Horst-Görtz Institut
für IT Sicherheit

New Lightweight DES Variants Suited for RFID Applications

G. Leander, C. Paar, A. Poschmann, K. Schramm

Workshop on Fast Software Encryption 2007

Outline

- Introduction
  - Why lightweight?
  - Why choose DES?
- DESL: DES Lightweight
  - Why change DES?
  - How to change DES?
  - What are the benefits?

Why Lightweight? – Paradigm Shift

Horst-Görtz Institut für IT Sicherheit

past | present | future

Mainframe (n : 1)

Personal (1 : 1)

Pervasive (1 : n)

Pervasive = wireless + embedded + cheap
= constrained in CPU, memory, battery

Why choose DES?

Horst-Görtz Institut für IT Sicherheit

„People who are still working on DES should probably start a self-help group.“

3 approaches for lightweight crypto:

1. Minimal implementation of standard ciphers
   - Cipher design usually SW optimization driven
   - If HW optimized, then for high throughput
2. Design a new HW optimized cipher
   - No trust in new ciphers
3. **Modify a trusted HW optimized cipher**
   - **Hope for a transition of trust**

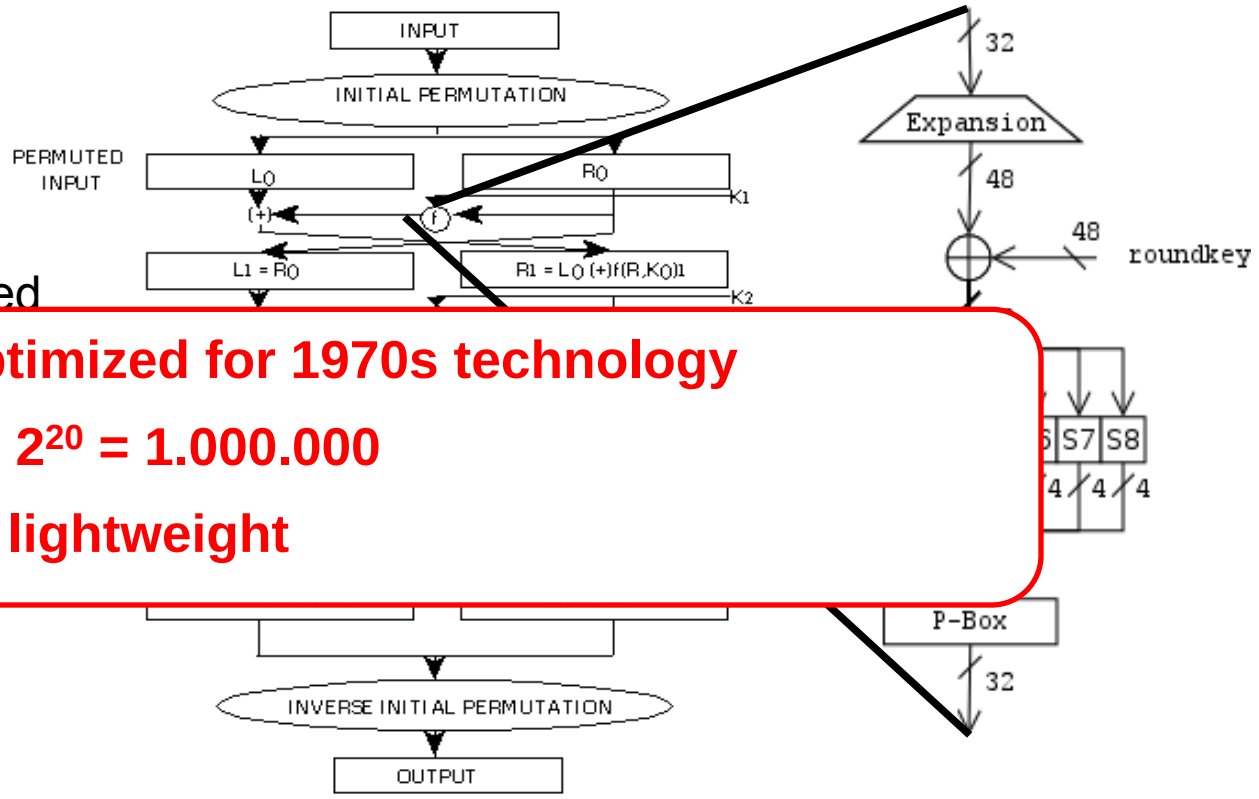
Recall DES

DES:

- Published in 1977
- Probably best investigated cipher
- Plenty of HW-operations

Major Drawback:

- Short keylength



HW optimized for 1970s technology

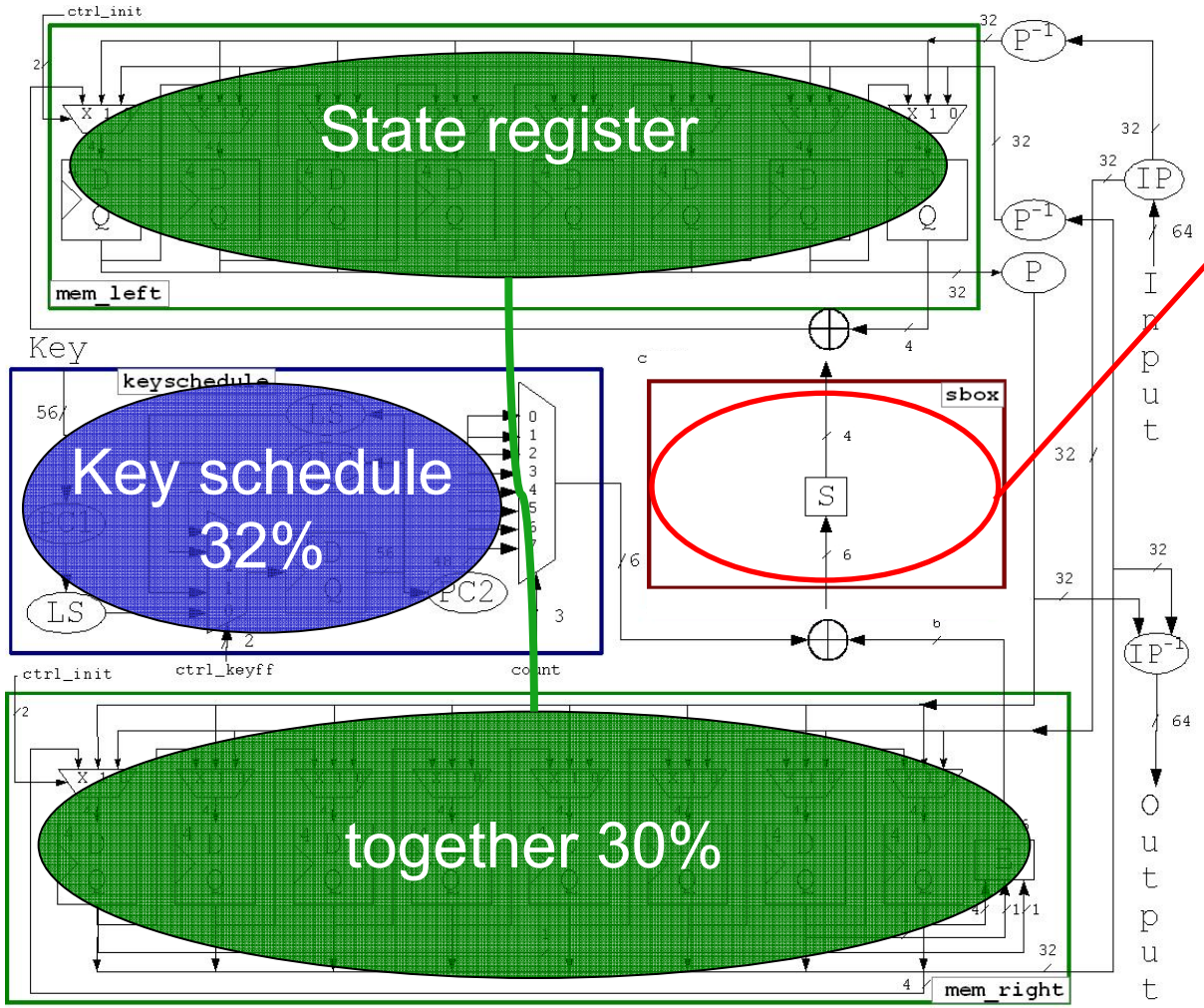
Factor 2^{20} = 1.000.000

DES = lightweight

DESX

Why change DES?

Horst-Görtz Institut
für IT Sicherheit



S-Boxes

- 6-to-4 substitution tables
- highly non-linear
