Making existing quantum position-verification protocols secure against arbitrary transmission loss

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

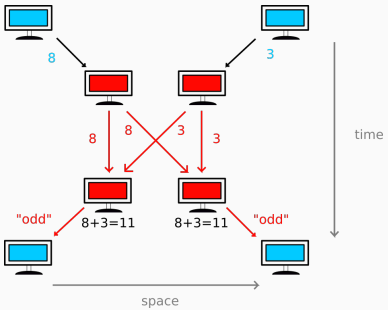
September 21, 2023, Perimeter Institute

Talk outline

Simple QPV protocols

Towards photon loss-tolerant protocols

Making QPV protocols fully loss-tolerant



Ongoing joint work with R. Allerstorfer, H. Buhrman, M. Christandl, L. Escolà-Farràs, F. Speelman, P. Verduyn Lunel

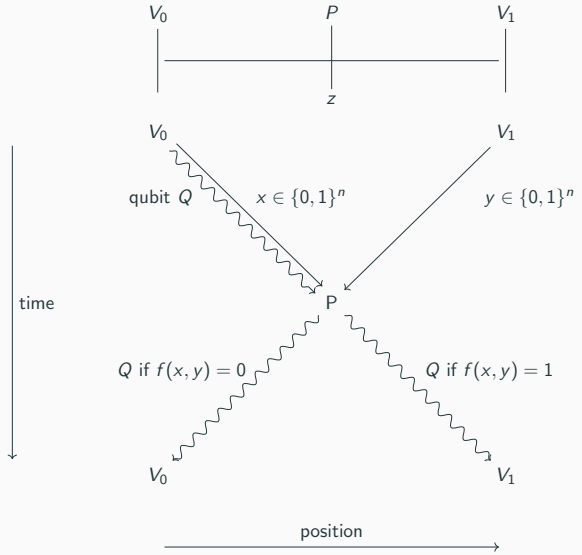
Introduction

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 be tolerant against photon loss

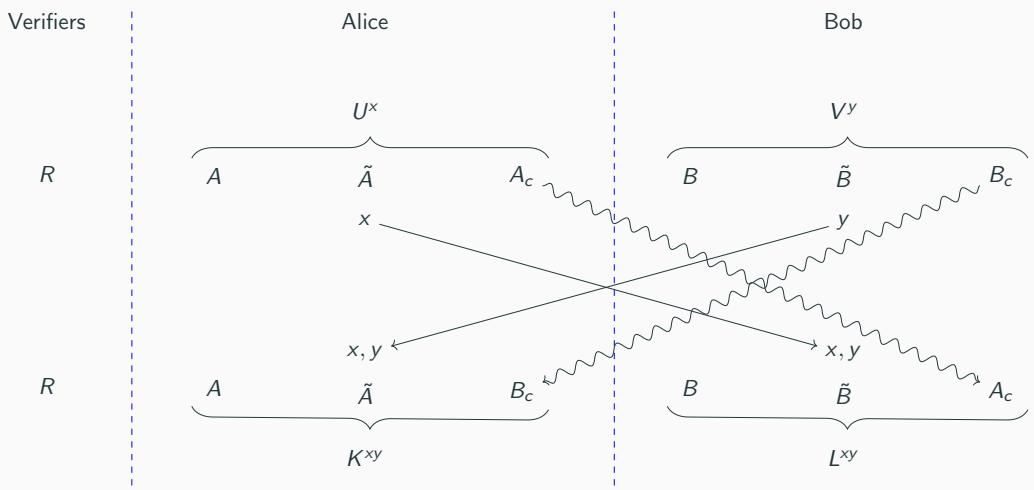
Simple QPV protocols

Qubit routing protocol



- Protocol goes back to *Kent et al.* [KMS11]
- Verifiers prepare entangled pair $|\Omega\rangle$
- Send one qubit Q of it and keep the other
- At the end of the protocol: Bell measurement

Quantum attacks



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

Proof idea (1/3)

