Do you trust the cryptography used in your devices?

Roel Verdult

Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands.

✉ *rverdult@cs.ru.nl* 🖱 *www.cs.ru.nl/~rverdult*



Introduction

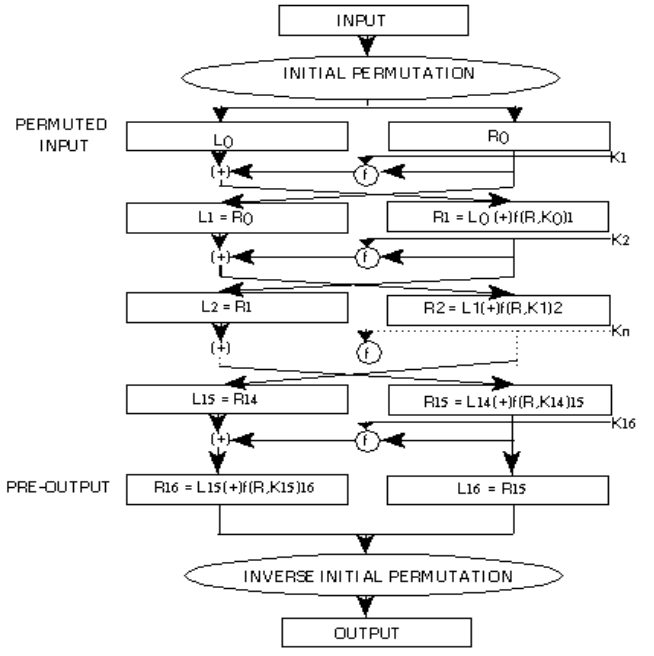
- Attack complexity and brute-force on an average PC
  - $2^0 = 1$
  - $2^{10} = 1{,}024$
  - $2^{20} = 1{,}048{,}576$ (<1 second)
  - $2^{32} = 4{,}294{,}967{,}296$ (~1 minute)
  - $2^{40} = 1{,}099{,}511{,}627{,}776$ (~1 hour)
  - $2^{48} = 281{,}474{,}976{,}710{,}656$ (~1 month)
  - $2^{56} = 72{,}057{,}594{,}037{,}927{,}940$ (~2 decades)
  - $2^{64} = 18{,}446{,}744{,}073{,}709{,}551{,}616$ (~50 centuries)
  - $2^{128} = 340{,}282{,}366{,}920{,}938{,}463{,}463{,}374{,}607{,}431{,}768{,}211{,}456$

Publicly Scrutinized Cryptography



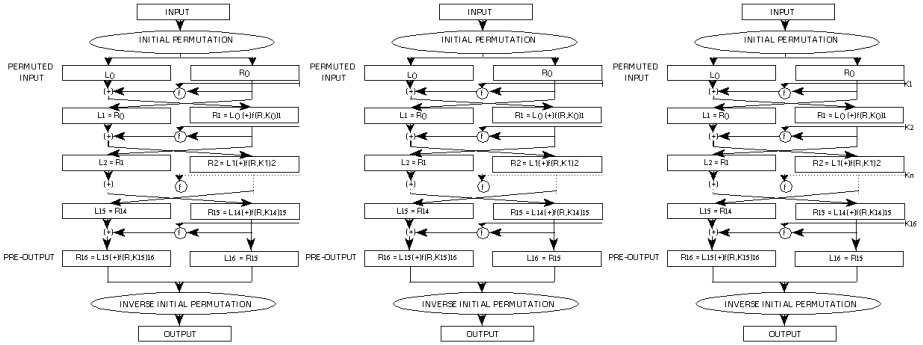
Data Encryption Standard (DES)

- Introduced in **1977** (≈ Lucifer from 1971)
- Key space = 2^{56}
- Cipher properties
  - Block cipher
    - Using blocks of 64 bit
  - Optimized for hardware
- Weak keys (00…0 and 11…1)
- Attacks
  - Linear cryptanalysis with 2^{43} known plaintexts



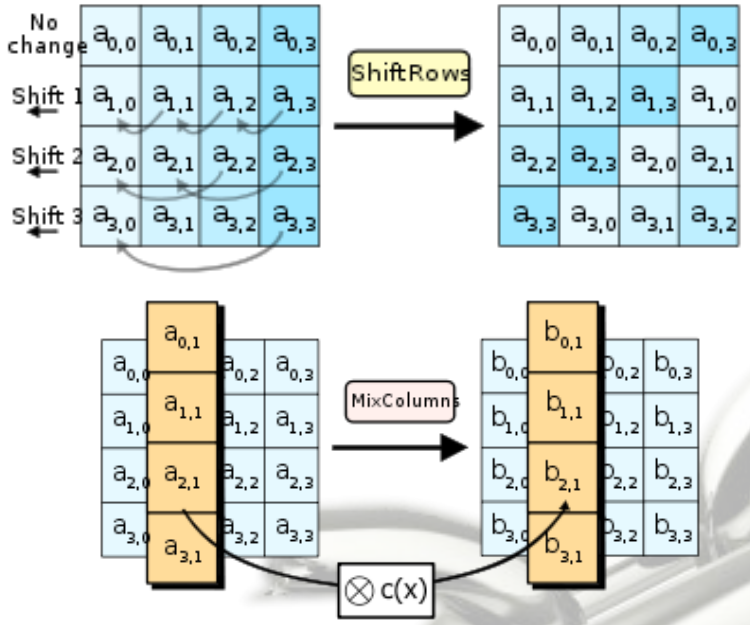
Triple DES (3DES or TDES)

- Specified in **1981**
- Key space = 2^{112}
- Cipher properties
  - Block cipher
    - Using blocks of 64 bit
  - Optimized for hardware
- Weak keys (00…0 and 11…1)
- Attacks
  - Best attack requires 2^{84} encryptions



Advanced Encryption Standard (AES)

- Introduced in **2001** (≈ Rijndael from 1998)
- Key space = $\mathbf{2^{128}}$ or $\mathbf{2^{192}}$ or $\mathbf{2^{256}}$
- Cipher properties
  - Block cipher
    - Using blocks of 128 bit
  - Optimized for both
    - Software
    - Hardware
- Attacks
  - Best attack requires 2^{126} encryptions



Proprietary Cryptography



Proprietary crypto systems

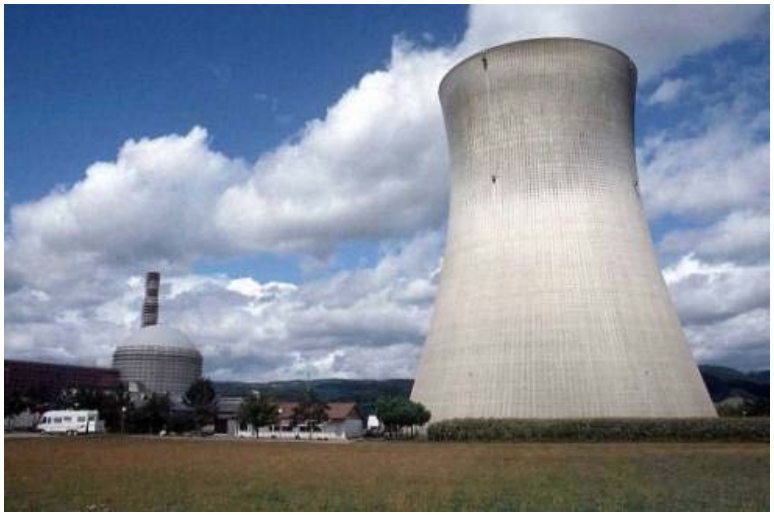
- **Access control**
  - Legic Prime
  - MIFARE Classic
  - Cryptomemory
  - iClass (Elite)
- **Wireless phones**
  - GSM A5-1/A5-2
  - DECT DSAA/DSC
  - Sat GMR-1/GMR-2
- **Vehicle immobilizer**
  - DST
  - KeeLoq
  - Hitag2
  - Megamos Crypto
- **Transmissions**
  - Bluetooth E0
  - WiFi WEP

Access Control Systems



LEGIC Prime Applications







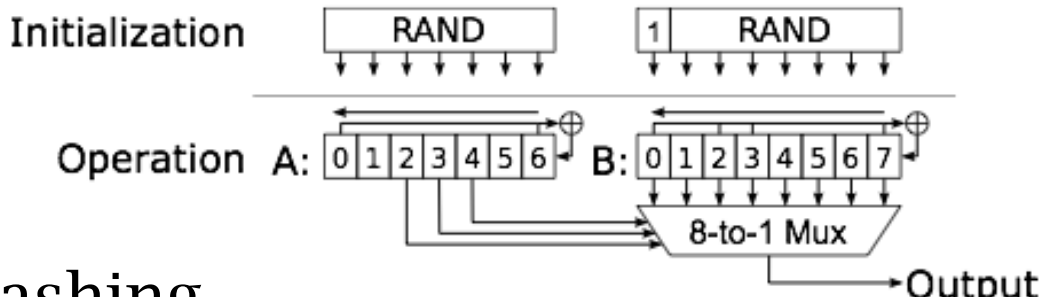






LEGIC Prime

- Introduced in 1992
  - Access control
- Key space = 2^0
- Weaknesses
  - No encryption / hashing
  - Relies only on obfuscation
- Attacks
  - Instant replay of recorded transaction
  - Abuse trust-delegation and create “über” token

