The only Rump Session Talk with Pamela Anderson

(or: New Lightweight Block Ciphers)

by Christof Paar

Part 1 of the Presentation

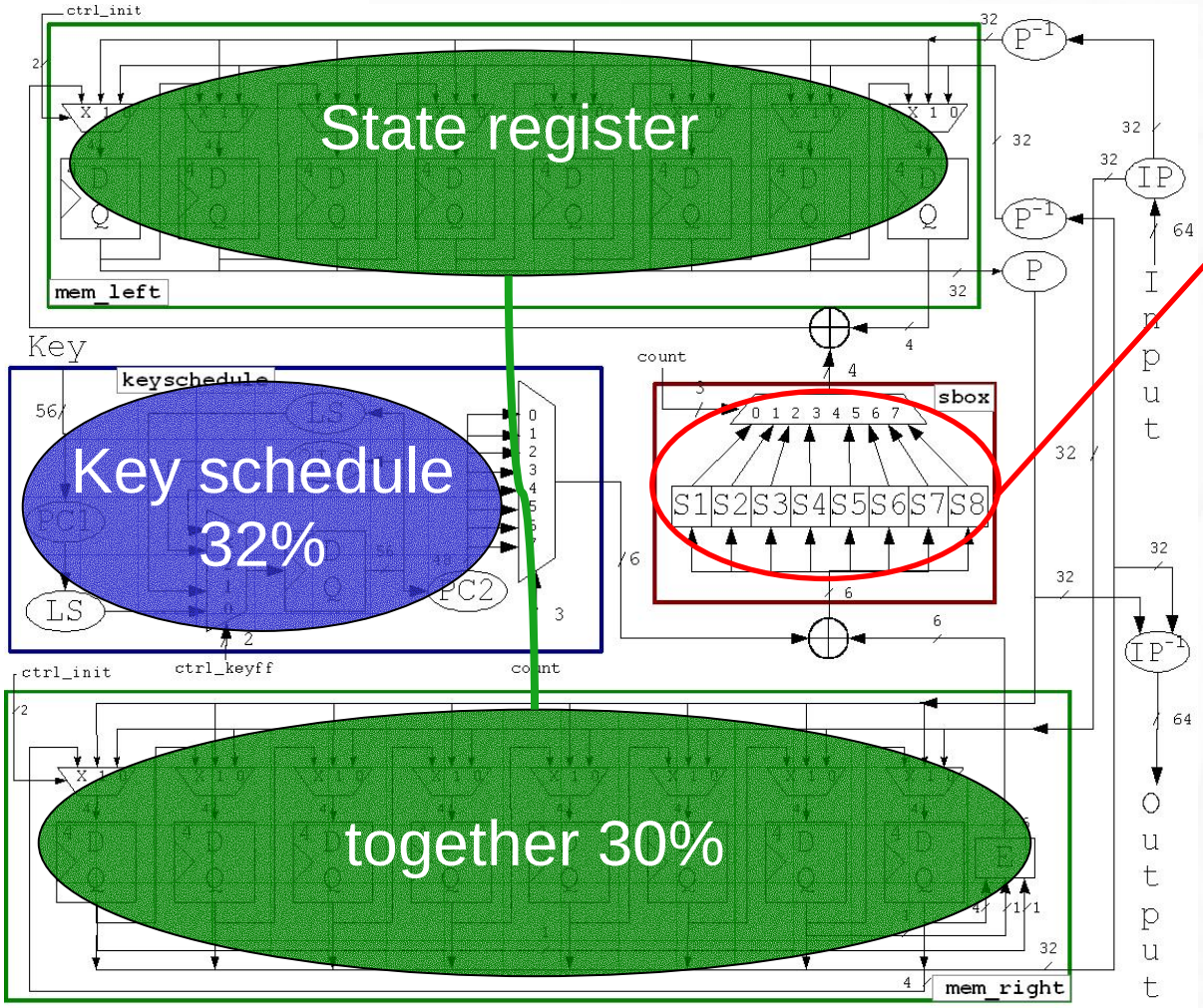
Part 2
PRESENT – A lightweight block cipher

- Really great symmetric cipher
- To be presented at CHES `07
- Expected to replace weak ciphers such as 3DES, AES256, or ECC512
- Number-of-authors-record at CHES `07:
  Andrey Bogdanov, Lars Kundsen,
  Christof Paar, Gregor Leander,
  Axel Poschmann, Matt Robshaw,
  Yannick Seurin, Charlotte Vikkelsoe

Starting Point

$1\ \text{Round}_{DES} = 6\%\ \text{of gates for}\ 1\ \text{Round}_{AES}$

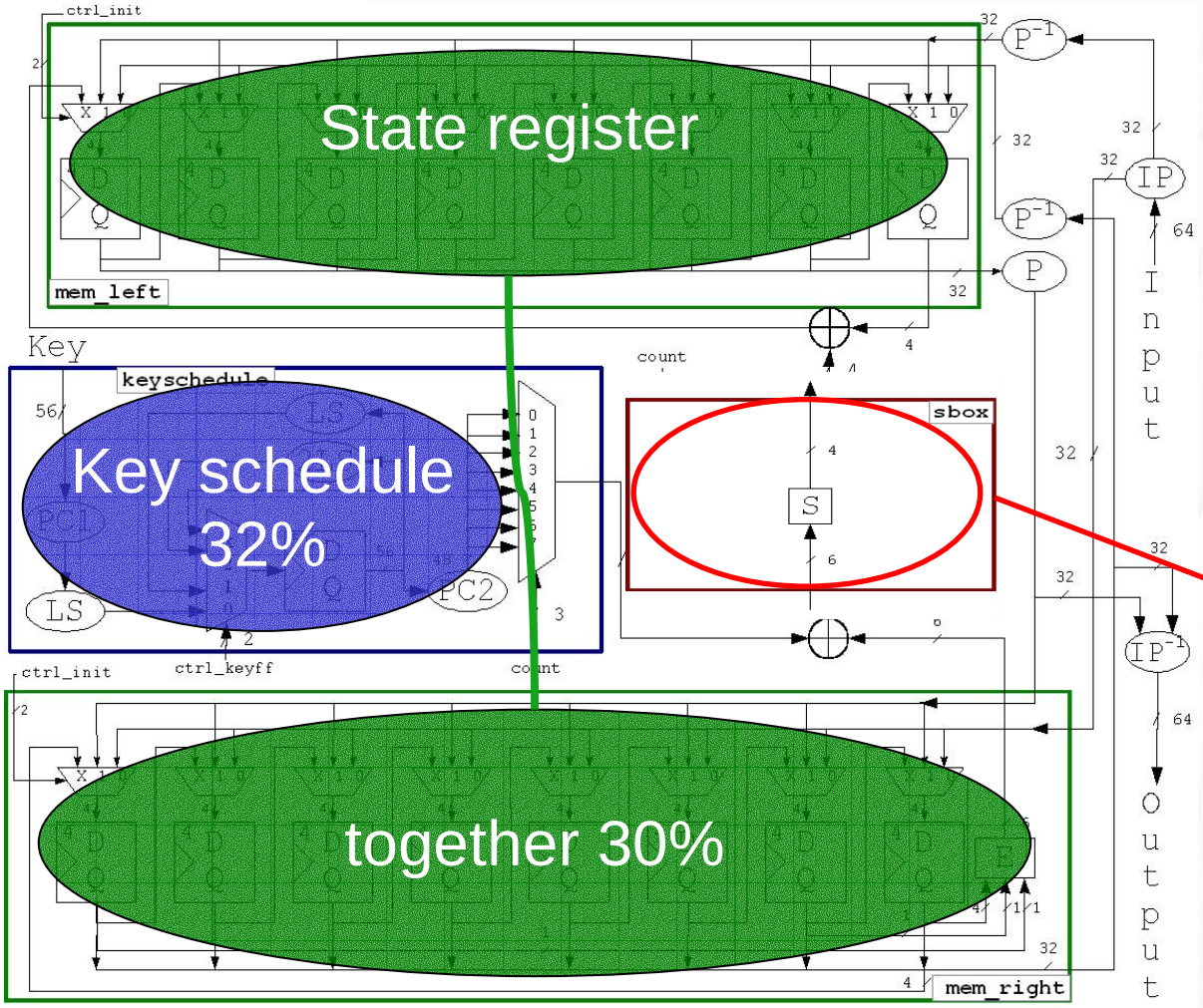
Serialized DES Architecture



S-Boxes

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

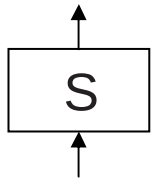
Serialized DES Architecture



Idea:

- Replace S1...S8 by S

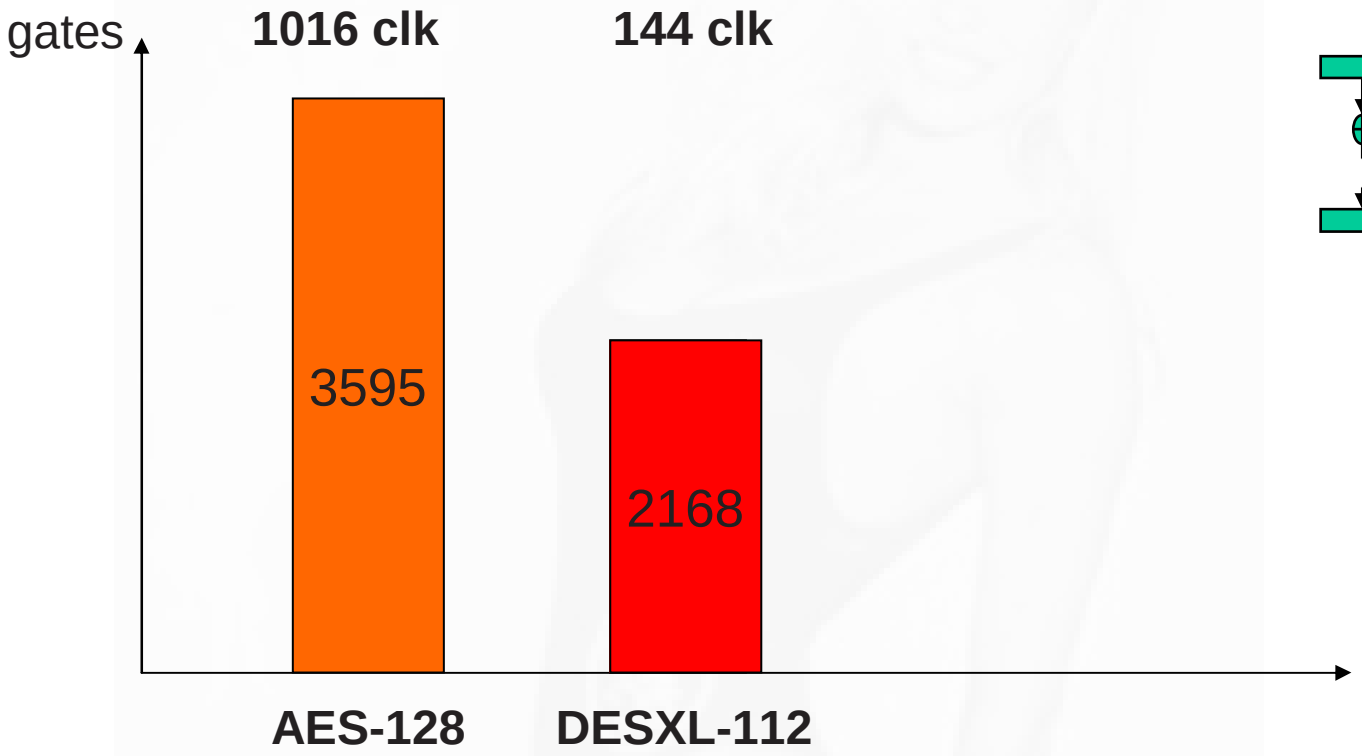
… 12 months later: new Sbox

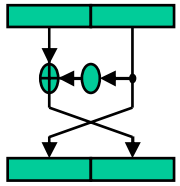


S															
14	5	7	2	11	8	1	15	0	10	9	4	6	13	12	3
5	0	8	15	14	3	2	12	11	7	6	9	13	4	1	10
