Old Attacks and Tricks on New Lightweight Designs or Oops I've Broke it Again

Orr Dunkelman

Computer Science Department
University of Haifa, Israel

September 19th, 2018

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 5, 10, or 15 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.
- Memory encryption needs low latency solutions.
- Good research direction...

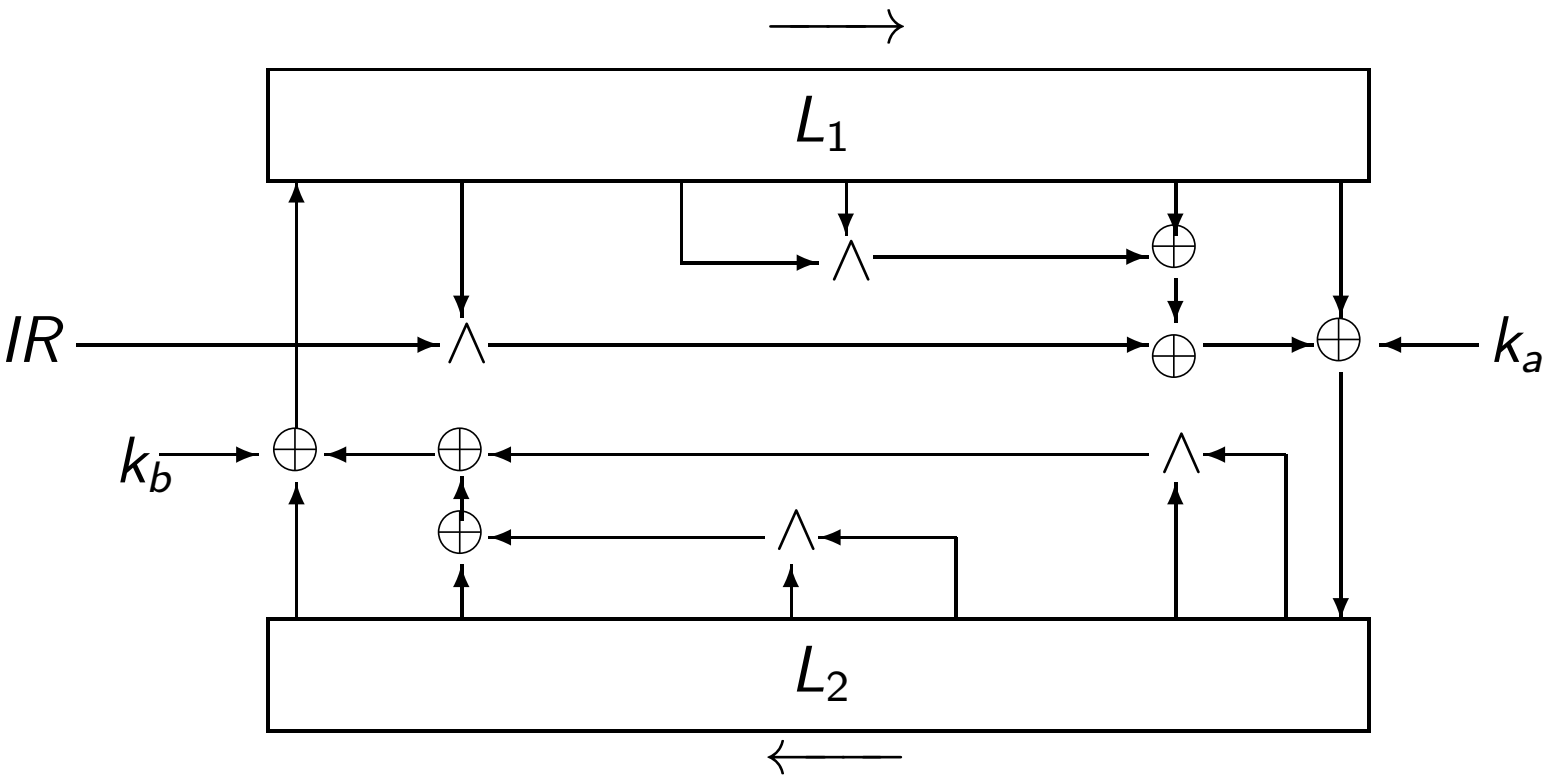
Security Challenges

- 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/
  - Ignore related-key attacks...
- Use provable approaches:
  - Even-Mansour (1-Key/Multiple Key)
  - FX-construction
  - Permutation-based (Duplex Monkey, Simp ...)
- As usual ... pray.

