Adaptive Versus Non-Adaptive Strategies in the Quantum Setting

Frédéric Dupuis[1], Serge Fehr[2], Philippe Lamontagne[3], and Louis Salvail[3]

[1] CWI, Amsterdam, The Netherlands
[2] Faculty of Informatics, Masaryk University, Brno, Czech Republic
[3] Université de Montréal (DIRO), Montréal, Canada

Adaptive Versus Non-Adaptive Attacks. We consider attacks on cryptographic schemes, and we compare adaptive versus non-adaptive strategies for the adversary. In our context, a strategy is adaptive if the adversary's action can depend on some auxiliary side information, and it is non-adaptive if the adversary has no access to any such side information. Non-adaptive strategies are typically much easier to analyze than adaptive strategies.

Adaptive strategies are clearly more powerful than non-adaptive ones, but this advantage is limited by the amount and quality of the side-information available to the attacker. In the classical case, this can be made precise by the following argument. If the side information consists of a classical n-bit string, then it is easy to see that adaptivity increases the adversary's winning probability (e.g., in opening a bit commitment to the wrong bit) by at most a factor of 2^n. Indeed, a particular non-adaptive strategy is to try to guess the n-bit side information and then apply the best adaptive strategy. Since the guess will be correct with probability at least 2^{-n}, it follows that $P^{\mathrm{NA}}_{\mathrm{succ}} \geq 2^{-n} P^{\mathrm{A}}_{\mathrm{succ}}$, and thus $P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^n P^{\mathrm{NA}}_{\mathrm{succ}}$, where $P^{\mathrm{A}}_{\mathrm{succ}}$ and $P^{\mathrm{NA}}_{\mathrm{succ}}$ respectively denote the optimal adaptive and non- adaptive winning probabilities. Even though there is an exponential loss, this is a very powerful relation between adaptive and non-adaptive strategies as it applies very generally, and it provides a non-trivial bound as long as we can control the size of the side information, and the non-adaptive winning probability is small enough.

Our Technical Result. In this work, we consider the case where the side information (and the cryptographic scheme as a whole) may be *quantum*. A natural question is whether the same (or a similar) relation holds between adaptive and non-adaptive quantum strategies. The quantum equivalent to guessing the side information would be to emulate the n-qubit quantum side information by the completely mixed state $\frac{\mathbb{I}_A}{2^n}$. Since it always holds that $\rho_{AB} \leq 2^{2n} \frac{\mathbb{I}_A}{2^n} \otimes \rho_B$, we immediately obtain a similar relation $P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^{2n} P^{\mathrm{NA}}_{\mathrm{succ}}$, but with an additional factor 2 in the exponent. The bound is tight for certain choices of ρ_{AB}, and thus this additional loss is unavoidable in general; this seems to pretty much answer the above question.

In this work, we show that this is actually not yet the end of the story. Our main technical result consists of a more refined treatment — and analysis — of the relation between adaptive and non-adaptive quantum strategies. We show that in a well-defined and rather general context, we can actually bound $P^{\mathrm{A}}_{\mathrm{succ}}$ as

$$P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^{I^{\mathrm{acc}}_{\max}(B;A)} P^{\mathrm{NA}}_{\mathrm{succ}} \ ,$$

where $I^{\mathrm{acc}}_{\max}(B;A)$ is a new (quantum) information measure that is upper bounded by the number of qubits of A. As such, we not only recover the classical relation $P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^n P^{\mathrm{NA}}_{\mathrm{succ}}$ in the considered context, but we actually improve on it.

In more detail, we consider an abstract "game", specified by an arbitrary bipartite quantum state ρ_{AB}, of which the adversary Alice and a challenger Bob hold the respective registers A and B, and by an arbitrary family $\{E^j\}_{j\in\mathcal{J}}$ of binary-outcome POVMs acting on register B. The game is played as follows: Alice chooses an index j, communicates it to Bob, and Bob measures his state B using the POVM $E^j = \{E^j_0, E^j_1\}$ specified by Alice. Alice wins the game if Bob's measurement outcome is 1. In the adaptive version of the game, Alice can choose the index j by performing a measurement on A; in the non-adaptive version, she has to decide upon j without resorting to A. As we will see, this game covers a large class of quantum cryptographic schemes, where Bob's binary measurement outcome specifies whether Alice succeeded in breaking the scheme.

