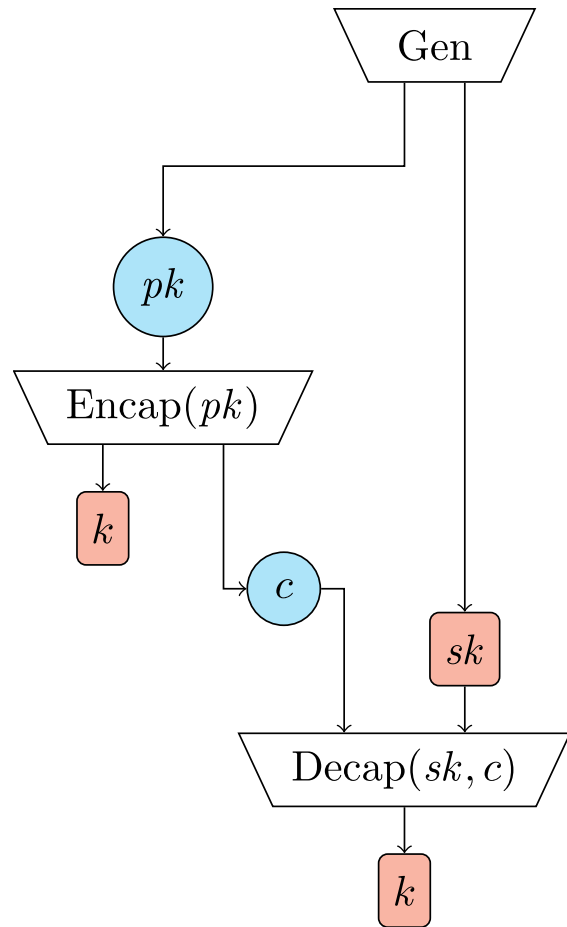
- **New algorithms are not "battle-tested"** 
 - e.g., SIDH, a former candidate, was broken in 2022
- **→ Hybridization**
 - Combine a classical algorithm (e.g., ECDH) with a PQC one (e.g., ML-KEM)
 - Security is at least as good as the strongest of the two
 - A crucial safety net if the PQC algorithm fails
 - See the recently-published articles on the Synacktiv blog ¹ ²

1: <https://www.synacktiv.com/en/publications/quantum-readiness-hybridizing-key-exchanges>

2: <https://www.synacktiv.com/en/publications/quantum-readiness-hybridizing-signatures>

