AFRICACRYPT 2010
STIAS
Stellenbosch
South Africa

SOME UNUSUAL CIPHERS: PROTEX AND KEELOQ

G J Kühn

Ciphertec cc

gjkuhn@global.co.za

Ciphertec

Contents

- Protex: First electronic crypto device in designed in South Africa
- Keeloq: A simple but effective secure remote entry device

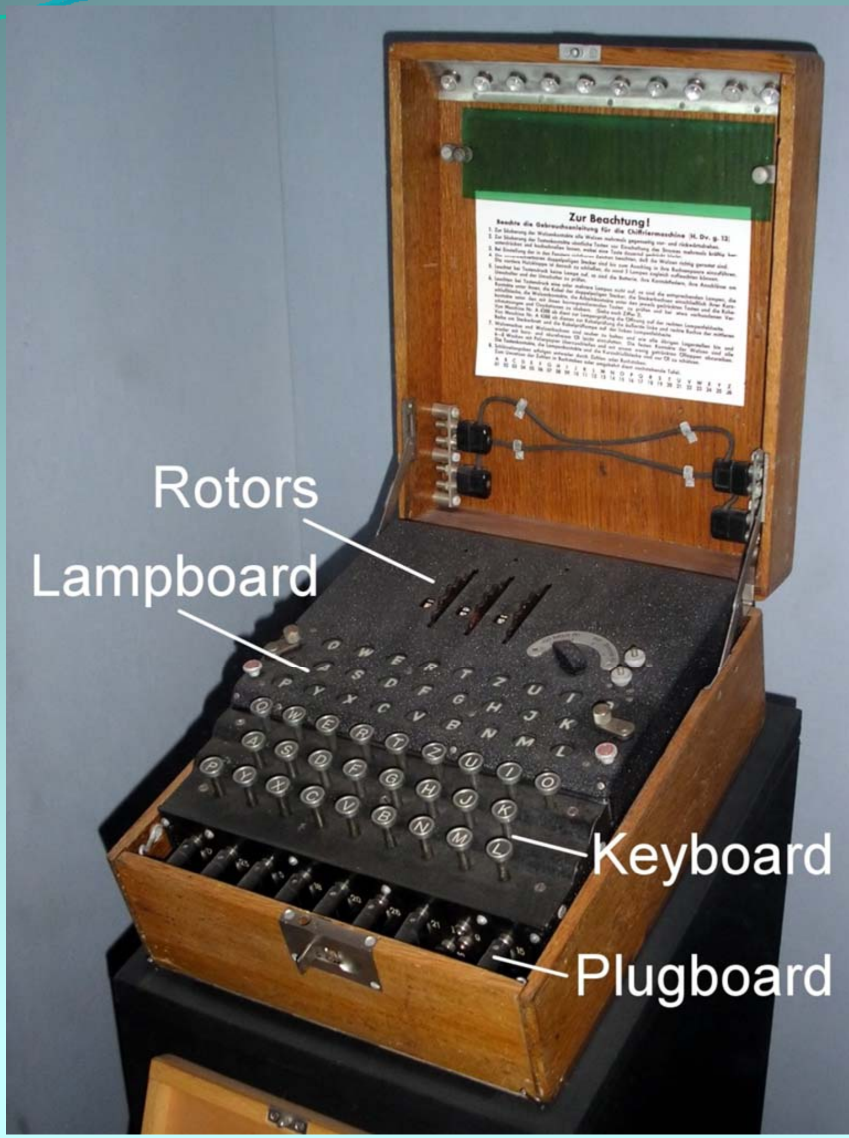
PROTEX CIPHER

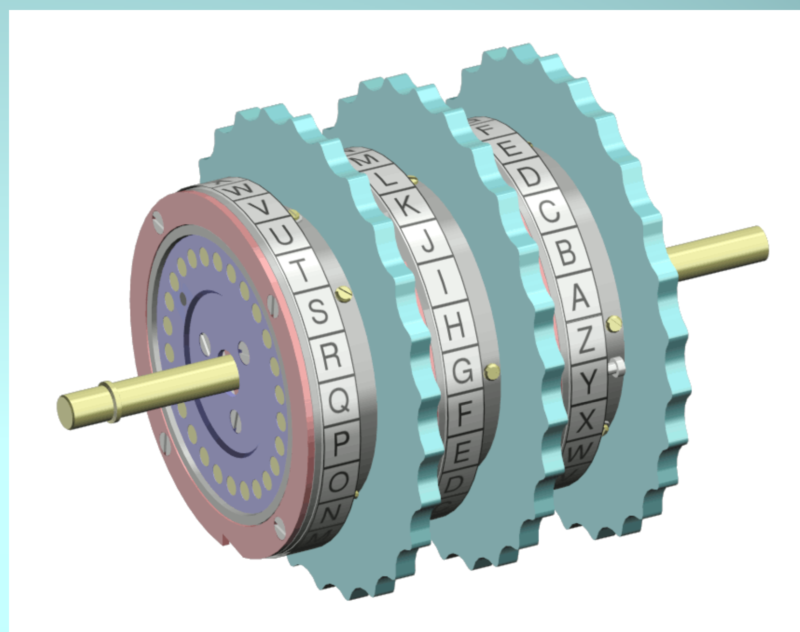
A rotor-inspired electronic cipher device

Rotor Cryptographic Machines

- The Protex cipher was based on rotor machine prototypes, such as
  - Enigma
  - Tsec-KL/7
  - Typex

