Loss-tolerance in quantum position verification

Andreas Bluhm
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG

July 14, 2026, Lorentz Center Leiden

Happy Bastille day!

Jean-Baptiste Lallemand, *Arrestation du gouverneur de la Bastille*, 1790

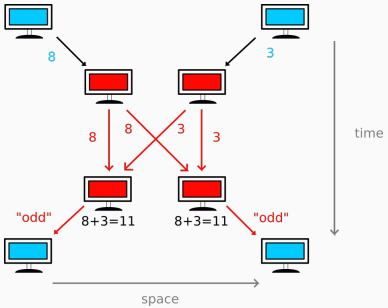
Talk outline

The f-measure protocol

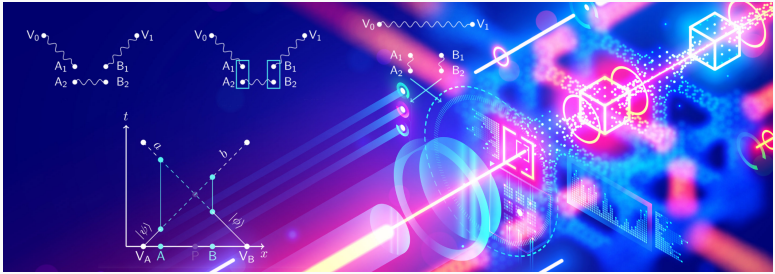
Towards loss-tolerant protocols

Partially loss-tolerant QPV protocols

Fully loss-tolerant QPV protocols



Introduction



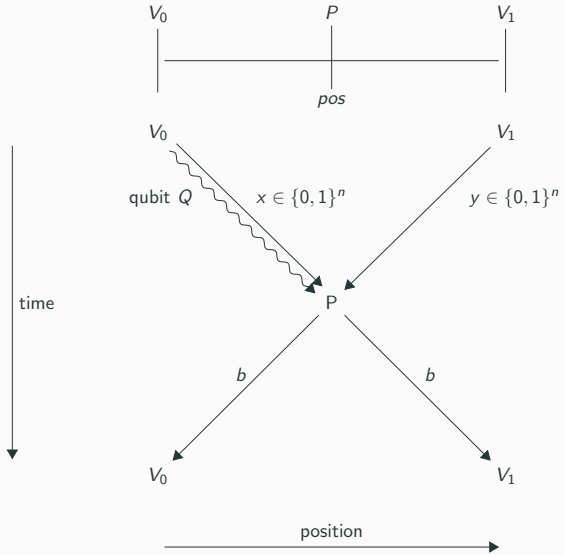
Which properties should a practically implementable QPV protocol have?

- Protocol should be as simple as possible for the honest parties
- Protocol should be as secure as possible against entangled attackers
- Protocol should not require quantum information to be sent at the speed of light
- Protocol should be tolerant against loss