Our main result shows that in any such game it holds that $P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^n P^{\mathrm{NA}}_{\mathrm{succ}}$ where $n = \mathrm{H}_0(A)$, i.e., the number of qubits of A. Actually, as already mentioned, we show a more general and stronger bound $P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^{I^{\mathrm{acc}}_{\max}(B;A)} P^{\mathrm{NA}}_{\mathrm{succ}}$ that also applies if we have no bound on the number of qubits of A, but we have some control over its "information content" $I^{\mathrm{acc}}_{\max}(B;A)$, which is a new information measure that we introduce and show to be upper bounded by $\mathrm{H}_0(A)$.

To give a first indication of the power of our result, we observe that it easily provides a lower-bound on the quantity, *or quality*, of entanglement (as measured by $I^{\mathrm{acc}}_{\max}(B;A)$ and as a function of the scheme) a dishonest committer needs to carry out the standard attack [5] on a quantum bit commitment scheme. Let Alice be the committer and Bob the receiver in a bit commitment scheme in which the opening phase consists of Alice announcing a classical string j and Bob applying a verification described by POVM $\{E^j_{\mathrm{accept}}, E^j_{\mathrm{reject}}\}$. In the standard attack, Alice always commits to 0 while purifying her actions and applies an operation on her register if she wants to change her commitment to 1. If we let ρ_{AB} be the state of Bob's register B that corresponds to a commitment to 0, then the probability that a memoryless Alice successfully changes her commitment to 1 is $P^{\mathrm{NA}}_{\mathrm{succ}} = \max_j \mathrm{tr}(E^j_{\mathrm{accept}} \rho_{AB})$ where the maximum is over all j that open 1. If Alice holds a register A entangled with B, our main result implies that $I^{\mathrm{acc}}_{\max}(B;A)$ must be proportional to $-\log P^{\mathrm{NA}}_{\mathrm{succ}}$ for Alice to have a constant probability of changing her commitment.

But the real potential lies in the observation that adaptivity is notoriously difficult to handle in the analysis of cryptographic protocols, and as such our result provides a very powerful tool: as long as we have enough control over the side information, it is sufficient to restrict ourselves to non-adaptive attacks.

Applications. We demonstrate the usefulness of this methodology by proving the security of two commitment schemes. In both examples, the fact that the adversary holds quantum side information obstructs a direct analysis of the scheme, and we circumvent it by analyzing a non-adaptive version and applying our general result.

One-bit cut-and-choose is universal for two-party computation. As a first example, we propose and prove secure a quantum bit commitment scheme that uses an ideal *1-bit cut-and-choose* primitive 1CC as a black box. Since bit commitment (BC) implies oblivious transfer (OT) in the quantum setting [1, 3, 6], and oblivious transfer is universal for two-party computation, this implies the universality of 1CC and thus completes the zero/xor/one law proposed in [4]. Indeed, it was shown in [4] that in the information-theoretic quantum setting, every primitive is either trivial (zero), universal (one), or can be used to implement an XOR — *except* there was one missing piece in their characterization: it excluded 1CC (and any primitive that implies 1CC but not 2CC). How 1CC fits into the landscape was left as an open problem in [4], and we resolve it here.

The BCJL bit commitment scheme is secure in (a variant of) the bounded quantum storage model. As a second application, we consider a general class of non-interactive commitment schemes and we show that for any such scheme, security against an adversary with no quantum memory *at all* implies security in a slightly strengthened version of the standard bounded quantum storage model[4], with a corresponding loss in the error parameter.[5]

As a concrete example scheme, we consider the classic BCJL scheme that was proposed in 1993 by Brassard *et al.* [2] as a candidate for an unconditionally-secure scheme — back when this was thought to be possible — but until now has resisted any rigorous *positive* security analysis. Our methodology of relating adaptive to non-adaptive security allows us to prove it secure in (a variant of) the bounded quantum storage model.

[4] Beyond bounding the adversary's quantum memory, we also restrict its measurements to be projective; this can be justified by the fact that to actually implement a non-projective measurement, additional quantum memory is needed.

[5] We have already shown above how to argue for the standard attack [5] against quantum bit commitment schemes; taking care of *arbitrary* attacks is more involved.

References

1. Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer, 1991.
2. G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science*, pages 362–371, 1993.
3. Claude Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.
4. Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas. Feasibility and completeness of cryptographic tasks in the quantum world. In Amit Sahai, editor, *Theory of Cryptography*, volume 7785 of *Lecture Notes in Computer Science*, pages 281–296. Springer Berlin Heidelberg, 2013.
5. Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, Apr 1997.
6. Dominique Unruh. Universally composable quantum multi-party computation. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 486–505. Springer Berlin Heidelberg, 2010.