TERM PAPER : PRIDE

Team CIPHERS

Department of Computer Science
Indian Institute of Technology Bhilai

November 27, 2020

Outline

1. Introduction
2. Cipher Specifications
3. Attacks
4. Observations
5. Brownie Point Nominations
6. Conclusion

Lightweight Cryptography

Lightweight Cryptography

- To implement the ciphers in constrained environments the lightweight ciphers were introduced.
- This means a trade off between security and efficiency, but not always.
- An effective implementation is PRIDE cipher which do not compromise security for efficiency.

Cipher PRIDE

PRIDE

- PRIDE is a lightweight block cipher introduced in CRYPTO 2014 by Albrecht et al.
- The block size and key size are 64-bit and 128-bit respectively and has 20-rounds using SPN implementation.
- PRIDE is Software-oriented for widely-used embedded microprocessors.

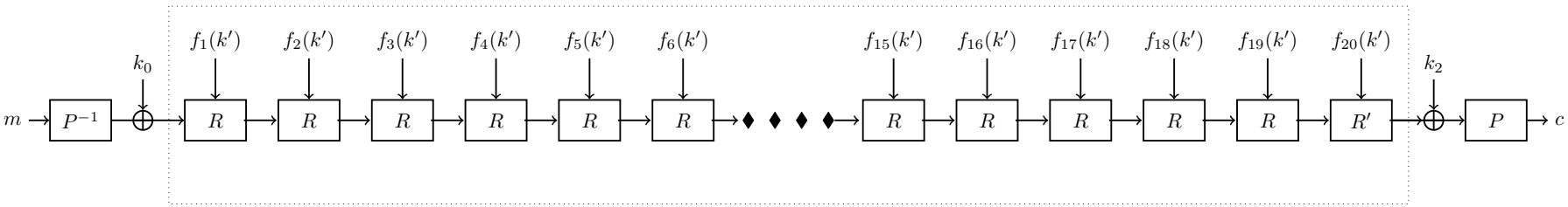

Figure: Overall Structure of PRIDE

Outline

1 Introduction

2 Cipher Specifications

3 Attacks

4 Observations

5 Brownie Point Nominations

6 Conclusion

Key-Scheduling

Master Key K of 128-bit is divided into two nibbles $k||k'$ each of 64-bit
k - Pre- and Post-whitening
k' - Key-scheduling for the round implementation

$$k' = k'_1||k'_2||k'_3||k'_4||k'_5||k'_6||k'_7||k'_8$$

These 8-bit words are used in key-schedule for generation of the Sub-keys $f_r(k')$ of different rounds as:

$$f_r(k') = k'_1||g_r^{(1)}(k'_2)||k'_3||g_r^{(2)}(k'_4)||k'_5||g_r^{(3)}(k'_6)||k'_7||g_r^{(4)}(k'_8)$$

where $1 \leq r \leq 20$ and g function.

g function in Key-Scheduling

$g_r^{(1)}(x)$	$(x + 193r)\%\ 256$
$g_r^{(2)}(x)$	$(x + 165r)\%\ 256$
$g_r^{(3)}(x)$	$(x + 81r)\%\ 256$
$g_r^{(4)}(x)$	$(x + 197r)\%\ 256$

Table: g function of PRIDE

Round Function

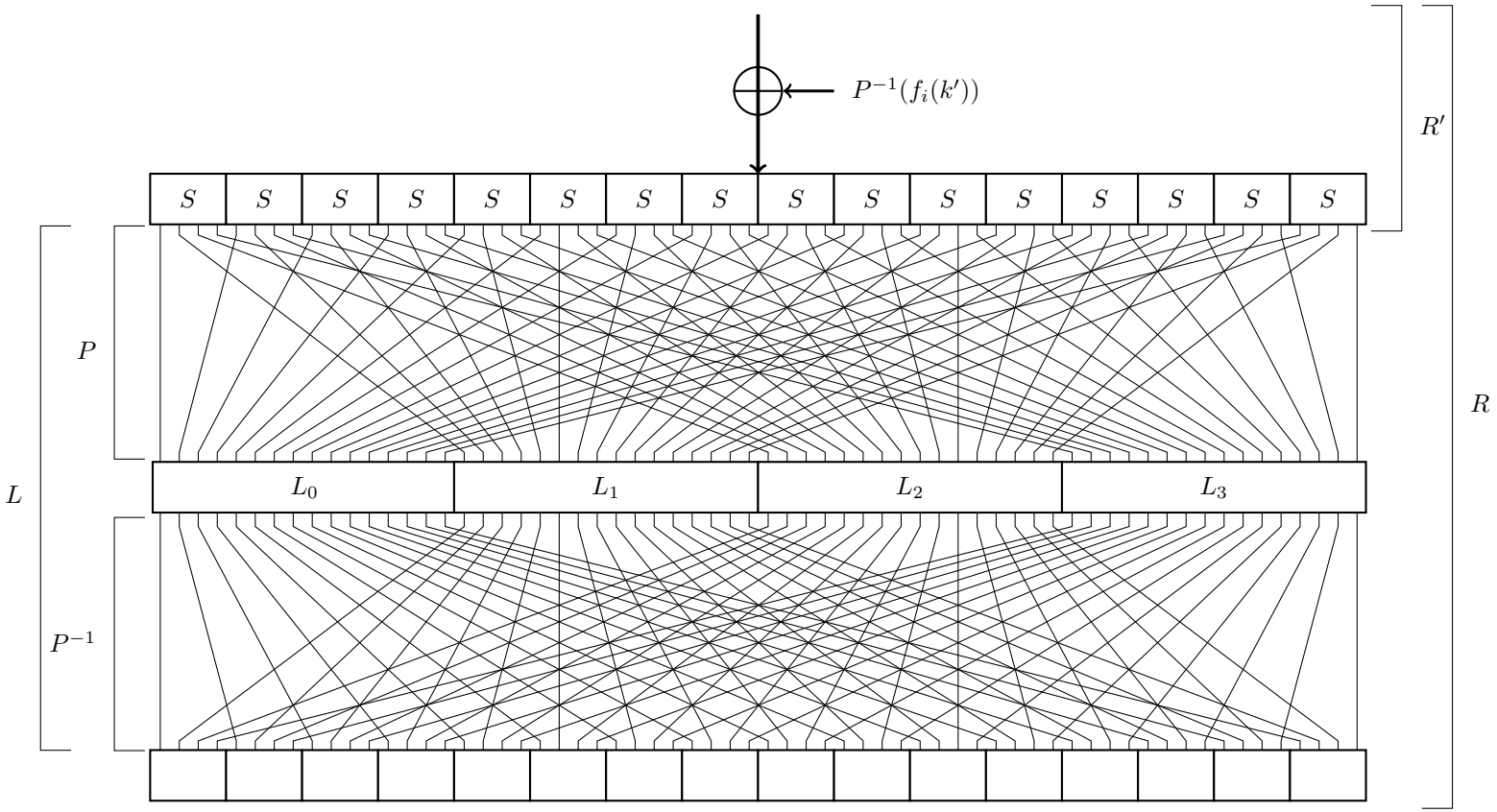

Figure: Round Function of PRIDE

Round Information

Rounds of PRIDE have different operations as given:

- Round-1 to Round-19 : Key addition, Substitution and Linear Layer
- Round-20 : Key addition and Substitution

Key-Addition

Xor-ing the round key and the input of the corresponding round.

Round Information

Substitution layer

Output after the key-addition operation is applied into a 4x4 S-Box (i.e to each nibble of the state).

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

Table: S-box of Cipher PRIDE

Round Information

Permutation layer

This consists of 3 different sub-operations

1. Application of bit permutation P.
2. Application of matrix L_i, for $i = 0, 1, 2, 3$ to the i^{th} word (16-bit) of the state.
3. Application of bit permutation P^{-1}.

LINEAR LAYER

LINEAR LAYER OF PRIDE CIPHER

- Use block interleaving construction
- Similar to s-box search of ULLrich et al
- search performed on hardware platform instead of software platform
- faster search, larger search space

LINEAR LAYER

LINEAR LAYER SEARCH ON HARDWARE

- Search in a subset of possible 16 * 16 matrices using an FPGA
- Limit number of instructions : (CLC,EOR,MOV,MOVW,CLR,SWAP,ASR,ROR,LSL)
- Limit number of used regsiters : (2 states,4 temporary registers)
- Save the matrices generating appropriate codes
- Ended up with 36 instructions for the whole linear layer..

SECURITY

SECURITY

- Linear and differential cryptanalysis performed
- Best possible linear and differential trails generated for 16 rounds.
- other attacks(zero-correlation,algebraic)
- Further security analysis encouraged..

Outline

1 Introduction

2 Cipher Specifications

3 Attacks

4 Observations

5 Brownie Point Nominations

6 Conclusion

Notation of PRIDE

I_r	r^{th} round : **input**
X_r	r^{th} round : the state after **key addition**
Y_r	r^{th} round : state after **substitution**
Z_r	r^{th} round : state after **permutation**
W_r	r^{th} round : state after **matrix layer**
O_r	r^{th} round : **output**
ΔX	$X \oplus X_0$
x	a bit have undetermined value
$X[l_1, l_2, \dots]$	state X with the nibbles $l_1, l_2, \cdots - th$ where $1 \leq l_1 < l_2 < \dots \leq 16$
$X\{m_1, m_2, \dots\}$	state X with the bits $m_1, m_2, \cdots - th$ where $1 \leq m_1 < m_2 < \cdots \leq 64$, enumerated from left to right.

