भारतीय प्रौद्योगिकी संस्थान भिलाई • Indian Institute of Technology Bhilai •

GIFT Block Cipher

Rule_Breaker

November 2020

1 Table of Contents

- Introduction
- Specification
  - Round Function
  - Key Schedule and Round Constants
- Design
  - Designing the GIFT Permutation
  - GIFT Sbox
- Security and Performances
  - Differential and Linear Cryptanalysis
- Conclusion

2 Introduction

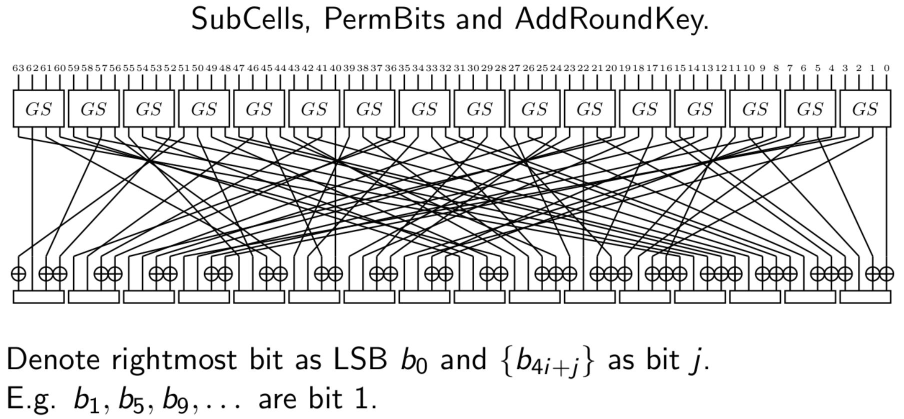
- A decade ago, a lightweight block cipher, PRESENT, was presented at CHES2007.
- 31-round SPN block cipher with 64-bit block size.Very simple design of Sbox layer and bit permutation
- But it is weaker against Linear Cryptanalysis
- In CHES2017, we present a new lightweight block cipher,improving over PRESENT, we called it — GIFT.
- Advantages of GIFT compared to PRESENT:
  - **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**

3 Specifications

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 Function**
  - Each round of GIFT Sbox have 3 Steps :- SubCells,Permutation Bits,Add Round Key.



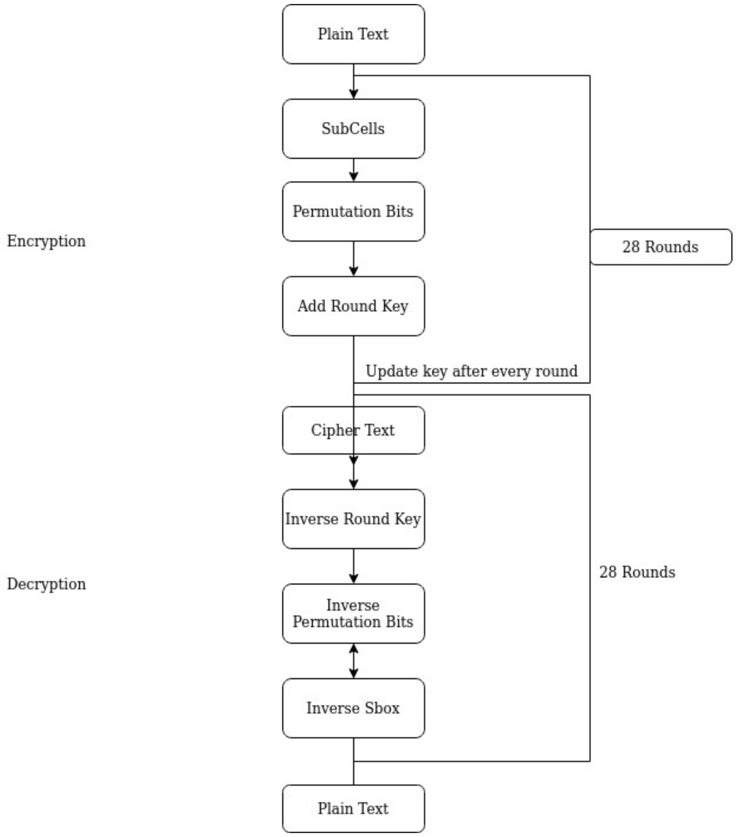
SubCells, PermBits and AddRoundKey.

Denote rightmost bit as LSB b_0 and $\{b_{4i+j}\}$ as bit j.
E.g. $b_1, b_5, b_9, \ldots$ are bit 1.

- **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

- **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 * \frac{i}{16} + 16((3 * \frac{imod16}{4} + (imod4))mod4) + (imod4)$

  $Specificationofgift-128bitpermutationcanbegivenbytheformulae- :$
  $p_(128)(i) = 4 * \frac{i}{16} + 32((3 * \frac{imod16}{4} + (imod4))mod4) + (imod4)$

– **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.

