Reply to "Comment on Bit-string oblivious transfer based on quantum state computational distinguishability"

A. Souto P. Mateus P. Adão N. Paunković

SQIG—Instituto de Telecomunicações
DM - Instituto Superior Técnico, Universidade de Lisboa

Abstract

In the Comment [15] the author states that the proposed all-or-nothing Oblivious Transfer (OT) protocol [30] is insecure against a dishonest Alice and, as a corollary, derives an attack to Crépeau's construction of 1-out-of-2 OT [4]. The security criterion used in [15] is indeed stronger than the one used in the original paper [30]. However, we argue that the criterion used in [30] is in the spirit of the original idea of the OT protocol proposed by Rabin [27]. Moreover, a protocol that satisfies the criterion in [30] can be used to construct useful multi-party protocols. Finally, the protocol in [30] can be used, together with a secure bit commitment scheme, to construct a 1-out-of-2 OT secure against malicious Alice [3], achieving the security requirement considered in the Comment.

In the Comment [15], the author suggests that our protocol presented in [30] fails on two points: (i) it does not meet the security requirement of all-or-nothing OT protocol; (ii) it is unsuitable for serving as a building block for 1-out-of-2 oblivious transfer in the reduction scheme proposed by Crépeau [4]. In fact, our protocol is secure against the criterion defined in our paper, and while the security criterion proposed by the author is indeed a sensible one, we argue below that our definition is also both in the spirit of the original idea of Rabin OT [27] and a suitable one for applications (see for example [33, 13]). Regarding (ii), although one cannot achieve 1-out-of-2 OT secure against malicious Alice using Crépeau's reduction [4] (as suggested in the Comment), it is possible to do so following the ideas presented in [3].

(i) In the proposed attack, a cheating Alice sends a wrong "key" (wrong permutation π), and as a consequence Bob obviously does not get any message. This is however the same as not sending the message at all, i.e., sending a random message, say a completely mixed state. In the original idea of Rabin [27], and also expressed in [5, 6], the goal of Alice in OT protocols is to reveal secrets to Bob (the title of Rabin's paper is in fact "How to exchange secrets by oblivious transfer"). Moreover, *"Rabin OT in fact corresponds to a binary erasure channel*

with erasure probability 1/2" [7]: a channel in which Alice *does send* a message to Bob, which then might be either lost or delivered, without Alice being aware of what happened.

In the proposed attack, Alice is not giving Bob a chance to open the secret intended to be shared. If Alice does not want to share a secret, then there is not much one can do to prevent it and in that case she obviously knows that Bob did not receive it. But this cheating strategy does not fall within the scope of the OT protocol discussed in our paper, where it is assumed that a successful cheating strategy is one in which *only one* security criterion is violated, while the others are satisfied (a cheating Alice does want to know if Bob got the message, but still wants to give him the 50% chance of opening the message).

(ii) The proposed attack [15] to Crépeau's reduction scheme is indeed correct, but a *dishonest* Alice can perform a similar attack using any all-or-nothing OT that is secure according to the stronger criterion considered in the Comment [15]. Namely, she can simply (in Step (7) of the protocol below) flip a fair coin and, depending on its outcome, either proceed with executing Crépeau's reduction honestly, or send the same value in both messages (bits):

Protocol 1 (Cheating 1-out-of-2 OT)

(1) Alice and Bob agree on a security parameter s.

(2) Alice chooses at random Ks bits $r_1, r_2, ..., r_{Ks}$ for some constant K.

(3) Alice runs the secure all-or-nothing OT Ks times;

(4) Bob selects $U = \{i_1, i_2, \cdots, i_{\alpha_s}\}$ and $V = \{i_{\alpha_s+1}, i_{\alpha_s+2}, \cdots, i_{2\alpha_s}\}$, where $\alpha_s = \lceil \frac{Ks}{3} \rceil$ with $U \cap V = \emptyset$ and such that he knows r_{i_ℓ} for each $i_\ell \in U$.

(5) Bob sends $(X, Y) = (U, V)$ or $(X, Y) = (V, U)$ to Alice according to a random bit k.

(6) Alice computes $m_0 = \bigoplus_{x \in X} r_x$ and $m_1 = \bigoplus_{y \in Y} r_y$.

(7) Alice flips a fair coin and if the outcome is heads she chooses an index $i_c \notin X \cup Y$ and continues with Crépeau's protocol, that is, sends to Bob $b_j \oplus m_0$ and $b_{\overline{j}} \oplus m_1$ for a random bit j; Otherwise, she chooses $i_c \in X \cup Y$ and deviates from the protocol by sending to Bob $b_j \oplus m_0$ and $b_j \oplus m_1$, using the same *bit b_j for a random bit j;*

(8) Bob computes $\bigoplus_{u \in U} r_u \in \{m_0, m_1\}$ and uses it to get his secret bit b_k.

The above protocol has the same behavior, with respect to Alice's knowledge of the bit received by Bob, as the one proposed in the Comment [15]: in 50% of the cases, Alice knows *"which of the secret bit b_0 or b_1 is finally known by Bob"*. A cheating Alice can always choose not to send the intended messages (Step (7)) and there is nothing that Bob can do to prevent that behavior. Moreover,

in our Protocol 1 Alice can choose which bit value Bob will get, while in the "Protocol for 1-out-of-2 OT" from the Comment [15] Alice can only learn which of the two bit values Bob got. We see that both our all-or-nothing OT [30] and the 1-out-of-2 OT presented in the Comment (and in [4]) fail to satisfy the security criterion against malicious Alice for essentially the same reason: the impossibility to enforce Alice to send valid message(s).

On the other hand, one can still consider the so-called semi-honest scenario, in which Alice follows the protocol, but is allowed to perform additional computations using the data gathered while running the protocol (for details, see for example [12], Chapter 7, or [20], Chapter 13). In the context of a semi-honest Alice, the 1-out-of-2 OT based on our all-or-nothing OT (through the mentioned Crépeau's reduction [4]) can be used to achieve secure multi-party computation, either based on Yao's garbled circuits [33] (cited in the original paper as one of the main motivations for considering OT as a cryptographic primitive), or through the construction proposed in [13]. Assuming a semi-honest Alice in the mentioned constructions is indeed a reasonable one. For example, considering a semi-honest model is enough for hospitals that wish to share information. Also, the construction achieving multi-party computation proposed in [13] assumes that the majority of the agents are not malicious, which is indeed often the case (the majority of the population are honest people).

An all-or-nothing OT, secure against the criterion adopted in the Comment [15], can nevertheless be used to, following the same reduction [4], construct a stronger version of the 1-out-of-2 OT which is secure against malicious Alice. By stronger we mean that, instead of a random choice of received bit-value b_i, with $i \in \{0, 1\}$, it is Bob who decides which of the two bits to receive–he chooses $i \in \{0, 1\}$– while Alice is oblivious of this choice, and not just the value b_i of the received bit (a notion of 1-out-of-2 OT that is predominantly used in recent literature [9, 2, 8, 31, 11]). For details see Figure 1.

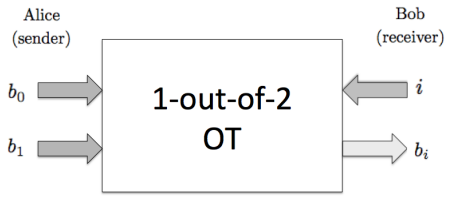

Figure 1: Alice sends two bits b_0 and b_1 labelled by 0 and 1, respectivelly. Bob inputs bit $i \in \{0, 1\}$ choosing to receive b_i as the output of the 1-out-of-2 OT protocol.

While the above construction does not work with our protocol, one can construct a 1-out-of-2 OT secure against malicious Alice using a semi-honest 1-out-of-2 OT (based on our all-or-nothing OT), together with a bit commitment scheme, as shown in [3].

In the following, we present the details of the reduction that uses our protocol as a black box, together with a bit commitment scheme, to construct a 1-out-of-2 OT that is secure against a malicious Alice (which includes the attack proposed in the Comment [15]). We strictly follow the idea presented in [3], which is a development over [16] and [14].

First, notice that our all-or-nothing OT protocol is secure against semi-honest Alice, and against malicious Bob. Therefore, the 1-out-of-2 OT obtained by Crepéau's construction [4] that uses our all-or-nothing OT protocol as a black box is consequently secure against semi-honest Alice and malicious Bob. From this protocol, using the OT-reversal scheme introduced in [32], one can construct a 1-out-of-2 OT protocol that is secure against malicious Alice (the sender) and semi-honest Bob (the receiver). Below, we schematically recall the OT-reversal protocol:

Protocol 2 (OT - Reversal)

Alice's input: *two bits s_0 and s_1.*

Bob's input: *a bit r.*

Black box: *A 1-out-of-2 OT protocol secure against semi-honest sender and malicious receiver.*

(1) Bob chooses bit ρ and computes $\rho \oplus r$. He performs the 1-out-of-2 OT to obliviously transfer bits b_0 and b_1, choosing either $b_0 = \rho$ and $b_1 = \rho \oplus r$, or $b_0 = \rho \oplus r$ and $b_1 = \rho$.

(2) Alice opens the bit $a = b_{s_0 \oplus s_1}$ and sends to Bob $\alpha = s_0 \oplus a$.

(3) Using α Bob computes the output $\rho \oplus \alpha$.

It is easy to see that Bob gets the desired bit s_r, i.e., $s_r = \rho \oplus \alpha$. Assuming, without the loss of generality, that Bob's choice was $b_0 = \rho$ and $b_1 = \rho \oplus r$, we have that:

- If $s_0 \oplus s_1 = 0$, then $s_0 = s_1$, and therefore Alice opens bit $a = b_0 = \rho$. She then sends to Bob bit $\alpha = s_0 \oplus a = s_0 \oplus \rho$. As a result, Bob's output is $\rho \oplus \alpha = \rho \oplus (s_0 \oplus \rho) = s_0 = s_1$.
- Otherwise, $s_0 \oplus s_1 = 1$ and thus $s_0 = \neg s_1$. Therefore Alice opens bit $a = b_1 = \rho \oplus r$ and sends to Bob bit $\alpha = s_0 \oplus a = s_0 \oplus (\rho \oplus r)$. As a result, Bob's output is $\rho \oplus \alpha = \rho \oplus (s_0 \oplus (\rho \oplus r)) = s_0 \oplus r$. In case $r = 0$, we have that Bob's output is $s_0 \oplus r = s_0$. Otherwise, if $r = 1$, the output is $s_0 \oplus r = \neg s_0 = s_1$.

We have started with a 1-out-of-2 OT secure against a semi-honest Alice (the sender) and malicious Bob (the receiver). Using the above OT-Reversal Protocol 2, we have turned it into 1-out-of-2 OT secure against malicious Alice and semi-honest Bob. To finally achieve 1-out-of-2 OT secure against both malicious agents, we need to improve the security against Bob (the receiver). This

is done by the construction introduced in [3], which in addition to semi-honest 1-out-of-2 OT uses bit commitment scheme as well (note that this construction improves the receiver's security level regardless of the sender's behavior, i.e., wether Alice follows the protocol or she is behaves maliciously). Below, we present in detail the construction from [3].

Protocol 3 (Comp)

Alice's input: *two bit-strings* s_0 *and* s_1.

Bob's input: *a random value* r.

Black boxes: OT *protocol secure against semi-honest receivers and a secure bit commitment scheme.*

Phase I: Random Tape Generation

1. *Bob choses* $2n$ *pairs* $(r_1^B, \tau_1^B), \ldots, (r_{2n}^B, \tau_{2n}^B)$ *of random bits* $r_i^B \in \{0,1\}$ *and strings* $\tau_i^B \in \{0,1\}^\ell$*, and using a secure bit commitment as a black box, commits to those strings that are sent to Alice.*[1]
2. *Alice generates* $2n$ *random strings* $(r_1^A, \tau_1^A), \ldots, (r_{2n}^A, \tau_{2n}^A)$ *where each* $r_i^A \in \{0,1\}$ *and* $\tau_i^A \in \{0,1\}^\ell$*, and send them to Bob.*
3. *Bob sets bit* $r_i = r_i^B \oplus r_i^A$ *and string* $\tau_i = \tau_i^B \oplus \tau_i^A$ *for all* $i = 1, \ldots, 2n$.

Phase II: Basic Execution

1. *Alice chooses* $2n$ *pairs of random pairs of bit-strings* (s_1^0, s_1^1), $\ldots$, (s_{2n}^0, s_{2n}^1) *as inputs of the OT protocol.*
2. *Alice and Bob engages in* $2n$ *executions of the* OT *protocol. In the* i*-th execution, Alice sends* (s_i^0, s_i^1) *and Bob's chooses to open the message with index* $r_i \in \{0,1\}$*, obtaining the string* $s_i^{r_i}$.

Phase III: Cut-and-choose

1. *Alice chooses a random* $q = (q_1, \ldots, q_n) \in \{0,1\}^n$*. The string* q *is used to define a set of indices* $Q \subset \{1, \ldots, 2n\}$*, with* $|Q| = n$*, such that* $Q = \{2j - q_j | j = 1, \ldots, n\}$.
2. *For every* $i \in Q$*, Bob opens the commitment* (r_i^B, τ_i^B) *to Alice.*
3. *Alice checks the validity of each commitment by checking the consistency of* τ_i^B *with Bob's message obtained in the execution of the* OT *protocol. If it is not consistent, Alice aborts and halts the protocol.*

Phase IV: Combiner

1. *For every* $j \notin Q$*, Bob computes* $\alpha_j = r \oplus r_j$ *and sends* $\{\alpha_j\}_{j \notin Q}$ *to Alice.*

[1] It is whordwhile mentioning that Bob is commiting to a randomn τ that he will use in each execution of the given OT protocol used as a black box. In the case of our original OT Protocol from [30] τ is in fact the permutation that Bob sends to Alice.