Upgrading to post-quantum

Hybridization

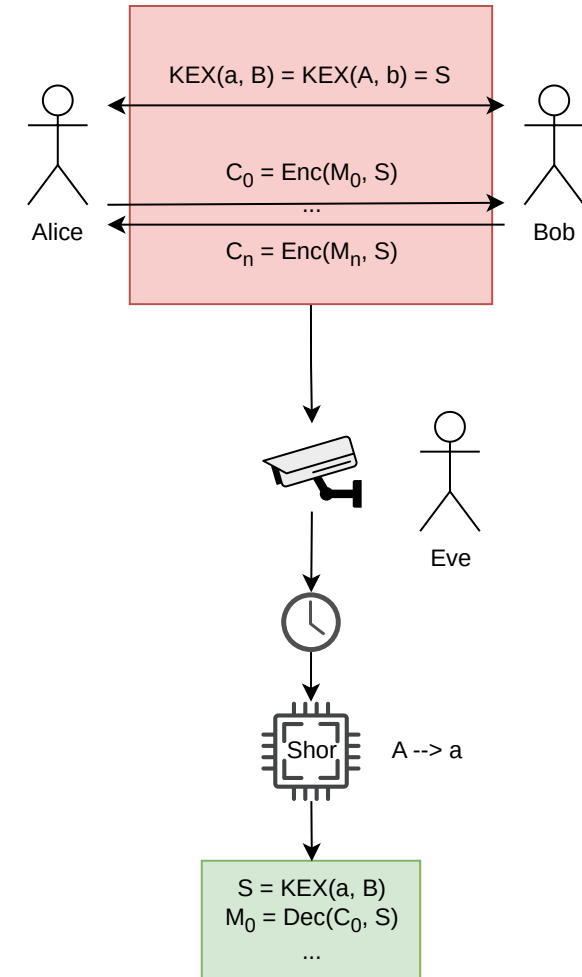


Left: https://en.wikipedia.org/wiki/Key_encapsulation_mechanism

Upgrading to post-quantum

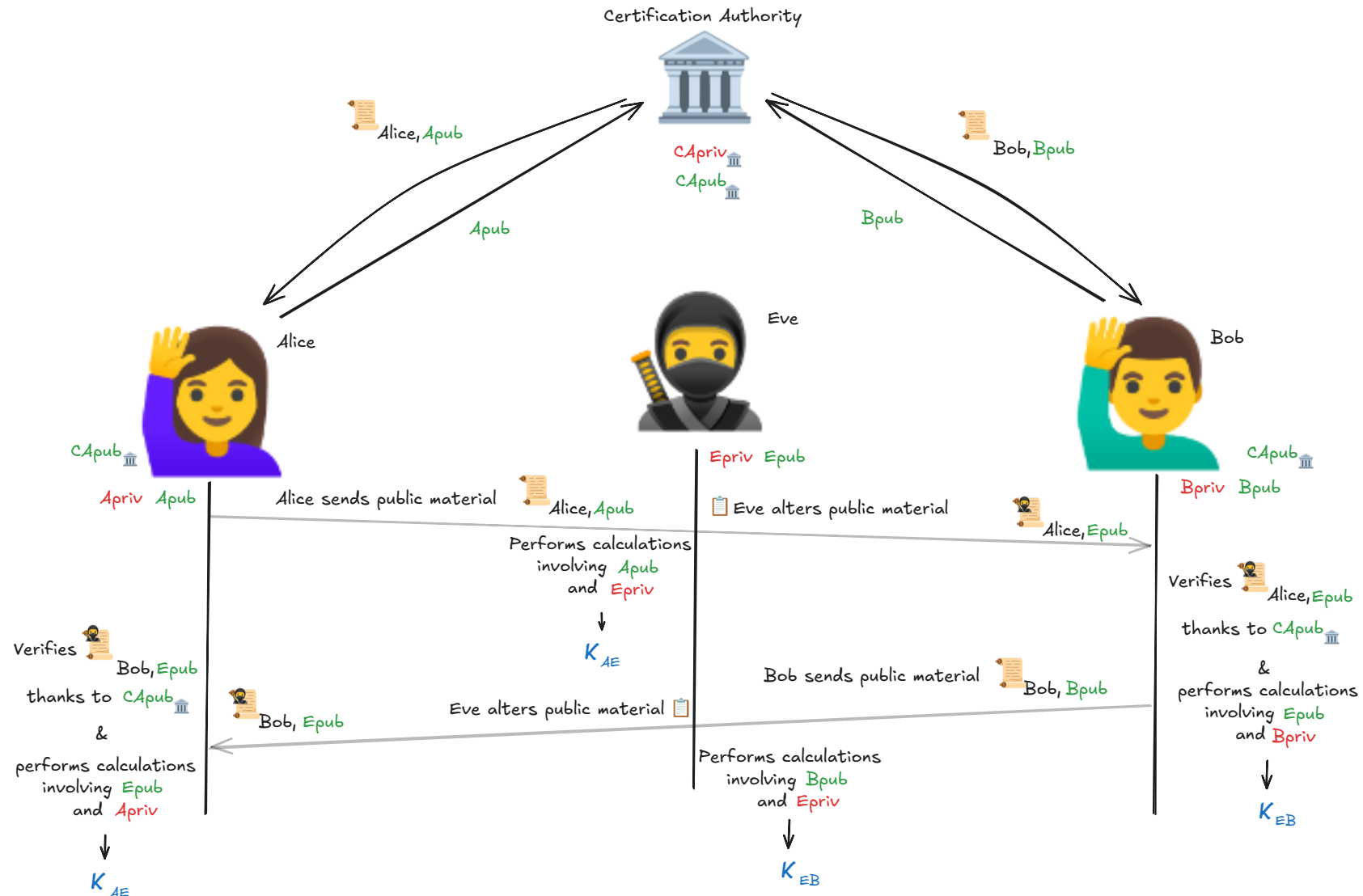
Issues to tackle

- **Today's issue:** Store now / Decrypt later
 - Upgrade key exchanges ASAP!
- **Tomorrow's issue:** Authenticating
 - Signature forgery with quantum computing
 - Update your keys / certificates to use PQ signature schemes
 - Needs regeneration of all secrets



Upgrading to post-quantum

Signature forgery



Upgrading to post-quantum

For organizations

- **Pre-requisite:** *What crypto do I use? Where do I use it in my organization?*
- **PQ transition may already have started in your organization**
 - Chrome >131 sends ClientHello with Hybrid ML-KEM / X25519 by default ¹
 - CloudFlare / Google / Azure support Hybrid ML-KEM / X25519
 - All major web reverse proxies support Hybrid ML-KEM / X25519 in their latest version
 - Recent OpenSSH (client & server) uses hybrid key exchange by default

1: <https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-support/>

Upgrading to post-quantum

For organizations

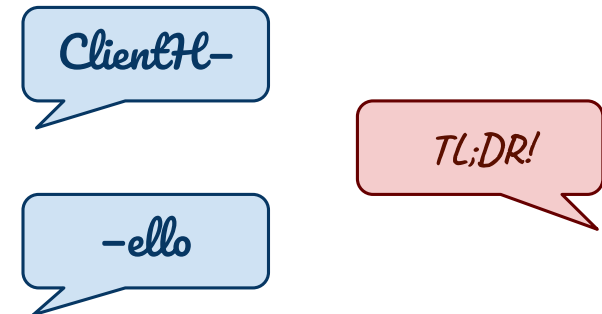
- **So it's *that* easy?**
 - You may use other stuff (MACSec? Exotic VPN?) with no automatic update process
 - Microsoft is *actively working to get PQC support to [their] Windows customers via the Windows TLS stack (Schannel)* ¹
 - All of the previous is for key exchanges, don't forget signatures !!
