Open encryption technology and social movements

2013 Cryptologic History Symposium
17-18 October

Niels Jørgensen

Roskilde University, Denmark

nielsj@ruc.dk

Research questions

1) How did the Chaos Computer Club break the user authentication method in GSM 2nd Gen.?

2) What would be a good conceptual framework
for describing social movements
that were part of the 1990s' crypto controversies?

Conceptual framework

- eg. Dennings' activism / hacktivism / cyberterrorism

Social movements

- hackers, privacy rights activists, if organized

Crypto controversies

- should (can) strong encryption be restricted by government?

Plan of talk

1) Case

The cloning in 1998 of a GSM 2nd Generation SIM-card by the Chaos Computer Club, Germany

2) Analysis

Existing conceptual frameworks

- hackers; social movements
- useful, but insufficient

Jamison's *The Making of Green Knowledge*, 2001

- conceptual framework should include technology

  how did the CCC-hackers use + create technology,
  in the process of struggling over technology

Crypto controversies

Started early 90s: phone/internet encryption a possibility

Ended ~2000: Strong, open encryption became dominant

- perhaps social movements influenced this?

US

- Standardization of AES (2001)
- Key escrow initiatives discontinued (~2000)
- Export restrictions lifted (2000, 2004)

Europe

- GSM 3rd Gen.: strong, open encryption (UMTS, 1999)
- Encryption restrictions lifted (France)
- Encrypt. regulation initiatives discontinued (UK, 2000-2005)

Studies of the crypto controversies

Include accounts by participants in the 1990s' debates:

Politics, activism

- *“Privacy advocates convinced the government”*
  NSA Director McConnell (The New Yorker, 2008)

Economics

- *“Businesses demanded strong encryption”*
  Diffie & Landau: “Privacy on the line” (2007)

Technical

- *“Key escrow was technically infeasible”*
  Matt Blaze: “Encrypting history at the NSA” (2008)

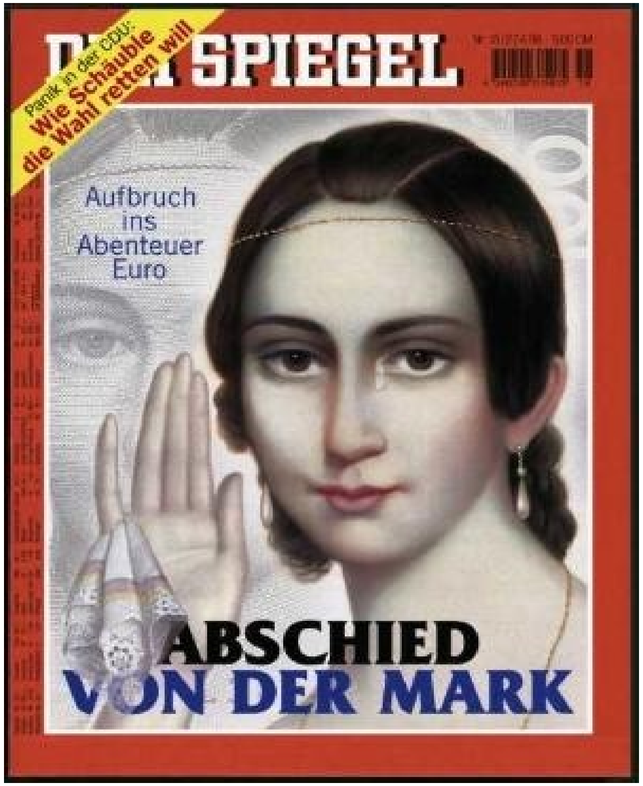
Case:
SIM-car cloning by the Chaos Computer Club