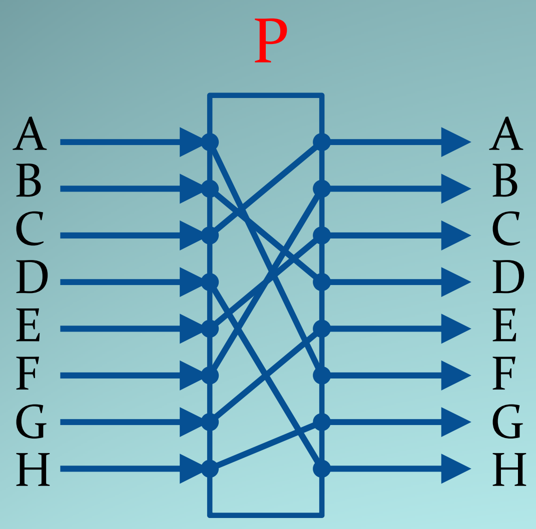
The Enigma machine was used commercially from the early 1920's, and was adopted by the militaries and governments of various countries.



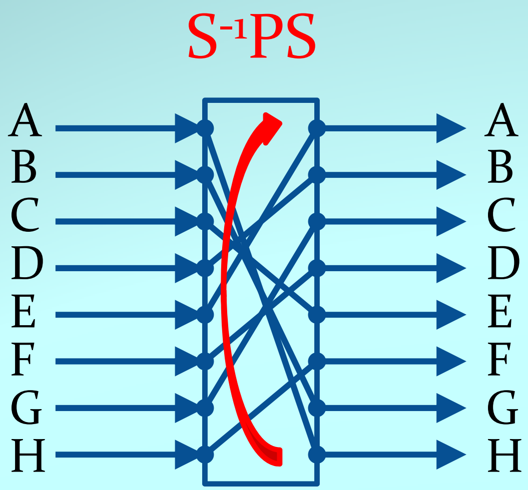


[Wikipedia]

Rotor Disk

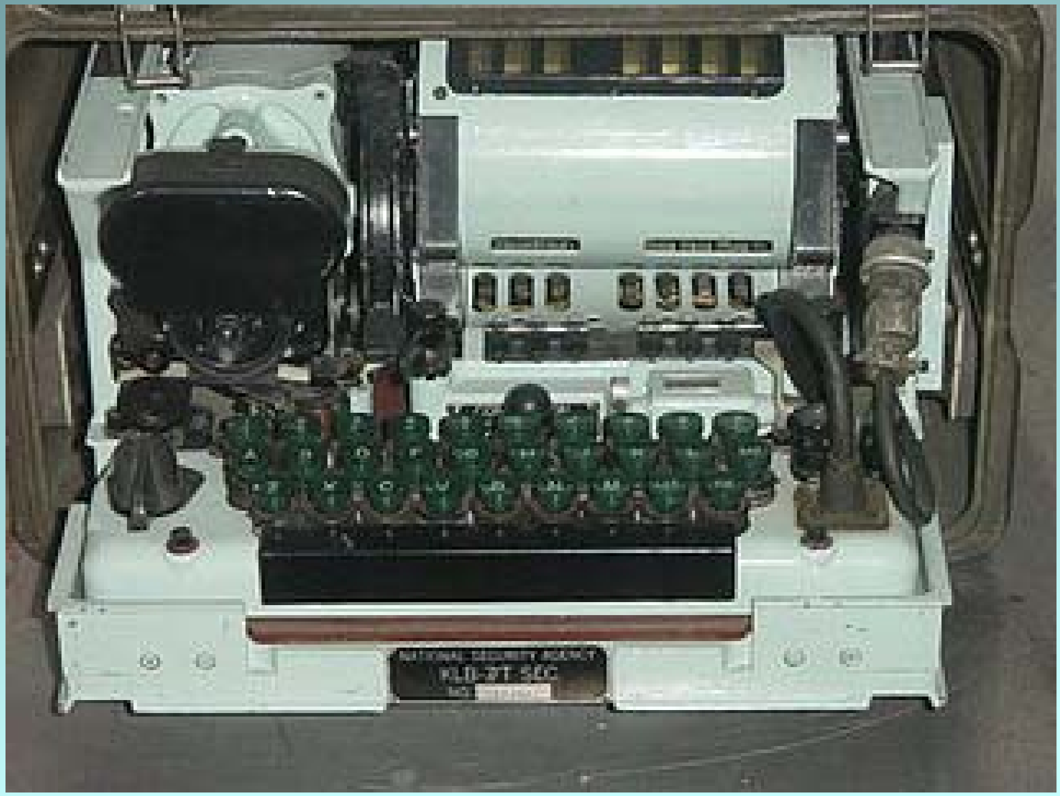


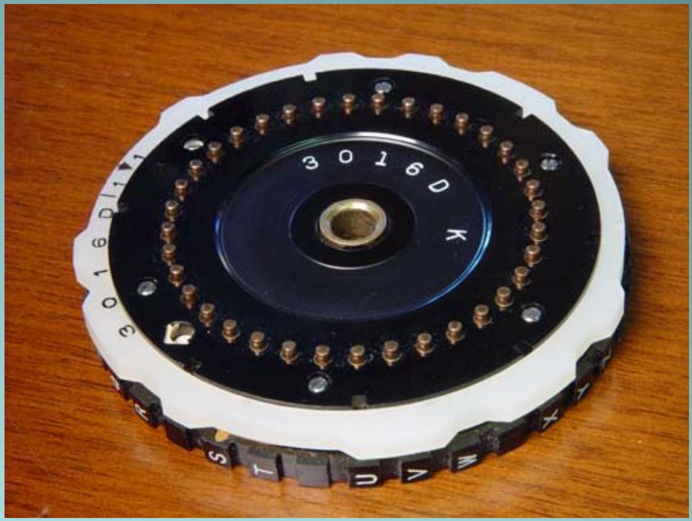
P = Permutation embedded in rotor



S = Single step cyclic permutation

TSEC/KL-7 adopted by the US National Security Agency





[Wikipedia]

Typex

- British cipher machine in use from 1937
- Based on the Enigma

[Wikipedia]

Concatenation of *r* Rotors

$$P = S^{-i_1} P_1 S^{i_1} \cdot S^{-i_2} P_2 S^{i_2} \cdots\cdots S^{-i_r} P_r S^{i_r}$$

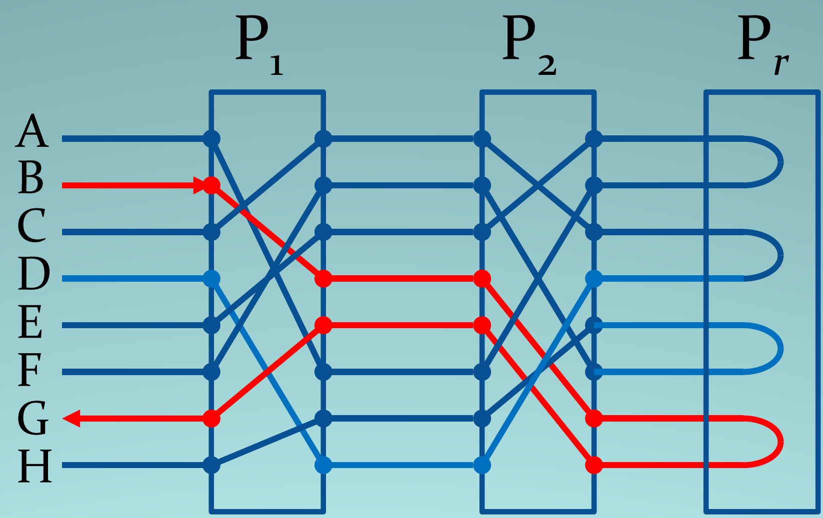
where

$P_1, P_2, \ldots, P_r$ are the rotor permutations

S is a 1-step rotation operation

$\sigma = (i_1, i_2, \ldots, i_r)$ is the state of the machine

Reflection Disk



Self-inverse permutation

$$Q = S^{-i_1} P_1 S^{i_1} \cdot S^{-i_2} P_2 S^{i_2} \cdot P_r \cdot S^{i_2} P_2^{-1} S^{-i_2} \cdot S^{i_1} P_1^{-1} S^{-i_1}$$

$$= X^{-1} P_r X$$

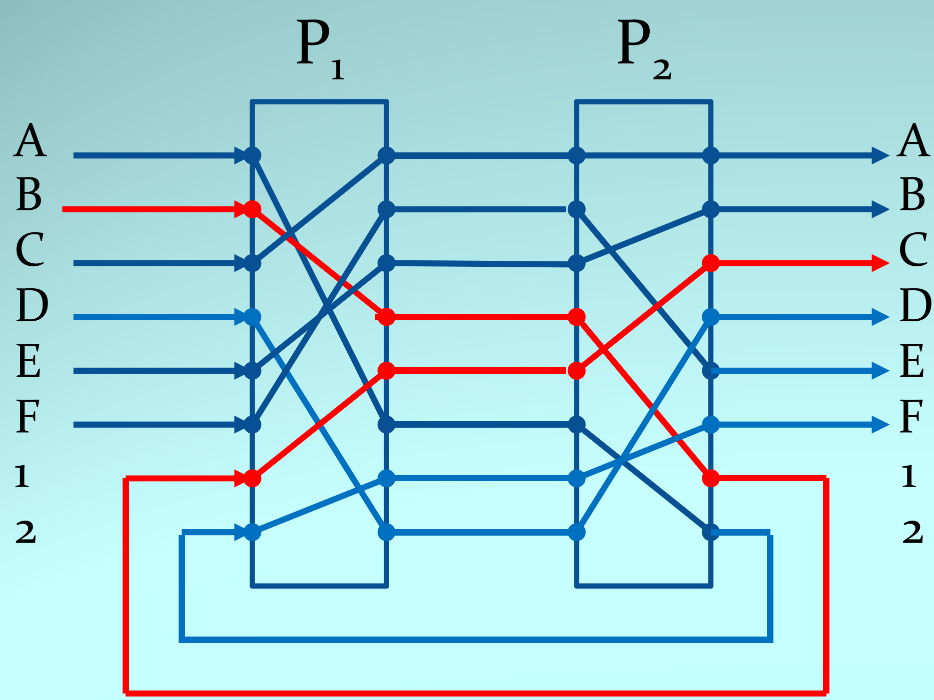
Q and P_r are conjugate permutations with the same *cycle structure*

Rotor Cycle Structure Properties

- Advantage:
  - Encryption/ decryption operations are identical
- Weakness:
  - A given letter is never encrypted into itself
    - This is due to the turn-around permutation being self-inverse with no fixed points – all cycles are of order 2
    - This represents a Shannon redundancy of 0.057 bits/letter

