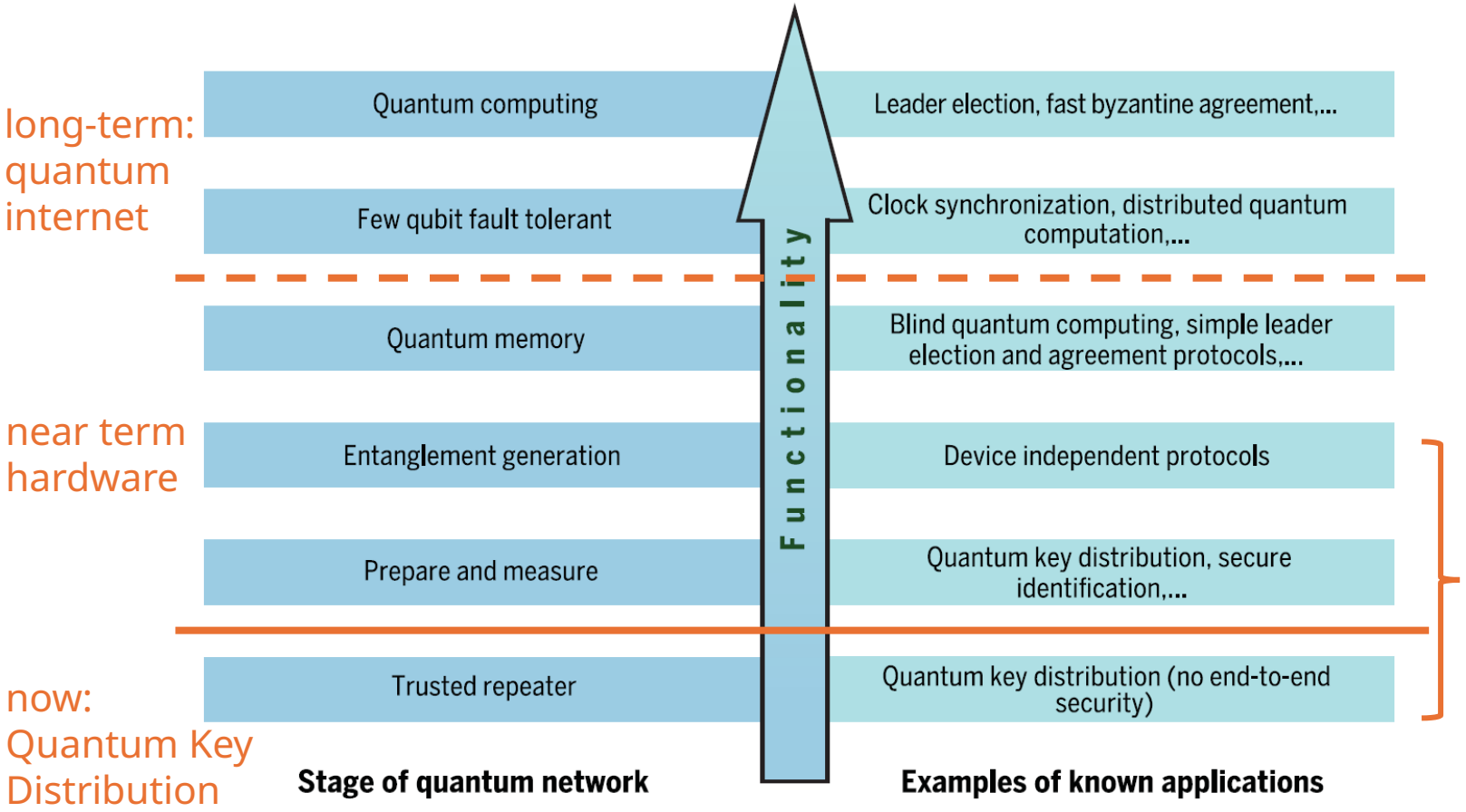
What can we do with near-term Quantum Networks?

Garazi Muguruza Lasa

21st July, 2026

What is a quantum network: node capabilities

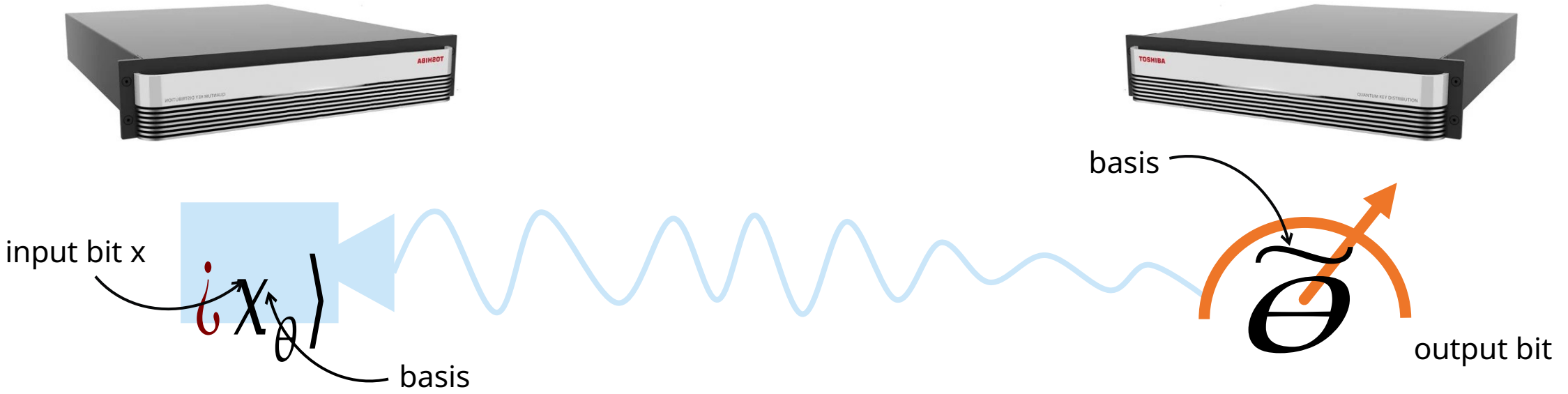


Can we use the QKD infrastructure of today (except distance) for other applications?

Quantum internet: A vision for the road ahead
S. Wehner, D. Elkouss, R. Hanson *Science* 362.6412 (2018): eaam9288. **See RFC 9583**.

Funded by the European Union

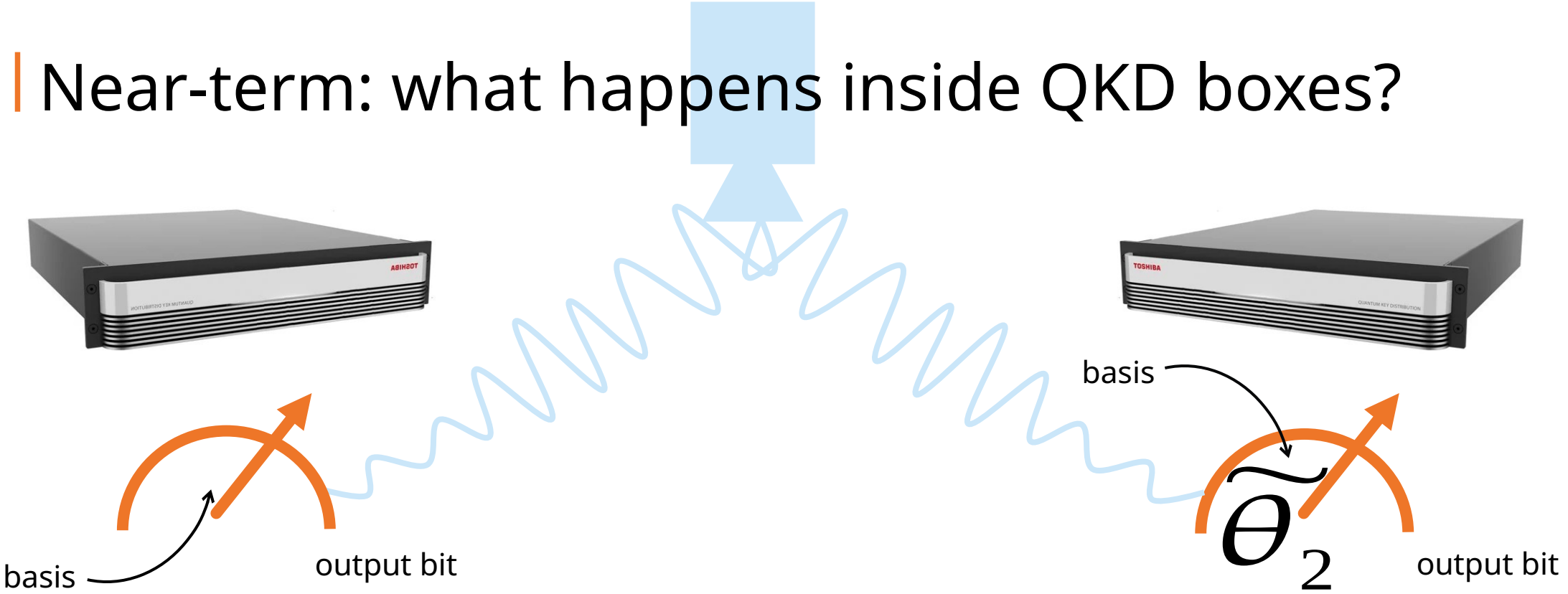
Near-term: what happens inside QKD boxes?



