Breaking simple quantum position verification protocols with little entanglement

Andrea Olivo[1,2], Ulysse Chabaud[3], Frédéric Grosshans[3], André Chailloux[1]

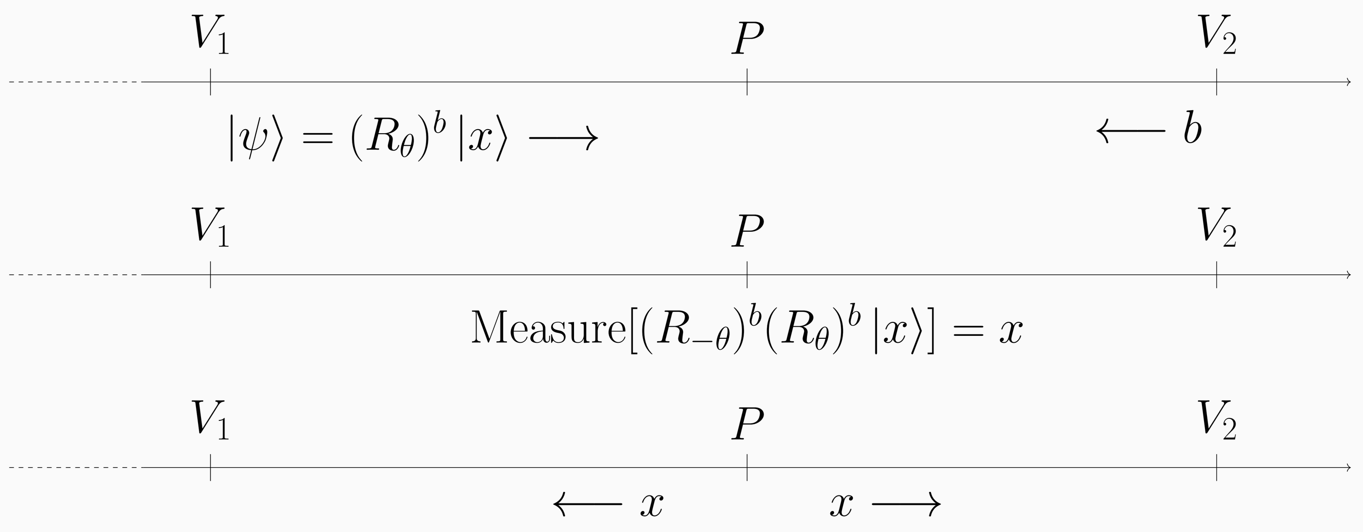
[1]Inria, Paris, France [2]LPGP, CNRS, Université Paris-Saclay, Orsay CEDEX [3]LIP6, CNRS, Sorbonne Université, Paris

Abstract

Instantaneous nonlocal quantum computation (INQC) evades apparent quantum and relativistic constraints and allows to attack generic quantum position verification (QPV) protocols (aiming at securely certifying the location of a distant prover) at an exponential entanglement cost. We consider adversaries sharing maximally entangled pairs of qudits and find low-dimensional INQC attacks against the simple practical family of QPV protocols based on single photons polarized at an angle θ. We find exact attacks against some rational angles, including some sitting outside of the Clifford hierarchy (e.g. $\pi/6$), and show no θ allows errors larger than $\simeq 5 \cdot 10^{-3}$ against adversaries holding two ebits per protocol's qubit.

QPV in general and QPV$_\theta$

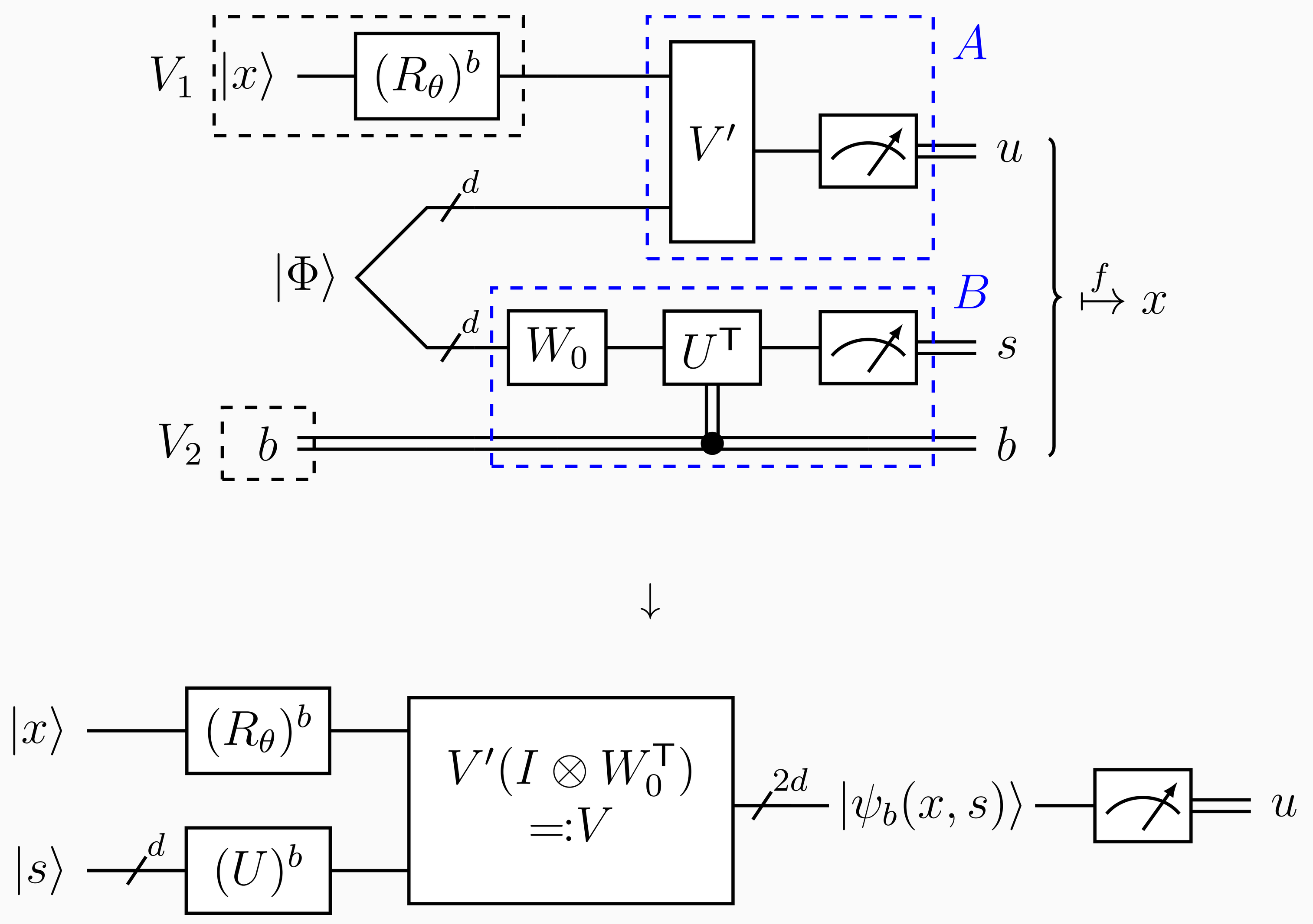
We could rely on geographical position as secure credential.



Unfortunately, for all PV protocols:

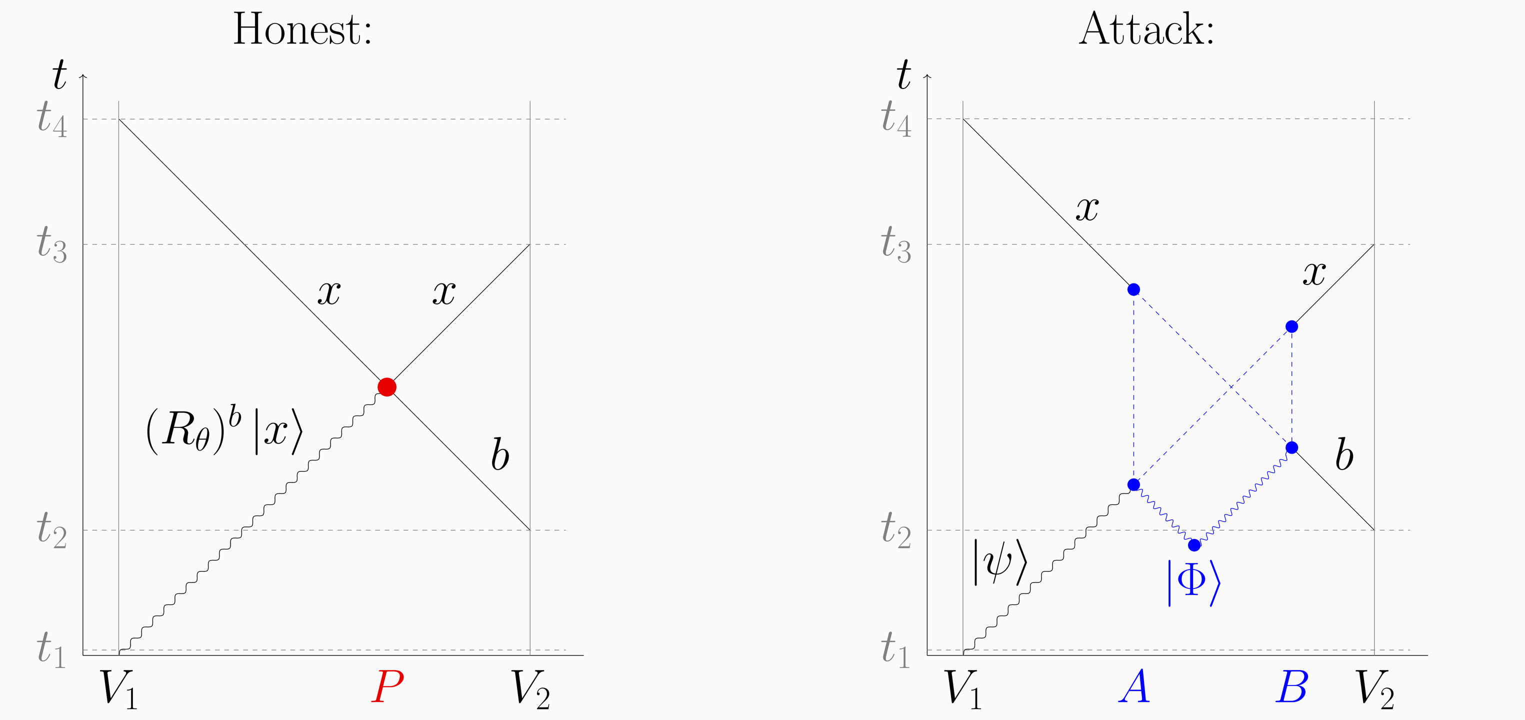
- Impossibility proof [3] in the classical setting: $\mathcal{O}(n)$ attacks for n-bit protocol
- More luck in the quantum setting?
  - Secure QPV in the No-Preshared-Entanglement [2] and Random Oracle model [6].
  - No information-theoretic security for unbounded adversaries: there are universal approximate attacks through INQC, $\sim \mathcal{O}(2^{8n})$ ebits [1].
  - Polynomial cost for (some) structured protocols

Circuit Picture



Any attack is specified by the unitaries V and U. By imposing specific requirements on the output states $|\psi_b(x,s)\rangle$, we obtain necessary and sufficient conditions for the existence of an attack in our model.

Spacetime diagram



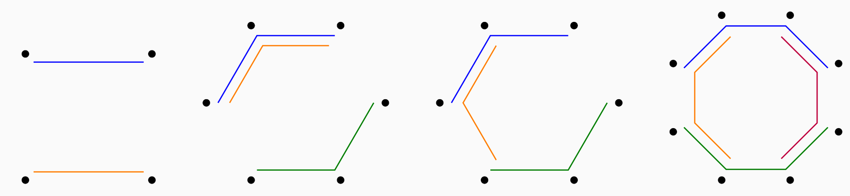
For $\theta = \pi/4$ attackers can perfectly win if $|\Phi\rangle$ is a maximally entangled qubit pair [4].

Exact attacks

We generalize this "teleportation" attack by allowing maximally entangled qu*d*its, and numerically discover many more angles, of the form $\theta = \pi/k$ (and multiples), that can be perfectly broken with small d. Conjectured pattern: dimension d breaks at least $\theta = \frac{n\pi}{2d}$.

