Merkle Puzzles in a Quantum World

Gilles Brassard[1], Peter Høyer[2], Kassem Kalach[1],
Marc Kaplan[1], Sophie Laplante[3] and Louis Salvail[1]

[1] *Département d'informatique et de recherche opérationnelle, Université de Montréal*
C.P. 6128, Succursale centre-ville, Montréal (QC), H3C 3J7 Canada.
[2] *Department of Computer Science, University of Calgary*
2500 University Drive N.W., Calgary, AB, T2N 1N4 Canada.
[3] *LRI, Université Paris-Sud, 91400 Orsay, France.*
{brassard,kalachka,kaplanm,salvail}@iro.umontreal.ca, hoyer@ucalgary.ca, Sophie.Laplante@lri.fr

August 28, 2011

Abstract

The first unclassified document ever written to solve the key establishment problem and propose the notion of public key cryptography was a project proposal in a course on computer security written by Ralph Merkle in 1974 [13]. We first introduce the model behind Merkle's scheme.

For any positive integer N, let $[N]$ denote the set of integers from 1 to N. We assume the existence of a random black-box function $f : [N^2] \to [N^k]$, where constant k is chosen large enough so that there is no collision in the image of f, except with negligible probability. The value of $f(x)$ can be obtained in unit time for any given input x, but the only way to retrieve x given $f(x)$ is to try preimages and compute f on them until one is found that maps to $f(x)$. This is known as the *random oracle* model. We also assume that (1) the legitimate parties communicate through an *authenticated classical channel* on which eavesdropping is unrestricted and (2) a protocol is deemed to be *secure* if the number of queries required of the eavesdropper to learn the secret established by the legitimate parties grows *super-linearly* with the number of legitimate queries. This will be the framework throughout this paper.

Merkle's scheme proceeds as follows. One party called Alice chooses N distinct random values $x_1, x_2, \ldots, x_N$ in the domain of f and transmits them, encrypted by the application of f, to the other party called Bob. Let us denote $X = \{x_i \mid 1 \leqslant i \leqslant N\}$ and $Y = \{f(x_i) \mid 1 \leqslant i \leqslant N\}$. Bob finds one preimage $x \in X$ and sends back $f(x)$ to Alice. Finally, given $f(x)$ and having kept $\{(x_i, f(x_i)) \mid 1 \leqslant i \leqslant N\}$, Alice can easily find x without further querying the oracle. This x, which is now known to both Alice and Bob, becomes their key.

We now analyse the effort required of each party. Alice makes N queries. Since there are N^2 points in the domain of f and N possible preimages, it suffices for Bob to make $O(N)$ random queries before the birthday paradox makes it overwhelming likely that he should chance to guess at one $x \in X$. However, an eavesdropper who listens to the entire conversation (Y and $f(x)$) has no way to obtain this x but to invert the function on $f(x)$ specifically, which requires a number of queries in $\Omega(N^2)$. This is quadratically more queries than the legitimate parties.

It took 35 years before Boaz Barak and Mohammad Mahmoody-Ghidary proved that this quadratic gap between the legitimate and eavesdropping efforts is best possible in a classical world [2], improving over the work of Impagliazzo and Rudich [11].

However, the situation is different in the quantum setting. There is an obvious quantum attack that makes this scheme completely insecure. Assume that function f can be *accessed in a quantum superposition of inputs*. In this case, *Grover's algorithm* [9] can be used to invert $f(x)$ with a number of queries in the order of the square root of the number of points in the domain of f, which is $O(\sqrt{N^2}) = O(N)$ quantum queries. Consequently, the cryptanalytic task is as easy (up to constant factors) as the key establishment process.

Can Merkle's idea be made secure again in our quantum world, keeping its defining characteristics? A first solution was proposed by Brassard and Salvail [8]. The idea is to allow Alice and Bob to use quantum computers as well (in fact, only Bob will make use of this power), and increase the domain of f from N^2 to N^3 points. This scheme is exactly as Merkle's except that Bob uses the BBHT algorithm [5], which is a generalization of Grover's algorithm [9], to find one element in X. Out of N^3 points in the domain of f, there are exactly $t = N$ solutions to the problem of finding one preimage $x \in X$. This problem is solved with $O(\sqrt{N^3/t}) = O(N)$ queries [5]. In total, Alice makes N classical queries and Bob makes $O(N)$ quantum queries.

