Position-based cryptography: Single-qubit protocol secure against multi-qubit attacks

Andreas Bluhm (QMATH, University of Copenhagen)
— joint work with Matthias Christandl and Florian Speelman arXiv:2104.06301

Brussels, May 31, 2022

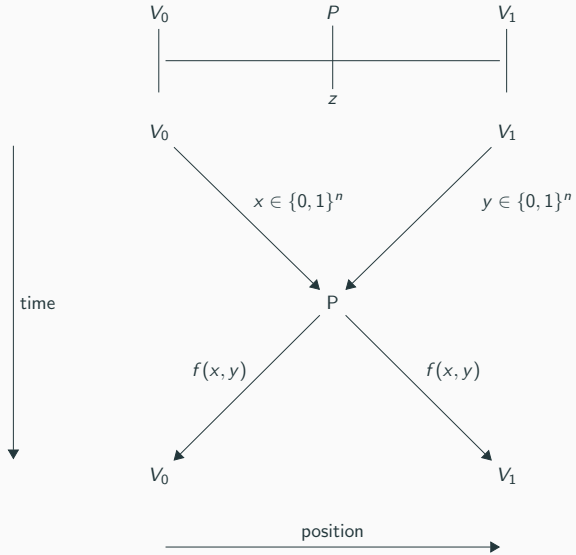
Introduction

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

The classical situation

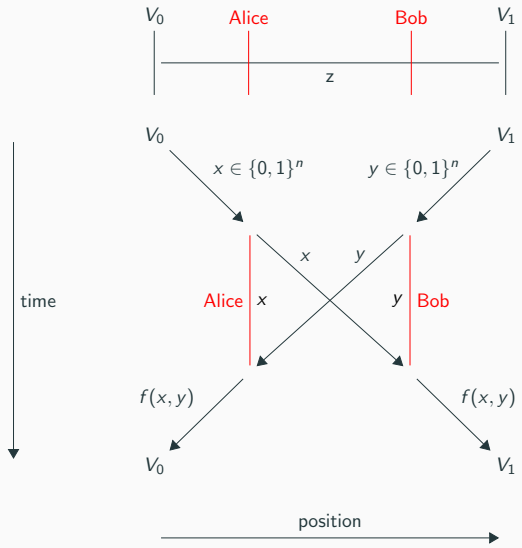
Classical protocols

- 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

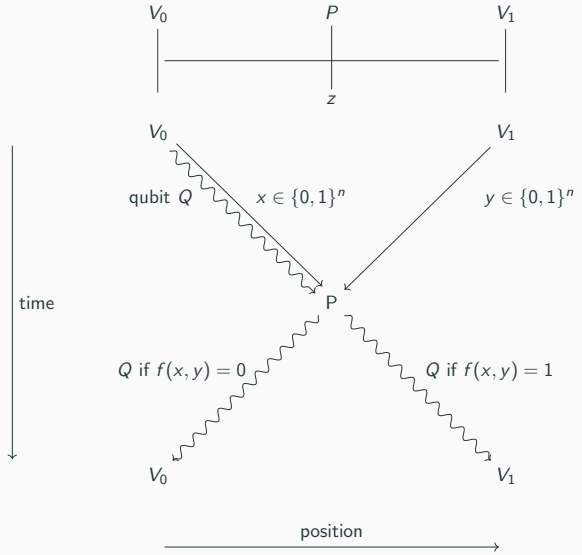


Why could going quantum help?

- Key step: Alice and Bob have to copy their bitstrings x and y
- No-cloning theorem: Quantum information cannot be copied perfectly
- In other words, there is no quantum channel such that $\rho \mapsto \rho \otimes \rho$ for all quantum states ρ
- 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

