

CONTRIBUTION TO: IEEE P1363

TITLE: Security Analysis of Feistel Ladder Formatting Procedure

SOURCE: Stephen M. Matyas, IBM
Mohammad Peyravian^Ψ, IBM
Allen Roginsky, IBM

DATE: March 1997

ABSTRACT:

At the November meeting of this committee a contribution [4] was submitted that showed a formatting method for encrypting a plaintext block using a block encryption algorithm (such as Elliptic Curve, RSA, DES, etc.) having a block size smaller than that of the plaintext block. In this contribution we present an analysis of the security of the scheme.

NOTICE:

This contribution has been prepared to assist the IEEE P1363 standard body. This proposal is made by the authors as a basis of discussion. This contribution should not be construed as a binding proposal on the authors or their companies. Specifically, the authors and their companies reserve the right to amend or modify the statements contained herein.

^Ψ Contact person - Mohammad Peyravian

Email: peyravn@vnet.ibm.com
Phone: +1-919-254-7576

1. Introduction

The encryption procedure presented in [4] consists of two steps: first, a formatting operation is performed on the input plaintext to produce a masked plaintext. The masking method is a reversible procedure which performs a “complete” mixing of the plaintext block such that no bit in the plaintext block can be determined unless every bit in the masked plaintext block is known. Then, a portion or all of the masked plaintext is encrypted using a block encryption algorithm (such as Elliptic Curve, RSA, DES, etc.). The formatting method is similar to a degree to the method of masking described by Bellare-Rogaway in Optimal Asymmetric Encryption [1] and by Johnson-Le-Martin-Matyas-Wilkins in the IBM method implemented in the Transaction Security System [2, 3].

A detail description of the formatting procedure is given in [4]. In this contribution, we present an analysis of the security of the scheme.

2. Overview of One-Way Hash Functions

The strength of the scheme presented in [4] relies to a large extent on the strength of the underlying hash function. In [5], Schneier states the following properties for a collision-resistant one-way hash function H that maps a message M into the output h :

1. Given M , it is easy to compute h .
2. Given h , it is hard to compute M such that $H(M) = h$.
3. Given M , it is hard to find another message M' such that $H(M) = H(M')$.
4. It is hard to find two random messages, M and M' , such that $H(M) = H(M')$.

For the sake of the analysis of the security of the proposed scheme, we give a quantitative meaning to how hard is “hard” in the above definition. For any $g \geq 1$ and any inputs

M_1, M_2, \dots, M_g only one of which is the correct value of M , it would take at least g operations (e.g., table lookup or a computation of hash function) to determine with *certainty* the correct value of any bit or bit-string in the output h . This means, that the output of the hash function gives no information about the input message.

3. Analysis of Strength of Feistel Ladder Scheme

The input PlaintextBlock is X and the Masked PlaintextBlock is Y , each of length m bits. Assume that X contains a secret value S of length s bits (where $s \leq m$) and that we encrypt n bits of Y (where $n \leq m$). Suppose that the secret value S of X is spread between L and R with s_1 secret bits in L and s_2 secret bits in R. Similarly, suppose that the encrypted (hidden) bits of Y are spread between mmL and mmR with n_1 hidden bits in mmL and n_2 bits in mmR. In this analysis, we assume that the hash function H satisfies properties 1-4 described above, and that $\|h\| = \|L\| = \|R\|$, where $\|h\|$ is the length in bits of the output produced by the hash function.

From the masking scheme it is clear that the values of s_1 , s_2 , n_1 , and n_2 are between 0 and $\|h\|$. Let's denote $s = s_1 + s_2$, $n = n_1 + n_2$, and $f = \min\{s, n\}$. We will demonstrate here that the four-iteration Feistel ladder masking procedure described in [4] is secure in a sense that the

number of operations required to determine the secret bits in the input message grows exponentially with the number of unknown bits. We will basically show that the secret bits can not be determined from the known portions of L , R , mmL , and mmR in less than 2^f operations.

First, we show that the hidden portion of Y can not be determined with certainty from the known bits of X and Y in fewer than 2^f operations.

Since there are s_1 and s_2 secret bits in L and R respectively, to determine with certainty the value of $mL = L \oplus H(R)$ from X requires at least $2^{s_1} \times 2^{s_2} = 2^s$ operations. Therefore to compute with certainty any substring of $H(mL)$ it takes at least 2^s operations. Note that $H(mL)$ can take at most $2^{\|H\|}$ possible values and that it is possible that $\|H\|$ is less than s . Yet it still takes at least 2^s operations to determine for sure which of the $2^{\|H\|}$ values of $H(mL)$ is the correct one.

Let us turn our attention now to mR . It can be obtained either from X as $R \oplus H(mL)$ or from Y as $mmR \oplus H(mmL)$. From what we know about how difficult it is to compute mL , we see that based on the information available of L and R , the value of any substring of mR can not be determined in fewer than 2^s operations from X .

If mR were computed as $mmR \oplus H(mmL)$ from Y then, similarly, its value could not be determined in fewer than 2^n operations. Therefore mR or any of its substrings can not be determined with certainty in fewer than $\min\{2^s, 2^n\} = 2^f$ operations.

Now, let us turn our attention to $mmL = mL \oplus H(mR)$. It takes at least 2^s operations to determine mL from X and at least 2^f operations to get the value of $H(mR)$. Since mL and $H(mR)$ are uncorrelated and due to the properties of the hash function described earlier, no bit string of mmL can be determined in fewer than 2^f operations.

Let us now show that the value of mmR can not be obtained in less than 2^f operations. We know that $mmR = mR \oplus H(mmL)$ and that it takes at least 2^f operations to compute each of mmL , mR . As before, using properties of our hash function H , we can claim that no bit string of $H(mmL)$, and hence of mmR , can be determined for sure in fewer than 2^f operations.

In exactly the same manner we can show that X can not be determined with certainty from Y with fewer than 2^f operations.

It is important to note that this proof would not work with only three iterations, that is, if the values of mmL and mR were saved at the bottom of Figure 2 in [4], then mR could have potentially been known under certain scenarios and then $H(mR)$ would have no uncertainty, thus making it possible to uncover some of the secret bits. Our proof relies heavily on the existence of a significant uncertainty in $H(mR)$.

3.1 Attacks Against This Scheme

No successful attack (i.e., deterministic, probabilistic, or any other) against this scheme is known at this time. In [6] Don Coppersmith describes an attack against a four-step Feistel Ladder scheme. This attack assumes that the entire value of Y is known and one needs to determine X from it. This attack does not seem to be applicable to the case of a partial encryption of X and Y as we describe it in this contribution.

References

- [1] M. Bellare and P. Rogaway, "*Optimal Asymmetric Encryption - How to Encrypt with RSA*," Eurocrypt '94 Proceedings, volume 950 of Lecture Notes in Computer Science, Sptinger-Verlag, New York.
- [2] D. Johnson, A. Le, W. Martin, S. Matyas, and J. Wilkins, "*Hybrid Key Distribution Scheme Giving Key Record Recovery*," IBM Technical Disclosure Bulletin, 37(2A), 5-16, February 1994.
- [3] D. Johnson and S. Matyas, "*Asymmetric Encryption: Evolution and Enhancements*," CryptoBytes, volume 2, number 1, Spring 1996.
- [4] D. Johnson, S. Matyas, and M. Peyravian, "*Encryption of Long Blocks Using a Short-Block Encryption Procedure*," Contribution to IEEE P1363, November 1996.
- [5] B. Schneier, "*Applied Cryptography*," 2nd edition, John Wiley & Sons Inc, 1996.
- [6] D. Coppersmith, "*Luby-Rackoff: Four Rounds is not Enough*," IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, Research Report RC 20674, December 24, 1996.