Print Cipher

Codebreakers

Department of EECS
Indian Institute of Technology Bhilai

November 27, 2020

Outline

1 Introduction

2 Implementation

3 SECURITY ANALYSIS

4 Conclusion

IC Printing or Integrated Circuit Printing

1. Print on thin and flexible materials
2. Cheaper than silicon-based deployments
3. Main driver - Cost effective

IC printing overlap closely with the **lightweight cryptography**

One of the applications of IC-printing is in the development of cheap RFID tags.

Radio-frequency identification (RFID) tags

RFID tags are a form of tracking system.

There are three types of RFID tags :-

1. Active tag
2. Passive tag
3. Semi-passive tag

Range :

$$\text{Active tag} > \text{Passive tag} = \text{Semi-passive tag}$$

Why not conventional cryptography?

Conventional cryptographic techniques require **higher** resources.

But RFID tags have **minimal** resources, like -

- limited computation
- limited memory
- power
- small size

Why Print Cipher?

For the proper functioning of the RFID, any cipher with more significant **gate equivalence (GE)** will create a problem.

For example :

- **RSA** algorithm of 1204 bits (Not suitable)
- **PRINT Cipher** - 402 / 726 GE (Suitable)
- **EPCBC Cipher** - 1008 GE (Suitable)

Approach

Block Cipher as a starting point.

Conceptually, we need an **encryption computation** and a **subkey computation**.
Cryptanalyst in mind.

Note : If we wanted to reduce the space occupied by an implementation, then we would most likely reduce the block size.

Outline

1. Introduction
2. Implementation
3. SECURITY ANALYSIS
4. Conclusion

Implementation of PRINTcipher

1) PRINTcipher is a block cipher with b-bit blocks, b $\epsilon\{48,96\}$.

2) An effective key-length of $5/3 \times$ b is supplied to the cipher.
. b-bit as round key and rest $2b/3$ bit for key-dependent
. permutation.

One round of PRINTcipher

Each round of PRINTcipher consists of the follwing steps:

1) Bitwise xor with a round key

2) Mixed up using a fixed linear diffusion layer

3) Bitwise xor with round counter

4) Permutation of 3-bit input to S-box

5) Passing cipher state through S-box

More details about a round

1) Key Xor: Bitwise xor of the cipher state is done with a b-bit subkey(sk1) from a total of 5/3 * b-bits effective key. This subkey is identical in all rounds

2) Linear Diffusion: SP-network with b-bit block size and s-bit S-boxes:

$$P(i) = (s \times i) mod(b-1); \text{for } 0 \leq i \leq b-2;$$
$$P(i) = b-1; \text{for } i = b-1$$

In case of PRINTcipher, s = 3

$$P(i) = (3 \times i) mod(b-1); \text{for } 0 \leq i \leq b-2;$$
$$P(i) = b-1; \text{for } i = b-1$$

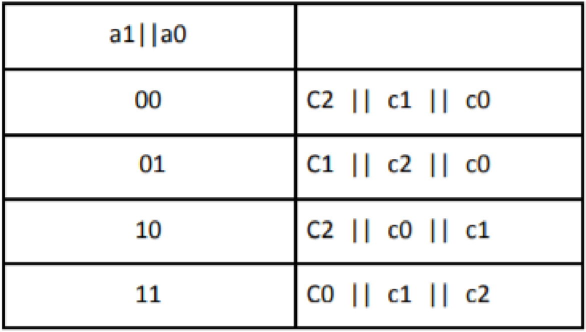
More details about a round

3) Round Counter RC_i: The round count RC_i is combined using xor to the least significant bits of the current state. The values of the round counter are generated using an n-bit shift-register (n = $[log_2 r]$) in the following way. Denote the state of the register as $X_{n-1}||......||X_1||X_0$. The shift register is initialised to all zeros and for each round round counter is computed as:

$$t = 1 + X_{n-1} + Xn - 2$$
$$X_i = X_{i-1}$$
$$X_0 = t$$

More details about a round

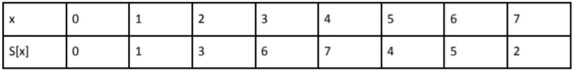
4) Keyed Permutation: The 2/3 b bits are divided into b/3 sets of two bits and each two bit quantity $a1||a0$ is used to pick one of the four available permutations. Specifically, the three input bits $c2||c1||c0$ are permuted to give the following output bits according to the value of $a1||a0$.