Classical post-processing:
share partial information about

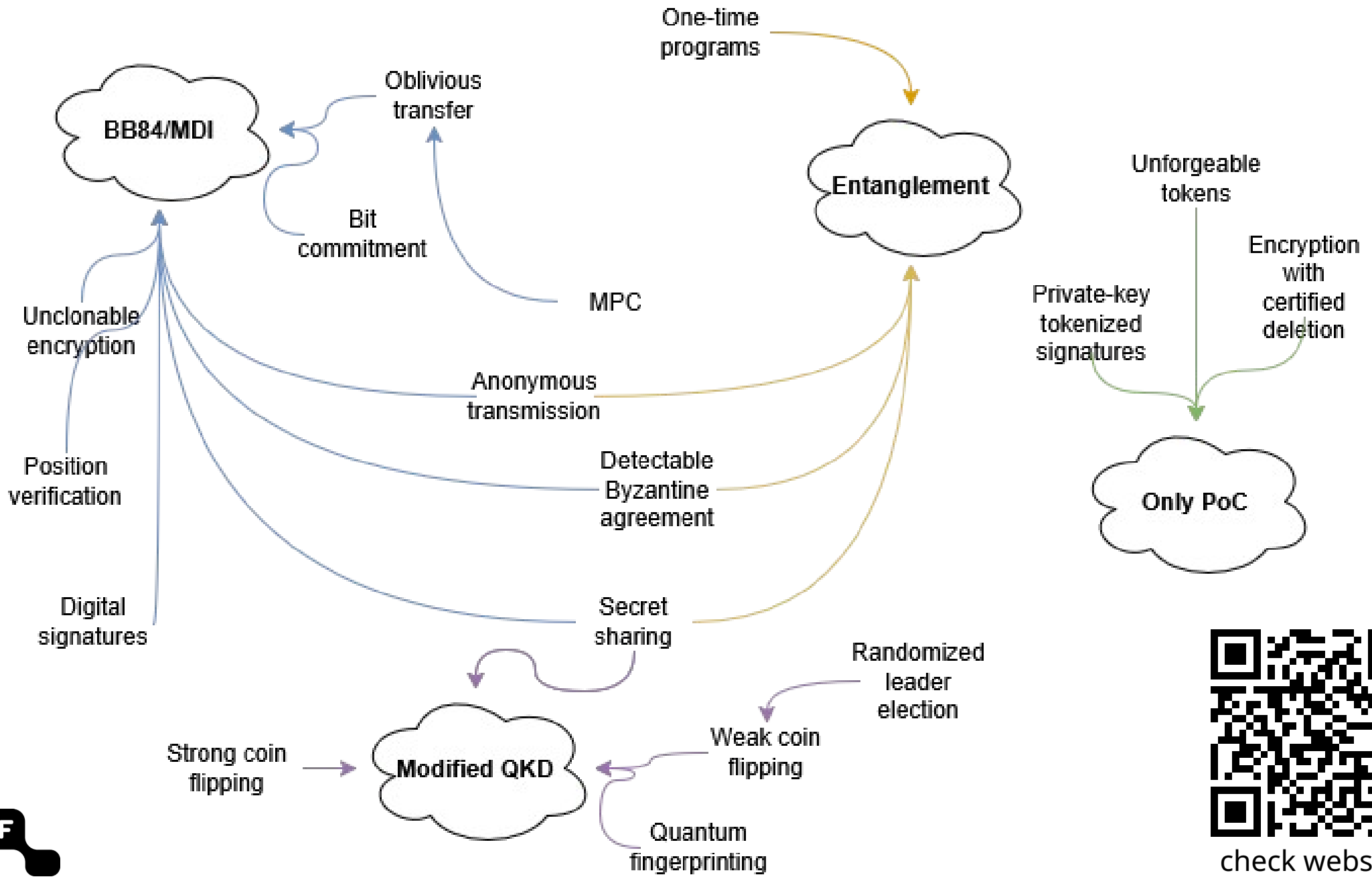
SURF

Near-term: what happens inside QKD boxes?



Classical post-processing:
share partial information about

What other applications are there by changing the classical post-processing?



check website

Quantum communication knowledge bank

SURF's Quantum Team | Home | Multi-Party Computing | Beyond QKD | Search | Previous | Next | Edit on GitLab

Beyond QKD

I. Introduction

II. Applications and primitives

III. Summary

IV. Diagram

V. Challenges

2.10 Multi-party computing

Distrusting parties can compute a function jointly on their private inputs, without having to reveal anything other than the outcome, that is, without having to share their data. In principle such protocol would be possible if we encrypted all our data in a way that we could compute homomorphically on it (the computations *commute* with the encryption), and in fact *Homomorphic Encryption* is a subset of Multi-Party Computing. However, the idea is that by relaxing the requirement of no communication between the parties we could obtain more efficient protocols. In practice, known quantum-enhanced constructions of MPC rely of quantum Oblivious Transfer, such that on a first stage oblivious keys are pre-processed using quantum communication, and can be later used when the function to compute is chosen, such that the second stage can consist only of classical communication.