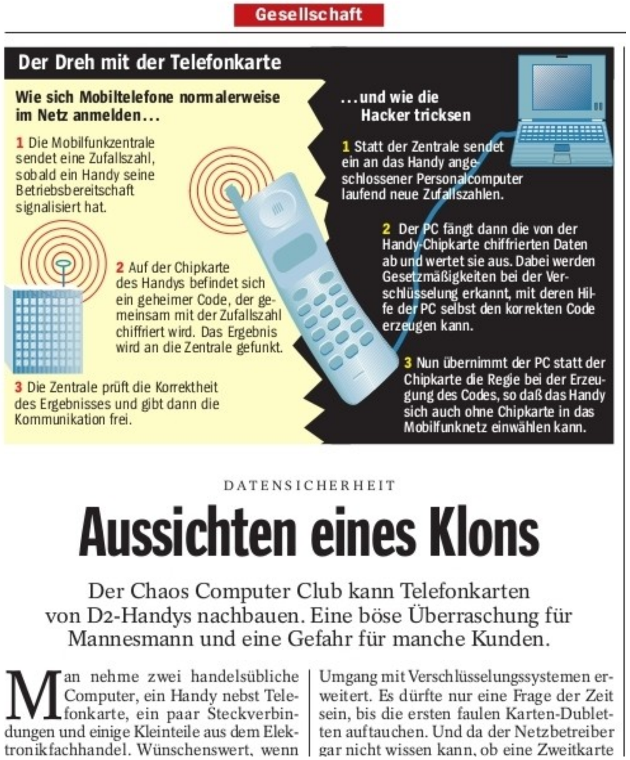
CCC is a German hacker group
•1981-present

Members of CCC cloned a GSM 2nd Generation SIM-card from operator D2

Used clone to make calls..
.. masquerading as the subscriber that holds the original card

Published in “Der Spiegel”,
april 1998


Panik in der CDU:
Wie Schäuble die Wahl retten will
DER SPIEGEL
Aufbruch ins Abenteuer Euro
ABSCHIED VON DER MARK



Gesellschaft

Der Dreh mit der Telefonkarte

Wie sich Mobiltelefone normalerweise im Netz anmelden...

1 Die Mobilfunkzentrale sendet eine Zufallszahl, sobald ein Handy seine Betriebsbereitschaft signalisiert hat.

2 Auf der Chipkarte des Handys befindet sich ein geheimer Code, der gemeinsam mit der Zufallszahl chiffriert wird. Das Ergebnis wird an die Zentrale gefunkt.

3 Die Zentrale prüft die Korrektheit des Ergebnisses und gibt dann die Kommunikation frei.

...und wie die Hacker tricksen

1 Statt der Zentrale sendet ein an das Handy angeschlossener Personalcomputer laufend neue Zufallszahlen.

2 Der PC fängt dann die von der Handy-Chipkarte chiffrierten Daten ab und wertet sie aus. Dabei werden Gesetzmäßigkeiten bei der Verschlüsselung erkannt, mit deren Hilfe der PC selbst den korrekten Code erzeugen kann.

3 Nun übernimmt der PC statt der Chipkarte die Regie bei der Erzeugung des Codes, so daß das Handy sich auch ohne Chipkarte in das Mobilfunknetz einwählen kann.

DATENSICHERHEIT

Aussichten eines Klons

Der Chaos Computer Club kann Telefonkarten von D2-Handys nachbauen. Eine böse Überraschung für Mannesmann und eine Gefahr für manche Kunden.

Man nehme zwei handelsübliche Computer, ein Handy nebst Telefonkarte, ein paar Steckverbindungen und einige Kleinteile aus dem Elektronikfachhandel. Wünschenswert, wenn

Umgang mit Verschlüsselungssystemen erweitert. Es dürfte nur eine Frage der Zeit sein, bis die ersten faulen Karten-Dubletten auftauchen. Und da der Netzbetreiber gar nicht wissen kann, ob eine Zweitkarte

The SIM-card in GSM security

User/subscriber authentication is by a “two-factor” method:
#1) user must *know* PIN-code
to uncover unique IMSI# from SIM-card
#2) user must *possess* SIM-card,
with its unique 128 bit *secret* key K (K_i)

