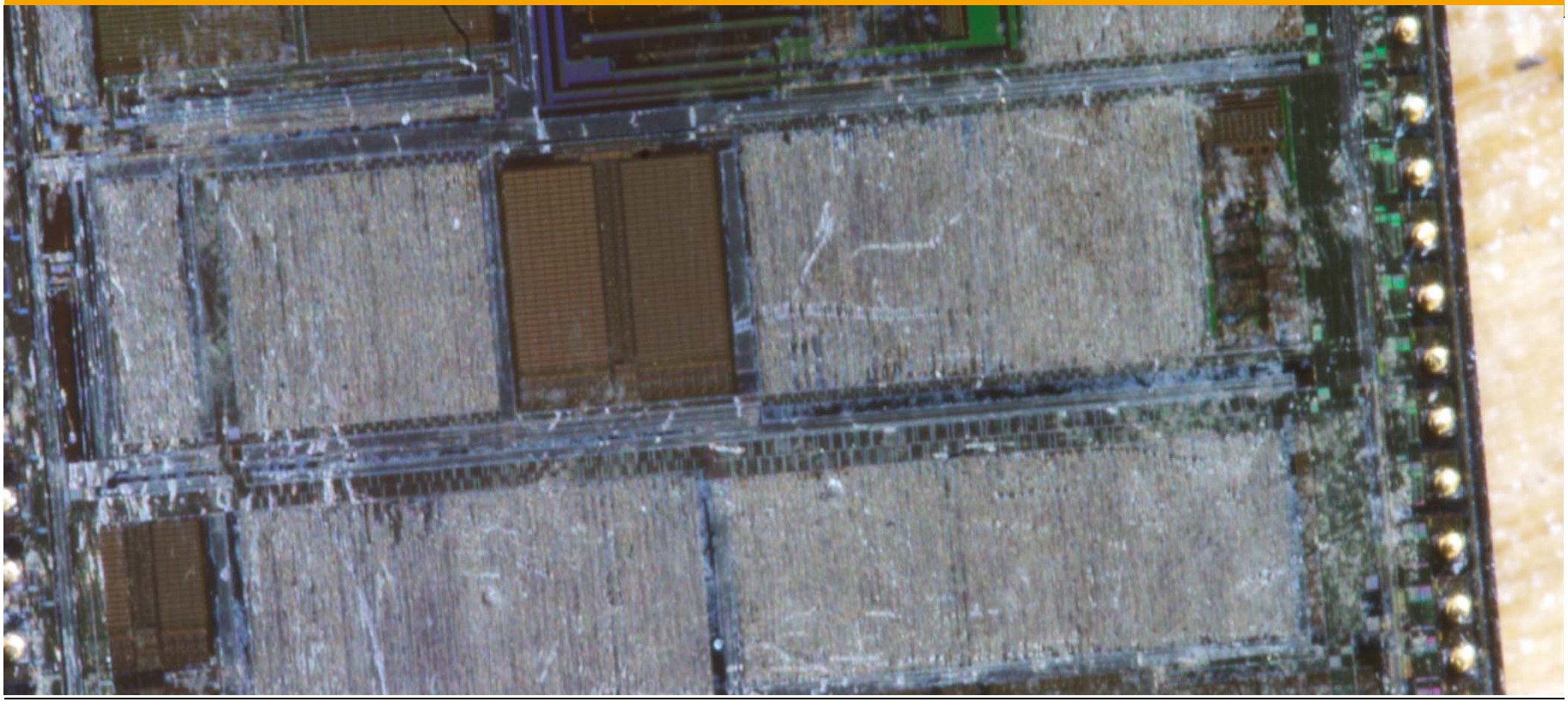
Cryptanalysis of the DECT Standard Cipher

Karsten Nohl <nohl@cs.virginia.edu>
Erik Tews <e_tews@cdc.informatik.tu-darmstadt.de>
Ralf-Philipp Weinmann <ralf-philipp.weinmann@uni.lu>

