New Protocols and Ideas for Practical Quantum Position Verficiation

arXiv:2106.12911

Rene Allerstorfer[1], Harry Buhrman[1,2], Florian Speelman[2], and Philip Verduyn Lunel[1]

[1]QuSoft, CWI Amsterdam
[2]QuSoft, University of Amsterdam

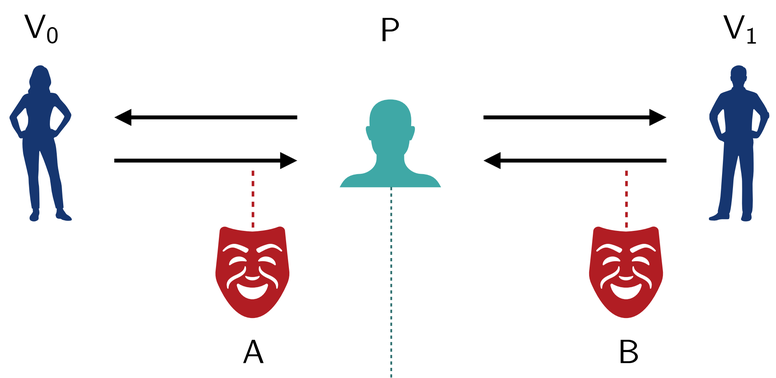
QuSoft Research Center for Quantum Software

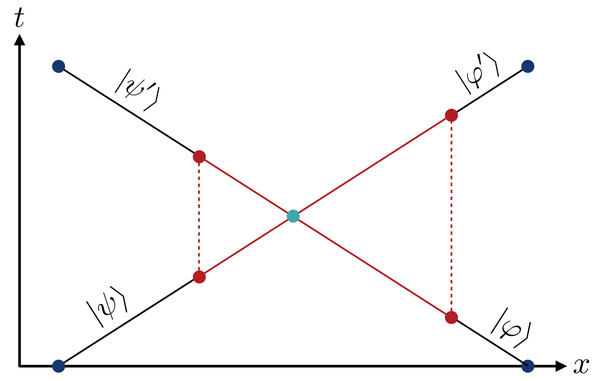
CWI Centrum Wiskunde & Informatica

Universiteit van Amsterdam

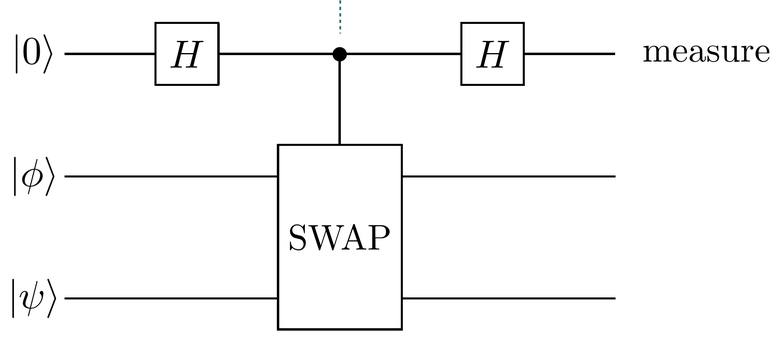
Quantum Position Verification

The setting in quantum position verification (QPV) consists of a set of trusted verifiers and an a priori untrusted party P at geographical location P, which will be their only cryptographic credential. The task for P is to convince the verifiers that P truly is at position P. To that end, the verifiers send challenges, possibly consisting of quantum and classical information, to P, who is asked to immediately perform a quantum operation $\mathcal{Q}$ (possibly depending on input information) on the inputs in order to produce a response. This then needs to be sent back to the verifiers again immediately and they check if the response is consistent with what they would expect if $\mathcal{Q}$ is applied to the inputs. Can a coalition of attackers A, B, not located at P, with *only local actions and one round of simultaneous communication*, classical (CC) or quantum (QC), fake being at P and convice the verifiers thereof? Yes [1, 2], but not necessarily if they only have access to a bounded amount of entanglement.





New protocol: $\mathsf{QPV}_{\mathsf{SWAP}}$



- Simplest case: Verifiers randomly choose between sending (uniformly random) orthogonal or identical states
- $\mathcal{Q}$ is the well known (and lab friendly) SWAP test, depicted on the left
- Expected statistics: $\mathbb{P}(0) = \frac{1+|\langle\psi|\phi\rangle|^2}{2}$ and $\mathbb{P}(1) = \frac{1-|\langle\psi|\phi\rangle|^2}{2}$
- After having run enough rounds a statistical test will accept P with high probability, while rejecting attackers with high probability
- Restricting attackers to no pre-shared entanglement and only positive-partial-transpose (PPT) actions $\{\Pi_0, \Pi_1, \Pi_\varnothing\}$ allows semi-definite program (SDP) formulation of attacker success probability

Result 1:

$\mathsf{QPV}_{\mathsf{SWAP}}(0,1)$ is secure since $p^{\mathsf{AB}}_{\mathsf{succ}} \leq \frac{2}{3} < \frac{3}{4} = p^{\mathsf{P}}_{\mathsf{succ}}$, obtained via SDP. This also holds if attackers are allowed to answer 'loss' ($\varnothing$) for a fraction $1-\eta \in [0,1)$ of the played rounds. Hence $\mathsf{QPV}_{\mathsf{SWAP}}(0,1)$ is *fully loss tolerant*.

Result 2:

$\mathsf{QPV}_{\mathsf{SWAP}}(0,1)$ fulfils parallel repetition, i.e. if executed in parallel n times then $p^{\mathsf{AB}}_{\mathsf{succ}} \leq \left(\frac{2}{3}\right)^n$. This, again, holds even if attackers are allowed to answer $\varnothing$ on any $k < n$ rounds. Hence $\mathsf{QPV}_{\mathsf{SWAP}}(0,1)$ retains security and full loss tolerance when run in parallel.

Result 3:

We show that the SWAP test can be simulated with one EPR pair and one round of CC. Therefore, a sufficient amount of pre-shared entanglement to break n rounds of $\mathsf{QPV}_{\mathsf{SWAP}}(0,1)$ perfectly is n EPR pairs, at least $\sim 0.103n$ EPR pairs are necessary.

Quantum Communication Attacks

- Often in QPV attackers are modelled to be constrained to LOCC or PPT actions, which does not capture all quantum communication attacks
- How does quantum communication affect the security of QPV?

Result 1:

We construct a protocol $\mathsf{QPV}_{\mathsf{sym/antisym}}$ that is secure (via SDP) against attackers constrained to CC but can be perfectly broken with one round of QC.

Result 2:

Any QPV protocol, that is secure under attackers restricted to CC but perfectly broken with one round of QC, can be transformed into a QPV protocol that is secure even if QC can be used. We re-use the hypothetical states attackers hold locally after one round of QC as inputs to two new QPV protocols, repeat this recursively and, using emergent classicality [3], show that at some level in this recursion a QPV protocol secure against QC has to exist.

Contact: rene.allerstorfer@cwi.nl, harry.buhrman@cwi.nl, f.speelman@uva.nl, phvl@cwi.nl

Loss, Entanglement and QPV

- Loss of signals or pre-shared entanglement can break security
- Can we have fully loss tolerant QPV that can only be attacked with superlinear entanglement resources? Unfortunately, no:

Result:

Any n-round QPV protocol can be broken with $\tilde{O}(n)$ pre-shared EPR pairs, if the fraction η of rounds used for security analysis is low enough (i.e. if the loss is high enough).

References

[1] Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., & Schaffner, C. (2014). Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1), 150-178

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

[3] Qi, X. L., & Ranard, D. (2020). Emergent classicality in general multipartite states and channels. *arXiv preprint* arXiv:2001.01507