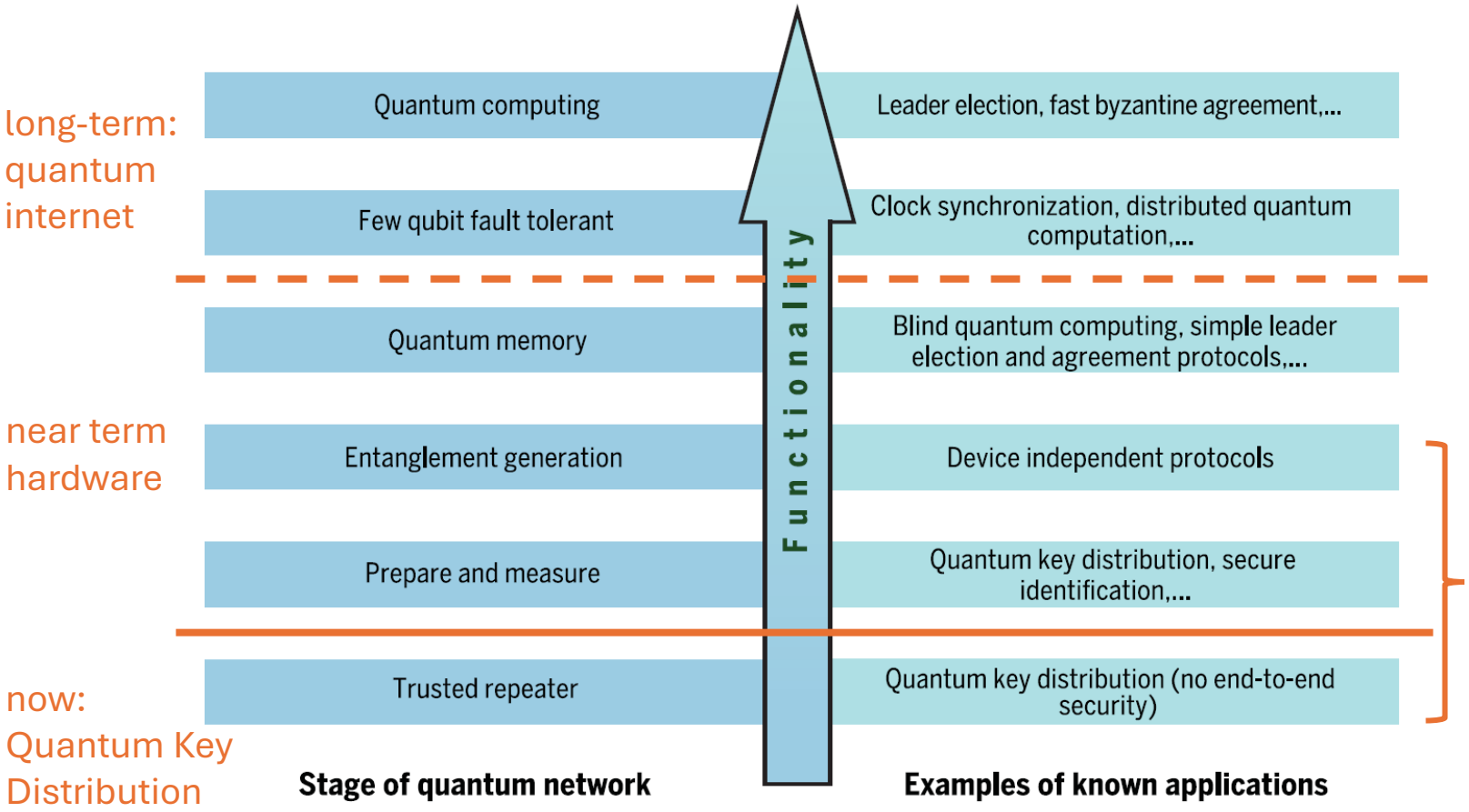
What can we do with near-term Quantum Networks?

Garazi Muguruza Lasa

21st July, 2026

SURF

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?

basis

input bit x

$|x_\theta\rangle$

$\tilde{\theta}$

$= \tilde{x}$

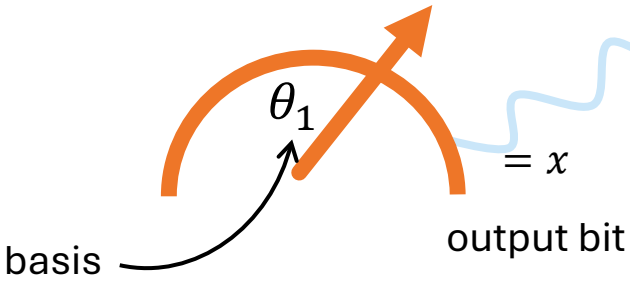
output bit

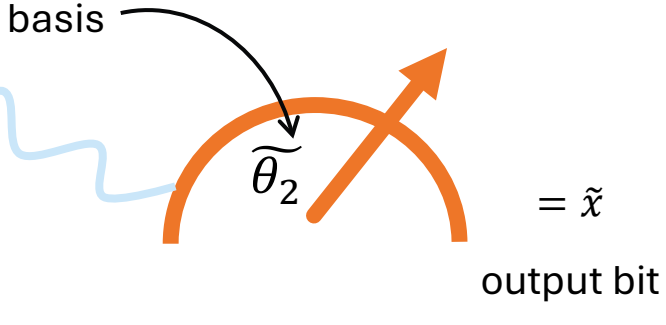
basis θ

Classical post-processing:
share partial information about
$x, \theta, \tilde{x}, \tilde{\theta}$

Near-term: what happens inside QKD boxes?