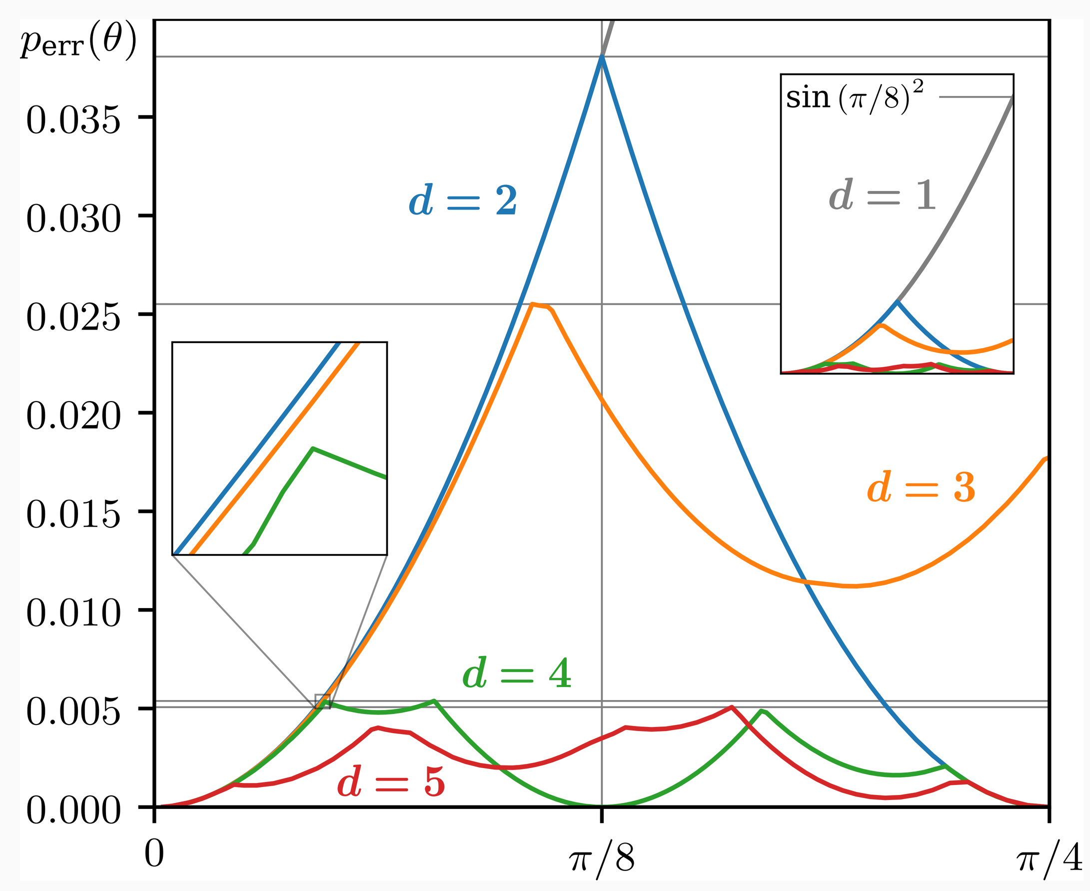
d	2	3	4	5	6	7	8	9	10	11	12
k	4	2	8	4	8, 12	4	16	4, 6	20	4	24

Through a hypergraph-based representation of the hilbert space, we easily (re)prove a result of Lau and Lo [5] about dimensions $d = 2, 3$ being unable to break anything but the BB84-like $\pi/4$ angle.

