Horst Görtz Institute for IT-Security

A Real-World Attack Breaking A5/1 within Hours

Timo Gendrullis, Martin Novotný, Andy Rupp
Ruhr University Bochum

Outline

Horst Görtz Institute for IT-Security

A5/1 cipher

COPACOBANA

Attack on A5/1 cipher

Architecture of the A5/1 cracker

Optimization

Implementation results

A5/1 Cipher

Horst Görtz Institute for IT-Security

Stream cipher

– produces the keystream **KS** being xored with the plaintext **P**

$$C = P \oplus KS$$

Encrypts GSM communication

– GSM communication organized in bursts

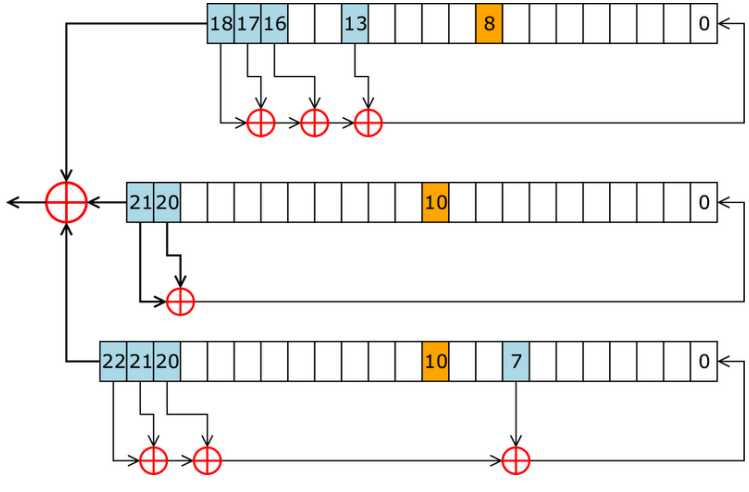
– 1 burst = 114 bits in each direction

Architecture of A5/1:

3 linear feedback shift registers (LFSRs)

LFSRs irregularly clocked

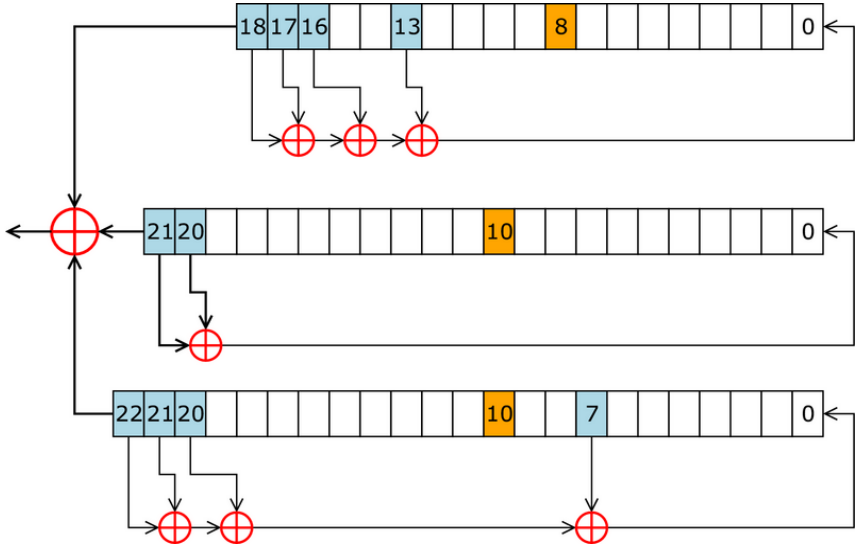
– the register is clocked iff its clocking bit (yellow) is equal to the majority of all 3 clocking bits ⇒ at least 2 registers are clocked in each cycle