Reference: The typical construction of MPC from OT consists of first obtaining 2-party computing as shown by https://dl.acm.org/doi/pdf/10.1145/62212.62215 (OT → 2PC) and https://mmp.cs.illinois.edu/pub/mpc-ot.pdf (2PC → MPC), these constructions where proven to be quantum-secure by Unruh https://arxiv.org/abs/0910.2912. If we instead assume the QROM, we can construct MPC from OT directly https://arxiv.org/abs/2304.10480.

Classical state of the art: Classically there are multiple constructions based on: secret sharing, FHE, OT... but they all rely on classical authenticated channels (thus trapdoor-OWF or public-key cryptography).

Quantum advantage: Since quantumly OT can be constructed just from extractable and equivocal commitments, quantum-enhanced MPC only requires the existence of OWF (as opposed to trapdoor-OWF classically). In practice, this means that it can be built from symmetric cryptography's tools, whose security hasn't been challenges by quantum computers.

Hardware requirements: The construction on top of OT is information-theoretically secure with an addition of constant rounds of classical communication, thus the same hardware requirements apply. That is, the ability to generate BB84 states suffices (although there are no complete security proofs for weak coherent pulses).

check website

SURF

Quantum communication knowledge bank

SURF's Quantum Team | Home | Multi-Party Computing | Beyond QKD | Search | Previous | Next | Edit on GitLab

Beyond QKD

I. Introduction

II. Applications and primitives

III. Summary

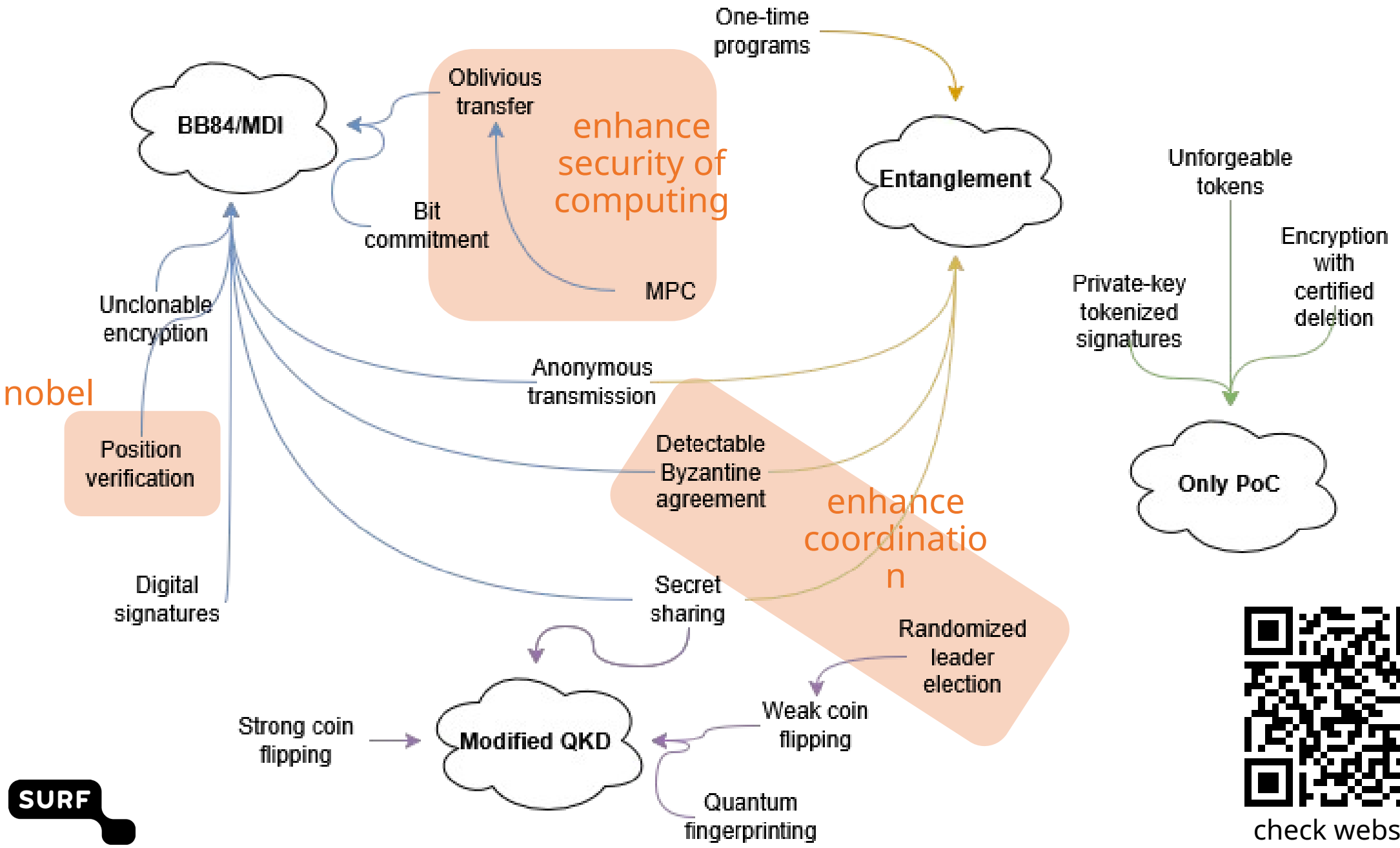
IV. Diagram

V. Challenges

10	Multi-Party Computing	Distrusting parties can compute a function jointly on their private inputs, without having to reveal anything other than the outcome.	There are multiple constructions based on: secret sharing, FHE, OT... but they all rely on classical authenticated channels (thus trapdoor-OWF).	Can be constructed from oblivious transfer, which in turn can be constructed from extractable and equivocal commitments, thus only require OWF (as opposed to trapdoor-OWF classically). In practice, this means that it can be built from symmetric cryptography's tools, whose security hasn't been challenges by quantum computers.	The construction on top of OT is ITS with an addition of constant rounds of classical communication, thus the same hardware requirements apply.
11	Strong coin flipping	Two remote parties agree on an unbiased uniformly random bitstring. Ideally should be: fair, secure and	Can be ITS with either (1) a trusted third party or (2) 1/2-sqrt(x/2) bias and x probability of abort. We can	ITS security achievable against unentangled adversaries, or better than classical bias.	Noise-robust protocol in the plain model using weak coherent modes present. Although such technology exists in QKD

