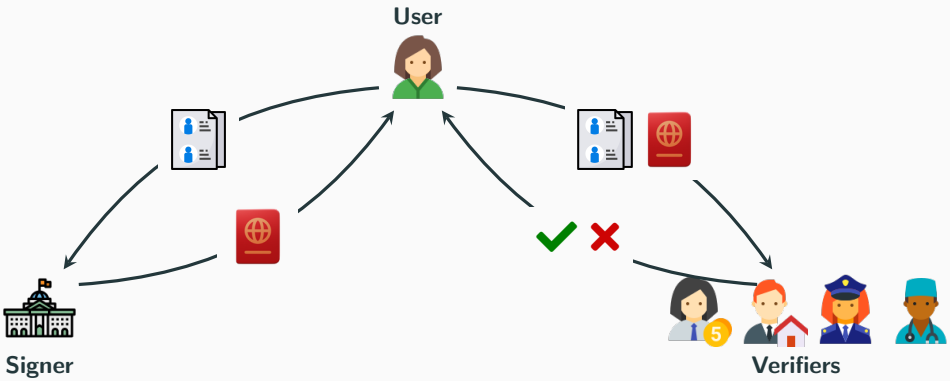
Orange
Innovation

Design of Advanced Post-Quantum Signatures

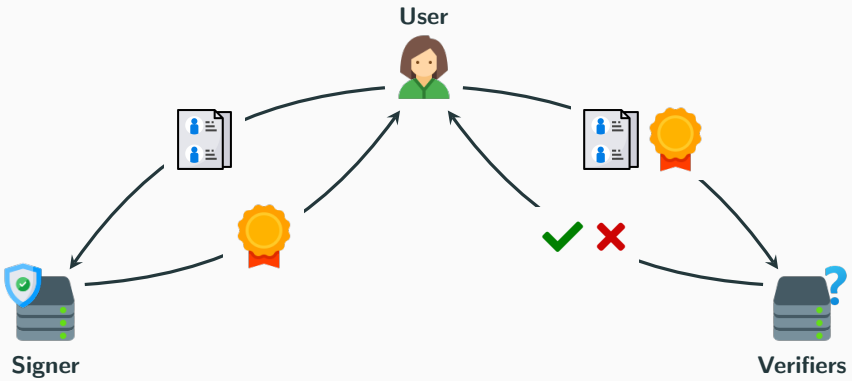
Corentin Jeudy

orange™

Signatures: Physical and Digital



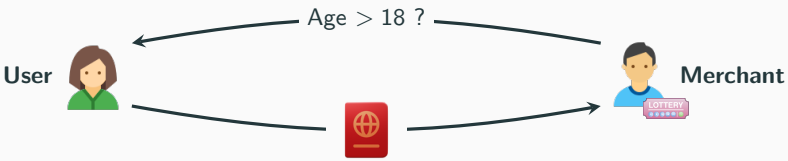
Signatures: Physical and Digital



Allows to certify digital data, and later prove its authenticity. What more do we need?

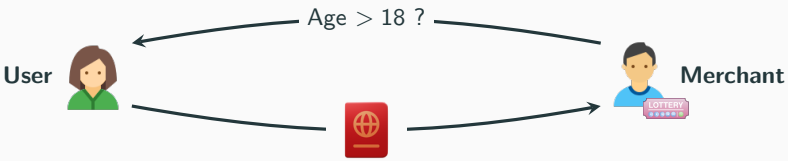
Example: Age Control

Temporarily showing an ID document to attest you are of age is **not really a privacy issue**.

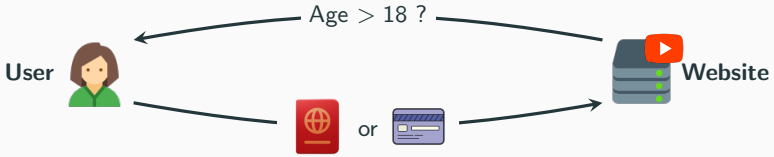


Example: Age Control

Temporarily showing an ID document to attest you are of age is **not really a privacy issue**.

