Direct Demonstration of the Power to Break Public-Key Cryptosystems

Kenji Koyama

NTT Basic Research Laboratories
Nippon Telegraph and Telephone Corporation
3-9-11, Midori-cho, Musashino-shi, Tokyo, 180 Japan

Abstract: This paper describes a method of proving that a prover (or a cryptanalyst) really knows a secret plaintext or a new code-breaking algorithm for a particular public-key cryptosystem, without revealing any information about the plaintext or algorithm itself. We propose a secure direct protocol which is more efficient than the conventional protocols. This protocol requires only two transmissions between a prover and a verifier. A general form of the secure direct protocol is shown. The explicit forms for the RSA cryptosystem and the discrete logarithm problem are also proposed.

1. Introduction

Let an encryption function for the target public-key cryptosystem be denoted by \( C = E(M) \), where \( C \) is a ciphertext and \( M \) is the plaintext. Breaking the cryptosystem is generally defined as obtaining \( M \) from any \( C \) by computing \( E^{-1}(C) \). A cryptanalyst may succeed in breaking a cryptosystem by inventing a new efficient algorithm. He may want to convince potential buyers that he knows an efficient code-breaking method without revealing the knowledge and the value of \( M \). What protocol is needed for a trade between a doubtful cryptanalyst and a potential buyer? The protocol must be non-cheatable and revealing no-knowledge.

It was shown by [GMW, BC] that a zero-knowledge proof protocol can be constructed for all problems in NP under certain conditions. The problem of breaking public-key cryptosystems, such as the RSA system, belongs to the NP class. Especially, if the encryption function \( E \) has the homomorphism property,
the practical zero-knowledge protocols for demonstrating the breaking of public-key cryptosystems can be constructed. For example, several practical protocols have been shown for the Rabin system [FS], the RSA system [KV], the discrete logarithm problem [CEG, K]. These protocols are interactive, that is, indirect. These conventional indirect protocols (with sequential or parallel versions) require large transmission information to prevent prover's cheating. Subsequently, some researchers have presented "non-interactive" protocols to improve transmission efficiency [BFM, DMP]. However, so far there has been no general method of constructing a direct protocol for demonstrating the breaking of public-key cryptosystems. The main purpose of this paper is to show a secure direct protocol for demonstrating the breaking of public-key cryptosystems. The proposed direct protocol requires only one interaction or two transmissions between a prover and a verifier. It is more efficient than the conventional indirect protocols.

A general form of the secure direct protocol is shown in Section 2. The explicit forms for the RSA system and the discrete logarithm problem are proposed in Sections 3 and 4, respectively.

2. General Form of Direct Protocol

2.1. Protocol

Before specializing in a certain cryptographic scheme, we describe a very general form of direct protocol for demonstrating the power of breaking the public key cryptography. Hereafter, the prover (cryptanalyst) is referred to A, and the verifier (buyer) is referred to B. Protocol 1 shows prover A convinces verifier B that he knows M such that \( C = E(M) \).

[Protocol 1]

\begin{enumerate}
    \item \textit{step 1 : } A and B share random input \( C \), and agree on functions \( E, f \) and \( g \) such that
    \[
    E(M) = g(f(M)).
    \]
    \item \textit{step 2 : } A computes \( M \) from \( C \) using an efficient attacking method as
    \[
    M = E^{-1}(C),
    \]
\end{enumerate}