Does Lightweight Cryptography Imply Slightsecurity?

Orr Dunkelman

Computer Science Department
University of Haifa

7th July, 2014

אוניברסיטת חיפה
University of Haifa

Outline

Lightweight Cryptography

- Targets constrained environments.
- Tries to reduce the computational efforts needed to obtain security.
- Optimization targets: size, power, energy, time, code size, RAM/ROM consumption, etc.

Why now?

Lightweight Cryptography is All Around Us

- Constrained environments today are different than constrained environments 10 years ago.
- Ubiquitous computing – RFID tags, sensor networks.
- Low-end devices (8-bit platforms).
- Stream ciphers do not enjoy the same “foundations” as block ciphers.
- Failure of previous solutions (KeeLoq, Mifare) to meet required security targets.
- Good research direction. . .

Some Lightweight Primitives

Block Ciphers	Stream Ciphers	Hash Functions	MACs
HIGHT	Grain	H-PRESENT	SQUASHSQUASH
mCrypton	Trivium	PHOTON	
DESL	Mickey	QUARK	
PRESENT	F-FCSR-HF-FCSR-H	ArmadilloArmadillo	
KATAN	WG-7	SpongeNT	
KTANTANKTANTAN	CAZAD	GLOUN	
PRINTCIPHERPRINTCIPHER		Keccak-f*	
SEA			
KleinKlein			
LBlock			
GOSTGOST			
ZORROZORRO			
TWINE			
LED			
PRINCE			
Simon			
Speck			

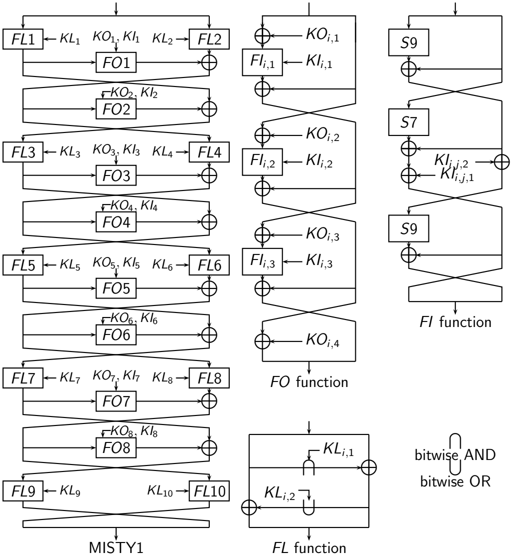
Security Challenges

- Lightweight $\Rightarrow$ pick the point on the security/performance curve with as little security margins as possible.
- Use best-of-the-art approaches:
  - Count the number of active S-boxes (wide trail),
  - Scale-down "known" ciphers (Misty1 $\rightarrow$ KASUMI, AES$\rightarrow$ LED, Zorro, DES$\rightarrow$ DESL, . . .)
  - Use "secure structures" (GFNs/AES-like/etc.)
  - Ignore related-key attacks. . .
- Use provable approaches:
  - Even-Mansour (1-Key/Multiple Key)
- As usual . . . pray.

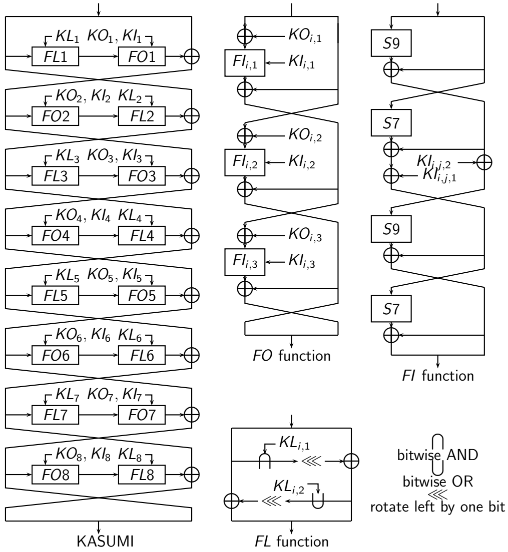
MISTY1

- Introduced by Matsui in 1997.
- 64-bit block, 128-bit key.
- Recursive structure — 8 Feistel rounds, each round function is a 3-round Feistel function.
- Each of these semi-round functions is a 3-round Feistel on its own.
- Uses 7-bit and 9-bit S-boxes for maximal nonlinearity.
- Every two rounds there is an *FL*-layer.
- Cryptrec-approved, NESSIE-portfolio, RFC, ISO.
- Predecessor of KASUMI.

