Performing private database queries in a real-world environment using a quantum protocol

Philip Chan, Itzel Lucio-Martinez, Xiaofan Mo, Christoph Simon, Wolfgang Tittel

Private query protocols [1-3] use uncertainty in quantum mechanics to offer functionality similar to 1-out-of-N oblivious transfer (where a user, Ursula, retrieves a single element from a database provider, Dave, who learns nothing about which of the N elements was retrieved). The difference in functionality varies for each private query protocol, but in all cases is motivated by the fact that perfect 1-out-of-N oblivious transfer has been shown to be impossible if the attacker possess an arbitrarily powerful quantum computer [4]. Nonetheless, quantum protocols can offer security against stronger adversaries than protocols relying only on classical information, and it remains an interesting question as to what level of security can be achieved using quantum information. We present a proof-of-principle demonstration of a novel private query protocol that is loss- and fault-tolerant, making it suitable for implementation in a real-world environment, and show that it offers excellent privacy against several quantum attacks [5]. This demonstration is performed over a deployed fibre link between the University of Calgary and SAIT Polytechnic using a slightly modified quantum key distribution (QKD) system [6].

Oblivious transfer (OT) is a well studied primitive in classical information theory, and protocols that exist rely on one of two assumptions: that an attacker has limited classical computational capabilities [7,8], or that some number of intermediaries may be trusted [9]. Recently several private query protocols have been proposed [1-3] that are secure against arbitrarily powerful classical computers, and do not require trusted intermediaries. These protocols also have the potential to be secure against arbitrarily powerful quantum computers (although security proofs remain an open question) as they relax the conditions for perfect 1-out-of-N oblivious transfer.[1] For example, in [2,3] Ursula learns more than a single element of the database, and Dave has the possibility of learning which element Ursula desired, but at the cost of introducing errors into the retrieved element. This latter property is known as cheat sensitivity, and is particularly useful for practical applications of private queries where Dave acts as a service provider (e.g. making financial recommendations), as the errors introduced by a dishonest Dave will give him a reputation of providing poor results. However, the practical use of these protocols is limited by the fact that they are not simultaneously loss- and fault-tolerant, preventing implementation over realistic channels.

The QPQ protocol we present is similar to [2,3], sharing the cheat sensitive property and implementing functionality that can be described as probabilistic n-out-of-N OT (where n is a distribution of probabilistic knowledge stemming from the uncertainty in quantum measurements). However, unlike previous protocols, our protocol can operate over a lossy and noisy channel, which is a crucial feature for practical implementations. The latter feature is achieved by integrating a novel error correction procedure into the protocol. A brief summary of our protocol follows (see [5] for a technical description). Dave begins by encoding classical bit values into qubits using four non-orthogonal states and sending them to Ursula (this step is similar to SARG04 QKD [11]). Ursula measures the qubits and announces which qubits were successfully detected, allowing information corresponding to lost qubits to be discarded by both parties. Dave then sends Ursula classical information which allows her to interpret her measurements. This information is deliberately limited such that, using her measurement results,

[1] We note that there has recently been an implementation of a quantum protocol implementing 1-out-of-N OT, where security holds under the assumption that the adversary's capabilities are limited by noisy quantum storage [10].

Ursula has a small probability to deterministically identify the classical bit Dave encoded, gaining only probabilistic information about the bit value in the majority of cases. A parity operation is then used to further reduce Ursula's knowledge of the classical bit values, forming an oblivious key. Dave also sends additional information for error-correction at this point. Ursula uses this information to calculate the probability that she knows each oblivious key bit, and if that probability is sufficiently high, she considers the bit value to be known. The parameters of the protocol are chosen such that Ursula learns a bit in this way with probability ~1/N. Note that the location of Ursula's known bits in the oblivious key are random, and unknown to Dave. In order to select a specific location to place her known bit to choose her query, Ursula selects a shift value to apply to the oblivious key. This shift value is communicated to Dave, and does not give him any knowledge of which bits Ursula knows. Finally, the query is performed by using one-time-pad encryption with the shifted oblivious key to send the database to Ursula, who can only recover the database elements for which she knows the corresponding oblivious key bit.

The selection of an appropriate error correcting code is crucial to ensuring that Ursula learns an appropriate number of bits of the oblivious key while simultaneously limiting the probabilistic knowledge that she gains about the rest of the key. As a result of these unique requirements, the error correction process required for our protocol differs from that used in telecommunications or QKD. In particular, we exploit the properties of our protocol in conjunction with error correction on short blocks (no more than 10 bits) so that Ursula has a high level of uncertainty about the majority of the oblivious key after error correction. The performance of an error correcting code is evaluated based on $\bar{n}$, the average number of bits of the oblivious key for which Ursula's probability of error after error correction is less than 10^{-3} (she considers these bits to be known), and on $\bar{m}$, the percentage of the oblivious key for which her probability of error is less than 1/3 (Dave considers this to be significant knowledge about the oblivious key bit). Note that these knowledge thresholds should be selected based on the application at hand.