4	9	2	14	8	7	13	0	10	12	15	1	5	11	3	6
9	6	15	5	3	8	4	11	7	1	12	2	0	14	10	13

- S replaces S1…S8

Results – Lightweight DES





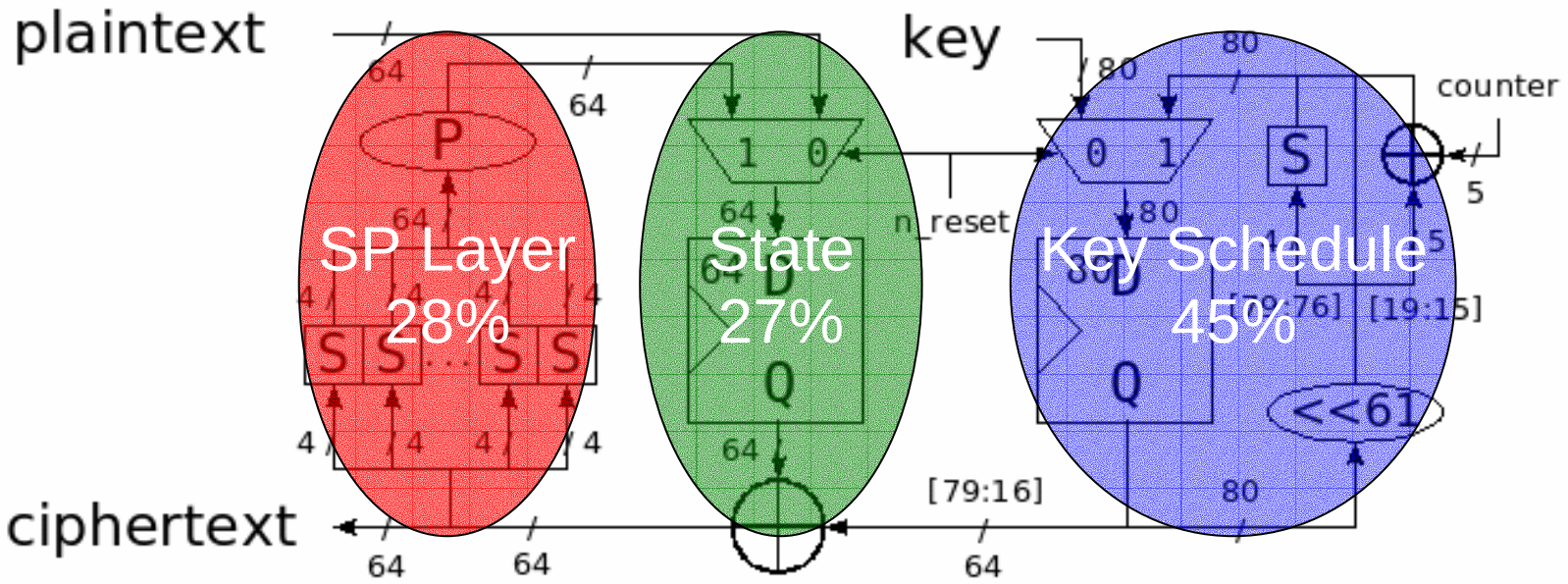
- details: FSE ‘07 paper
- **Q: Can we do better??**

PRESENT – A Lightweight Block Cipher for RFID

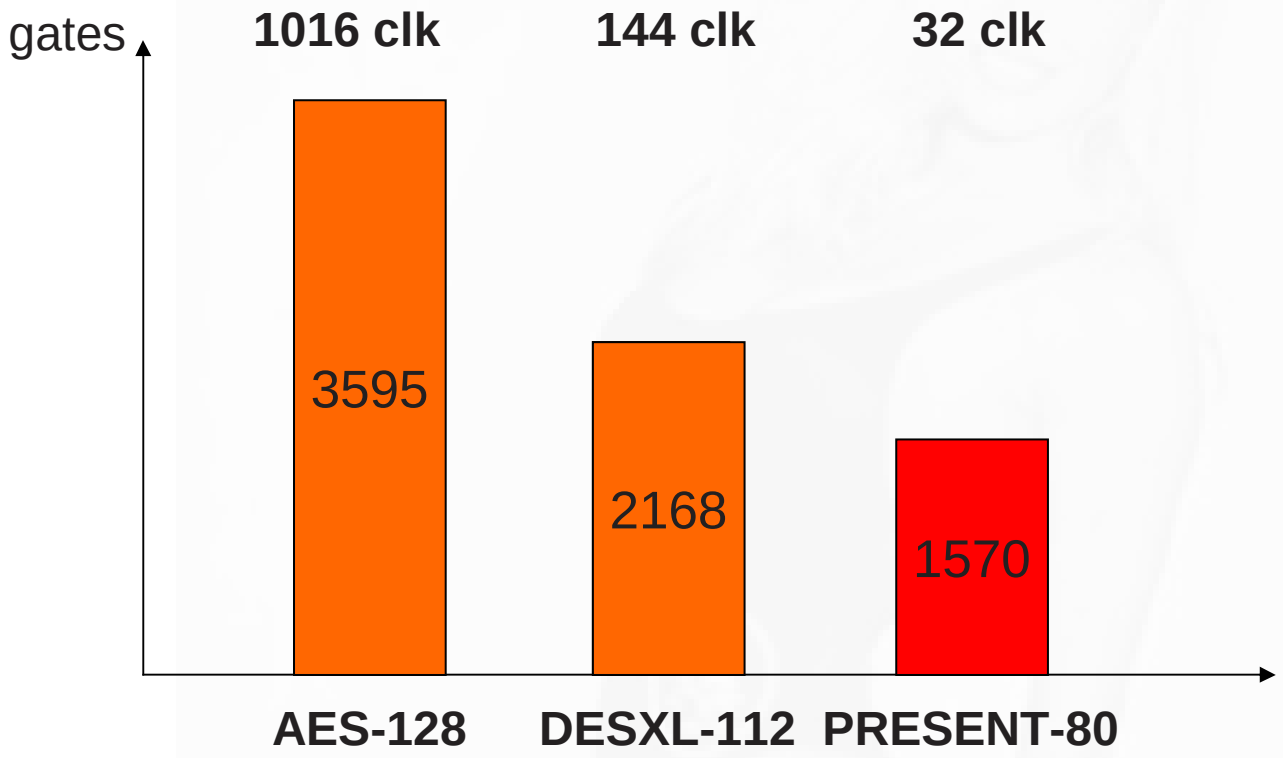
Agressively hardware-optimized block cipher

- pure substitution-permutation network
- 64 bit block, 80/128 bit key
- 4-4 bit Sbox
- 31 round

PRESENT Block Cipher
A Hardware-Optimized SP Network



Results – PRESENT



- TA product 60+ times better than smallest AES architecture
- complexity approaches theoretical limit! (smaller than most stream ciphers)
- well suited for RFID and such
- details: CHES ’07 paper

Thank you for your attention