– **Round Key**

- ∗ The 128-bit key is split into 8 16-bit words. K = k7 || k6 || k5 || k4 || k3 || k2 || k1 || k0, where k i is 16-bit words.k1 and k0 are extracted as the round key RK = U||V .

- Key state is updated after key extraction.

– **Round Constant**

- Round constants are generated using a 6-bit affine LFSR with 1 XNOR gate (same as SKINNY's) is denoted as (c5,c4,c3,c2,c1,c0).

  It's update function is defined as (c5,c4,c3,c2,c1,c0) ¡—-(c4,c3,c2,c1,c0,c5 xor c4 xor1).

  Initialisation of all the 6 bits is done to 0 and are updated before their use in each round.

  The value of the constants of each round is given below in a table –:

Rounds	constants
1-16	01,03,07,0f,1f,3e,3d,3b,37,2f,1e,3c,39,33,27,0e
17-32	1d,3a,3,2b,2c,18,16,30,21,02,05,0b,17,2e,1c,38
33-48	31,23,06,0d,1b,36,2d,1a,29,34,08,24,12,22,11,04

– **GIFT SBOX CRITERIA**

- Gift sbox is relatively lighter then present sbox that is they score at least 4 for both differential and linear cases.There exists BOGI identity permutation for both differential and linear cases. For I , 0 s.t. $p(I \rightarrow O\ ) > 2$,(2) , $wt(I\ ) + wt(O\ ) > 4$.

– **DDT of GIFT SBOX**

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	2	2	0	2	2	2	2	2	0	0	2
2	0	0	0	0	0	4	4	0	0	2	2	0	0	2	2	0
3	0	0	0	0	0	2	2	0	2	0	0	2	2	2	2	2
4	0	0	0	2	0	4	0	6	0	2	0	0	0	2	0	0
5	0	0	2	0	0	2	0	0	2	0	0	0	2	2	2	4
6	0	0	4	6	0	0	0	2	0	0	2	0	0	0	2	0
7	0	0	2	0	0	2	0	0	2	2	2	4	2	0	0	0
8	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4
9	0	2	0	2	0	0	2	2	2	0	2	0	2	2	0	0
a	0	4	0	0	0	0	4	0	0	2	2	0	0	2	2	0
b	0	2	0	2	0	0	2	2	2	2	0	0	2	0	2	0
c	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2	0
d	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2
e	0	4	0	0	4	0	0	0	2	2	0	0	2	2	0	2
f	0	2	2	0	4	0	0	0	0	2	0	2	0	0	2	2

4 Security Analysis

Here we have given some cryptanalysis we have done on GIFT.

4.1 Differential and Linear Cryptanalysis

These are the two ways to test block ciphers.Finding the lower bound of the number of active Sboxes involved in differential and linear characteristic the it would be a good measure to see the stand of this cipher against these Cryptanalysis.

4.2 Integral Attacks

Here we discuss about the security against integral attacks.

Integral Distinguishers Using Division Property. First we have to find the integral distinguisher by using the (bit-based) division property.

Now we are finding the propagation of division property in GIFT Sbox. The algebraic normal form for the same is given below

$$
\begin{gathered}
y_0 = 1 + x_0 + x_1 + x_0x_1 + x_2 + x_3 \\
y_1 = x_0 + x_0x_1 + x_2 + x_0x_2 + x_3 \\
y_2 = x_1 + x_2 + x_0x_3 + x_1x_3 + x_1x_2x_3 \\
y_3 = x_0 + x_1x_3 + x_0x_2x_3
\end{gathered}
$$

and the propagation of the division property is given in below Table

Now let u and v be the input and output division property, respectively. For the cell corresponding to u and v we can see the propagation is possible if it is labelled as x . Else propagation is not possible.

Keeping in mind the bit-permutation of GIFT, we can find the propagation of the divison property on the reduced-round GIFT. To find the longest integral distinguisher , we keep only one bit in plaintext as constant , and the others are active. We can find the integral distinguishers on 9 rounds for GIFT-64, we can see using this example.

$$(A^{60}, ACAA) \ 9R \ ((UUBB)^{16})$$

In the example only 2nd bit in plaintext is constant , and (4xi)th and (4xi + 1)th bits in 9-round ciphertexts are balanced. The plaintext was not XORed with round key in first round. So we can extend integral ditinguishers by one round , and GIFT-64 has 10 round integral distinguishers.

u/v	0x0	0x1	0x2	0x4	0x8	0x3	0x5	0x9	0x6	0xA	0xC	0x7	0xB	0xD	0xE	0xF
0x0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
0x1		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
0x2		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
0x4		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
0x8		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
0x3		x	x			x	x	x	x	x	x	x	x	x	x	x
0x5			x		x	x	x	x	x	x	x	x	x	x	x	x
0x9				x	x	x	x	x	x	x	x	x	x	x	x	x
0x6				x		x	x	x	x	x	x	x	x	x	x	x
0xA				x	x	x	x	x	x	x	x	x	x	x	x	x
0xC				x	x	x	x	x	x	x	x	x	x	x	x	x
0x7							x					x	x	x	x	x
0xB									x			x	x	x	x	x
0xD					x	x	x	x		x	x	x	x	x	x	x
0xE				x			x	x	x	x	x	x	x	x	x	x
0xF																x

14-Round Attack on GIFT-64-128.