TECHNISCHE UNIVERSITÄT DARMSTADT



http://www.flickr.com/photos/oliver_leitzgen/2781778797/

Digital Enhanced Cordless Telecommunications

TECHNISCHE UNIVERSITÄT DARMSTADT

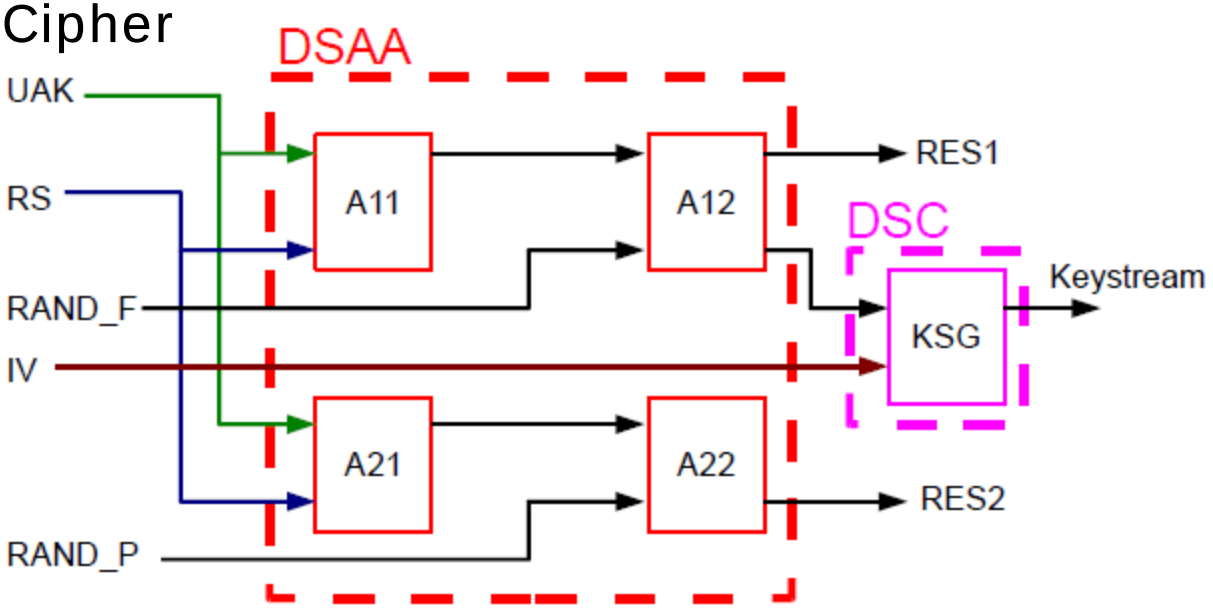
- Standard for short range portable phones
- Frequency around 1.9 GHz
- Range up to 300 meters for standard devices
- Invented in 1992
- More than 670,000,000 devices sold

http://www.flickr.com/photos/almekinders/2205176736/sizes/o/

DECT Security

TECHNISCHE UNIVERSITÄT DARMSTADT

- DECT uses two proprietary algorithms
- DSAA: DECT Standard Authentication Algorithm
  - Initial pairing of devices
  - (mutual) Authentication
  - Key Allocation
- DSC: DECT Standard Cipher
  - Encryption of traffic
  - Passive authentication
- Both are optional!



DECT standards were reverse-engineered

TECHNISCHE UNIVERSITÄT DARMSTADT

- Open security research started in 2006
- Project *deDECTed.org* in 2007/08 jointly worked on disclosing DECT security
  - Reverse engineering of DSAA
  - Partial reverse engineering of DSC
  - Found attacks on DSAA, PRNGs and DECT itself
  - Wrote open source sniffer for DECT PCMCIA Card
- First public talk at 25c3 (end of 2008, Berlin, Germany)

On to new research: DSC was reverse engineered

TECHNISCHE UNIVERSITÄT DARMSTADT

US005608802A

United States Patent [19]