$|\phi\rangle_{12}$

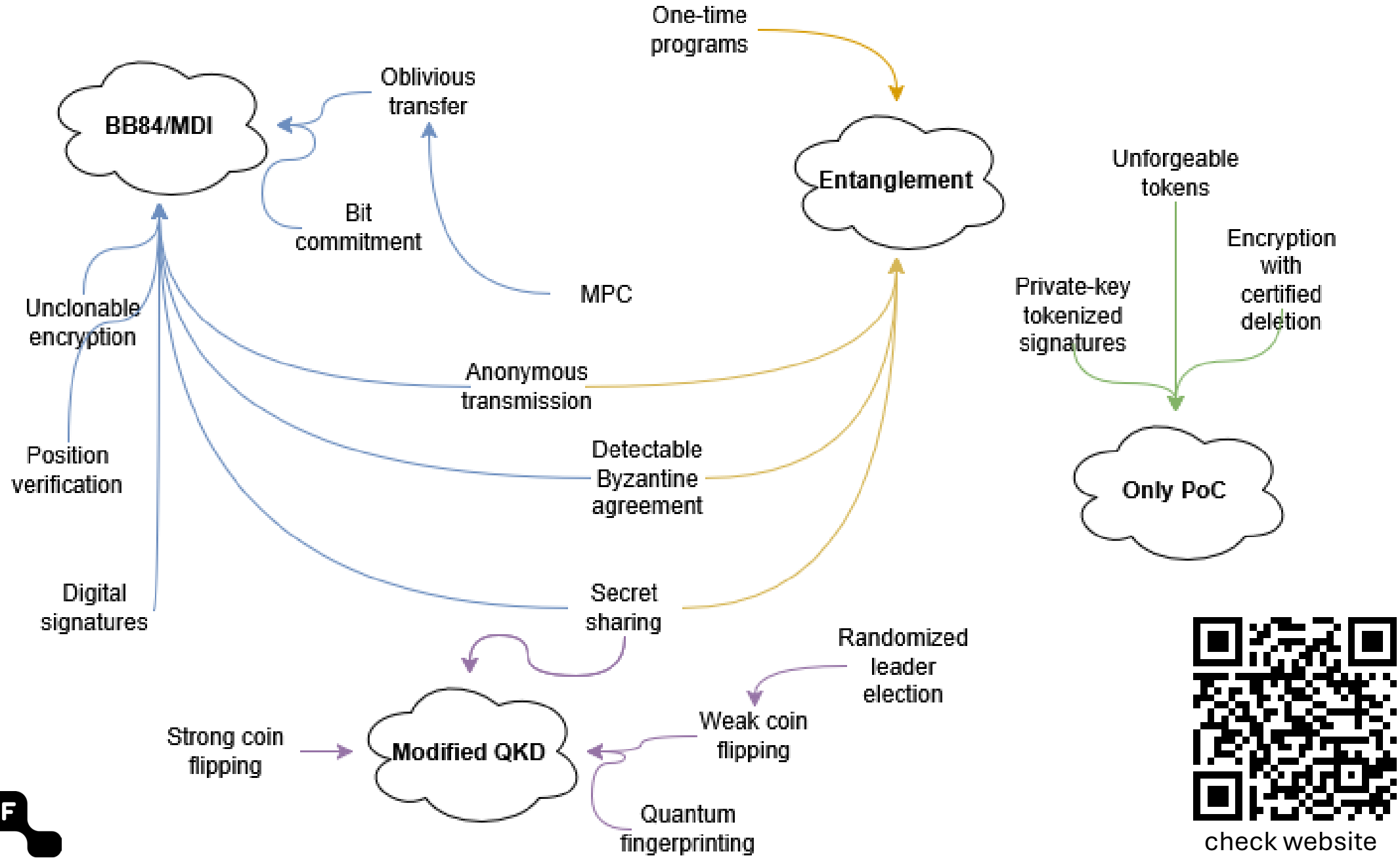




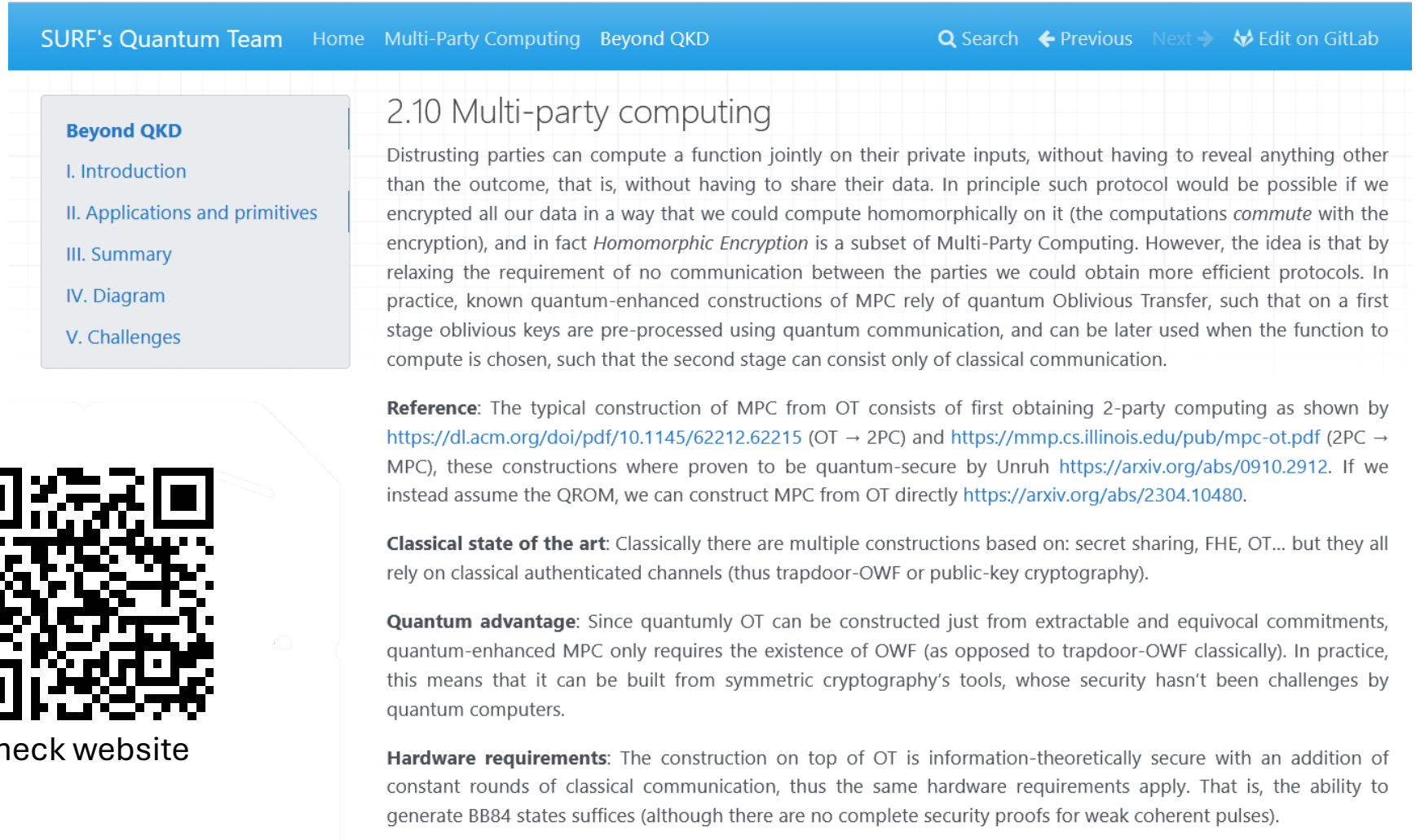
Classical post-processing:
share partial information about
$x, \theta, \tilde{x}, \tilde{\theta}$

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

SURF


One-time programs
BB84/MDI
Oblivious transfer
Entanglement
Unforgeable tokens
Bit commitment
Encryption with certified deletion
Private-key tokenized signatures
MPC
Unclonable encryption
Anonymous transmission
Only PoC
Position verification
Detectable Byzantine agreement
Digital signatures
Secret sharing
Randomized leader election
Strong coin flipping
Modified QKD
Weak coin flipping
Quantum fingerprinting
check website

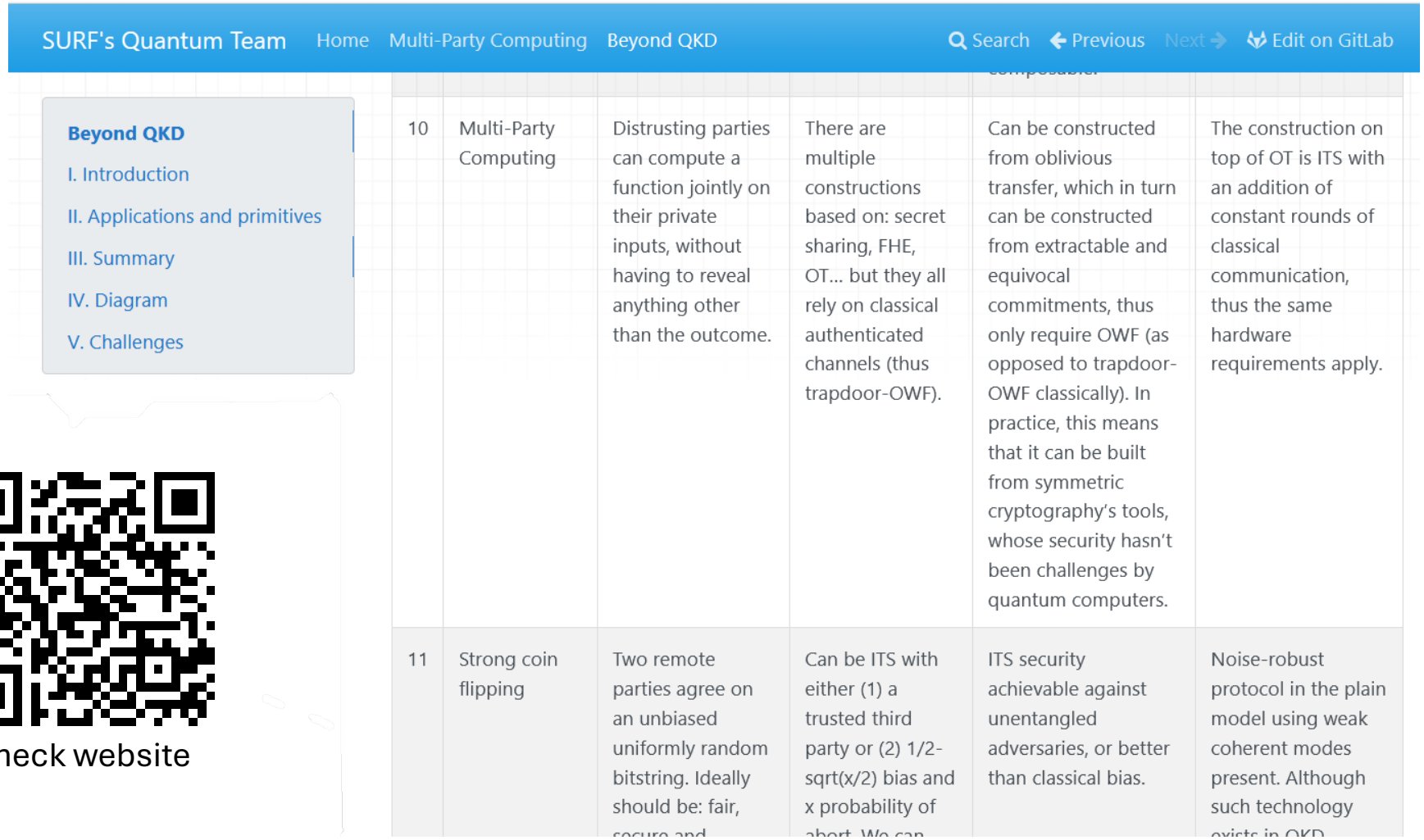
Quantum communication knowledge bank



check website

SURF

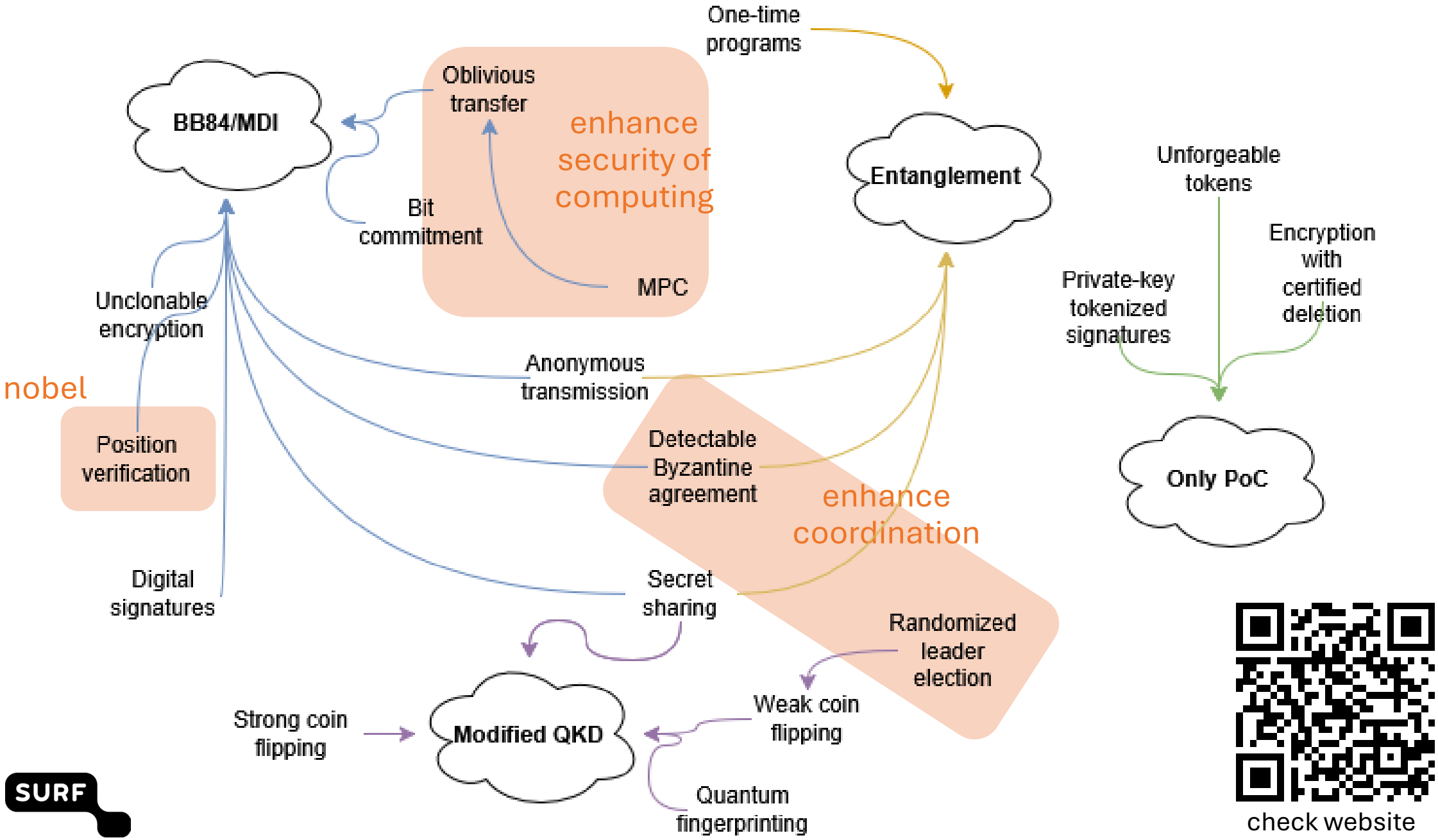
Quantum communication knowledge bank



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,	Can be ITS with either (1) a trusted third party or (2) 1/2-sqrt(x/2) bias and x probability of	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

