Families of Quantum Fingerprinting Protocols

Benjamin Lovitz and Norbert Lütkenhaus

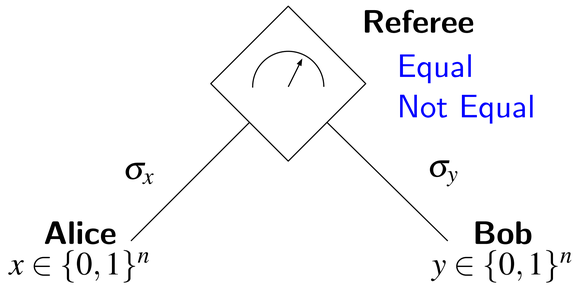
Department of Physics and Astronomy, Institute for Quantum Computing, University of Waterloo.

Research supported in part by NSERC, Industry Canada and ARL CDQI program. The Institute for Quantum Computing is supported in part by the Government of Canada and the Province of Ontario.

Project overview

Quantum fingerprinting (QF) is a fundamental communication task in which two nonlocal parties wish to evaluate the equality function on their inputs by each communicating with a single referee. We are interested in protocols which minimize the information leakage, that is, the amount of information the referee learns about the parties' inputs. An existing coherent state QF protocol of [Arrazola and Lütkenhaus, 2014] (henceforth, "optical protocol") has recently been implemented using binary phase-encoded laser pulses. However, the number of signals required poses a challenge to the long-term stability of experimental set-ups, and has prevented implementations from beating the classical information leakage lower bound. In this work, we find several families of QF protocols which reduce the number of signals required.

Review: quantum fingerprinting



CC=Communication Cost $= \log\dim(A) + \log\dim(B)$

QIL=Information Leakage $= \sup_P \mathrm{I}(XY;AB)_{\rho_P}$

Where: $\rho_P = \sum_{x,y\in\{0,1\}^n} P(x,y)|xy\rangle\langle xy| \otimes \sigma_x^A \otimes \sigma_y^B$

$P \in \Pr(\{0,1\}^n \times \{0,1\}^n)$

In quantum fingerprinting, Alice and Bob attempt to evaluate the equality function on their respective inputs $x, y \in \{0,1\}^n$. To do so, they each send quantum states σ_x, σ_y to a central referee, who performs a measurement and outputs either Equal or Not Equal (pre-shared randomness is disallowed in this model). Using classical states, the CC and QIL must be $\Omega(\sqrt{n})$ to attain a fixed error probability, whereas there exist protocols using quantum states with CC, QIL $\mathcal{O}(\log n)$.

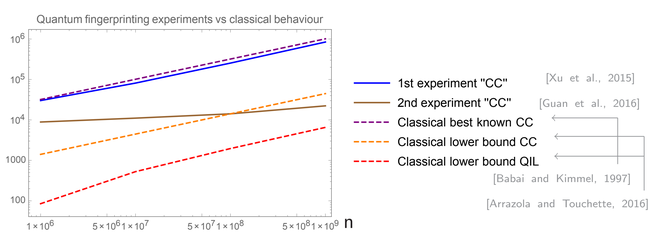
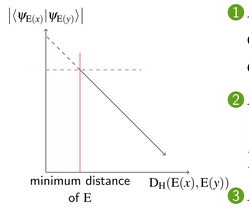


Figure: Past experimental implementations of the existing optical protocol. A remaining experimental challenge is to beat the classical lower bound in terms of QIL.

A general framework for all our protocols



1. Alice encodes her input $x \in \{0,1\}^n$ into a codeword $\mathrm{E}(x) \in \{0,1\}^m$ of an error-correcting code E.
2. Alice maps $\mathrm{E}(x)$ to a state $|\psi_{\mathrm{E}(x)}\rangle$ for which $|\langle\psi_{\mathrm{E}(x)}|\psi_{\mathrm{E}(y)}\rangle|$ is a decreasing function of the Hamming weight $\mathrm{D}_H(\mathrm{E}(x),\mathrm{E}(y))$.
3. Alice sends $|\psi_{\mathrm{E}(x)}\rangle$ to the referee.