Re-entry

- The technique matches the alphabet size to the number of contacts on the rotor



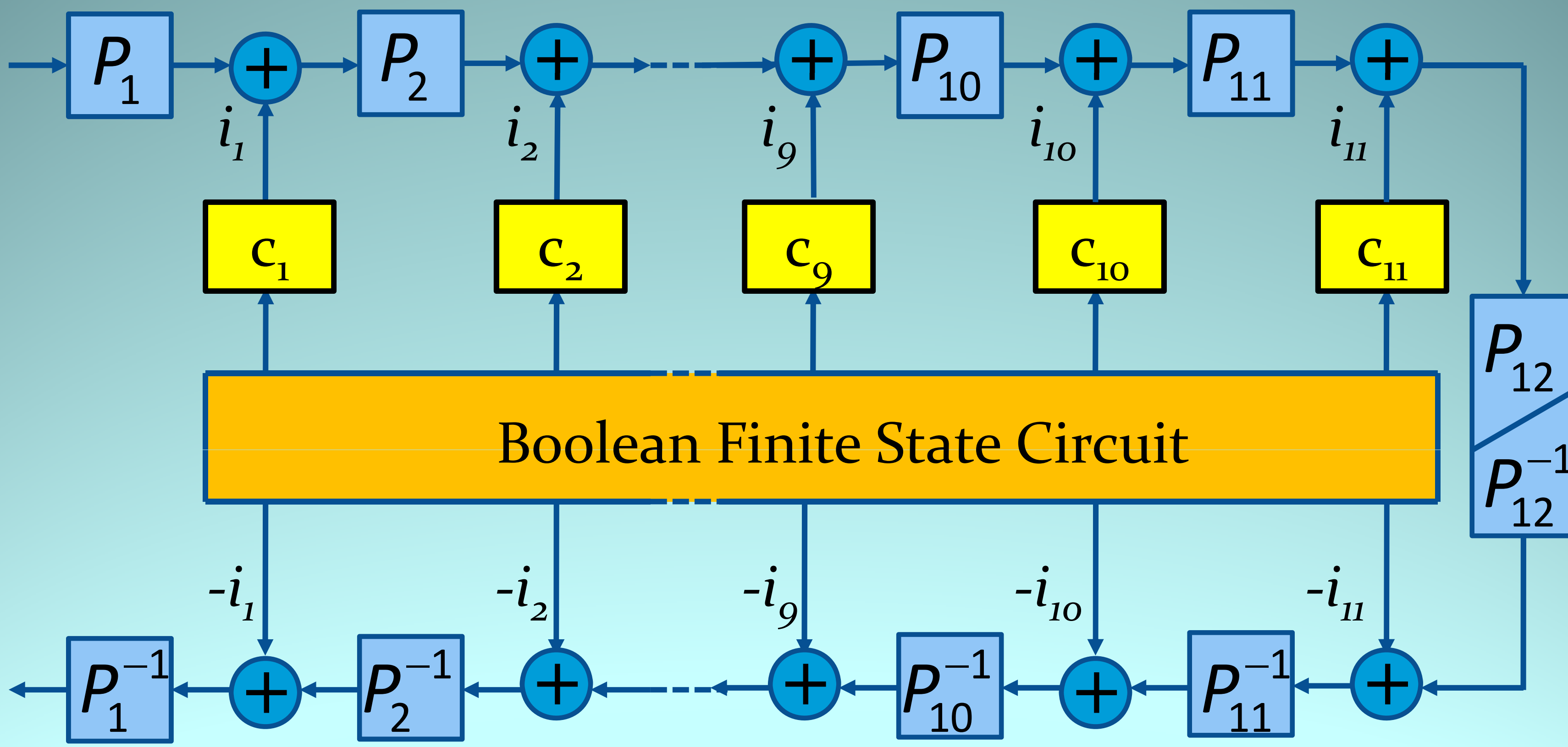
KL-7:	26 : 36 : 26
Protex:	26 : 32 : 26

B→D→1→E→C

Protex Design

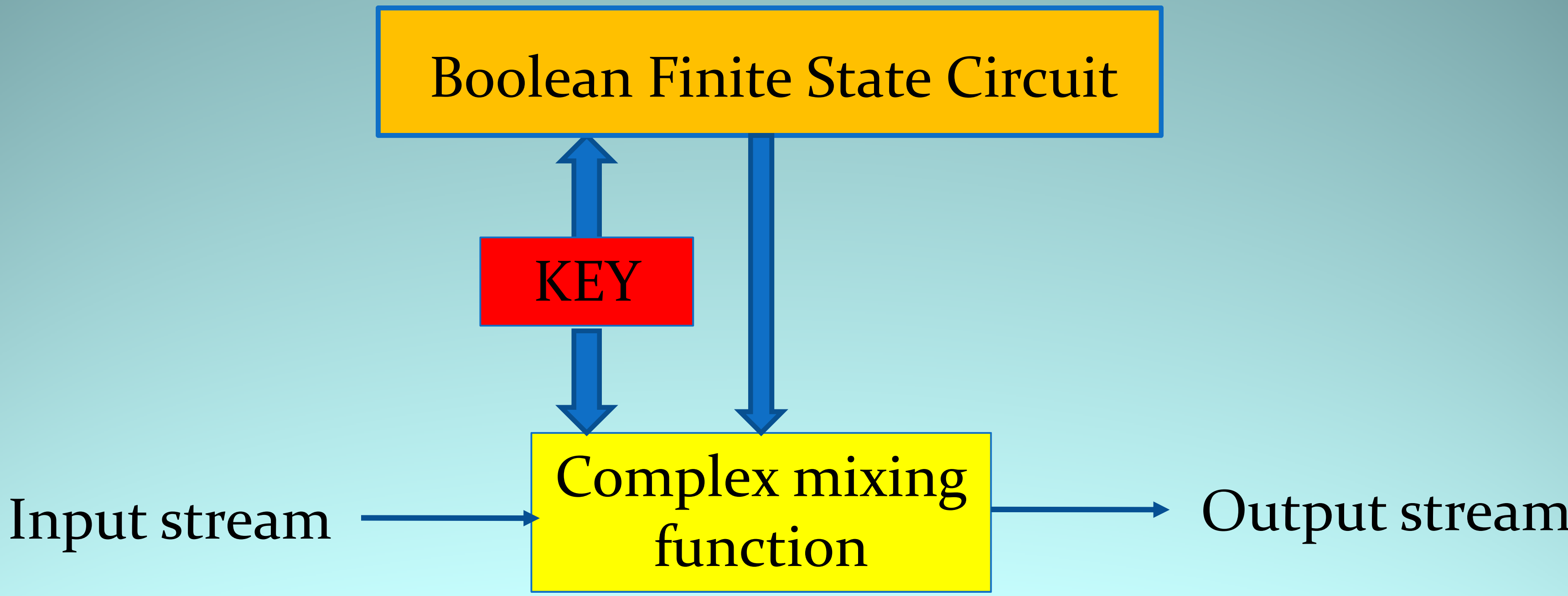
- 5-bit alphabet
- 12 random permutations on 32 characters
  - One permutation is used as a reflector
  - The permutations are chosen such that $P \bullet S \neq S \bullet P$ *(Shannon product cipher condition)*

