GIFT BLOCK CIPHER

Rule_Breaker

Department of <EECS>
Indian Institute of Technology Bhilai

November 27, 2020

Outline

Slide One

A decade ago, a lightweight block cipher, PRESENT, was presented at C CHES2007.

31-round SPN block cipher with 64-bit block size.Very simple design of Sbox layer and bit permutation

But it is weaker against Linear Cryptanalysis

Slide Two

In CHES2017, we present a new lightweight block cipher,improving over PRESENT, we called it — GIFT.

Due to its simplicity and natural bitslice organisation of the inner data flow, our cipher is very versatileand performs also very well on software.

Advantages of GIFT compared to PRESENT:

Slide Three

Smaller area thanks to smaller Sbox and also lesser subkey additions

better resistance against LC thanks to good choice of Sbox and bit permutation

lesser rounds

simpler and **faster key schedule**

Outline

Slide One

There are two versions of GIFT,

- GIFT-64-128 is a 28-round SPN Cipher with 64-bit size of the key.
- GIFT-128 is a 40-round SPN Cipher with 128-bit size of the key.
- Round Constant
  - Each round of GIFT Sbox have 3 Steps :- SubCells,Permutation Bits,Add Round Key.

Slide Two

SubCells :-

- Applying 16 4-bit Sboxes to every 64 nibble of the state
- Sbox

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
GS(x)	1	a	4	c	6	f	3	9	2	d	b	7	5	0	8	e

Slide Three

Permutation Bits

- Bits Permutation maps bits from nit position i of cipher state to bit position i.
- Specification of gift-64 bit permutation can be given by the formulae -: p_64(i)= 4*i$\frac{}{16+16((3*\frac{imod16}{4}+(imod4))mod4)+(imod4)}$

- Specification of gift-128 bit permutation can be given by the formulae -: p_128(i)= 4*i$\frac{}{16+32((3*\frac{imod16}{4}+(imod4))mod4)+(imod4)}$

Add round Key

- Add 32-bit round key RK to the state, RK = U||V = u15 ...u0 ||v15 ...v0.
  U and V are XORed to bit 1 and bit 0 respectively.
- Add a single bit '1' is to the most significant bit, and a 6-bit round constant C = c5 c4 c3 c2 c1 c0 is XORed to bit 3 of the first 6 nibbles.

Outline

Slide One

28 round GIFT-64 is enough to resist against DC and LC.

40 round GIFT-128 is enough to resist against DC and LC.

Slide Two

Time complexity for 14 Round attack on GIFT-64-128 is 2^{97}

Data complexity for 14 Round attack on GIFT-64-128 is 2^{63}.

Algebraic attacks are harmless to GIFT.

Outline

Slide One

The total time complexity is about 2^{97} and the data complexity is 2^{63} .

Algebraic attacks do not threaten GIFT.

Outline

Slide One

We here explained about 2 lightweight block ciphers GIFT-64 and GIFT-128.

As we know Gift cipher is an improved version of present cipher. So we used lighter Sbox then of present, removed the weakness of linear cryptanalysis of present cipher which resulted in better performances.

Slide Two

The security level of gift is far better then some of the other lightweight cipher i.e are secured against linear cryptanalysis and differential cryptanalysis.

Thanks

Team Members

- ABHAS BIND
- PRAGYANSHU KHARE
- RISHABH SINGH

Implementation Info

- Github Link: