A Short Review: Quantum Immunity of KSI

Ritobroto Maitra
Intern: Guardtime

Draft Report

1

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 migrate the security proofs to the quantum setting.

Note: In this draft version, all definitions and related terminologies are borrowed from the original paper on the security proof of the BLT scheme. In the final version, for the sake of completeness, we will include them for a complete reading.

This draft is merely for walking through the essential ideas of the migration, the full version (which is ready, pending comments on this one) includes all the extra material such as theorems and references of the proofs of those theorems from relevant papers.

Assume that the adversary A_1 has committed the hash value r as well as the advice a. We make no assumption about the nature of a at this stage. Assume that A_2 is able to come up with a forgery x‘.

In this case, walking step-by-step through the original proof, let us see if we can migrate or preserve the conditions.

[All work referenced after this, if not mentioned otherwise, is from *Security Proofs for the BLT Signature Scheme, Ahto Buldas, Risto Laanoja, and Ahto Truu*].

Theorem 3 is respectful, which means that in a quantum game, there is no need to find if there exists an interpreter to translate it. This is straight-forward, since this follows a balanced structure.

The same follows for the entire oracle model used. However, we must make an important observation here - there is nothing, theoretically, preventing an adversary with full control from performing queries in quantum superposition. However, even using the quantum oracle model, we can use the following reduction:

Let us say that our construction involving R is value-dominating. This is easy to prove since $w_{G^e}(T(A)) = w_{G^e}(T(B))$ whenever $w_{G^i}(T(A)) = w_{G^i}(T(B))$. In this case, however, we can also use the *effective* reduction, since $alpha_{G^e}(T(A)) \geq w_{G^i}(T(A))$.

For the next one, however, we can *not* use game-preserving reductions anymore. Let us, instead, use a translator T or a quantum transformer that uses a quantum game G‘ instead. From the underlying assumptions of security, we have an (A, B)-consistent reduction. Also, we can use in this context the property that $alpha_{G`e}(T`(A`)) \geq w_{G`i}(T`(A`))$. This directly implies that with this reduction, we can apply a game-updating condition. Although this reduction is non-trivial, it can be verified using the proof by Katz et al, (but using the respectful reduction instead of the consistent-successive reduction used in the original proof).

Given this, it is now a trivial task to propose the migration of the proof in its entirety, by only proving that there exists a translator - which also stems as a by-product of the previous transformation, as a value-dominating, extendible and straight-line transformation.

The novelty of this entire proof is in that we do not have to a lot of "re-working" of the original proof - we can just use the original assumptions and the original games with the reductions and updates. It could have been done in a lot more trivially but in a rather tedious way by re-working the entire path, but in my opinion this is more useful since it keeps intact all the other parts of the infrastructure.

Q.E.D.