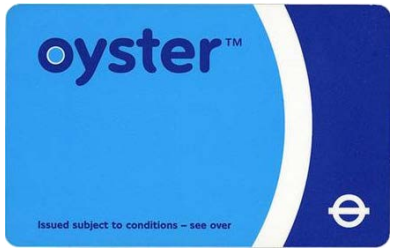


MIFARE Classic Applications





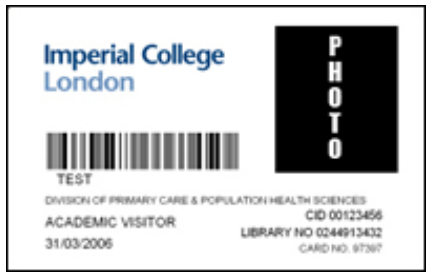








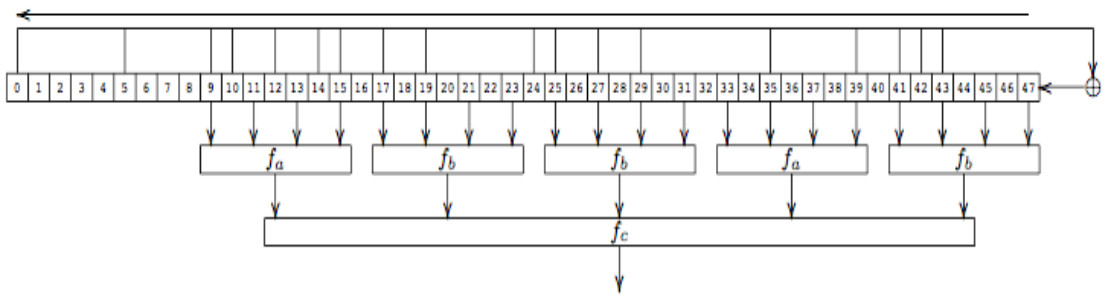






MIFARE Classic

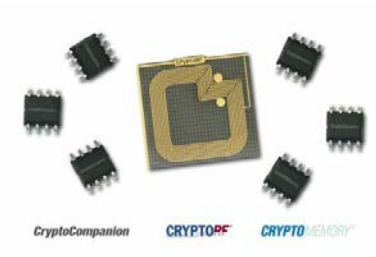
- Introduced in 1994
  - Public transpor
  - Access control
- Key space = 2^{48}
- Sold billion+ times
- Weaknesses
  - Weak random nonces
  - Only odd filter-inputs
  - Encrypts parity bits



- Attacks
  - Eavesdrop (1 trace)
  - Reader-only (2 traces)
  - Card-only (300 traces)

CryptoMemory Applications

- ID and access cards
- healthcare
- loyalty cards
- e-purses
- energy meters
- e-government
- printers and print cartridges
- Digital-TV
- subassembly authentication
- counterfeit protection
- Vegas!







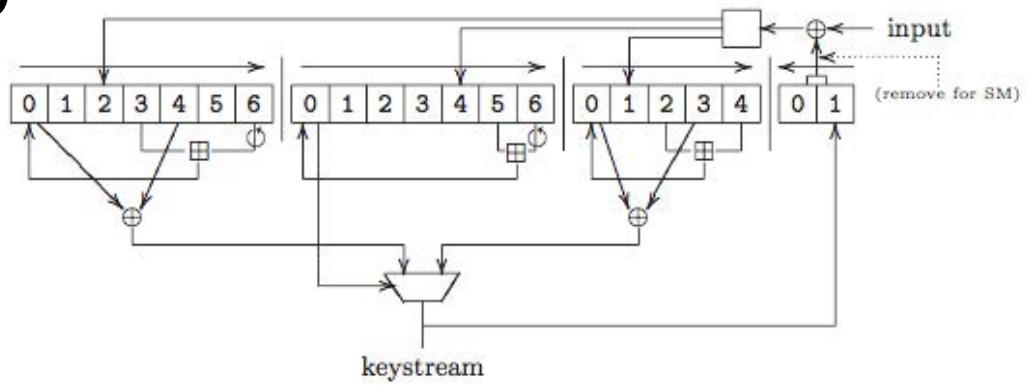






SecureMemory & CryptoMemory

- Introduced in 1999
  - Casino and e-cash
  - Anti-counterfeit
  - Access control
- Key space = 2^{64}
- Weaknesses
  - No tag nonce
  - Register correlation
  - Rollback of cipherstate



- Attacks
  - SecureMem (1 trace / month)
  - CryptoMem (24 traces / days)
  - DPA attack (card-only seconds)

iClass Applications













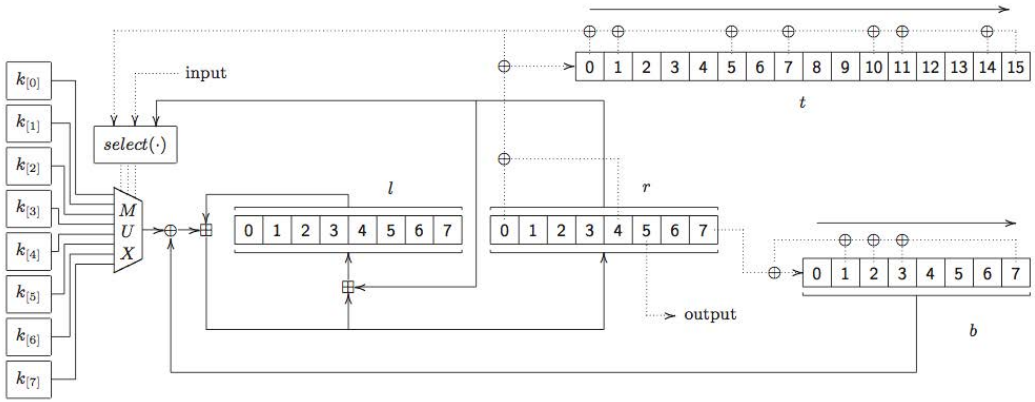






iClass

- Introduced in 2002
  - Smart login
  - E-cash
  - Access control
- Key space = 2^{64}
- Weaknesses
  - No tag nonce
  - Privilege escalation
  - Weak diversification
  - Number of weak keys



- Attacks
  - Standard (1 trace and 2^{22} card queries, few hours)
  - Elite (reader-only, seconds)

Vehicle Immobilizers



DST Applications

Speedpass



Ford

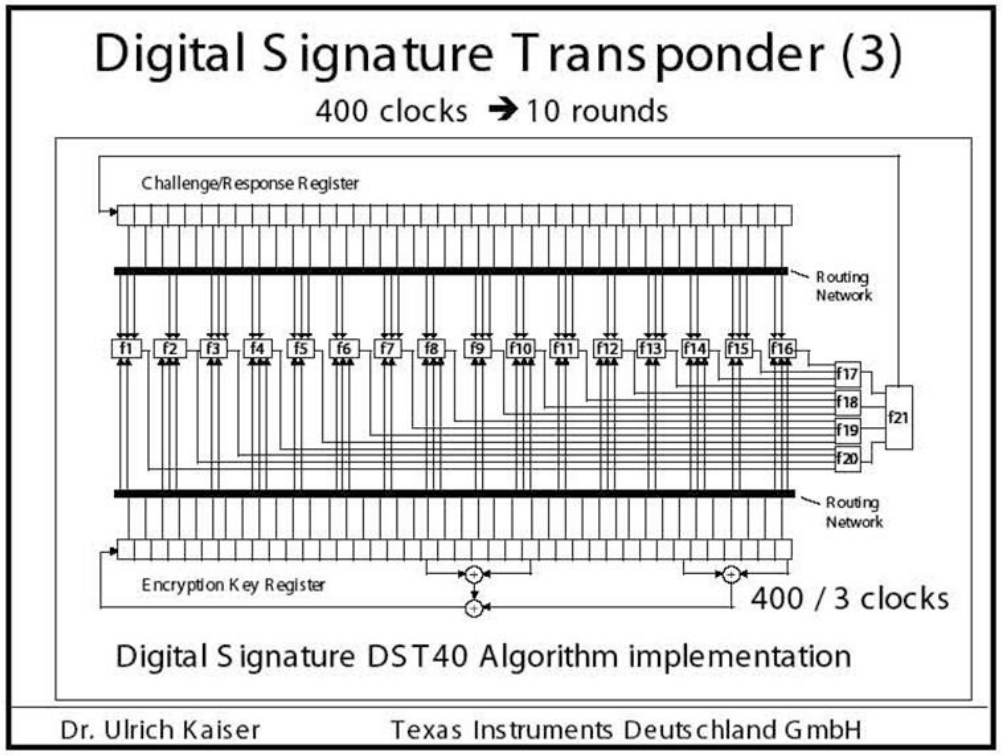
SUZUKI

mazda



Digital Signature Transponder (DST)

- Introduced in 1995
  - Immobilizers
- Key space = 2^{40}
- Weaknesses
  - No tag nonce
  - Low complexity
  - Unbalanced cipher
- Attacks:
  - Brute-force



KeeLoq Applications





CHRYSLER

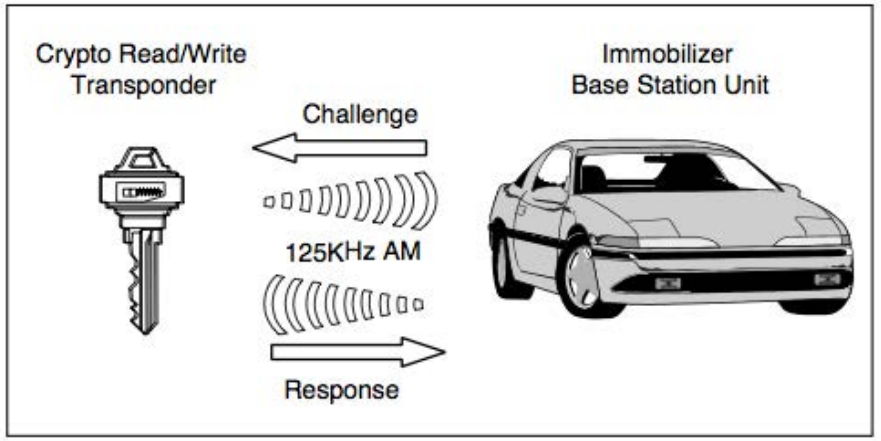
JAGUAR

FIAT

SEAT

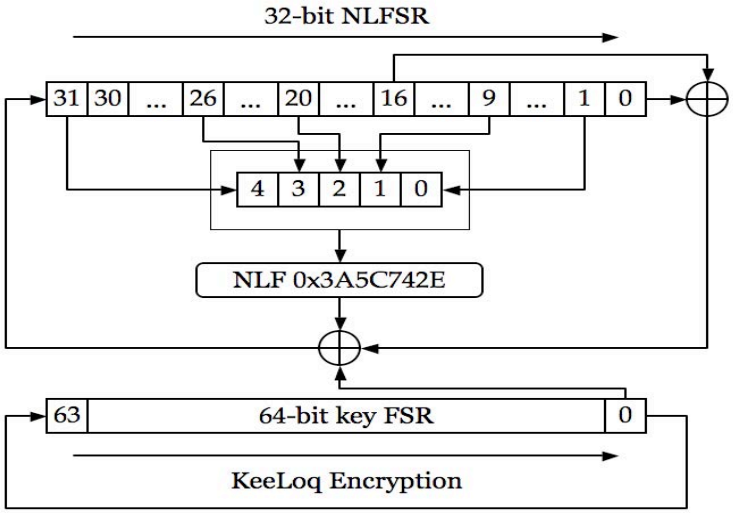
VOLVO

DAEWOO



KeeLoq Encryption

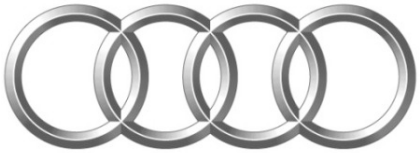
- Introduced in 1996
  - Remote keyless entry
- Key space = 2^{64}
- 11+ makes, 30+ models
- Weaknesses
  - Jamming of code hopping
  - Small internal state
  - Linear relation over cipher bits
  - Missing hardware protection



- Attacks
  - Side-channel (DPA)
  - Eavesdrop (2 traces)

Megamos Crypto Applications































Megamos Crypto

- Introduced in 1995/1996
  - Immobilizers
- Key space = 2^{96}
- 26+ makes, 135+ models
- Weaknesses
  - …
  - …
  - …



- Attacks
  - …
  - …

Hitag2 Applications







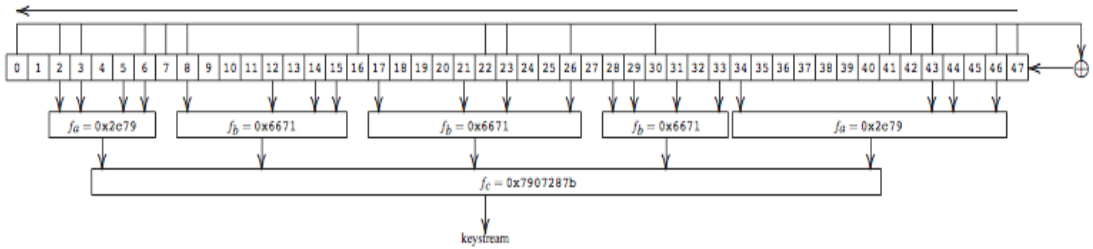






Hitag2 Cipher

- Introduced in 1996
  - Immobilizers
  - Access control
- Key space = 2^{48}
- 34+ makes, 200+ models
- Weaknesses
  - No tag nonce
  - Weak filter function
  - Session dependencies
  - Key stream oracle



- Attacks
  - Eavesdrop (134 traces)
  - 5 minutes computation

Wireless Telecommunication



DECT Applications



DECT

DIGITAL DECT



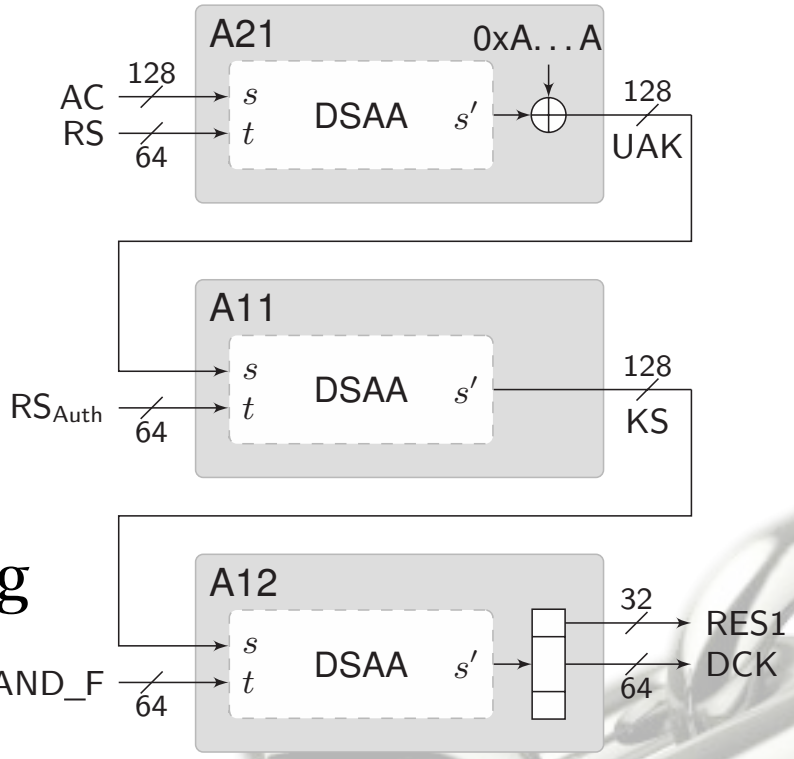






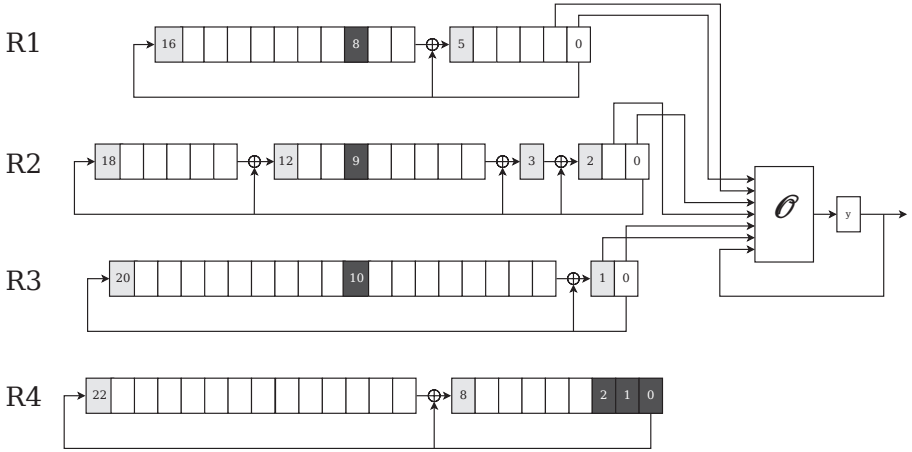
DECT Standard Authentication Algorithm (DSAA)

- Introduced in 1992
  - Most cordless phones
  - Various remote sensors
- Key space = 2^{128}
- Weaknesses
  - Weak PRNG
  - Low influence of key bits
  - Not optimal key scheduling
- Attacks
  - Differential attack
  - Only seconds because of very weak PRNG



DECT Standard Cipher (DSC)

- Introduced in 1992
  - Cordless phones
  - Remote sensors
- Key space = 2^{64}
- Weaknesses
  - Initialization rounds
  - Clocking mechanism
- Attacks
  - Practical attack on eavesdropped traces
  - Takes only a few hours on a regular pc



GSM Applications

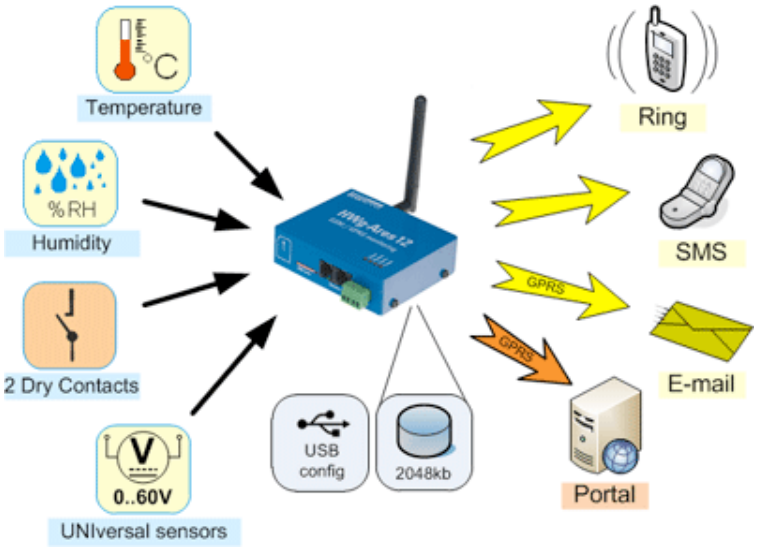












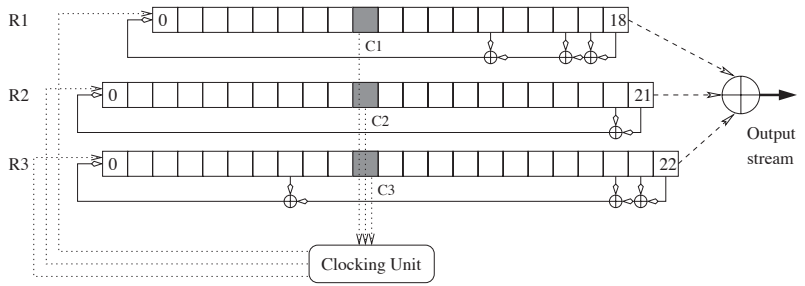
GSM



SMS
Banking

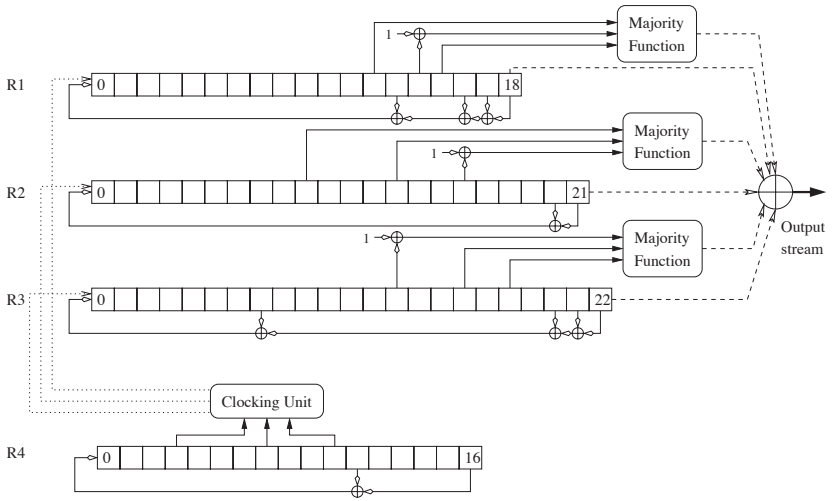
GSM A5/1

- Introduced in 1987
  - 5+ billion subscribers
  - Export-restricted
- Key space = 2^{64}
- Weaknesses
  - Redundant bits reveal linear relation
  - Small number of LFSR feedback taps
  - Linear output filter function
- Attacks
  - Algebraic guess and determine attack
  - Linear relation enables cipher-text only attack