MISTY1


FL1
KL1
KO1, KI1
KL2
FL2
FO1
KO2, KI2
FO2
FL3
KL3
KO3, KI3
KL4
FL4
FO3
KO4, KI4
FO4
FL5
KL5
KO5, KI5
KL6
FL6
FO5
KO6, KI6
FO6
FL7
KL7
KO7, KI7
KL8
FL8
FO7
KO8, KI8
FO8
FL9
KL9
KL10
FL10
MISTY1
KOi,1
FIi,1
KIi,1
KOi,2
FIi,2
KIi,2
KOi,3
FIi,3
KIi,3
KOi,4
FO function
S9
S7
KIi,j,2
KIi,j,1
S9
FI function
KLi,1
KLi,2
FL function
bitwise AND
bitwise OR

KASUMI


KL1 KO1, KI1
FL1 FO1
KO2, KI2 KL2
FO2 FL2
KL3 KO3, KI3
FL3 FO3
KO4, KI4 KL4
FO4 FL4
KL5 KO5, KI5
FL5 FO5
KO6, KI6 KL6
FO6 FL6
KL7 KO7, KI7
FL7 FO7
KO8, KI8 KL8
FO8 FL8
KASUMI
KOi,1
FIi,1 KIi,1
KOi,2
FIi,2 KIi,2
KOi,3
FIi,3 KIi,3
FO function
S9
S7
KIi,j,2
KIi,j,1
S9
S7
FI function
KLi,1
KLi,2
FL function
bitwise AND
bitwise OR
rotate left by one bit

KASUMI — Changes from MISTY1

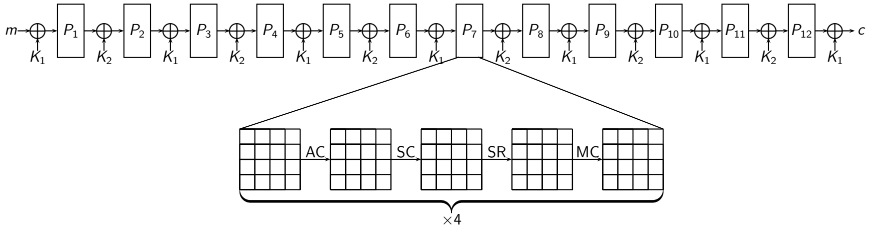
- Done by ETSI's SAGE group to fit mobile handsets.
- *FL* functions to be moved from datapath to round-path.
- One key addition reduced from the *FO* function.
- Extra *S*7 in *FI* ($\Rightarrow$ *FO* can no longer be divided into 4 parallel functions, but only 2).
- Key schedule changed significantly.

KASUMI vs. MISTY1

- In the single-key model: KASUMI $\approx$ MISTY1:
  - 6-Round Misty1 [JL12]: $2^{52.5}$ CPs, $2^{112.4}$ time.
  - 6-Round KASUMI [K12]: 2^{55} CPs, 2^{100} time.
- In the related-key model: MISTY1 $\gg$ KASUMI.
  - Practical key recovery attack against the full KASUMI ([DKS10]).
  - MISTY1: not even close (without FL, [DK13]).

The LED Block Cipher

- Introduced by [G+11].
- 64-bit block with 64-bit key (LED-64) or 128-bit key (LED-128).
- LED-64: 8-Step 1-Key Even-Mansour.
- LED-128: 12-Step 2-Key Even-Mansour.
- The "public permutation": 4-round unkeyed AES-like construction.



The LED Block Cipher (cont.)

- 48-round (12-step LED-128) offer security against differential, linear, meet-in-the-middle, ...
- No related-key issues/weakness in key schedule.
- As long as the 8-Step 1-Key Even-Mansour secure (LED-64) or 5-Step 1-Key Even-Mansour secure (LED-128).

