

Quantum Cryptanalysis of Hash and Claw-Free Functions

(Invited Paper)

Gilles Brassard^{1*}, Peter Høyer^{2**}, and Alain Tapp^{1***}

¹ Université de Montréal, Département IRO

C.P. 6128, succursale centre-ville, Montréal (Québec), Canada H3C 3J7

{brassard,tappa}@iro.umontreal.ca

² Odense University, Department of Mathematics and Computer Science

Campusvej 55, DK-5230 Odense M, Denmark

u2pi@imada.ou.dk

Abstract. We give a quantum algorithm that finds collisions in arbitrary r -to-one functions after only $O(\sqrt[3]{N/r})$ expected evaluations of the function, where N is the cardinality of the domain. Assuming the function is given by a black box, this is more efficient than the best possible classical algorithm, even allowing probabilism. We also give a similar algorithm for finding claws in pairs of functions. Further, we exhibit a space-time tradeoff for our technique. Our approach uses Grover's quantum searching algorithm in a novel way.

1 Introduction

A *collision* for function $F : X \rightarrow Y$ consists of two distinct elements $x_0, x_1 \in X$ such that $F(x_0) = F(x_1)$. The *collision problem* is to find a collision in F under the promise that there is one.

This problem is of particular interest for cryptology because some functions known as *hash functions* are used in various cryptographic protocols. The security of these protocols depends crucially on the presumed difficulty of finding collisions in such functions. A related question is to find so-called *claws* in pairs of functions; our quantum algorithm extends to this task. In particular, this has consequences for the security of classical signature and bit commitment schemes.

A function F is said to be *r -to-one* if every element in its image has exactly r distinct preimages. We assume throughout this note that function F is given as a black box, so that it is not possible to obtain knowledge about it by any other means than evaluating it on points in its domain. When F is two-to-one,

* Supported in part by Canada's NSERC, Québec's FCAR, and the Canada Council.

** Supported in part by the ESPRIT Long Term Research Programme of the EU under project number 20244 (ALCOM-IT). Research carried out while this author was at the Université de Montréal.

*** Supported in part by postgraduate fellowships from NSERC and FCAR

the most efficient classical algorithm possible for the collision problem requires an expected $\Theta(\sqrt{N})$ evaluations of F , where $N = |X|$ denotes the cardinality of the domain. This classical algorithm, which uses a principle reminiscent of the birthday paradox, is reviewed in the next section.

Recently, at a talk held at AT&T, Eric Rains [8] asked if it is possible to do better on a quantum computer. In this note, we give a positive answer to this question by providing a quantum algorithm that finds a collision in an arbitrary two-to-one function F after only $\Theta(\sqrt[3]{N})$ expected evaluations.

Earlier, Simon [9] addressed the *XOR-mask problem* defined as follows. Consider a positive integer n . We are given a function $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$ and promised that either F is one-to-one or it is two-to-one and there exists an $s \in \{0, 1\}^n$ such that $F(x_0) = F(x_1)$ if and only if $x_0 \oplus x_1 = s$, for all distinct $x_0, x_1 \in \{0, 1\}^n$, where \oplus denotes the bitwise exclusive-or. Simon's problem is to decide which of these two conditions holds, and to find s in the latter case. Note that finding s is equivalent to finding a collision in the case that F is two-to-one. Simon gave a quantum algorithm to solve his problem in expected time polynomial in n and in the time required to compute F . The running time required for this task on a quantum computer was recently improved to being polynomial in the worst case (rather than in the expected case), thanks to a more sophisticated algorithm [3]. Simon's algorithm is interesting from a theoretical point of view because any classical algorithm that uses only sub-exponentially (in n) many evaluations of F cannot hope to distinguish between the two types of functions significantly better than simply by tossing a coin, assuming equal *a priori* probabilities [9, 3]. Unfortunately, the XOR-mask constraint when F is two-to-one is so restrictive that Simon's algorithm has not yet found a practical application.

More recently, Grover [6, 7] discovered a quantum algorithm for a different searching problem. We are given a function $F : X \rightarrow \{0, 1\}$ with the promise that there exists a unique $x_0 \in X$ so that $F(x_0) = 1$, and we are asked to find x_0 . Provided the domain of the function is of cardinality a power of two ($N = 2^n$), Grover gave a quantum algorithm that finds the unknown x_0 with probability at least $1/2$ after only $\Theta(\sqrt{N})$ evaluations of F .

A natural generalization of this searching problem occurs when $F : X \rightarrow Y$ is an arbitrary function. Given some $y_0 \in Y$, we are asked to find an $x \in X$ such that $F(x) = y_0$, provided such an x exists. If $t = |\{x \in X \mid F(x) = y_0\}|$ denotes the number of different solutions, Grover's algorithm can be generalized [1] to find a solution whenever it exists ($t \geq 1$) after an expected number of $\Theta(\sqrt{N/t})$ evaluations of F . Although the algorithm does not need to know the value of t ahead of time, it is more efficient (in terms of the hidden constant in the O notation) when t is known, which will be the case for most algorithms given here. From now on, we refer to this generalization of Grover's algorithm as **Grover**(F, y_0). Note that the number of evaluations of F is not polynomially bounded in $\log N$ when $t \ll N$; nevertheless Grover's algorithm is considerably more efficient than classical brute-force searching.

In the next section, we give our new quantum algorithm for solving the collision problem for two-to-one functions. We then discuss a straightforward gen-