GSM A5/2

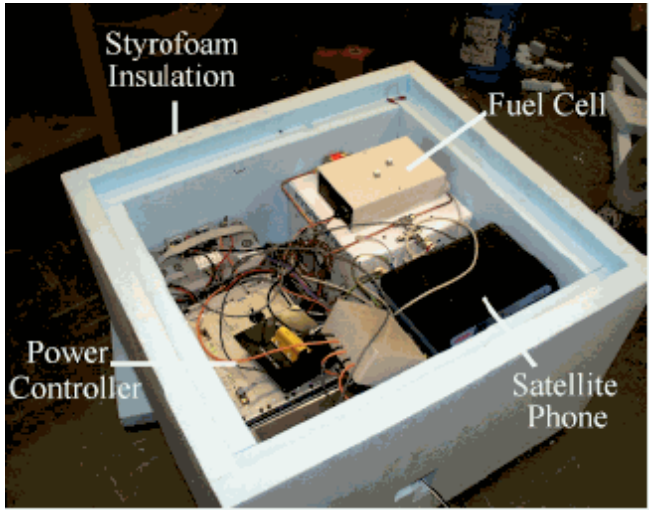
- Introduced in 1989
  - Cordless phones
  - Remote sensors
- Key space = 2^{64}
- Weaknesses
  - Similar to A5/1
  - Separate clocking LFSR
- Attacks
  - Instant key recovery with only a few passively eavesdropped consecutive cipher-text frames



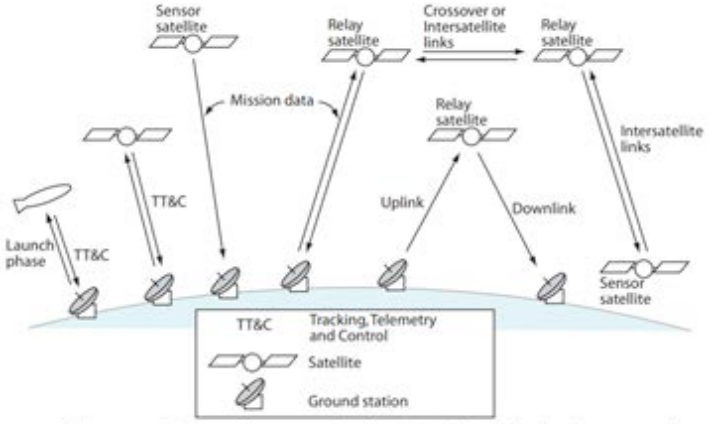
Sat-Phones (GMR) Applications







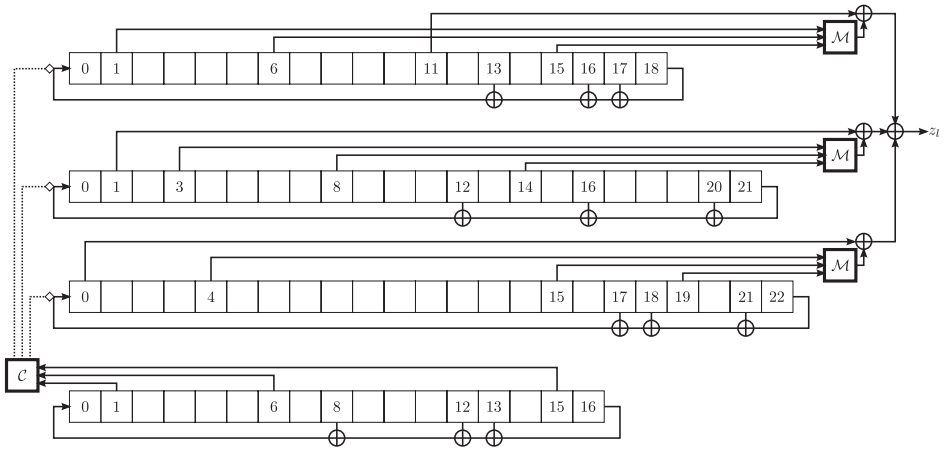




The communications architecture consists of satellites and ground stations interconnected with communications links. (Adapted from SMAD.)

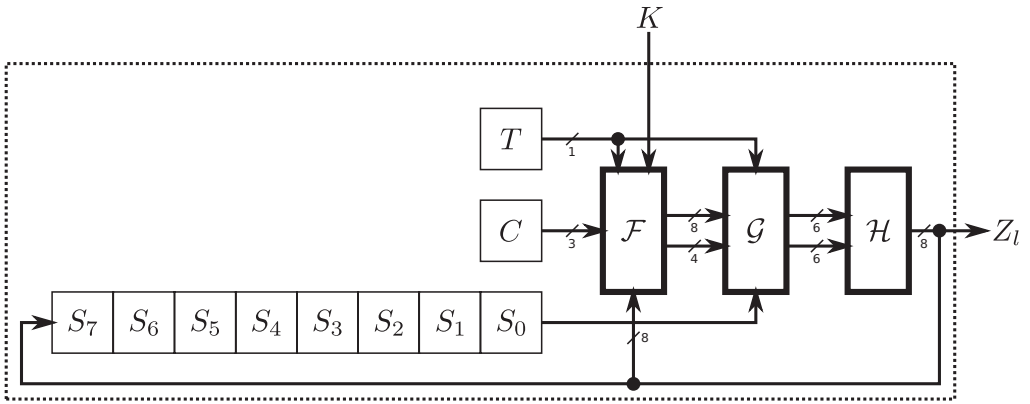
GMR-1 Cipher

- Introduced in 2001
  - De-facto standard
  - Sensitive domains
- Key space = 2^{64}
- Weaknesses
  - Entropy of non-linear clocking is too small
  - Encryption of redundant bits and parity check
- Attacks
  - Attack complexity = 2^{32} with known plaintext
  - Allows cipher-text only attack