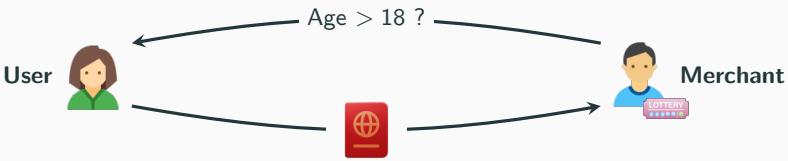


Sending an ID document or credit card to a website is more **permanent**. It can **store**, **share**, **exploit**. Requires **trust**.

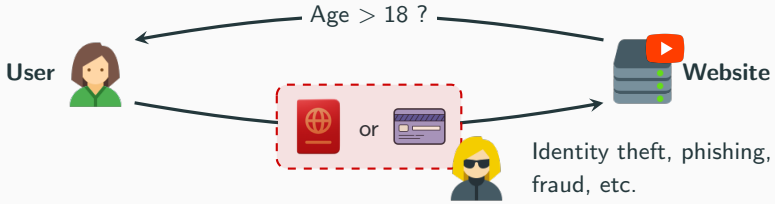


Example: Age Control

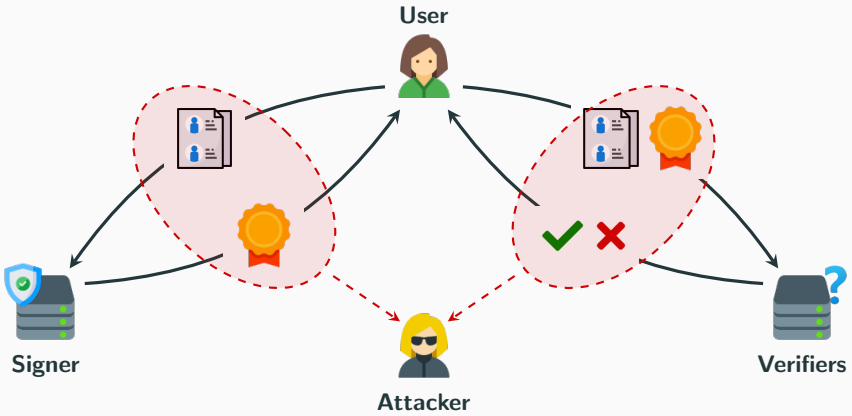
Temporarily showing an ID document to attest you are of age is **not really a privacy issue**.



Sending an ID document or credit card to a website is more **permanent**. It can **store**, **share**, **exploit**. Requires **trust**.

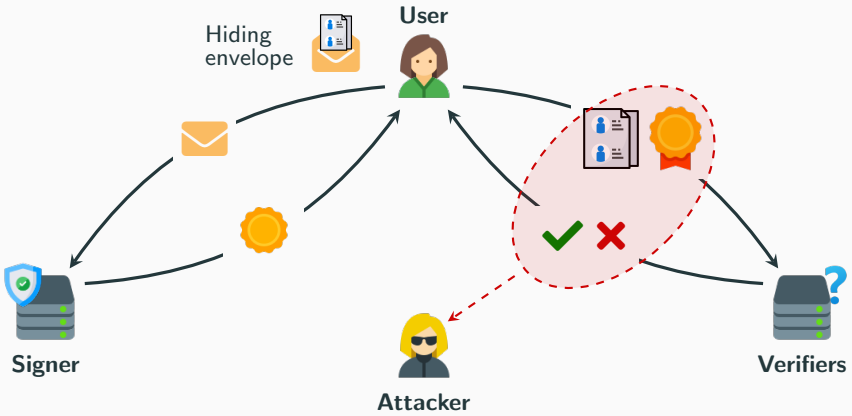


Adding Privacy



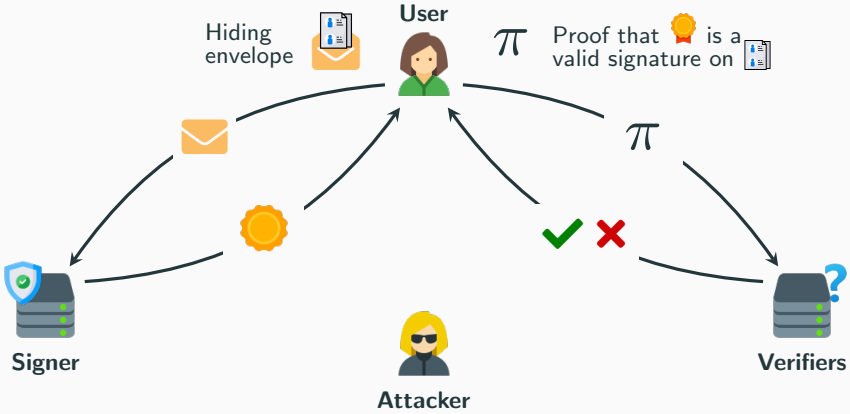
No control over the disclosed information: Verifiers (and attacker) learn everything
Simple but *not suited for privacy*

Adding Privacy



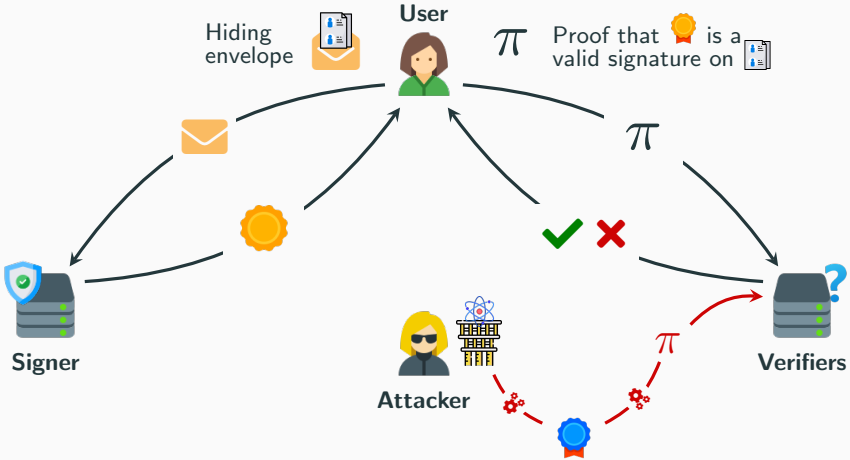
No control over the disclosed information: Verifiers (and attacker) learn everything
Simple but *not suited for privacy*

Adding Privacy



Full control of user information: Selective disclosure to verifiers (and attacker)
But need for *more complex tools*: hiding envelope, specific signature, proofs

Adding Privacy

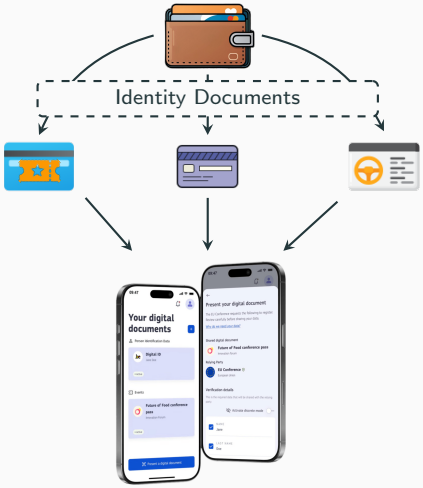


Quantum-enabled attacker could **forge valid credentials**:
Quantum risk of impersonation. Need for **Post-Quantum** solutions!

Privacy as Positive Differentiator in Use-Cases: Digital Identity

European Digital Identity (EUDI) Wallet initiative

"a safe, reliable, and private means of digital identification for everyone in Europe."



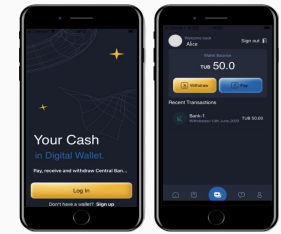
Emphasis on

- **Anonymity**
- **Unlinkability**
- **Selective disclosure**

Anonymous Credentials

Privacy as Positive Differentiator in Use-Cases: Digital Cash

Digital Euro initiative (ECB) & **Project Tourbillon** (BIS & SNB)
"would not identify you or track your payments [...] for cash-like privacy"



Emphasis on

- **(Payer) Anonymity**
- **Unlinkability**
- **Scalability**

Anonymous Credentials

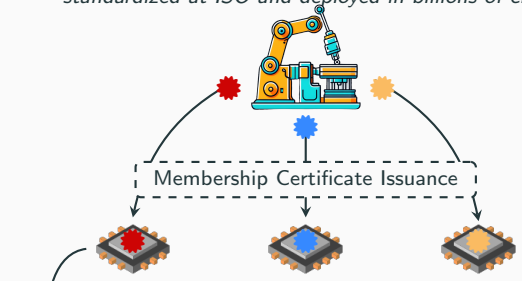
Blind Signature

eCash

Privacy as Positive Differentiator in Use-Cases: Trusted Computing

Group Attestation with **Built-in Revocation Mechanisms**

"standardized at ISO and deployed in billions of chips (TPM, Intel)"



Emphasis on

- **Anonymity**
- **Unlinkability**
- **Revocability**

Anonymous Credentials

eCash

EPID

(group signatures)

Our Framework: Practical Post-Quantum Privacy

Our Framework

Fast

Implementation with efficient runtimes aligned with UX requirements

Versatile

Many privacy-driven applications

Compact

Small credentials and credential proofs

Robust

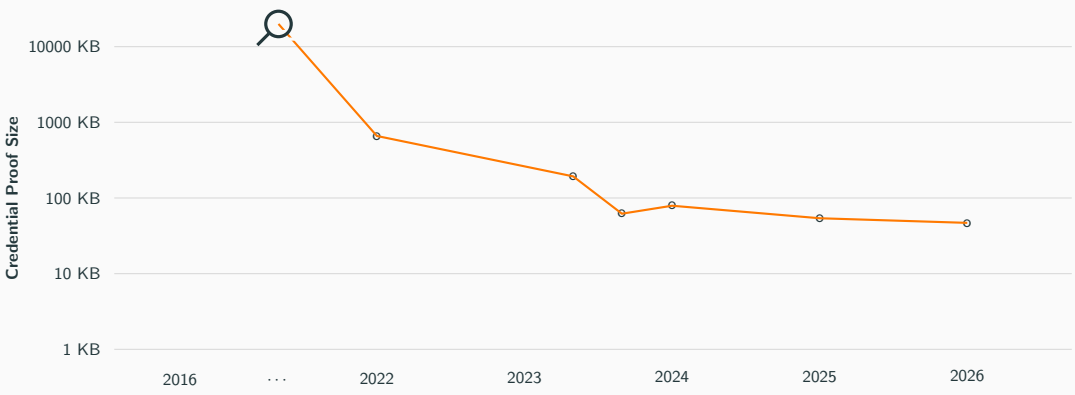
Post-quantum secure on well-studied assumptions from lattices

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

Our (several iterations) framework vastly improved **post-quantum anonymous credentials**

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

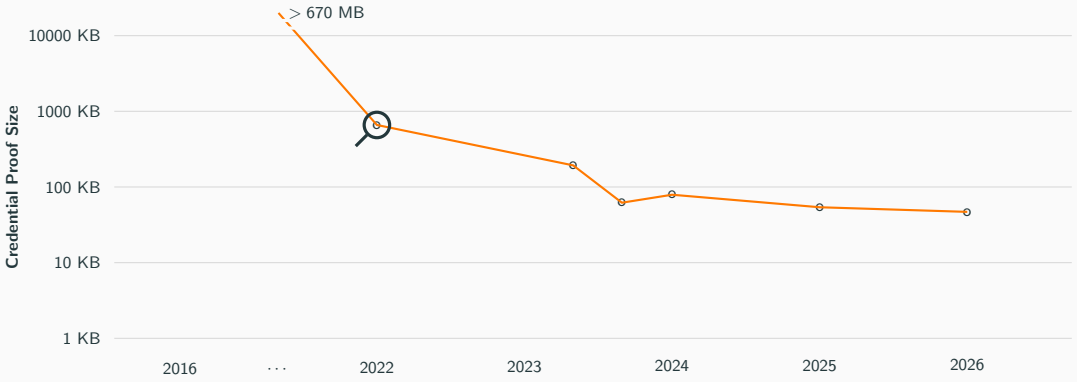
Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



$>$ **670 000 KB** (Asiacrypt 2016, ENS Lyon)