Protex Encryption/Decryption



Decryption uses P_{12}^{-1} as turn-around permutation

Rotor Machine Categorisation



Stream cipher with a dynamic key-dependent mixing function

Key Size

- BFSC initial state : 11x5 = 55 bits
- Counters initial states : 11x5 = 55 bits
- Ordering of 12 permutations: 12! ≡ 28.8 bits

- Total key size : 138.8 bits

Re-Entry

- Re-entry on six 5-bit teleprinter control characters

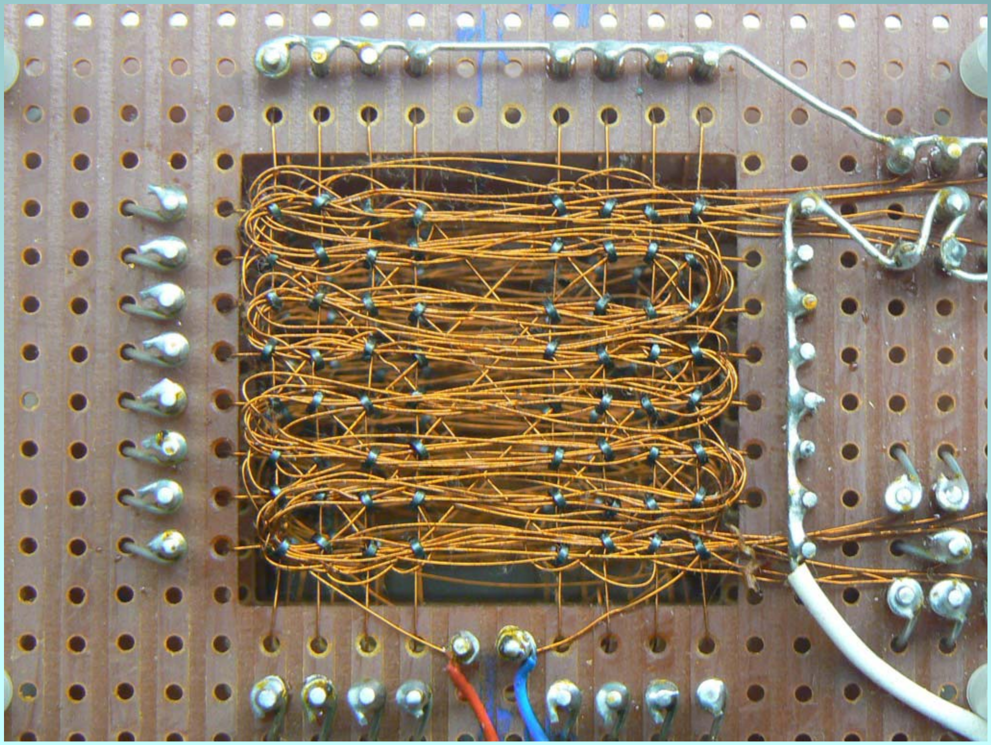
No. of re-entries	Probability
0	0.812500
1	0.157258
2	0.026210
3	0.003615
4	0.000387
5	0.000029
6	0.000001