Image taken from: events.perimeterinstitute.ca

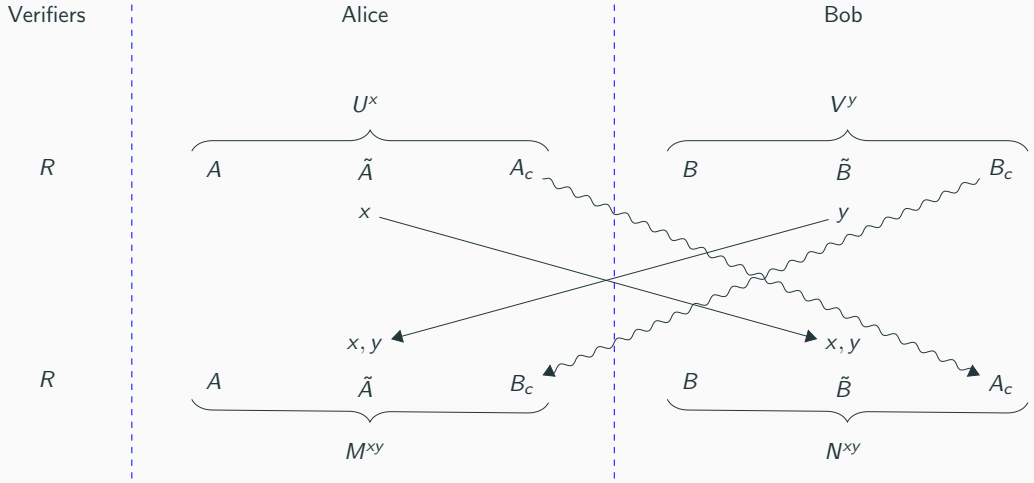
The f-measure protocol

The f-measure protocol



- Protocol goes back to *Unruh* [Unr14] (for f a hash function)
- Verifiers choose uniformly random bit b and prepare Q as $H^{f(x,y)}\,|b\rangle$
- Prover measures in basis specified by $f(x,y)$, sends back outcome b
- Verifiers check timing and consistency of b with the Q they sent

Quantum attacks



U^x, V^y are unitaries, M^{xy}, N^{xy} are POVMs

Main theorem

Theorem [BCS22]

Let $n \geq 10$. Let us assume that the verifiers choose the bit strings x, y of length n uniformly at random. Then there exists a function $f : \{0,1\}^{2n} \to \{0,1\}$ with the property that, if the number q of qubits each of the attackers controls satisfies

$$q \leq \frac{1}{2}n - 5,$$

the attackers are caught with probability at least $2 \cdot 10^{-2}$. Moreover, a uniformly random function f will have this property (except with exponentially small probability).

- Success probability of the attackers can be suppressed exponentially by sequential repetition

Concrete functions

Binary inner product function

$$IP(x, y) = \sum_{i=1}^{n} x_i y_i \pmod 2,$$

Theorem

Let $n \geq 10$. Let us assume that the verifiers choose the bit strings x, y of length n uniformly at random. If the number q of qubits each of the attackers controls satisfies

$$q \leq \frac{1}{2} \log n - 5,$$

the attackers are caught during the f-measure protocols with probability at least $2 \cdot 10^{-2}$, respectively.

- Proof based on communication complexity

How close is f-measure to a practically implementable protocol?

- Protocol only uses a single qubit, so it is as simple as possible
- It is secure against (possibly entangled) attackers with $\mathcal{O}(n)$ qubits. We have no idea whether this is optimal, but currently there is nothing better
- The protocol is still secure if Q does not travel at the speed of light

Is the protocol tolerant against loss?

Towards loss-tolerant protocols

Noise robust f-measure protocol (1/2)

- Hitherto, we assumed that the honest prover succeeds perfectly
- Now, we only assume that she succeeds with probability at least 0.99
- Repeat the protocol independently r-times and accept if the final measurement accepts more than $(1-\delta)r$ times, where δ is a small constant

Theorem

Let r, q, $n \in \mathbb{N}$, $n \geq 10$. Assume that a function $f : \{0,1\}^{2n} \to \{0,1\}$ is chosen uniformly at random. Then, an honest prover succeeds in a protocol with noise level at most 1% with probability at least $1 - c^r$. Attackers controlling at most $q \leq \frac{1}{2}n - 5$ qubits each round will succeed with probability at most c'^r, where $c, c' < 1$ are universal constants.

- Proof: Chernoff bound

Noise robust f-measure protocol (2/2)

Pros:

- The noise robustness of 1% holds against any form of noise
- Tweaking numbers, we can get about 6% noise robustness

Cons:

- 1% is not enough since if telecom wavelength (ca. $1550nm$) single-photon sources are used and the photons are sent through optical fibers, the loss is $0.15dB/km$. So 1% loss corresponds to a distance of only $300m$. After $100km$, only 3% will be left
- At 50% photon loss, the attackers can simply guess a basis and claim that they have lost the qubit if they guessed wrong. This breaks the protocol perfectly. Thus, distances of more than $20km$ are impossible

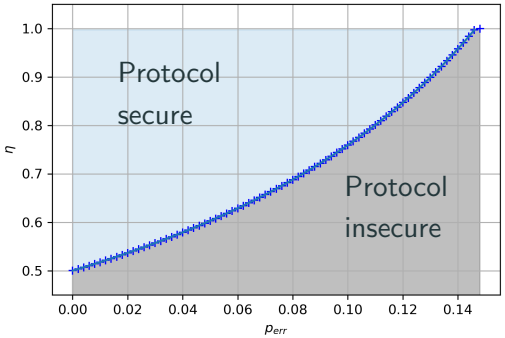
Partially and fully loss-tolerant protocols