  → high Boolean compl.
- **34% of area!**

Idea:

- Replace S1...S8 by S

How to change DES?

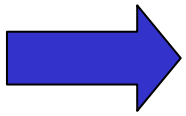
Horst-Görtz Institut für IT Sicherheit

Plenty of previous work during the 1990s…

- DES design criteria (Coppersmith)
- Improved resistancy against DC, LC, and DMA (Kim et al.)

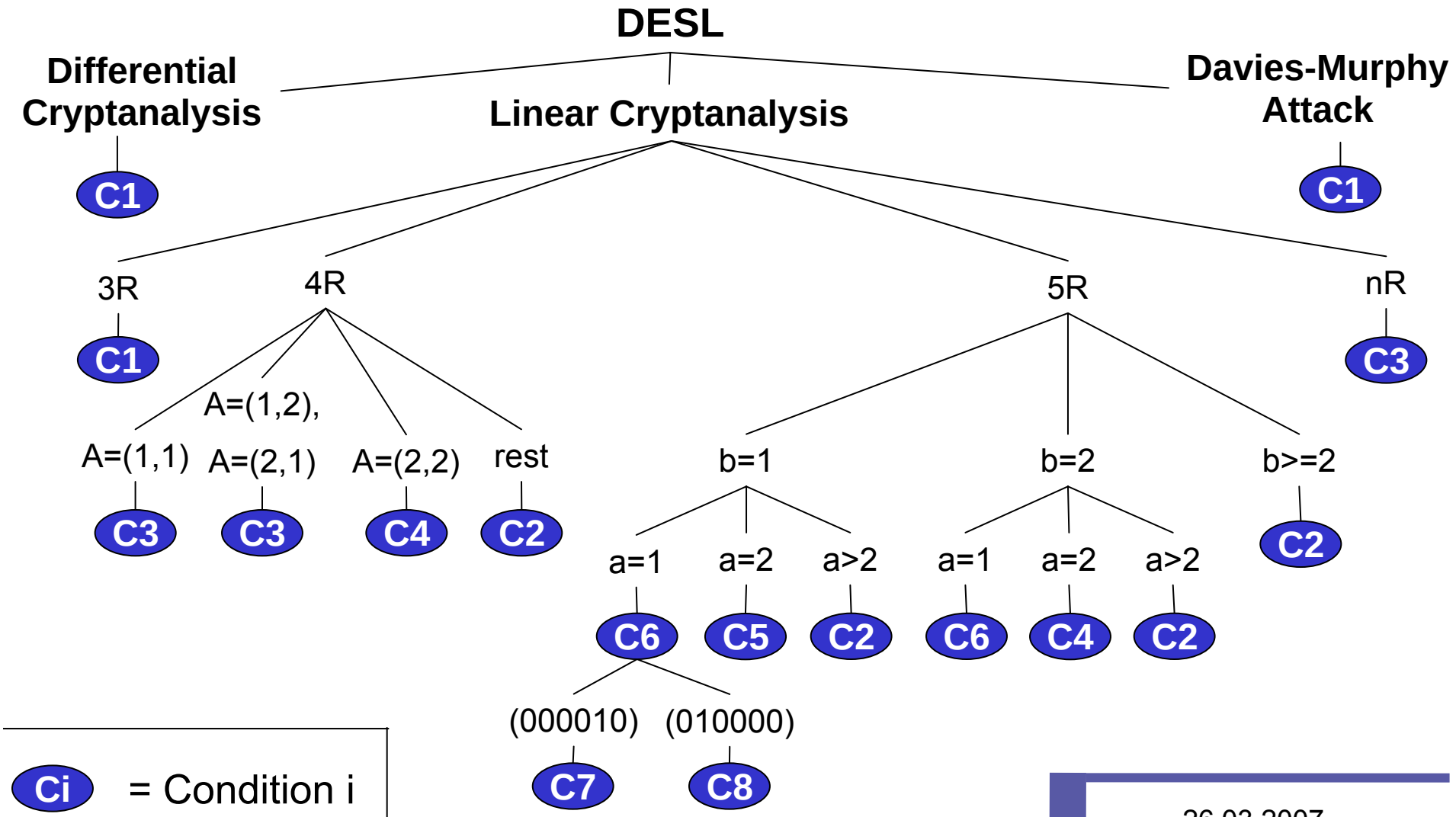
…But:

- All previous work focused on 8 different S-boxes
- No S-box fulfills all criteria by Kim et al.



Detailed look on the criteria by Kim et al.

Design Criteria for single S-box DES



…18 Months later

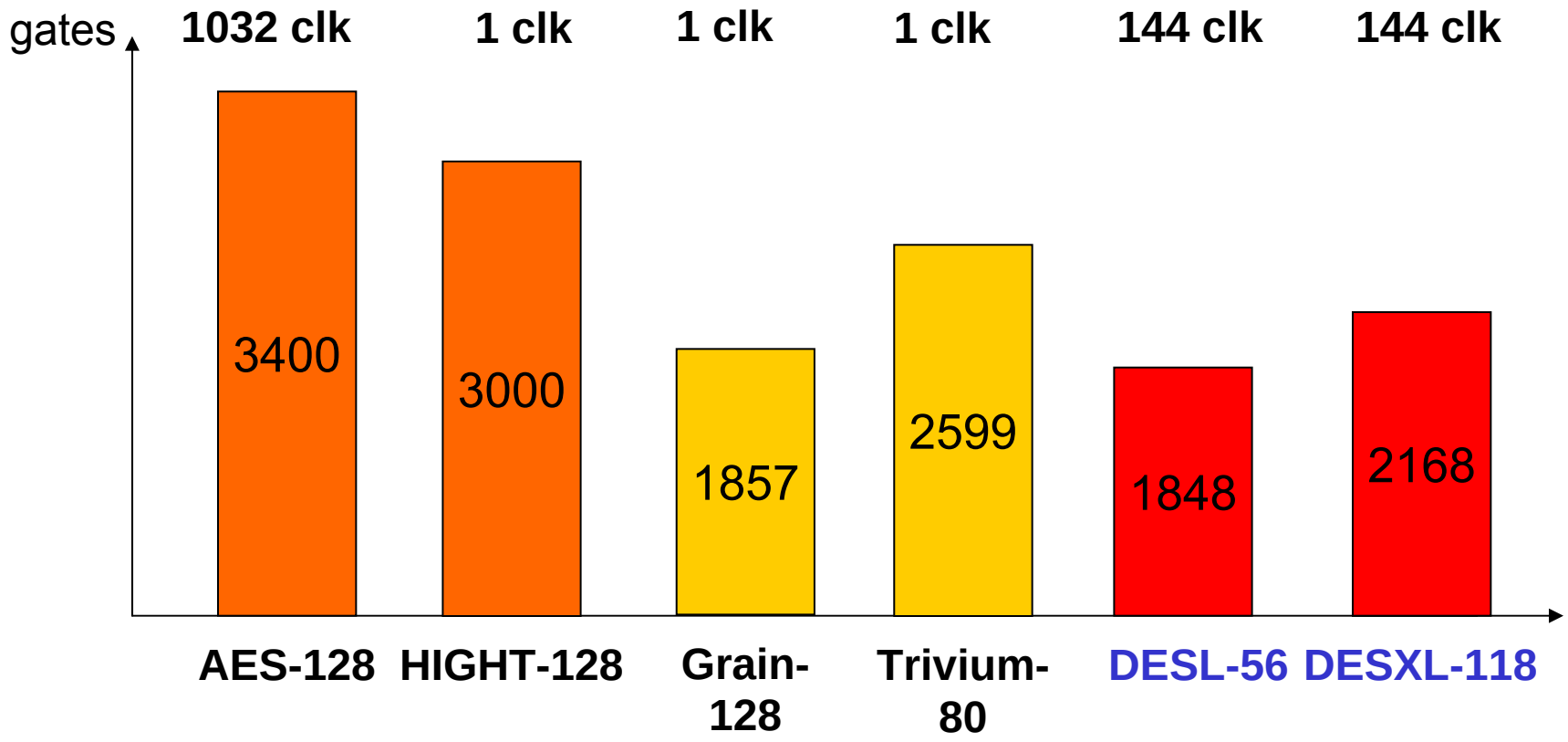
Horst-Görtz Institut für IT Sicherheit

S															
14	5	7	2	11	8	1	15	0	10	9	4	6	13	12	3
5	0	8	15	14	3	2	12	11	7	6	9	13	4	1	10
4	9	2	14	8	7	13	0	10	12	15	1	5	11	3	6
9	6	15	5	3	8	4	11	7	1	12	2	0	14	10	13

Improved DESL S-box:

- Satifies all conditions
- Resistant against
  - certain Differential Cryptanalysis,
  - Linear Cryptanalysis, and
  - Davies-Murphy Attack
- Results in total area saving of 20 %

What are the benefits?



- Smallest known secure block cipher
- Very small footprint (=cheap) in hardware
- Comparable even to streamciphers

Horst-Görtz Institut
für IT Sicherheit

S															
14	5	7	2	11	8	1	15	0	10	9	4	6	13	12	3
5	0	8	15	14	3	2	12	11	7	6	9	13	4	1	10
4	9	2	14	8	7	13	0	10	12	15	1	5	11	3	6
9	6	15	5	3	8	4	11	7	1	12	2	0	14	10	13

Thank you!

Questions?

www.crypto.rub.de, poschmann@crypto.rub.de

Example: 4-Round Linear Characteristic

Horst-Görtz Institut für IT Sicherheit

A: $\langle I_2,Z_1\rangle + \langle K_2,Z_3\rangle = \langle O_2,Z_2\rangle$

B: $\langle I_3,Y_1\rangle + \langle K_3,Y_3\rangle = \langle O_3,Y_2\rangle$

$O_2 = I_1 + I_3$, $O_3 = I_2 + I_4$

15-round approximation: -AB-BA-AB-BA-AB

Kim et al. Use two conditions:

- General: $S_b^W(a) \le 20, a \in GF(2)^6, b \in GF(2)^4, wt(a), wt(b) \le 2$
- Special: No occurence of 18 sub-cases for wt(a)=wt(b)=1

Our conditions:

- General: $S_b^W(a) \le 20, a \in GF(2)^6, b \in GF(2)^4, wt(a), wt(b) \le 2$
- Special: $S_b^W(a) \le 4, a \in GF(2)^6, b \in GF(2)^4, wt(a) = wt(b) = 1$