ETSI/IQC Quantum Safe Cryptography Conference 2026

Certification-ready security proofs for quantum key distribution

Presented by: Devashish Tupkary

18/06/2026

Protocol Security Status

What people hear (short version)
“There are no full security proofs of QKD”

Position Paper on
Quantum Key Distribution

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

What the France/Sweden/Netherlands/Germany Position paper says:

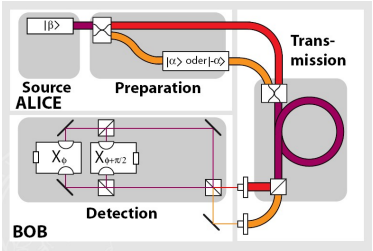
“QKD security proofs
… QKD protocols can provide security based on quantum-physical principles without requiring assumptions about the hardness of mathematical problems. … A security proof should describe the QKD protocol in a precise mathematical model with well-stated assumptions, and derive a precise statement expressing and quantifying the security of the protocol in this model. In order for a security proof, which is purely theoretical and conducted in an abstract model, to relate to the security of an actual implementation in a meaningful way, the security statement should be proved in a model that reflects realistic conditions as much as possible.
…
However, to the best of our knowledge, no security proof for a practically relevant protocol has been written up in a cohesive and comprehensive way that satisfies the requirements outlined above. “

➔ In short: there is no scientific reference available which gives a self-contained mathematical security proof for a practical protocol
➔ It does not mean such a paper cannot be written …

Protocol Security

Actual Device
e.g. reality based

modelling



Mathematical Model of protocol
Quantum Optics,
Randomness,
Classical post-processing...

Security Proof

We deal with Protocol Security (rigorous math ...)

Implementation Security
(best practice ...)

Requirements for security proofs

It must

- specify a **complete** protocol relevant to **practical** implementations.
- clearly **state all assumptions**.
- precisely state the **security criterion**.
- provide a **rigorous mathematical proof** that, under the stated assumptions, the protocol achieves the desired level of security with the specified parameters.

NO such proof existed for a practical protocol!

Rigor + Generality

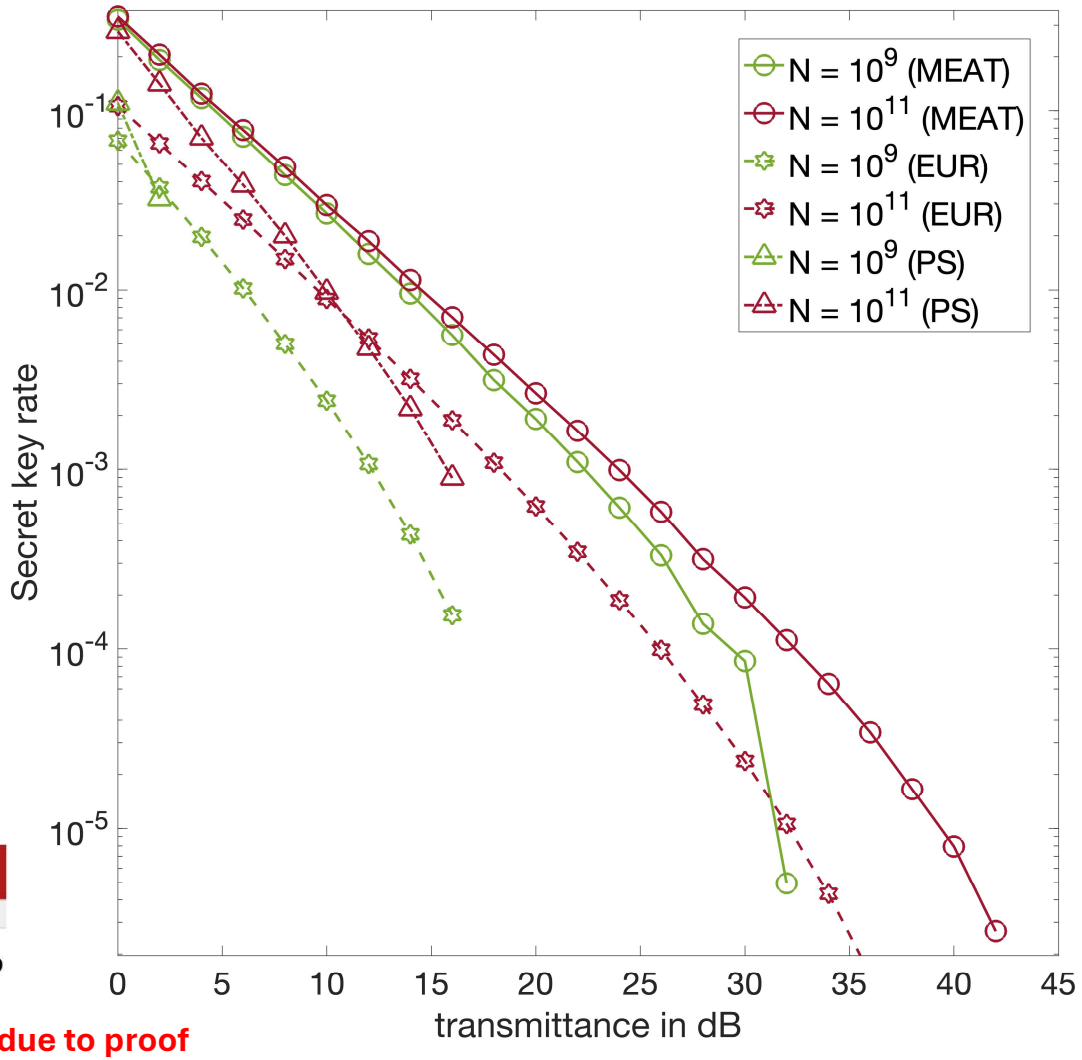
Symbol	Meaning
$n \in \mathbb{N}$	Total number of rounds of the QKD protocol.
$\sigma_k^{(j)} \in \mathrm{S}_=(A')$	The kth signal state sent by Alice, in round j.
$p_k^{(j)} \in [0,1]$	Probability with which Alice sends kth signal state in round j.
$M_k^{(j)} \in \mathrm{Pos}(B_j)$	The POVM element corresponding to for outcome k of Bob's measurement in the jth round.
$f_{\mathrm{ann}}^{(j)} : \mathcal{X} \otimes \mathcal{Y} \to \widehat{\mathcal{C}}$	Function mapping Alice and Bob's local data (X_j, Y_j) to public announcements, for the jth round.
$f_{\mathrm{kmap}}^{(j)}(\cdot,\cdot) : \mathcal{X} \times \widehat{\mathcal{C}} \to \mathcal{S}$	Function implementing the mapping Alice's local data stored in X_j to S_j, based on public announcements stored in $\widehat{C}_j$, for round j.
$\lambda_{\mathrm{EC}}(\cdot) : \widehat{\mathcal{C}}^n \to \mathbb{N}$	Function that determines the number of transcripts of error-correction protocol, as a function of public announcements $\widehat{C}_1^n$.
$\ell(\cdot) : \widehat{\mathcal{C}}^n \to \mathbb{N}$	Function that determines the number of bits of output key, as a function of public announcements $\widehat{C}_1^n$.
$\varepsilon_{\mathrm{EV}} \in [0,1]$	Epsilon for error-verification. Determines output length of hash family used in error-verification, and the final correctness parameter.
$\varepsilon_{\mathrm{PA}} \in [0,1]$	Epsilon for privacy amplification. The exact input and output lengths are determined by the protocol during runtime.
$\mathcal{F}_{\mathrm{hash}}\,(l_{\mathrm{in}}, l_{\mathrm{out}})$	Universal$_2$ hash family from l_{in} bits to l_{out} bits. Used for error-verification. The exact input and output lengths are determined by the protocol during runtime.
$\mathcal{F}_{\mathrm{hash}}^{\mathrm{ideal}}\,(l_{\mathrm{in}}, l_{\mathrm{out}})$	Ideal universal$_2$ hash family from l_{in} bits to l_{out} bits. Used for privacy-amplification.

TABLE VIII: Parameters required to define an instance of Generic QKD Protocol.

- Protocol is specified via abstract elements. Same framework can be applied to different protocols.
- Framework is general enough to apply to practical decoy-state BB84 + variations.
- Proof is written in transparent manner to allow for third-party verification.

Tight performance

We used MEAT, which performs better than other proof techniques (and allows more freedom in protocol design).



arXiv > quant-ph > arXiv:2502.02563

Quantum Physics

[Submitted on 4 Feb 2025 (v1), last revised 25 Jul 2025 (this version, v4)]

Marginal-constrained entropy accumulation theorem

Amir Arqand, Ernest Y.-Z. Tan

arXiv > quant-ph > arXiv:2504.12248

Quantum Physics

[Submitted on 16 Apr 2025 (v1), last revised 13 Oct 2025 (this version, v2)]