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

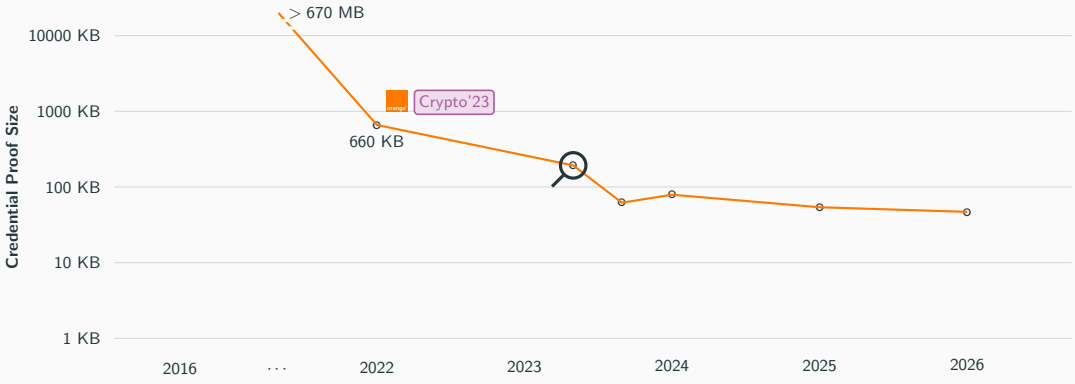
Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



660 KB (Crypto 2023, **Orange**)

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

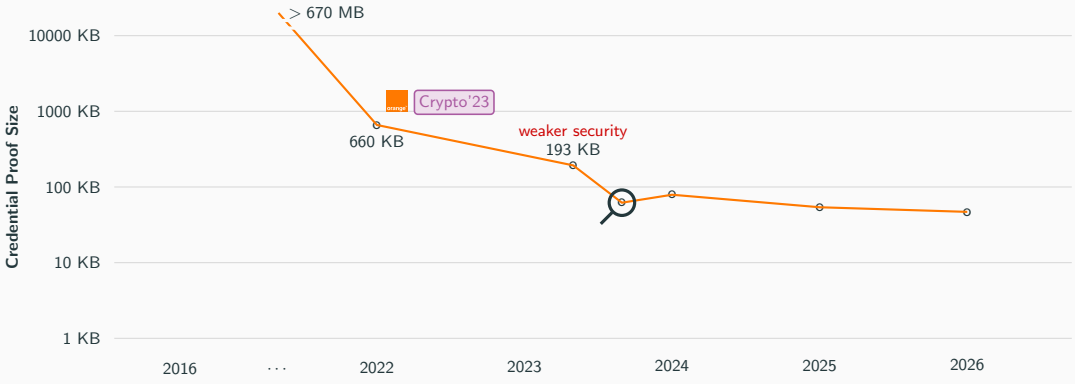
Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



193 KB (not published, Shaanxi & Brown University, weakened security model)

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

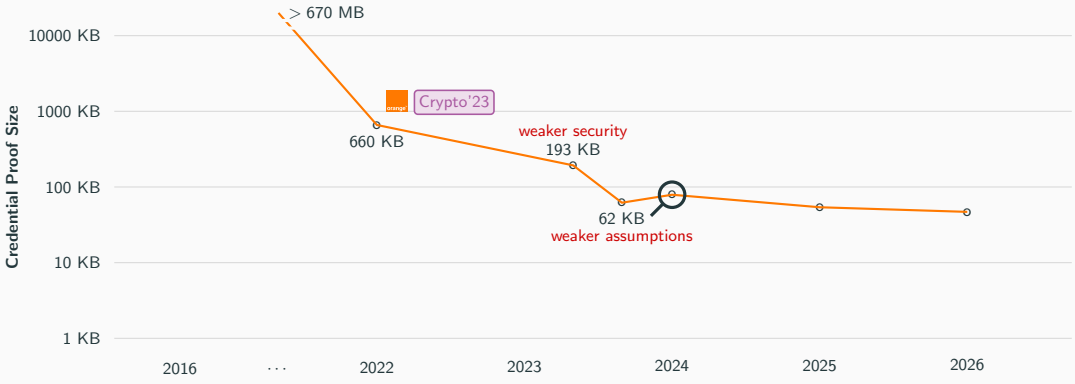
Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