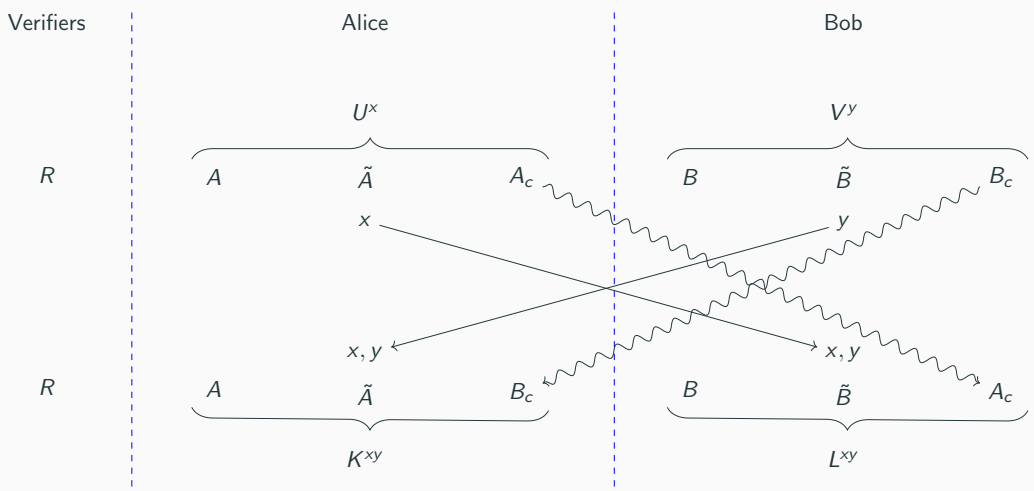
The qubit routing protocol

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

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 verifiers 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

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

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

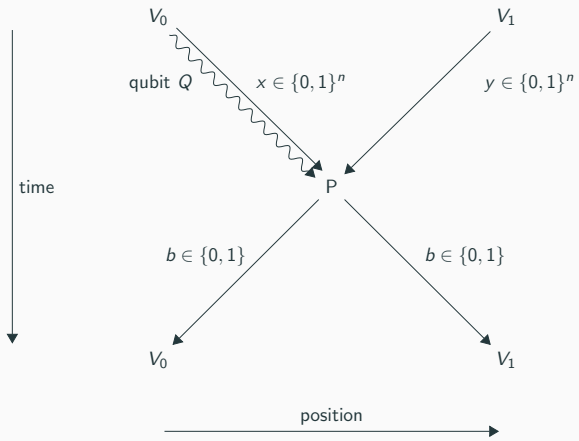
$$\lambda\colon \text{label of } |\psi\rangle,\ k\text{-bits string}$$

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

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 $1 - \epsilon 2$ 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)

Noise robust 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

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

Related work and outlook

The ultimate goal

- One would like to prove that attackers need an exponential amount of entanglement to break some position-verification protocol
- In our case, the honest prover only manipulates one qubit, whereas the attackers need $\Omega(n)$ qubits
- That's not only exponentially more resources, but unboundedly many more!
- That is still true for concrete functions, where the attackers need $\Omega(\log n)$ qubits
- Why does that not already show everything we could wish for?
- $\rightarrow$ The honest prover needs to manipulate $\Theta(n)$ classical bits

How to count resources

Questions to ask before comparing results:

- Do we only count quantum information manipulated by the attackers and the honest parties, or do we also quantify classical information?
- Do we look at the size of all quantum resources required, or do we just want to limit the pre-shared state of the attackers?
- Do we allow quantum communication between the attackers, or do we assume this communication to be classical and subsume these messages in the entanglement by way of teleportation?
- Would it be possible to bound the resources using something else than the number of qubits, such as entanglement entropy?

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?
- Bounds in number of qubits. Another entanglement measure? Entropies or Schmidt rank?
- Linear lower bounds vs attacks with 2^n EPR pairs. Can we close the gap?

Conclusion

The routing and measuring protocols have some nice features:

- 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

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

References

[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.

[JKPP]: M. Junge *et al*. Geometry of Banach spaces: a new route towards position based cryptography. arXiv-preprint arXiv:2103.16357, 2021.

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

Junge et al.

- Independent work [JKPP21]
- Classical information of n^2 bits is not counted
- Honest prover needs to manipulate $2 \log n$ qubits
- Attackers need $\Omega(n^\alpha)$ qubits for some $\alpha > 0$
- Security relies on conjecture in Banach space theory
- Introduces new tools to tackle the problem