Average = 0.22

Implementation

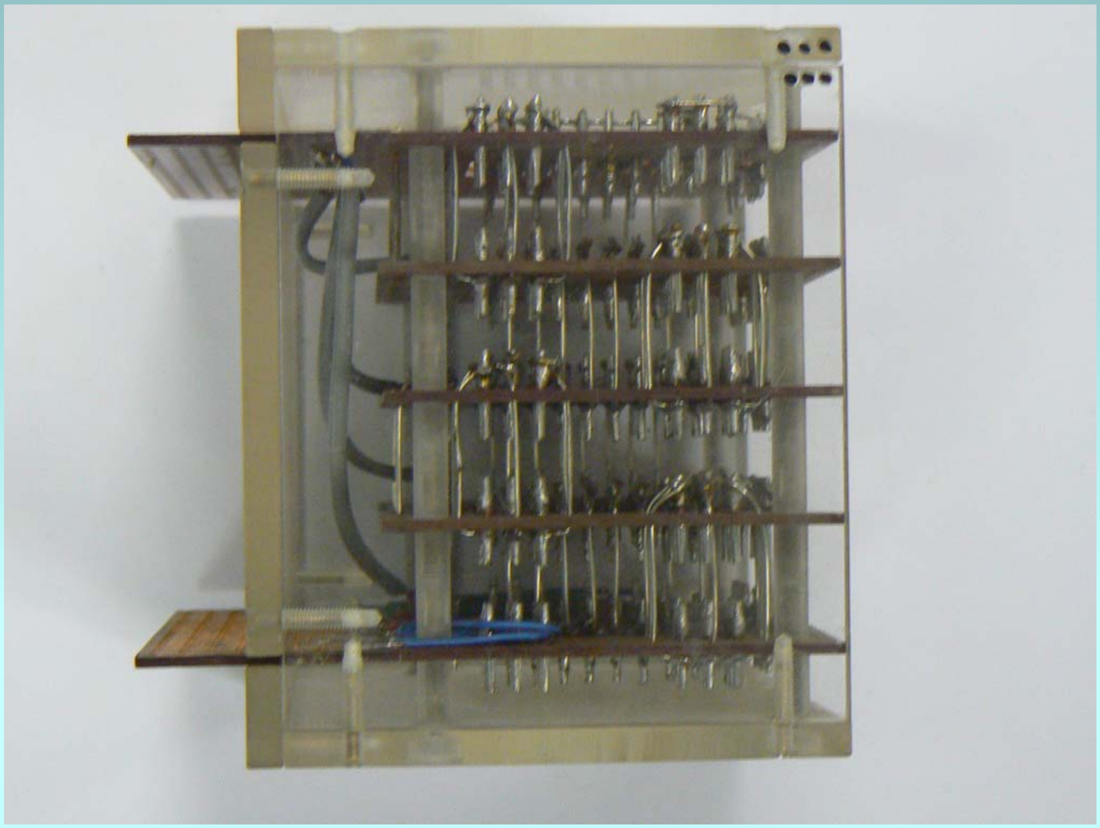
Ferrite core memory storing 12 permutations and their inverses

Permutations were optimised to reduce the number of conductors threaded through aeach ferrite core



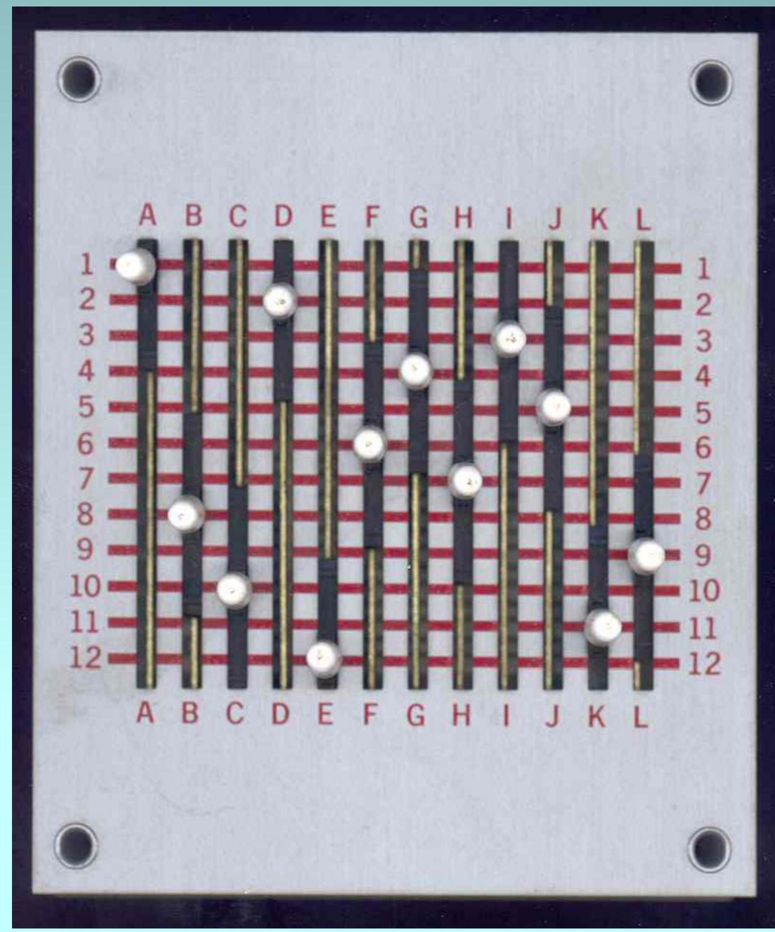
S-Box

Laboratory model S-Box showing 5 planes corresponding to the 5-bit words



Patch Panel

Patch panel to select a rearrangement of the 12! permutations



Attacks on Protex

- Cryptanalysis depends critically on the properties of the BFSC
  - Advance of the counters are irregular
- Side-channel attacks:
  - Timing attacks
    - Re-entry
    - Propagation of carry bit
  - Power analysis
    - Power surges due to switching of magnetic ferrite cores

Benefit of Hindsight

- The reflector structure of rotor machines offers no cryptographic advantage
  - Input-output permutations conjugate to a fixed permutation decreases entropy
- Re-entry is a serious weakness, making the cipher vulnerable to a timing attack

KEELOQ CIPHER

The travails of a 32-bit block cipher

KEELOQ

- Designed at Nanoteq in the 1980's
- Purpose: To provide increased security for remote keyless entry systems
  - Applications: car door, garage door openers, etc.
- Constraints
  - 32-bit radio transmission
  - low power
  - low component count

