Breaking simple quantum position verification protocols with little entanglement

Andrea Olivo, Ulysse Chabaud, André Chailloux, and Frédéric Grosshans
(affiliations provided in the full version of the paper)

In this work, we study a cryptographic primitive known as position verification (PV), the quantum version of which (QPV) was introduced in 2010 independently by multiple works [1–3]. Secure implementations of PV, if they exist, aim to provide some *prover* P with the possibility of certifying to a third party (the *verifier* V) its location in space. One of PV's applications is the authentication of a physical channel, where the prover's position is used as the only token. In this scenario, a bank's new user could trust a connection to the bank's services by securely certifying it comes from the (public) bank's location, thus avoiding the need of public-key authentication schemes whose security in a post-quantum world is still a major open question.

PV has been shown [4] to be insecure in the classical setting, even under computational assumptions. A coalition of colluding adversaries, neither of which at the claimed position, can mimic the honest prover's actions by copying and sharing the data sent by the verifiers, while also being able to comply with the timing constraints. It is then natural to ask how the situation changes if we allow the verifier's challenges to be quantum states, knowing that (in the general case) they cannot be faithfully copied. The problem is interesting in its own right, as it sits at the subtle interplay between quantum constraints on measurements and relativistic effects. The design of generic attacks to QPV led to a technique, consuming an exponential amount of entanglement in the verifier's qubits, called instantaneous nonlocal quantum computation (INQC) [5, 6]. Security proofs for QPV have proven to be elusive, with the notable exception of a hash-function based protocol [7], and linear-entanglement lower bounds for the protocol class we analyze [8, 9]. On the other hand, the entanglement requirement has been reduced to polynomial for some classes of structured protocols [10–13].

The focus of our work is to explore the security against small entangled adversaries of a class of experimentally simple protocols (described in the full version of the paper), a variation on the BB84-inspired protocols where the polarisation angle θ is not a multiple of $\frac{\pi}{4}$. These protocols with non-Clifford angles have already been introduced [1] to defeat teleportation based attacks, and their security partly characterized in previous work [14]. We provide:

- A definition of the attack model (in quantum circuit representation) that encompasses a wider class of attacks for adversaries sharing a maximally entangled pair of d-level systems.

- A no-go proof for $d = 2$ and $d = 3$ (equivalent to the one in [14]) by introducing a possibly more intuitive graphical representation of the attacker's Hilbert space.

- A thorough numerical exploration of exact attacks up to $d = 12$ by reducing the problem to finding solutions of a nonlinear system of polynomial equations, giving new INQC attacks for many θ using much smaller entangled states than previous techniques [11–13].

- A numerical analysis of non-exact attacks for $d \leq 5$, by allowing the attackers a probability of failure p_{err} that we seek to minimize, finding that with just two ebits per verifier's qubit $\min\{p_{\text{err}}\}$ is upper bounded by $\simeq 5 \cdot 10^{-3}$. An extension of the protocol where the verifier is allowed more than two basis choices is similarly explored.

The full preprint can be found at `arxiv.org/abs/2007.15808`.

[1] A. Kent, W. J. Munro, and T. P. Spiller, Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints, Phys. Rev. A **84**, 012326 (2011), arXiv:1008.2147.

[2] R. A. Malaney, Location-dependent communications using quantum entanglement, Phys. Rev. A **81**, 042319 (2010), arXiv:1003.0949.

[3] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, Position-based quantum cryptography (2010), withdrawn and replaced by [5].

[4] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, Position based cryptography, in *Advances in Cryptology - CRYPTO 2009*, Lecture Notes in Computer Science, Vol. 5677, edited by S. Halevi (Springer Berlin Heidelberg, 2009) pp. 391–407, IACR:2009/364.

[5] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, Position-based quantum cryptography: Impossibility and constructions, SIAM Journal on Computing **43**, 150 (2014), arXiv:1009.2490.

[6] S. Beigi and R. König, Simplified instantaneous non-local quantum computation with applications to position-based cryptography, New Journal of Physics **13**, 093036 (2011), arXiv:1101.1065.

[7] D. Unruh, Quantum position verification in the random oracle model, in *Advances in Cryptology – CRYPTO 2014*, Lecture Notes in Computer Science, Vol. 8617, edited by J. A. Garay and R. Gennaro (Springer Berlin Heidelberg, 2014) pp. 1–18, IACR:2014/118.

[8] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, A monogamy-of-entanglement game with applications to device-independent quantum cryptography, New Journal of Physics **15**, 103002 (2013), arXiv:1210.4359.

[9] J. Ribeiro and F. Grosshans, A tight lower bound for the BB84-states quantum-position-verification protocol, arXiv:1504.07171 (2015).

[10] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman, The garden-hose model, in *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ITCS '13 (Association for Computing Machinery, New York, NY, USA, 2013) p. 145–158.

[11] K. Chakraborty and A. Leverrier, Practical position-based quantum cryptography, Phys. Rev. A **92**, 052304 (2015), arXiv:1507.00626.

[12] F. Speelman, Instantaneous non-local computation of low T-depth quantum circuits, in *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 61, edited by A. Broadbent (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2016) pp. 9:1–9:24.

[13] A. Gonzales and E. Chitambar, Bounds on instantaneous nonlocal quantum computation, IEEE Transactions on Information Theory **66**, 2951 (2020), arXiv:1810.00994.

[14] H.-K. Lau and H.-K. Lo, Insecurity of position-based quantum-cryptography protocols against entanglement attacks, Phys. Rev. A **83**, 012322 (2011), arXiv:1009.2256.