- A protocol is partially loss tolerant if there exists an η_0 such that for any $\eta \geq \eta_0$, the protocol is secure. If the loss rate is significantly exceeded, the protocol needs to be aborted. Such protocols only work up to a specific distance
- A protocol is fully loss tolerant if it is secure for any η. In particular, the protocol stays secure if we condition on the rounds in which no loss was reported. Such protocols work over arbitrary distances

Partially loss-tolerant QPV protocols

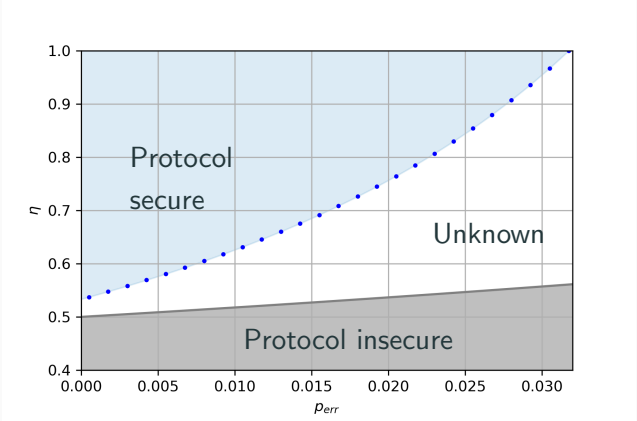
Partially loss-tolerant f-measure protocol (1/3)

- Paper [EFS22] analyzed the f-measure protocol under loss
- First result: Security region for protocol with $f(x, y) = y$, unentangled attackers
- Form of monogamy of entanglement game with loss
- NPA + combination of guessing attack and optimal attack (Breidbart measurement)



Partially loss-tolerant f-measure protocol (2/3)

- Previous protocol insecure if attackers share EPR pair
- Second result: Security region for arbitrary functions f, linear amount of entanglement
- Security proof very similar to f-measure protocol without loss



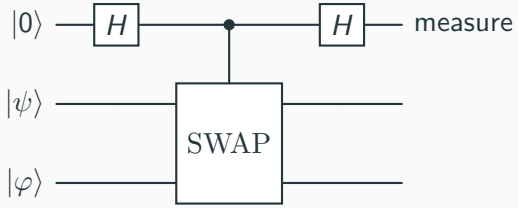
Partially loss-tolerant f-measure protocol (3/3)

- So far, we could not go further than $\eta_0 = 0.5$
- At that point, attackers can just guess the basis, thus a better analysis won't save us
- How to go beyond this threshold? $\implies$ Use more than m bases instead of 2. These protocols could be partially loss-tolerant up to $\eta_0 = \frac{1}{m}$
- This was already realized in [QS15] and [Spe16], but without full security analysis
- Third result: This allows us to go to lower η, for example to almost $\eta_0 = 0.3$ for $m = 5$ (ca. $35km$)
- Downside: becomes experimentally more challenging as well

Fully loss-tolerant QPV protocols

SWAP test protocol (1/2)

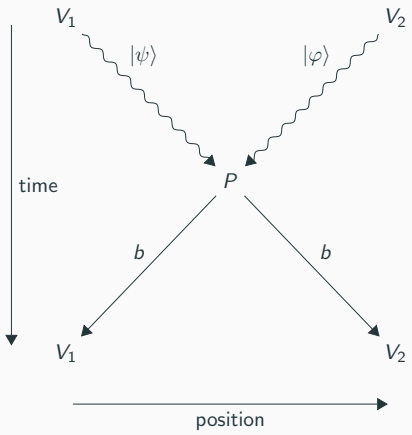
- First fully loss-tolerant protocol in [LXS+16]
- Slightly simpler protocol analyzed in [ABSVL21]
- Based on SWAP test:



Here, SWAP : $|i\rangle \otimes |j\rangle \mapsto |j\rangle \otimes |i\rangle$. Output statistics of the measurement:

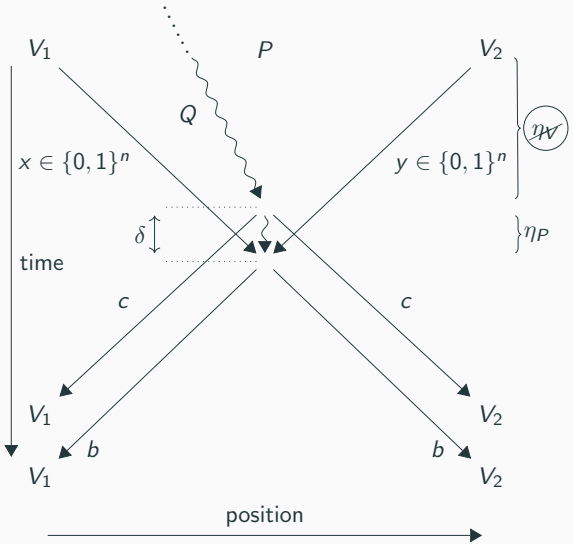
$$\mathbb{P}(0) = \frac{1 + |\langle\psi|\varphi\rangle|^2}{2}, \qquad \mathbb{P}(1) = \frac{1 - |\langle\psi|\varphi\rangle|^2}{2}.$$

SWAP test protocol (2/2)



- Verifiers send states $|\psi\rangle$, $|\varphi\rangle$ with known overlap β, prover performs SWAP test. Verifiers compare statistics of the replies given by the prover with what they expect
- Fully loss-tolerant protocol secure against unentangled attackers with quantum communication
- Secure under parallel repetition (not known for [LXS+16])
- Can be broken with a single EPR pair per round
- First experimental results [KPB+25]

Protocol with commitment



- [ABB+25] added a commitment step
- If qubit received prover sends $c = 1$; otherwise $c = 0$
- Strings x, y arrive slightly later than Q (delay δ)
- Eliminates transmission loss η_V
- Only loss at prover η_P remains
- Challenge: Commitment allows attackers to start with $\rho^{x,y}$

Taming quantum instruments

- For their commitment, the attackers can use quantum instruments $\mathcal{I}^{A/B} = \{\mathcal{I}_c^{A/B}\}_{c\in\{0,1\}}$, i.e., collections of CP maps summing to a quantum channel
- Instruments model a measurement with post-measurement state

Lemma (see, e.g., M. Hayashi's book)

Let $\mathcal{I} = \{\mathcal{I}_i\}_{i\in\Omega}$ be an instrument, and $\{M_i\}_i$ its corresponding POVM, i.e. $\mathcal{I}_i^*(\mathbb{1}) = M_i$. Then, for every $i \in \Omega$, there exists a quantum channel $\mathcal{E}_i$ such that

$$\mathcal{I}_i(\rho) = \mathcal{E}_i\left(\sqrt{M_i}\rho\sqrt{M_i}\right)$$

Upon committing, we can absorb the quantum channel into the protocol, need only deal with the measurement.

Gentle measurement helps

- Alice and Bob can perform POVMs $\{M_A^x, \mathbb{1} - M_A^x\}$ and $\{M_B^y, \mathbb{1} - M_B^y\}$ to decide their commitment
- Intuition: Even noise can ever produce different commitments at V_0, V_1. Since Alice and Bob may not commit differently, they cannot use their knowledge of x, y

Lemma (Gentle Measurement Lemma)

Let ρ be a quantum state and $\{M, \mathbb{1} - M\}$ be a two-outcome measurement. If $\mathrm{tr}[M\rho] \geq 1 - \varepsilon$, then the post-measurement state

$$\rho' = \frac{\sqrt{M}\rho\sqrt{M}}{\mathrm{tr}[M\rho]}$$

of measuring M fulfills

$$||\rho - \rho'||_1 \leq 2\sqrt{\varepsilon}.$$

Gentle measurement helps, continued

Post-measurement state after Lüders instrument:

$$\rho^{xy} := \frac{\left(\sqrt{M_A^x} \otimes \sqrt{M_B^y}\right) \rho \left(\sqrt{M_A^x} \otimes \sqrt{M_B^y}\right)}{\mathrm{tr}\left[\left(M_A^x \otimes M_B^y\right) \rho\right]}.$$

Using the gentle measurement lemma, we can prove:

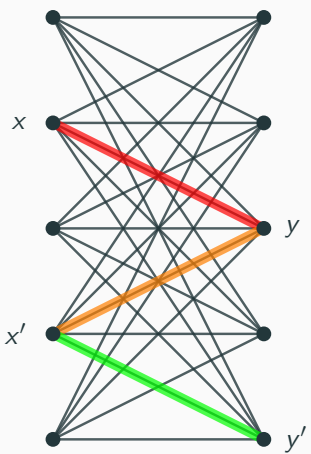
Lemma

Assume that for inputs (x, y), (x', y) and (x', y') in $\{0,1\}^{2n}$ the probability of answering different commitments is upper bounded by some $\varepsilon > 0$. Then,

$$\|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}.$$

If no error was permitted, we could just replace all ρ^{xy} by ρ^{00}, say.

Erasing edges from graphs



- What happens if the attackers make different commitments only on some pairs (x, y)?
- Corresponds to erasing edges from the fully connected bipartite graph
- If we erase a fraction $\tilde{c}$, how many vertices can we still reach in 2 steps?
- There is one x' with at least $(1 - \tilde{c})2^n$ edges
- Each of the vertices reached used to have 2^n edges attached, but we removed $\tilde{c}2^{2n}$
- $(1 - 2\tilde{c})2^{2n}$ can still be reached within 2 steps from x'

Replacing by a fixed state

Set of (x, y) where commitment errors are low:

$$\Sigma_\varepsilon = \{(x, y) \mid \mathbb{P}[c_B = 0 \mid c_A = 1, x, y] \leq \varepsilon \wedge \mathbb{P}[c_A = 0 \mid c_B = 1, x, y] \leq \varepsilon\},$$

On these pairs we can replace by a fixed state:

Lemma

If $|\Sigma_\varepsilon^c| \leq \tilde{c} 2^{2n}$, *then there is a pair* (x^*, y^*) *such that there exist at least* $(1 - 2\tilde{c})2^{2n}$ *pairs* $(x', y') \in \Sigma_\varepsilon$ *fulfilling*

$$\|\rho^{x^* y^*} - \rho^{x' y'}\|_1 \leq 8\sqrt{\varepsilon}.$$

Main result

Combining the previous ideas, we can prove:

Theorem

Let ε and $\tilde{c}$ be as described above and sufficiently small. On the rounds the attackers commit to play, the following bound on the probability of attacking c-$\mathrm{QPV}^{f}_{\mathrm{BB84}}$ holds:

$$\mathbb{P}[\text{attack c} - \mathrm{QPV}^{f,\eta_P,\eta_V}_{\mathrm{meas}}] \leq \mathbb{P}[\text{attack } \mathrm{QPV}^{f,\eta_P}_{\mathrm{meas}}] + \Delta(\varepsilon, \tilde{c}, \eta_P).$$

How do we get $\tilde{c}$ and ε such that $\Delta(\varepsilon, \tilde{c}, \eta_P)$ can be made small?

Parameter estimation

Idea: If we run the protocol a couple of times, the attackers will only escape detection if their commitment error is low on most pairs.

Theorem

Let $k \geq 2$ be a security parameter and suppose $\mathrm{c}-\mathrm{QPV}_{\mathrm{meas}}^{f,\eta_P;\eta_V}$ is executed sequentially until we have $640k/\tilde{c}^3 = O(k^7)$ rounds in which both attackers commit, where $\tilde{c} = C(\eta_P)k^{-2}$. Then, either the attackers are detected with probability bigger than $1 - 3 \cdot 10^{-9}$ via an inconsistent commitment, or there is a set $\mathcal{R}$ of size $1 - 1/k$ times the number of rounds such that, for all rounds in $\mathcal{R}$,

$$\mathbb{P}(\text{attack } c\text{-}\mathrm{QPV}_{\mathrm{meas}}^{f,\eta_V,\eta_P}) \leq \mathbb{P}(\text{attack } \mathrm{QPV}_{\mathrm{meas}}^{f,\eta_P}) + \frac{1}{k}.$$

The commitment step has made f-measure fully loss-tolerant while keeping all other desirable properties. Security under parallel repetition: [EFS+26].