a1||a0	
00	C2 || c1 || c0
01	C1 || c2 || c0
10	C2 || c0 || c1
11	C0 || c1 || c2

More details about a round

5) S-box layer: A total of 3-bit to 3-bit S-box is used b/3 times in parallel. The S-box is used in the following way:



x	0	1	2	3	4	5	6	7
S[x]	0	1	3	6	7	4	5	2

Outline

1. Introduction
2. Implementation
3. SECURITY ANALYSIS
4. Conclusion

DIFFERENTIAL AND LINEAR CHARACTERSTICS

$$q=(2p\text{-}1)^2$$

p be the probability of a linear characteristic,

q be correlation of the linear characteristic

→ any differential characteristic over any S-box has a probability of at most $1/4$

→ any linear characteristic over any S-box has a correlation of at most $1/4$.

→ an s-round differential characteristic will have a probability of at most 2^{-2s}

→ any s-round linear characteristic will have a correlation of at most 2^{-2s}.

Consider the following one-round iterative characteristic (octal representation):
(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1) → (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1).
→ probability $1/4$ when the active S-box is V_0 or V_1 .
→ The iterative characteristic above has an expected probability of 2^{-24} for 12 rounds.

High Order Differentials and Algebraic Attacks

→ Algebraic degree of the S-box is 2

→ Due to the large number of 48 rounds we expect the total degree of the cipher to be close to the maximum.

For algebric attacks:

→ there exist quadracticequations over all 3-bit S-boxes, also those of PRINTcipher.

→ complicated to solve

Related-Key Attacks

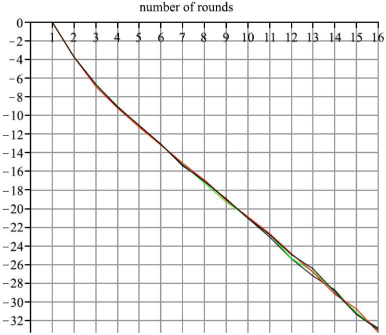
The four S-boxes in PRINT cipher are closely related.
For example, S-box 0 and S-box 1 produce the same output for each of four inputs and similarly for S-boxes 2 and 3 and for S-boxes 4 and 5
→ Consider two keys different only in the selection of one S-box, say, the leftmost one. Assume further that one key selects S-box V0 and the other key selects S-box V1.The encryption functions over s rounds can beexpected to produce identical ciphertexts for one in 2^s texts.

→ Consider two keys different only in xor halves and only in the input to one S-box.If it is assumed that there is only one active S-box in all rounds and input differnce=output difference, then one gets an s-round differential characteristic of probability 2^{-s} (for even s).

Statistical Saturation Attacks

→ The key idea is to make use of low diffusion trails in the linear layer of cipher.
→ The attack applies to reduced round versions of PRINT cipher.
→ Increasing the number of S-boxes in the trail makes estimating the complexity of the attack very complicated. Thus, in our experiments we focused only on the case of three active S-boxes in the trail.
→ The data complexity for attacking r + 3, resp. r + 4 rounds, depending on how many key bits are guessed, is approximately the reciprocal of the squared euclidian distance for r rounds.

S-boxes in the trail	$\{0,1,5\}$	$\{2,6,7\}$	$\{10,14,15\}$	$\{8,9,13\}$
Round 1	0	0	0	0
Round 2	-3.72	-3.72	-3.74	-3.73
Round 3	-6.67	-6.74	-6.89	-6.65
Round 4	-9.14	-8.98	-9.19	-9.05
Round 6	-13.08	-13.17	-13.17	-13.10
Round 8	-16.92	-17.25	-16.96	-17.10
Round 10	-21.02	-20.88	-20.87	-21.03
Round 12	-25.38	-25.33	-24.82	-24.93
Round 14	-28.72	-28.94	-29.19	-28.94
Round 16	-32.83	-33.05	-33.27	-33.00



Outline

1 Introduction

2 Implementation

3 SECURITY ANALYSIS

4 Conclusion

Conclusion

We have considered the technology of IC-printing and we have seen how it could impact the cryptography we use.

We specifically suggested the PRINT cipher lightweight block cipher, which directly takes advantage of this(IC printing) modern manufacturing strategy.

Of course, it must be stressed that PRINT cipher-48 is intended not to be appropriate for deployment, but rather to be an object of study.

Thank You...

Thanks

Team Members

- Rahul Kumar Mina(11840890)
- Prashant Kumar(11840820)
- Meghna Singh(11840710)

Implementation Info

- Github Link : https://github.com/prashantkumars289/PRINTcipher