... and Bob does the same with his input y. The minimum distance of the code E ensures that states corresponding to different inputs are sufficiently distinguishable to the referee.

Our results: improved optical protocol

We find several families of coherent state protocols which reduce the number of signals below that of the optical protocol. One such protocol reduces the number of signals by a factor 1/2 while also reducing the information leakage. We find that further reduction in the number of signals is not advantageous.

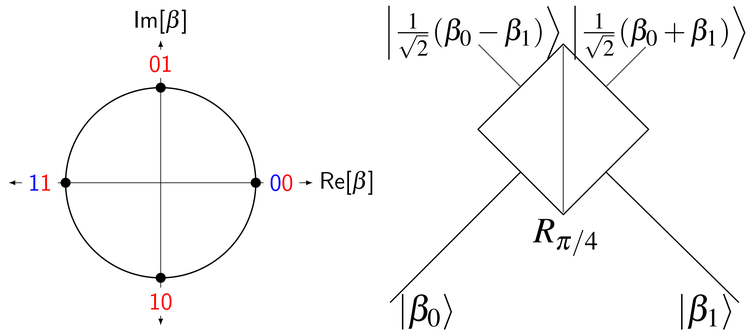


Figure: At left, a phase space representation of the existing optical coherent state protocol (blue) and our improved protocol (blue and red). In the existing protocol, each bit of $\mathrm{E}(x)$ is encoded into a coherent state signal of $\pm$ phase. Our improved protocol encodes two bits of $\mathrm{E}(x)$ into each signal, thus sending half the signals. At right, we review the 50/50 beamsplitter measurement used in both protocols: the referee outputs Not Equal if any clicks occur in the dark port (left port).

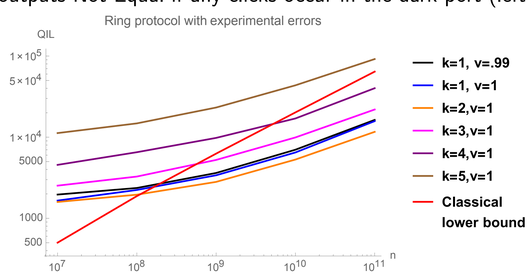


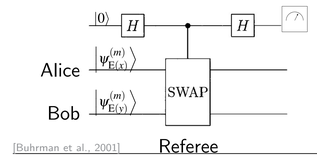
Figure: QIL, measured in bits, as a function of the input size n for our coherent state protocols with block-size k to attain error probability $\epsilon = 0.01$ under transmittivity $\eta = 0.3$ and dark count probability $p_{\mathrm{dark}} = 7.3 \times 10^{-11}$. Note that our improved optical protocol ($k = 2$) outperforms the existing optical protocol ($k = 1$). And protocols using fewer signals ($k > 2$) are not advantageous.

Our results: interpolation protocols

There is also interest in experimental realization of QF using possibly non-coherent quantum states. The existing optical protocol can be implemented using any physical system which can represent two qubits, but the number of signals required is again a drawback to experimental implementation. We find a family of abstract quantum protocols which reduces the number of signals required while maintaining information leakage $\mathcal{O}(\log n)$. Of added theoretical interest, this family converges to the existing optical protocol on one end, and to the original quantum fingerprinting protocol of [Buhrman et al., 2001] on the other, and demonstrates a trade-off between the number of signals sent and the dimension of each signal.