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 Design of KTANTAN — 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:

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

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

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

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

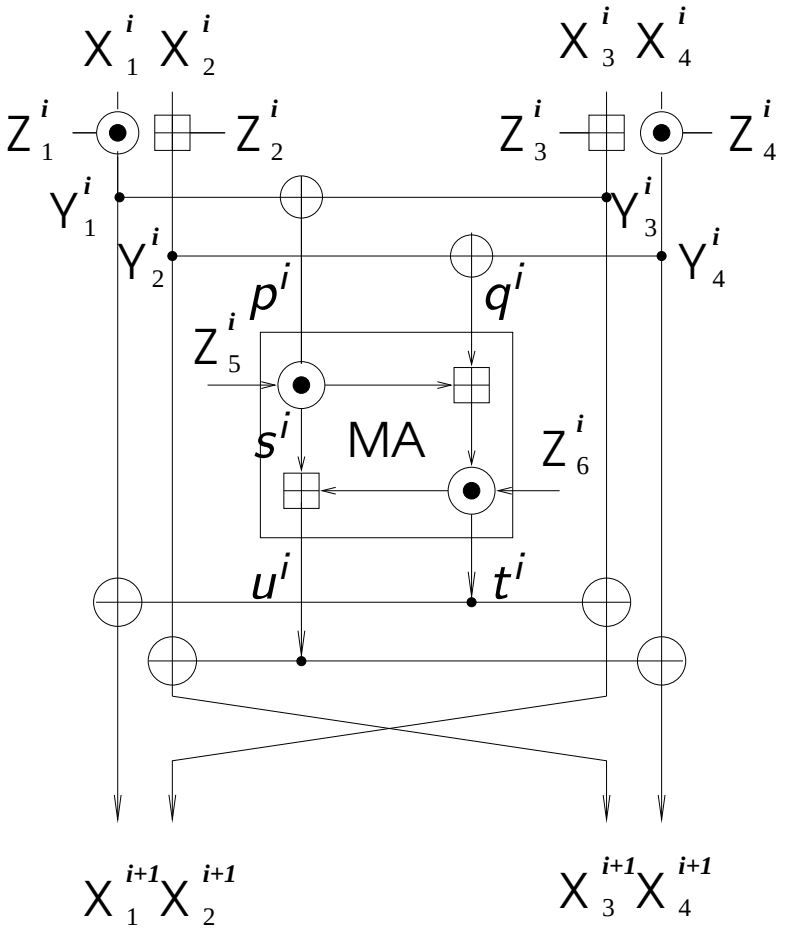
- Data: 4 CPs, Time: $\approx 2^{73}/2^{74}/2^{75}$, Memory: $O(1)$.

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 also not "uniform".
- This can be used in several ways (MitM, RK differentials).

The IDEA Block Cipher [LM91]

- 64-bit block, 128-bit key block cipher
- Presented by Lai and Massey in 1991
- Widely used in many applications
- Has 8.5 rounds
- A "red cape" for cryptanalysts — Many papers. No real break.



The $\odot$ Operation

- $\odot$ is multiplication over $GF(2^{16}+1)$, i.e., $A \odot B = (A \cdot B) \bmod 2^{16}+1$.
- But $0 \cdot B \equiv 0 \bmod 2^{16}+1$!
- Before applying $\odot$, any operand equal to zero is "transformed" into 2^{16}.
- If $A' \cdot B' \equiv 2^{16} \bmod 2^{16}+1$, then the output is set to 0.
- An efficient implementation:

```
int ideamult(a,b) {
    int c1 = a*b;
    if (c1) return ((c1%0x10001)&0xFFFF);
    return ((1-a-b)&0xFFFF);
}
```

Key Schedule of IDEA

- Subkeys are 16 consecutive bits of the key.
- A 128-bit register is initialized with the key. To generate the next subkey, the next 16 bits are taken. After 8 of these, the register is rotated to the left by 25 bits.

