# Non-interactive zero-knowledge proofs in the quantum random oracle model

Dominique Unruh
University of Tartu

**Abstract.** We present a construction for non-interactive zero-knowledge proofs of knowledge in the random oracle model from general sigma-protocols. Our construction is secure against quantum adversaries. Prior constructions (by Fiat-Shamir and by Fischlin) are only known to be secure against classical adversaries, and Ambainis, Rosmanis, Unruh (FOCS 2014) gave evidence that those constructions might not be secure against quantum adversaries in general.

To prove security of our constructions, we additionally develop new techniques for adaptively programming the quantum random oracle.

[This paper will appear at Eurocrypt 2015. A full version is provided in [15].]

**Classical NIZK proofs.** Zero-knowledge proofs are a vital tool in modern cryptography. Traditional zero-knowledge proofs (e.g., [10]) are interactive protocols, this makes them cumbersome to use in many situations. To circumvent this problem, non-interactive zero-knowledge (NIZK) proofs were introduced [3]. NIZK proofs circumvent the necessity for interaction by introducing a CRS, which is a publicly known value that needs to be chosen by a trusted third party. The ease of use of NIZK proofs comes at a cost, though: generally, NIZK proofs will be less efficient and based on stronger assumptions than their interactive counterparts. So-called sigma protocols (a certain class of three move interactive proofs, see below) exist for a wide variety of problems and admit very generic operations for efficiently constructing more complex ones [5, 7] (e.g., the "or" of two sigma protocols). In contrast, efficient NIZK proofs using a CRS exist only for specific languages (most notably related to bilinear groups, using Groth-Sahai proofs [11]). To alleviate this, Fiat and Shamir [8] introduced so-called Fiat-Shamir proofs that are NIZK proofs in the random oracle model.[1] Those can transform any sigma protocol into a NIZK proof. (In fact the construction is even a proof *of knowledge*, but we will ignore this distinction for the moment.) The Fiat-Shamir construction (or variations of it) has been used in a number of notable protocols, e.g., Direct Anonymous Attestation [4] and the Helios voting system [1]. A second construction of NIZK proofs in the random oracle model was proposed by Fischlin [9]. Fischlin's construction is less efficient than Fiat-Shamir (and imposes an additional condition on the sigma protocol, called "unique responses"), but it avoids certain technical difficulties that Fiat-Shamir has (Fischlin's construction does not need rewinding).

**Quantum NIZK proofs.** However, if we want security against quantum adversaries, the situation becomes worse. Groth-Sahai proofs are not secure because they are based on hardness assumptions in bilinear groups that can be broken by Shor's algorithm [13]. And Ambainis, Rosmanis, and Unruh [2] show that the Fiat-Shamir construction is not secure in general, at least relative to a specific oracle. Although this does not exclude that Fiat-Shamir is still secure without oracle, it at least makes a proof of security less likely – at the least, such a security proof would be non-relativizing, while all known proof techniques that deal with rewinding in the quantum case [18, 14] are relativizing. Similarly, [2] also shows Fischlin's scheme to be insecure in general (relative to an oracle). Of course, even if Fiat-Shamir and Fischlin's construction are insecure in general, for certain specific sigma-protocols, Fiat-Shamir or Fischlin could still be secure. (Recall that both constructions take an *arbitrary* sigma-protocol and convert it into a NIZK proof.) In fact,

[1] [8] originally introduced them as a heuristic construction for signatures schemes (with a security proof in the random oracle model by [12]). However, the construction can be seen as a NIZK proof of knowledge in the random oracle model.

Dagdelen, Fischlin, and Gagliardoni [6] show that for a specific class of sigma-protocols (with so-called "oblivious commitments"), a *variant* of Fiat-Shamir is secure. However, sigma-protocols with oblivious commitments are themselves already NIZK proofs in the CRS model. Also, sigma-protocols with oblivious commitments are not closed under disjunction and similar operations (at least not using the constructions from [5]), thus losing one of the main advantages of sigma-protocols for efficient protocol design. Hence sigma-protocols with oblivious commitments are a much stronger assumption than just normal sigma-protocols; we lose one of the main advantages of the classical Fiat-Shamir construction: the ability to transform *arbitrary* sigma-protocols into NIZK proofs. Summarizing, prior to this paper, no generic quantum-secure construction was known to transform sigma-protocols into NIZK proofs or NIZK proofs of knowledge in the random oracle model. ([6] left this explicitly as an open problem.)

**Our contribution.** We present a NIZK proof system in the random oracle model, secure against quantum adversaries. Our construction takes any sigma protocol (that has the standard properties "honest verifier zero-knowledge" (HVZK) and "special soundness") and transforms it into a non-interactive proof. The resulting proof is a zero-knowledge proof of knowledge (secure against polynomial-time quantum adversaries) with the extra property of "online extractability". This property guarantees that the witness from a proof can be extracted without rewinding. (Fischlin's scheme also has this property in the classical setting, but not Fiat-Shamir.) Furthermore the scheme is non-malleable, more precisely simulation-sound. That is, given a proof for one statement, it is not possible to create a proof for a related statement. This property is, e.g., important if we wish to construct a signature-scheme from the NIZK proof.

As an application we show how to use our proof system to get strongly unforgeable signatures in the quantum random oracle model from any sigma protocol (assuming a generator for hard instances).

In order to prove the security, we additionally develop a result on random oracle programming in the quantum setting (see the full version [15]) which is a strengthening of a lemma from [17, 16] to the adaptive case. It allows us to reduce the probability that the adversary notices that a random oracle has been reprogrammed to the probability of said adversary querying the oracle at the programmed location. (This would be relatively trivial in a classical setting but becomes non-trivial if the adversary can query in superposition.)