Experimental photon-presence detection

How does the honest prover know whether she has received the qubit from the verifiers?

- Recent demonstration of true non-destructive photon presence detection [NFLR21]
- At the moment high dark count rate and experimentally very challenging, will hopefully improve in the future
- Poor-person's photon presence detection: Prover teleports photon to herself
- Can in principle be realized with linear optics, has been demonstrated in [MMWZ96]
- Experimentally more within reach, small success probability enough
- Requirements: EPR pair on demand, partial Bell state measurement, short-time quantum memory, measurements depending on (x, y)

Which protocols can we make loss-tolerant?

- We have implicitly assumed that the underlying protocol to be made loss-tolerant was f-measure
- However, we only used few properties of it in the proof
- In principle, the commitment works for all protocols that can deal with slow quantum information and where the prover returns classical bits
- We have found a general method to make such protocols fully tolerant against loss

Open questions

- Bring down the number of rounds required for making f-measure with commitment secure
- Do similar ideas work to make continuous-variable protocols fully loss-tolerant?
- Better lower bounds for concrete functions (since random functions are not efficient to evaluate)
- Replace qubit count in the security statement for f-measure by entanglement measure
- Superpolynomial lower bounds on the entanglement cost of f-measure

Conclusion

- f-measure is a very simple protocol (1 qubit only)
- Secure against amount of entanglement that scales linearly with the classical bits sent by the honest parties
- The honest parties, however, do not need more quantum resources
- Can be made partially loss-tolerant using more bases
- Can be made fully loss-tolerant by adding commitment
- Seems experimentally feasible in principle

We can make many QPV protocols fully loss-tolerant by adding a commitment step

References

[ABB+25] R. Allerstorfer, AB, H. Buhrman, M. Christandl, L. Escolà-Farràs, F. Speelman, and P. Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss. *Physical Review Letters*, 135(26):260801, 2025.

[ABSVL21]: R. Allerstorfer, H. Buhrman, F. Speelman, and P. Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint* arXiv:2106.12911, 2021.

[BCS22]: AB, M. Christandl, and F. Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 18(6):623–626, 2022.

[EFS+26] L. Escolà-Farràs, B. Škorić, and F. Speelman. Arbitrarily Loss-Tolerant Quantum Position Verification in a Single Execution. *arXiv preprint* arXiv:2606.25037, 2026.

More references

[EFS22] L. Escolà-Farràs and F. Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *Physical Review Letters*, 131(14):140802, 2023.

[KPB+25] K. Kanneworff, M. Poortvliet, D. Bouwmeester, R. Allerstorfer, P. Verduyn Lunel, F. Speelman, H. Buhrman, P. Steindl, and W. Löffler. Towards experimental demonstra- tion of quantum position verification using true single photons. *Quantum Science and Technology*, 10(4):045004, 2025.

[LXS+16] C. C. W. Lim, F. Xu, G. Siopsis, E. Chitambar, P. G. Evans, and B. Qi. Loss-tolerant quantum secure positioning with weak laser sources. *Physical Review A*, 94(3):032315, 2016.

[MMWZ96] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger. Interferometric Bell-state analysis. *Physical Review A*, 53(3):R1209, 1996.

Even more references

[NFML21] D. Niemietz, P. Farrera, S. Langenfeld, and G. Rempe. Nondestructive detection of photonic qubits. *Nature*, 591(7851):570–574, 2021.

[QS15] B. Qi and G. Siopsis. Loss-tolerant position- based quantum cryptography. *Physical Review A*, 91(4):042337, 2015.

[Spe16] F. Speelman. Position-based quantum cryptography and catalytic computation. *PhD thesis*, University of Amsterdam, 2016.

[Unr14] D. Unruh. Quantum position verification in the random oracle model. *Advances in Cryptology–CRYPTO 2014*, 1—18, 2014.