OBS: K is secret to prevent cloning

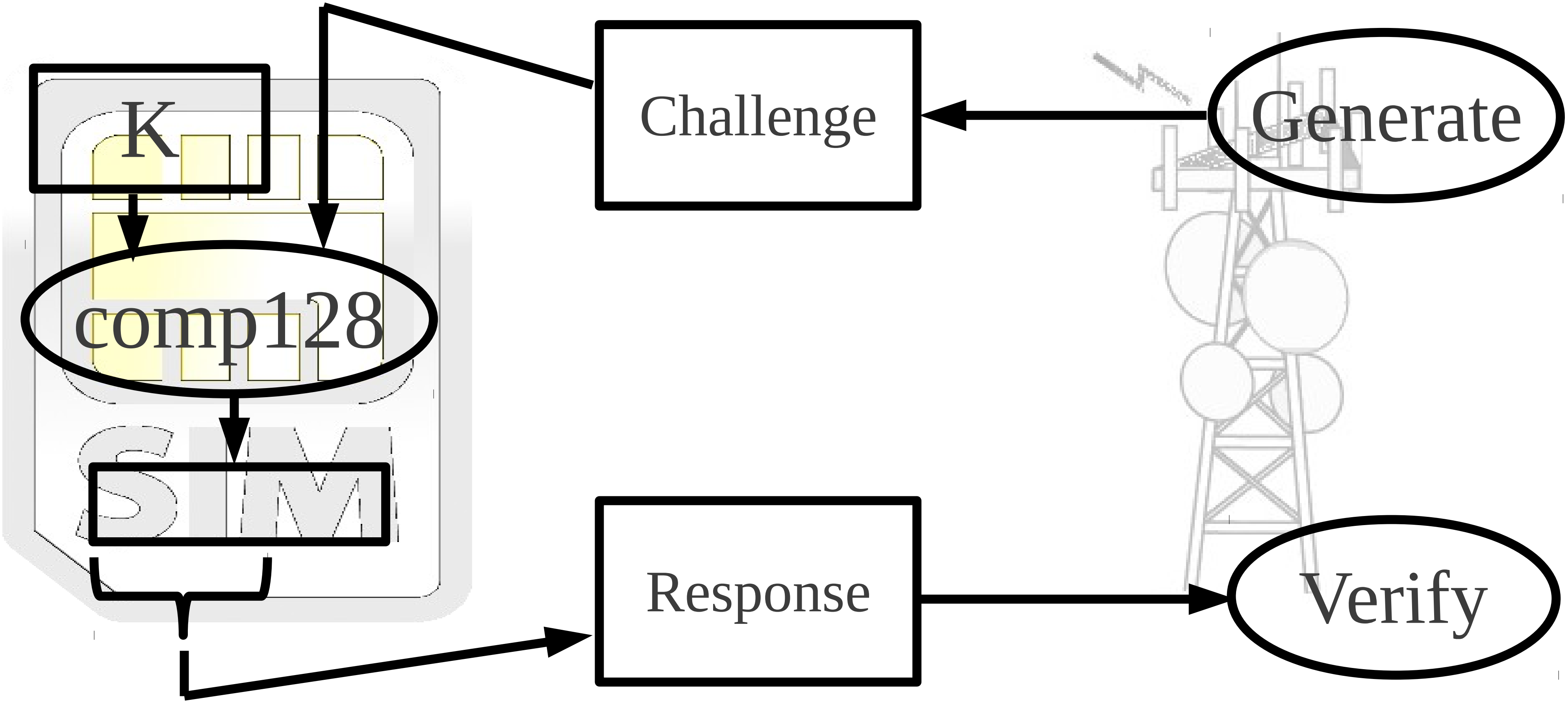
Members of the CC were able to uncover K

- by probing the card's standard interface
- not tampering
- then make phone calls without the SIM-card

Factor #2

GSM 2nd G. authentication uses a function called “comp128”

- in a challenge-response protocol
- response proves SIM-card has correct key K



comp128 ..

.. is a hash (compression) function

- input 256 bits (K + challenge)
- output 128 bits (of which 32 bits form the response)
- 8 rounds of: add K + compress in 5 steps + permute

.. implements "A3" in G2 spec.

- a "reference" implementation used by most operators
- specified ~1988, leaked 1997-98, reverse engineered

.. cryptanalyzed in 1998

- Goldberg, Wagner (UC Berkeley), Briceno (Smartcard D.A.)
- collision attack: recover two bytes of K at a time
- violation of "strong collision resistance"
- "not a novel attack"
    - black-box cryptanalysis (Schnorr & Vaudenay, 1993)

What the Chaos Computer Club did

Made the Goldberg, Wagner & Briceno attack practical

recovered key K in 11 hours
- using self-engineered card reader
- cryptanalysis implemented on ordinary PC

then made actual phone calls
- using self-engineered interface to mobile phone
- SIM-card emulator on PC
- calls worked
- except simultaneous calls blocked by network (original SIM-card + clone)

Der Spiegel, April 1998

Avoid “Unsicherheit bei Geheimniskrämerei”. (Müller-Maguhn, CCC)

Customers need not worry. Cloning requires theft of SIM-card + PIN-code. (Kuczkowski, D2)

Vendors can clone SIM-cards

schlüsselt, vor allem dient der eingesetzte Chip dazu, den Handy-Besitzer beim Mobilfunkbetreiber zu identifizieren.