Rényi security framework against coherent attacks applied to decoy-state QKD

Lars Kamin, John Burniston, Ernest Y.-Z. Tan

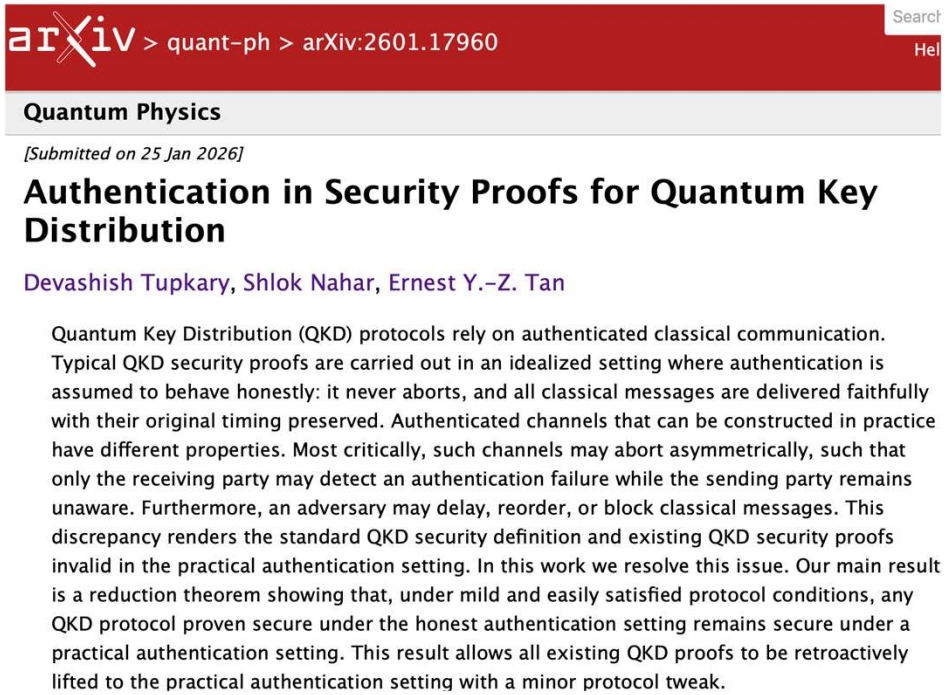
*** Not exactly the same protocol is compared due to proof technique variations…**

Many issues in rigorously combining all elements!

1. ***Authentication assumption:*** Typically assumed that all messages sent are received correctly (+some assumptions on timing).

2. ***Authentication reality:*** Eve can try tamper messages, affect timings. Some of her attempts will lead to authentication failure (with high prob). If authentication fails, only *receiving* party notices!

3. How do Alice and Bob coordinate decisions? (such as whether they accept or abort)?



arXiv > quant-ph > arXiv:2601.17960

Search

Hel

Quantum Physics

[Submitted on 25 Jan 2026]

Authentication in Security Proofs for Quantum Key Distribution

Devashish Tupkary, Shlok Nahar, Ernest Y.-Z. Tan

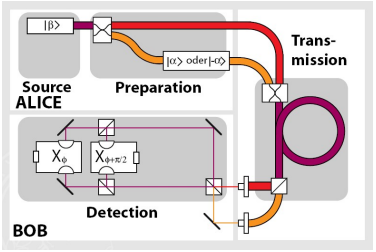
Quantum Key Distribution (QKD) protocols rely on authenticated classical communication. Typical QKD security proofs are carried out in an idealized setting where authentication is assumed to behave honestly: it never aborts, and all classical messages are delivered faithfully with their original timing preserved. Authenticated channels that can be constructed in practice have different properties. Most critically, such channels may abort asymmetrically, such that only the receiving party may detect an authentication failure while the sending party remains unaware. Furthermore, an adversary may delay, reorder, or block classical messages. This discrepancy renders the standard QKD security definition and existing QKD security proofs invalid in the practical authentication setting. In this work we resolve this issue. Our main result is a reduction theorem showing that, under mild and easily satisfied protocol conditions, any QKD protocol proven secure under the honest authentication setting remains secure under a practical authentication setting. This result allows all existing QKD proofs to be retroactively lifted to the practical authentication setting with a minor protocol tweak.

What about implementation security?

Actual Device
e.g. reality based

modelling

Try to absorb as many imperfections / side-channels as possible in the model, and handle it within the mathematical proof



Mathematical Model of protocol
Quantum Optics,
Randomness,
Classical post-processing

Security Proof

We deal with Protocol Security (rigorous math ...)

Implementation Security
(best practice ...)

