Secure quantum position verification

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

QuantAlps Days, October 2, 2023

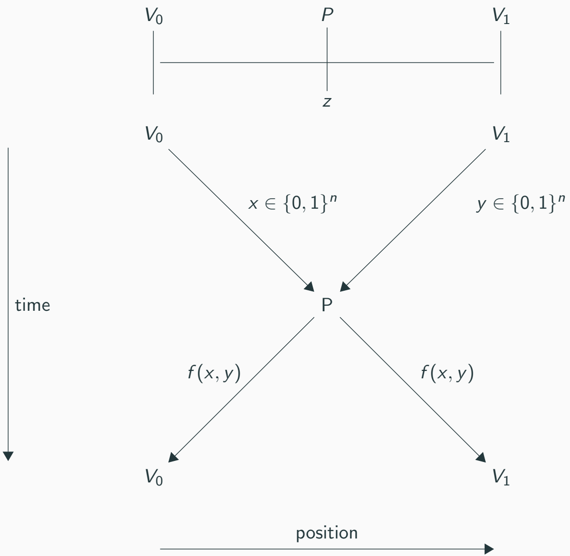
Introduction

- Why do you trust the clerk behind the counter at the bank?
- Answer: Because of her location!
- Position-based cryptography: Use position as credential
- Primitive: Secure (quantum) position verification

The classical situation

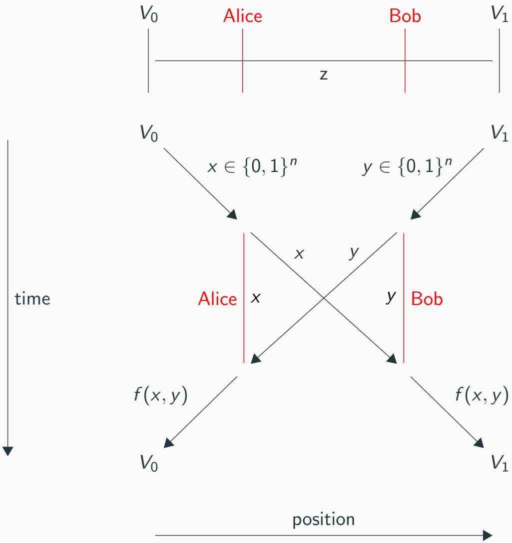
Classical protocols

- Special relativity: Information cannot travel faster than the speed of light
- Distance bounding: Send questions, accept if answers arrive fast enough



Classical attacks

- Is this protocol secure?
- No, collaborating attackers can break this protocol

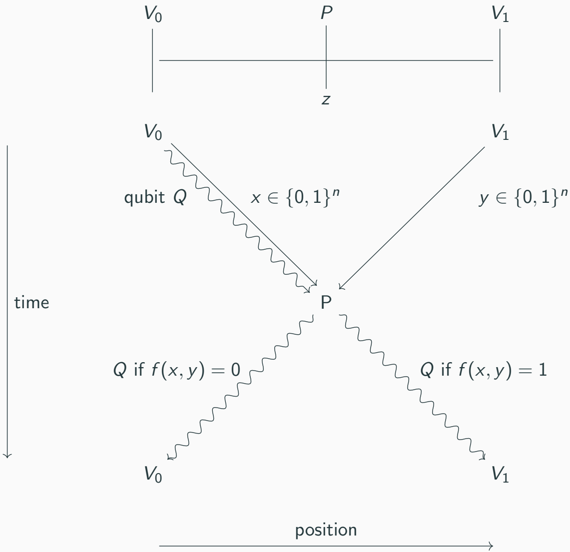


Why could going quantum help?

- Key step: Alice and Bob have to copy their bitstrings x and y
- No-cloning theorem: Quantum information cannot be copied perfectly
- On the downside, quantum attackers are more powerful as well
- In particular, they can use entanglement for quantum teleportation
- Unconditional security impossible, but we want to prove that attackers need a lot of entanglement

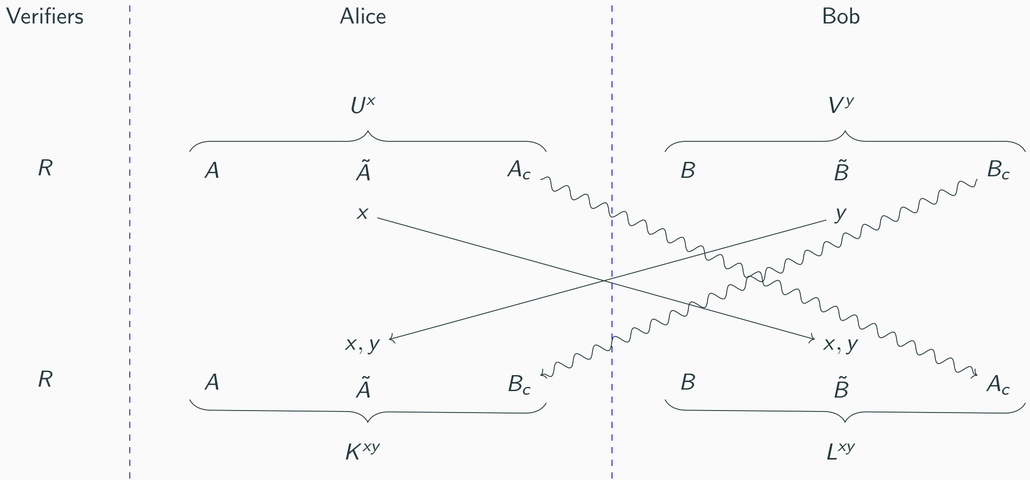
Simple quantum protocols

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



Security of qubit routing

Theorem[BCS22]

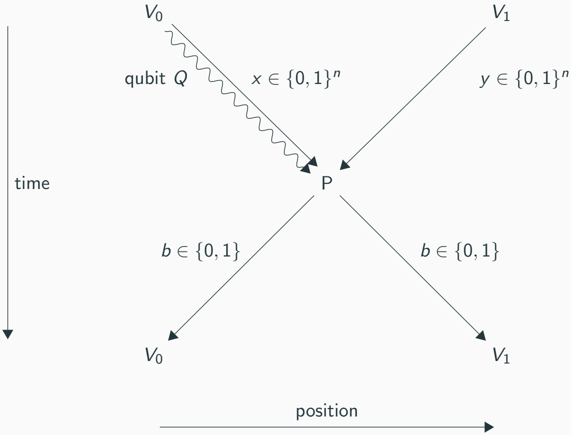
Let $n \geq 10$. Let us assume that the verifiers choose the bit strings x, y of length n uniformly at random. Then there exists a function $f : \{0,1\}^{2n} \to \{0,1\}$ with the property that, if the number q of qubits each of the attackers controls satisfies

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

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).

- Develops further prove method in [BFSS13]
- Success probability of the attackers can be suppressed exponentially by sequential repetition

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

Dealing with photon loss

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

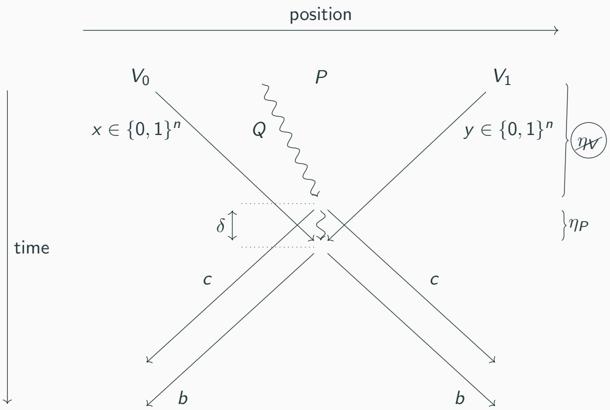
Pros:

- 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

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 $\rho^{x,y}$

Main result loss-tolerance

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

Corollary

Suppose we run $320k^3$ rounds of c-$\mathrm{QPV}^f_{\mathrm{BB84}}$. 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-$\mathrm{QPV}^f_{\mathrm{BB84}}$ depending only on k:

$$\mathbb{P}[\text{attack } c\text{-}\mathrm{QPV}^f_{\mathrm{BB84}}] \leq \mathbb{P}[\text{attack } \mathrm{QPV}^f_{\mathrm{BB84}}] + \frac{4}{k}. \quad (1)$$

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

Outlook

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)

Open questions

- f has to be truly random in our proof $\rightarrow$ circuit of exponential size. Can we get a function with circuit of polynomial size? Pseudo-randomness?
- Can we prove linear lower bounds also for concrete functions?
- We proved security for sequential repetition. Can we do parallel repetition securely?
- Bounds in terms of the number of qubits. Can we replace by an entanglement measure? Perhaps entropies or Schmidt rank?
- Linear lower bounds vs attacks with 2^n EPR pairs. Can we close the gap?

Conclusion

The routing are simple, secure against entanglement, and experimentally feasible

- The honest prover only needs to handle one qubit and needs not even measure it
- The verifiers need not create entangled states or have quantum memory
- The more classical bits the verifiers send, the more qubits the attackers need
- The honest prover, however, does not need more quantum resources
- Can be made fully loss-tolerant by adding commitment
- Seems experimentally feasible in principle

We can spend classical resources to increase the quantum cost of the attackers without increasing the quantum cost of the prover!

References

[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.

[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.

[NFLR21] D. Niemietz *et al.* Nondestructive detection of photonic qubits. *Nature*, 591(7851):570–574, 2021.