check website

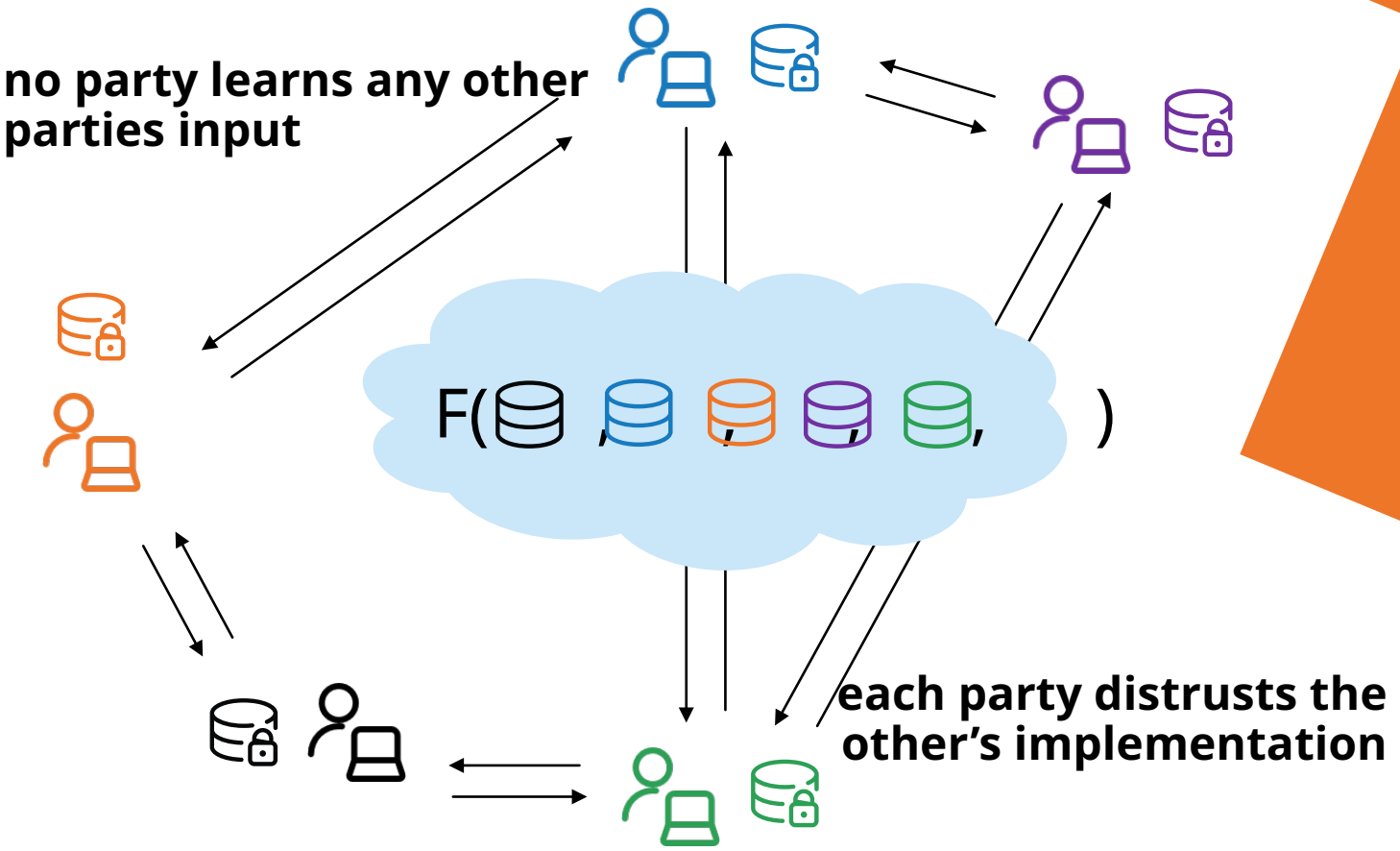
SURF



check website

Multi-Party Computing

Joint operations on datasets of mutually distrusting parties.

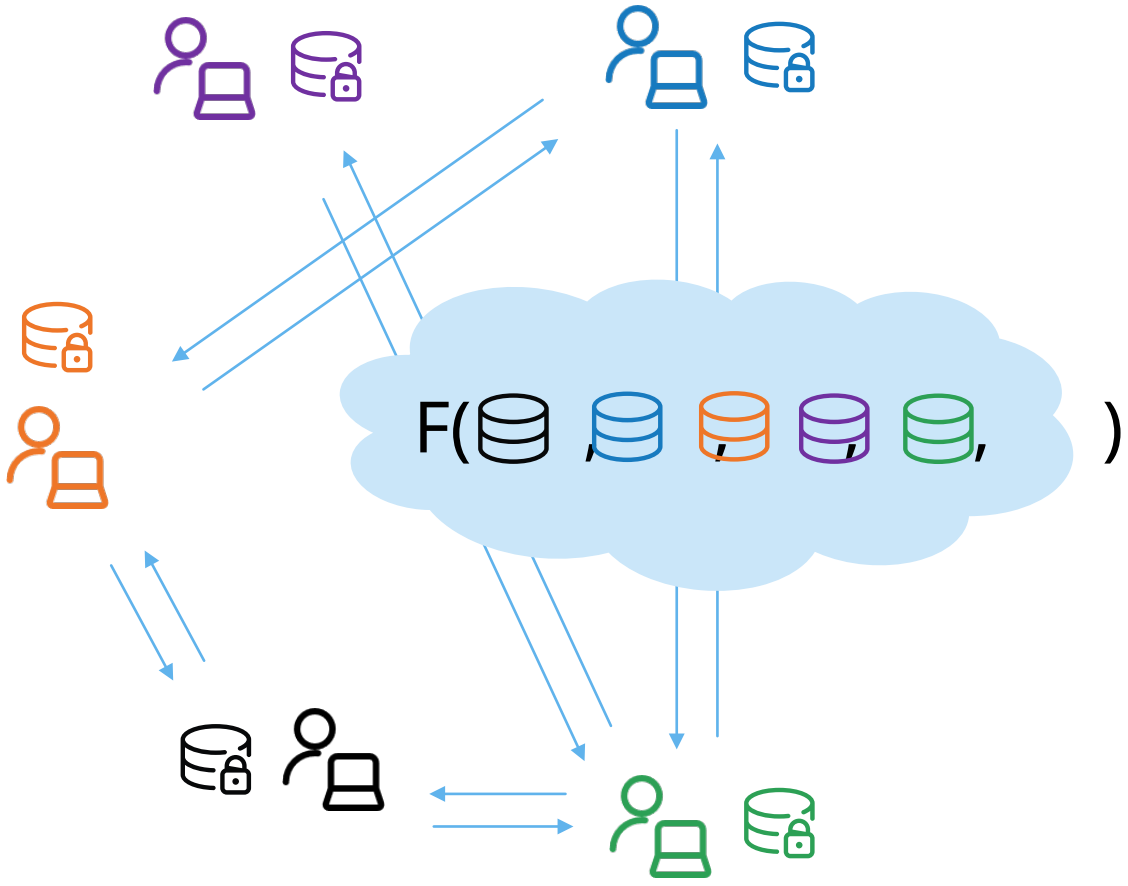


Classically:
~~PKI~~ → Oblivious Transfer (OT)→ MPC

can we replace PKI by quantum communication?

