On the Security of Symmetric Key Ciphers against Quantum Adversaries

M. Kaplan[*] G. Leurent[†] A. Leverrier[†] M. Naya-Plasencia[†]

Abstract

Our trust in specific symmetric primitives relies on their ability to resist all known cryptanalytic attacks. Therefore, cryptanalysis is the only proper way to evaluate their security. In this paper, we investigate the behavior of symmetric primitives in the quantum world. This requires to extend the toolkit of symmetric cryptanalysis to the quantum setting, eventually including new attacks.

While running Grover's search algorithm on a quantum computer brings a quadratic speedup for brute-force attacks, we show that the situation is more subtle when considering differential cryptanalysis. We consider two variants of differential cryptanalysis and apply them to concrete implementations of block ciphers. From these applications, we conclude that increasing the key length may not always be the best strategy to increase the security, and that the best quantum attack is not always the same as the best classical attack.

1 Introduction

Large quantum computers would have huge consequences in cryptography. For instance, Shor's factoring algorithm [Sho97] makes asymmetric primitives such as RSA totally insecure in a post-quantum world. Current pre-quantum long-term secrets would also be at risk. Even if quantum computers are unlikely to become widely available in near future, the cryptographic community has decided to worry about it and to study its impact.

In this paper, we focus on symmetric cryptography. Symmetric primitives also suffer from a reduced security in the quantum world, but this security reduction is much less drastic than for many asymmetric primitives. So far, the main quantum attack on symmetric algorithms follows from Grover's algorithm [Gro96] for searching an unsorted database of size N in $O(N^{1/2})$ time. It can be applied to any generic exhaustive key search, but merely offers a quadratic speed-up compared to a classical attack. Therefore, the consensus is that key lengths should be doubled in order to restore the security.

Doubling the key length is a good heuristic, but a more accurate analysis is definitely called for. Most of the crypto-systems used in practice rely in part on symmetric ciphers but our current understanding of their security against quantum adversaries is very incomplete. In order to devise alternatives to post-quantum cryptography, an evaluation of the security of symmetric ciphers is deeply needed.

The security of symmetric primitives relies heavily on cryptanalysis, and it is crucial to evaluate how the availability of quantum computing affects it. In particular, we must evaluate the toolbox of symmetric cryptanalysis in a quantum setting in order to understand the security of symmetric algorithms against quantum adversaries. In this paper, we consider this issue, and evaluate the advantage an adversary gets from performing some attacks on symmetric ciphers with a quantum computer.

Our results. We study block cipher encryption, where the cipher is a collection of permutations of the block space indexed by keys. The goal for the attacker is to recover a secret key k given a number of pairs of plaintext and ciphertext encoded with k. The attacks we consider are two variants of differential cryptanalysis: simple differential and truncated differential cryptanalysis. We also consider two different security models. In the *semi-quantum* model, the adversary collects data classically and only uses quantum computing in the analysis phase. In the *fully-quantum* model where the adversary can collect the data quantum-mechanically. Similar models have been considered in [BDF$^+$11, DFNS11, BZ13].

We find the following non-obvious results: **(i)**Differential cryptanalysis usually offers a *quadratic gain* in the fully quantum model over the classical model. **(ii)** Truncated differential cryptanalysis, however, offers *smaller gains* in the fully quantum model. From these results, we conclude that the

[*]LTCI, Télécom ParisTech, 23 avenue dItalie, 75214 Paris CEDEX 13, France

[†]Inria, EPI SECRET, Le Chesnay, France

best attacks may not be the same for classical and quantum adversaries. **(iii)** In the semi-quantum model, cryptanalytic attacks might offer *little gain* over the classical model when the key-length is the same as the block length (*e.g.* AES-128). **(iv)** The gain of cryptanalytic attacks in the semi-quantum model can be quite significant (*similar to the fully quantum model*) when the key length is longer (e.g., AES-256). Theses results show that increasing the key length may not always lead to improving the security of the considered cryptosystem.

In the quantum setting, the equivalent to the classical brute-force attack in the quantum world is to search through the key space using a Grover's search algorithm. Our goal is to devise quantum attacks that might be a threat to symmetric primitives by having a smaller complexity than the generic quantum exhaustive search.

2 Differential Cryptanalysis

Simple Differential attacks. Differential cryptanalysis was introduced in [BS90] by Biham and Shamir. They exploit the fact that there exists an input difference δ_{in} and an output difference δ_{out} to a cipher E such that $h_S = -\log \Pr_x[E(x \oplus \delta_{\text{in}}) = E(x) \oplus \delta_{\text{out}}] < n$. This non-random behaviour can already be used to attack a cryptosystem by *distinguishing* it from a random function. The classical and quantum simple differential distinguishers have time complexity $T_{\text{C}}^{\text{s. dist.}} = 2^{h_S+1}$ and $T_{\text{FQ}}^{\text{s. dist.}} = 2^{h_S/2+1}$, respectively. Since the most expensive part of the attack is collecting the data, the distinguisher is meaningful only in the fully-quantum model.

We assume that the cipher is an iterated design and that such a distinguisher exists on R rounds of a cipher, we can transform the attack into a key recovery on more rounds by adding some rounds at the end or beginning of the cipher. This is called a *last-rounds attack*, and allows to attack more rounds than the distinguisher, typically one or two, depending on the cipher.

For a pair that generates the difference δ_{out} after R rounds, we denote by $\mathcal{D}_{\text{fin}}$ the set of possible differences generated in the output after the final round, the size of this set by $2^{\Delta_{\text{fin}}} = |\mathcal{D}_{\text{fin}}|$. Let $2^{-h_{\text{out}}}$ denote the probability of generating the difference δ_{out} from a difference in $\mathcal{D}_{\text{fin}}$ when computing the last r_{out} rounds in the backward direction, and by k_{out} the number of key bits involved in these rounds. The last round simple differential attack then has time complexity

$$\begin{aligned}
T_{\text{C}}^{\text{s. att.}} &= 2^{h_S+1} && +2^{h_S+\Delta_{\text{fin}}-n}\Big(C_{k_{\text{out}}} + 2^{k-h_{\text{out}}}\Big)\\
T_{\text{SQ}}^{\text{s. att.}} &= 2^{h_S+1} && +2^{(h_S+\Delta_{\text{fin}}-n)/2}\Big(C^*_{k_{out}} + 2^{(k-h_{\text{out}})/2}\Big)\\
T_{\text{FQ}}^{\text{s. att.}} &= 2^{h_S/2+1} && +2^{(h_S+\Delta_{\text{fin}}-n)/2}\Big(C^*_{k_{out}} + 2^{(k-h_{\text{out}})/2}\Big)
\end{aligned}$$

in the classical, semi-quantum and fully-quantum model, respectively. Here, $C_{k_{\text{out}}}$ (resp. $C^*_{k_{\text{out}}}$) denotes the average time of generating the partial keys of length k_{out}, on a classical (resp. quantum) computer.

Truncated differential attacks. Truncated differential cryptanalysis was introduced by Knudsen [Knu94] in 94. Instead of fixed input and output differences, it considers sets of differences. We assume that we are given two sets $\mathcal{D}_{\text{in}}$ and $\mathcal{D}_{\text{out}}$ of input and output differences such that the probability of generating a difference in $\mathcal{D}_{\text{out}}$ from one in $\mathcal{D}_{\text{in}}$ is 2^{-h_T}. We further consider that $\mathcal{D}_{\text{in}}$ and $\mathcal{D}_{\text{out}}$ are vector spaces.

The advantage of truncated differentials is that they allow the use of structures, i.e., sets of plaintext values that can be combined into input pairs with a difference in $\mathcal{D}_{\text{in}}$ in many different ways: one can generate $2^{2\Delta_{\text{in}}-1}$ pairs using a structure of size $2^{\Delta_{\text{in}}}$. This reduces the data complexity with respect to simple differential attacks. The attack then amounts to searching for collisions into structures.

For the truncated differential distinguisher, we get time complexities $T_{\text{C}}^{\text{tr. dist.}} = \max\{2^{(h_T+1)/2}, 2^{h_T-\Delta_{\text{in}}+1}\}$ and $T_{\text{FQ}}^{\text{tr. dist.}} = \max\big\{2^{(h_T+1)/3}, 2^{(h_T+1)/2-\Delta_{\text{in}}/3}\big\}$ in the classical and fully-quantum model, respectively. The truncated differential last-rounds attacks have time complexites

$$\begin{aligned}
T_{\text{C}}^{\text{tr. att.}} &= \max\big\{2^{(h_T+1)/2}, 2^{h_T-\Delta_{\text{in}}+1}\big\} && + 2^{h_T+\Delta_{\text{fin}}-n} && \Big(C_{k_{\text{out}}} + 2^{k-h_{\text{out}}}\Big)\\
T_{\text{SQ}}^{\text{tr. att.}} &= \max\big\{2^{(h_T+1)/2}, 2^{h_T-\Delta_{\text{in}}+1}\big\} && + 2^{(h_T+\Delta_{\text{fin}}-n)/2} && \Big(C^*_{k_{out}} + 2^{(k-h_{\text{out}})/2}\Big)\\
T_{\text{FQ}}^{\text{tr. att.}} &= \max\big\{2^{h_T/2}, 2^{h_T-\Delta_{\text{in}}+1}\big\}2^{-(n-\Delta_{\text{fin}})/6} && + 2^{(h_T-n+\Delta_{\text{fin}})/2} && \Big(C^*_{k_{\text{out}}} + 2^{(k-k_{\text{out}})/2}\Big),
\end{aligned}$$

in the classical, semi-quantum and fully-quantum model, respectively.

3 Discussion and applications

The first clear conclusion we draw from our results is that truncated attacks are in general less accelerated than simple differential ones. This has two main interesting consequences. Paradoxically, having smaller keys implies smaller security gains over the best generic attacks. This conclusion is particularly interesting. The obvious security measure for resisting quantum generic attacks is to use longer keys. We show here that with this strategy, it is likely that if a classical attack breaks the cryptosystem, then its quantized version also breaks it.

Another conclusion is that a truncated differential attack might be the best known attack in the classical world, while the simple differential might become the best in the quantum world. Therefore, just quantizing the best known attack does not ensure obtaining the best possible attack in the post-quantum world, which emphasizes the importance of studying quantum symmetric cryptanalysis. Finally, we apply our attacks to concrete examples.

LAC. Applying our formulas, the best attack in the classical setting is a truncated differential attack (with complexity $2^{60.9}$ instead of $2^{62.5}$), while the best attack in the quantum setting is a simple differential attack (with complexity $2^{31.75}$ instead of $2^{33.4}$). Moreover, the quantum truncated differential attack is actually less efficient than a generic attack using Grover's algorithm.

KLEIN-64. We consider the truncated the attack from [LNP14], which gives the following parameters: $h_T = 69.5$, $\Delta_{\text{in}} = 16$, $\Delta_{\text{fin}} = 32$, $k = 64$, $k_{\text{out}} = 32$, $n = 64$, $C_{k_{\text{out}}} = 2^{20}$ and $h_{\text{out}} = 45$. In this case, we can recover the time and data complexities from the original result as $D = 2^{54.5}$ and $T = 2^{54.5} + 2^{57.5} + 2^{56.5} = 2^{58.2}$, which is considerably faster than exhaustive search (2^{64}), breaking in consequence the cipher.

In the quantum scenario, the generic exhaustive search has complexity 2^{32}, and therefore we need to compare the attacks with this value. In both the semi-quantum case and the fully quantum model, the first term becomes larger than 2^{32}, thus the attack does not work. We have seen here an example of a primitive broken in the classical world, but remaining secure in the quantum one, for both models.

KLEIN-96. Here we consider the attack of type III given in [LNP14], as it is the only one with data complexity lower than 2^{48}, and therefore the only possible candidate for providing also an attack in the semi-quantum model.

The parameters of this classical attack are: $h_T = 78$, $\Delta_{\text{in}} = 32$, $\Delta_{\text{fin}} = 32$, $k_{\text{out}} = 48$, $n = 64$, $C_{k_{\text{out}}} = 2^{30}$ and $h_{\text{out}} = 52$. We compute and obtain the same complexities as the original results in time and data: $D = 2^{47}$ and $T = 2^{47} + 2^{46+30} + 2^{90}$.

When quantizing this attack, we have to compare the complexities with $2^{96/2} = 2^{48}$. In the semi quantum model we obtain $2^{47} + 2^{23+23} + 2^{45} = 2^{47.7}$, which is lower that 2^{48}, so the attack still works. In the fully-quantum model, we can, additionally accelerate the first term by a factor $2^{-(n-\Delta_{out})/6} = 2^{-5.33}$, and the final complexity stays a bit lower than in the semi-quantum model: 2^{46}.

Full version. The full version of the paper is not yet available, but can be found at the address `http://perso.telecom-paristech.fr/~kaplan/papers/qsym.pdf`

References

[BDF+11] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *Advances in Cryptology – ASIACRYPT*, 2011.

[BS90] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In *Advances in Cryptology - CRYPTO*, 1990.

[BZ13] D. Boneh and M. Zhandry. Quantum-secure message authentication codes. In *Advances in Cryptology – EUROCRYPT*, 2013.

[DFNS11] I. Damgaard, J. Funder, J. B. Nielsen, and L. Salvail. Superposition attacks on cryptographic protocols. *arXiv preprint arXiv:1108.6313*, 2011.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *ACM Symposium on the Theory of Computing 1996*, pages 212–219. ACM, 1996.

[Knu94] L. R. Knudsen. Truncated and higher order differentials. In *Fast Software Encryption: Second International Workshop*, 1994.

[LNP14] V. Lallemand and M. Naya-Plasencia. Cryptanalysis of KLEIN. In *FSE 2014*, Lecture Notes in Computer Science. Springer, 2014.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.