Clear path to handling imperfections

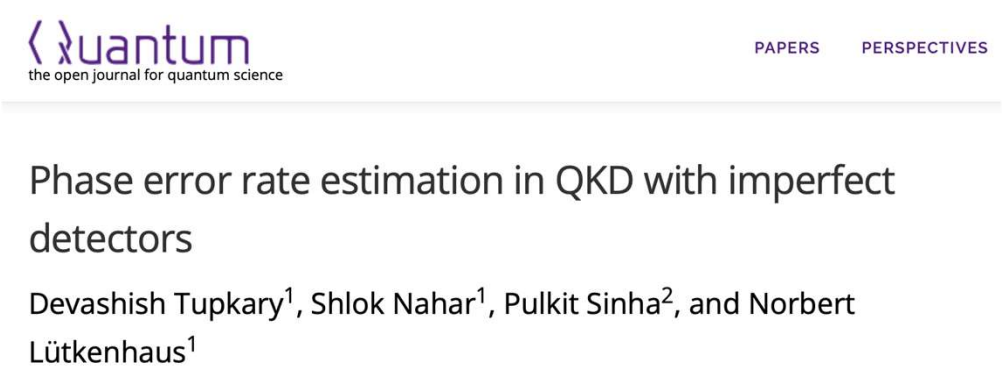
- Modularity allows a clear path to handling imperfections in devices.
- Many isolated results, frameworks for handling imperfections exist. The missing step is the combination.
- We are working on a follow-up work to accomplish this task.

What if I have my own security proof…..

1. ***Is it correct?*** Does it avoid all the gaps pointed out in this review?

2. ***Does your protocol fit the analysis exactly?*** There are many protocol variations!

3. ***Do you know how to handle imperfections?*** If proof contains “phase error rate”, it almost certainly assumes perfectly identical detectors!