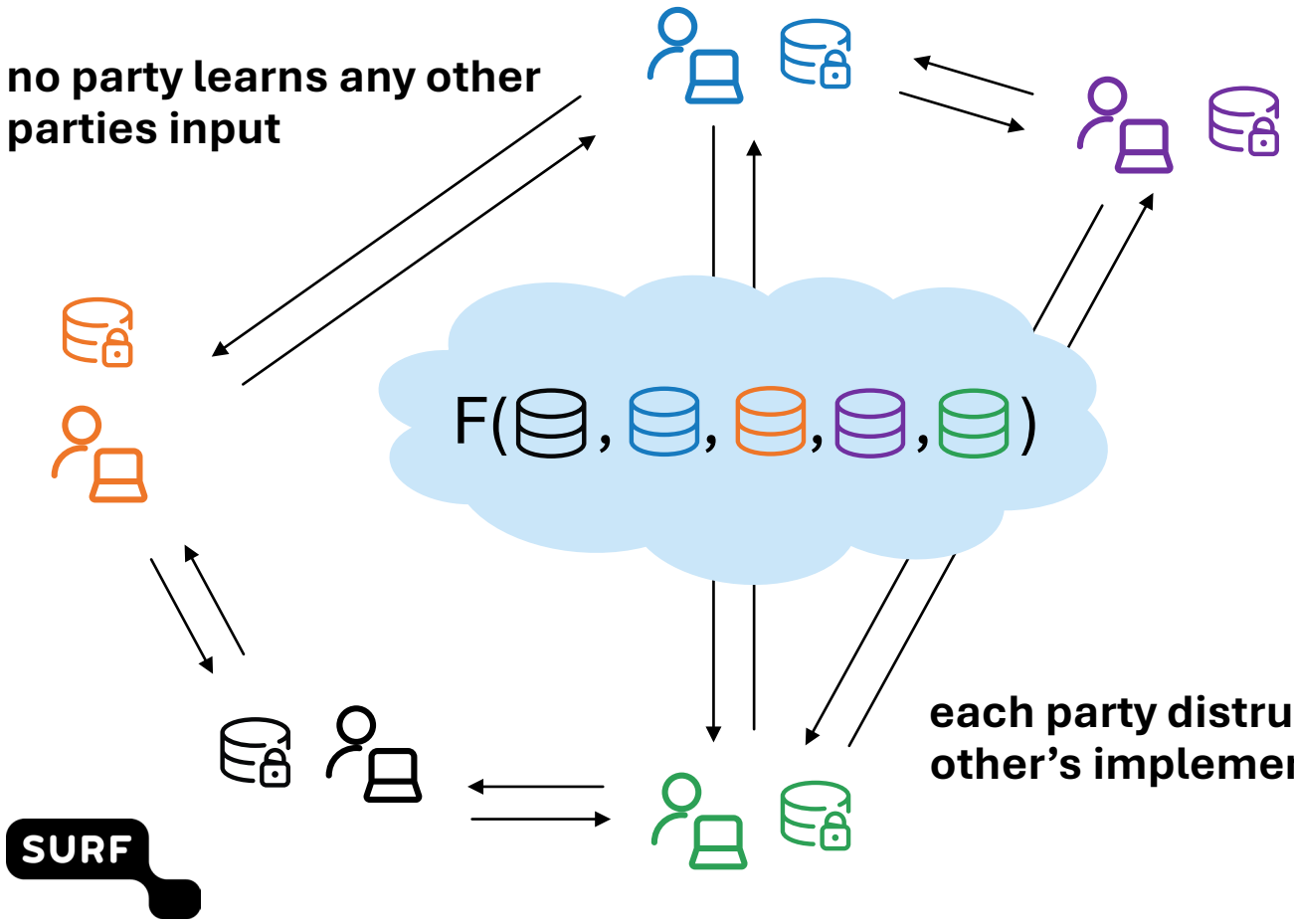
check website

SURF


One-time programs
BB84/MDI
Oblivious transfer
enhance security of computing
Bit commitment
MPC
Entanglement
Unforgeable tokens
Encryption with certified deletion
Private-key tokenized signatures
Only PoC
Unclonable encryption
nobel
Position verification
Anonymous transmission
Detectable Byzantine agreement
enhance coordination
Digital signatures