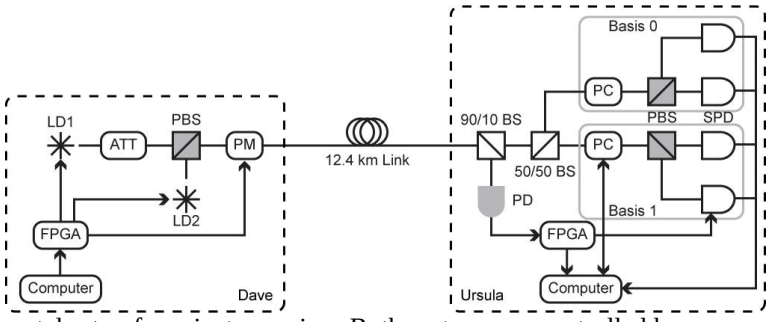

Figure 1 – Experimental setup for private queries. Both systems are controlled by a computer interfaced with a field-programmable gate-array (FPGA). Dave creates faint pulses using a laser diode (LD1) and an attenuator (ATT) and modulates them using a polarization modulator (PM). Ursula uses a 50/50 beamsplitter to randomly select a measurement basis, and detects the qubits using single photon detectors (SPDs). A second laser diode (LD2) is used to generate strong light (detected by the photodiode (PD) after the 90/10 beamsplitter) which is used for system timing and as a reference for the polarization controllers (PC).

Error correcting codes for our demonstration were selected using an exhaustive search of codes up to 10 bits in length given our system parameters (e.g. loss, noise), and targeting a database size of $N=10^6$. We performed our experiment over a 12.4 km dark fibre link with 4.5 dB loss between the University of Calgary and SAIT Polytechnic, using the system depicted in Figure 1 (see [6] for a detailed description). Private queries were first performed at the single photon level (μ=0.95), where 11 queries were performed, yielding $\bar{n}$ = 4.1 and $\bar{m}$ = 6.1% with a total of 45 bits learned.

Due to the fact that 10^7 bits were required per query, the experiment was repeated with μ=9.5 in order to quickly gather statistically significant results[2], where 104 queries were performed, yielding $\bar{n}$ = 3.9 and $\bar{m}$ = 6.3% with a total of 405 bits learned. No errors were observed in the learned bits in both cases. The results of the latter experiment are also summarized in the histograms in Figure 2, which compare the distribution of experimental results to simulation results. Finally, we also performed simulations based on state-of-the-art single photon detectors with high efficiency and low noise, such as in [12], showing that $\bar{n}$ = 4.4 and $\bar{m}$ = 0.96% can be achieved.

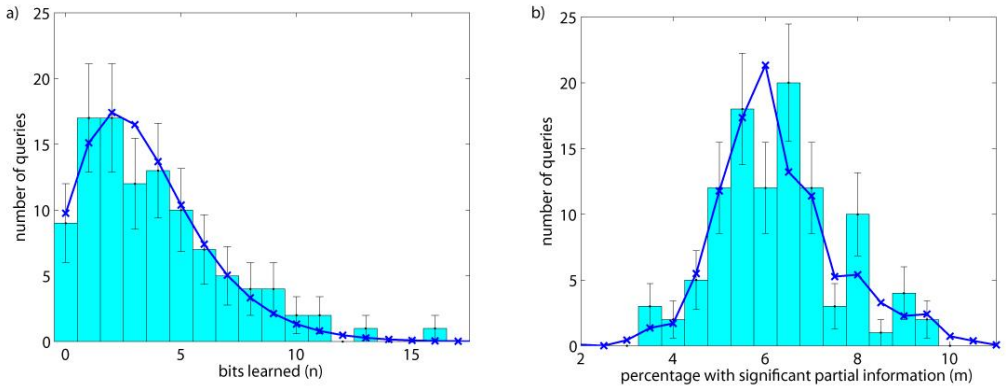

Figure 2 – Histogram of experimental (bars) and simulated (crosses) private query results for μ=9.5. **a)** Number of bits learned by Ursula (i.e. with an error rate less than 10^{-3}). **b)** Percentage of the database where Ursula has significant partial information (i.e. with an error rate less than 1/3).

We note that an information theoretic analysis of our protocol remains an open question. However, we have considered individual quantum attacks similar to those in [2,3]. Our analysis has shown that the error correction process can be used to improve the security of the protocol. In terms of user privacy, the information Ursula is given during error correction provides her additional opportunities to detect a cheating database. In terms of database privacy, the construction of the error correcting code can be adapted to limit the amount of information Ursula gains about the oblivious key. The latter property is particularly interesting when considering potential measurement strategies that a user could employ to gain additional information about the oblivious key. This is due to the fact a measurement strategy that is sufficiently simple to implement can be adopted as the honest procedure for Ursula, with the error correcting code adjusted to accommodate database security. Thus, our protocol has the potential to be adapted to remain secure as theoretical understanding of the protocol is improved.

References

[1] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. 100, 230502 (2008).
[2] M. Jakobi, et al., Phys. Rev. A 83, 022301, (2011).
[3] F. Gao, B. Liu, Q.-Y. Wen, and H. Chen, Opt. Express, Vol. 20, p. 17411-17420 (2012).
[4] H.-K. Lo, Phys. Rev. A 56, 1154 (1997).
[5] P. Chan, I. Lucio-Martinez, X.-F. Mo., C. Simon, and W. Tittel, arXiv:1303.0865 (2013).
[6] I. Lucio-Martinez, P. Chan, X.-F. Mo, S. Hosier, and W. Tittel, New J. Phys., 11, 095001 (2009).
[7] M.O. Rabin, Technical Report TR-81, Aiken Computation Lab, Harvard University (1981).
[8] M. Naor, and B. Pinkas, LNCS, Vol. 1976 (Springer, Berlin, 2000), p. 205.
[9] C. Blundo, P. D'Arco, A. De Santis, and D. Stinson, J. Cryptology, 20, 323-373.
[10] C. Erven, S. Wehner, N. Gigov, R. Laflamme, and G. Weihs, manuscript in preparation.
[11] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901, (2004).
[12] F. Marsili *et al.*, Nat. Photon. 7, 210-214 (2013).

[2] This duplicates the statistics of the μ=0.95 experiment, but is certainly not secure due to multi-photon emissions.