Rechner, Handys und Elektronikkram lagern in den Räumen des Chaos Computer Clubs (CCC) zuhauf – und so ließen die deutschen Elitehacker vergangene Woche den Alptraum der Firma Mannesmann Mobilfunk wahr werden: Sie entschlüsselten eine D2-Mobilfunkkarte und kopierten deren Datensatz in ihrem Computer.

Bösewichter könnten diese Kopie nutzen, um zu telefonieren – kostenlos, denn die Rechnung ginge an den Besitzer der Originalkarte.

Noch müssen die rund drei Millionen D2-Kunden nicht fürchten, daß schon morgen 16jährige Computerfreaks auf ihre Kosten mit der halben Welt telefonieren, doch die Erfolgsstory von Mannesmann Mobilfunk wird um ein häßliches Kapitel über mangelnde Datensicherheit und sorglosen

ka eren – mit geklauter wie mit geklon e.

Die g dürfte allerdings, weil's schneller a auch schneller gesperrt werden als di klonte. Potentielle Abnehmer für Kart oppel gibt es genug:

Ide ch Ki nicht mehr erken lassen gebnis wird an D geschic ler Rechner gleiche rfel nen vor nommen Grafik). Kommt er zu dem rgebnis wie das Handy, gilt

N. MICHALKE

T. GEIGER / TANDEM

Hacker Müller-Maguhn, D2-Chef Kuczkowski: *Häckselmaschine mit Macken*

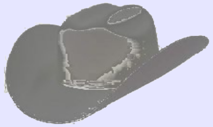
98

DER SPIEGEL 18/1998

Analysis: concepts from analyses of hackers

Dennings, 2001

- activism, hacktivism, cyberterrorism
- hacktivism = “marriage of hacking and activism”
- “disrupting normal operations but not causing serious damage”
- resembles white hat / grey hat / black hat distinction

Concept	*Chaos Computer Club, the GSM hack*
Unlawful damage	•GSM cloning legal •jail sentence, phone stealing  •jail sentence, espionage

Concepts from social movements studies

McAdams et al. (1996)

- mobilizing structure / opportunity structure / framing struct.
- typical case: civil rights movement

Concept	*Chaos Computer Club, the GSM hack*
Organization	Formal •board, membership, journal, conferences Informal •network, non-members, Erfa-Kreise
Alliances	Concerns in Germany about surveillance

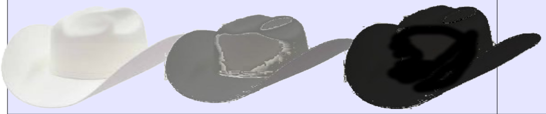
The Making of Green Knowledge (Jamison, 2001)

Social movements as cognitive praxis, with
- world view (ecology; sustainability; ..)
- technical issues knowledge

Environmental movement in Denmark
- built windmills (1890s, 1950s, 1970s)
- Danish “windmill adventure”
  - 20% of electrical energy (today)
  - ~ 50% of world market for windmills (1990s)

New technology was created in the movement
- windmills built as “proof of concept”

Extended set of concepts

Concept	*Chaos Computer Club, the GSM hack*
	
Organization	
Alliances	
..	
Technology •novelty? •purpose? •impact? •..	•*made a theoretical attack practical* •*demonstration (not use)* •*perhaps one small step towards GMS 3G*