- Qubit routing already considered in [BFSS13], but only for perfect attacks
- Our paper makes the proof strategy robust
- First observation (already present in [BFSS13]): Let $|\psi_0\rangle$ be a state from which the qubit can be recovered at V_0 by acting on $A\tilde{A}B_c$ and $|\psi_1\rangle$ a state from which the qubit can be recovered at V_1 by acting on $B\tilde{B}A_c$. Then, the overlap of the two states cannot be too large.
- $\rightarrow$ action of attackers before communicating already determines where the qubit ends up

Classical rounding

Definition

Let $\epsilon > 0$, $l \in \mathbb{N}$. A q-qubit strategy for PV^f_{qubit} is (ϵ, l)-*perfect* if on l pairs of strings (x, y), Alice and Bob are caught by the verifiers with probability at most ϵ^2. Equivalently, Alice and Bob produce a state $\left|\tilde{\psi}\right\rangle$ at the end of the protocol such that $\mathcal{P}(\rho_{RA}, |\Omega\rangle\langle\Omega|_{RA}) \leq \epsilon$ if $f(x, y) = 0$ and $\mathcal{P}(\rho_{RB}, |\Omega\rangle\langle\Omega|_{RB}) \leq \epsilon$ if $f(x, y) = 1$.

Definition

Let q, k, $n \in \mathbb{N}$, $\epsilon > 0$. Then,

$$g : \{0,1\}^{3k} \to \{0,1\}$$

is an (ϵ, q)-*classical rounding* of size k if for all $f : \{0,1\}^{2n} \to \{0,1\}$, for all states $|\psi\rangle$ on $2q + 1$ qubits, for all $l \in \{1, \ldots, 2^{2n}\}$ and for all (ϵ, l)-perfect q-qubit strategies for PV^f_{qubit}, there are functions $f_A : \{0,1\}^n \to \{0,1\}^k$, $f_B : \{0,1\}^n \to \{0,1\}^k$ and $\lambda \in \{0,1\}^k$ such that $g(f_A(x), f_B(y), \lambda) = f(x, y)$ on at least l pairs (x, y).

Proof idea (2/3)

- Action of attackers before communicating determines where qubit will end up
- Use ϵ-nets of size 2^k to discretize Alice's and Bob's unitaries and their initial state

$$f_A\colon\ x \in \{0,1\}^n \longrightarrow \text{label of } U^x,\ k\text{-bits string}$$

$$f_B\colon\ y \in \{0,1\}^n \longrightarrow \text{label of } V^y,\ k\text{-bits string}$$

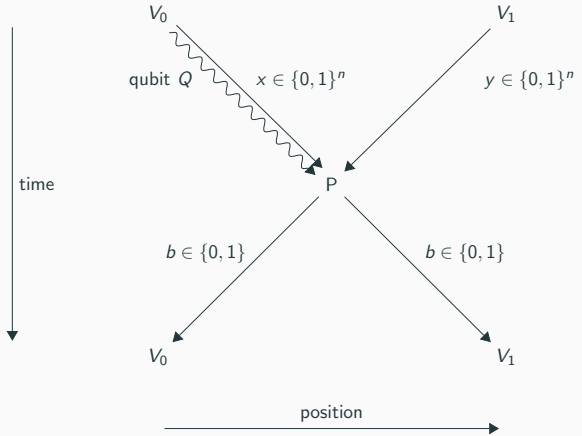
$$\lambda\colon \text{label of } |\psi\rangle,\ k\text{-bits string}$$

- You can determine from there where the qubit goes$\rightarrow$ (ϵ, q)-classical rounding $g : \{0,1\}^{3k} \to \{0,1\}$

Proof idea (3/3)

- Constructed (ϵ, q)-classical rounding
- Counting argument: number of (ϵ, q)-classical roundings $\ll$ number of Boolean functions f (on $2n$ bits)
- $q \leq n/2 - 5 \rightarrow$ most Boolean functions are far from any functions produced from classical roundings
- For $q \leq n/2 - 5$, Alice and Bob cannot succeed with probability at least $1 - \epsilon$ on too many input pairs (x, y)

Measuring protocol



- Protocol resembles [BK11]
- Verifiers prepare Q randomly as $|0\rangle$ or $|1\rangle$, apply Hadamard gate if $f(x, y) = 1$
- Prover measures in basis specified by $f(x, y)$, sends back outcome b
- Verifiers check consistency of b with the Q they sent

Pros and cons

- The protocol in [BK11] uses n-qubits, whereas we use a single qubit and a Boolean function on $2n$ bits
- Using an entropic uncertainty relation and modifying the proof slightly, we can prove the same security as for the routing protocol
- The routing protocol is simpler for the prover because there is no need to measure
- Security proof for the measuring protocol still holds if quantum information travels slowly
- Fits current technology better (qubits transmitted using fiber optics)

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 routing and measuring protocols with probability at least $2 \cdot 10^{-2}$, respectively.

- Proof based on communication complexity

Towards photon loss-tolerant protocols

Noise robust measuring protocol

- 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 measuring protocol, continued

Pros:

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

Cons:

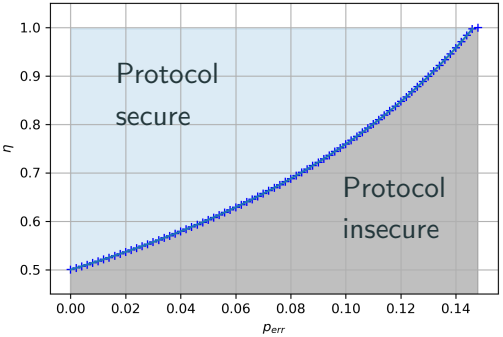
- 1% is not enough since photon loss in reasonable settings is 90% and more
- At 50% photon loss, the attackers can simply guess a basis and claim that they have lost the qubit if they guessed wrong. This breaks the protocol perfectly

SWAP test protocol

- Protocol analyzed in [ABSVL21]
- Based on SWAP test, verifiers send states with known overlap and compare statistics
- Fully photon loss-tolerant protocol secure against unentangled attackers with quantum communication
- Parallel repetition
- Practically feasible
- Can be broken with linear amount of EPR pairs

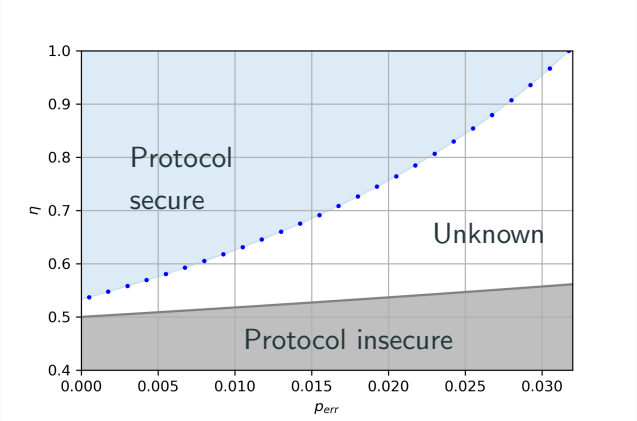
Partially loss-tolerant measuring protocol (1/3)

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



Partially loss-tolerant measuring 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 measuring protocol without loss

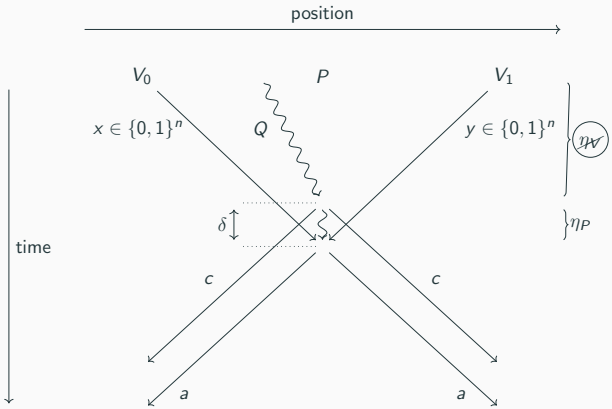


Partially loss-tolerant measuring protocol (3/3)

- So far, we could not go further than $\eta = 0.5$
- At that point, attackers can just guess the basis
- How to go beyond this threshold?
- Use more than 2 bases
- Third result: allows to go to lower η
- Downside: becomes experimentally more challenging as well