Round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
$i = 1$	0–15	16–31	32–47	48–63	64–79	80–95
$i = 2$	96–111	112–127	25–40	41–56	57–72	73–88
$i = 3$	89–104	105–120	121–8	9–24	50–65	66–81
$i = 4$	82–97	98–113	114–1	2–17	18–33	34–49
$i = 5$	75–90	91–106	107–122	123–10	11–26	27–42
$i = 6$	43–58	59–74	100–115	116–3	4–19	20–35
$i = 7$	36–51	52–67	68–83	84–99	125–12	13–28
$i = 8$	29–44	45–60	61–76	77–92	93–108	109–124
$i = 9$	22–37	38–53	54–69	70–85		

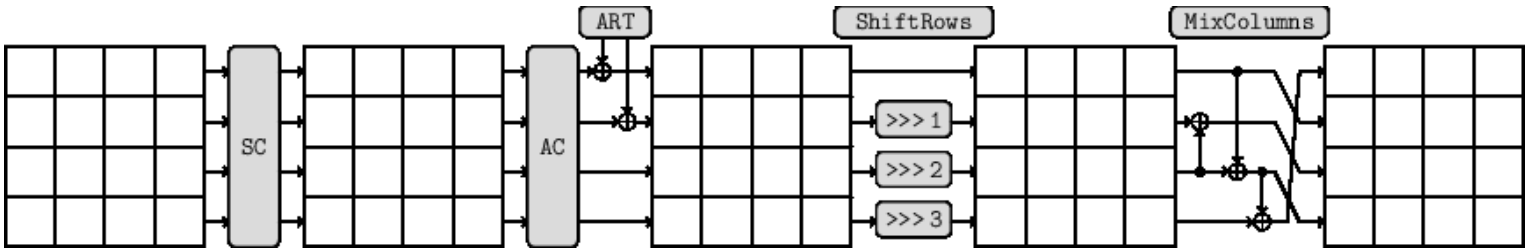
The Evolution of Attacks against IDEA

Rounds	Attack Type	Data	Time
2	Differential [M93]	2^{10} CP	2^{40}
2.5	Differential [M93]	2^{10} CP	$2^{104.7}$
3	Differential-Linear [BKR97]	2^{29} CP	2^{44}
3.5	Differential [BKR97]	2^{56} CP	2^{67}
4	Impossible Differential [BBS99]	$2^{36.6}$ CP	$2^{66.6}$
4.5	Impossible Differential [BBS99]	2^{64} KP	$2^{110.4}$
5	Demirci-Selçuk-Türe [DST06]	$2^{24.6}$ CP	2^{124}
5	ZitM BD-relation [BDK06]	2^{19} KP	2^{103}
5.5	ZitM BD-relation [BDK07]	2^{32} CP	$2^{126.85}$
5.5	Key-dependent Linear [L09]	2^{21} CP	$2^{112.1}$
6	Key-dependent Linear [L09]	2^{49} CP	$2^{112.1}$
6	MitM BD-relation [B+11]	2 KP	$2^{123.4}$
6	MitM BD-relation [B+11]	16 KP	$2^{111.9}$
6.5	SaC MitM BD-relation [B+11]	2^{10} CP	2^{122}

The SKINNY Family [B+16]

- Family of tweakable block ciphers with 64-bit or 128-bit blocks.
- Follows the TWEAKEY framework (supports tweaks of n, $2n$, or $3n$ bits).
- AES-like structure up to two main differences:
  - Tweakey is added to two rows out of four.
  - MixColumns is very very light.
- S-box very light.

The SKINNY Family [B+16]



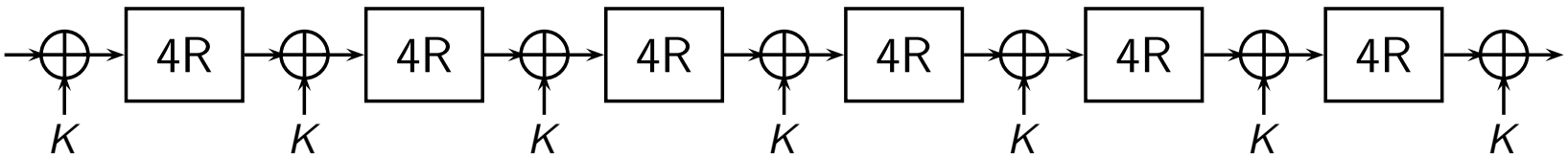
The SKINNY Cryptanalysis Competition

- 2016–2017: Attack as many rounds as possible (23-round SKINNY-64-128 under related tweakey, 20 rounds under related-key model).
- 2017–2018: Attack as many rounds as possible (23-round attack improved).
- 2018–2019: 2^{20} known plaintexts. Currently, best results are on 12-round SKINNY-64-128 and 10-round SKINNY-128-128). Probably found through meet in the middle.

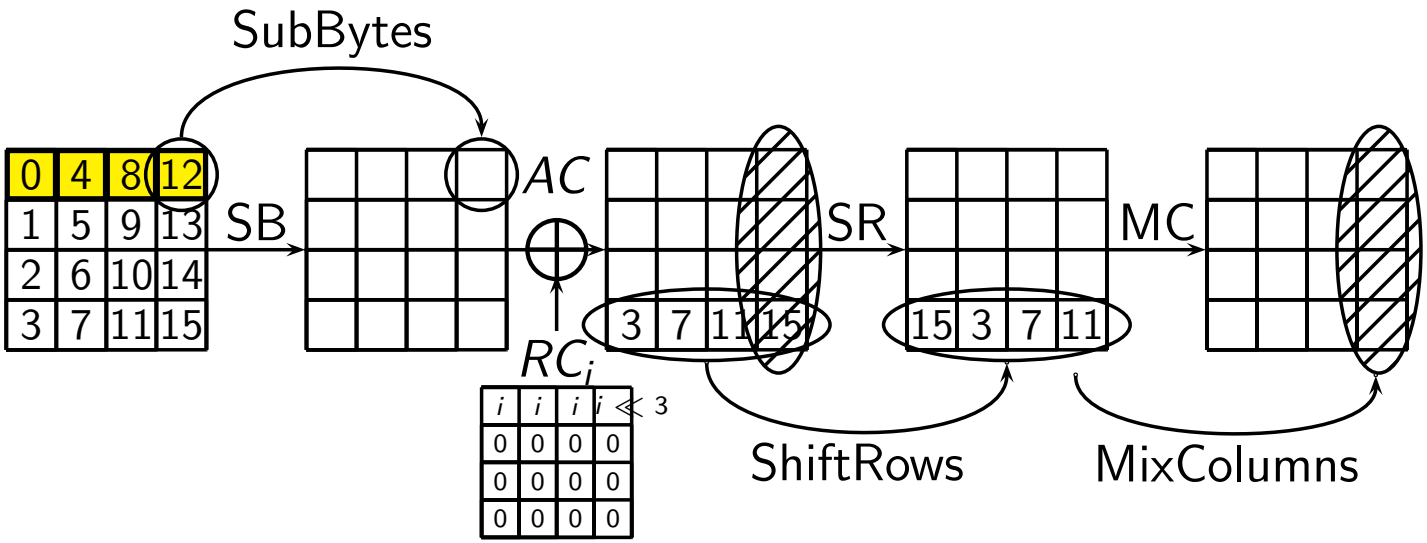
Zorro block cipher [G+13]

- 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...

Differential/Linear Properties of Zorro (cont.)

$$\begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 \\ c \\ d \\ e \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 \\ c \\ d \\ e \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 \\ f \\ 0 \\ g \end{pmatrix} \xrightarrow{SB}$$

$$\begin{pmatrix} 0 \\ f \\ 0 \\ g \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} \mathbf{h} \\ i \\ j \\ k \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} \mathbf{h} \\ i \\ j \\ k \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix} \xrightarrow{AK} \begin{pmatrix} 0 \\ a \\ 0 \\ b \end{pmatrix}$$

Implications [W+13]

- Using the iterative characteristic it is possible to devise:
  - Differential attack (20-round characteristic, $2^{-108.3}$ probability, 4-R attack, $2^{112.4}$ CPs, $2^{112.4}$ time).
  - Linear distinguisher (24-round characteristic, $2^{-52.62}$ bias, 0-R attack, $2^{105.3}$ KPs).

