Quantum Period Finding is Compression Robust

Alexander May Lars Schlieper

Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany

download the full paper

Introduction

We study quantum period finding algorithms. For a periodic function f these algorithms produce -- via some quantum embedding of f -- a quantum superposition $\sum_x |x\rangle |f(x)\rangle$, which requires a certain amount of output qubits that represent $|f(x)\rangle$. We show that one can lower this amount to a single output qubit by hashing f down to a single bit in an oracle setting. Namely, we replace the embedding of f in quantum period finding circuits by oracle access to several embeddings of hashed versions of f. We show that on expectation this modification only doubles the required amount of quantum measurements, while significantly reducing the total number of qubits.

Simon's problem

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. We call f a *Simon function* if there exists some period $\mathbf{s} \in \mathbb{F}_2^n \setminus \mathbf{0}$ such that for all $\mathbf{x} \neq \mathbf{y} \in \mathbb{F}_2^n$ we have

$$f(\mathbf{x}) = f(\mathbf{y}) \Leftrightarrow \mathbf{y} = \mathbf{x} + \mathbf{s}.$$

In *Simon's problem* we have to find $\mathbf{s}$ given oracle access to f.

It is well-known that Simon's algorithm finds $\mathbf{s}$ in time polynomial in n on quantum devices [3].

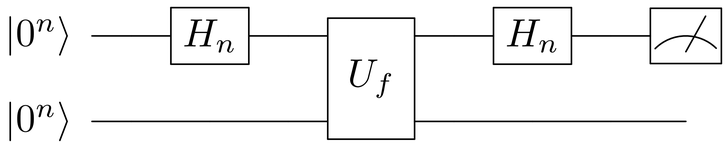

Figure: Quantum circuit to Simon's algorithm.

Conclusion

We hash in our oracle model for Simons's algorithm $f(x)$ in the output qubits down to t qubits, where t can be as small as 1. Our basic observation is that hashing preserves the periodicity of f. The drawback of hashing is of course that h introduces many more undesirable collisions $h(f(x)) = h(f(x'))$ where x, x' are not a multiple of s apart. Surprisingly, even for 1-bit range hash functions this plethora of undesirable collisions does not at all affect the correctness of our hashed quantum period finding algorithms, and only insignificantly increases their runtimes.

These uniform probability distributions are destroyed by moving to the hashed version of the algorithms. We show that if the probability to measure $y \neq \mathbf{0}$ is $p(y)$ when using f, then we obtain probability $p(y)/2$ (taken over the random choice of h from a family of universal hash functions) to measure y when using $h \circ f$. If we condition on the event that we do *not* measure $y = \mathbf{0}$ in the input bits in both cases -- using f itself or its hashed version $h \circ f$ -- we obtain exactly the same probability distribution for the measurements of any $y \neq 0$. This implies that our hashing approach preserves not only the correctness but also the runtime analysis of any processing of the measured data in a classical post-process.

Thus, at the cost of only twice as many quantum measurements we save all but one of the output qubits. Moreover, we show that this leads to a (non-oracle) realization of the quantum Even-Mansour attack [1] with only $n + 1$ qubits.

Distribution

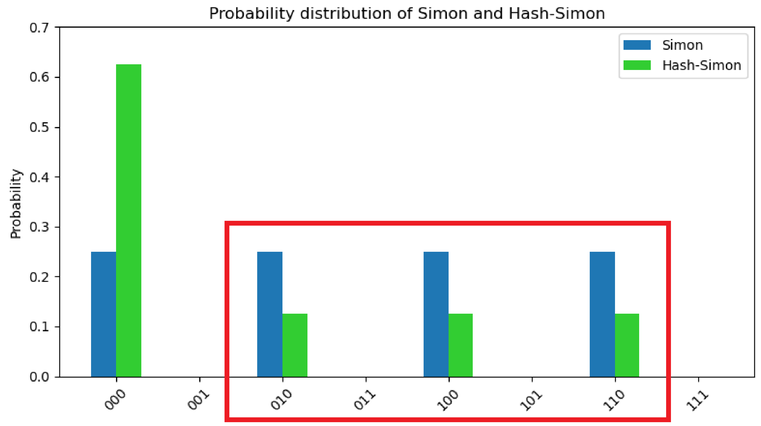

Figure: Simon Distribution for $\mathbf{s} = 001$ and hashing to 1-bit.

We measure every $y \neq \mathbf{0}$ with probability $p(y)/2$ in Hash-Simon, where $p(y)$ is the probability to measure y after Simon's circuit. The remeining probablity moves to $\mathbf{0}$. We measure $\mathbf{0}$ with probability $1/2 + p(\mathbf{0})/2$

Even Mansour example

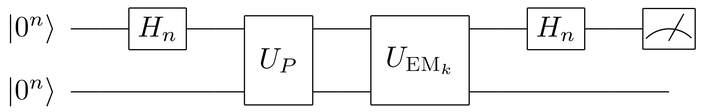

Figure: Quantum circuit for Simon-attack on Even-Mansour (EM) with permutation P.

We implement an in-place example of this attack, using the fact that the permutation and thus the Even-Mansour cipher are reversible functions. As permutation we use the SiMeck-cipher with fixed key.

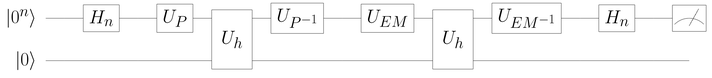

Figure: Quantum circuit Q_{HS} for a Hashed-Simon-Attack on Even-Mansour

SiMeck

We provide an in-place implementation of SiMeck, via the specification of an in-place embedding of the round function.

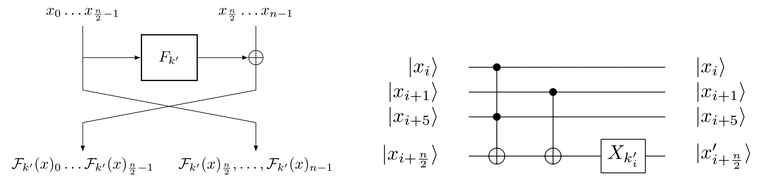

Figure: In-place implementation of the SiMeck round function.

References

[1] Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012. pp. 312--316 (2012), http://ieeexplore.ieee.org/document/6400943/

[2] May, A., Schlieper, L.: Quantum period finding is compression robust. CoRR (2019), http://arxiv.org/abs/1905.10074

[3] Simon, D.R.: On the power of quantum computation. In: FOCS. pp. 116--123. IEEE Computer Society (1994)

CASA

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES