Breaking the Stream Cipher Whitenoise

Hongjun Wu

Institute for Infocomm Research, Singapore
hongjun@i2r.a-star.edu.sg

Abstract. Whitenoise is a stream cipher with specification given at http://eprint.iacr.org/2003/249. In this paper, we show that Whitenoise is extremely weak. It can be broken by solving about 80,000 linear equations. And only about 80,000 bytes keystream are needed in the attack.

1 Introduction

The stream cipher Whitenoise was proposed at http://eprint.iacr.org/2003/249. A security evaluation has been given at http://eprint.iacr.org/2003/218. No secuirty flaw of Whitenoise has been reported.

However we notice that the stream cipher Whitenoise is extremely weak. The poorly designed non-linear function in Whitenoise fails to resist the simple crypto attack. With about 80,000 bytes keystream, we can break that cipher by solving about 80,000 linear equations. We will describe the Whitenoise in Section 2 and give our attack in Section 3.

2 The Cipher Whitenoise

The key schedule of Whitenoise generates some session key from the secret key and initialization vector. We will ignore the key schedule of Whitenoise since it is not relevant to our attack.

The sesseion key is used to encrypt only one message and it consists of the following components.

1. n, a secret interger in the range [50,99].
2. n distinct secret intergers ℓ^i $(1 \leq i \leq n)$. Each ℓ^i is a prime number not larger than 1021.
3. n subkeys s^i $(1 \leq i \leq n)$. Each s^i consists of ℓ^i bytes. The j-th byte of s^i is denoted as s^i_j $(0 \leq j \leq \ell^i - 1)$
4. a secret array S[256] that is a one-to-one mapping 8-bit-to-8-bit S-box.

Denote the key stream being generated as $Y = y_0||y_1||y_2||\cdots\cdots$, where || denotes concatenation. The key stream is generated as follows:

1. Let $z_j = s^1_{j \bmod \ell^1} \oplus s^2_{j \bmod \ell^2} \oplus s^3_{j \bmod \ell^3} \oplus \cdots s^n_{j \bmod \ell^n}$
2. The j-th byte of the keystream is given as $y_j = S[z_j]$.

3 Break the Whitenoise

There are two fatal flaws in the design of Whitenoise.

Flaw 1: The S-box leaks a lot of infomation of the subkeys. Since the 8-bit-to-8-bit S-box in Whitenoise is one-to-one mapping, so if $y_j = y_k$, then $z_j = z_k$.

Flaw 2: The secret lengths of the subkeys, the ℓ^i $(1 \le i \le n)$, are pseudo-secret information. The subkeys in Whitenoise is a subset of all the possible subkeys. In our attack, we solve for all the subkeys, then the ℓ^i $(1 \le i \le n)$ become useless.

The attack to break Whitenoise is illustrated below.

There are 172 prime numbers not larger than 1021. Denote the t^i $(1 \le i \le 172)$ as the i-th prime, i.e. $t^1 = 2$, $t^2 = 3$, $t^3 = 5$, $\cdots$, $t^{172} = 1021$. Consider all the 172 possible subkeys $\bar{s}^i$ $(1 \le i \le 172)$, and each $\bar{s}^i$ with t^i bytes. Now observe the keystream, if $y_j = y_k$, then we know that $z_j = z_k$. Consequently, we know that

$$\begin{array}{l}\bar{s}^1_{j \bmod 2} \oplus \bar{s}^2_{j \bmod 3} \oplus \bar{s}^3_{j \bmod 5} \oplus \cdots \oplus \bar{s}^{172}_{j \bmod 1021} = \\ \bar{s}^1_{k \bmod 2} \oplus \bar{s}^2_{k \bmod 3} \oplus \bar{s}^3_{k \bmod 5} \oplus \cdots \oplus \bar{s}^{172}_{k \bmod 1021}\end{array}$$

This equation leaks one byte information of the subkeys. Note that there are $2 + 3 + 5 + 7 + \cdots + 1021 = 80189$ bytes in all the subkeys. So with slightly more than 80189 such equations, we can recover all the 172 subkeys. Among these subkeys, about one hundered of them are with value 0 because in Whitenoise only n subkeys are used in the encryption. The non-zero subkeys are those being used in Whitenoise.

We note that to obtain slightly more than 80189 equations as above, we only need slightly more than 80445 bytes of keystream. To solve these linear equations, the complexity is about $2^{48.4}$. If we implement this attack on the current Pentium 4 processor, the time required to break Whitenoise is estimated to be at most a few days.

Finally we need to recover the S-box S[256]. We now know the inputs and outputs of S, it is straight forward to recover S.

4 Conclusion

Do not use the cipher Whitenoise in any application.