The eavesdropper, on the other hand, must again invert f on a specific point in its image. Even with a quantum computer, the eavesdropper needs $\Omega(\sqrt{N^3}) = \Omega(N^{3/2})$ queries using Grover, which is optimal [3]. This is not as good as $\Omega(N^2)$ queries required by a *classical* eavesdropper against Merkle's original scheme, but significantly better than $O(N)$ queries sufficient for a *quantum* eavesdropper against the same scheme. Two questions were left open in Ref. [8]:

1. Can the quadratic security of Merkle's scheme be restored if all parties make use of quantum powers?

2. Can every key exchange protocol in the random oracle model be broken with $O(N)$ queries when both legitimate parties are classical but the eavesdropper is quantum?

In this context, the main challenge is that the communication channel is classical, thus preventing the use of Quantum Key Distribution [4]. Another challenge, particularly when the legitimate parties are classical, is that the eavesdropper is allowed to use unrestricted quantum computation. In this paper, we give two novel provably secure protocols to address these issues. We make progress on the first question and answer negatively the second one.

In our first protocol, Bob makes use of quantum computational powers but Alice remains purely classical, as was the case in Ref. [8]. We assume the existence of *two* black-box random functions $f : [N^3] \to [N^k]$ and $g : [N^3] \to [N^{k'}]$ that can be accessed in quantum superposition of inputs. Again, constant k is chosen large enough so that there is no collision in the image of f, except with negligible probability. The condition on k' is that we choose it large enough to ensure that $g(a) \oplus g(b) \oplus g(c) \oplus g(d) \neq 0$ whenever $\{a, b, c, d\}$ contains at least three distinct elements in the domain of g, again except with negligible probability, where "$\oplus$" denotes the bitwise exclusive-or. The legitimate parties proceed as follows.

1. Alice picks at random N distinct values $\{x_i\}_{i=1}^{N}$ in the domain of f and transmits their images $f(x_i)$ to Bob. Let X and Y denote $\{x_i \mid 1 \leqslant i \leqslant N\}$ and $\{f(x_i) \mid 1 \leqslant i \leqslant N\}$, respectively. Note that Alice knows both X and Y, whereas Bob has knowledge of Y only.

2. Bob finds *two* distinct preimages x and x' of random elements in Y. There are exactly $t = N$ solutions to the problem of finding one preimage in X, out of N^3 points in the domain of f. Using BBHT [5], this is accomplished with $O(\sqrt{N^3/t}) = O(N)$ queries to f.

3. Bob sends back $w = g(x) \oplus g(x')$ to Alice.

4. Alice queries the oracle g on the set X. Given w, she uses the table $\{(x_i, g(x_i)) \mid 1 \leqslant i \leqslant N\}$ to find Bob's pair (x, x'), which becomes their common secret.

All counted, Alice makes N queries to f in step 1 and N queries to g in step 4, whereas Bob makes $O(N)$ queries to f in step 2 and two queries to g in step 3. Therefore, the legitimate parties make a total of $O(N)$ queries. If we also cared about computation time, it seems at first that Alice has to try about $N^2/2$ pairs in step 4. Fortunately, this can be done in linear time.

One important difference between this protocol and the previous ones [13, 8] is that Bob finds *two* preimages instead of one. Can this make the eavesdropper's life more difficult? We devised a quantum attack that allows him to find the secret (x, x') with $O(N^{5/3})$ queries to f and g by way of a quantum walk in a Johnson graph reminiscent of Ambainis' quantum algorithm for the element distinctness problem [1]. Furthermore, we proved that this attack is optimal (up to logarithmic factors). Therefore, we don't quite restore the quadratic security possible in a classical world, but we make significant progress towards it. Our lower-bound proof proceeds in three steps: (1) We define a search problem related to element distinctness; (2) We prove a lower bound on the difficulty to solve this search problem; and (3) We reduce the search problem to the eavesdropping problem against our protocol. The crucial observation is that the defined search problem is the composition of a variant of element distinctness on N elements with searching each element in a set of size N^2 using Grover. We would have liked to apply the composition theorem of Refs. [10, 12]. However, it is not applicable in our case because the inner function is not Boolean and thus we had to prove a new composition theorem to establish the lower bound of the underlying problem.

