FAST CORRELATION ATTACKS ON BLUETOOTH COMBINER

Ma Weiju  Feng Dengguo
(State Key Laboratory of Information Security, the Graduate School of Chinese Academy of Sciences, Beijing 100039, China)

Abstract A simple fast correlation attack is used to analysis the security of Bluetooth combiner in this paper. This attack solves the tradeoff between the length of the keystream and the computing complexity needed to recover the secret key. We give the computing complexities of the attack algorithm according to different lengths of the known keystream. The result is less time-consuming than before. It is also shown that the security of the modified Bluetooth combiner by Hermelin and Nyberg is not significantly enhanced.

Key words Bluetooth combiner; Combiner with memory; Correlation attacks

I. Introduction

Bluetooth™ is a standard for wireless short-range connectivity specified by the Bluetooth™ special interest group in Ref.[1]. The specification defines a stream cipher algorithm $E_0$ to be used for point-to-point encryption within the Bluetooth network. The main component of the Bluetooth stream cipher algorithm is the keystream generator (Bluetooth combiner) which is derived from the well-known summation generator with four input Linear Feedback Shift Registers (LFSRs).

A simple fast correlation attack is used to analysis the security of Bluetooth combiner in this paper. The attack method is first proposed by Chepyzhov, Johansson, and Smeets in Ref.[2]. This attack solves the tradeoff between the length of the keystream and the computing complexity needed to recover the secret key. In an actual real time attack, the cryptanalysis can choose different parameters $d$ and $k$ according to the keystream bits he has received and the storage space he achieves at the precomputation step. The computing complexities of the attack algorithm are studied according to different lengths of the known keystream. We also show that the security of the modified Bluetooth combiner by Hermelin and Nyberg is not significantly enhanced. For example, if $N = 2^{60}$ keystream bits have been known, we can select $d = 2$ and $k = 16$, then the attack complexity is $2^{125}$. In the situation $d = 2$, an index table for looking-up should be worked out in the precomputation step with complexity in order of $O(N)$, and stored in a space of at most $2^{13} k(k + 2\log_2 N)$ bits. In the situation $d = 3$, fewer known keystream bits are required but more precomputation is needed. The calculation of parity checks in the precomputation step is in order of $O(N^2)$ and the storage requirement is at most $2^{19} k(k + 3\log_2 N)$ bits. For $d = 3$, $k = 4$, the required length of the keystream segment is $N = 2^{14}$, and the attack complexity is of order $2^{36}$. For $d = 3$, $k = 32$, the required length of the keystream segment is $N = 2^{16}$, and the attack complexity is of order $2^{46}$.

In Section II, The structure of Bluetooth combiner is described and previous results about its correlation properties are pointed out. The Bluetooth combiner is cryptanalyzed by a fast correlation attack in Section III and the complexity of the algorithm is given in Section IV. Brief summary is given in Section V.

II. Description of Bluetooth Combiner and Previous Work

1. Description of Bluetooth combiner

The main component of the Bluetooth stream cipher algorithm is the keystream generator (Bluetooth combiner) which is derived from the well-known summation generator with four input LFSRs. The LFSR lengths are 25, 31, 33, and 39 (128 in total), respectively, and all the feedback polynomials are primitive and have 5 nonzero terms each. All the LFSRs are regularly clocked and their binary outputs are combined by a nonlinear function with 4 bits of memory. Let $\{x_{ij}\}_{i=0}^{\infty}$ denote the output sequence of the $i$-th LFSR, $1 \leq i \leq 4$. The vector $\mathbf{x}_t = [x_{t,1} \ x_{t,2} \ x_{t,3} \ x_{t,4}]$ is the input at time $t$. The internal memory of the combiner at time $t$ consists of 4 memory bits $C = (c_1, c_2, c_3)$, where 2 carry bits $c_i = (c_{i,1}, c_{i,2})$ are defined in terms of 2 auxiliary carry bits $s_i = (s_{i,1}, s_{i,2})$. Let $\{z_{ij}\}_{i=0}^{\infty}$ denote the output sequence of the combiner. Then the output sequence of the combiner is defined by...
where $\epsilon$ is the probability $P(f = g)$ is related to $c(f, g)$ by
\[ P(f = g) = 1/2(1 + c(f, g)) \]

**Definition 1** Let $f, g : \text{GF}(2)^n \rightarrow \text{GF}(2)$ be Boolean functions. The correlation between $f$ and $g$ is
\[ c(f, g) = 2^{-n} \left( \# \{ x \in \text{GF}(2)^n \mid f(x) = g(x) \} - \# \{ x \in \text{GF}(2)^n \mid f(x) \neq g(x) \} \right) \]

Clearly, the probability $P(f = g)$ is related to $c(f, g)$ by
\[ P(f = g) = 1/2(1 + c(f, g)) \]

**Definition 2** The correlation coefficient between two binary random variables $a$ and $b$ is defined as
\[ c(a, b) = 2P(a = b) - 1 \]

**Property 1** For binary random variables $a$, $b$, and $c$, $c(a, b \oplus c) = c(a \oplus b, c)$.

The general method for solving binary systems of approximate linear equations and its application to the Bluetooth combiner are presented in Ref.[6]. The conditional correlation and maximal correlation of the Bluetooth combiner are also analyzed in Ref.[10]. Let $Wx^w = \oplus_{i=1}^{m-1} \oplus_{j=0}^{\oplus_{i=1}} w_j x_{i,j}$ and $vz^w = \oplus_{i=0}^{m-1} v_j z_j$ denote two such linear functions defined by a matrix $W$ and a vector $v$, respectively. We want to find all $W$ and $v$ such that the correlation coefficient $c(Wx^w, vz^w)$ is relatively large in absolute value. The following proposition gives some linear correlations for $m = 4$.

**Proposition 1** (Golić[6]) Let $Wx^w$ and $vz^w$ denote the output and input linear functions, respectively. Define the column weights of $W$ to be $w_j = \sum_{i=0}^{m-1} w_{i,j}$, $0 \leq j \leq m - 1$. If $W$ has the weight patterns $(4, w_1, w_2, 4)$ and $v$ has the weight patterns $(1, v_1, v_2, l)$, such that $(w_1)_2 \neq v_1$, where $(w_2)_2 = w_1 \mod 2$, the correlation coefficient between $Wx^w$ and $vz^w$ is $\pm 1/16$. Each of $2$ output linear functions with $v_2 = 0$ is correlated to $16 = 2^4$ input linear functions with $w_2 \in \{0, 4\}$. Each of $2$ output linear functions with $v_2 = 1$ is correlated to $32 = 2^5 \times 4$ input linear functions with $w_2 = 3$. There are $96$ pairs of input/output linear functions that are mutually correlated, with nonzero correlation coefficients $\pm 1/16$.

**III. A Fast Correlation Attack on Bluetooth Combiner**

In Ref.[2], a fast correlation attack is proposed which transforms the cryptanalyst’s problem into decoding a code whose information bits are a small part of the target LFSRs’ initial state. Let the $128$ initial state bits of the four LFSRs be $a_1, a_2, \ldots, a_{128}$. By Proposition 1, it is easy to know that $z_i + z_{i-2} + z_{i-3}$ is correlated to $32$ linear functions $l_i$ of the input vectors, $1 \leq i \leq 32$ with $l_i$. That is to say
\[ P(z_i + z_{i-2} + z_{i-3}, l_i(X_1, X_{i-1}, X_{i-2}, X_{i-3})) = \frac{1}{2} - \frac{1}{16}, \quad 1 \leq i \leq 32 \] (1)

Denote the correlation coefficient $\epsilon = 1/16$. 