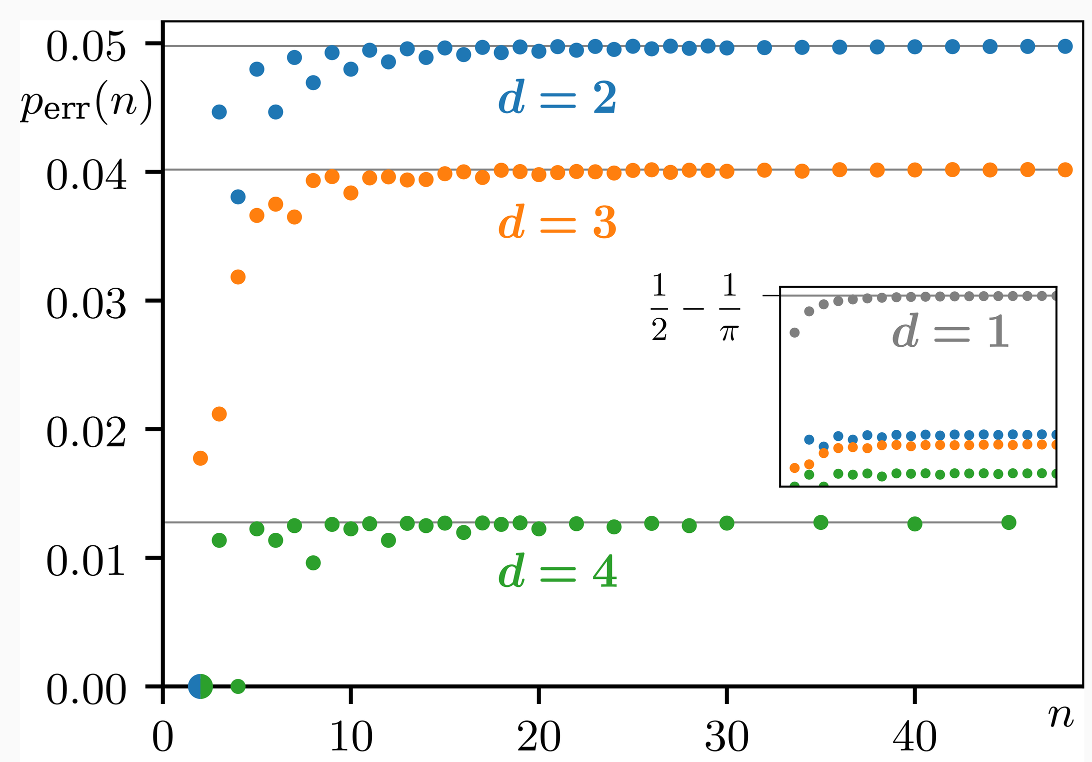


Approximate attacks

For $d \leq 5$, we numerically optimize for the attack strategy minimizing the error.



We also consider QPV$_{(n)}$, a variant of the protocol where multiple bases are used, in the form of n equally spaced angles in $[0, \pi/2]$.



References

[1] Salman Beigi and Robert König. "Simplified instantaneous non-local quantum computation with applications to position-based cryptography". In: *New Journal of Physics* 13 (2011), p. 093036. DOI: 10.1088/1367-2630/13/9/093036. arXiv: 1101.1065.

[2] Harry Buhrman et al. "Position-Based Quantum Cryptography: Impossibility and Constructions". In: *SIAM Journal on Computing* 43.1 (2014), pp. 150–178. DOI: 10.1137/130913687. arXiv: 1009.2490.

[3] Nishanth Chandran et al. "Position Based Cryptography". In: *Advances in Cryptology - CRYPTO 2009*. Ed. by Shai Halevi. Vol. 5677. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009, pp. 391–407. ISBN: 978-3-642-03355-1. DOI: 10.1007/978-3-642-03356-8_23. IACR: 2009/364.

[4] Adrian Kent, William J. Munro, and Timothy P. Spiller. "Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints". In: *Phys. Rev. A* 84 (1 July 2011), p. 012326. DOI: 10.1103/PhysRevA.84.012326. arXiv: 1008.2147.

[5] Hoi-Kwan Lau and Hoi-Kwong Lo. "Insecurity of position-based quantum-cryptography protocols against entanglement attacks". In: *Phys. Rev. A* 83 (1 Jan. 2011), p. 012322. DOI: 10.1103/PhysRevA.83.012322. arXiv: 1009.2256.

[6] Dominique Unruh. "Quantum Position Verification in the Random Oracle Model". In: *Advances in Cryptology – CRYPTO 2014*. Ed. by Juan A. Garay and Rosario Gennaro. Vol. 8617. Lecture Notes in Computer Science. Springer Berlin Heidelberg, Aug. 2014, pp. 1–18. ISBN: 978-3-662-44380-4. DOI: 10.1007/978-3-662-44381-1_1. IACR: 2014/118.

ID of arXiv preprint: [quant-ph] 2007.15808

LaTeX TikZposter