Our second protocol, which is *purely classical*, is almost identical to the first one except for two differences: (1) both legitimate parties use *classical* computation while the adversary still uses quantum computation; and (2) the domain of the two black-box functions is reduced from N^3 to N^2 to make it possible for classical Bob to find his two preimages by virtue of the birthday paradox. Using the same quantum attack and lower bound techniques, *mutatis mutandis*, we prove that a quantum eavesdropper requires $\Theta(N^{7/6})$ queries to f and g in order to find the key.

In conclusion, we present two key establishment protocols *à la* Merkle over a classical channel. The first is a quantum protocol that improves over the scheme of Brassard and Salvail [8] and the second is a classical protocol secure against a quantum adversary. Are these two protocols optimal? We conjecture that they are not. Indeed, we discovered a sequence of quantum protocols in which our most efficient quantum attack tends to $\Theta(N^2)$ queries and a sequence of classical protocols in which our most efficient quantum attack tends to $\Theta(N^{3/2})$ queries. Our current problem is to prove matching lower bounds. We also proved a new composition theorem for quantum query complexity.

A preliminary version of this paper appeared in the Proceedings of Crypto 2011 [6] and a full version is accessible on the arXiv [7], but the two protocols we present here are slightly different. In particular, our classical protocol improves over the one in Refs. [6, 7], against which a quantum eavesdropper could obtain the key with merely $\Theta(N^{13/12})$ queries to the oracle. Nevertheless, that had been the first classical scheme in the random oracle model secure against a quantum adversary.

References

[1] A. Ambainis, "Quantum walk algorithm for element distinctness", *SIAM Journal on Computing* **37**:210–239, 2007.

[2] B. Barak and M. Mahmoody–Ghidary, "Merkle puzzles are optimal — An $O(n^2)$–query attack on any key exchange from a random oracle", *Advances in Cryptology – Proceedings of Crypto 2009*, Santa Barbara, California, pp. 374–390, 2009.

[3] C. H. Bennett, E. Bernstein, G. Brassard and U. V. Vazirani, "Strengths and weaknesses of quantum computing", *SIAM Journal on Computing* **26**(5):1510–1523, 1997.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[5] M. Boyer, G. Brassard, P. Høyer and A. Tapp, "Tight bounds on quantum searching", *Fortschritte Der Physik* **46**:493–505, 1998.

[6] G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante and L. Salvail, "Merkle puzzles in a quantum world", *Advances in Cryptology – Proceedings of Crypto 2011*, Santa Barbara, California, pp. 391–410, 2011.

[7] G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante and L. Salvail, "Merkle puzzles in a quantum world", `http://arxiv.org/abs/1108.2316`.

[8] G. Brassard and L. Salvail, "Quantum Merkle puzzles", *Proceedings of Second International Conference on Quantum, Nano, and Micro Technologies* (ICQNM08), Sainte Luce, Martinique, pp. 76–79, 2008.

[9] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack", *Physical Review Letters*, **79**(2):325–328, 1997.

[10] P. Høyer, T. Lee and R. Špalek, "Negative weights make adversaries stronger", *Proceedings of 39th Annual Symposium on Theory of Computing (STOC)*, June 2007, pp. 526–535. The complete version can be found at `http://arxiv.org/abs/quant-ph/0611054v2`.

[11] R. Impagliazzo and S. Rudich, "Limits on the provable consequences of one-way permutations", *Advances in Cryptology – Proceedings of Crypto '88*, Santa Barbara, California, pp. 8–26, 1988.

[12] T. Lee, R. Mittal, B. W. Reichardt and R. Špalek, "An adversary for algorithms", `arXiv:1011.3020v1`, 2010.

[13] R. Merkle, "Publishing a new idea", including a link to his 1974 original UC Berkeley CS244 project proposal, `http://www.merkle.com/1974`.