Discussion

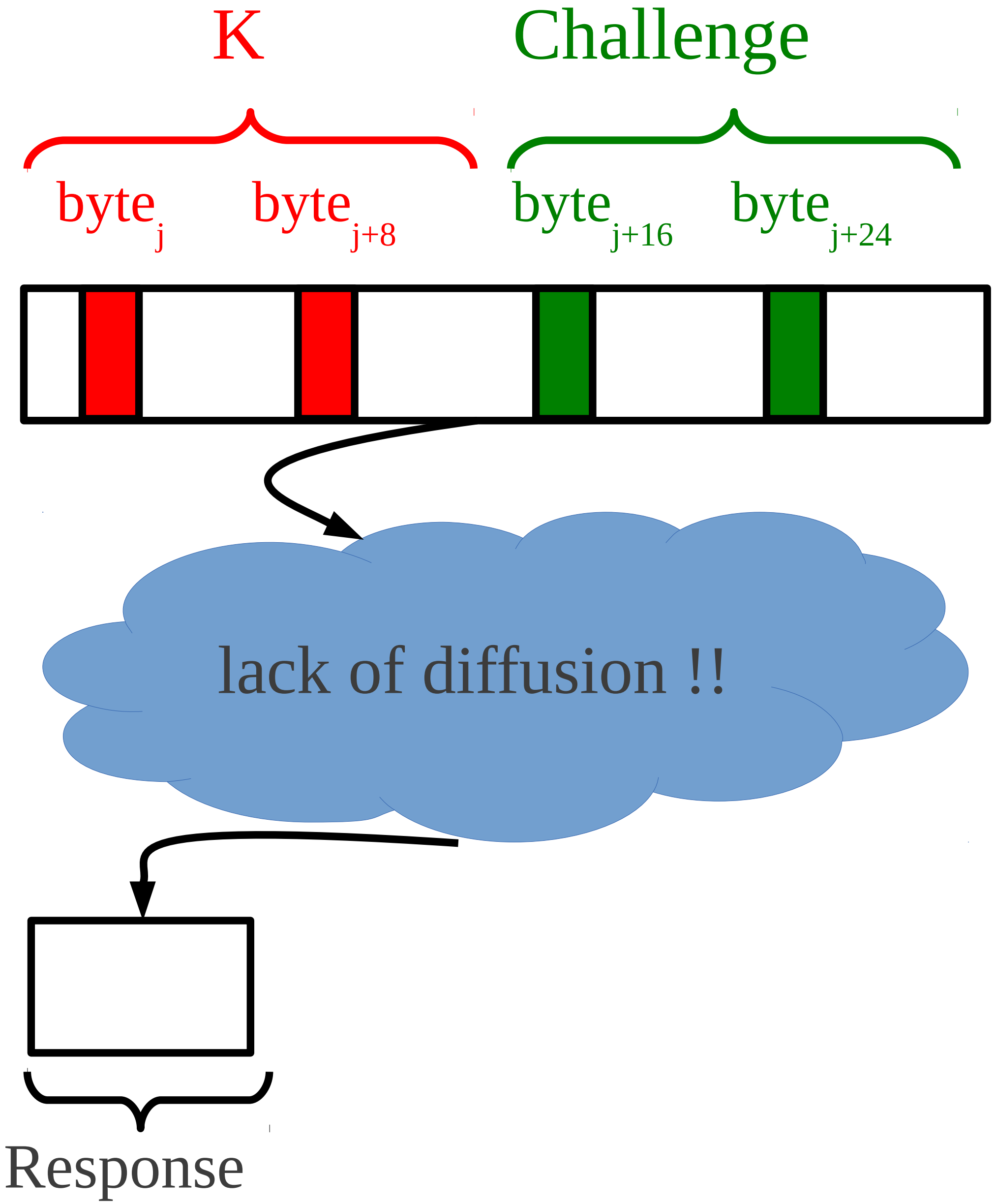
Novelty: *made a theoretical attack practical*

- compare DES-cracker by EFF (1998)
- the theory/practice gap can be large
- there are $2^{76.7}$ keys that protect against the attack (Wray 2003)

Purpose: *demonstration (not use)*

- cryptanalysis can play a constructive role
  - GSM 3rd G. had stronger hash functions
- other products were made for use, during the controversy
  - PGPmail, PGphone by Phil Zimmermann

The comp128 collision attack (Wray, 2003)



