Breaking GSM phone privacy

Karsten Nohl, karsten@srlabs.de

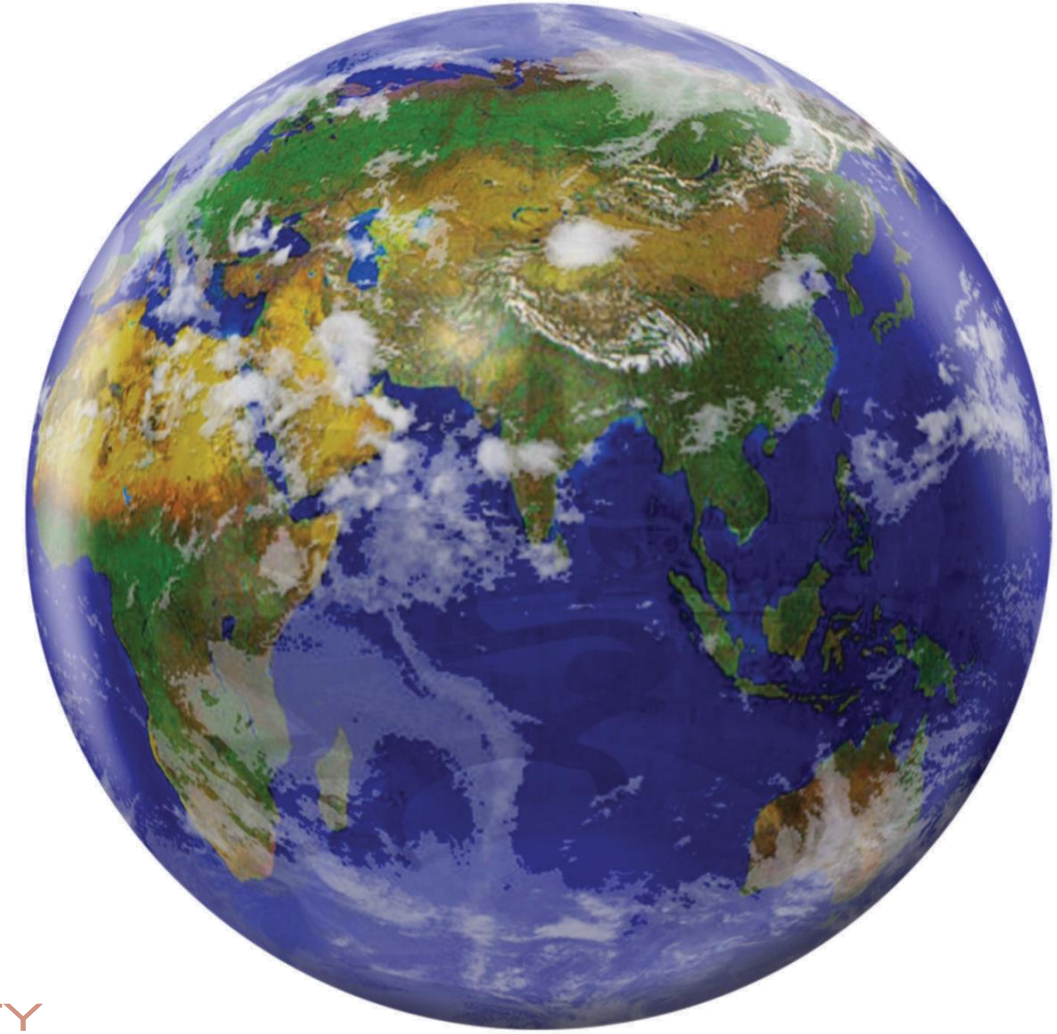
SECURITY RESEARCH LABS

GSM is global, omnipresent and wants to be hacked

80% of mobile phone market

200+ countries

5 billion users!



GSM encryption introduced in 1987 …

… then disclosed and shown insecure in 1994

SECURITY RESEARCH LABS

Source:Wikipedia, Bitkom press statement July 28th 2010

Industry responds to GSM cracker by creating a new challenge

"… the GSM **call has to be** identified and **recorded** from the radio interface. […] we strongly suspect **the team** developing the intercept approach **has underestimated its practical complexity**.
A hacker would need a radio receiver system and the **signal processing software** necessary to process the raw radio data."