Results on LED (Single-Key)

Source	Cipher	Steps	Time	Data	Memory
[IS12]	LED-64	2	2^{56}	2^{8} CP	2^{8}
[D+14]	LED-64	2	2^{48}	2^{16} CP	2^{17}
[D+14]	LED-64	2	2^{48}	2^{48} KP	2^{48}
[D+13]	LED-64	3	$2^{60.2}$	2^{49} KP	2^{60}
[IS12]	LED-128	4	2^{112}	2^{16} CP	2^{19}
[M+12]	LED-128	4	2^{96}	2^{64} KP	2^{64}
[NWW13]	LED-128	4	2^{96}	2^{32} KP	2^{32}
[NWW13]	LED-128	6	$2^{124.4}$	2^{59} KP	2^{59}
[D+13]	LED-128	6	$2^{124.5}$	2^{45} KP	2^{60}
[D+13]	LED-128	8	$2^{123.8}$	2^{49} KP	2^{60}

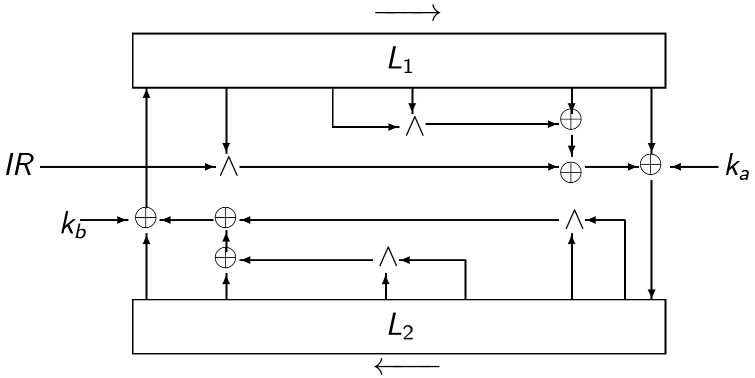
Related-Key Attacks on LED-64 [M+12]

- Find iterative characteristic $\Delta \to \Delta$ through P_i.
- Set key difference to Δ, plaintext difference to 0 ...
- 3-Step immediate related-key attack on LED-64, can be extended to 4-Step.
- 6-Step immediate related-key attack on LED-128.

The KTANTAN Block Ciphers [DDK09]

- KTANTAN has 3 flavors: KTANTAN-32, KTANTAN-48, KTANTAN-64.
- Block size: 32/48/64 bits.
- Key size: 80 bits.
- KATAN-n and KTANTAN-n are the same up to key schedule.
- In KTANTAN, the key is burnt into the device and cannot be changed.

General Structure of KATAN/KTANTAN



The KTANTAN Block Ciphers — Key Schedule

- Main problem — related-key and slide attacks.
- Solution A — two round functions, prevents slide attacks.
- Solution B — divide the key into 5 words of 16 bits, pick bits in a nonlinear manner.
- Specifically, let $K = w_4||w_3||w_2||w_1||w_0$, $T = T_7 \ldots T_0$ be the round-counter LFSR, set:

$$a_i = MUX16to1(w_i, T_7T_6T_5T_4)$$

$$k_a = \overline{T_3} \cdot \overline{T_2} \cdot (a_0) \oplus (T_3 \vee T_2) \cdot \overline{T_3} \cdot T_2 \cdot (a_4) \oplus (T_3 \vee \overline{T_2}) \cdot MUX4to1(a_3a_2a_1a_0, \overline{T_1T_0})$$

$$k_b = \overline{T_3} \cdot T_2 \cdot (a_4) \oplus (T_3 \vee \overline{T_2}) \cdot MUX4to1(a_3a_2a_1a_0, \overline{T_1T_0})$$

Security Analysis — Differential Cryptanalysis

- Computer-aided search for the various round combinations and all block sizes.
- KATAN32: Best 42-round characteristic has probability 2^{-11}.
- KATAN48: Best 43-round characteristic has probability 2^{-18}.
- KATAN64: Best 37-round characteristic has probability 2^{-20}.
- This also proves that all the differential-based attacks fail (boomerang, rectangle).

Related-Key Differentials in KATAN

- No good methodology for that.
- In KATAN32 — each key bit difference must enter (at least) two linear operations and two non-linear ones.
- Hence, an active bit induces probability of 2^{-2}, and cancels four other bits (or probability of 2^{-4} and 6).
- So if there are 76 key bits active — there are at least 16 quintuples, each with probability 2^{-2}.
- The key expansion is linear, so check minimal hamming weight in the code.
- Our analysis, so far revealed 72 as the lower bound.

Attacks on the KTANTAN Family

- [BR10] Meet in the middle attacks
  - Data: 2–3 KPs, Time: $\approx 2^{75}$, Memory: $O(1)$.
- [A11] Related-key attacks
  - Data: A few pairs of RK CPs (with 2–4 keys), Time: 2^{30}, Memory: $O(1)$.
- [W+11] Meet in the middle attacks
  - Data: 4 CPs, Time: $\approx 2^{73}/2^{74}/2^{75}$, Memory: $O(1)$.

