# Imperfect Oblivious Transfer Extended Abstract

Ryan Amiri,[1] Petros Wallden,[2] and Erika Andersson[1]

[1]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom**

[2]*LFCS, School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*

## I. INTRODUCTION

Oblivious transfer (OT) is one of the most widely used and fundamental primitives in cryptography. Its importance stems from the fact that it can be used as the foundation for secure two-party computations; with oblivious transfer, all secure two-party computations are possible [1],[2]. Unfortunately, it has been shown that unconditionally secure oblivious transfer is not possible, and that even quantum mechanics cannot help [3], [4]. In fact, the results of Lo actually go further, and show that it is impossible to securely evaluate *any* one sided two-party computation. Since then it has been an interesting and productive open question to determine the optimal security parameters achievable for some important two-party computations. In this paper we address the theoretical question "How close to ideal can unconditionally secure OT protocols be?" Our paper contains two main contributions:

1. For general 2-round OT protocols, we increase the lower bound on the minimum cheating probabilities achievable for Alice and Bob, i.e. we show that any OT protocol with at most two rounds of (classical or quantum) communication must have a cheating probability of at least 2/3. If the states in the final round of the (honest) protocol are pure, this bound is increased to 0.749. In the case that the final round contains pure states, we extend our 0.749 bound to general $N$-round OT protocols. We further conjecture that the 2/3 bound holds in general.

2. We present a new application of unambiguous state elimination (USE) measurements and motivate their use in quantum cryptography by presenting a protocol implementing OT relying on USE. The protocol improves on the best previously known protocol (in the sense that it decreases the participants cheating probabilities) and is fully implementable with current technology. The protocol is almost tight with the bounds proved in this paper.

Thus our paper aims to close the gap between the security that is theoretically possible for unconditionally secure OT, and the security in known OT protocols. For most two-party cryptographic primitives, this question of finding optimal security parameters has been definitively answered. For strong coin flipping, Kitaev [5] introduced the semi-definite programming formalism to show that the product of Alice's and Bob's cheating probabilities must be greater than $1/2$, implying the minimum cheating probability is at least $1/\sqrt{2}$. For weak coin flipping, it was shown by Mochon [6] that it is possible to achieve a cheating probability of $1/2 + \epsilon$ for any $\epsilon > 0$, and that this is optimal. Chailloux and Kerenidis [7] utilised the results on weak coin flipping to generate a protocol for strong coin flipping achieving the bound set by Kitaev. Lastly, for quantum bit commitment, Chailloux and Kerenidis [8] proved the minimum cheating probability is 0.739, and presented a protocol achieving this bias. Thus, for both bit commitment and coin flipping, the known bounds are tight with the known protocols.

For OT on the other hand, the situation is not so clear cut. Intuitively, OT is a two-party protocol where Alice inputs two bits, $x_0, x_1$, and Bob inputs a single bit, $b$. The protocol outputs $x_b$ to Bob with the guarantees that Alice does not know $b$, and that Bob does not know $x_{\overline{b}}$. A cheating Alice aims to find the value of $b$, while a cheating Bob aims to correctly guess both $x_0$, $x_1$. This can also be called 1-2 OT in order to distinguish it from the many different forms of OT which have arisen over the years. OT was first introduced informally by Wiesner as "a means for transmitting two messages, either but not both of which may be received" [9], [10], and subsequently formalised as 1-2 OT in [11]. In related work, Rabin [12] introduced a protocol (now called Rabin OT), which was later shown by Crépeau [13] to be equivalent to 1-2 OT. Various "weaker" variants of OT have also been proposed, most notably Generalised OT, XOR OT and Universal OT, but all have been shown to be equivalent to 1-2 OT [14], [15] in the sense that if it is possible to do one, it is possible to use this to implement the others. There is also work by Damgård, Fehr, Salvail and Schaffner [16] who define OT in a slightly different way, and who use binary

*Electronic address: ra2@hw.ac.uk

linear functions to characterise security. With these definitions (and their quantum counterparts), and by utilising the additional assumption of bounded quantum storage, the authors give a secure 1-2 OT protocol [17].

In this paper we consider stand-alone quantum protocols for 1-2 OT, and we are concerned only with information-theoretic security, with the definitions as stated by Chailloux and Kerenidis in [18]. Previously, [18] gave the best known lower bound for the minimum cheating probability of 1-2 OT protocols as

$$\max\{A_{OT}, B_{OT}\} \geq 0.5852 \tag{1}$$

as well as the best known protocol with $A_{OT} = B_{OT} = 0.75$.