Secret sharing
Randomized leader election
Strong coin flipping
Modified QKD
Weak coin flipping
Quantum fingerprinting
SURF
check website

Multi-Party Computing

Joint operations on datasets of mutually distrusting parties.

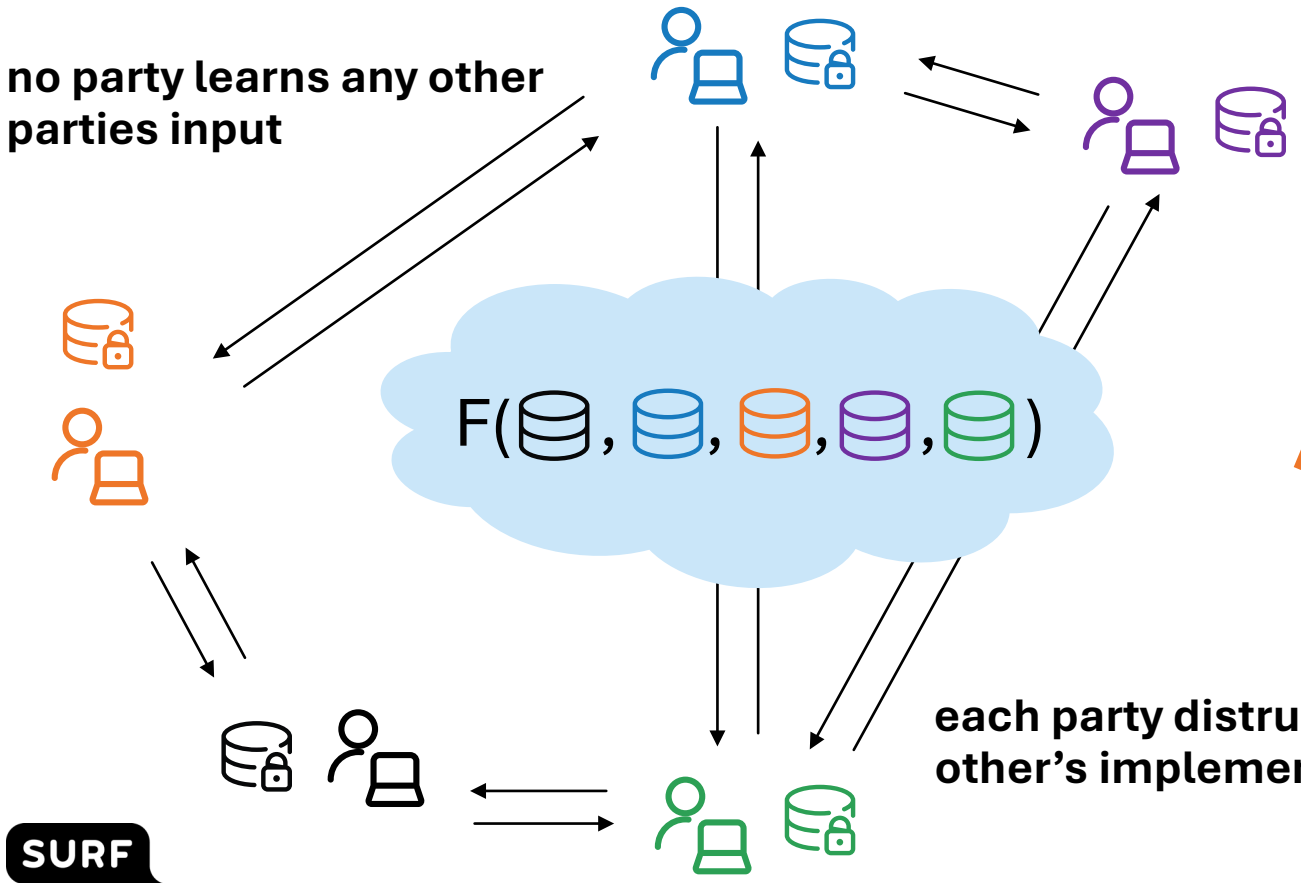


Classically:
PKI → Oblivious Transfer (OT)→ MPC

SURF

Multi-Party Computing

Joint operations on datasets of mutually distrusting parties.



