UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model

Seminar Essay
by Sayalee Chavan

Arbeitsgruppe
Codes und Kryptographie

Contents

1 Abstract

Cryptographic schemes are designed for secure communication between two parties and to protect data from being compromised. In a quantum setting, defining security is easy, but achieving it is challenging, unlike a classical environment. Fiat–Shamir protocol converts zero-knowledge interactive Σ-protocol into a non-interactive proof system in random oracle. Security is proven by preserving properties like soundness and proof of

knowledge in a quantum state. This technical paper briefly reviews the security definition of Σ-protocol implies the security definition of Fiat-Shamir protocol against a quantum attacker in the quantum random oracle model.

2 Introduction

In complexity theory, the concept of interactive proof is crucial. The interactive proof system [GMS87] includes two parties - a prover and a verifier. While a prover has unbounded computational power, the verifier has bounded computational power, i.e., the verifier is limited to be a (probabilistic) polynomial-time calculation. Proofs are generated to persuade someone about the particular statement is true. The prover's goal is to provide proof that persuades the verifier that the statement is valid. Formally, the statement can be defined by Language L, where the language is a set of strings and x is the input. The statement is represented as $x \in$ L [GMS87].

Interactive proof system [GMS87] has two security notions categorized as Completeness and Soundness. Completeness defines, if $x \in$ L, then verifier will always accept proofs generated by an honest prover that follows the defined protocol specification. The honest prover can always create a proof for all valid statements. Soundness characterizes that if $x \in$ L, no prover can convince the verifier about false statements, except negligible probability. Eventually, no proof exists for the invalid statement. Through completeness and soundness, valid statements can be proven with high probability, whereas invalid statements proved with negligible probability. Furthermore, the soundness property guarantees that the prover can not produce proof for invalid statements.

Zero-knowledge is an essential property in terms of security. The zero-knowledge property[GO94] ensures that the prover should not reveal any other information apart from the fact of the statement. Verifier cannot prove the statement to anyone else if the prover has secret information to generate valid proof for the statement. Therefore, the verifier learns nothing about secret information prover possesses. The notion of proof of knowledge [FKMV12] is intimately associated with that of interactive proof systems, although it is more subtle. In Proof of Knowledge(PoK), P tries to persuade V that he knows a hidden witness, which means that every statement is true, not only valid. The prover "knows something" if he can persuade the verifier with a high probability. There exist an efficient "knowledge extractor" that can extract witness from prover. The prover is considered honest if the probability of extracting witness and the probability of convincing the verifier is matched up.[BG92]

3 Sigma-Protocol (Σ-protocol)

Definition 3.1 *: A Σ-protocol is public coin three-round two party interactive protocol where Σ = (P,V) for a relation $R \subseteq \mathcal{X} \times W$ [DFMS19]:*

*Prover P(*x*,w)* *Verifier V(*x*)*

$\xrightarrow{a}$

$\xleftarrow{c}$

$\xrightarrow{z}$

where $c \leftarrow \{0,1\}^l$ *and after receiving z by V(x) accepts iff V (x, a, c, z) = 1*

Σ-protocol is a particular form of the zero-knowledge interactive proof system. At first, common public input x is given to the prover and verifier where $x \in \mathcal{X}$. Prover computes the message a to prove the statement. Additionally, P knows about witness $w \in$ W called as a private input (secret information) needed for proving the validity of the statement, such that $(x, w) \in$ R. Σ-protocol executes as follows [DFMS19]:

- Prover P sends a message a to verifier V.
- Verifier sends random challenge c to the Prover P to check if the prover is a malicious party.
- Upon receiving the challenge, prover generates response z and sends it to the Verifier. Finally, acceptance or rejection of proof is based on parameters (x, a, c, z).

3.1 Security properties of Sigma-Protocol

Security of sigma protocol is defined by three properties as follows:

1) *Completeness: V always accepts if P and V follow the protocol on input x and private input w to P where (x, w) ∈ R.[HL10]*

2) *Special Soundness: Given any x and any pair of accepting transcripts (a, c, z),(a, c', z') for x, where c ≠ c', there exists a polynomial-time algorithm A that outputs w such that (x, w) ∈ R.[HL10]*

3)*Special Honest-Verifier Zero-Knowledge (SHVZK): On inputs x and c, there is a probabilistic polynomial-time simulator M that produces a transcript of the form (a, c, z) of the same probability distribution as transcripts between the honest P and V on common input x. Formally, it is true that for every x and w such that (x, w) ∈ R and every* $c \in \{0,1\}^t$,

$$\{M(x,c)\} \equiv \{\langle P(x,w),\ V(x,c)\rangle\}$$

where M(x, c) denotes the output of simulator M on given inputs x and c, and P(x, w), V (x, c) denotes the output transcript of execution between P and V, where P has input (x, w), V has input x, and V's random tape (determining its query) equals c. ≡ denotes the similarity but not the same as equals. The value t denotes the length of the challenge.[HL10]

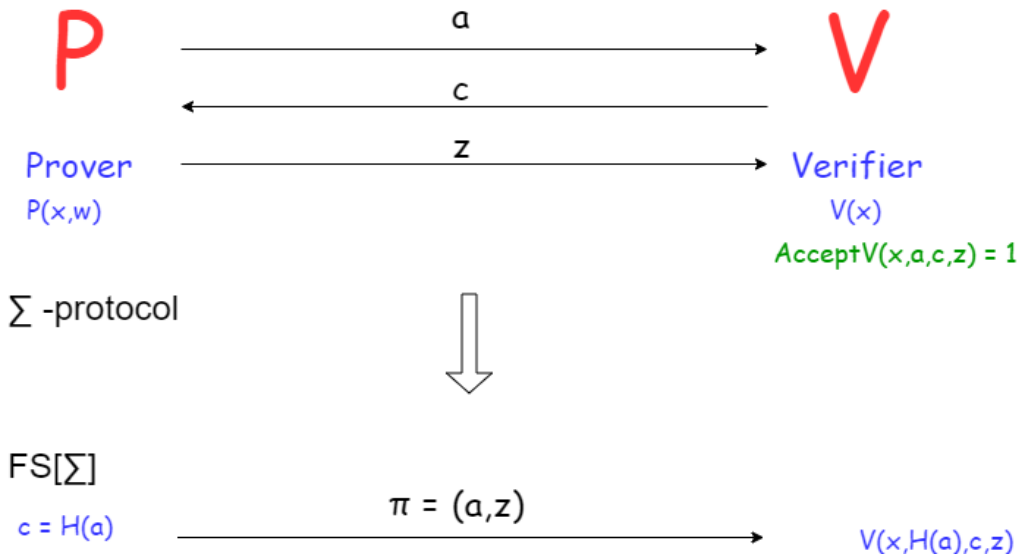

Figure 1: Transformation of Σ-protocol to Fiat-Shamir Protocol [DFMS19]

Furthermore, Soundness/Knowledge errors are considered to be negligible. Even if the prover has no witness for input x and x is invalid, the prover can succeed with negligible probability. Parallel repetition can help to reduce soundness errors.[DFMS19]

4 The Fiat-Shamir Transformation (FS[Σ])

Fiat-Shamir transformation [DFMS19] removes the interaction from Σ-protocol and converts it into the non-interactive protocol as it only requires one round, i.e., only one message can be transmitted from the prover to verifier. Correspondingly, the random challenge is replaced by using hash function H. As a result, the prover has absolute control over the interaction. [LZ19]

Figure 1 represents working of Fiat-Shamir transformation[DFMS19] as follows:

- First, prover P generates message a as before.
- Prover p computes challenge c by using secured random hash functions $c := \mathrm{H}(x,a)$
- The prover then computes the response z by utilizing a and determine challenge c. After obtaining challenge c, he produces proof $\pi = (a, z)$ by running Σ-protocol and send it to the verifier. The verifier decides to accept or reject proof based on predicate $\mathrm{V}(x, a, \mathrm{H}(x, a), z)$. In brief, an honest prover generates π until the Verifier accepts the predicate if Σ is statistically not correct.

Fiat-Shamir inherits the underlying Σ-protocol's security properties if H is a quality cryptographic function and acts as a random function. Security of Fiat-Shamir

transformation[DFMS19] is related to hash functions used for computing the challenge. One can find the difference between the fixed input x and x chosen by attacker A adaptively. Attacker A is considered a *static* attacker; if x is fixed, else attacker is *adpative*. For security purposes, the random oracle is used to model the hash function.

4.1 Random Oracle Model(ROM)

In general, a random oracle [BDF+11] defined as BlackBox, access given to parties for fully random functions. Any Honest or dishonest prover can make queries to a random oracle model. Random oracle model handles hash function H randomly. This random hash function is unknown to Prover P and Verifier V and only accessible via the random oracle model. A hash function H is selected among a set of random functions. Random oracle always gives consistent answers for the same query being made to it.

4.2 Fiat-Shamir transformation using Random Oracle Model

Figure 2 shows the working of Fiat-Shamir transformation in random oracle model. The main idea behind using the random oracle model is hash function should be only accessible via the random oracle. Ideally, hash functions computed through random oracle are proven to be secured. The prover queries to ROM with the message a and receives a hash function as an output. Typically, an honest prover can query the random oracle a few times, but on the other hand, the dishonest prover will make a query to a random oracle many times.[DFMS19]

Security of cryptographic scheme in random oracle ensured by measuring queries made by an attacker and reprogramming hash values with some random values for the given input.[DFMS19] Generally, proving security in a random oracle is relatively easier than establishing security in a quantum random oracle model. According to [DFMS19] If Σ-protocol-protocol is secure in the random oracle model, then Fiat-Shamir is also secured in the classical random oracle model. Security is always considered against dishonest prover.

4.3 Quantum Random Oracle Model(QROM)

Quantum attackers can compute the hash function "in a superposition" for different inputs by querying into ROM. Such queries should be allowed in ROM. In a quantum state, queries can not be recorded or copied in QROM without disturbing the quantum attacker's state. It is not easy to prove security in QROM. Conversely, measure and reprogramming are achieved without disturbing the state of the attacker.[DFMS19]

5 Measure and reprogramming

The paper's key technical result is measure and reprogramming in QROM. To calculate the hash function, the attacker queries to the random oracle. The model copies the query and extracts x from the query. After extracting, x can be reprogrammed with

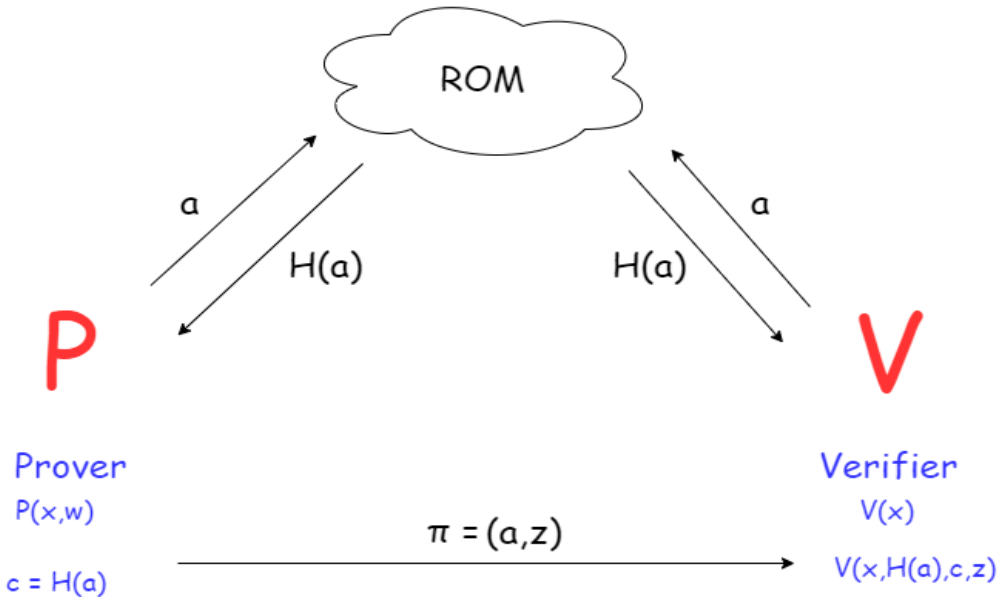

Figure 2: Fiat-Shamir transformation using random oracle model(ROM) [DFMS19]

random value Θ that produces output a pair (x, z) received by an attacker so verifier can be satisfied with the predicate $\mathrm{V}(x, a, \mathrm{H}(x), z)$. However, the verifier accepts this pair but with security loss of q^2 where q is a number of queries made to the oracle by an attacker.[DFMS19]

