Small-Footprint Block Cipher Design - How far can you go?

A. Bogdanov[1], L.R. Knudsen[2], G. Leander[1], C. Paar[1], A. Poschmann[1], M.J.B. Robshaw[3], Y. Seurin[3], C. Vikkelsoe[2]

[1]Ruhr-University Bochum, Germany

[2]Technical University Denmark, Denmark

[3]France Telecom R&D, France

3rd Conference on RFID Security, Malaga, 2007

Table of Contents

Motivation

Ultra Light-Weight Symmetric Cipher

Context

- Tiny computing devices in the future
- Pervasive computing becoming more common
- Known ciphers and the low-resource requirements
- $\Rightarrow$ An ultra light-weight symmetric cipher needed

Motivation
Ultra Light-Weight Block Cipher

Why a Block Cipher?

- Security properties well understood
- Sound building blocks and design principles available
- More universal
  - block cipher in e.g. CTR mode = synchronous stream cipher
- Attempt to build a block cipher with a smaller footprint than most dedicated stream ciphers

Motivation

Ultra Light-Weight Block Cipher

Basic Design Principles

- At least 64-bit block and 80-bit key
- Highly iterative and repetitive design
- $\Rightarrow$ the PRESENT block cipher!

Motivation

Existing Light-Weight Block Ciphers and PRESENT

Known Light-Weight Block Ciphers

- AES 3400 GE
- DES 3000 GE
- HIGHT 3000 GE
- serialized DES 2300 GE
- DESXL 2200 GE
- TEA 2100 GE and XTEA 2000 GE

PRESENT Block Cipher

- about 1570 GE!

Requirements

Requirements on PRESENT

- The cipher is to be implemented in hardware
- Applications with moderate security levels (80 bit)
- Small amounts of encrypted data
- Often no rekeying possible
- Metrics: 1) security, 2) area, 3) power consumption, 4) timing
- RFID authentication devices $\Rightarrow$ encryption only

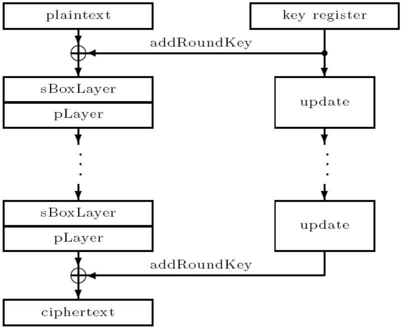
Top-Level Specification of PRESENT

PRESENT

- Extremely simple substitution-permutation network (SPN)
- 80-bit key (optionally but not recommended 128 bit)
- 64-bit block
- 16 4x4 S-boxes (16 copies of the **same** S-box!)
- simple bit permutation, no linear layers
- 31 rounds

Top-Level Specification PRESENT

generateRoundKeys()
for $i = 1$ to 31 **do**
  addRoundKey(STATE,K_i)
  sBoxLayer(STATE)
  pLayer(STATE)
end for
addRoundKey(STATE,K_{32})



S-Box Design Criteria

We denote the Fourier coefficient of S by

$$S_b^W(a) = \sum_{x \in \mathbb{F}_2^4} (-1)^{\langle b, S(x) \rangle + \langle a, x \rangle}.$$

1. For any fixed non-zero input difference $\Delta_I \in \mathbb{F}_2^4$ and any fixed non-zero output difference $\Delta_O \in \mathbb{F}_2^4$ we require
$$\#\{x \in \mathbb{F}_2^4 | S(x) + S(x + \Delta_I) = \Delta_O\} \leq 4.$$
2. For any fixed non-zero input difference $\Delta_I \in \mathbb{F}_2^4$ and any fixed output difference $\Delta_O \in \mathbb{F}_2^4$ such that $\mathrm{wt}(\Delta_I) = \mathrm{wt}(\Delta_O) = 1$ we have
$$\{x \in \mathbb{F}_2^4 | S(x) + S(x + \Delta_I) = \Delta_O\} = \emptyset.$$
3. For all non-zero $a \in \mathbb{F}_2^4$ and all non-zero $b \in \mathbb{F}_4$ it holds that $|S_b^W(a)| \leq 8$.
4. For all $a \in \mathbb{F}_2^4$ and all non-zero $b \in \mathbb{F}_4$ such that $\mathrm{wt}(a) = \mathrm{wt}(b) = 1$ it holds that $S_b^W(a) = \pm 4$.