To do a 14 round attack first we append four extra rounds to the 10-round integral distinguisher as the key recovery and attack 14-round GIFT-64-128. Let $s^r i, j$ be the input to the $(r+1)th$ round function. Then, $s^1 0i, 0$ and $s^1 0_{i,1}$ are balanced for any $i \in 0, 1, ..., 16$. The attack is done using the partial-sum method.

Now we find if $s^{10}0, 0$ and $s^{10}0, 1$ are balanced from ciphertexts. To find the balancedness, we need to find the value of

$$(s^{12}15, 3, ..., s^{12}12, 3, s^{12}11, 2, ..., s^{12}8, 2, s^{12}7, 1, ..., s^{12}4, 1, s^{12}3, 0, ..., s^{12}_{0,0})$$

$(s^{12}3, 0, ..., s^{12}_{0,0})$ are computed from 16 bits in ciphertexts by guessing 16 bits . Therefore guess of 2^{16} round keys for 2^{63} ciphertexts, reduce the memory size from 2^{63} to 2^{52} , therefore time complexity is $2^{16+63} = 2^{79}$. Now for next additional 2^{16} guess of round keys for 2^{52} memory, reduce the memory size from 2^{52} to 2^{40}, and the time complexity is $2^{16\times2+52} = 2^{84}$. Now for the other 2^{16} round keys for 2^{40} memory, reduce the memory size from 2^{40} to 2^{28}, and the time complexity is $2^{16\times3+40} = 2^{88}$.

Now additional guess of 2^{16} round keys for 2^{28} memory reduce the memory size from 2^{28} to 2^{16}, and then the time complexity is $2^{16\times4+10+16} = 2^{90}$. In total the time complexity in partial sum is about 2^{92}. On doing this 16 times by changing the bit position we find the balancedness, and the total time complexity came out to be 2^{96}. So the number of possible candidates of secret key is reduced to $2^{128-32} = 2^{96}$, , and we exhaustively guess these keys.Therefore, the total time complexity is about 2^{97} and the data complexity is 2^{63} . **Differential Cryptanalysis** : For the n $-$bit block cipher to test against Differential cryptanalysis , there is some differential propagation with differential probability larger than 2^{1-n}. The differential probability can be calculated by taking the sum of probabilities of all the differential characteristics using same input and output differences.

- GIFT-64 on 9 rounds have probability of $2^{-44.415}$. So approx 28 round of GIFT-64 withstand against DC.
- GIFT-128 on 9 rounds have differential probability of $2^{-46.99}$. So approx 40 round of GIFT-128 is enough to withstand against DC.

Linear Cryptanalysis : For the n-bit block cipher to test against Linear Cryptanalysis. As we did in differential cryptanalysis , we find a optimal linear chracterstic and then fixing the input and output to find the best linear characterstics and get the sum of these correlation potentials.

- GIFT-64 on 9 round linear hull effect of $2^{-49.997}$. So approx 28 round GIFT-64 is enough to withstand against LC.
- GIFT-128 on 9 round linear hull effect of $2^{-45.99}$. So approx 40 round GIFT-64 is enough to withstand against LC.

4.3 Impossible Differential Attacks

What happens in impossible differential cryptanalysis is that it tries to exploit a pair of difference Δ_1 and Δ_2 in which the state difference Δ_1 never reaches state difference Δ_2.Many rounds were added before and after these impossible differentials.

We are given two pairs of plaintext and ciphertext with difference let ΔP , ΔC. Now what the attacker does is try to guess the subkeys for those added rounds, and apply the partial encryption/decryption to those impossible differentials. Subkeys which take to impossible differentials are found to be wrong.

In case of GIFT-64-128 it takes 3 rounds to accomplish full diffusion.

4.4 Algebraic Attacks

Algebraic attacks are not harmful for GIFT. The Sbox has algebraic degree of 3. The Sbox is also described by 21 quadraitc equations. The number of equations and variables for Algebraic attack on GIFT are very high . So due to these very high complexity of Algebraic attack GIFT is secure against it.

5 Conclusion

- 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.
- 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.

6 referece

- google,youtube,github,wikipedia.
- gift a small present towards reaching the limit of lieghtweight enryption by subhadeep banik,sumit kumar pandey .