Analysis - "Post-Quantum Security of Fiat-Shamir" by Dominic Unruh

Bruno Produkt
Institute of Computer Science
University of Tartu
produit@ut.ee

December 19, 2017

Abstract

This document is an analysis of the paper [Unr17]. The purpose of this document is to resume and simplify the paper in order to make it easy to understand for a standard computer science student. It is done in the context of the cryptography seminar at the University of Tartu.

Contents

1 Introduction .......................................................... 2
2 Context .............................................................. 2
3 Definitions ........................................................... 2
   3.1 Random Oracle model ........................................... 2
   3.2 Completeness .................................................. 3
   3.3 Soundness ...................................................... 3
   3.4 Proof of knowledge ............................................ 4
   3.5 (Honest-Verifier) Zero-knowledge proof of knowledge .... 4
   3.6 Σ-Protocol ..................................................... 5
   3.7 Non-interactive proof system ................................ 5
   3.8 Fiat-Shamir ................................................... 6
   3.9 Non-interactive zero-knowledge proof (NIZKPoK) ........ 7
4 Analysis .............................................................. 7
   4.1 Soundness of Fiat-Shamir .................................... 7
   4.2 Zero-knowledge, Fiat-Shamir ................................ 8
   4.3 Signatures .................................................... 8
   4.4 Contributions of the paper .................................. 9
1 Introduction

This document will be divided in three parts. First, the global context will be given. Secondly some definitions and general explanation of the main concepts are presented in order to understand the document. Finally, the main aspects of the paper, with proof of soundness of Fiat-Shamir under certain circumstances. This paper is about the post-quantum security of Fiat-Shamir and how this construction could be used in this context. As Fiat-Shamir is an effective way to transform interactive protocols to non-interactive protocols in the random oracle model and provides a good signature scheme, there is great interest in using this construction in post-quantum cryptography.

2 Context

In the context of the cryptography seminar of the University of Tartu, this is an analysis of the paper [Unr17], which aims to construct a hardened Fiat-Shamir scheme, proven to be secure in the quantum setting [ARU14]. As before the non-hardened Fiat-Shamir was proven to be insecure in the quantum setting, this paper gives a solution to be able to continue using this scheme post-quantum. In this document, the main theorems and definition will be cited informally to be understood easily, and the sketch of the proof for those theorems is shown.

3 Definitions

3.1 Random Oracle model

An oracle machine is a black box function with a specific behavior. In cryptography the oracle machine are used to define a function, upon which the security analysis can be constructed. The random oracle model is a oracle which responds with a consistent, perfectly random, uniformly distributed output to each unique input. Every time a new input is given, a perfectly random output is given and kept in a table. If the same input is given, the oracle first looks up in the table and returns the value assigned to the input. In this particular paper, this is the oracle model used in the proofs of the cryptographic constructions. As an illustration, the black-box can be seen in the following way, assuming that the output is uniquely random for each input:
3.2 Completeness

Completeness in the case of a proof is the fact that we can be mathematically convinced by the proof if the statement is true, i.e. the probability of the proof being false is negligibly small. In the case of a proof system, completeness of the proof systems guarantees that the proof system really does prove the statement. Formally, it means that a honest verifier will always accept the proof of an honest prover.

3.3 Soundness

Soundness is the fact that if the statement is false, it is not possible to cheat someone to convince him it is true, i.e. the probability of cheating is negligibly small. Formally, it means that a honest verifier never accepts a proof of a non honest prover. In the paper soundness is more precisely defined according to the following table:

<table>
<thead>
<tr>
<th>Adversary power</th>
<th>normal</th>
<th>special</th>
</tr>
</thead>
<tbody>
<tr>
<td>computational</td>
<td></td>
<td>↘ stronger</td>
</tr>
<tr>
<td>Statistical</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Types of soundness

Soundness types compare to the power of the adversary. As an example, a protocol could be sound against a classical computer but broken by a quantum computer, like all protocols relying on discrete logarithm. As such soundness is divided into categories. Computable soundness is the soundness against unreasonably strong computational power. Statistical soundness is a stronger argument, which guarantees the soundness against unlimited computational power with a negligible probability $\mu$ of the proof not being accepted (perfect soundness $\Rightarrow \mu = 0$). As other characteristic of soundness special soundness, means the protocol is sound against rewinding attacks. Rewinding is an attack which can be explained as the adversary taking a snapshot of a specific transaction and replaying the same procedure in order to prove something else, as he knows the output of the input he is giving.
3.4 Proof of knowledge

A proof of knowledge is a construction defined to prove a statement between two parties. The prover constructs a proof that a verifier can check in order to validate the knowledge of the statement. There are two possibilities to prove the knowledge, either divulge the knowledge to the verifier, which can verify the statement. The second possibility is to provide a function or a protocol, which attests the knowledge of the statement without divulging it.

![Diagram of proof of knowledge](image)

Figure 2: Proof of knowledge

3.5 (Honest-Verifier) Zero-knowledge proof of knowledge

Here we talk about zero-knowledge proof of knowledge, which means that the construction should prove a known statement without disclose it to the verifier. Such proofs are important in many cryptographic schemes and can be used to construct signatures with public/private key pairs.

The following figure illustrates a proof of knowledge of the variable $x$ from a prover A to a verifier B. This figure is meant as an illustration of the construction and is only secure in the classical setting, as the discrete logarithm is calculated easily by a quantum computer.

\[
y := g^x \\
x := \log_g^e(y) \\
v := \text{rand()} \\
\text{comm} = g^v \\
\text{resp} = v - ch \times x
\]

In order to be secure, a proof of knowledge must have:
1. Completeness
2. Soundness
3. Zero-knowledge

Honest verifier is a specification explaining that the verifier is not trying to do something else than verifying (like simulate a bad proof or stealing the knowledge of the prover).
3.6 Σ-Protocol

A Σ-Protocol is a 3-messages protocol, consisting of commitment, challenge and response, for proof of knowledge. The sigma protocol used here is a well-known protocol to prove the authenticity of a statement $x$ of a Prover to a Verifier. The protocol works as follows:

![Diagram of Sigma Protocol]

Where $P_1, P_2$ are functions generating comm and resp and $V_1, V_2$ generating $ch$ and the validity check. The commitment is a value calculated by the prover, to be sent to the verifier. The challenge is a randomly selected value given by the verifier to the prover. The response is a proof, calculated with challenge, commitment and the statement, which proves the knowledge of the statement and can be checked positively by the verifier.

3.7 Non-interactive proof system

Non-interactive proof systems are construction that take away the necessity of the proof system to be interactive between the two parties: prover and verifier. To the contrary of an interactive proof system, The prover sends only one message to the verifier $B$, the single message being sufficient to prove his knowledge of the statement. Comparing the non-interactive proof to the Σ-protocol, the construction can be illustrated by the following figure:
3.8 Fiat-Shamir

Fiat-Shamir is a construction which transforms a $\Sigma$-protocol to a non-interactive proof system. This transformation works transparently in the classical setting and keeps the characteristics of the $\Sigma$-protocol. In the quantum setting, without any hardening parameters, the transformation was proven to take away the security of the $\Sigma$-protocol in the paper [ARU14]. The scheme was first presented in the paper [FS87] and was then used a lot to construct other schemes, like e-voting or signature schemes, because of its simplicity. The main idea of Fiat-Shamir is to let the challenge be produced by the prover with a hash function instead of taking an input from the verifier. The hash function is formally defined to be a random oracle. With the random oracle model, the hash will be uniformly random as before, but will unique for each statement and commitment as they are used for the hash. The scheme is defined as follows:
With this scheme, the only difference with the $\Sigma$-protocol, is that the challenge is produced by the prover. As the verifier will check the response at the end, which itself depends on the challenge, commitment and statement, it is not possible for the prover to cheat if the hash function is defined as the random oracle model. As we can see, the construction is a non-interactive proof system, which prove the knowledge of a statement.

In the paper, Fiat-Shamir is formally defined as $\Sigma: (l_{\text{com}}, l_{\text{ch}}, l_{\text{resp}}, P, P_1, P_2, V)$, $l$ being integers, $P$ prover and $V$ verifier. This can be done by calculating the challenge on the prover side securely, by hashing together $x$ and the commitment $\text{comm}$:

$$\text{ch} := H(x||\text{comm})$$

The end result $\text{resp}$ can then be sent to the Verifier who can check if it is valid.

3.9 Non-interactive zero-knowledge proof (NIZKPoK)

A Non-interactive zero-knowledge proof (NIZKPoK), is, in short, a zero-knowledge proof of knowledge without the need to interact with the verifier. It is indeed possible to change the standard protocol of zero-knowledge proofs to be non-interactive. This can then be used as a signature scheme, where someone can prove their ownership by proving they own the private key corresponding to the public key with a NIZKPoK.

Fiat-Shamir is a common NIZKPoK, and it is the main goal of the paper to achieve a quantum secure NIZKPoK with Fiat-Shamir.

4 Analysis

4.1 Soundness of Fiat-Shamir

It is important for the Fiat-Shamir scheme to be secure against an adversary which tries to prove a false statement. As Fiat-Shamir is used for signatures, if it is possible to create a fake signature in the quantum setting, then Fiat-Shamir would not be usable and thus not post-quantum secure.

In order to prove the soundness of Fiat-Shamir in the quantum setting it is needed that the, to be transformed, underlying, $\Sigma$-protocol has "perfect special soundness" (see 3.3). This necessity was given by the paper [ARU14] for the result to be sound (it was proven that computational special soundness is too weak).

Proof:

When taking a $\Sigma$-protocol with perfect special soundness, it is possible to deduct the following claim:

For any $x \in \{0,1\}^l \setminus L_R$ and any $\text{comm} \in \{0,1\}^{l_{\text{com}}}$, there exist at most one promising $\text{ch}$. ("Promising" means $\forall \text{resp} \exists! \text{ch} : V_\Sigma(x,\text{comm},\text{ch},\text{resp}) = 1$)

This claim means that there is only one unique challenge which produces a valid proof for any unique pair of statement and commitment.

1) Two promising $\text{ch} \neq \text{ch}'$ for a pair of $(x,\text{comm})$ will, by definition, yield a $\text{resp}, \text{resp}'$, such that the proof is valid: $V_\Sigma(x,\text{comm},\text{ch},\text{resp}) = V_\Sigma(x,\text{comm},\text{ch}',\text{resp}') = 1$. By definition of perfect special soundness, it is the same witness $w$ in both cases, where $(x,\text{comm}) \in R$. That implies that $(x,\text{comm}) \in L_R$, which is contradictory to the claim. Thus the challenge $\text{ch}$ is indeed unique.

2)
If we define a function going from any bitstring of length \( l^x + l^{comm} \) to a bitstring of length \( l^ch \) and \( x \notin L_R \), by 1) there exists a unique \( ch \), defined by a function \( ch := f(x||comm) \). Any other case gives \( f(x, comm) = 0^{l^ch} \). As the bitstrings of length \( l^x + l^{comm} \) cover all possible combinations of concatenations of \( x \) and \( comm \), this is true \( \forall (x, comm) \exists! ch \).

3) In the third step, we define a non negligible, hypothetical probability \( \delta \), of an adversary breaking the soundness in quantum-polynomial-time, given some initial state \( \rho \). The idea is to prove that this probability \( \delta \) is in fact negligible, and thus Fiat-Shamir sound. We know by 2), that \( ch \) is unique if \( V_\Sigma(x, comm, ch, resp) = 1 \) and by definition of Fiat-Shamir that \( ch = H(x||comm) \) where \( H \) is a random oracle, hence by 2) the function \( f(x, comm) = H(x, comm) \). As \( ch \) is unique and perfectly random as given by the random oracle, the probability of finding it is bigger than \( \delta \).