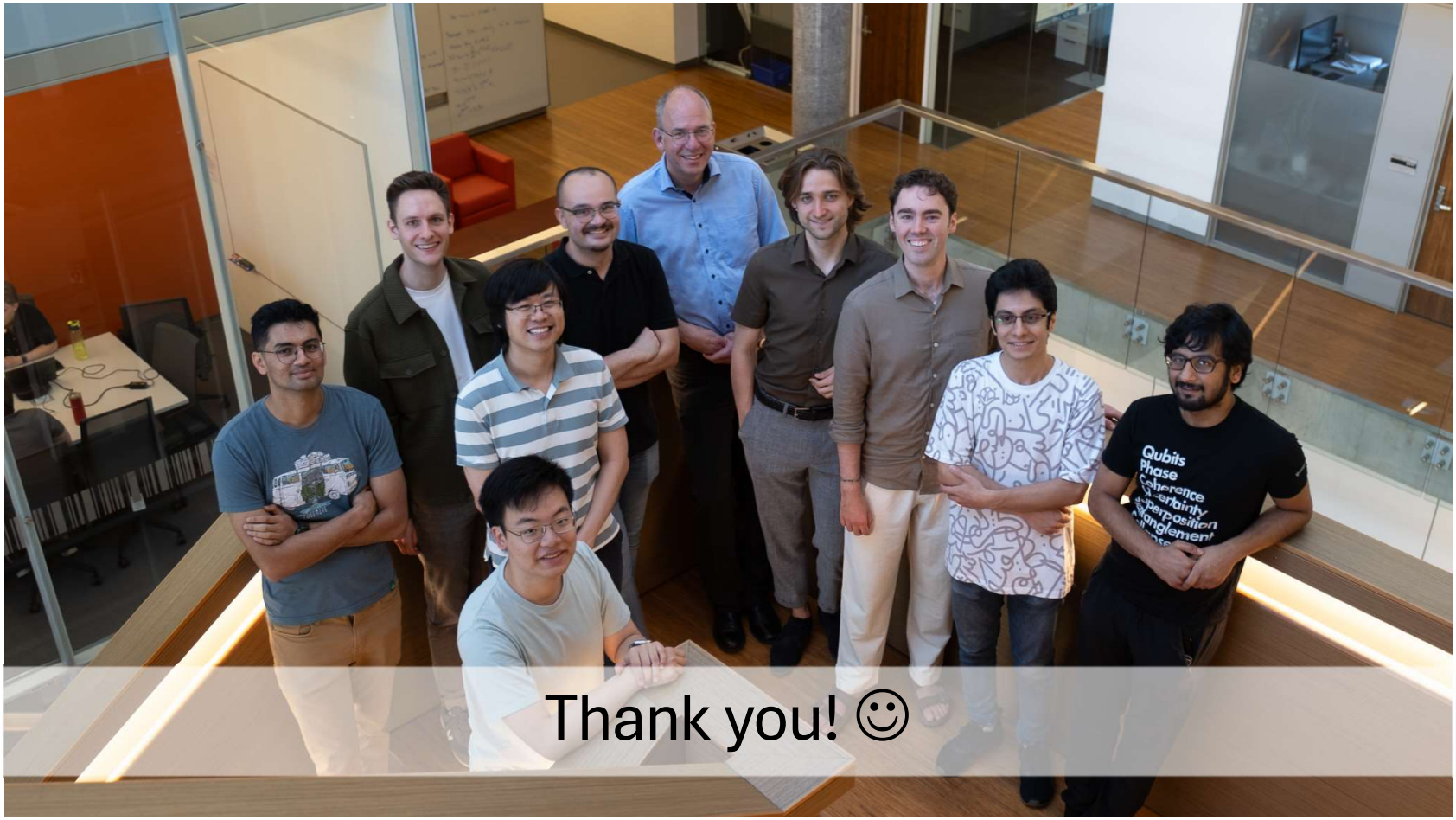


Many pending questions….

1. ***Numerics:*** Key rate requires one to solve a convex optimization problems, for which one requires *reliable* bounds. What are the requirements for such calculations?

2. ***Combining imperfections / side channels?:*** What are reasonable models of imperfections and countermeasures? (and how should they be certified?). What is the resulting impact on performance?.

3. ***Standardized protocol across vendors:*** While we can accommodate a wide class of protocols, which specific variation should we standardize?



Thank you! ☺

Marginal-constraint EAT

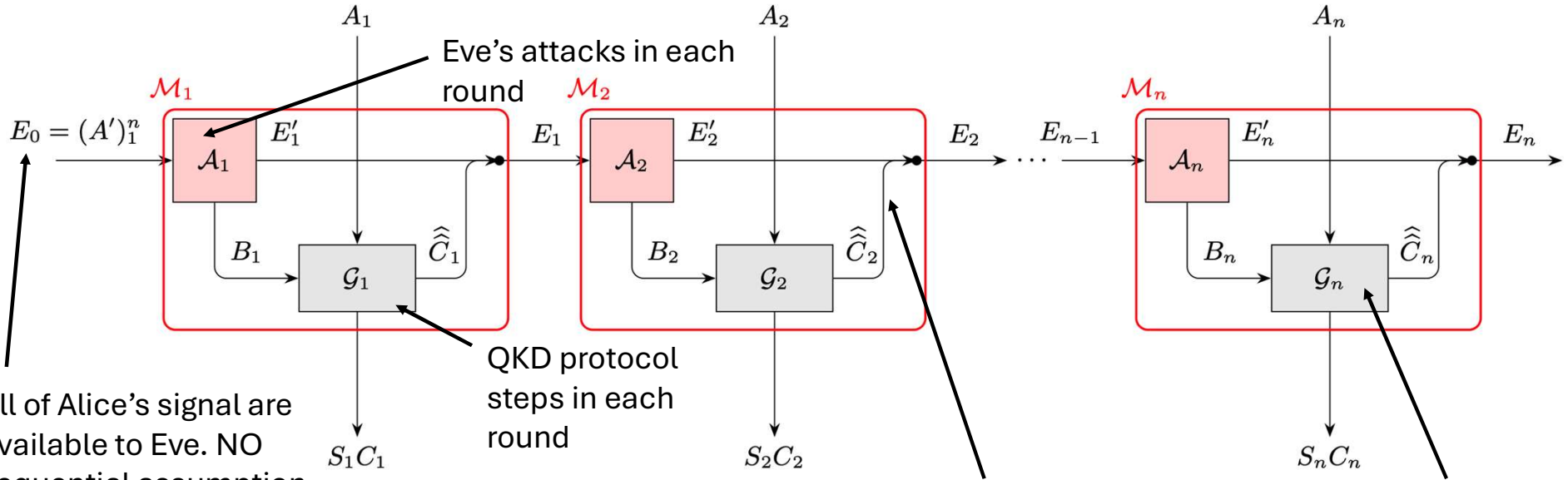
arXiv > quant-ph > arXiv:2502.02563

Quantum Physics

[Submitted on 4 Feb 2025 (v1), last revised 25 Jul 2025 (this version, v4)]

Marginal-constrained entropy accumulation theorem

Amir Arqand, Ernest Y.-Z. Tan



Eve's attacks in each round

All of Alice's signal are available to Eve. NO sequential assumption.

QKD protocol steps in each round

On-the-fly announcements:
Eve can modify attack based on announcements.

Minimal conditions on per-round protocols:
In fact, it can *change* between rounds! Can handle imperfections.

S: Secret Data.
C: Public announcements