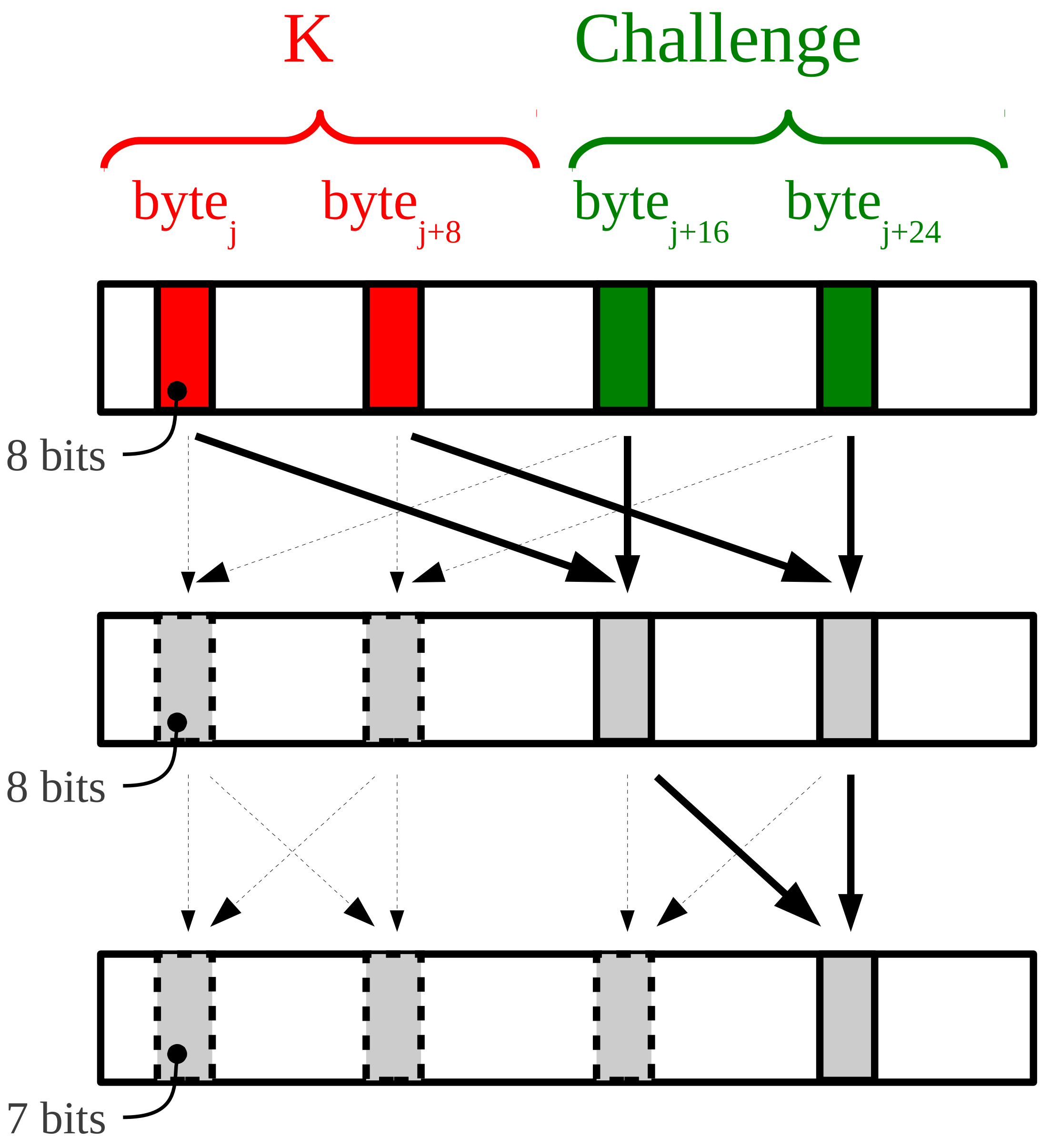
For j=0,..7 do:

1) Probe SIM-card to find two pairs of bytes (b_{j+16}, b_{j+24}), (b'_{j+16}, b'_{j+24}) that collide

2) Use comp128 to find a pair (b_j, b_{j+8}) that collides with both pairs from step 1

Search space: 2^{2*8}

The comp128 collision attack (Wray, 2003)



First round, first two steps

For j=0,..7 do:

1) Probe SIM-card to find two pairs of bytes (b_{j+16}, b_{j+24}), (b'_{j+16}, b'_{j+24}) that collide

2) Use comp128 to find a pair (b_j, b_{j+8}) that collides with both pairs from step 1

Search space: 2^{2*8}

Collision space: 2^{4*7}