Theorem 5.1 (Measure and reprogram) *Let $\mathcal{X}$, Y be finite non-empty sets. There exists a black-box polynomial-time two-stage quantum algorithm S with the following property. Let A be an arbitrary oracle quantum algorithm that makes q queries to a uniformly random H: $\mathcal{X} \to Y$ and that outputs some $x \in \mathcal{X}$ and a (possibly quantum) output z. Then, the two-stage algorithm S^A outputs some $x \in \mathcal{X}$ in the first stage and, upon a random $\theta \to Y$ as input to the second stage, a (possibly quantum) output z, so that for any x'$\to \mathcal{X}$ and any predicate V [DFMS19]:*

$$\Pr_\theta[x{=}x' \wedge \mathrm{V}(x,\theta,z){:}(x,z){\leftarrow}(\mathrm{S}^A,\theta)] \gtrsim \tfrac{1}{O(q^2)} \Pr_H[x{=}x' \wedge \mathrm{V}(x,\mathrm{H}(x),z){:}(x,z) \leftarrow \mathrm{A}^H]$$

The left term states that at point x', S^A generates x in the first stage and produces response z by receiving θ. $\Pr_\theta$ implies that the probability is calculated over a random θ. A^H represents the purpose of executing A with the oracle generated by H. The right term states that at point x', A^H generates x in the first state and produces response z in the second state upon random hash function $\mathrm{H}(x)$. $\Pr_H$ implies that the probability is calculated over a random hash function H.[DFMS19]

6 Generic security reduction

Fiat-Shamir transformation attacker produces proof $\pi = (a, z)$ by computed challenge using hash function so (x, a, z) should be satisfied by predicate $\mathrm{V}(x, a, \mathrm{H}(x,a), z)$ refer to $x' \to \mathcal{X}$. However, At first Σ-protocol attacker generates message a and input x, then produces reply z by obtaining random challenge where $x' \to \mathcal{X}$. By applying theorem 5.1[DFMS19]:

$$\Pr_c[x{=}x' \wedge \mathrm{V}(x,a,\mathrm{c},z){:}(x,a,z){\leftarrow}(\mathrm{S}^A,\mathrm{c})] \gtrsim \tfrac{1}{O(q^2)} \Pr_H[x{=}x' \wedge \mathrm{V}(x,a,\mathrm{H}(x,a),z){:}(x,a,z) \leftarrow(\mathrm{A}^H)]$$

Pair (x, a) is also considered the output of Σ-protocol attacker. Verifier accepts or rejects based on parameters (x, a). Verifier's decision can be denoted by v so it can be written as [DFMS19]:

$$\Pr_c[x{=}x' \wedge \mathrm{v}{=}\mathrm{accept}{\leftarrow}(\mathrm{S}^A,\mathrm{V})] \gtrsim \tfrac{1}{O(q^2)} \Pr_H[x{=}x' \wedge V_{FS}\ (x,\pi){:}\ (x,\pi) \leftarrow(\mathrm{A}^H)]$$

By summing over $x' \in \mathcal{X}$,

$$\Pr[(\mathrm{S}^A,\mathrm{V}) = \mathrm{accept}] \geq \tfrac{1}{O(q^2)} \Pr_H[V_{FS}\ (x,\pi){:}\ (x,\pi) \leftarrow(\mathrm{A}^H)] \text{ - } \tfrac{1}{2q|C|}$$

The above argument states that there is a Σ-attacker for any Fiat-Shamir attacker who also has the same success probability loss and the same security definitions against dishonest attackers. Therefore, Fiat-Shamir protocol inherits security properties of Σ-protocol.[DFMS19]

The below theorem states the security reduction from Fiat-Shamir attacker to Σ attacker.