62 KB (Crypto 2023, IBM, weakened security assumptions)

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

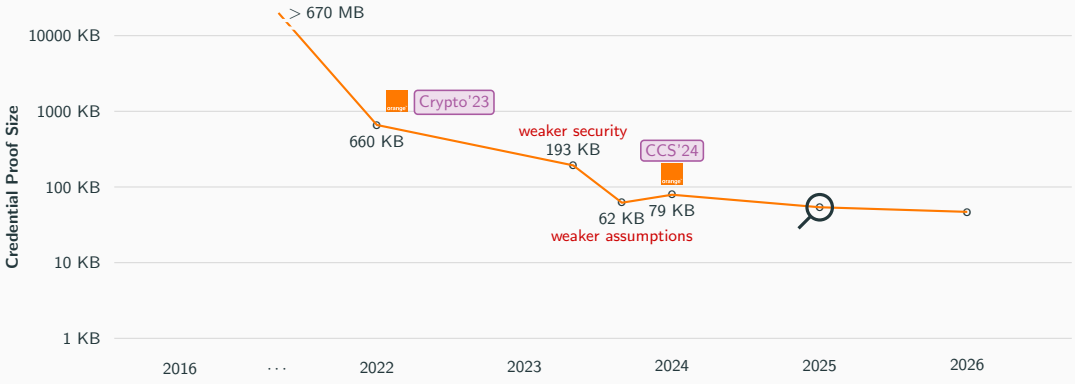
Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



79 KB (CCS 2024, **Orange** & Bochum University, standard security model and assumptions)

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

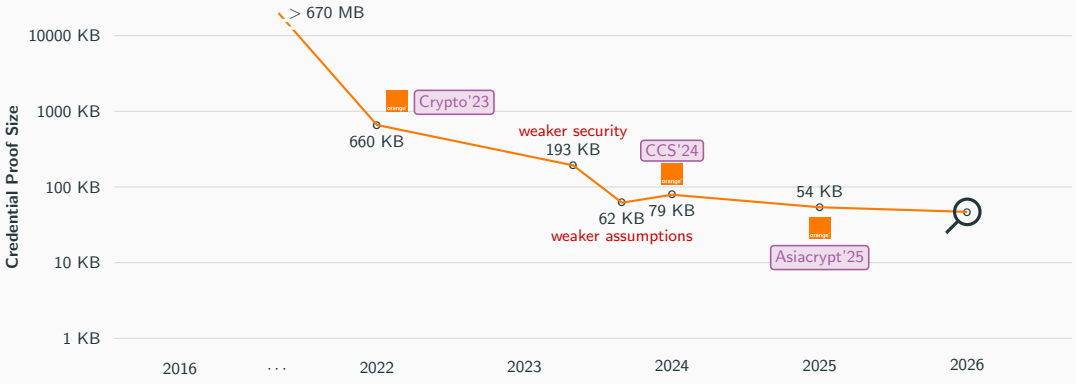
Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



54 KB (Asiacrypt 2025, **Orange**, standard security model and assumptions)

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

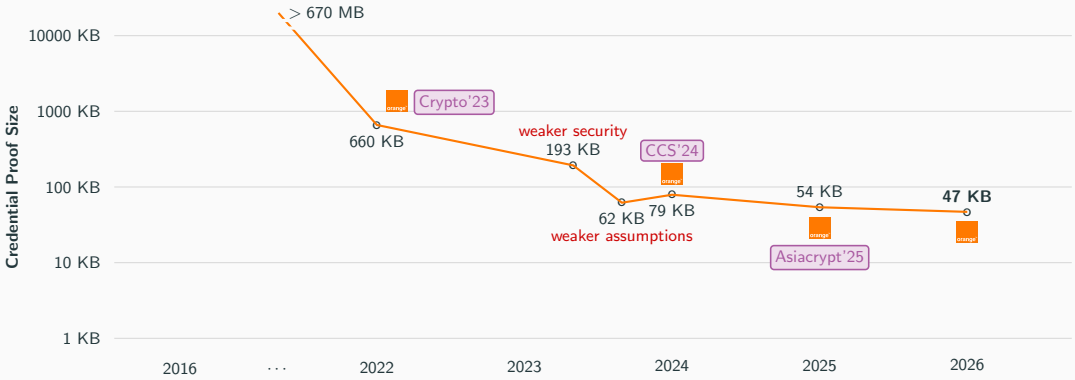
Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



47 KB (submitted at Asiacrypt 2026, **Orange**, standard security model and assumptions)

Zoom on Performance: Evolution of Post-Quantum Anonymous Credentials

Our (several iterations) framework vastly improved **post-quantum anonymous credentials**



Orange
Innovation

Thank You

orange™