Efficient Shared-Key Authentication Scheme from Any Weak Pseudorandom Function*

Ryo Nojima[1], Kazukuni Kobara[2,3], and Hideki Imai[2,3]

[1] Information Security Research Center,
National Institute of Information and Communications Technology,
4-2-1 Nukui Kitamachi, Koganei-shi, Tokyo 184-8795, Japan
ryo-no@nict.go.jp
[2] Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology,
1102 Akihabara Daibiru, 1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan
{k-kobara, h-imai}@aist.go.jp
[3] Faculty of Science and Engineering,
Department of Electrical Electronics and Communication Engineering
Chuo University,
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

Abstract. One of the most widely used shared-key authentication schemes today is a challenge-response scheme. In this scheme, a function such as a message authentication code or a symmetric encryption scheme plays an important role. To ensure the security, we need to assume that these functions are included in a certain kind of functions family, e.g., a pseudorandom functions family. For example, functions such as SHA1-HMAC, DES and AES often assumed as the pseudorandom functions. But unfortunately, nobody knows that these functions are really pseudorandom functions and if not, then the security of the challenge-response scheme is not ensured any more. The common way to reduce this kind of fear is to construct the shared-key authentication scheme which can be proven secure with a weaker assumption on these functions. In this paper, we show that a *blind-challenge-response* shared-key authentication scheme which is a simple modified version of the original challenge-response authentication scheme can be constructed from a weaker cryptographic assumption known as *weak pseudorandom functions*.

1 Introduction

The challenge-response scheme is one of the most widely used shared-key authentication schemes among our lives. In this scheme, two parties, say Alice and Bob, share a secret key (shared-key) beforehand, and, when Alice wants to authenticate to Bob, Alice proves that she has a key without disclosing it entirely.

* The essential part of this paper was done when the authors were in the university of Tokyo.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 303–316, 2006.

The reason why this scheme deploys widely is that it can be implemented easily with small devices such as RFID tags, mobile phones, or even humans [7,8,9].

Intuitively, we say that a shared-key authentication scheme is secure if the adversary, say Eve, who attempts to impersonate Alice, cannot be identified as Alice by Bob. We can classify the security levels more precisely concerning the ability of Eve. The weakest one is that Eve has ability of eavesdropping the interactions between Alice and Bob before impersonation attempt. We say a shared-key authentication scheme is *secure against passive attacks* if it is secure against this type of an adversary. The stronger one is *secure against active attacks* where Eve can actively play the role of Bob, i.e., Eve can interact with Alice numerous times before the impersonation attempt. Security against active attack has been the goal of the shared-key authentication schemes [7]. In this paper, we concentrate on the shared-key authentication scheme which is secure against active attacks.

The challenge-response scheme is secure against active attacks if the function used inside has a certain property which is similar to the pseudorandom functions (PRFs). Good candidacies for the PRFs are DES, AES, or SHA1-HMAC [3]. But unfortunately, nobody knows that these functions are really PRFs and also design criteria of these functions are different from it. In fact, if these functions are not pseudorandom functions then there is a possibility that these functions embedded challenge-response scheme is not secure anymore. The common choice of reducing this kind of fear in the cryptography is to construct the shared-key authentication scheme which can be proven secure with a weaker assumption on them. For instance, consider the following recent situation. SHA1 has conjectured to be a collision-resistant hash function but it seems not [15]. As a result, security of SHA1-HMAC [3] which security was proven under this conjecture becomes danger.[1] Therefore, constructing the cryptographic schemes with a weaker assumption is important not only from the theoretical viewpoint but also from the practical viewpoint.

In this paper, we show an efficient shared-key authentication scheme which can be proven secure with a weak assumption. The scheme is a simple modified version of the challenge-response scheme, named a *blind-challenge-response* authentication scheme. The good property of this scheme is that we can construct and prove the security from any *weak PRF* (WPRF for short). The WPRF was first defined explicitly in [14] and there are many applications [1,6,10,12,13]. Highly efficient candidacies for WPRFs are described in [5]. The WPRFs are not studied extensively as PRFs, but the notion of a WPRF is substantially weaker than the notion of a PRF. Thus, potentially, there must be a lot of WPRFs compared to the PRFs.

Related works: As authors know, the blind-challenge-response authentication scheme was first appeared in [7] with a specific function. This scheme has been proposed to be suitable for small devices, such as RFID tags. The function they employ is based on the Learning Parity with Noise (LPN) problem and

[1] Later this was repaired [2].