(similar constrains as QKD)

Quantum Multi-Party Computing



Assumptions: quantum links between every 2 parties

Steps:

1. quantum comm between every 2 parties

2. classical post-processing of OT keys:

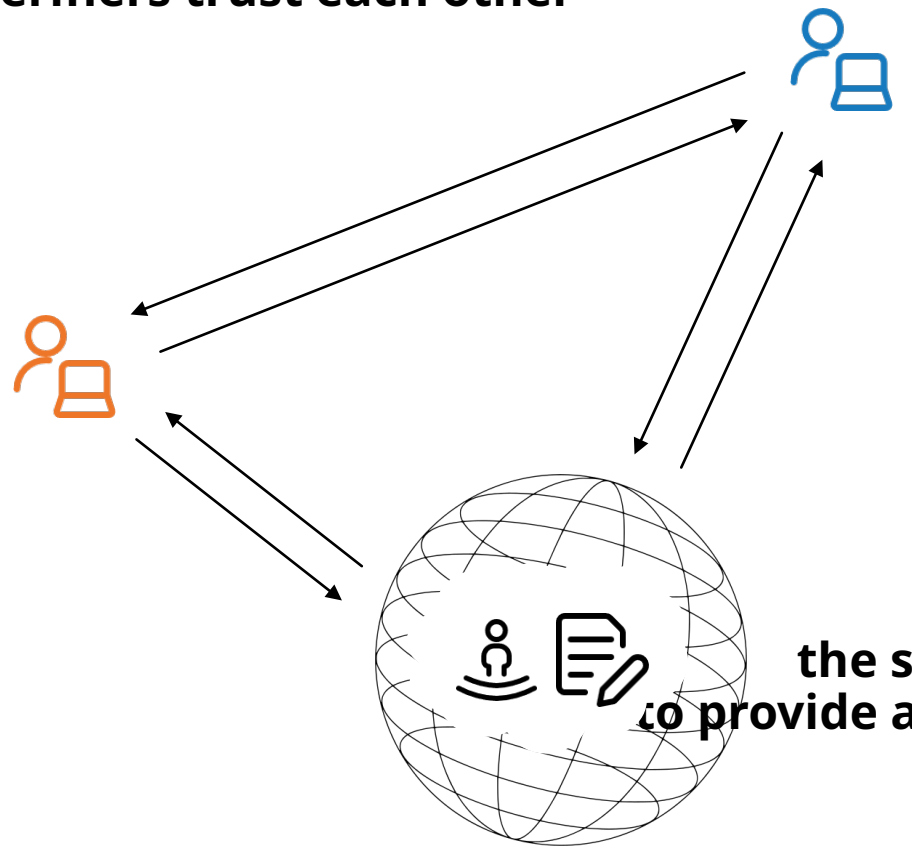
3. chose a function to jointly compute
4. classical post-processing of MPC

Bonus: if parties have access to **quantum computers** they can jointly compute **quantum operations**.

Position Verification

Verify that a message comes from a specific location.

verifiers trust each other



the sender needs to provide a proof

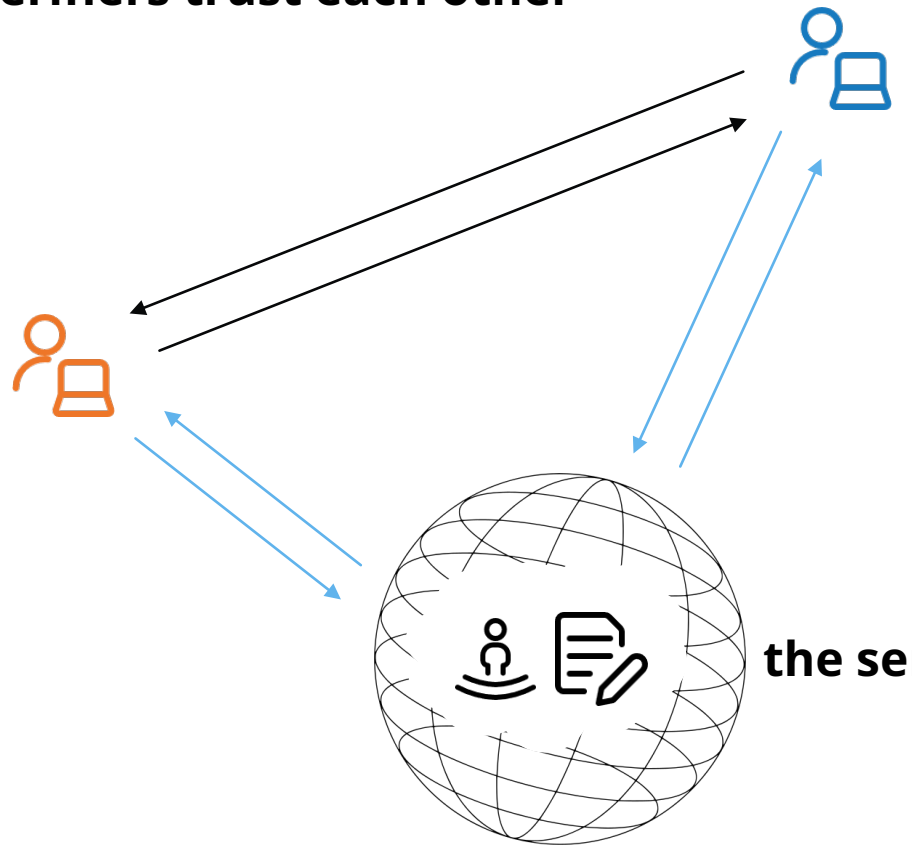
Classically:
GNSS positioning, radio-wave signals