Table: Notation of PRIDE

DDT

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

Table: DDT of PRIDE

18-Round Differential Attack

16 2-Round iterative differential characteristics of the form as below are found.

$$(8000000000000000) \xrightarrow{1r} (0008000800080000) \xrightarrow{1r} (8000000000000000)$$

15-Round attack

15-round differential characteristic = 7 2-round differential at the top + 1 1-round differential at the bottom
Probability of 15-round differential characteristic = $\frac{1}{2^{58}}$

18-Round attack

18-round differential attack = 1 1-round differential at the top + 15-round differential in the middle + 2 1-round differential at the bottom

Complexity of the attack

Data : 2^{60}
Time : 2^{66}
Memory : 2^{64}

Outline

1 Introduction

2 Cipher Specifications

3 Attacks

4 Observations

5 Brownie Point Nominations

6 Conclusion

ATTACKS

Proposed Complexity : $(D, T, M) = (2^{60}, 2^{66}, 2^{64})$
Round key bits and their captured layers:

- 40-bit round key is captured in 18^{th} round key layer
- 12-bit round key is captured in 17^{th} round key layer
- 12-bit round key is captured in 1^{st} round key layer

This is erroneous because the differentials in the 1st and 17th rounds were unidentified viz
$Y_1[10], Y_1[6], Y_1[2] and X_{17}[10], X_{17}[6], X_{17}[2]$.
This leads to capturing only 58 bits in place of 64 as said, which make the time complexity 2^{70} by correcting 2^{66} as it needs exhaustive search.

LINEAR LAYER

OBSERVATIONS AND IMPROVEMENTS

1. Improve hardware search,cover larger space
2. Find more efficient constructions
3. Explore trade-offs
4. Extend to different platforms(PIC,ARM,etc,)

SECURITY

OBSERVATIONS AND IMPROVEMENTS

1. Zhao et al.: Differential analysis on Block Cipher PRIDE
2. Found 16 different 2-round iterative characteristics
3. constructed several 15-round differentials
4. Based on these, launched differential attack on 18-round PRIDE
5. Data,time,and memory complexity are 2^{60} 2^{66} 2^{64}
6. Even more security analysis.

Outline

1 Introduction

2 Cipher Specifications

3 Attacks

4 Observations

5 Brownie Point Nominations

6 Conclusion

The cipher PRIDE given is analyzed for different implementations and it is found out that PRIDE performs best in terms of Security when compared to SPECK and SIMON and other lightweight block ciphers. While SPECK and SIMON outperformed PRIDE in terms of efficiency, the security level of these when ranked will be in the order of:

1. PRIDE
2. SPECK
3. SIMON

- The proposed complexity of 18-round differential attack $(D, T, M) = (2^{60}, 2^{66}, 2^{64})$ is again observed and it is found out that there are rounds where round key captures were said to be 64 in place of 58 bits. Re-evaluating the complexity we get 2^{70} in place of (2^{66}).
  So, the complexity now is $(D, T, M) = (2^{60}, 2^{70}, 2^{64})$
- Figure 1 and 2 are drawn using `\tikzlibrary` package in latex with cryptographic symbols class.

Outline

1 Introduction

2 Cipher Specifications

3 Attacks

4 Observations

5 Brownie Point Nominations

6 Conclusion

Conclusion

Using Bit-Sliced implementation our Cipher PRIDE gets benefited in many ways as:

- Speed
- Parallelization
- Constant execution time

Conclusion

- In the described complexity of the attack, it is said that 40-bits round key is captured in 18^{th} round key layer, 12-bit key in the 17^{th} round and 12-bit in 1^{st} round. This makes the time complexity 2^{64} a whole.

- This is an error because the differentials in the 1st and 17th rounds were unidentified viz $Y_1[10], Y_1[6], Y_1[2] and X_{17}[10], X_{17}[6], X_{17}[2]$. This leads to capturing only 58 bits in place of 64 as said, which make the time complexity 2^{70} by correcting 2^{66} as it needs exhaustive search.

Conclusion

- we can view the PRIDE linear layer as a strong benchmark for efficient linear layers with the given parameters and encourage others to try to beat its performance.

- Finally, we note that, despite its target being software implementations, PRIDE is also efficient in hardware. It can be considered a hardware-friendly design, due to its cheap linear and S-box layers.

- Finally, regarding PRIDE, we obviously encourage further cryptanalysis

Thanks

Team Members

- Pagidimarri Nagendar - 11840790
- Ganta Hemanth Sai Kiran - 11840500

Implementation Info

- Github Link: https://github.com/Hemanth702/CRYPTOGRAPHY–CS553/tree/master