S-box Specification and Additional Properties

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

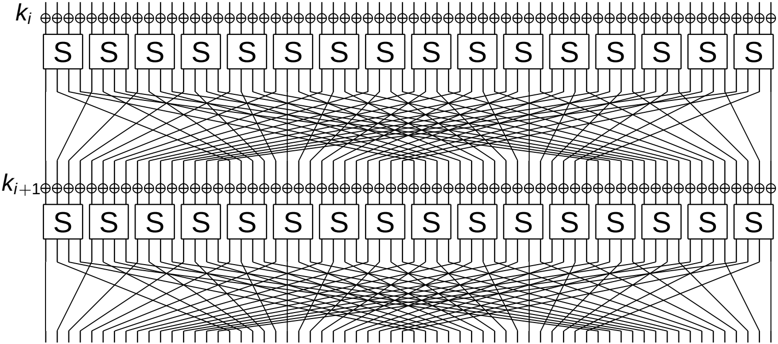
S-box Selection

- The smallest (in hardware) 4x4 S-box ...
  - ... fulfilling the criteria above (differential and linear)
  - ... having no fixed points

Permutation Layer Specification

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Permutation Layer Specification (Two Rounds)



Key Schedule Design Criteria

Criteria and Mechanisms

- Eliminate symmetry (e.g. to prevent slide attacks) $\Rightarrow$ round-dependent constants (counter)
- Some diffusion $\Rightarrow$ bit rotation
- Non-linearity and further diffusion $\Rightarrow$ S-box
- Small-footprint implementation $\Rightarrow$ recursive structure

Key Schedule Specification

Notation

- K 80-bit key register
- At round 1: $K = k_{79}k_{78}\ldots k_0$ = the 80-bit user supplied key
- At round i: The 64-bit round key $K_i = \kappa_{63}\kappa_{62}\ldots\kappa_0 = k_{79}k_{78}\ldots k_{16}$ consists of the 64 leftmost bits of the current contents of register K

Updating K after round $i = 1, 2, \ldots, 31$:

1. $[k_{79}k_{78}\ldots k_1k_0] = [k_{18}k_{17}\ldots k_{20}k_{19}]$
2. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus \texttt{round\_counter}$

Key Schedule Properties

Dependency and Algebraic Degree

- All bits in the key register are a non-linear function of the 80-bit user-supplied key by round 21,
- Each bit in the key register after round 21 depends on at least 4 of the user-supplied key bits, and
- By the time we arrive at deriving K_{32}:
  - 6 bits are degree 2 expressions
  - 24 bits are of degree 3
  - remaining bits are degree 6 and 9 functions

Differential Cryptanalysis

Theorem (5-round differential characteristic)

Any five-round differential characteristic of PRESENT has a minimum of 10 active S-boxes. EXPERIMENTS: The 5-round bound is tight.

Resistance against Differential Cryptanalysis

- Any differential characteristic over 25 rounds must have at least 50 active S-boxes
- Maximum differential probability of PRESENT is 2^{-2}
- The probability of a single 25-round characteristic is bounded by $(2^{-2})^{50} = 2^{-100}$
- $2^{100} \gg 2^{64}$ (available PT/CT pairs)
- $2^{100} \gg 2^{80}$ (key length)

Linear Cryptanalysis

Theorem (4 round linear approximation bound)

Let ϵ_{4R} be the maximal bias of a linear approximation of four rounds of PRESENT. Then $\epsilon_{4R} \leq \frac{1}{2^7}$.