Algorithm of A5/1

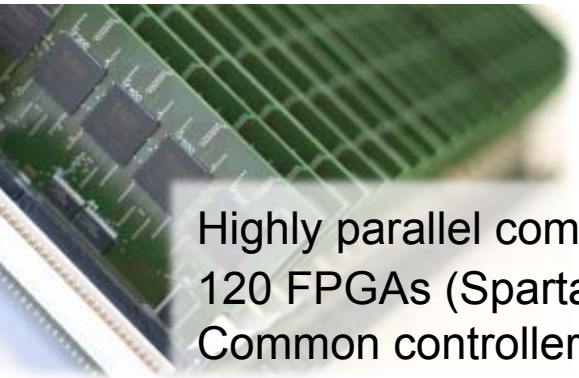
Horst Görtz Institute for IT-Security

1. Reset all 3 registers
2. (Initialization) Load 64 bits of key **K** + 22 bits of frame number **FN** into 3 registers
   - **K** and **FN** xored bit-by-bit to the least significant bits
   - registers clocked *regularly*
3. (Warm-up) Clock for 100 cycles and discard the output
   - registers clocked *irregularly*
4. (Execution) Clock for 228 cycles, generate 114+114 bits (for each direction)
   - registers clocked *irregularly*
5. Repeat for the next frame



COPACOBANA

Horst Görtz Institute for IT-Security

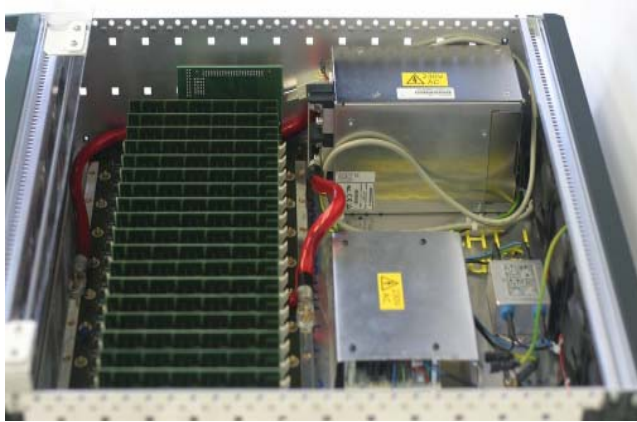


Highly parallel computing machine
120 FPGAs (Spartan 3 – 1000)
Common controller ⇒ shared interface

high computation power × **low** communication bandwidth

Developed at Christian-Albrechts-University Kiel
and Ruhr-University Bochum

http://www.copacobana.org (a suffix is "**.org**", not "**.de**"!)

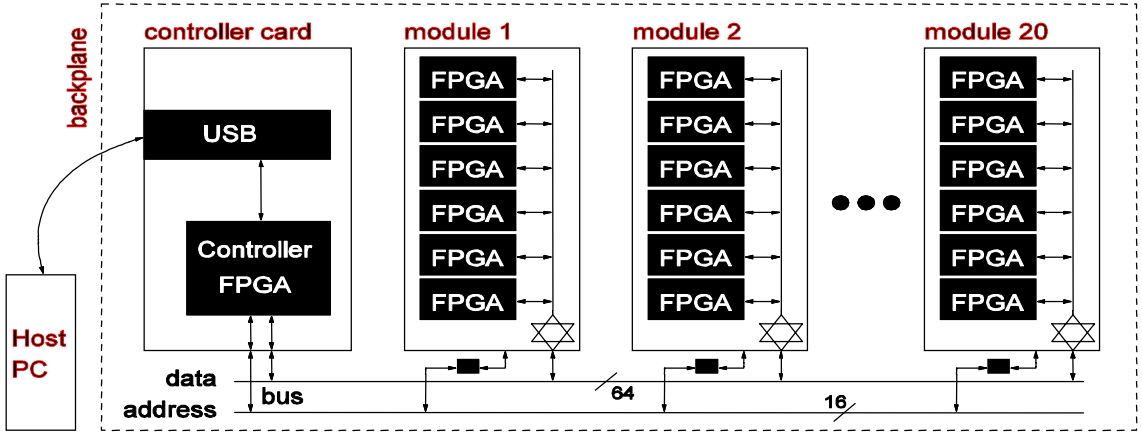


COPACOBANA: Basic Design

Horst Görtz Institute for IT-Security

Modular design

- Backplane
- FPGA modules (each with 6 low-cost FPGAs)
- Controller card with USB/Ethernet interface



Easily extendable

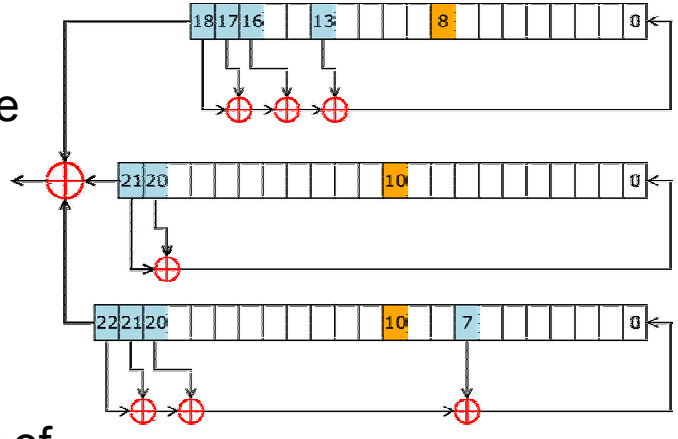
- Up to 20 FPGA modules with 6 FPGAs each
- Connect multiple COPACOBANAs via USB/Ethernet

Attack on A5/1

Horst Görtz Institute for IT-Security

Based on the guess-and-determine attack by Keller&Seitz (2001)

Goal: From the known keystream **KS** to determine the content of all 3 registers (internal state)



Repeat:

1. Guess the content of shorter registers **R1** and **R2** (19+22=41 bits)
2. Try to run the cipher, inspect the potential content of register **R3**
   1. from the known keystream *derive* the MSB of **R3**
   2. from clocking/non-clocking of **R3** *derive* the clocking bit of **R3**
3. When **R3** is completed, run the cipher, compare output with the known keystream
4. If not successful, goto 1

Example

Horst Görtz Institute for IT-Security

Step (0):

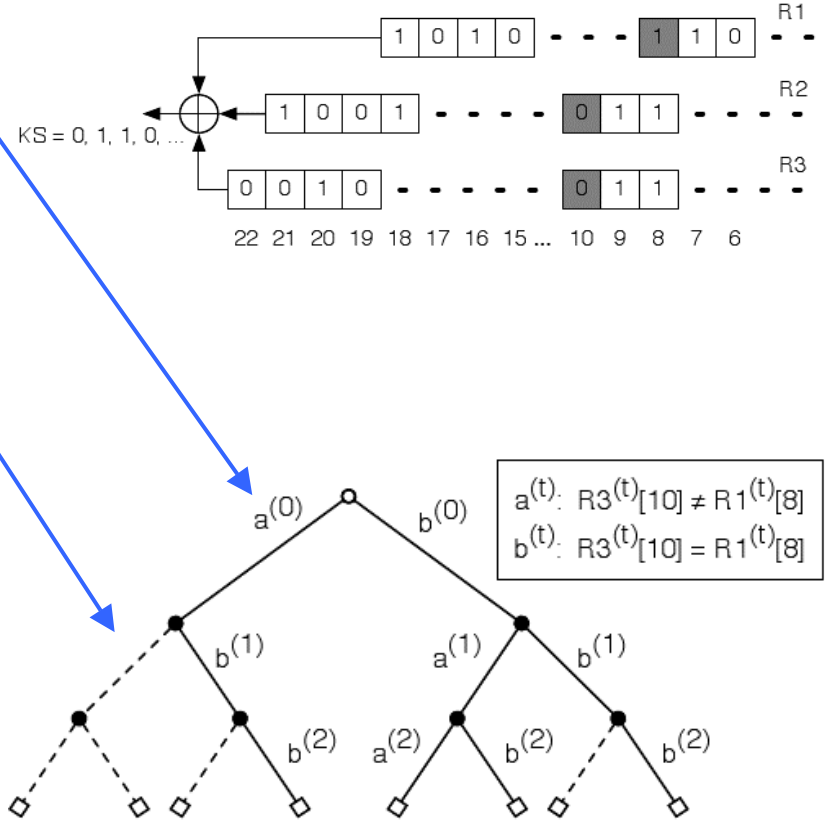
- *calculate*
  R3[22] = R1[18]+R2[21]+KS[0] = 0
- *choose* R3[10] = 0 ≠ R1[8] $a^{(0)}$
- clocking bits 1,0,0 ⇒ clock R2 and R3