2. *Alice computes* $\sigma_0 = s_0 \oplus (\bigoplus_{j \notin Q} s_j^{\alpha_j})$ *and* $\sigma_1 = s_1 \oplus (\bigoplus_{j \notin Q} s_j^{1-\alpha_j})$. *She sends* (σ_0, σ_1) *to Bob;*

3. *Bob computes the outputs* $s_r = \sigma_r \oplus (\bigoplus_{j \notin Q} s_j^{r_j})$.

The above reduction relies on the use of secure bit commitment protocol. There exist a number of practical quantum bit commitment schemes that, providing certain technological limitations such as imperfect and/or bounded quantum memories, achieve secure bit commitment [1, 31, 29, 19, 26, 22]. Note that in the case of imperfect memories, no matter how small the (finite) noise is, the security achieved is based on the laws of physics, which is stronger than the computational security of the classical counterparts. Unlike the discrete states of classical bits, the states of quantum bits are continuous, therefore it is a viable assumption that, at least in the very long foreseeable future, no perfect quantum memories will exist (if ever). Moreover, there exist unconditionally secure bit commitment schemes, both classical [18] and quantum [17, 1], that use relativistic effects.

Finally, one could, instead of bit commitment, use bit-string commitment scheme, such as the one proposed by Kent [17]. In this case, one should take r_i^B to be strings instead of bits, and use the inner product (modulo 2) instead of xor when defining bits r_i in point 3 of Phase I. Note though that the equivalence between single-bit and genuine bit-string protocols, that exists in the classical realm, does not necessarily have to be valid in the quantum setting, which is the reason why Kent's result on bit-string commitment does not contradict the bit-commitment no-go theorems [21, 25, 10, 23]. Indeed, while no bit from a committed string in Kent's protocol could be changed with a non-negligible probability, this does not mean that a whole string cannot be altered with a non-negligible probability. The analysis of the degree of security of such implementation goes beyond the scope of this Reply.

OT protocols are security primitives, and as such, not useful *per se* (unless their application is outside the field of cryptography, for example when modeling the binary erasure channel). Only when used (as black boxes) in more complex reduction schemes, they serve the purpose in achieving relevant real-life security protocols. The above discussion suggests that, instead of talking of "(im)proper" security criteria in absolute terms, one should perhaps rather talk of "suitable" criteria *with respect to* certain applications and their requirements. While the attack proposed in the Comment [15] is indeed valid for the case of a "unverified" all-or-nothing OT [2], our protocol can: (i) in the context of semi-honest model be used to achieve useful secure multi-party computations, and (ii) together with a commitment scheme, achieve 1-out-of-2 OT secure against malicious Alice, a protocol that satisfies the stronger security criterion adopted in the Comment [15]. Finally, we note that this analysis applies to any all-or-nothing OT that fulfills our security criteria, in particular the one presented in [28, 24].

[2] By "unverified" we mean that it is not required for Bob to be able to verify if Alice indeed sent the message, as it is assumed that it is of her interest to do so, i.e., Alice is semi-honest agent.

Acknowledgements

We thank Jeroen van de Graaf for very helpful discussions regarding Oblivious Transfer. This work was partially supported, under the CV-Quantum internal project at IT, by FCT PEst-OE/EEI/LA0008/2013 and UID/EEA/50008/2013, namely via the FCT CaPri initiative. A.S. also acknowledges the FCT postdoc grant SFRH/BPD/76231/2011.

References

[1] N. Bouman, S. Fehr, C. Gonzalez-Guillen, and C. Schaffner. An all-but-one entropic uncertainty relation, and application to password-based identification. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 7582 of *Lecture Notes in Computer Science*, pages 29–44. Springer Berlin Heidelberg, 2013.

[2] G. Brassard, C. Crépeau, and S. Wolf. Oblivious transfers and privacy amplification. *Journal of Cryptology*, 16(4):219–237, 2003.

[3] SeungGeol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. Simple, black-box constructions of adaptively secure protocols. In Omer Reingold, editor, *Theory of Cryptography*, volume 5444 of *Lecture Notes in Computer Science*, pages 387–402. Springer Berlin Heidelberg, 2009.

[4] C. Crépeau. Equivalence between two flavours of oblivious transfers. In *CRYPTO*, pages 350–354, 1987.

[5] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *Foundations of Computer Science, 1988., 29th Annual Symposium on*, pages 42–52, Oct 1988.

[6] C. Crépeau and J. Kilian. Weakening security assumptions and oblivious transfer. In Shafi Goldwasser, editor, *Advances in Cryptology CRYPTO' 88*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7. Springer New York, 1990.

[7] C. Crépeau, K. Morozov, and S. Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In Carlo Blundo and Stelvio Cimato, editors, *Security in Communication Networks*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59. Springer Berlin Heidelberg, 2005.

[8] C. Crépeau and G. Savvides. Optimal reductions between oblivious transfers using interactive hashing. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 201–221. Springer Berlin Heidelberg, 2006.

[9] C. Crépeau, J. van de Graaf, and Alain. Tapp. Committed oblivious transfer and private multi-party computation. In Don Coppersmith, editor, *Advances in Cryptology*, volume 963 of *Lecture Notes in Computer Science*, pages 110–123. Springer Berlin Heidelberg, 1995.

[10] G. D'Ariano, D. Kretschmann, D. Schlingemann, and R. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Phys. Rev. A*, 76:032328, Sep 2007.

[11] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs. An experimental implementation of oblivious transfer in the noisy storage model. *Nat Commun*, 5, 03 2014.

[12] O. Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, New York, NY, USA, 2004.

[13] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 218–229, New York, NY, USA, 1987. ACM.

[14] I. Haitner. Semi-honest to malicious oblivious transfer: The black-box way. In *Proceedings of the 5th Conference on Theory of Cryptography*, TCC'08, pages 412–426, Berlin, Heidelberg, 2008. Springer-Verlag.

[15] G. He. Comment on "bit-string oblivious transfer based on quantum state computational distinguishability". *Phys. Rev. A.*, 2015.

[16] Y. Ishai, E. Kushilevitz, Y. Lindell, and E. Petrank. Black-box constructions for secure computation. In *Proceedings of the Thirty-eighth Annual ACM Symposium on Theory of Computing*, STOC '06, pages 99–108, New York, NY, USA, 2006. ACM.

[17] A. Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[18] A. Kent. Secure classical bit commitment using fixed capacity communication channels. *J. Cryptology*, 18(4):313–335, 2005.

[19] R. Koenig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[20] Y. Lindell. Foundations of cryptography 89-856, 2010. Lecture notes written for a graduate course in the foundations of cryptography at Bar-Ilan University, Israel. Available at http://u.cs.biu.ac.il/ lindell/89-856/complete-89-856.pdf (last access: July 20, 2015).

[21] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410–3413, Apr 1997.

[22] R. Loura, Á. Almeida, P. André, A. Pinto, P. Mateus, and N. Paunković. Noise and measurement errors in a practical two-state quantum bit commitment protocol. *Phys. Rev. A.*, 89:052336, May 2014.

[23] L. Magnin, F. Magniez, A. Leverrier, and N. Cerf. Strong no-go theorem for gaussian quantum bit commitment. *Phys. Rev. A*, 81:010302, Jan 2010.

[24] P. Mateus, N. Paunković, J. Rodrigues, and A. Souto. Enhancing privacy with quantum networks. In *Communications and Multimedia Security - 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings*, pages 147–153, 2014.

[25] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physycal Review Letters*, page 3414, 1997.

[26] N. Ng, S. Joshi, C. Ming, C. Kurtsiefer, and S. Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nature Communications*, 3:1326–, 2012.

[27] M. Rabin. How to exchange secrets by oblivious transfer, 1981. Tech. Memo TR-81, Aiken Computation Laboratory, Harvard University.

[28] J. Rodrigues, P. Mateus, N. Paunković, and A. Souto. Oblivious transfer based on single-qubit rotations, 2014. Last access: September 7, 2015).

[29] C. Schaffner, B. M. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Information & Computation*, 9(11):963–996, 2011.

[30] A. Souto, P. Mateus, P. Adão, and N. Paunković. Bit-string oblivious transfer based on quantum state computational distinguishability. *Phys. Rev. A*, 91:042306, Apr 2015.

[31] S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, Jun 2008.

[32] S. Wolf and J. Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232. Springer Berlin Heidelberg, 2006.

[33] A. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82, pages 160–164, Washington, DC, USA, 1982. IEEE Computer Society.