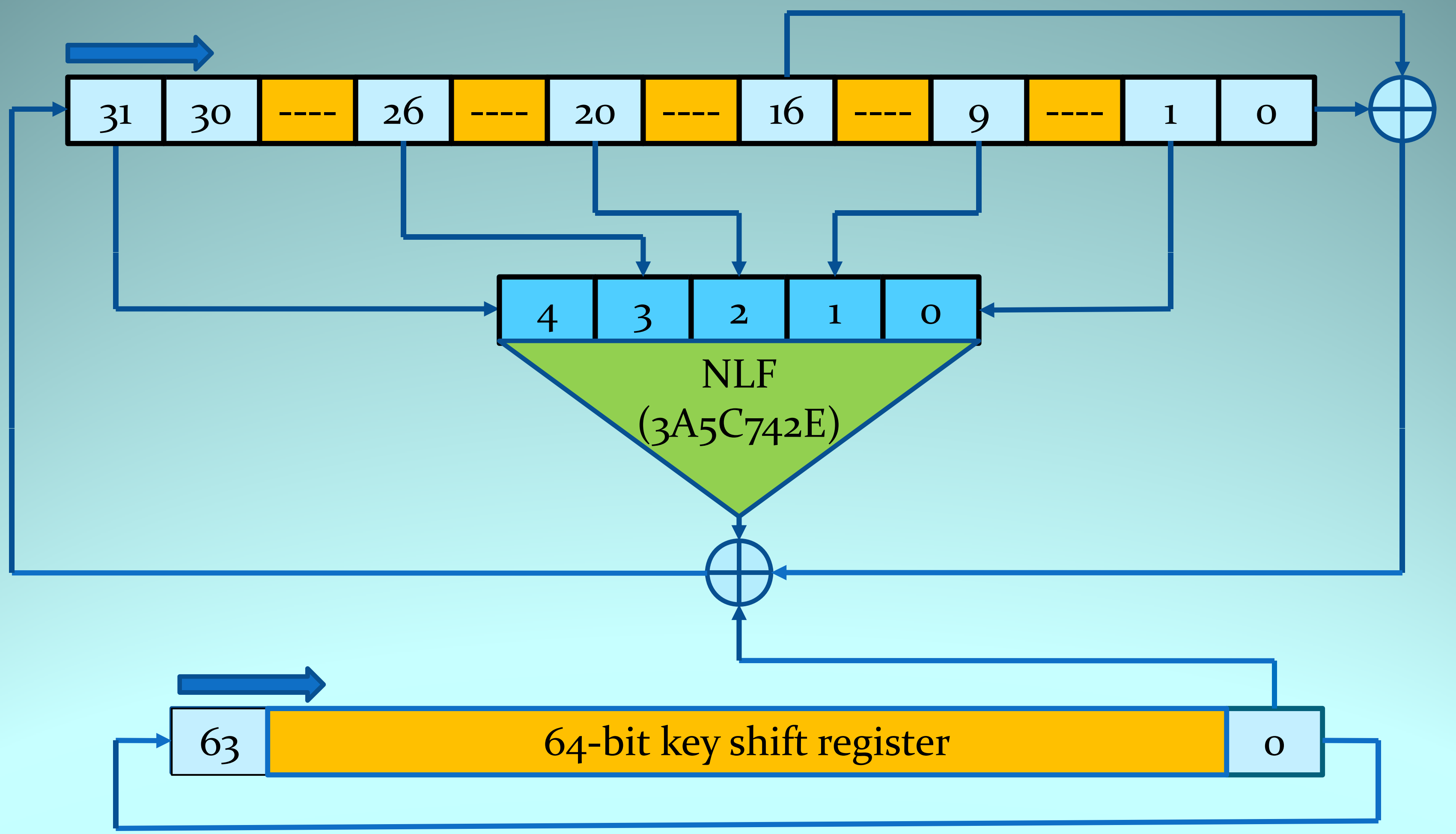
Protocol

- A block cipher to encrypt the state of a counter
- Key length: Initially 32 bits, but later increased to 64 bits
- Block length limited to 32 bits due to transmitter constraints