Original protocol

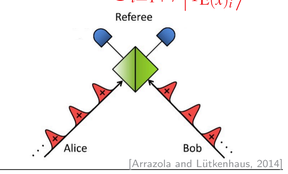
$$\left|\psi^{(m)}_{\mathrm{E}(x)}\right\rangle = \tfrac{1}{\sqrt{m}}\textstyle\sum_{i=1}^m |i\rangle\,|\mathrm{E}(x)_i\rangle = \tfrac{1}{\sqrt{m}}\textstyle\sum_{i=1}^m |i\rangle\left|q^{(m)}_{\mathrm{E}(x)_i}\right\rangle$$



[Buhrman et al., 2001]

Optical protocol

$$\left|\psi^{(1)}_{\mathrm{E}(x)}\right\rangle = \textstyle\bigotimes_{i=1}^m \left|(-1)^{\mathrm{E}(x)_i}\tfrac{\alpha}{\sqrt{m}}\right\rangle_i \cong \textstyle\bigotimes_{i=1}^m |i\rangle\left|q^{(1)}_{\mathrm{E}(x)_i}\right\rangle$$



[Arrazola and Lütkenhaus, 2014]

# signals	Signal dimension	Information leakage
$O(1)$	$O(n)$	$O(\log n)$
"$O(n/k)$"	"$O(k)$"	"$O(\log n)$"
$O(n)$	2	$O(\log n)$

Interpolation protocol with block-size k

$$\left|\psi^{(k)}_{\mathrm{E}(x)}\right\rangle = \textstyle\bigotimes_{j=1}^{m/k}\left[\frac{1}{\sqrt{k}}\sum_{i\in \mathrm{I}[j,k]}|i\rangle\left|q^{(k)}_{\mathrm{E}(x)_i}\right\rangle\right]$$

$\mathrm{I}[j,k]$ indexes the j-th block of k bits of $\{0,1\}^m$

Measurement is combination of controlled-SWAP and beamsplitter measurements

Our results: improved ED protocol

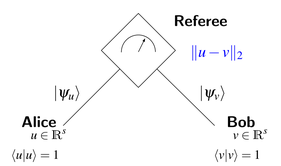
Using a similar technique as in our improved optical QF protocol, we reduce the number of signals by a factor 1/2 and also reduce the information leakage of the coherent state Euclidean distance protocol proposed in [Kumar et al., 2017].

Existing optical protocol

$$|\psi_u\rangle_1 = \bigotimes_{j=1}^{s} |u_j\alpha\rangle_j.$$

Our protocol

$$|\psi_u\rangle_2 = \bigotimes_{\substack{j=1\\ \text{odd}}}^{s} |(u_j + iu_{j+1})\alpha\rangle_j$$



[Arrazola and Lütkenhaus, 2014] Arrazola, J. M. and Lütkenhaus, N. (2014). Quantum fingerprinting with coherent states and a constant mean number of photons. *Phys. Rev. A*, 89:062305.

[Arrazola and Touchette, 2016] Arrazola, J. M. and Touchette, D. (2016). Quantum Advantage on Information Leakage for Equality. *ArXiv e-prints*.

[Buhrman et al., 2001] Buhrman, H., Cleve, R., Watrous, J., and de Wolf, R. (2001). Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902.

[Guan et al., 2016] Guan, J.-Y., Xu, F., Yin, H.-L., Li, Y., Zhang, W.-J., Chen, S.-J., Yang, X.-Y., Li, L., You, L.-X., Chen, T.-Y., Wang, Z., Zhang, Q., and Pan, J.-W. (2016). Observation of quantum fingerprinting beating the classical limit. *Phys. Rev. Lett.*, 116:240502.

[Kumar et al., 2017] Kumar, N., Diamanti, E., and Kerenidis, I. (2017). Efficient quantum communications with coherent state fingerprints over multiple channels. *Phys. Rev. A*, 95:032337.

[Xu et al., 2015] Xu, F., Arrazola, J. M., Wei, K., Wang, W., Palacios-Avila, P., Feng, C., Sajeed, S., Lütkenhaus, N., and Lo, H.-K. (2015). Experimental quantum fingerprinting with weak coherent pulses. *Nature communications*, 6.