Distinguishing attack on FastFlex stream cipher

Orumiehchi@yahoo.com

Abstract: Fastflex is a fast and flexible stream cipher that is designed for hardware and software environments. In this article, we point out that the keystream generated from FastFlex can be distinguished from a truly random stream with probability 1 and a few output streams.

1 Brief Description of cipher [1]

The overall structure of FastFlex is given in Fig. 1. FastFlex uses a Hash Function as its core, and a 256×256 sbox as a nonlinear layer. In each round, 256 bits is generated by sbox output and this process will be continued. We don't discuss about hash core and focus on the sbox. The sbox is composed from four layers which are presented as follows:

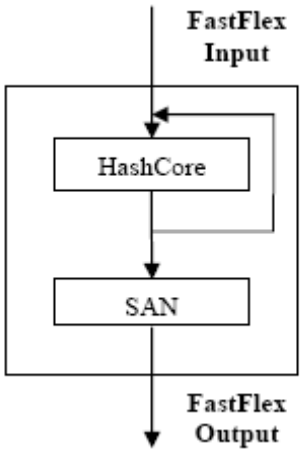

Fig.1 Structure of FastFlex

Layer 1:
A' = [A + S(B) + F]
B' = [B + S(C) + G]
C' = [C + S(D) + H]
D' = [D + S(A) + E]

Layer 2:
E' = [E + S(A')]
F' = [F + S(B')]
G' = [G + S(C')]
H' = [H + S(D')]

Layer 3:
A'' = [A' $\oplus$ S(G')]
B'' = [B' $\oplus$ S(H')]
C'' = [C' $\oplus$ S(E')]
D'' = [D' $\oplus$ S(F')]

Layer 4:
E'' = [E' + A''] $\oplus$ F'
F'' = [F' + B''] $\oplus$ G'
G'' = [G' + C''] $\oplus$ H'
H''=[H'+D'']$\oplus$E'

Where S( ) is defined as S(X) = [Qbox(X_H)$\oplus$ X] and X_H is the most significant byte of X.

2 Distinguishing Attack on Fastflex Stream Cipher

We concentrate on the randomness of layer 4, the sequences E'', F'', G'', H'' are constructed by linear and nonlinear functions (xor, modular additive), but the least significant bits in modular additive have linear relations, hence we can write a linear relation as follows:

$$\begin{aligned}
[E'']_0 &= [E']_0 \oplus [A'']_0 \oplus [F']_0 \\
[F'']_0 &= [F']_0 \oplus [B'']_0 \oplus [G']_0 \\
[G'']_0 &= [G']_0 \oplus [C'']_0 \oplus [H']_0 \\
[H'']_0 &= [H']_0 \oplus [D'']_0 \oplus [E']_0
\end{aligned} \qquad (1)$$

Where $[X]_0$ present the least significant bit of X word. With xoring the right side and left side relations, we have:

$$[E'']_0 \oplus [F'']_0 \oplus [G'']_0 \oplus [H'']_0 = [A'']_0 \oplus [B'']_0 \oplus [C'']_0 \oplus [D'']_0 \qquad (2)$$

The relation (2) is a deterministic relation and is occurred with probability 1. Therefore the generated key stream of fastflex can be distinguished from a truly random stream with a few output keystreams with probability 1.

2.1 The other biases

In addition, we can write a lot of probabilistic linear relations from layer4. For example, there are some efficient methods for determination of linear approximation of additive modular.

$$\begin{aligned}
L.E'' &= L.[E' + A'' \oplus F'] \\
L.F'' &= L.[F' + B'' \oplus G'] \\
L.G'' &= L.[G' + C'' \oplus H'] \\
L.H'' &= L.[H' + D'' \oplus E']
\end{aligned}$$

Where L is a suitable linear relation which has high bias value and (.) is internal multiplication.

3 Conclusion

In this paper, it was shown that the keystream generated from fastflex can be distinguished from a random stream with a few outputs and with probability 1. In the other word, we exposed that SAN is far from a random substitution box and more likely behaves as a non-randomly function which is not acceptable for cryptographic purposes.

4 References

[1]http://fastflex.sourceforge.net/ and
http://www.infosecwriters.com/text_resources/pdf/Cipher_Infosec.pdf