A Somewhat Historic View of Lightweight Cryptography

Orr Dunkelman

Department of Computer Science, University of Haifa
Faculty of Mathematics and Computer Science
Weizmann Institute of Science

September 29th, 2011

Outline

1 Introduction
- Lightweight Cryptography
- Lightweight Cryptography Primitives

2 The History of Designing Block Ciphers

3 The KATAN/KTANTAN Family
- The KATAN/KTANTAN Block Ciphers
- The Security of the KATAN/KTANTAN Family
- Attacks on the KTANTAN Family

4 The PRINTCIPHER
- The PRINTCIPHER Family
- Attacks on PRINTCIPHER

5 Future of Cryptanalysis for Lightweight Crypto

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.

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	SQUASH
mCrypton	Trivium	PHOTON	
DESL	Mickey	QUARK	
PRESENT	F-FCSR-H	Armadillo	
KATAN	WG-7	Spongent	
KATANTAN			
PRINTCIPHER			
SEA			
Klein			
LBlock			
GOST			

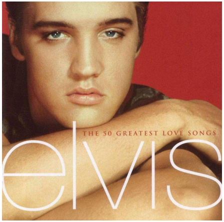
Some Lightweight Primitives

Block Ciphers	Stream Ciphers	Hash Functions	MACs
HIGHT	Grain	H-PRESENT	SQUASH
mCrypton	Trivium	PHOTON	
DESL	Mickey	QUARK	
PRESENT	F-FCSR-H	Armadillo	
KATAN	WG-7	Spongent	
KTANTAN			
PRINTCIPHER			
SEA			
Klein			
LBlock			
GOST			

Outline

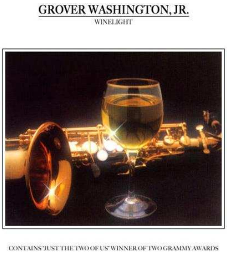
Block Cipher Design in the 1970s

- First years of academic research in the field.
- Lucifer/DES (Feistel constructions).
- Bad diffusion properties.
- Analysis methods: Meet in the middle, avalanche criteria.
- Time-Memory tradeoff presented.
- Hellman-Merkle exhaustive search machine.



Block Cipher Design/Analysis in the 1980s

- Linear factors, Linear syndrome/decoding,
- Strict avalanche criteria,
- Cycle analysis (DES is not a group),
- Non-randomness tests,
- Structure of S-boxes.
- Take DES and change something.
- FEAL...

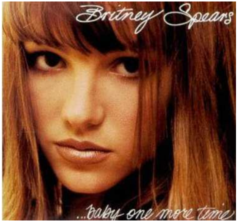


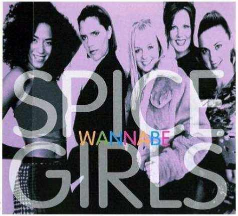
Block Cipher Design/Analysis in the 1990s

- Differential cryptanalysis [BS90].
- Linear cryptanalysis [M92].
- Related-key attacks [B93,K92].
- IPES/IDEA [LM91,LM92].
- Provable security against differential cryptanalysis/linear cryptanalysis:
  - Inversion/power S-boxes [N93,K93].
  - Counting number of active S-boxes as a measure of security.
  - Number of rounds.
  - Wide trail strategy [DR97].
  - Nicer/Cleaner proofs of security.

AES Competition

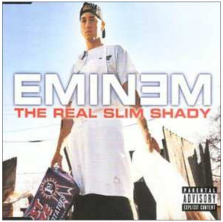
- Lots of new techniques and ideas.
- SPNs become the "leading" design.
- Boomerang, slide, related-key differentials, impossible differential cryptanalysis, . . .





Block Cipher Design in the 2000s

- Take AES.
- Tweak something.
- Do some analysis.
- Claim innovation.



Block Cipher Design/Analysis in the 2000s (cont.)

- Heavy use of wide trail.
- Ideas such as using involution round functions for SPNs (Anubis, Khazad).
- Generalized Feistels (unbalanced/switching mechanism).
- Security against related-key attacks.
- Related-key variants of other attacks, related-subkey attacks.
- AES is no longer the most secure cipher ever (but still useful for any practical purpose*).

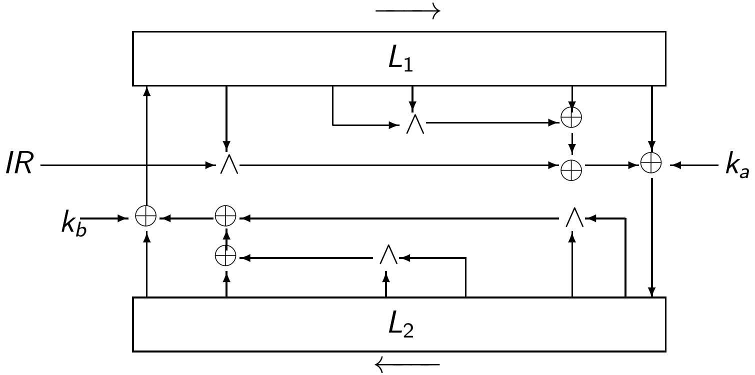
Outline

The Basic Building Blocks

- Bivium (Trivium with two registers) in a block cipher mode.
- LFSR counts rounds (rather than a counter).
- Two round functions (the one to use is controlled by a bit of the LFSR).

Joint work with Christophe De Cannière and Miroslav Knežević.

KATAN/KTANTAN Structure



The LFSR Round Counter

- When counting the number of rounds, you can use a counter.

The LFSR Round Counter

- When counting the number of rounds, you can use a counter.
- n-bit counter $\Rightarrow$ $n-1$-long carry chain.
- n-bit LFSR — a bit of control.

The LFSR Round Counter

- When counting the number of rounds, you can use a counter.
- n-bit counter $\Rightarrow$ $n-1$-long carry chain.
- n-bit LFSR — a bit of control.
- Checking end conditions: overflow in counter (carry chain longer) or special internal state (LFSR/counter).
- Another advantage: a stream of bits which is “more random”.

Two Round Functions

- *IR* is a bit which defines which of the two round functions to use.
- It toggles between two functions.

Two Round Functions

- *IR* is a bit which defines which of the two round functions to use.
- It toggles between two functions.
- Prevents any slide attacks, and increases diffusion.
- Uses the MSB of from the LFSR to pick the function.

The KATAN Block Ciphers

- KATAN has 3 flavors: KATAN-32, KATAN-48, KATAN-64.
- Block size: 32/48/64 bits.
- Key size: 80 bits.
- Share the same key schedule algorithm, and the only difference in the encryption — tap positions, and the number of times the update is done every round.
- Share same number of rounds — 254 (LFSR of 8 positions).

Key Schedule for KATAN

- Key is loaded into an 80-bit LFSR.
- Each round, the LFSR is clocked twice, and two bits are selected k_a and k_b.
- (Polynomial: $x^{80} + x^{61} + x^{50} + x^{13} + 1$).

The KTANTAN Block Ciphers

- 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.

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.

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:

$$a_i = MUX16to1(w_i, T_7 T_6 T_5 T_4)$$

$$k_a = \overline{T_3} \cdot \overline{T_2} \cdot (a_0) \oplus (T_3 \vee T_2) \cdot MUX4to1(a_4 a_3 a_2 a_1, T_1 T_0),$$
$$k_b = \overline{T_3} \cdot T_2 \cdot (a_4) \oplus (T_3 \vee \overline{T_2}) \cdot MUX4to1(a_3 a_2 a_1 a_0, \overline{T_1 T_0})$$

Security Targets

- Differential cryptanalysis — no differential characteristics with probability 2^{-n} for 127 rounds.
- Linear cryptanalysis — no approximation with bias $2^{-n/2}$ for 127 rounds.
- No related-key/slide attacks.
- No related-key differentials (probability at most 2^{-n} for the entire cipher).
- No algebraic-based attacks.

Security Analysis — Differential Cryptanalysis

- Computer-aided search for the various round combinations and all block sizes.
- KATAN32: Best 42-round charteristic has probability 2^{-11}.
- KATAN48: Best 43-round charteristic has probability 2^{-18}.
- KATAN64: Best 37-round charteristic has probability 2^{-20}.

Security Analysis — Differential Cryptanalysis

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

Security Analysis — Linear Cryptanalysis

- Computer-aided search for the various round combinations and all block sizes.
- KATAN32: Best 42-round approximation has bias of 2^{-6}.
- KATAN48: Best 43-round approximation has bias of 2^{-10}.
- KATAN64: Best 37-round approximation has bias of 2^{-11}.
- This also proves that differential-linear attacks fail.

Security Analysis — Slide/Related-Key Attacks

- Usually these are prevented using constants.
- In the case of KATAN/KTANTAN — solved by the irregular function use.
- In KATAN — the key "changes" (no slide).
- In KTANTAN — order of subkey bits not linear.

Related-Key Differentials in KATAN

- No good methodology for that.

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).

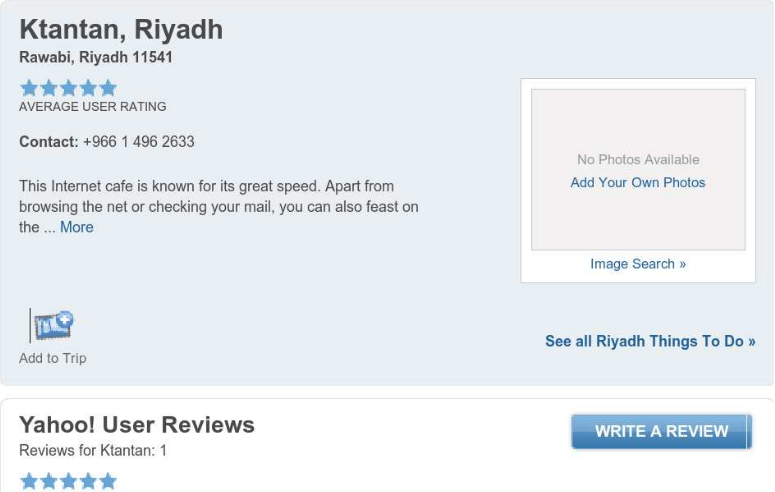
Related-Key Differentials in KATAN

- 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}.

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.

Some Views on KTANTAN



Attacks on the KTANTAN Family

- Bogdanov and Rechberger — Meet in the middle attacks (SAC'10):
  - Data: 2–3 KPs, Time: $\approx 2^{75}$, Memory: $O(1)$.
- Ågren — Related-key attacks (SAC'11):
  - Data: A few pairs of RK CPs (with 2–4 keys), Time: 2^{30}, Memory: $O(1)$.
- Wei, Rechberger, Guo, Wu, Wang, and Ling — Meet in the middle attacks (ePrint 2011/201):
  - Data: 4 CPs, Time: $\approx 2^{73}/2^{74}/2^{75}$, Memory: $O(1)$.

What Went Wrong?

- The key schedule.

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).

What to Do?

- Wait for KTANTAN-The Next Generation.
- Better key schedule.
- Even smaller footprint.
- (main idea: pick a good key schedule, e.g., KATAN's one, compute it a-priori, and burn the full "unrolled" subkey to the device)

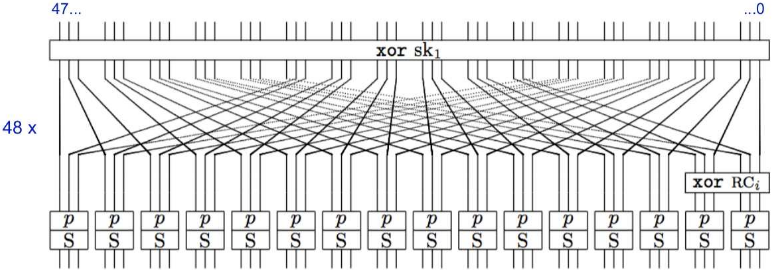
Joint work with Andrey Bogdanov, Miroslav Knežević and Christian Rechberger.

