Tel Aviv University

Algebraic Side-Channel Analysis in the Presence of Errors

Yossi Oren, Mario Kirschbaum,
Thomas Popp and Avishai Wool,

CHES 2010, August 2010

Tel Aviv University

Tel Aviv University

\end
{personal_statement}

Set of *m* logical statements over *n* variables $x_1, \dots, x_n$

Satisfying assignment (or proof of unsatisfiability)

Cryptanalysis with Solvers

- Recall the basic problem of cryptanalysis: Given a **description of a crypto algorithm** and a set of **plaintext and ciphertext pairs**, find the **cryptographic key**
- Idea: Use solvers to perform cryptanalysis [MM ‘00]
- Resu… o is strong enough to resis…

Massacci and Marraro, Journal of Automated Reasoning 2000

Side-Channel Analysis with Solvers

- Recall the basic problem of side-channel analysis : Given a **description of a crypto <u>device</u>, plaintexts, ciphertexts** and a set of **power measurements**, find the **crypto key**
- Idea: Use solvers to perform side-channel analysis [PRR+ ’07 & RSV-C‘09]
- Result: key c[illegible] be recovered f[illegible]m side channel d[illegible]

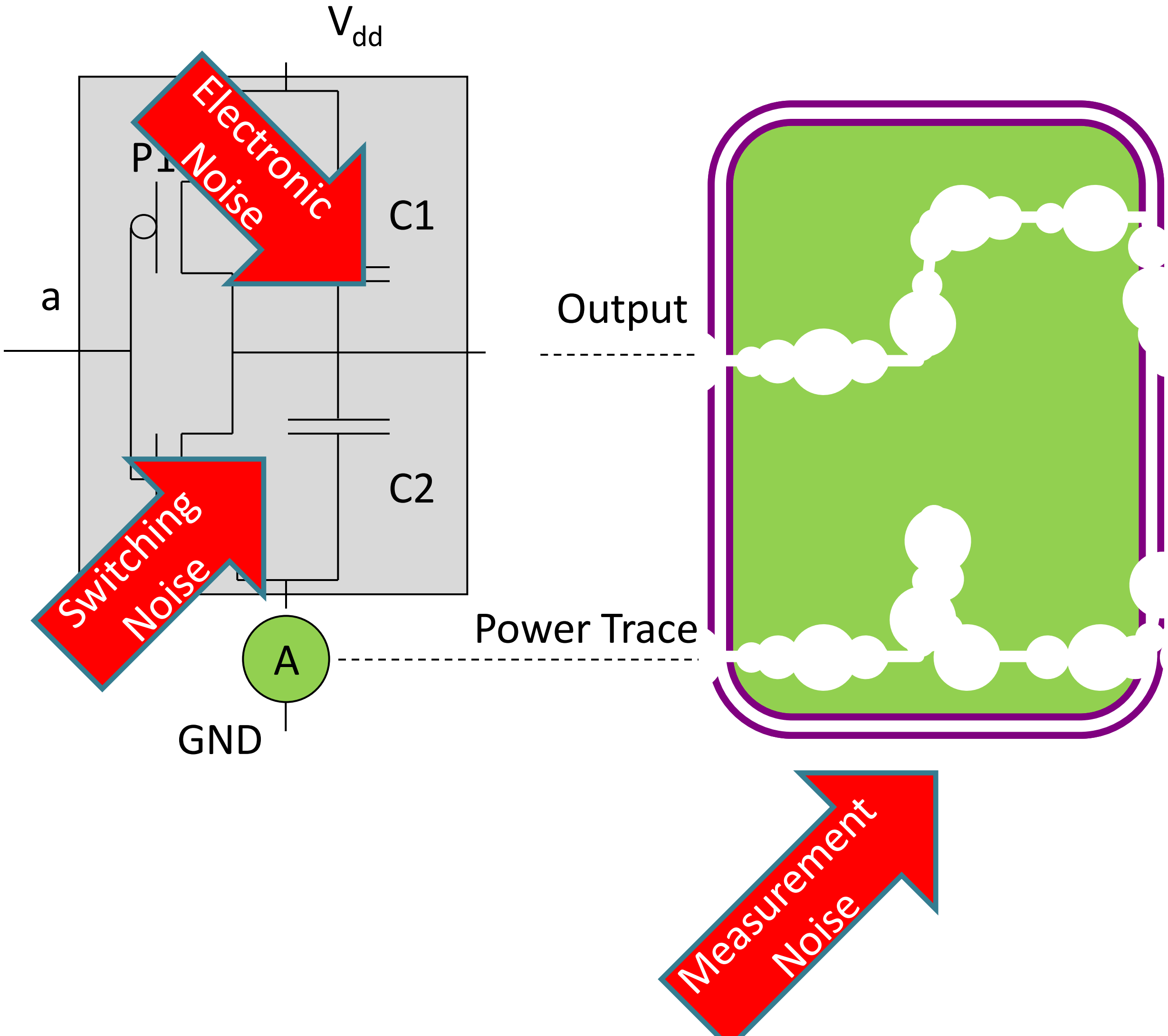
Potlapally, Raghunathan,
Ravi, Jha, Lee
IEEE Trans. VLSI 2007

Renauld, Standaert,
Veyrat-Charvillon
CHES 2009

Tel Aviv University

but…

The Harsh Reality of Power Analysis



The Harsh Reality of Power Analysis

- The side channel traces have **errors**
- When using solver-based approaches, this results in **unsatisfiability**
- **Can we find a solver that deals with errors?**

Pseudo-Boolean Optimizers

- Linear PBOPT:

$$\min c^{\mathrm{T}} x$$

$$Ax \geq b$$

$$x \in \{0,1\}^n$$

(all coefficients are signed integers)

- Non-linear PBOPT allows NL constraints

Tel Aviv University

PBOPT is Great for Side-Channels

- The variables (=flipflops) are pseudo-Boolean
- The constraints(=measurements) are integers
- NL notation rich enough to represent arbitrary functions (such as XORs)

- **NOR:** $-out + \sim x_1 \sim x_2 = 0$
- **XOR:** $-out + x_1 + x_2 - 2x_1x_2 = 0$
- **Keeloq NLF:**

$$-\sim out + x_1x_5 - x_5 - x_1x_3 - x_2x_3 - x_4 + x_2x_5 + x_3x_4 + x_4x_5 + x_1x_2x_3 + x_1x_2x_4 - 2x_1x_2x_5 + x_1x_3x_5 - x_1x_4x_5 = -1$$

The Keeloq Cipher

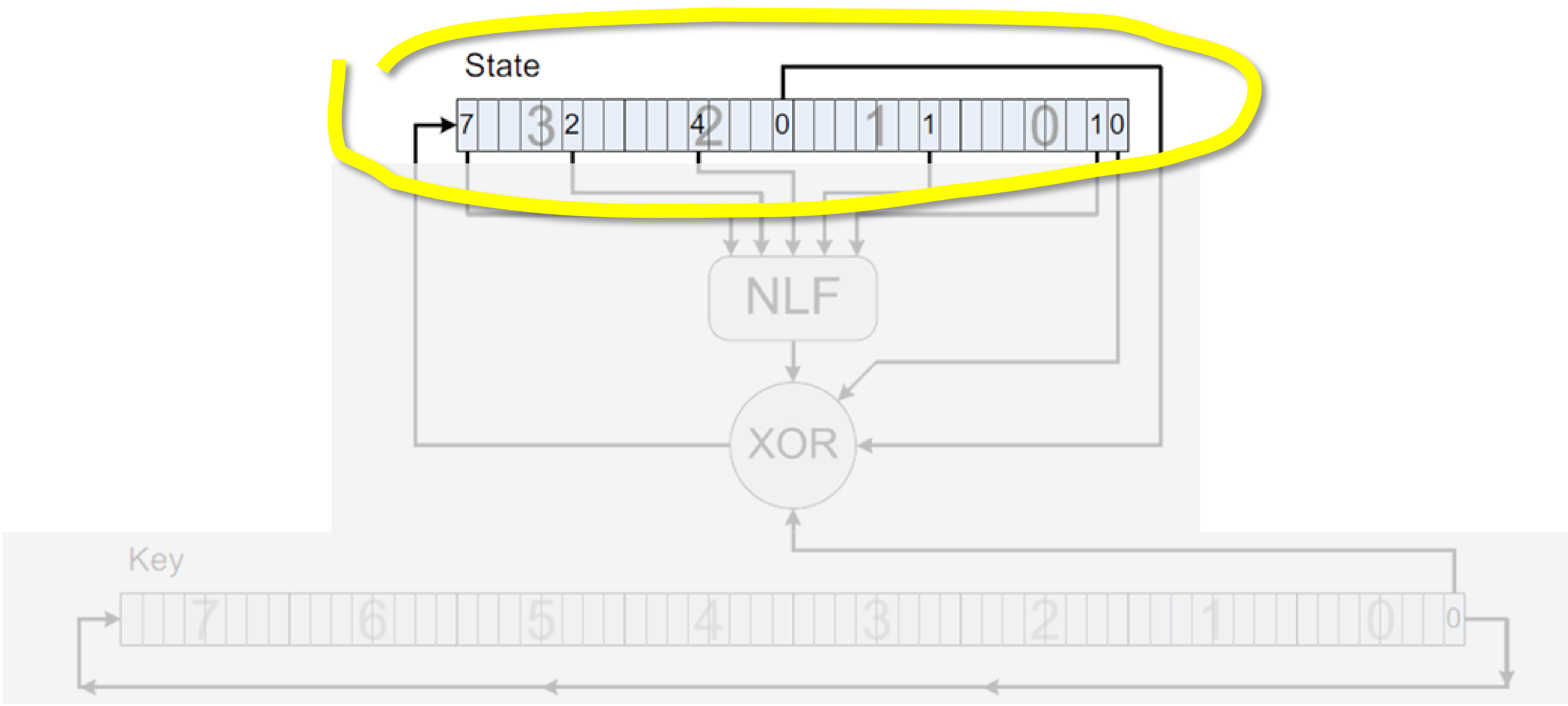
- Block cipher used for car alarm systems
- Reduced version broken with solvers [CBW'08]
- Full version broken with classical DPA [EKM+'08]