Alvarez Alvarez

[11] **Patent Number: 5,608,802**

[45] **Date of Patent: Mar. 4, 1997**

[54] **DATA CIPHERING DEVICE**

[75] Inventor: **Manuel J. Alvarez Alvarez**, Madrid, Spain

[73] Assignee: **Alcatel Standard Electrica S.A.**, Madrid, Spain

[21] Appl. No.: **364,126**

[22] Filed: **Dec. 27, 1994**

[30] **Foreign Application Priority Data**

Dec. 31, 1993 [ES] Spain 9302742

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/50**; 380/28; 380/49

[58] **Field of Search** 380/28, 50, 9, 380/49, 4

[56] **References Cited**

U.S. PATENT DOCUMENTS

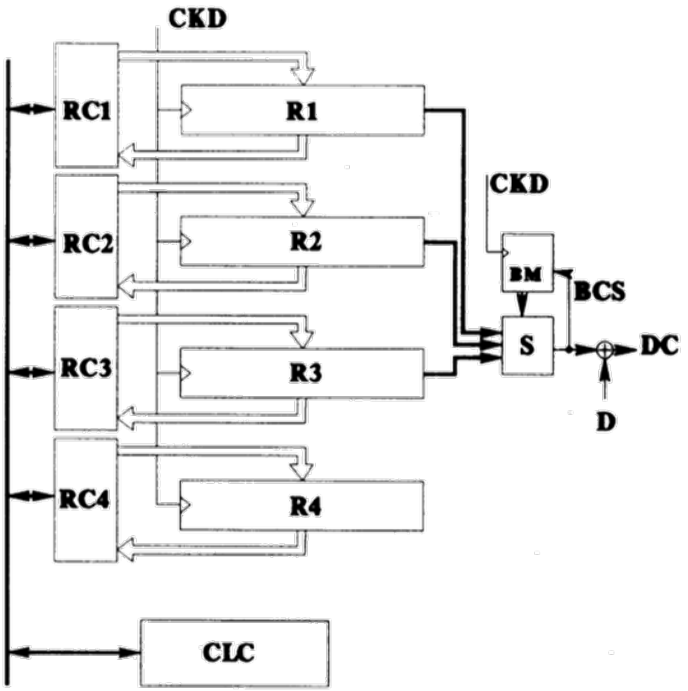
4,188,506 2/1980 Schmid et al. 380/50

Primary Examiner—David C. Cain
Attorney, Agent, or Firm—Ware, Fressola, Van Der Sluys & Adolphson

[57] **ABSTRACT**

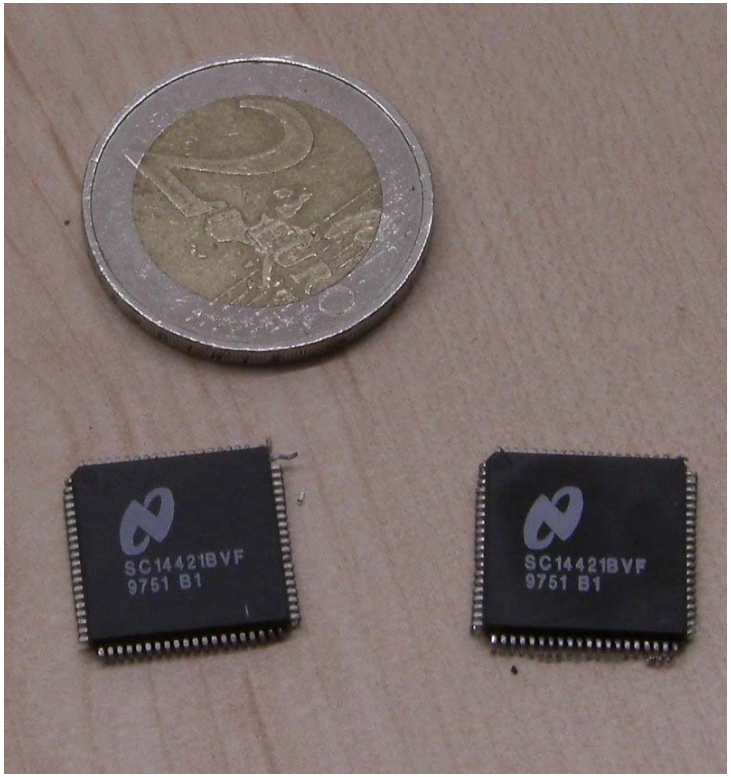
A data ciphering device that has special application in implementing the Digital European Cordless Telephone (DECT) standard data ciphering algorithm which requires a lengthy procedure of key loading and logic operations during the stages of pre-ciphering and ciphering which require clocks operating at different frequencies. The device performs parallel mode loading of the shift registers, with a ciphering keyword. It also calculates, in a first cycle, during the pre-ciphering, the values of the bits of each shift register that determine the value of the next shift in order to, in a second cycle, effect parallel mode shifting in these registers with a value equal to the sum of the two previous shift values. During the ciphering process, the shifting is done in the registers, in parallel mode and in a single data clock cycle, with a value equivalent to the serial value obtained by the algorithm.

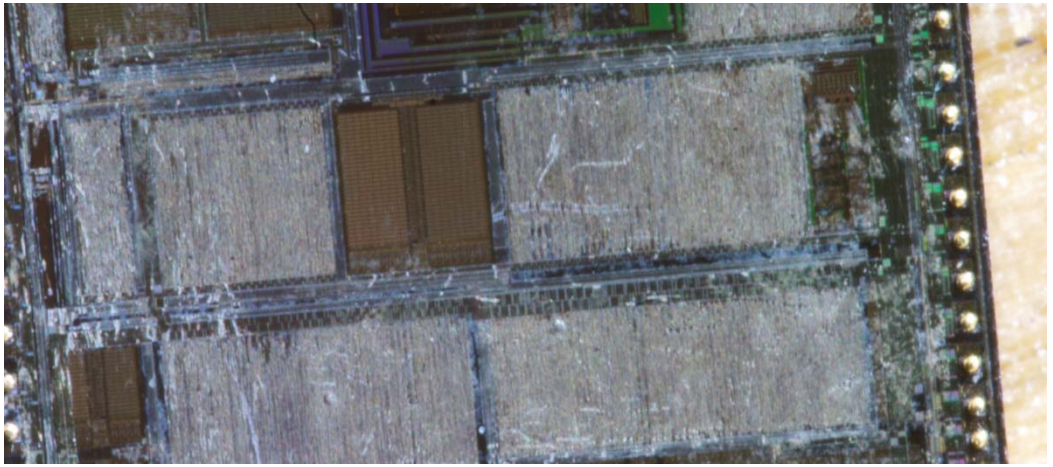
5 Claims, 3 Drawing Sheets

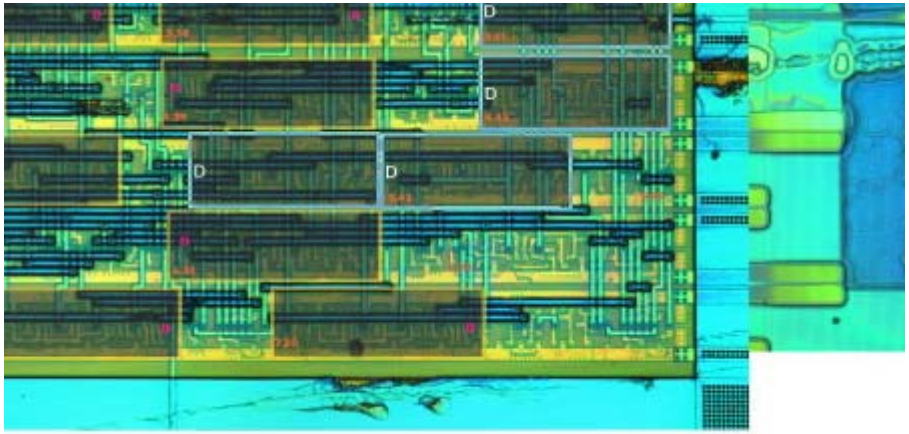


We also used Chip reverse engineering!