Theorem 6.1 *There exists a black-box quantum polynomial-time two-stage quantum algorithm S such that for any* adaptive *Fiat-Shamir attacker A, making q queries to a uniformly random function H with appropriate domain and range, and for any $x' \in \mathcal{X}$ [DFMS19]:*

$$\Pr[x{=}x' \wedge \mathrm{v}{=}\mathrm{accept}{:}\ (x,\mathrm{v}){\leftarrow}(\mathrm{S}^A,\mathrm{V})] \gtrsim \tfrac{1}{O(q^2)} \Pr_H[x{=}x' \wedge V_{FS}(x,\pi){:}\ (x,\pi) \leftarrow(\mathrm{A}^H)]$$

The above theorem shows that the probability of accepting predicate for Σ-attacker has the same loss of success probability for Fiat-Shamir attacker. This reduction can apply to show the preservation of properties like soundness and proof of knowledge statistically or computationally.[DFMS19]

6.1 Preservation of Soundness

Preservation of soundness property shows that no malicious prover can make verifier to accept false proof except some negligible probability. Two-party Σ-protocol consists of prover P and V. Fiat-Shamir represented by FS[Σ]. Consider, Σ = (P,V) for Relation R has parameter L such that L := $x \in \mathcal{X} \mid \exists w \in \mathrm{W} : \mathrm{R}(x, w)$. P, V, R, L depends on security parameters n, while A is commonly denoted for *static* and *adaptive* attackers.[DFMS19]

Definition 6.2 *Σ is computationally or statistically sound if there exist a negligible function μ(n) such that for any (quantum polynomial-time/unbounded) attacker a and any n ∈N [DFMS19]:*

$$\Pr[(\mathrm{A},\mathrm{V}(x)) = \text{accept}] \leq \mu(\mathrm{n})$$

In the case of an *adaptive* attacker, for all input $x \notin L$:

$$\Pr[x \notin L \wedge \mathrm{v} = \text{accept} : (x, \mathrm{v}) \leftarrow (\mathrm{A},\mathrm{V}) \,] \leq \mu(\mathrm{n})$$

Definition 6.3 *FS[Σ] is computationally or statistically sound if there exist a negligible function μ(n) and a constant e such that for any (quantum polynomial-time/unbounded) attacker a and any n ∈N [DFMS19]:*

$$\Pr_H[V_{FS}(x, \pi): \pi \leftarrow \mathrm{A}^H] \leq \mathrm{q}^e \, \mu(\mathrm{n})$$

In case of an *adaptive* attacker, for all input $x \notin L$:

$$\Pr_H[V_{FS}(x, \pi) \wedge x \notin L{:}(x, \pi) \leftarrow \mathrm{A}^H] \leq \mathrm{q}^e \, \mu(\mathrm{n})$$

In soundness definition, for Σ includes the negligible function to reduce soundness error to negligible as well as FS[Σ] has the negligible function and constant e.

Lemma 6.4 *if Σ is computationally or statistically sound against static attacker then it also computationally or statistically sound against adaptive attacker [DFMS19]:*

The lemma is the application of the definition of soundness for the *static* and *adaptive* attacker and theorem 6.1.

Corollary 6.5 *FS[Σ] is computationally or statistically sound against an adaptive attacker if Σ is computationally or statistically sound against static attacker where Σ is a Σ-protocol with superpolynomially sized challenge C.[DFMS19]*

Proof: There exists an *adaptive* Σ-protocol attacker for any *adaptive* FS-attacker in a computationally bounded setting by applying theorem 6.1. Therefore, by the soundness of an *adaptive* FS-attacker[DFMS19]:

$$Pr[x \notin L \wedge V_{FS}(x,\pi) : (x,\pi) \leftarrow A^H] \tag{1}$$

$$= \sum_{x' \notin L} Pr[x = x' \wedge V_{FS}(x,\pi) : (x,\pi) \leftarrow A^H] \tag{2}$$

$$\leq O(q^2)((\sum_{x' \notin L} Pr[x = x' \wedge v = accept : (x,v) \leftarrow (S^A, V]) + \frac{1}{2q|C|}) \tag{3}$$

$$= O(q^2)(Pr[x \notin L \wedge v = accept : (x,v) \leftarrow (S^A, V)]) + \frac{O(q)}{|C|)} \tag{4}$$

$$\leq O(q^2).\mu(n). + \frac{O(q)}{|C|)} \tag{5}$$

Equation (2), starting with the definition of *adaptive* FS-attacker at point x', there exists Σ-attacker with the probability loss of $O(q^2)$ same as FS-attacker. The term (3) produces after applying 6.1. By summing over x' in term (4). After applying the definition of soundness for *adaptive* Σ-attacker, the term(4) was replaced by μ(n). In the end, inequality shows that there exist some negligible function means Σ-protocol is sound against the *static* attacker. By applying lemma6.4, it proves that if it is sound against *static* attacker for Σ-protocol then also sound against FS[Σ] attacker.[DFMS19]

6.2 Preservation of Proof of Knowledge

By the informal definition of proof of knowledge, a knowledge extractor extracts secret information (witness w) from attackers with negligible knowledge error. It is possible to extract witness w for input x if A is able to prove instance x.[DFMS19]

Definition 6.6 Σ *is computationally or statistically proof of knowledge if there exist a quantum polynomial-time black-box 'knowledge extractor' K, a polynomial p(n), a constant d ≥ 0, and a negligible function k(n) such that for any (quantum polynomial-time/unbounded) attacker A and any n ∈N and* x ∈ $\mathcal{X}$ *[DFMS19]:*

$$\Pr[(x,w) \in R : w \leftarrow K^A(x)] \geq \tfrac{1}{p(n)}.\Pr[(A,V(x)) = \text{accept}]^d - k(n)$$

For attacker A:

$$\Pr[x \in X \wedge (x,w) \in R : (x,w) \leftarrow K^A] \geq \tfrac{1}{p(n)}.\Pr[x \in X \wedge v = \text{accept}:(x,v) \leftarrow (A,V)]^d - k(n)$$

for subset $X \subseteq \mathcal{X}$

Definition 6.7 *FS[Σ] is computationally or statistically proof of knowledge if there exist a quantum polynomial-time black-box 'knowledge extractor' ε, a polynomial p(n), a constant d,e ≥ 0, and a negligible function μ(n) such that for any (quantum polynomial-time/unbounded) attacker A and any n ∈N and* x ∈ $\mathcal{X}$ *[DFMS19]:*

$$\Pr[(x,w) \in \mathrm{R} : \mathrm{w} \leftarrow \varepsilon^{A}(x)] \geq \frac{1}{q^{e}p(n)}.\Pr_{H}[\ V_{FS}(x,\pi):\pi \leftarrow \mathrm{A}^{H}\ ]^{d} - \mu(\mathrm{n})$$

for subset $X \subseteq \mathcal{X}$

For attacker an *adaptive* A:

$$\Pr[x \in \mathrm{X} \wedge (x,w) \in \mathrm{R} : (x,w) \leftarrow \varepsilon^{A}] \geq \frac{1}{q^{e}p(n)}.\Pr_{H}[x \in \mathrm{X} \wedge V_{FS}(x,\pi):(x,\pi) \leftarrow \mathrm{A}^{H}\ ]^{d} - \mu(\mathrm{n})$$

Proof of knowledge is considered stronger than soundness. The presence of negligible function leads to the reduction of knowledge error.[DFMS19]

Lemma 6.8 *if Σ is computationally or statistically proof of knowledge against static attacker A then it also computationally or statistically proof of knowledge against adaptive attacker A [DFMS19]:*

The lemma is the application of the definition of proof of knowledge for the *static* and *adaptive* attacker and theorem 6.1.