Making QPV protocols fully loss-tolerant

Protocol with commitment



- New step: commitment
- If qubit received prover sends $c = 1$; otherwise $c = 0$
- Strings x, y arrive slightly later (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

$$\mathcal{I}_i(\rho) = \mathcal{E}_i\left(\sqrt{M_i}\rho\sqrt{M_i}\right) \tag{1}$$

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: 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

$$\rho' = \frac{\sqrt{M}\rho\sqrt{M}}{\mathrm{tr}[M\rho]} \tag{2}$$

of measuring M fulfills

$$||\rho - \rho'||_1 \leq 2\sqrt{\varepsilon}. \tag{3}$$

Gentle measurement helps, continued

Post-measurement state after Lüders instrument:

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

Using the gentle measurement lemma, we can prove:

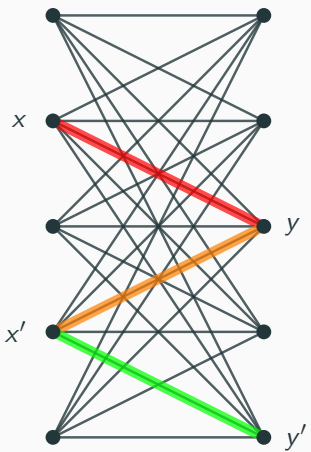
Lemma

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 significant commitment 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 $c2^{2n}$
- $(1 - 2\tilde{c})2^{2n}$ can still be reached within 2 steps from x'

Replacing by a fixed state

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

$$\Sigma_\varepsilon := \{(x,y) \mid \mathrm{tr}\{(M_A^x \otimes (\mathbb{I} - M_B^y))\,\rho\} \leq \varepsilon \wedge \mathrm{tr}\{(\mathbb{I} - M_A^x) \otimes M_B^y)\,\rho\} \leq \varepsilon\}.$$

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. On the rounds the attackers commit to play, the following bound on the probability of attacking c-$\mathrm{QPV}^f_{\mathrm{BB84}}$ holds:

$$\mathbb{P}[\text{attack } c\text{-}\mathrm{QPV}^f_{\mathrm{BB84}}] \leq \mathbb{P}[\text{attack } \mathrm{QPV}^f_{\mathrm{BB84}}] + (1 - 2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c}.$$

How do we get $\tilde{c}$ and ε?

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.

Corollary

Suppose we run $320k^3$ *rounds of* $c\text{-QPV}^f_{\text{BB84}}$. *Then either the attackers are detected with probability bigger than* $1 - 10^{-9}$ *or we have the following bound on the probability of attacking a single round* $c\text{-QPV}^f_{\text{BB84}}$ *depending only on* k*:*

$$\mathbb{P}[\text{attack } c\text{-QPV}^f_{\text{BB84}}] \leq \mathbb{P}[\text{attack QPV}^f_{\text{BB84}}] + \frac{4}{k}. \tag{4}$$

So far, we do not have a proof for adaptive attacks $\implies$ work in progress

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 the measurement protocol
- 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 photon loss

Open questions

- Better lower bounds for concrete functions
- Replace dimension count by entanglement measure
- Parallel repetition
- Superpolynomial lower bounds

Conclusion

- Measuring protocol is a very simple protocol (1 qubit only)
- Secure against linear amount of entanglement
- Can be made fully loss-tolerant by adding commitment
- The honest prover, however, does not need more quantum resources
- Seems experimentally feasible in principle

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

References

[ABSVL21]: R. Allerstorfer *et al*. 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.

[BFSS13]: H. Buhrman *et al*. The garden-hose model. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ITCS '13, pages 145–158. ACM, 2013.

[BK11]: S. Beigi and R. König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

More references

[EFS22] L. Escolà-Farràs and F. Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *arXiv preprint* arXiv:2212.03674, 2022.

[KMS11] A. Kent *et al*. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84:012326, 2011.

[MMWZ96] M. Michler *et al*. Interferometric Bell-state analysis. *Physical Review A*, 53(3):R1209, 1996.

[NFML21] D. Niemietz *et al*. Nondestructive detection of photonic qubits. *Nature*, 591(7851):570–574, 2021.