Insecure against jamming, spoofing, collusions... (classical attacks)

Quantum Position Verification

Verify that a message comes from a specific location.

verifiers trust each other

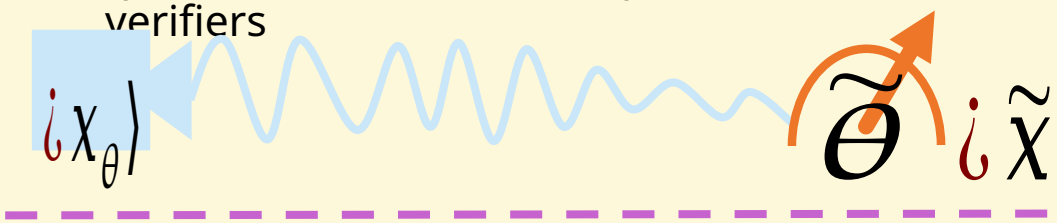


the sender cannot lie

Assumptions: quantum links to the prover

Steps:

1. quantum comm from the prover to the verifiers



2. classical post-processing

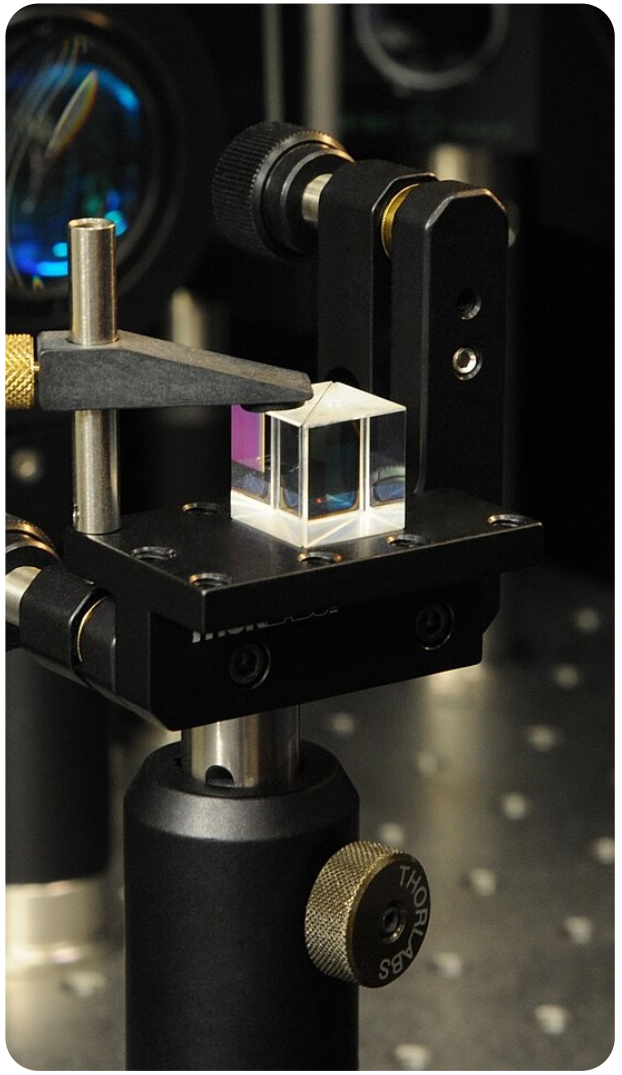
- Position-based authentication.
- Its security is much less understood than QKD.

Conclusions

- We need more access to the QKD devices.
- We need to understand what is the quantum advantage (if any) of the primitives.
- We need more noise and performance analysis of cryptographic primitives.
- We need to know which trade-offs between security and performance we deem acceptable.

does any of these applications ring a bell?

what network architectures would they need?



Thank you for your attention!

garazi.muguruzalasa@surf.nl

SURF