- **Check your infra and contact vendors!**

1: <https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-comes-to-windows-insiders-and-linux/4413803>

Upgrading to post-quantum

Some bugs along the way

-  **PQC algorithms have much larger keys and signatures**
- **Sometimes broke existing protocols and systems¹**
 - Large PQC keys may not fit in a single TCP packet
 - → fragmented ClientHello / ServerHello
 - Packet fragmentation can cause network gear to fail



¹: See <https://tldr.fail/> & <https://blog.cloudflare.com/post-quantum-to-origins/#when-things-break-and-how-to-move-forward>

... and auditing it!

... and auditing it!

The math is new, but the audit process is not.

Auditing PQC implementations is like auditing classical crypto.

- **Verify standards compliance**
 - Uses standard parameters (e.g., NIST FIPS 204)?
 - Passes all official **test vectors**?
- **Hunt for implementation bugs and leaks**
 - Random number generation
 - Key management
 - Look for common **side-channel vulnerabilities**
 - **Timing attacks**: Is execution time constant?
 - **Cache attacks**: Do memory access patterns leak secrets?
 - **Physical attacks**: Power analysis, EM emissions, ...

If you can audit classical crypto implementations now, you can audit PQ crypto implementations now.

Questions ?



<https://www.linkedin.com/company/synacktiv>



<https://x.com/synacktiv>



<https://bsky.app/profile/synacktiv.com>



<https://synacktiv.com>