Step (1):

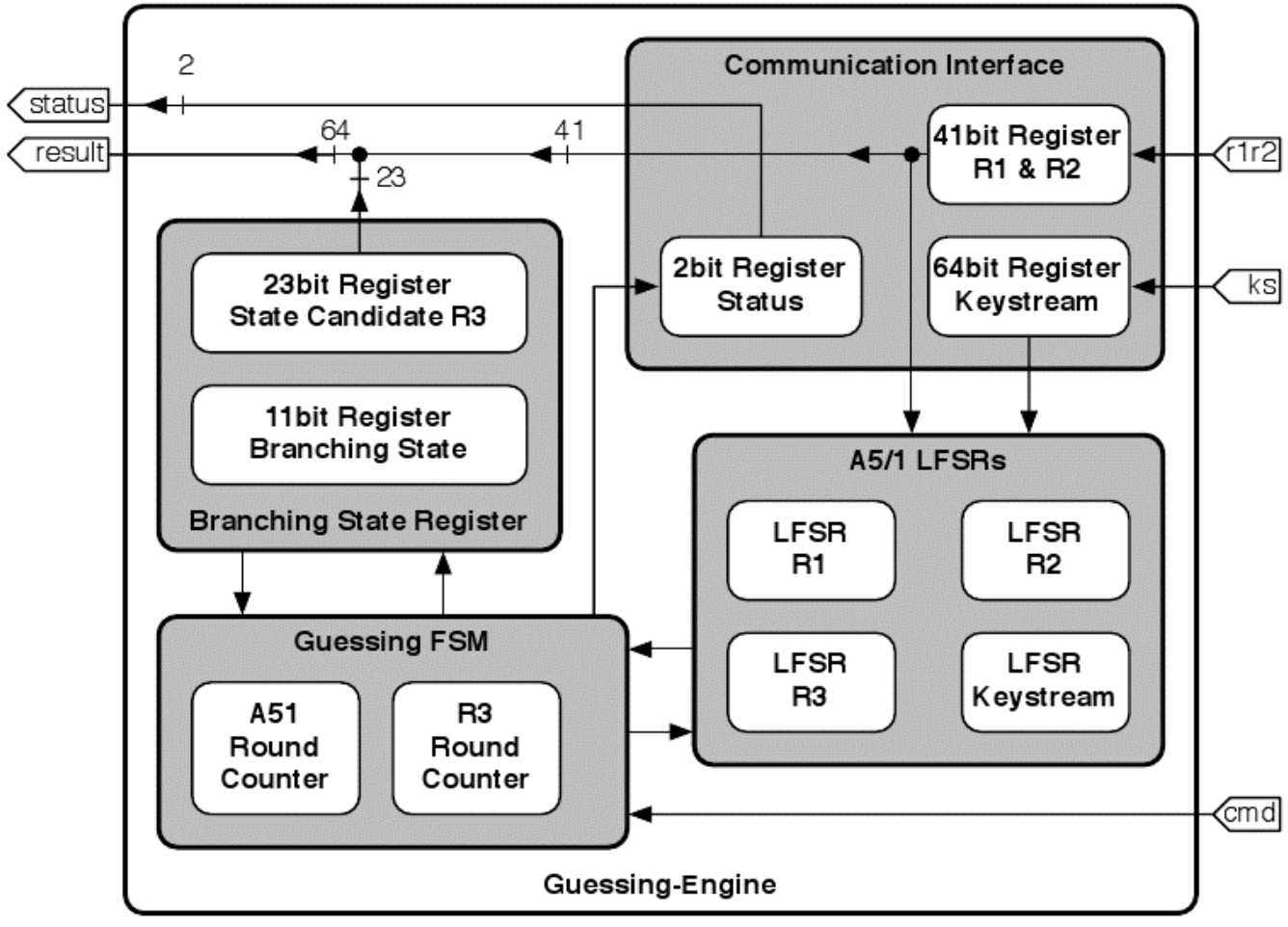
- *calculate*
  R3[21] = R1[18]+R2[20]+KS[1] = 0
- *choose* R3[9] = 0 ≠ R1[8] $a^{(1)}$
- clocking bits 1,1,0 ⇒ clock R1 and R2