Possible Improvements

- The mask can be changed a bit, to obtain characteristics with 2 active S-boxes every two rounds:

$$\begin{pmatrix} 0 & 0 \\ x_1 & x_3 \\ x_2 & x_2 \\ x_3 & x_1 \end{pmatrix} \xrightarrow{SB} \begin{pmatrix} 0 & 0 \\ x_1 & x_3 \\ x_2 & x_2 \\ x_3 & x_1 \end{pmatrix} \xrightarrow{SR} \begin{pmatrix} 0 & 0 \\ x_3 & x_1 \\ x_2 & x_2 \\ x_1 & x_3 \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} \mathbf{c}' & 0 \\ a' & a \\ d & d' \\ b' & b \end{pmatrix}$$

$$\xrightarrow{SB} \begin{pmatrix} \mathbf{c}' & 0 \\ a' & a \\ d & d' \\ b' & b \end{pmatrix} \xrightarrow{SR} \begin{pmatrix} c' & 0 \\ a & a' \\ d & d' \\ b & b' \end{pmatrix} \xrightarrow{MC} \begin{pmatrix} 0 & 0 \\ x_1 & x_3 \\ x_2 & x_2 \\ x_3 & x_1 \end{pmatrix}$$

Possible Improvements (Cont.)

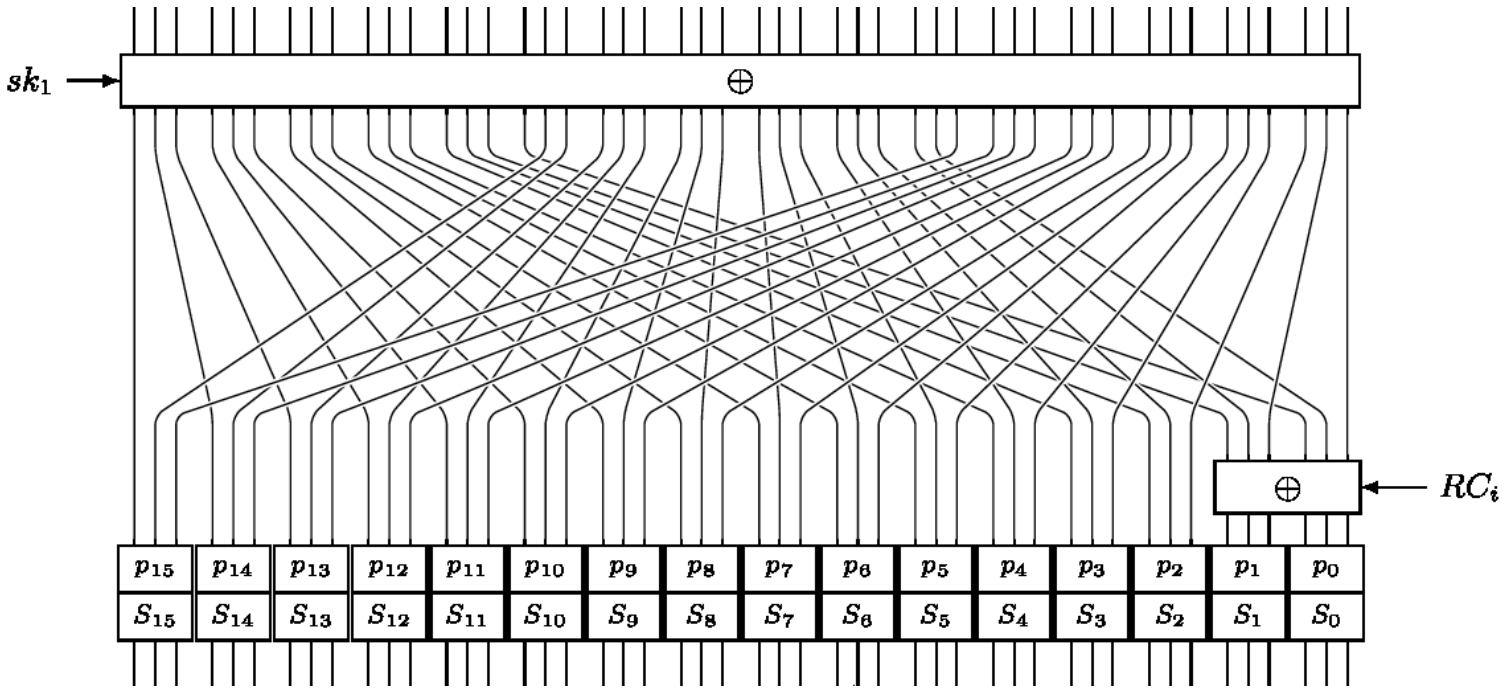
- Using linear algebra it is possible to define conditions for a lower number of active S-boxes:
  - 2 active S-boxes every 4 rounds [Z+14],
  - 1 active S-box every 2 rounds [B+15].
- The result, a linear approximation of a bias $\approx 2^{-22}$ for 20-round Zorro (or 2^{-43} for 20-round differential characteristic).
- Together with optimized key-recovery algorithms, the resulting attacks of [B+15]:

Attack	Data	Time
Differential	$2^{41.5}$ CP	2^{45}
Linear	2^{45} KP	2^{45}

PRINTCIPHER [K+10]

- Lightweight block cipher for printable ICs.
- 48-bit block/80-bit key or 96-/160-.
- Number of rounds = Block size.
- Simple SPN structure with 3-bit S-boxes and a small twist — a key dependent permutation before the application of the S-box.

PRINTCIPHER [K+10]



Invariant Subspaces [L+10]

- The 3-bit S-box permits subspaces, e.g., $S(00*) = 00*$ or $S(1*0) = 1*1$.
- If the plaintext is part of some (specific) subspace $P \in V + c$, then $S(P) \in V + d$, and the key $k \in U + c + d$ then:

$$S((U+d)+k) = S((U+d)+(u+c+d)) = S(U+c) = U+d$$

- In other words, the round function operates on some subspace in a linear function (assuming the subkey is "good").
- For PRINTCIPHER-48, this implies a weak-key class of 2^{51} weak keys (which are easily identifiable).
- One can switch different c and d throughout the subspace characteristic.
- Also, one can work with nonlinear spaces.

Archeology and Related Results

- Linear Structures in Blockciphers, Evertse, Eurocrypt 1987.
- Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers, Paterson, FSE 1999.
- Partition-Based Trapdoor Ciphers, Bannier, Bodin, and Filiol, Eprint 2016/493.
- A New Structural-Differential Property of 5-Round AES, Grassi, Rechberger, and Rønjom, Eurocrypt 2017.

History Mystery Tour

- DES' design criteria was kept secret.
- This led to the question whether there is some hidden backdoor in it.
- Early works were interested in whether an algebraic backdoor existed —

Does DES form a Group?

Testing for "Groupness"

- If DES indeed forms a group, the cycle structure of encryption is expected to be different than for a random permutation [CG75].
- [EG83,DF84] suggested that DES might form a group.
- [KRS85] found out short cycles when DES' weak keys were used.
- Coppersmith suggested that these are to do with the increased number of fixed points [C85].
- Other works exist (e.g., [SM87])
- Finally, [CW92] showed that DES is not a group.

Fixed Points

- Actually, fixed points are extremely useful in cryptanalysis.
- For example, in a series of papers on GOST, Courtois (et al.) are using fixed points.
- This also was the base of [I11] first full key recovery attack on GOST.
- And it appears that many times fixed points can replace slide/reflection attacks [D+14].
- For example, [S13] used fixed points to attack variants of the lightweight cipher PRINCE.

Conclusions

- With the reintroduction of classical designs, classical attacks may become relevant again.
- Sometimes, the advanced techniques are not necessarily the best.
- With the advance in computing power, we can expect more and more attacks being verified:
  - Build trust in the "theory" of cryptanalysis,
  - Find discrepancies between "theory" and practice which lead to better theory.

A Proposed Roadmap

- Read old papers.
- Recover wisdom from old papers.
- Think of the values rather than the differences/approximations.
- Attack and break new schemes using old attacks.

Questions?

Thank you for your attention!