Resistance against Linear Cryptanalysis

- The max. bias of a 28-round linear approximation is

$$2^6 \times \epsilon_{4R}^7 = 2^6 \times (2^{-7})^7 = 2^{-43}.$$

- About $(2^{43})^2 = 2^{86}$ known PT/CT pairs needed
- $2^{86} \gg 2^{64}$ (pairs available)
- $2^{86} > 2^{80}$ (key length)

Algebraic Cryptanalysis

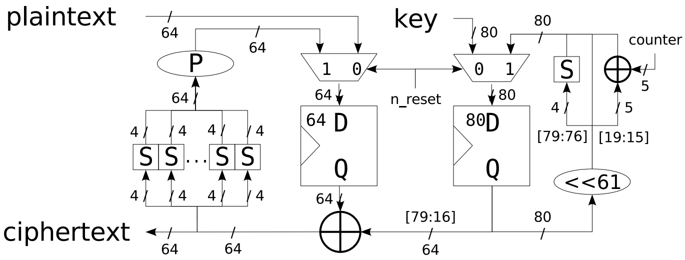
Equations

- The PRESENT 4x4 S-box can be described using 21 equations over $GF(2)$ in 8 variables (4 inputs and 4 outputs)
- $11,067$ quadratic equations in $4,216$ variables for PRESENT

Analysis

- A small-scale version analyzed
- 7 S-boxes $\Rightarrow$ 28-bit block, 2 rounds
- Buchberger and F_4 algorithms fail to deliver a solution in a reasonable time for this 2 round 28-bit PRESENT version

PRESENT Data Path Implementation



Implementation Tools

Details

- Implementation in VHDL
- Synthesized for the Virtual Silicon (VST) standard cell library based on the UMC L180 0.18μ 1P6M Logic process
- *Mentor Graphics Modelsim SE PLUS 5.8c* for simulation
- *Synopsys Design Compiler* for synthesis and power simulation
- Core voltage of 1.8 Volt and temperature of 25°C

Area Requirements of PRESENT

module	GE	%	module	GE	%
data state	**384.39**	**24.48**	**KS: key state**	**480.49**	**30.61**
s-layer	**448.45**	**28.57**	KS: S-box	28.03	1.79
p-layer	0	0	KS: Rotation	0	0
counter: state	28.36	1.81	KS: counter-XOR	13.35	0.85
counter: combinatorial	12.35	0.79	key-XOR	170.84	10.88
other	3.67	0.23			
			sum	**1569.93**	**100**

Notes

- Data state, key state and 16 S-boxes account for 83.66% of the hardware complexity
- Input/output logic not considered

Comparison of Light-Weight Cipher Implementations

	Key size	Block size	Cycles per block	Throughput at 100KHz (Kbps)	Logic process	Area	
						GE	rel.
Block ciphers							
PRESENT-80	80	64	32	200	0.18μm	1570	1
AES-128	128	128	1032	12.4	0.35μm	3400	2.17
HIGHT	128	64	1	6400	0.25μm	3048	1.65
mCrypton	96	64	13	492.3	0.13μm	2681	1.71
Camellia	128	128	20	640	0.35μm	11350	7.23
DES	56	64	144	44.4	0.18μm	2309	1.47
DESXL	184	64	144	44.4	0.18μm	2168	1.38
Stream ciphers							
Trivium	80	1	1	100	0.13μm	2599	1.66
Grain	80	1	1	100	0.13μm	1294	0.82

Conclusions

Conclusions

- Extremely hardware-efficient block cipher $\Rightarrow$ about 1570 GE
- Throughput of 200 Kbps at 100 KHz (2 bits per clock)
- Very low power consumption of 3.3μW
- Very conservative design: simple SP-network
- 80-bit key
- Further cryptanalysis needed: Try to break it!