Courtois, Bard, Wagner
FSE 2008

Eisenbarth, Kasper, Moradi, Paar, Salmasizadeh, Manzuri Shalmani, CRYPTO 2008

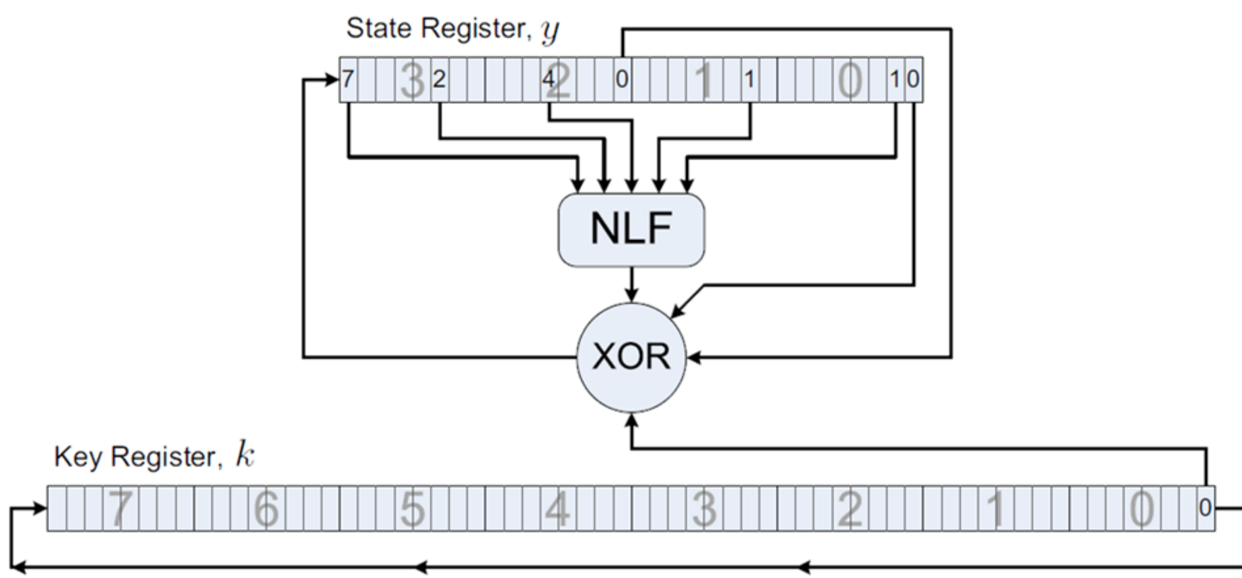
Tel Aviv University

The Keeloq Cipher



An equation system for Keeloq

- Round function
- Input Assignment
- Side channel setup
- Side channel measurement **with errors**



SCIP

- Stands for **Solving Constraint Integer Programs**
- Developed by Konrad-Zuse-Zentrum für Informationstechnik Berlin – free under academic license
- “Fastest non-commercial mixed integer programming solver”
- Won first prize for NL OPT in PB 2009 and PB 2010 competitions

A Successful Attack

- Solver: SCIP
- Cryptosystem: Keeloq
- Error rate: 18%
- Avg. Solving time: 3.6 hours
- 10-100 times faster than greedy Viterbi methods

Future Work

- More cryptosystems (e.g. AES)
- More optimizers (e.g. Weighted CSP)
- Integrate into an ASIC workflow

Tel Aviv University

Thank you!

http://iss.oy.ne.ro/TASCA