– GSMA, Aug.'09

This talk introduces signal processing software to decode GSM calls

SECURITY RESEARCH LABS

Source: GSMA press statement

GSM uses symmetric session keys for call privacy

Operator and phone share a master key to derive session keys

Random nonce → Hash function
Master key → Hash function
Hash function → Session key

Operator Home Location Register

Random nonce and **session key** →

Base station

Random nonce →

Communication A5/1-encrypted with **session key** ↔

Cell phone

This talk discusses a technique for extracting session keys

SECURITY RESEARCH LABS

A5/1 is vulnerable to generic pre-computation attacks

Code book attacks

- Code books break encryption functions with small keys

Secret state	Output
A52F8C02	52E91001
62B9320A	52E91002
C309ED0A	52E91003

- Code book provides a mapping from known output to secret state
- An A5/1 code book is 128 Petabyte and takes 100,000+ years to be computed on a PC

This talk revisits techniques for computing an A5/1 code book fast and storing it efficiently

SECURITY RESEARCH LABS

Key requirement of code book generation is a fast A5/1 engine

Time on single threaded CPU: **100,000+ years**

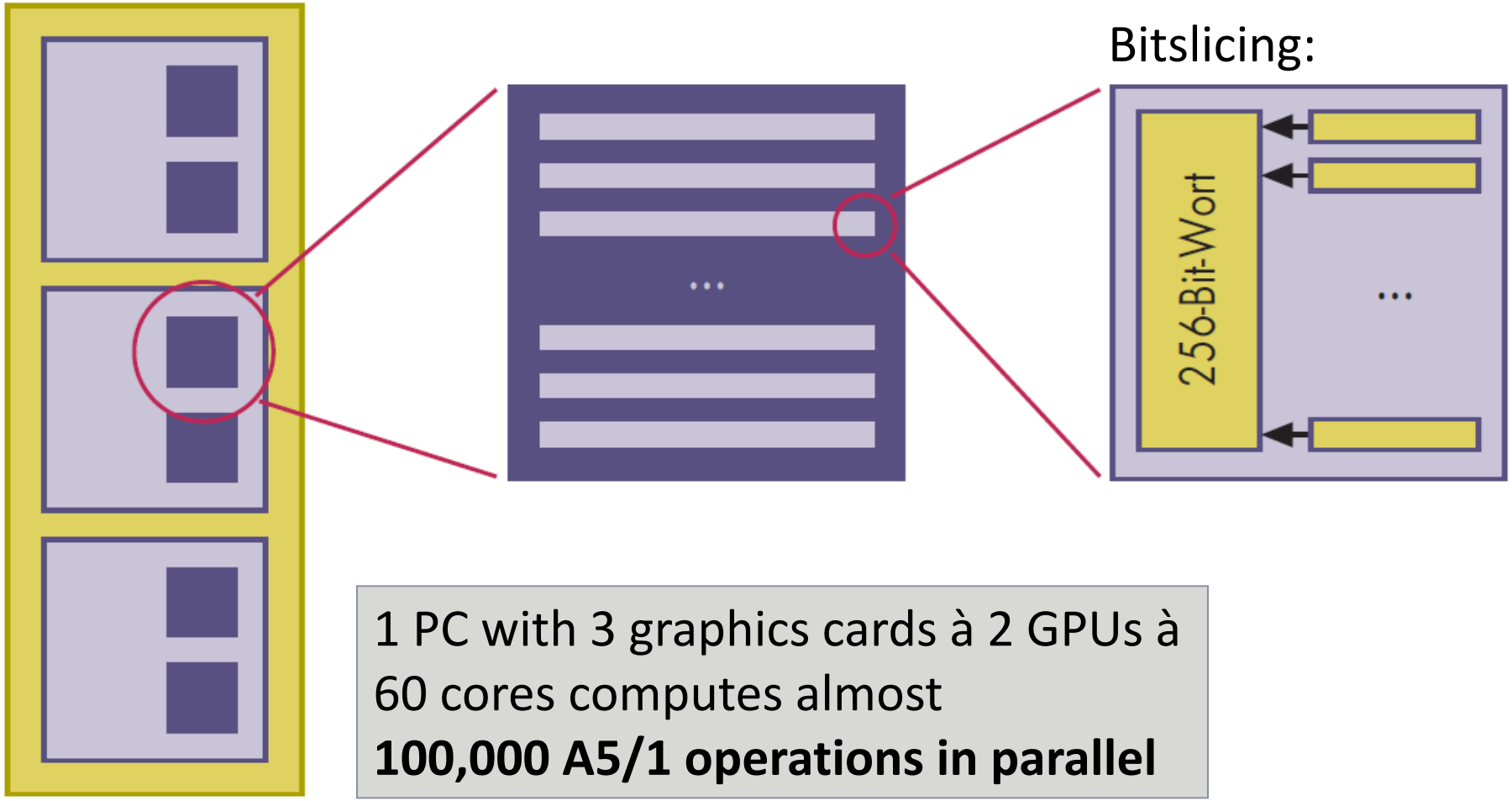
1. Parallelization
   - Bitslicing increases already large number of parallel computations by a factor of 256
2. Algorithmic tweaks
   - Compute 4 bits at once
3. Cryptographic tweaks
   - Executing A5/1 for 100 extra clock cycles decreases key space by 85%

Result: **1 month** on **4 ATI GPUs**

SECURITY RESEARCH LABS

*NVidia CUDA and ATI Brook GPUs are supported

1 GPUs allow for massive parallelization of code book computation

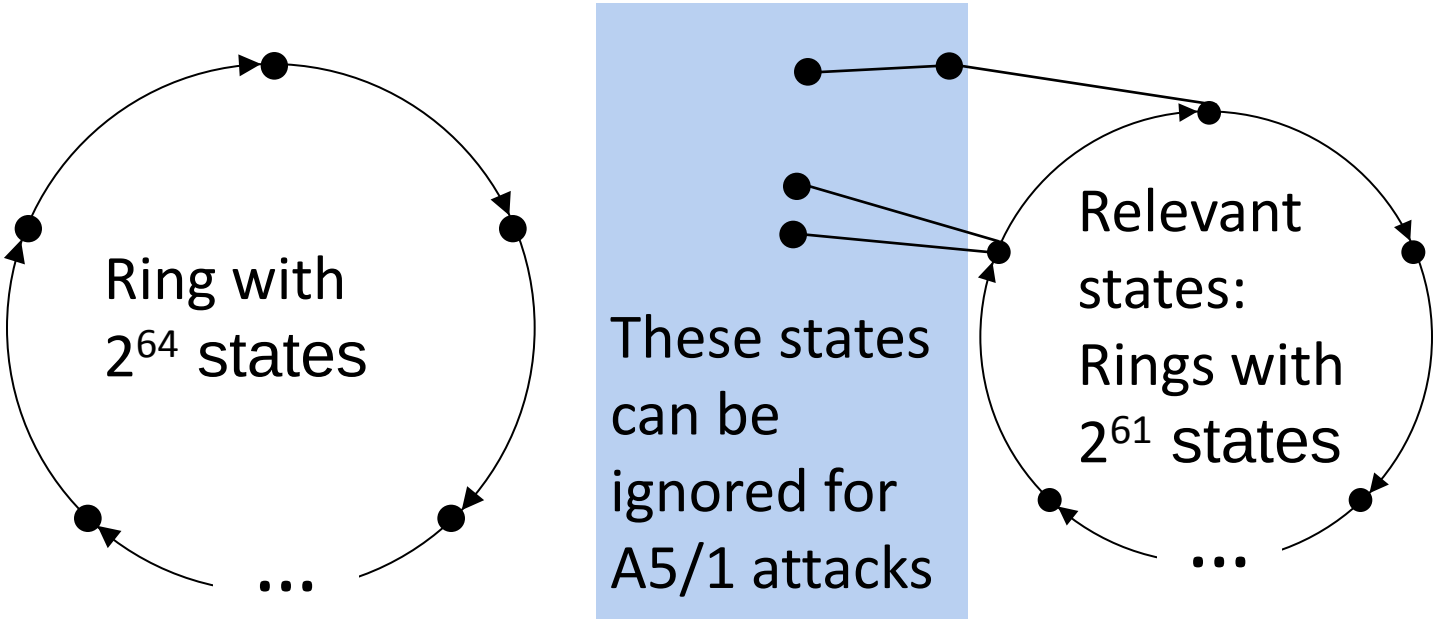


1 PC with 3 graphics cards à 2 GPUs à 60 cores computes almost **100,000 A5/1 operations in parallel**

SECURITY RESEARCH LABS

Source:iX 5/2010: Geheimnislos

3 A5/1 key space shrinks to 2^{61} secret states

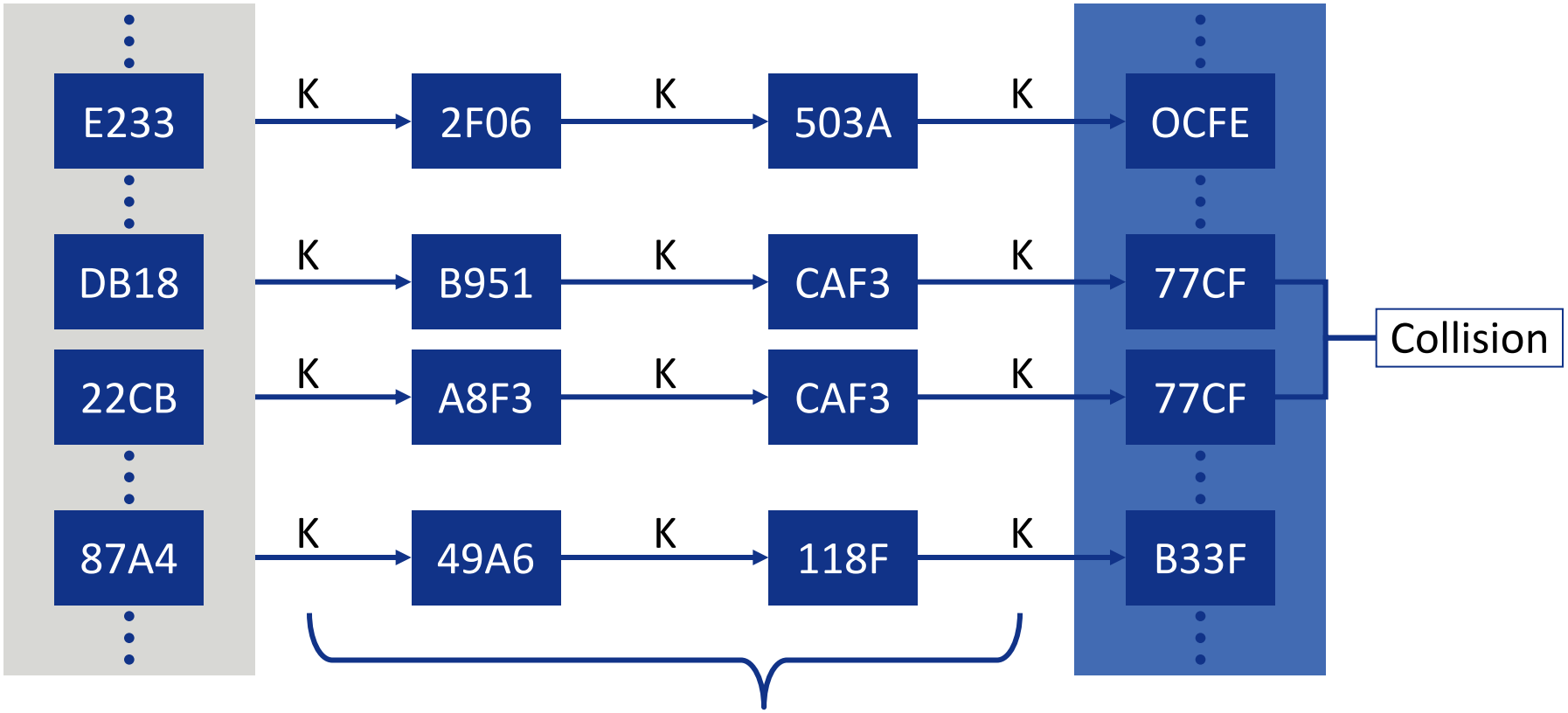


- LFSR used in older stream ciphers preserve the full output space of a function
- However, they have statistical weaknesses

- Newer stream ciphers therefore use NLFRs
- The output space of NLFSR slowly collapses
- The 100 extra A5/1 clocks in GSM shrink the output space by 85% (resulting in 30 faster cracking!)

SECURITY RESEARCH LABS

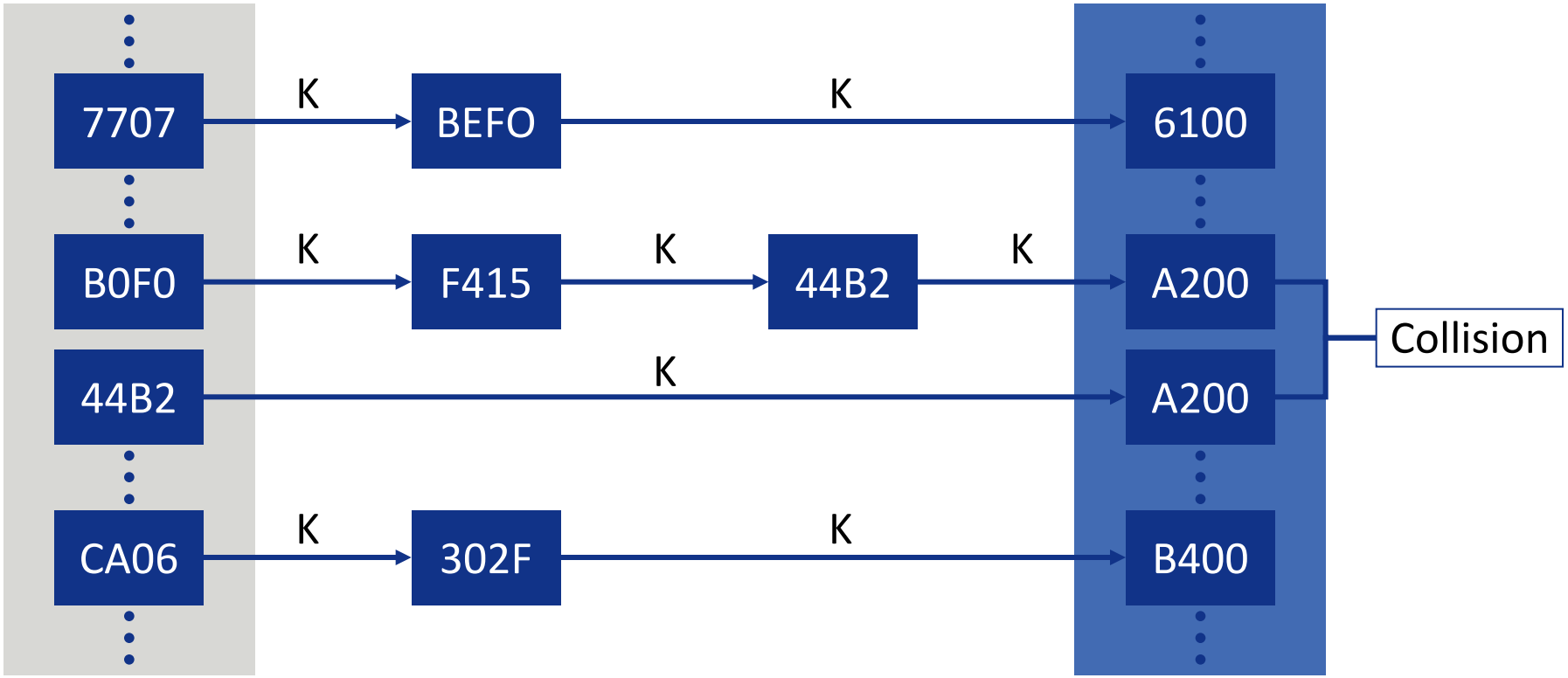
Pre-computation tables store the code book condensed



Longer chains := a) less storage, b) longer attack time

Source:c't

Distinguished point tables save hard disk lookups

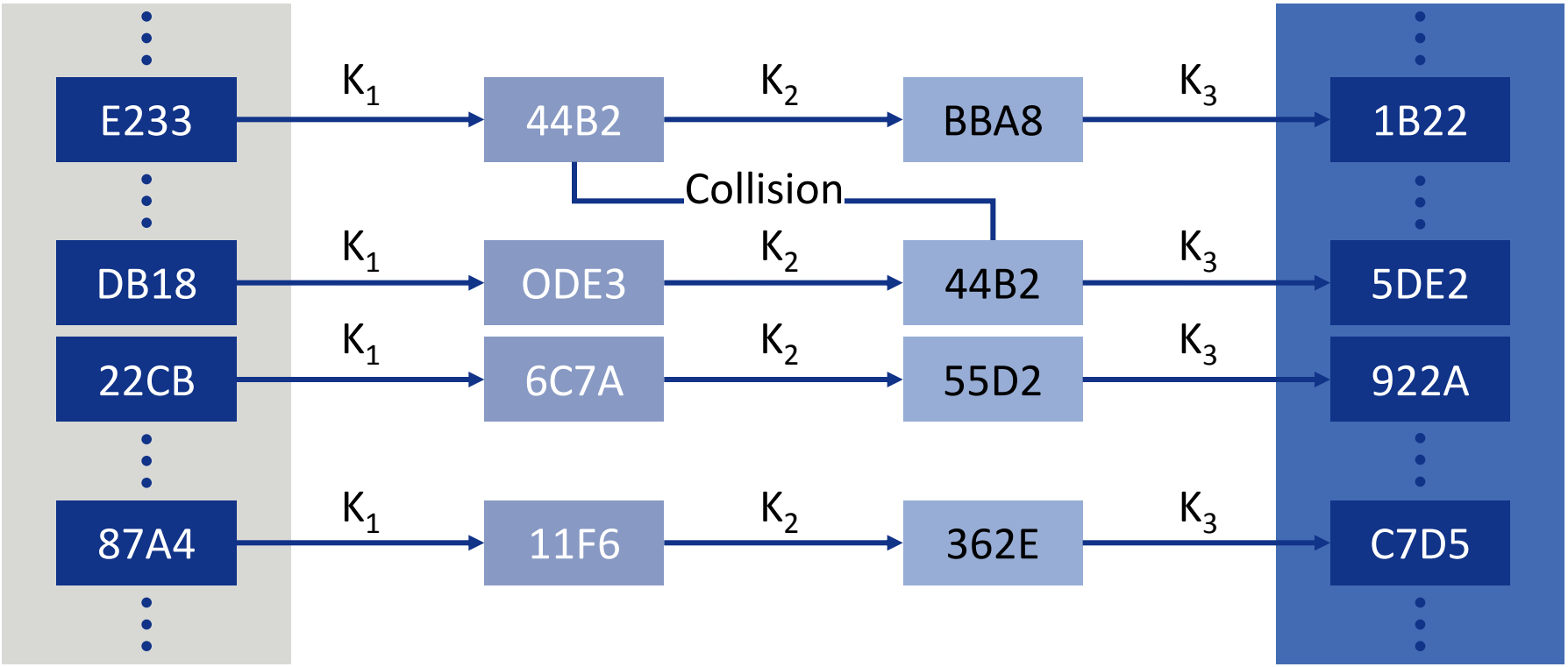


Hard disk access only needed at distinguished points

SECURITY RESEARCH LABS

Source:c't

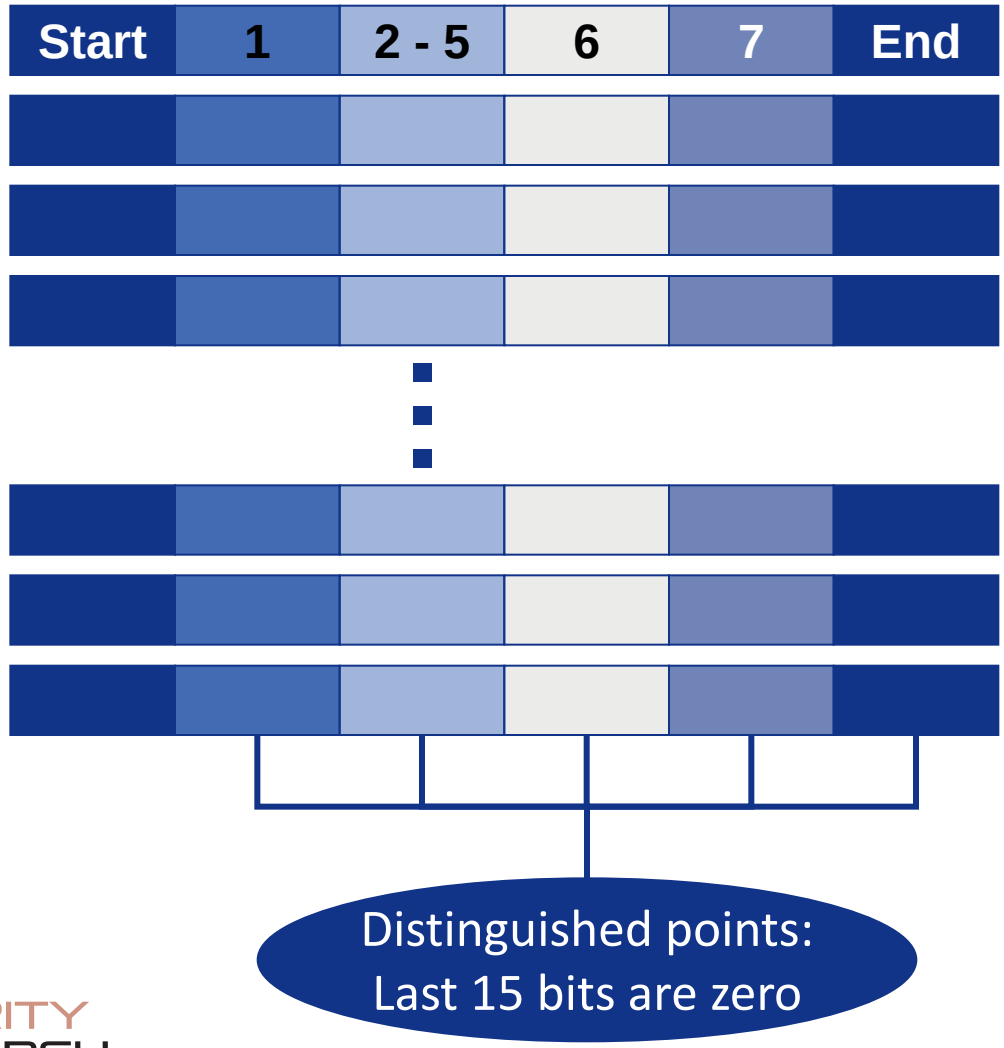
Rainbow tables mitigate collisions



Rainbow tables have no mergers, but an exponentially higher attack time

Source:c't

The combination of both table optimizations provides best trade-off



SECURITY RESEARCH LABS

Open source components fit together in analyzing GSM calls

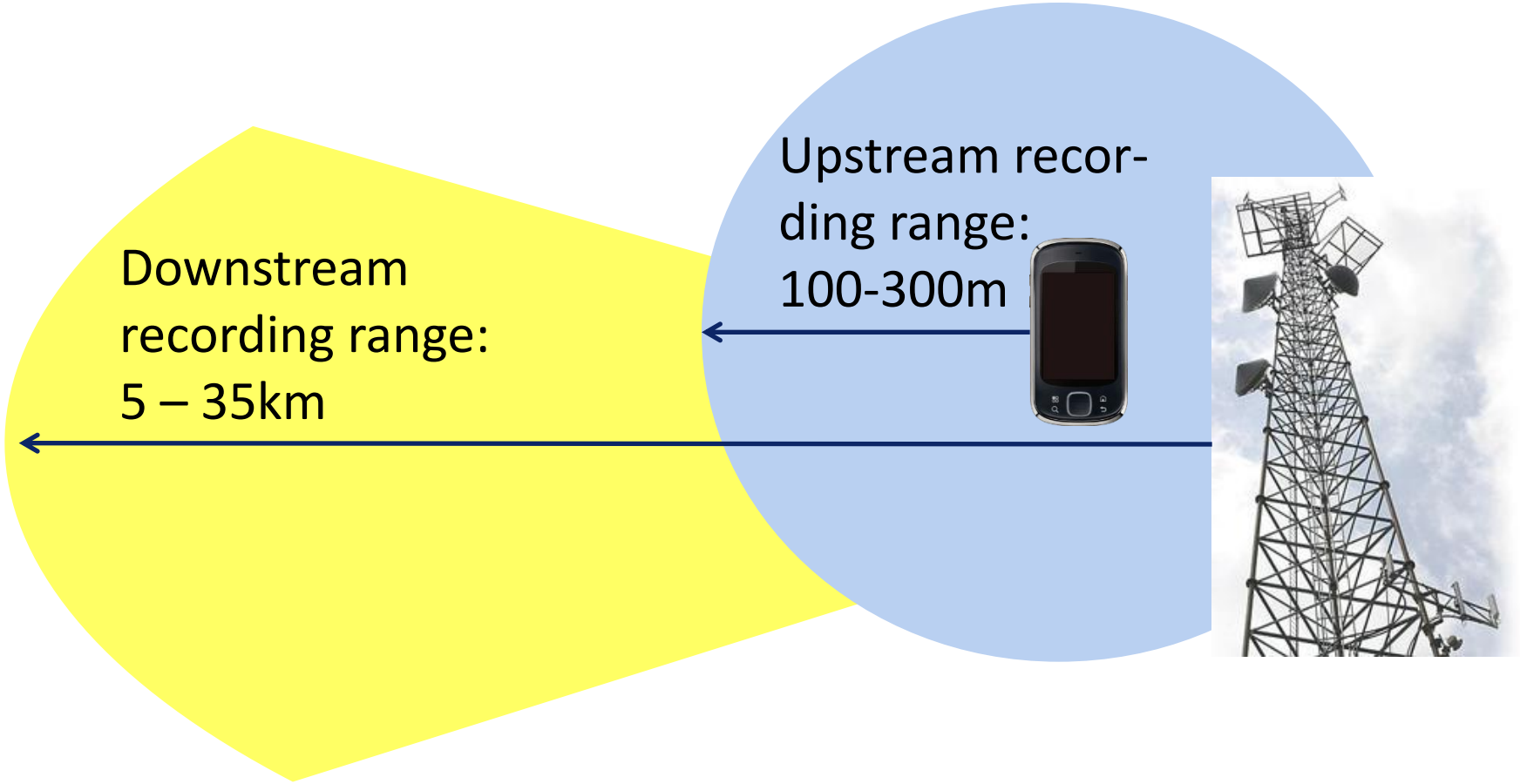
GnuRadio records data from air → Airprobe parses control data → Kraken cracks A5/1 key → Airprobe decodes voice

Requires
- Software radio, ie. USRP
- Recommended for upstream: BURX board

Requires
- 2TB of rainbow tables
- ATI graphics card and SSD/RAID for fast cracking

SECURITY RESEARCH LABS

Downstream can be recorded for large areas



SECURITY RESEARCH LABS

GSM discloses more known keystream than assumed in previous crack attempts

● Known Channel ○ Unknown Channel

	Frame with known or guessable plaintext	Assignment: Very early	Assignment: Early	Assignment: Late	Timing known through
Mobile terminated calls	1. Empty Ack after 'Assignment complete'	●	○	○	**"Stealing bits"**
	2. Empty Ack after 'Alerting'	○	○	○	
	3. 'Connect Acknowledge'	○	○	○	
	4. Idle filling on SDCCH (multiple frames)			●	
	5. System Information 5+6 (~1/sec)	◐	○	◐	
	6. LAPDm traffic	●	●	●	**Counting**
Network terminated calls	1. Empty Ack after 'Cipher mode complete'	●	●	●	**Counting frames**
	2. 'Call proceeding'	●	●	●	
	3. 'Alerting'	●	○	●	**"Stealing bits"**
	4. Idle filling (multiple frames)			●	
	5. 'Connect'	●	○	○	
	6. System Information 5+6 (~1/sec)	◐	○	◐	
	7. LAPDm	●	●	●	**Counting**

SECURITY RESEARCH LABS

Source:GSM standards

Randomized padding would mitigate attack potential

SDCCH trace	
238530	03 20 0d 06 35 11 **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238581	03 42 45 13 05 1e 02 ea 81 5c 08 11 80 94 03 98 93 92 69 81 **2b 2b 2b**
238613	00 00 03 03 49 06 1d 9f 6d 18 10 80 00 00 00 00 00 00 00 00 00 00 00
238632	01 61 01 2b **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238683	01 81 01 2b **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238715	00 00 03 03 49 06 06 70 00 00 00 00 00 04 15 50 10 00 00 00 00 0a a8
238734	03 84 21 06 2e 0d 02 d5 00 63 01 **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238785	03 03 01 **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**

Padding in GSM has traditionally been predictable (2B)

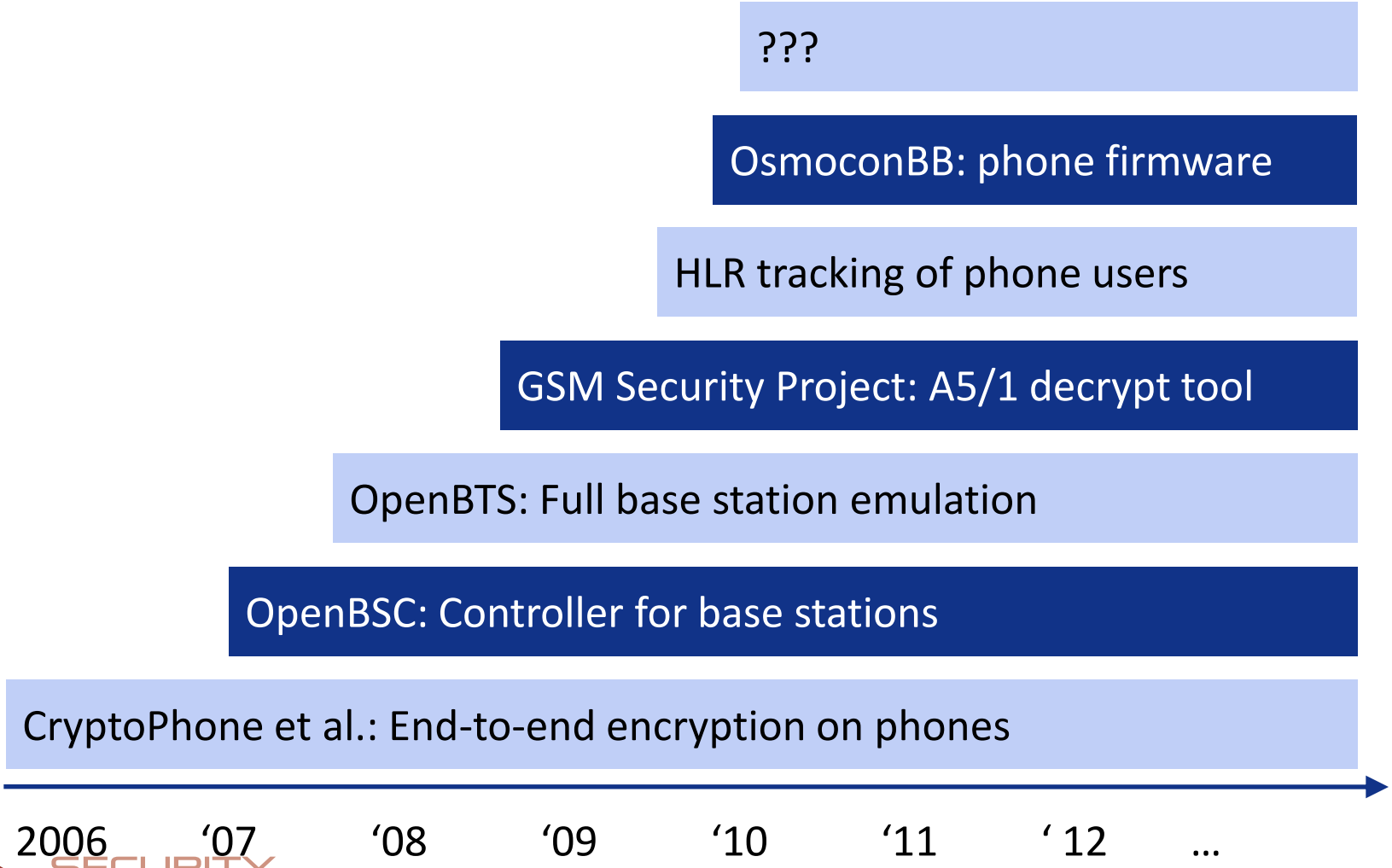
Every byte of randomized padding increasing attack cost by two orders of magnitude!

Randomization was specified in 2008 (TS44.006) and should be implemented with high priority

Additionally needed: randomi-zation of system information msg.

SECURITY RESEARCH LABS

Open research into GSM security grows exponentially



SECURITY RESEARCH LABS

Questions?

Research supported by

Tables, Airprobe, Kraken	srlabs.de
Project Wiki	reflextor.com/trac/a51

Karsten Nohl	**karsten@srlabs.de**

Many thanks to Sascha Krißler, Frank A. Stevenson, MvdS, Dieter Spaar, Harald Welte, Philipp Maier and David Burgess!

SECURITY RESEARCH LABS