A Family of Fast Syndrome Based Cryptographic Hash Functions

Daniel Augot[1], Matthieu Finiasz[1,2], and Nicolas Sendrier[1]

[1] Projet Codes, INRIA Rocquencourt,
BP 105, 78153 Le Chesnay - Cedex, France
{Daniel.Augot,Matthieu.Finiasz,Nicolas.Sendrier}@inria.fr
[2] LASEC, École Polytechnique Fédérale de Lausanne (EPFL),
Station 14, 1015 Lausanne, Switzerland

Abstract. Recently, some collisions have been exposed for a variety of cryptographic hash functions [20,21] including some of the most widely used today. Many other hash functions using similar constructions can however still be considered secure. Nevertheless, this has drawn attention on the need for new hash function designs.

In this article is presented a family of secure hash functions, whose security is directly related to the syndrome decoding problem from the theory of error-correcting codes.

Taking into account the analysis by Coron and Joux [4] based on Wagner's generalized birthday algorithm [19] we study the asymptotical security of our functions. We demonstrate that this attack is always exponential in terms of the length of the hash value.

We also study the work-factor of this attack, along with other attacks from coding theory, for non asymptotic range, i.e. for practical values. Accordingly, we propose a few sets of parameters giving a good security and either a faster hashing or a shorter description for the function.

Keywords: cryptographic hash functions, provable security, syndrome decoding, NP-completeness, Wagner's generalized birthday problem.

1 Introduction

The main cryptographic hash function design in use today iterates a so called compression function according to Merkle's and Damgård's constructions [6,12]. Classical compression functions are very fast [13,16] but, in general, cannot be proven secure. However, provable security may be achieved with compression functions designed following public key principles, at the cost of being less efficient. This has been done for instance by Damgård in [6], where he designed a hash function based on the Knapsack problem. Accordingly, this function has been broken by Granboulan and Joux [8], using lattice reduction algorithms. The present paper contributes to the hash function family by designing functions based on the syndrome decoding problem, which is immune to lattice reduction based attacks.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 64–83, 2005.

Unlike most other public key cryptosystems, the encryption function of the McEliece cryptosystem [10] (or of Niederreiter's version [14]) is nearly as fast as a symmetric cipher. Using this function with a random matrix instead of the usual parity check matrix of a Goppa code, a provably secure one-way function has been constructed in [1]: since there is no trapdoor, its security can be readily related to the difficulty of syndrome decoding. For instance, there is no polynomial time algorithm to decode a random code, thus there is no polynomial time algorithm to invert the compression function and/or find a collision.

However, for the practical parameters which have been proposed in [1], there is an efficient attack with a cost as low as 2^{43} (or 2^{62} depending on the set of parameters), as demonstrated by Coron and Joux [4], using Wagner's method for the generalized birthday problem [19].

The purpose of this paper is to propose updated parameters for the hash function family presented in [1]. We do not only extend the parameters to be out of reach of the Coron-Joux attack, but we also thoroughly study the asymptotical behavior of their attack. We shall establish that this attack is exponential, such that the design for the hash function is sound.

The paper is organized as follows. In Section 2, we introduce the *Fast Syndrome Based* (FSB) compression function, derived from a hard problem similar to syndrome decoding. In Section 3 we show that the security of FSB is reduced to the average case difficulty of two new NP-complete problems. Then, in Section 4, we show how the best known decoding techniques, and the new method based on Wagner's ideas, can be adapted to the cryptanalysis of our functions. From that we can evaluate the practical security and the scalability of the system. In Section 5, we propose some choices of parameters and, eventually, we compare the obtained functions with other existing constructions. For clarity of the presentation, NP-completeness proofs are postponed in the appendix.

2 The Hash Function

We present what is called the *Fast Syndrome Based* (FSB) hash function in [1].

2.1 General Construction of Hash Functions

We follow Merkle's and Damgård's design principle of hash functions [6,12]: iterating a compression function (here denoted $\mathcal{F}$), which takes as input s bits and returns r bits (with $s > r$). The resulting function is then chained to operate on strings of arbitrary length (see Fig. 1). The validity of such a design has been established [6,12], and its security is proven not worse than the security of the compression function. Therefore we will only concentrate on the security of the latter.

2.2 Description of the Compression Function

The core of the compression function is a random binary matrix $\mathcal{H}$ of size $r \times n$. The parameters for the hash function are: