A Short Review: Quantum Immunity of KSI

Ritobroto Maitra
Intern: Guardtime

Week 1 - Report

1 Background

The Keyless Signature Infrastructure developed by Guardtime brings in a new paradigm that has several technical and practical advantages against the traditional PKI. We need to, however, work on the provable quantum security of KSI. The best outcome will be to provide a full-scale mathematically modelled reasoning and proof, rather than the current reasoning that *intuitively* feels correct.

2 Major Claims

Note: I am using notation that is either in the anonymous submission paper, or is widely accepted and known in cryptographic literature.

The three main claims that we need to back up are as follows:

- Known quantum collision finders are no faster than classical ones for a given hash function.
- If A_1 and A_2 are both quantum computations using classical inputs, the proofs still remain valid.
- If the advice a is quantum information, it seems *reasonable* to assume *practical* security.

3 Observations and Inputs

Let us first deal with the apparently most straightforward claim - that quantum collision finders for hash functoins are no faster than classical ones. Several applications of quantum algorithms to hash functions exist in literature, including applications of Grover's algorithm [Gro96] that allows us to sieve through an unsorted list in $O(\sqrt{n})$ time rather than the classical linear case. The best known work in this regard is the work by Brassard et al [Bra97] and Boyer et al [Boy96].

More recent work by Daniel Bernstein, has shown that these attacks, although they bring down the immunity of an n-bit hash function to $2^{\frac{n}{3}}$ from $2^{\frac{n}{2}}$, they are not very effective in a real-world scenario in terms of building hardware and actually executing the attack [Dan09]. Moreover, as observed before, this

particular attack can be easily circumvented by using a hash function with a size of $1.5n$-bit output, or say, using SHA-384 or SHA-512 instead of SHA-256.

However, this in itself does not prove the quantum security of hash functions. All classical hash functions are birthday-secure, and no attack actually attempts to breach that bound. All popular attacks - including rebound attacks, joint local-collision analysis, differential cryptanalysis, boomerang attacks, linear and algebraic cryptanalysis - are much better than the birthday bound, and these have developed through independent research. So, these functions are secure in a sense that we are not really in a position to say anything about them - very little or no work has been done on dedicated quantum attacks against hash functions. A lower bound was proposed by Aaronson on query complexity at $\Omega(n^{\frac{1}{5}})$ [Aar02] which was improved to $\Omega(n^{\frac{1}{3}})$ by Shi [Shi04].

So, to be quantum-secure at this point of time to avoid collisions, at least 384 bits are required to be future-proof for some years. If only pre-image resistance is required, then we may still consider 256 bits. The conclusion is open - fast, dedicated quantum cryptanalytic techniques are unknown and have not seen intensive research (with the exception of Shor's algorithm), unlike certain areas of classical cryptanalysis - for example, work on DES, AES or MD4 and MD5. Unless we see a lot of academic interest generating new literature on the topic, we can't really say anything for sure.

The other alternative is to consider functions that are provably-secure. But these, most of the time, have severe drawbacks that make them unsuitable for use in practical scenarios. One such example is SWIFFT, based on fast Fourier transforms. Although it can be reduced to a strong mathematical basis, it is not pseudorandom at all, and in fact has the property $f(x_1) + f(x_2) = f(x_1 + x_2)$ which can be massively exploited in our applications. The same holds true for several coding-theory based functions [NCB11].

On migrating our security proofs to the quantum setting, we have to deal with two cases separately: when the information available is classical and the attacker himself has access to quantum algorithms and quantum computers that are sufficiently powerful; and when the information itself is quantum.

For the first case, a formal proof looks likely. This can be done using the frameworks provided in the work of Luis Carlos Coronado Garcıa [Gar06] where he carefully analyzes the security and efficiency of the Merkle signature scheme, and the work of Fang Song [FAN13] where he provides an efficient scheme to "move" the classical proof of a system using games to a quantum setting, using one of the two possibilities of preserving the game or updating the game. Studying the frameworks and using the existing security proofs of KSI in the public domain, there is a fair possibility that we can provide a formal proof of security of KSI in the face of a quantum adversary.

For a fully quantum digital signature scheme that takes classical information but outputs a quantum state is a relatively new domain that has seen little cryptanalysis or efforts to prove or disprove security. One of the relatively better known works on quantum hashing is by Ablayev and Vasiliyev [FAV13]. So, providing a formal proof on the second case should ideally be done after we are done with the first case - this will also allow me sufficient time to grasp concepts that might be instrumental in proving the second one.

4 Intended Future Work

As of now, having done a survey of the publications in public domain about quantum security of hash-based schemes, and on provable security of schemes in the quantum setting where the adversary has access to a powerful quantum computer and it can be assumed that he can manipulate known quantum algorithms to his advantage, it would be prudent to try and provide a formal proof in the above mentioned setting for KSI. For this, we can use the works referenced in the previous section to first assume a "reasonable" security of the underlying hash function, and then move on to analyze the protocol itself. The work will be, on the lines of Fang Song's research, to scrutinize each aspect of the infrastructure, and look at existing classical security proofs. Then, we decide if that particular "game" should remain exactly the same in a quantum setting (*game-preserved*) or if it should be updated, and after updating if we can say that the adversary has no significant advantage over the protocol (*game-updated*). This series of new and migrated games will give us a complete formal proof.

References

[Gro96] A fast quantum mechanical algorithm for database search, Lov K. Grover

[Bra97] Quantum Algorithm for the Collision Problem, Gilles Brassard, et al.

[Boy96] Tight Bounds on Quantum Searching, M. Boyer, et al.

[Dan09] Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?, Daniel J. Bernstein

[Shi04] Quantum lower bounds for the collision and the element distinctness problems, Scott Aaronson and Yaoyun Shi

[Aar02] Quantum lower bound for the collision problem, Scott Aaronson

[NCB11] Improving the efficiency of Generalized Birthday Attacks against certain structured cryptosystems, Robert Niebuhr, Pierre-Louis Cayrel, and Johannes Buchmann.

[Gar06] On the security and the efficiency of the Merkle signature scheme, Luis Carlos Coronado Garcıa

[FAN13] A Note on Quantum Security for Post-Quantum Cryptography, Fang Song.

[FAV13] Quantum Hashing, Farid Ablayev, Alexander Vasiliev.