Classically:

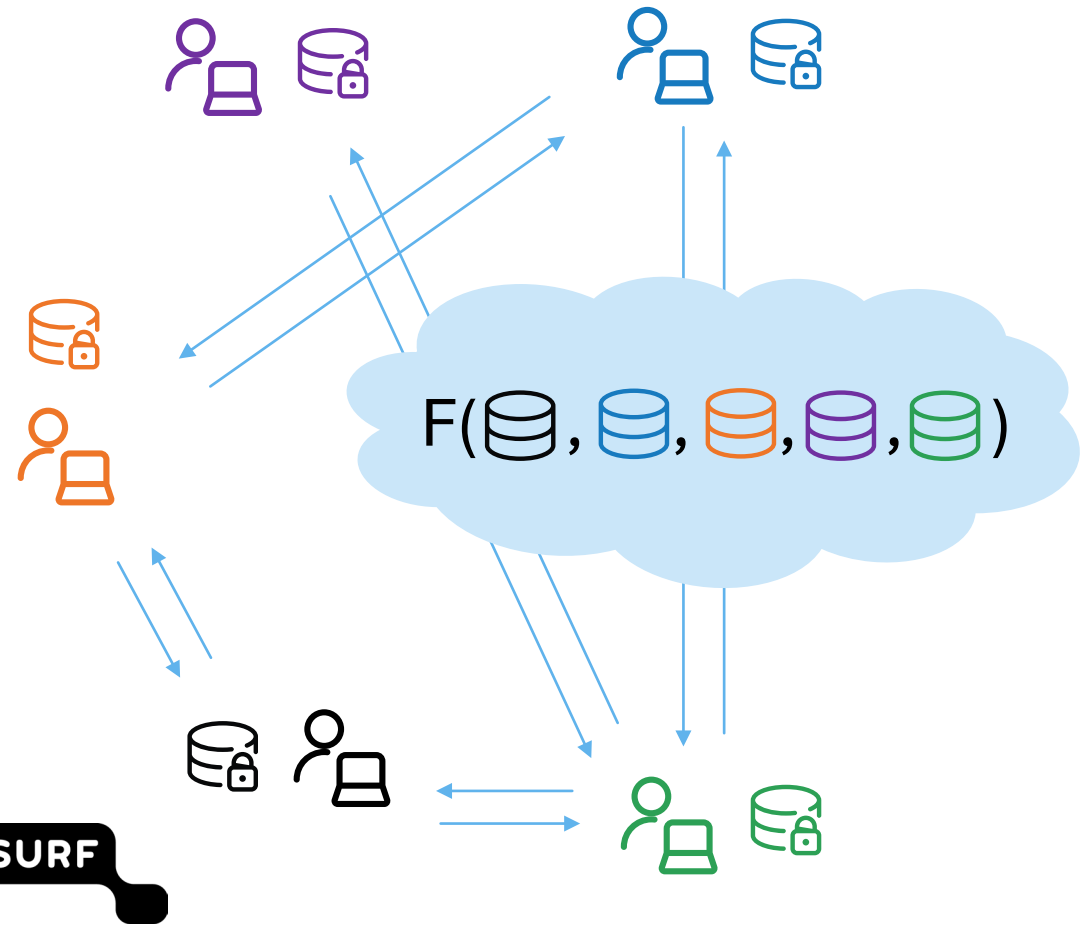
~~PKI~~ → Oblivious Transfer (OT)→ MPC

can we replace PKI by quantum communication?

(similar constrains as QKD)

SURF

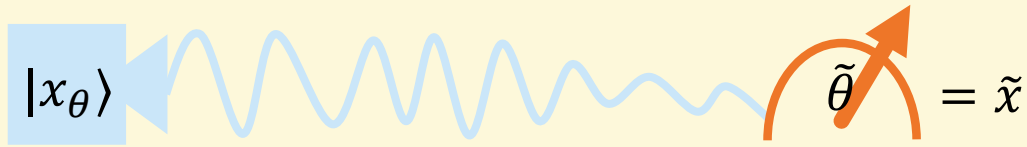
Quantum Multi-Party Computing



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

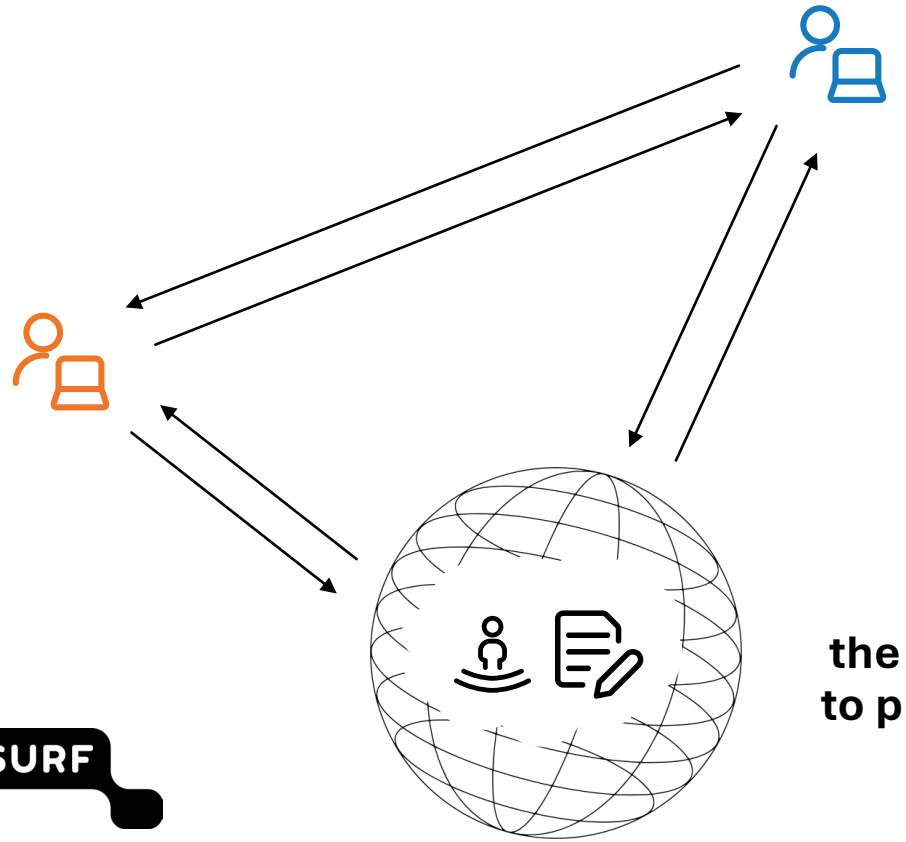
Bonus: if parties have access to **quantum computers** they can jointly compute **quantum operations**.