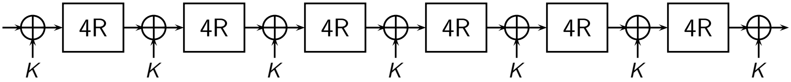
What Went Wrong?

- The key schedule.
- The bits which are chosen as the key are not "well distributed".
- For example, bit 32 of the key, does not enter the first 218 rounds...
- Other bits which are not that common also appear.
- This can be used in several ways (MitM, RK differentials).

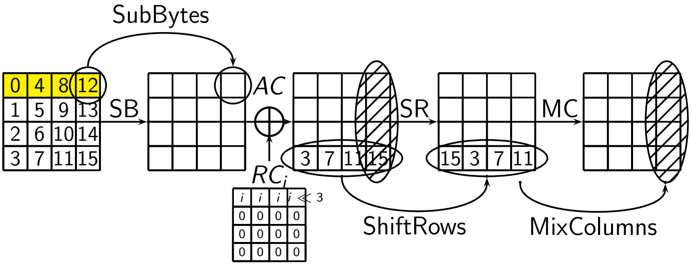
Zorro block cipher [G+13]

- Lightweight block cipher that targets side channel security.
- 128-bit block, 128-bit key.
- Single-key iterated Even-Mansour construction.
- 24 rounds, every four rounds the key is XORed to the state.
- Based on the AES

The ZORRO Block Cipher (cont.)



The ZORRO Round Function



Interesting Properties of Zorro [W+13]

- S-boxes are used only in the first row.
- Circulant matrices have interesting properties when raised to the power. Namely,

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- **So what?**

Differential/Linear Properties of Zorro [W+13]

- Consider differences/masks of the form:

$$\begin{pmatrix} a & a & a & a \\ b & b & b & b \\ c & c & c & c \\ d & d & d & d \end{pmatrix}$$

- The equality of different columns remains, up to the S-boxes.
- Which are applied only to the first row.
- So let's try to not activate it...

Our* Improvments

- Using linear algebra and solving for low number of active S-boxes, we can reduce the number of active S-boxes starting from:

$$\begin{pmatrix} a & 0 & a & 0 \\ b & e & b & e \\ c & f & c & f \\ d & g & d & g \end{pmatrix}$$

- Independently found by [R+14].

Differential/Linear Properties of Zorro (cont.)

$$\begin{pmatrix} 0 & 0 \\ 9E & 88 \\ 16 & 16 \\ AF & 95 \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 & 0 \\ 9E & 88 \\ 16 & 16 \\ AF & 95 \end{pmatrix} \xrightarrow[MC]{SR} \begin{pmatrix} 0 & 0 \\ A4 & B2 \\ 00 & 58 \\ AF & CD \end{pmatrix} \xrightarrow{SB}$$

$$\begin{pmatrix} 0 & 0 \\ A4 & B2 \\ 00 & 58 \\ AF & CD \end{pmatrix} \xrightarrow[MC]{SR} \begin{pmatrix} 0 & 0 \\ B2 & 14 \\ FE & FE \\ 33 & B9 \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 & 0 \\ B2 & 14 \\ FE & FE \\ 33 & B9 \end{pmatrix} \xrightarrow[MC]{SR}$$

$$\begin{pmatrix} \mathbf{7B} & 0 \\ 88 & 14 \\ 23 & 0 \\ 83 & 2A \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} \mathbf{7B} & 0 \\ 88 & 14 \\ 23 & 0 \\ 83 & 2A \end{pmatrix} \xrightarrow[MC]{SR} \begin{pmatrix} 0 & 0 \\ 9E & 88 \\ 16 & 16 \\ AF & 95 \end{pmatrix}$$

Summary of the Attacks

Attack	Complexity		
	Data	Time	Memory
Differential	$2^{41.5}$ CPs	2^{45}	2^{10}
Linear	2^{45} KPs	2^{45}	2^{17}

Joint work with Achiya Bar-On, Itai Dinur, Virginie Lallemand, and Boaz Tsaban.

What Went Wrong?

- Too few active S-boxes.
- Circulant matrices, which are good for implementation, may have undesirable security properties.
- Adding the key a few times — may cause some security problems.

Conclusions/Discussions

- How much are we willing to pay for security in lightweight schemes?
- What is the target for lightweight schemes optimization?
- Scale-down or "innovate"?
- Related-key attacks? Weak key schedules? How? Why? What?
- Side channel? Yes? No?

Questions?

Thank you for your attention!

謝謝