Coin-Flipping-based Quantum Oblivious Transfer

Minh-Dung Dang[1] and Patrick Bellot[1]
[1]*GET-ENST & LTCI-UMR 5141 CNRS, 46 rue Barrault, 75634 Paris Cedex 13, France*
e-mail: *{dang,bellot}@enst.fr*

Oblivious Transfer (OT), Bit Commitment (BC), and Coin Flipping (CF) are the central primitives to build Two-party Secure Computations [1]. It is well known that OT and BC are equivalent, while CF can be trivially obtained from BC [2]. Nevertheless, Kent set a particular model where CF is possible while quantum BC is not and concluded that "coin flipping is strictly weaker than bit commitment" [3]. We show however that quantum oblivious transfer can be built upon coin flipping.

First, we propose a Quantum Non-Orthogonal Coding (QNOC) scheme where the two possible values $0, 1$ of a classical bit are encoded by two nonorthogonal pure states $|\psi_0\rangle, |\psi_1\rangle$. With $\beta = 1 - |\langle\psi_0|\psi_1\rangle| < 1$, we denote the scheme as β-QNOC. Then, we define the standard measurement for optimally detecting the encoded bit:

$$\hat{E} = \left\{ \begin{array}{l} \hat{E}_0 = \frac{1}{2-\beta}(I_2 - \rho_1), \\ \hat{E}_1 = \frac{1}{2-\beta}(I_2 - \rho_0), \\ \hat{E}_2 = I_2 - \hat{E}_0 - \hat{E}_1 \end{array} \right\} \quad (1)$$

where $\rho_0 = |\psi_0\rangle\langle\psi_0|, \rho_1 = |\psi_1\rangle\langle\psi_1|$ and I_2 is the identity operator. Let Alice encode a bit b by the β-QNOC and send the qubit to Bob who can only detecting b with the maximal probability β by measuring the qubit with $\hat{E}$: Bob can infer b when $\hat{E}$ outputs 0 or 1. We denote the execution of such a Weak Oblivious Transfer (β-WOT) by a bit e where $e = 1$ ($p(e = 1) = \beta$) when the measurement of $\hat{E}$ gives 0 or 1. Of course, in this quantum β-WOT protocol, Alice can control the probability distribution of e, and Bob can violate the scheme by using any measurement to detect b.

Based on this β-WOT, we propose a coin-flipping-based quantum One-out-of two Oblivious Transfer (O-OT) protocol where Alice has two bits b_0, b_1 and sends them to Bob who is allowed choose to get only one of them. We denote c for Bob's choice.

Protocol 1. ***CF-based Quantum O-OT***$(b_0, b_1)(c)$

1. *Alice and Bob agree on security parameters β, K, L and M.*
2. *For i from 1 to $(M+1)K$, Alice picks a random bit m_i and sends to Bob a quantum states encoding m_i with our QNOC scheme.*
3. *Alice and Bob use coin flipping to generate K random numbers of $log((M+1)K)$ bits to select $U \subset \{1, ..., (M+1)K\}$ with $|U| = K$.*
4. *For $i \in T = \{1, .., (M+1)K\} \setminus U$, Alice unveils m_i to Bob; Bob verifies by measuring the i^{th} qubit with the projection $\{\rho_{m_i}, I_2 - \rho_{m_i}\}$.*
5. *For $i \in U$, Bob measures the i^{th} qubit to complete the i^{th} β-WOT run.*
6. *Bob randomly builds two disjoint index subsets $R_0, R_1 \subset U$ such that $|R_0| = |R_1| = L$, and $\forall i \in R_0$, the i^{th} WOT execution yields $e_i = 1$.*
7. *Bob sends the ordered pair (R_c, R_{1-c}) to Alice, according to his choice c.*
8. *Alice, receiving (R_c, R_{1-c}), sends back $(\hat{b}_0, \hat{b}_1)$ to Bob where $\hat{b}_0 = b_0 \oplus \bigoplus_{i \in R_c} m_i$, $\hat{b}_1 = b_1 \oplus \bigoplus_{i \in R_{1-c}} m_i$.*
9. *Bob deciphers $b_c = \hat{b}_c \oplus \bigoplus_{i \in R_0} m'_i$.*

We show that, with $\beta = 1 - \cos 75^o > 1/2$ and $L/K = 1/2$, we can choose a large value of K to secure the protocol on Bob's side. In fact, based on the proof of Bennett et al. [4], the accessible information about the parity of all m_i from the qubits can be made arbitrarily small by increasing K. Thus, the security of the parity of b_0, b_1 can be assumed.

Besides, if Alice violates the β-QNOC to control the probability distribution of β-WOT runs, then she must be detected by the tests in step 5 when M is large. The coin flipping is required to generate random bits in such a way that neither Alice nor Bob can cheat on the selection of U and T.

E-print: http://arxiv.org/abs/quant-ph/0605027.

References

[1] *Foundations of Cryptography - Volume II: Basic Applications*, Oded Goldreich, (Cambridge University Press, 2004).

[2] *Quantum Oblivious Transfer*, C. Crepeau, (Journal of Modern Physics, vol. 41, no. 12, pp. 2445 - 2454, 1994).

[3] *Coin Tossing is Strictly Weaker Than Bit Commitment*, Adrian Kent, (Phys. Rev. Lett., vol. 83, pp. 5382, 1999).

[4] *The parity bit in quantum cryptography*, Charles H. Bennett et al., (Phys. Rev. A, vol. 54, pp. 2675-2684, 1996).