In our paper, we consider Random OT (ROT), a protocol closely related to 1-2 OT. In ROT, Alice and Bob have no inputs, and in the honest case the protocol simply outputs $(x_0, x_1)$ to Alice, and $(b, x_b)$ to Bob, where $x_0$, $x_1$, $b$ are chosen uniformly at random from $\{0, 1\}$. This is known to be equivalent to the usual 1-2 OT in that, if there exists a protocol implementing ROT with cheating probabilities $A_{OT}, B_{OT}$, then this can be used to implement 1-2 OT with the same cheating probabilities, and vice versa. Our work improves both the lower bound on the minimum cheating probability, and gives a protocol which lowers Bob's cheating ability, thus bringing the known security bounds closer to the security of known protocols. We start by defining a completely general 2-round protocol for implementing ROT. By this we mean there are at most two rounds of (classical or quantum) communication between Alice and Bob, and the second round of communication can depend on the first. Given this, we use a constructive method to explore specific cheating strategies available to Alice and Bob which are always undetectable. We are able to express the cheating probabilities of both Alice and Bob in terms of the same parameter, $F$, which is the maximum fidelity between the different possible states sent back to Bob in the final round of the protocol. The cheating probability of a protocol is defined as $\max\{A_{OT}, B_{OT}\}$. By parametrising both $A_{OT}$ and $B_{OT}$ in terms of $F$, we are able to calculate the minimum cheating probability achievable by any protocol, and we find that for any 2-round ROT protocol we have

$$\max\{A_{OT}, B_{OT}\} \geq 2/3 \tag{2}$$

or, if the protocol returns pure states to Bob

$$\max\{A_{OT}, B_{OT}\} \geq 0.749 \tag{3}$$

We can extend this result to the general case of $N$-round protocols in the scenario in which the protocol returns pure states to Bob in the final round, in which case the above bound of 0.749 still holds. We conjecture that the bound of $2/3$ also holds in the most general setting.

Lastly, we explore a new application of USE measurements by presenting a protocol utilising USE which implements 1-2 OT with $A_{OT} = 0.75$ and $B_{OT} = 0.729$. We believe that this relatively new and unknown type of measurement is well suited to cryptography, and will likely find many applications. Unambiguous measurements give "perfect" information – in the sense that, given a successful measurement outcome, it is certain the information obtained is correct – but successful measurement outcomes do not give complete information, or do not occur with probability 1. To date, unambiguous measurements have been proposed in two forms: unambiguous state discrimination (USD), and unambiguous state elimination. A successful USD measurement gives full information on the identity of the quantum state being measured; a successful USE measurement allows the observer to rule out one or more of the possible quantum states with certainty. Intuitively, it seems that unambiguous measurements are well suited to cryptographic applications – their ability to provide "perfect yet partial" information on the states being sent is often exactly what is needed in cryptographic applications. More concretely, USD can be seen as very similar to Rabin OT, while USE measurements seem closely related to the more common 1-2 OT. Since OT plays a central role in secure two-party computations, it seems likely that unambiguous measurements could also play a major role in the developing field. By presenting a new application of USE measurements, we hope to encourage its use in future work.

---


[1] Goldrcich, Oded, and Ronen Vainish. "How to solve any protocol problem-an efficiency improvement." Advances in Cryptology - CRYPTO'87. Springer Berlin Heidelberg, 1987.

[2] Kilian, Joe. "Founding crytpography on oblivious transfer." Proceedings of the twentieth annual ACM symposium on Theory of computing. ACM, 1988.

[3] Mayers, Dominic. "Unconditionally secure quantum bit commitment is impossible." Physical review letters 78.17 (1997): 3414.

[4] Lo, Hoi-Kwong. "Insecurity of quantum secure computations." Physical Review A 56.2 (1997): 1154.

[5] Kitaev, Alexei. "Quantum coin-flipping." Talk at QIP (2003).

[6] Mochon, Carlos. “Quantum weak coin flipping with arbitrarily small bias.” arXiv preprint arXiv:0711.4114 (2007).
[7] Chailloux, André., and Iordanis Kerenidis. “Optimal quantum strong coin flipping.” Foundations of Computer Science, 2009. FOCS’09. 50th Annual IEEE Symposium on. IEEE, 2009.
[8] Chailloux, André, and Iordanis Kerenidis. “Optimal bounds for quantum bit commitment.” Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on. IEEE, 2011.
[9] S. Wiesner. “Conjugate coding.” SIGACT News, 15(1):78?88, 1983
[10] Wullschleger, Jürg. “Oblivious-transfer amplification.” Springer Berlin Heidelberg, 2007.
[11] Even, Shimon, Oded Goldreich, and Abraham Lempel. “A randomized protocol for signing contracts.” Communications of the ACM 28.6 (1985): 637-647.
[12] Rabin, Michael O. “How To Exchange Secrets with Oblivious Transfer.” IACR Cryptology ePrint Archive 2005 (2005): 187.
[13] Crépeau, Claude. “Equivalence between two flavours of oblivious transfers.” Advances in Cryptology - CRYPTO’87. Springer Berlin Heidelberg, 1987.
[14] Brassard, Gilles, and Claude Crépeau. “Oblivious transfers and privacy amplification.” Advances in Cryptology - EUROCRYPT’97. Springer Berlin Heidelberg, 1997.
[15] Brassard, Gilles, Claude Crépeau, and Stefan Wolf. “Oblivious transfers and privacy amplification.” Journal of Cryptology 16.4 (2003): 219-237.
[16] Schaffner, Christian. “Cryptography in the bounded-quantum-storage model.” arXiv preprint arXiv:0709.0289 (2007).
[17] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. “Cryptography in the bounded quantum-storage model.” In 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 449–458, 2005.
[18] **Chailloux, André, Iordanis Kerenidis, and Jamie Sikora. “Lower bounds for quantum oblivious transfer.” arXiv preprint arXiv:1007.1875v2 (2010).**