Another Exhaustive Key Search of Common-Key Cryptosystems

Kazuo Ohta
ota@ice.uec.ac.jp
The University of Electro-Communications

Tetsuro Nishino
nishino@ice.uec.ac.jp
The University of Electro-Communications

Kazumaro Aoki
maro@isl.ntt.co.jp
NTT Communications

September 5, 2001

Abstract

In this note, we discuss quantum algorithms that finds a secret key k_0 satisfying $c = E(k_0, p)$, where an encryption algorithm, $E : \mathcal{K} \times \mathcal{P} \longrightarrow \mathcal{C}$, is publicly available, k_0 is a secret element of a key space $\mathcal{K}$, p is a given element of a plaintext space $\mathcal{P}$, and c is a given element of a ciphertext space $\mathcal{C}$.

We describe another quantum algorithm **Grover**$(H_d, 1)$ than **Grover**$(F, 1)$ under the assumption of $\mathcal{C} = \mathcal{K}$ holds and a permuation $\pi : \mathcal{C} \longrightarrow \mathcal{K}$ is given, by replacing the oracle function F by another oracle function H_d, where

$$\begin{aligned} F : \mathcal{K} \ni k \mapsto 1 \in \{0,1\} \quad &\text{iff} \quad E(k,p) = c \text{ holds, and} \\ H_d : \mathcal{K} \ni k \mapsto 1 \in \{0,1\} \quad &\text{iff} \quad \overbrace{E(E'(E'(\cdots E'}^{l_0\text{-times}}(k, \overbrace{p)\cdots), p), p), p)}^{l_0\text{-times}} \\ &= c \text{ for some } l_0 \text{ satisfying } 0 < l_0 \leq d, \text{ and } E' = \pi \circ E. \quad (1) \end{aligned}$$

Here, **Grover**$(F, 1)$ is Grover's algorithm corresponding to the usual exhaustive key search.

We estimate the running time and the success probability of the proposed one. At first, we prove that the new algorithm does not have any advantage more than the naive one under the reasonable situation, where a permutation π is selected randomly. Then we point out that there is some possibility of the trap-door common-key cryptosystems when quantum computers are available, that is, a polynomial time algorithm can break the cryptosystems with the trap-door using quantum computers.

Keywords: Grover's Algorithm, Common-Key Cryptosystem, Collision Search, Secret-Key Search.