SURF

Position Verification

Verify that a message comes from a specific location.

verifiers trust each other



the sender needs to provide a proof

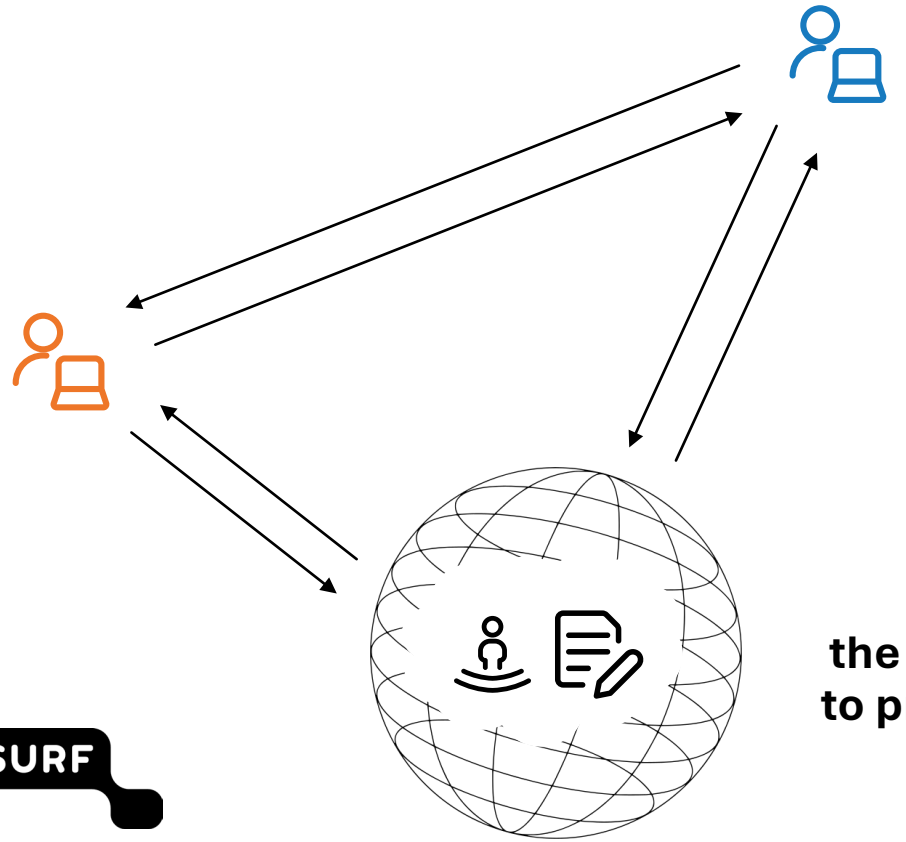
Classically:
GNSS positioning, radio-wave signals

SURF

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

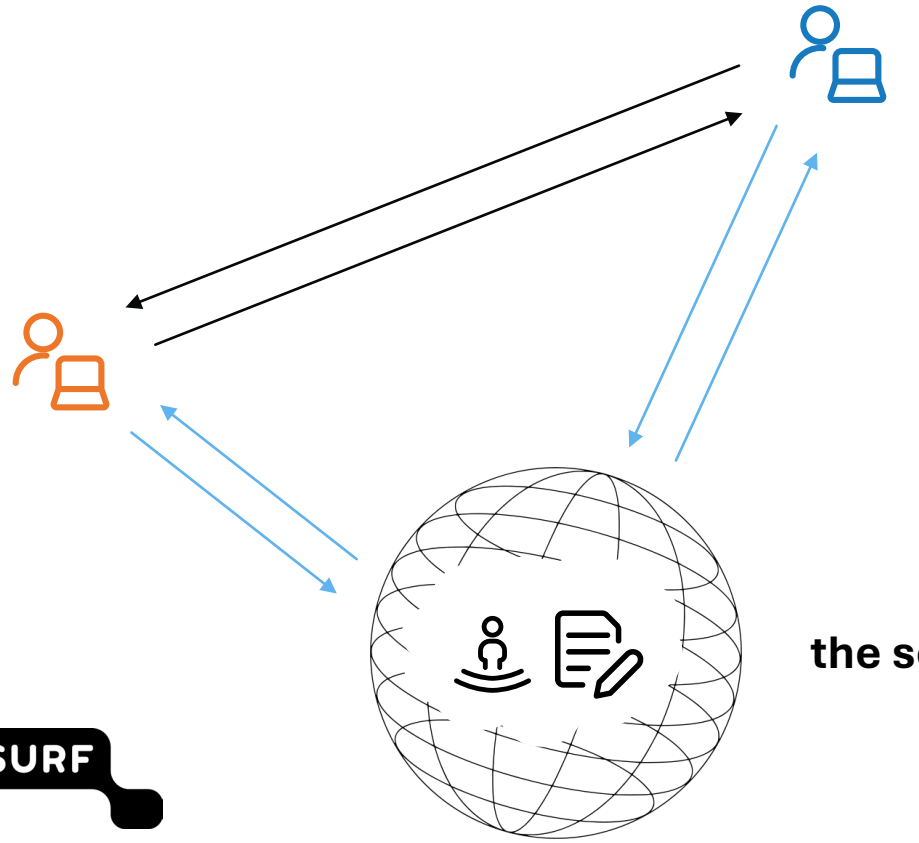
Insecure against jamming, spoofing, collusions… (classical attacks)

SURF

Quantum Position Verification

Verify that a message comes from a specific location.

verifiers trust each other

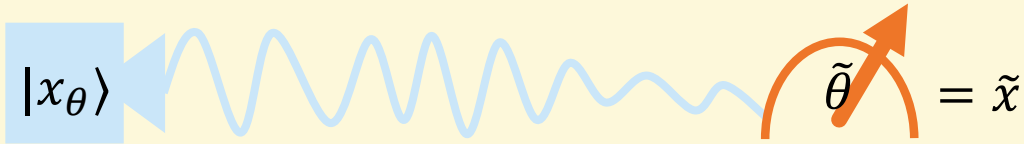


the sender cannot lie

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.

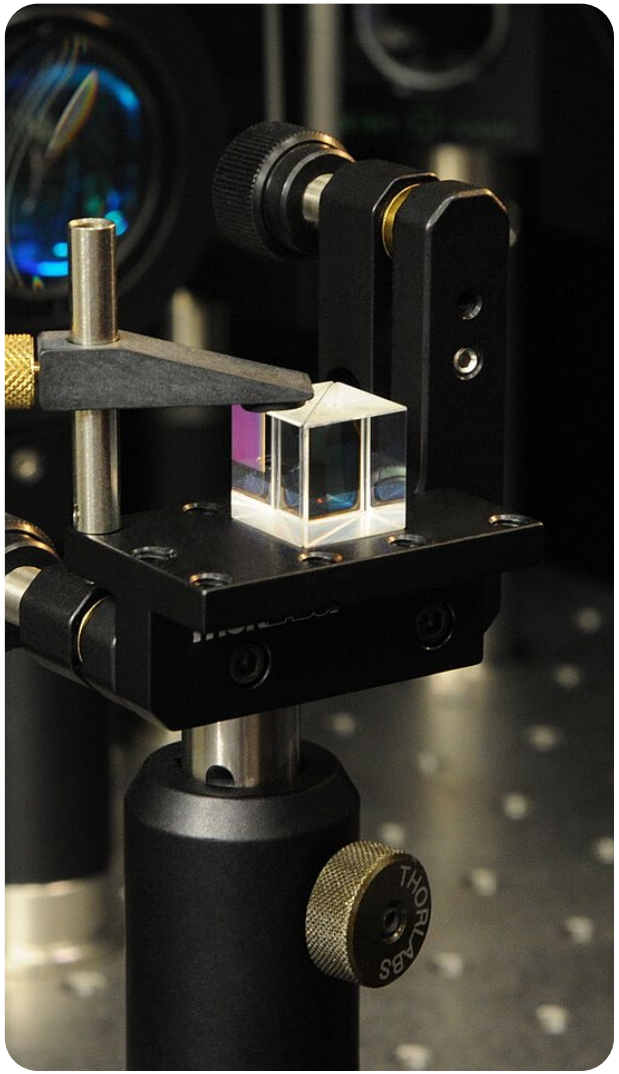
SURF

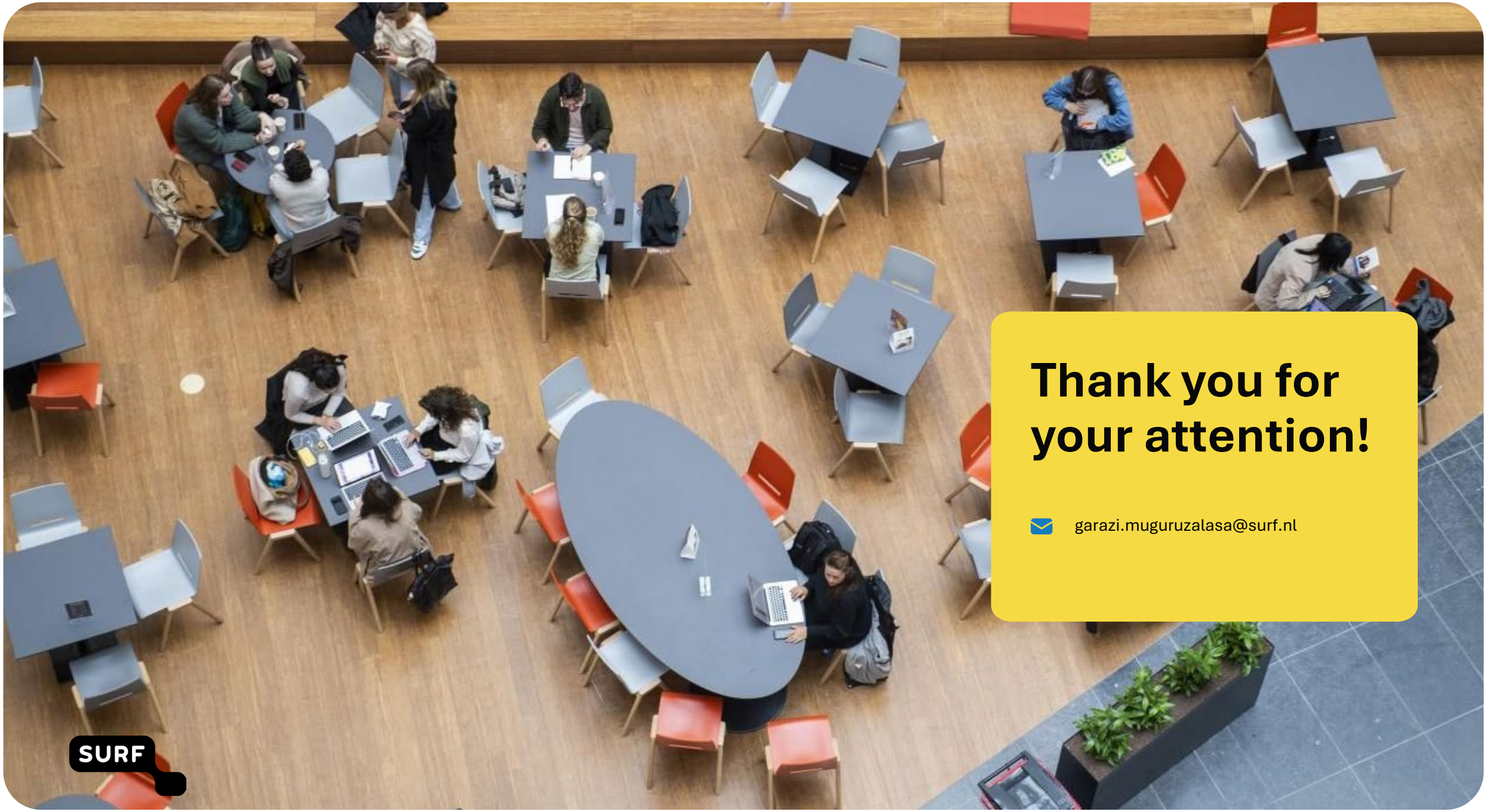
Conclusions

- 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