Corollary 6.9 *FS[Σ] is computationally or statistically proof of knowledge against an adaptive attacker if Σ is computationally or statistically proof of knowledge against static attacker where Σ is a Σ-protocol with superpolynomially sized challenge C. [DFMS19]*

Proof: Consider K as a knowledge extractor, *adaptive* FS[Σ] attacker as A, ε as FS[Σ] knowledge extractor. Assume that Σ is computationally/statistically proof of knowledge against an *adaptive* attacker by lemma 6.8. For FS[Σ], ε is the black-box knowledge extractor. By calling theorem 6.1 the *adaptive* Σ S^{A} is obtained. Applying Σ proof of

knowledge property[DFMS19]:

$\Pr[x\in X \wedge (x,w) \in \mathrm{R} : (x,w) \leftarrow \varepsilon^{A}]$

$= \Pr[x\in X \wedge (x,w) \in \mathrm{R} : (x,w) \leftarrow \mathrm{K}^{S^{A}}]$

$= \frac{1}{p(n)} \Pr[x\in X \wedge \mathrm{v} = \mathrm{accept}(x,\mathrm{v}) \leftarrow (\mathrm{S}^{A},\mathrm{V})]^{d}$ - k(n))

$= \frac{1}{p(n)} (\sum_{x'\in X} \Pr[x\in X \wedge \mathrm{v} = \mathrm{accept}(x,\mathrm{v}) \leftarrow (\mathrm{S}^{A},\mathrm{V})])^{d}$ - k(n))

$\geq \frac{1}{p(n)}(\frac{1}{O(q^2)} \sum_{x'\in X} \Pr_{H}[x=x' \wedge V_{FS}(x,\pi) : (x,\pi) \leftarrow \mathrm{A}^{H}]$ - $\frac{1}{2q|C|})^{d}$ - k(n))

$\geq \frac{1}{p(n)} \frac{1}{O(q^{2d})} Pr_{H}[x\in X \wedge V_{FS}(x,\pi) : (x,\pi) \leftarrow \mathrm{A}^{H}]^{d}$ - μ(n)

ε^{A} runs by invoking theorem 6.1 and running $K^{\varepsilon A}$, where S^{A} is the *adaptive* Σ-protocol attacker. Starting with proof of knowledge definition for Σ-attacker, there exist an *adaptive* FS-attacker which has probability loss of $O(q^2)$. The corollary shows the transformation of proof of knowledge Σ-protocol attacker to FS-attacker. Invoking Σ proof of knowledge proves that FS[Σ] is also proof of knowledge against *adaptive* attacker for negligible function.[DFMS19]

7 Conclusion

This report highlights the central aspect of proving the security of cryptographic schemes in quantum and classical settings against the attacker. The interactive proof system has properties that define the security of cryptographic protocols. Σ-protocol is the standard interactive protocol with some security properties that secure against the attacker. Furthermore, Fiat-Shamir transformation is used to remove interaction between the two parties to prevent exposing secret information to an attacker. One of the fundamental approaches is to use random oracle and quantum random oracle models to compute the hash function, which has strong randomness. The main result of the paper is to show the security of Σ and FS[Σ], which is the extension of the Σ protocol in the quantum state. This paper concludes that if Σ is secured against the attacker, then FS[Σ] is also secured against the attacker.

References

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *International conference on the theory and application of cryptology and information security*, pages 41–69. Springer, 2011.

[BG92] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In *Annual International Cryptology Conference*, pages 390–420. Springer, 1992.

[Dam02] Ivan Damgård. On σ-protocols. *Lecture Notes, University of Aarhus, Department for Computer Science*, 2002.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model. In *Annual International Cryptology Conference*, pages 356–383. Springer, 2019.

[FKMV12] Sebastian Faust, Markulf Kohlweiss, Giorgia Azzurra Marson, and Daniele Venturi. On the non-malleability of the fiat-shamir transform. In *International Conference on Cryptology in India*, pages 60–79. Springer, 2012.

[GMS87] Oded Goldreich, Yishay Mansour, and Michael Sipser. Interactive proof systems: Provers that never fail and random selection. In *28th Annual Symposium on Foundations of Computer Science (sfcs 1987)*, pages 449–461. IEEE, 1987.

[GO94] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, 1994.

[HL10] Carmit Hazay and Yehuda Lindell. *Efficient secure two-party protocols: Techniques and constructions*. Springer Science & Business Media, 2010.

[LZ19] Qipeng Liu and Mark Zhandry. Revisiting post-quantum fiat-shamir. In *Annual International Cryptology Conference*, pages 326–355. Springer, 2019.