TECHNISCHE UNIVERSITÄT DARMSTADT







DSC can be accessed via firmware

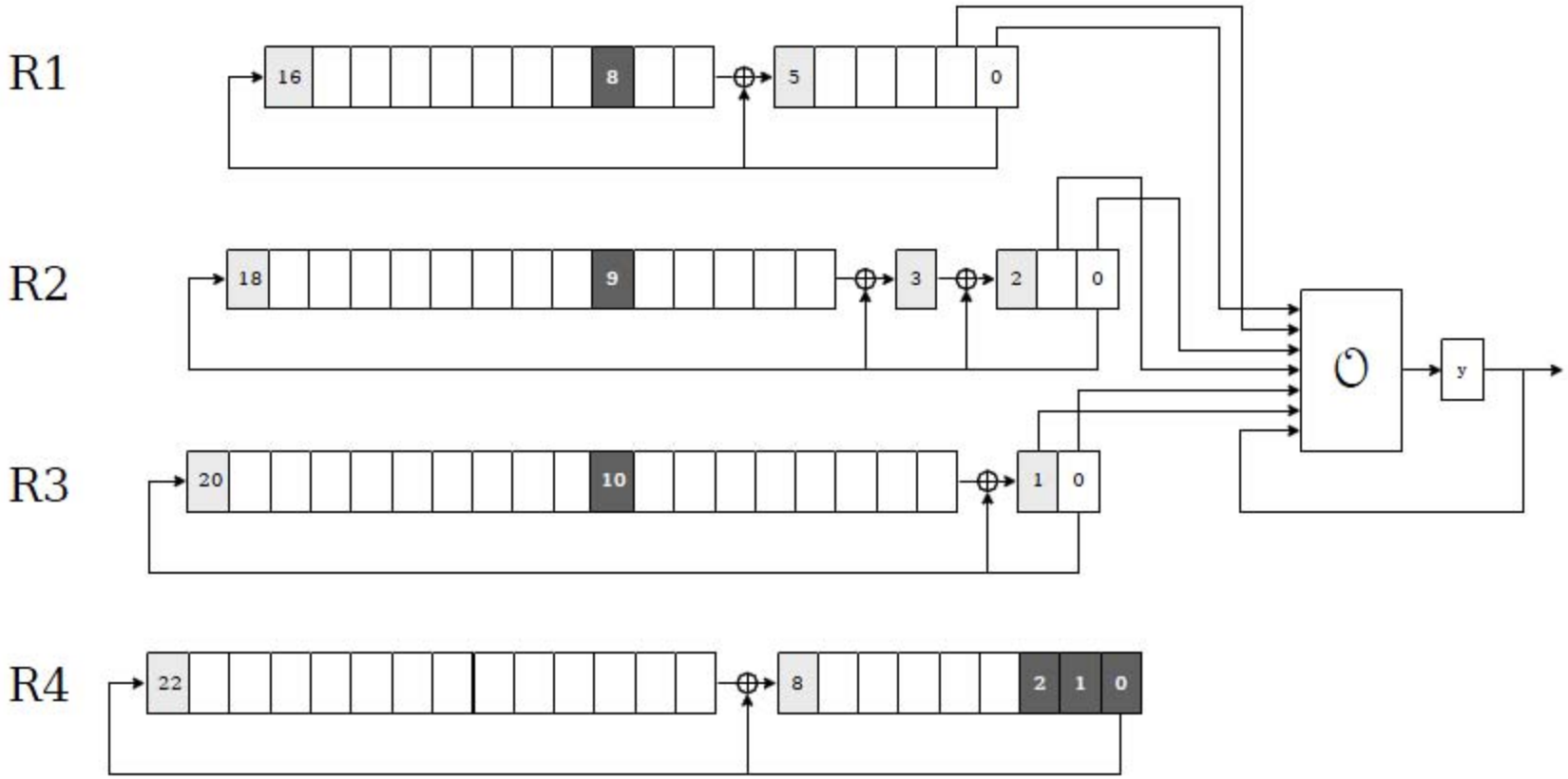
TECHNISCHE UNIVERSITÄT DARMSTADT

```
D_LDK memory        // Enable loading of IV || Key from &memory
WT 16               // Wait 16 clocks ( = 16 bytes)
D_LDK 0x0           // Disable loading of IV || Key
D_PREP              // Enable blank rounds
WT 39               // Wait 39 clocks ( = 40 rounds)
D_PREP              // Disable blank rounds

D_WRS state         // Enable writing of state to &state
WT 11               // Wait 11 clocks ( = 11 bytes of state)
D_WRS 0x0           // Disable writing of state
```

Result: The Cipher!

TECHNISCHE UNIVERSITÄT DARMSTADT



DSC compared to A5/1 is only weaker in a single dimension!

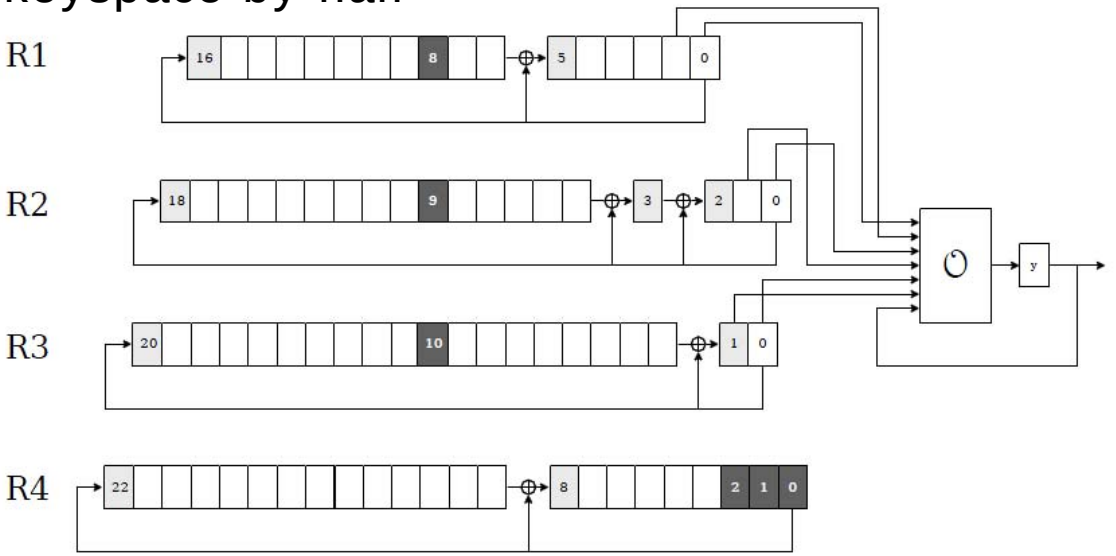
TECHNISCHE UNIVERSITÄT DARMSTADT

	A5/1	DSC
Number of registers	3	**4**
Irregular clocked registers	3	3
Internal state in bits	64	**81**
Output combiner	Linear	**Non-linear**
Bits used for output	3	**7**
Bits used for clocking	3	**6**
Clocking decision	0/1	**2/3**
Clocks per register until first bit of output	0 -100	**80-120**
Average clocks of registers until first bit of output	75	**100**
Pre-cipher rounds	**100**	40

DSC Cryptanalysis

TECHNISCHE UNIVERSITÄT DARMSTADT

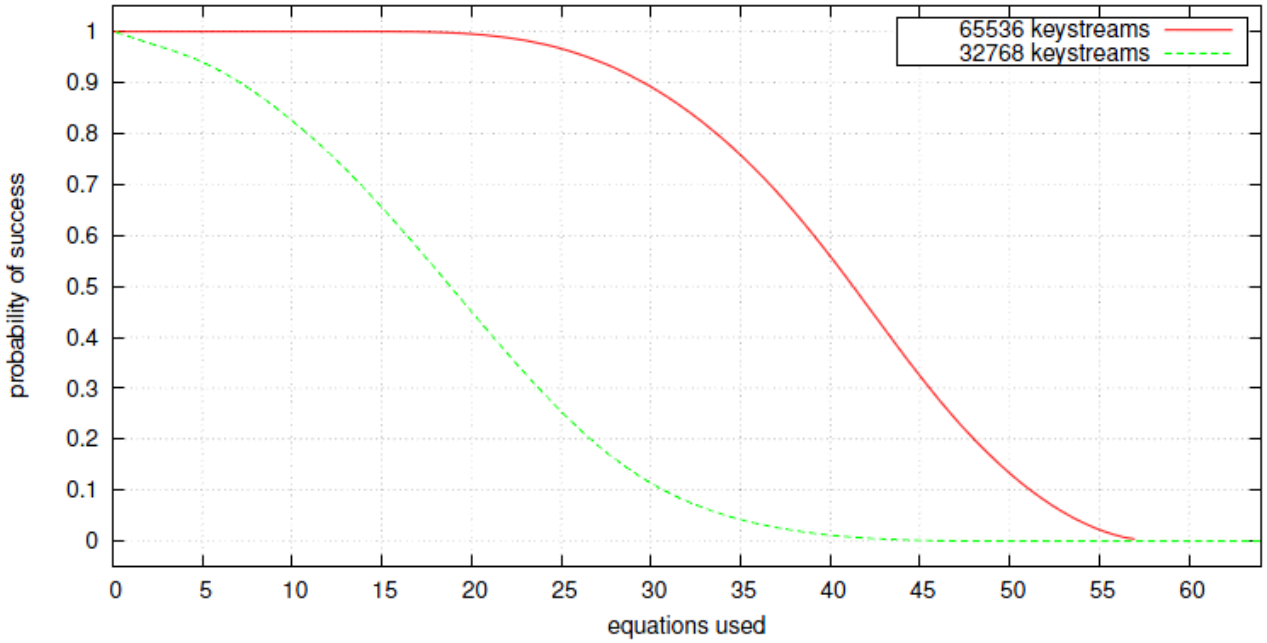
- Imagine:
  - All registers are clocked 103 times before the second bit of output is produced
  - The first and second bit of output allow you to eliminate half of the possible states at this time
  - This also reduces the keyspace by half
- This happens with probability 2^{-9}



An effective correlation attack on the DSC

TECHNISCHE UNIVERSITÄT DARMSTADT

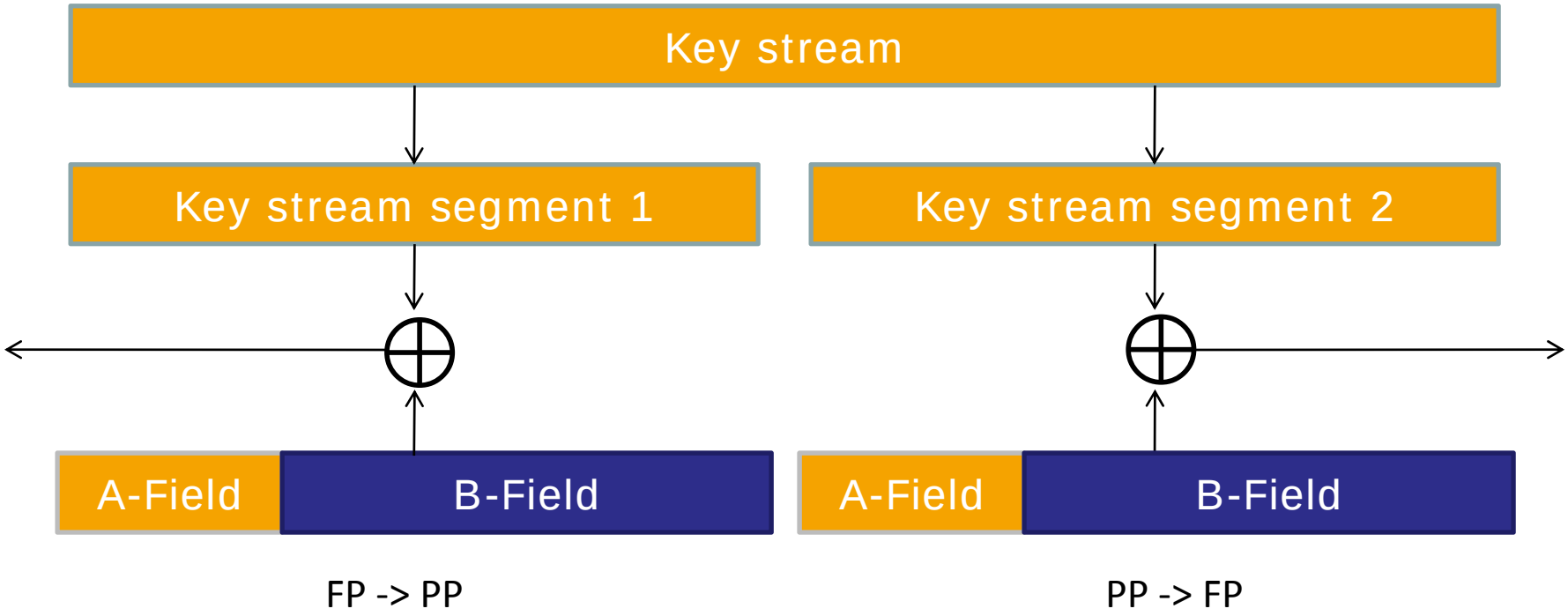
- Attack allows key recovery on a PC in minutes to hours with 2^{16} available keystreams
- Tradeoffs are possible
- Attack is much faster using Nvidia high-end graphic cards



Recovering Keystreams is possible

TECHNISCHE UNIVERSITÄT DARMSTADT

- The DECT C-channel transports control data
- First 40 bits of output are used to encrypt that data



Typical C-channel data

TECHNISCHE UNIVERSITÄT DARMSTADT

Encrypted	Decrypted (hex)	Decrypted (plain)
!2 1e b4 f5 69 8b	13 00 41 83 7b	A {
!1 1f b1 3d a0 61	28 0c 02 30 30	(0 0
!2 a9 02 d6 c0 bf	3a 30 30 3a 30	: 0 0 : 0
!1 5e f0 ca 6f fa	35 1a 0a 0d f0	5
	f0 f0 f0 b6 3d	=
	13 02 41 83 7b	A {
	28 0c 02 30 30	(0 0
	3a 30 30 3a 30	: 0 0 : 0
	36 1a 0a 0d f0	6
	f0 f0 f0 61 71	a q

Countermeasures and future work

TECHNISCHE UNIVERSITÄT DARMSTADT

- **SAGE Activity Report 2008:** …The Group produced a new set of algorithms for DECT based on AES – DECT Standard Cipher 2 (DSC2) and DECT Standard Authentication Algorithm 2 (DSAA2). …

- Improve the methods, how multiple correlations and keystream bits in this attack are used
- Find an attack on DSC which requires less keystreams

Contact and Questions?

TECHNISCHE UNIVERSITÄT DARMSTADT

Karsten Nohl nohl@cs.virginia.edu

Erik Tews e_tews@cdc.informatik.tu-darmstadt.de

Ralf-Philipp Weinmann ralf-philipp.weinmann@uni.lu

Thanks to Andreas Schuler, Patrick McHardy, Starbug, Flylogics and many more (including Alcatel) who helped!

Download the paper at: http://dedected.org/

Questions?