Outline

The PRINTCIPHER Family

- Two ciphers: PRINTCIPHER48, PRINTCIPHER96.
- 48-bit block/80-bit key or 96-bit block/160-bit key.
- Instead of having a key schedule — print the key into the circuit.
- The key just alters the round function.
- Solving slide attacks with a round counter.
- Uses 3x3 S-boxes, bit re-ordering, and that's about it.

The PRINTCIPHER Family



Attacks on PRINTCIPHER

- A subspace attack:
  - A large class of weak keys, for which the round function copies some subspace of the values to itself.

Attacks on PRINTCIPHER

- A subspace attack:
  - A large class of weak keys, for which the round function copies some subspace of the values to itself.
  - In other words: A few bits of the ciphertext are equal to the bits of the plaintext.

Attacks on PRINTCIPHER

- A subspace attack:
  - A large class of weak keys, for which the round function copies some subspace of the values to itself.
  - In other words: A few bits of the ciphertext are equal to the bits of the plaintext.
  - Simple distinguishers.

Attacks on PRINTCIPHER

- A subspace attack:
  - A large class of weak keys, for which the round function copies some subspace of the values to itself.
  - In other words: A few bits of the ciphertext are equal to the bits of the plaintext.
  - Simple distinguishers.
  - Many such weak keys (2^{52} for PRINTCIPHER-48 and 2^{102} for PRINTCIPHER-96).

What Went Wrong?

- Mixing.

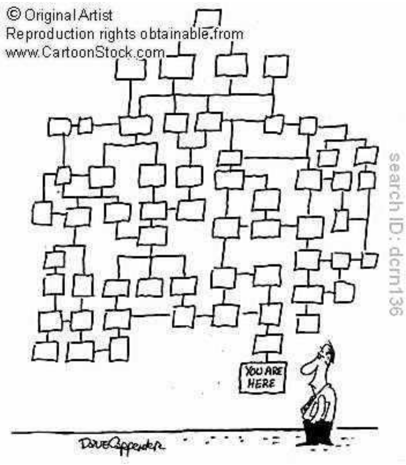
What Went Wrong?

- Mixing.
- The update is too local, and effects of changing a bit do not necessarily propagate.
- Topped with a fixed point for the other bits (partial fix-point), subspace issues arise.

Outline

Current State of Affairs

- We forgot the "old" traditions and ways of building crypto.
- We care more about differential/linear cryptanalysis mitigation than "good ol'" techniques.
- No one* really uses (or trusts) statistical tests.
- We do not have an available test suite for checking these "simple" problems.

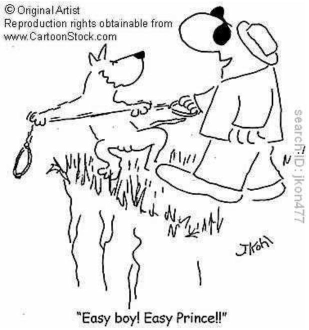


Roadmap — Towards Mathematically Sound LW Ciphers

- Revive Avalanche Criteria/Strict Avalanche Criteria tests.
- Statistical testing, statistical testing, statistical testing.
- New and open tools for automatic analysis.
- Starting to focus (again) on restricted adversaries.

Roadmap — Towards Mathematically Sound LW Ciphers

- Revive Avalanche Criteria/Strict Avalanche Criteria tests.
- Statistical testing, statistical testing, statistical testing.
- New and open tools for automatic analysis.
- Starting to focus (again) on restricted adversaries.
- We should not forget the newer techniques. . .



Questions?

Thank you for your attention!

Questions?

Thank you for your attention!

and happy new 5772!