4) As we know that the probability of breaking the soundness is smaller than \( \delta \), the last thing to prove is that \( \delta \) is in fact negligible. In order to do that, we decline an algorithm \( B^{H'} \), which defines that \( H'(x||comm) = H(x||comm) \oplus f(x||comm) \). When running \( A^{H'} \), it will yield \( x||comm \), which breaks the soundness, as the statement is uncovered. A \( H \) and \( H' \) are uniformly random and \( H'(x||comm) = f(x||comm) \) with probability \( \geq \delta \), and \( H(x||comm) = 0^{l^ch} \), by definition of \( \oplus \). As \( \delta \) depends on the length of \( l^ch \), which is super-logarithmic, \( \delta \) is negligible, hence Fiat-Shamir is sound.

4.2 Zero-knowledge, Fiat-Shamir

In order to be post-quantum secure, Fiat-Shamir has to be zero-knowledge. In the paper it is proven that it is indeed, and combined with completeness and soundness, shows that Fiat-Shamir can indeed be secure in he quantum setting.

4.3 Signatures

Fiat-Shamir is used a lot for signature schemes in the classical setting. In order to be able to have a signature scheme based on Fiat-Shamir, it is necessary to have extractability. As the paper states that it is unknown if Fiat-Shamir has extractability (we know the witness) the signature scheme cannot be based on that. Another possibility is to use Dual mode hard instance generator, which gives a simulation-sound extractability (not possible to simulate a false proof) under certain circumstances described in the paper.

A dual mode hard instance generator is a construction which make a certain public key \( p_k \) indistinguishable from another public key \( p'_k \) which has no witness. As we cannot have extractability, we assume that the enemy cannot distinguish a valid \( p_k \) from an invalid \( p'_k \), in that way its still an unforgeable signature as the enemy cannot use \( p_k \) to prove something as it could be a false \( p'_k \). With some more assumptions not covered in this document it is then possible to rely on this to construct a strongly unforgeable signature scheme.
4.4 Contributions of the paper

The main contributions made by this paper are to prove that the Fiat-Shamir proof system is indeed post-quantum secure with strengthened conditions. This is formalized in 3 main theorems which are the following:

1. **Theorem 1 (Post-quantum security of Fiat-Shamir):**
   Assume that $\Sigma$ has honest-verifier zero-knowledge and perfect special soundness.
   Then the Fiat-Shamir proof system $(P_{FS}, V_{FS})$ is zero-knowledge and simulation proof

2. **Theorem 2 (Simulation-soundness of Fiat-Shamir):**
   Assume that $\Sigma$ has honest-verifier zero-knowledge, perfect special soundness, and unique responses.
   Then the Fiat-Shamir proof system $(P_{FS}, V_{FS})$ has simulation-soundness

3. **Theorem 3 (Fiat-Shamir signatures):**
   Assume that $G$ is a dual-mode hard instance generator. Fix a sigma-protocol $\Sigma$ (For showing that a given public key has a corresponding secret key).
   Assume that $\Sigma$ has honest-verifier zero-knowledge, perfect special soundness, and unique responses.
   Then the Fiat-Shamir signature scheme is strongly unforgeable.

[Unr17]

Those theorems take into account the proof of soundness given in 4.1, and its zero-knowledge 4.2, which are the necessary arguments to formulate the formal post-quantum security of Fiat-Shamir.

5 Conclusion

As Fiat-Shamir is a widely-used signature scheme, as of the last paper [ARU14], it would have been not usable if the adversary had a quantum computer. This means that a lot of those widely-used schemes would all have been obsolete and other schemes have to be used in the case of this threat model. This paper shows that Fiat-Shamir can actually be used under certain circumstances and keep its security.

References