**Difficulties with Fiat-Shamir and Fischlin.** In order to understand our protocol construction, we first explain why Fiat-Shamir and Fischlin's scheme are difficult to prove secure in the quantum setting. Classically, to prove the security of Fiat-Shamir [12], we run the malicious prover such that it outputs a valid proof. This proof contains values $com$ and $ch$ such that $H(com) = ch$. The properties of sigma-protocols guarantee that, if we find another proof with the same $com$ and a different $ch'$, we can efficiently compute a witness (which then shows that Fiat-Shamir is a proof of knowledge). To do so, we rewind the malicious prover, and rerun it, except that the random oracle $H$ is changed to give different a different answer for the query $H(com)$. One can show that with sufficiently high probability, we get two valid proofs with the same $com$, but with different answers $ch = H(com)$.

What happens if we try and translate this proof idea into the quantum setting? First of all, rewinding is difficult in the quantum setting. We can rewind $P$ by applying the inverse unitary transformation $P^\dagger$ to reconstruct an earlier state of $P$. However, if we measure the output of $P$ before rewinding, this disturbs the state, and the rewinding will return to an undefined earlier state. In some situations this can be avoided by showing that the output that is measured contains little information about the state and thus does not disturb the state too much [14], but it is not clear how to do that in the case of Fiat-Shamir.

Even if we have solved the problem of rewinding, we face a second problem. We wish to reprogram the random oracle at the input where it is being queried. Classically, the input of a random oracle query is a well-defined notion. In the quantum setting, though, the query input may be in superposition, and we cannot measure the input because this would disturb the state.

Similarly, translating the classical proof [9] of Fischlin's scheme fails. Although that proof does not rely on rewinding, it assumes that the list of queries made to the random oracle is well-defined. In fact, the extractor computes a witness from the list of queries made. In the quantum setting, this list is not well-defined, since one can query the random oracle in superposition, thus querying

all inputs simultaneously. Also, we cannot measure what the inputs to the queries are, since this would disturb the malicious prover.

The problems with Fiat-Shamir and Fischlin seem not to be just limitations of our proof techniques, [2] shows that relative to some oracle, Fiat-Shamir and Fischlin actually become insecure.

**Our protocol.** So both in Fiat-Shamir and in Fischlin's scheme we face the challenge that it is difficult to get the query inputs made by the malicious prover. Nevertheless, in our construction we will still try to extract the query inputs, but with a twist: Assume for a moment that the random oracle $G$ is a permutation. Then, given $G(x)$ it is, at least in principle, possible to extract $x$. Can we use this idea to save Fischlin's scheme? No, because in Fischlin's scheme we do not see the outputs of the queries, either; inverting $G$ will not help. In our scheme, we make sure that using only the query inputs for queries that are contained in the final proof, one can compute a witness. This implies that, if we can invert $G$, we can extract a witness from any valid proof.

But how do we make the random oracle invertible? Zhandry [19] shows that a random oracle is indistinguishable from a $2q$-wise independent function (where $q$ is the number of queries), in particular from a random polynomial of degree $2q$. Thus, in the security proof, we replace $G$ by a random polynomial over a finite field, and use the fact that polynomials can be inverted. (The inverse is not unique, but the above approach can be adapted to that idea.)

For a more intuition, a full description of the protocol, and the proofs, we refer to the full version [15].

**References.**


[1] B. Adida. Helios: Web-based open-audit voting. In P. C. van Oorschot, editor, *USENIX Security Symposium 08*, pages 335–348. USENIX, 2008.

[2] A. Ambainis, A. Rosmanis, and D. Unruh. Quantum attacks on classical proof systems (the hardness of quantum rewinding). In *FOCS 2014*, pages 474–483. IEEE, October 2014.

[3] M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 103–112, New York, NY, USA, 1988. ACM.

[4] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In *ACM CCS '04*, pages 132–145, New York, NY, USA, 2004. ACM.

[5] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Y. Desmedt, editor, *Crypto 94*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer, 1994.

[6] Ö. Dagdelen, M. Fischlin, and T. Gagliardoni. The Fiat-Shamir transformation in a quantum world. In *Asiacrypt 2013*, volume 8270 of *LNCS*, pages 62–81. Springer, 2013.

[7] I. Damgård. On $\sigma$-protocols. Course notes for "Cryptologic Protocol Theory", `http://www.cs.au.dk/~ivan/Sigma.pdf`, 2010.

[8] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Crypto '86*, number 263 in LNCS, pages 186–194. Springer, 1987.

[9] M. Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In *Crypto 2005*, volume 3621 of *LNCS*, pages 152–168. Springer, 2005.

[10] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J ACM*, 38(3):690–728, 1991.

[11] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. Smart, editor, *Eurocrypt 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2008.

[12] D. Pointcheval and J. Stern. Security proofs for signature schemes. In U. Maurer, editor, *Eurocrypt 96*, volume 1070 of *LNCS*, pages 387–398. Springer, 1996.

[13] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS 1994*, pages 124–134. IEEE, 1994.

[14] D. Unruh. Quantum proofs of knowledge. In *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012. Preprint on IACR ePrint 2010/212.

[15] D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. IACR ePrint 2014/587, 2014. Full version of this paper.

[16] D. Unruh. Quantum position verification in the random oracle model. In *Crypto 2014*, LNCS. Springer, February 2014. To appear, preprint on IACR ePrint 2014/118.

[17] D. Unruh. Revocable quantum timed-release encryption. In *Eurocrypt 2014*, volume 8441 of *LNCS*, pages 129–146. Springer, 2014. Full version on IACR ePrint 2013/606.

[18] J. Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.

[19] M. Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Crypto 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, 2012.