GMR-2 Cipher

- Introduced in 2001
  - Network is more similar to GSM
- Key space = 2^{64}
- Weaknesses
  - Key-bytes scheduling
  - Many relations in the internal state
- Attacks
  - Attack complexity negligible
  - With at most 65 bytes of contiguous keystream



Transmission Cryptography



Bluetooth Applications





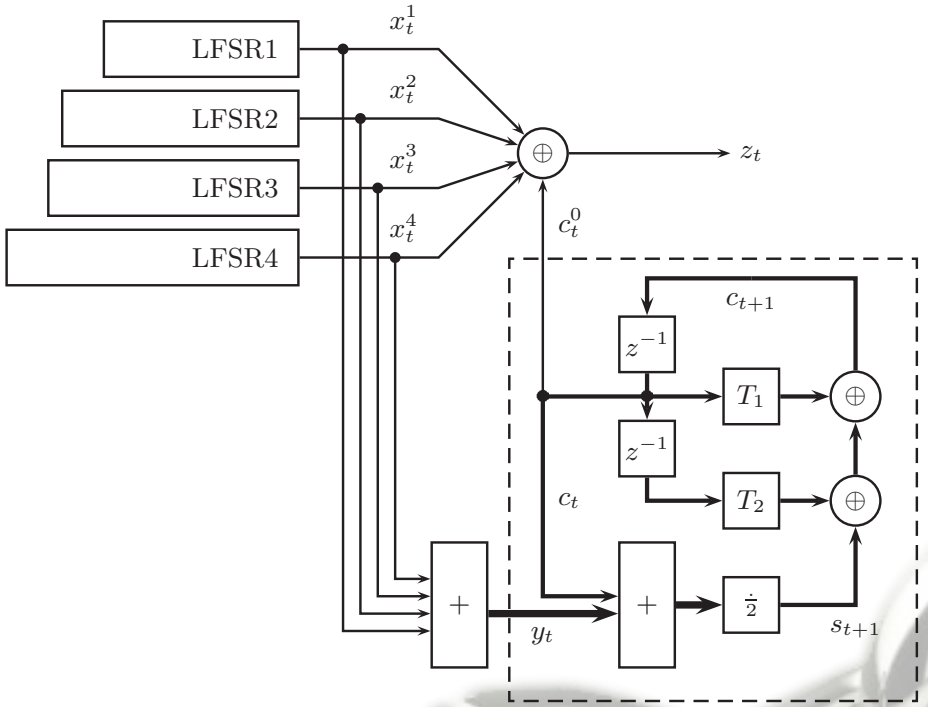






Bluetooth E0 Cipher

- Introduced in 1994
  - Various connections
  - Privacy sensitive
- Key space = 2^{128}
- Weaknesses
  - No tag nonce
  - Weak filter function
- Attacks
  - Eavesdrop (first 2^{23} frames)
  - Only seconds of computation



WiFi Applications







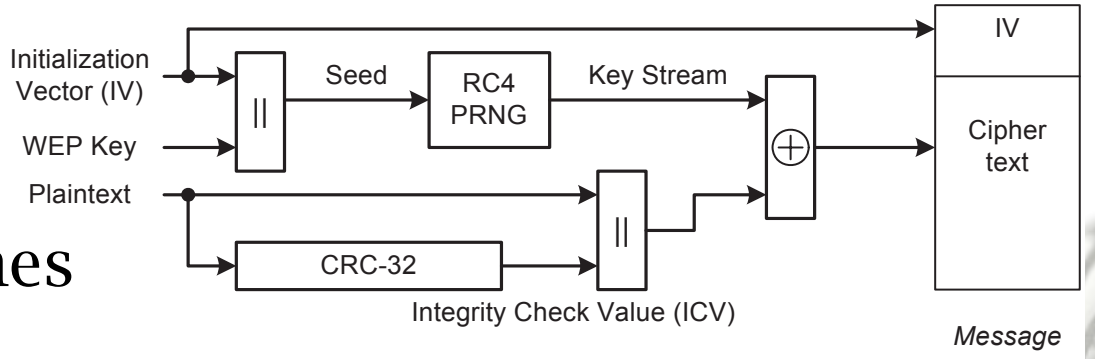






WiFi WEP Encryption

- Introduced in 1999
  - The default WiFi standard for many years
  - Most consumer product still support it
- Key space = 2^{40} or 2^{104}
- Weaknesses
  - Loading the IV
  - Predictable frames
- Attacks
  - Active attack, injection in only few seconds
  - Passive one, with less than 28000 frames



Proprietary **VS** Standardized crypto

- Proprietary crypto systems rely on **secret algorithms**
- Secrets algorithms enable **vendor lock-in** situation
- When secret leaks out, all products are **vulnerable**
  - The more it is sold/used, the more likely victim
- *"Security by obscurity"* – obscurity = **no security**
- Most reversed-engineered proprietary algorithms are **badly broken** and allow **practical attacks**
- **Peer-review** seems to be **inevitable**, why not start with this anyway.
- Migrate to **publicly scrutinized** schemes such as **DES, 3DES, AES** and **SHA-3**