Step (2):

- R3 was not clocked, therefore also
  R3[21] = R1[17]+R2[19]+KS[2]
  but: R1[17]+R2[19]+KS[2] = 1 !!!
  ⇒ contradiction, $a^{(1)}$ impossible

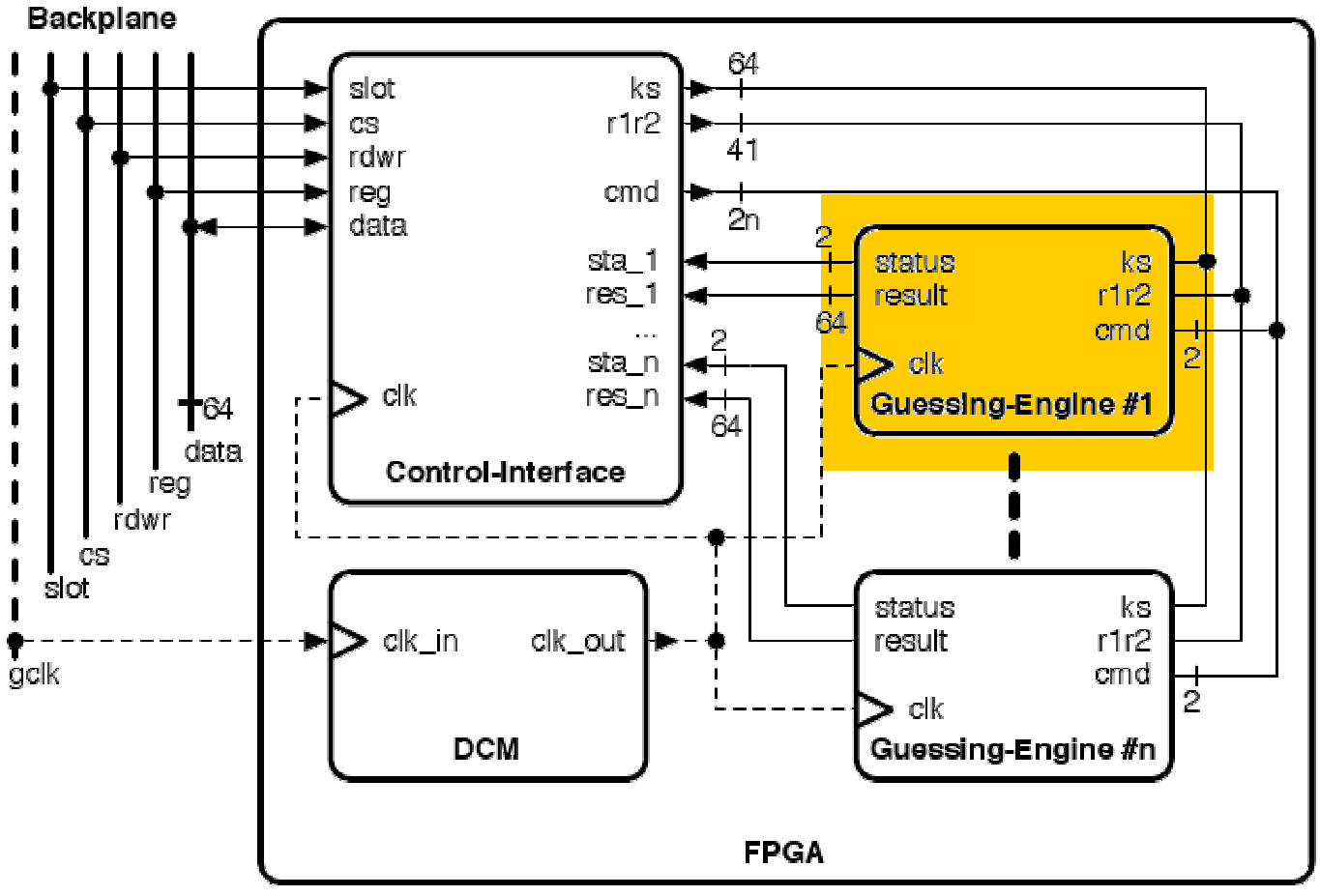


Guessing engine



FPGA hosts several guessing engines

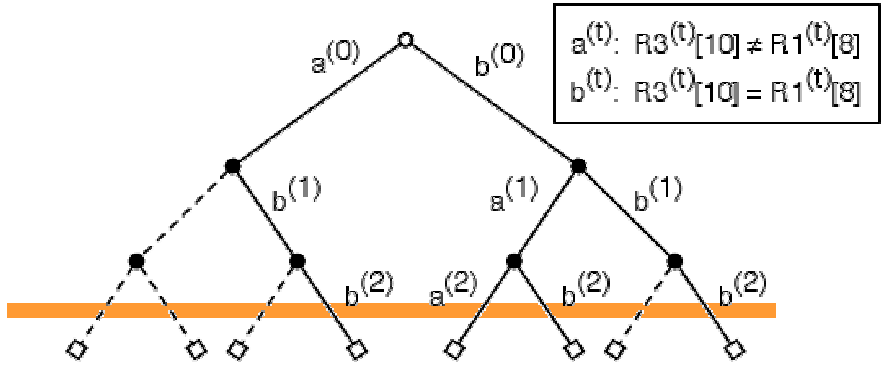
Horst Görtz Institute for IT-Security



Optimization

Original approach:

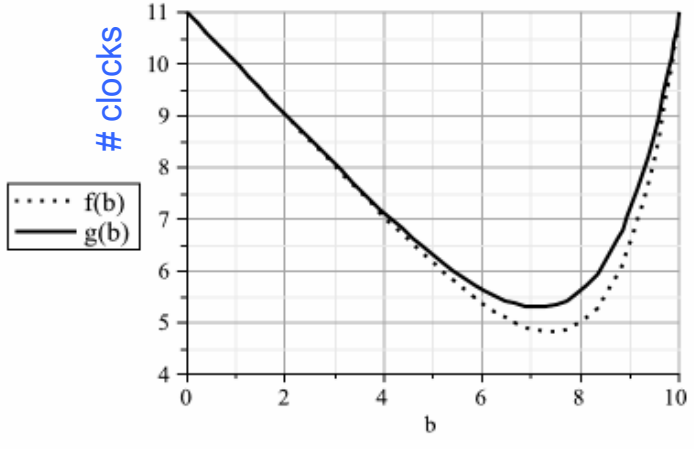
The tree is traced always from the root



Optimization:

When tracing from the root, the state of the guessing engine is stored at certain depth (at recovery point) and later reloaded

Reduces #clock cycles to reach the leaf of the decision tree:



depth of recovery point

Implementation results

Horst Görtz Institute for IT-Security

#guessing engines	#slices	#FFs	#LUTs	f_{max} [MHz]	f_{test} [MHz]	maximum time	
						estim.	measured
36 standard	6953	10730	10576	81.85	72.00	16.31 h	
32 standard	6614	9636	9417	102.42	92.00	14.36 h	13.58 h
23 optimized	7494	10141	10562	104.65	92.00	11.40 h	11.78 h
Spartan3-1000	7680	15360	15360	300.00			

Average time to reveal the internal state:

5.89 hours