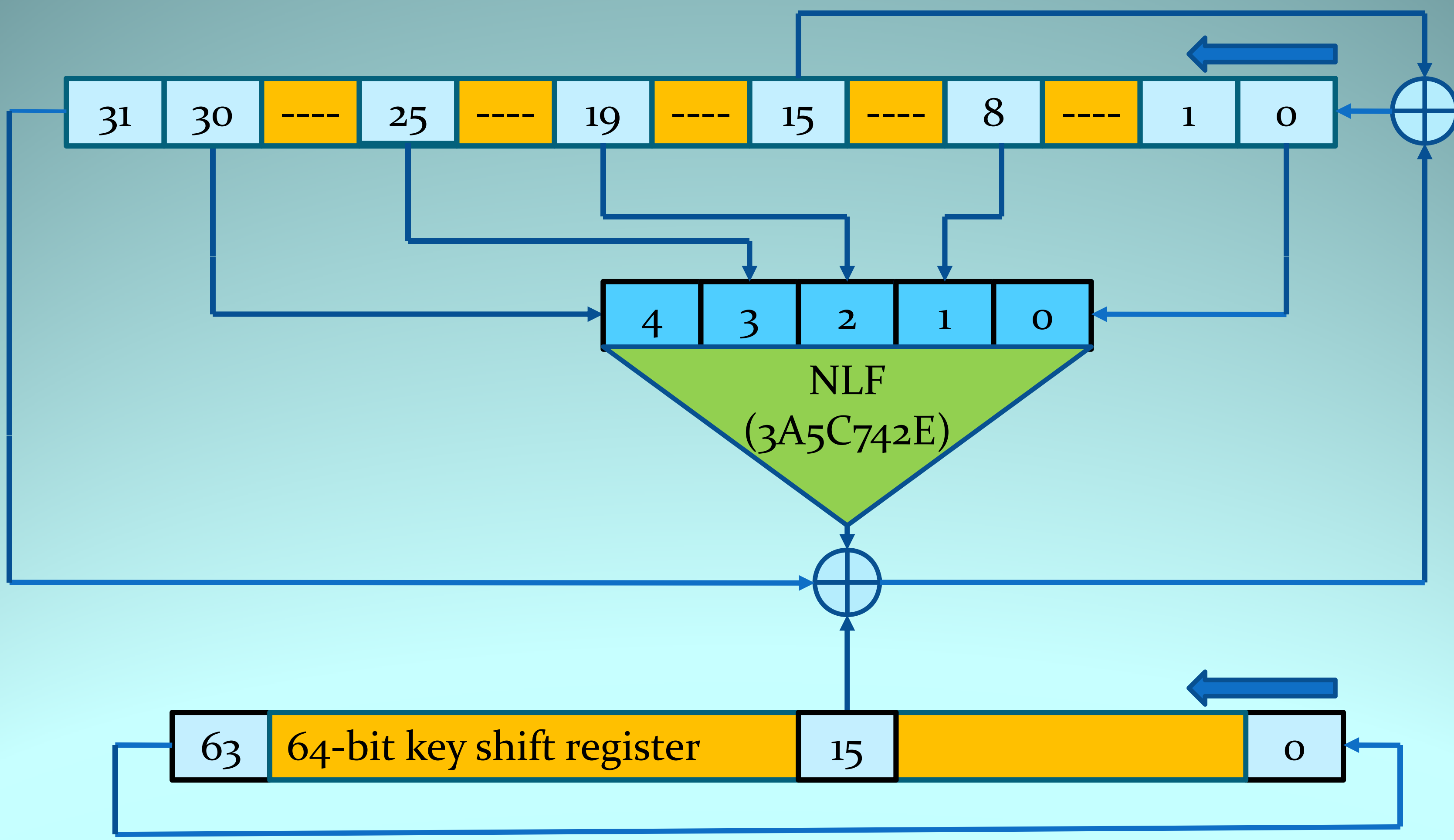
Design

- No *nxn* S-boxes, as these would be too expensive in component count
- Eventually it was decided to insert a single 5x1 S-box
- An elementary key schedule to save components
  - Circulating shift register

Keeloq Encryption



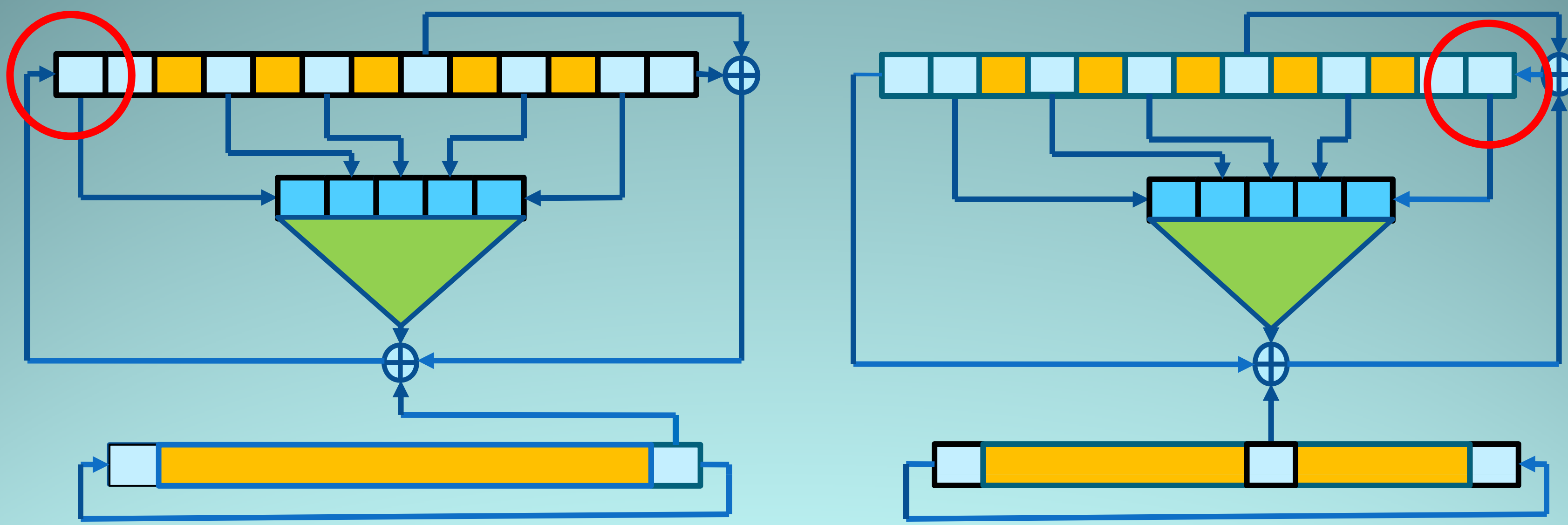
Keeloq Decryption



Number of Steps (Rounds)

- Number of shift register steps: 528
- This was decided on as follows
  - Good SAC properties from plaintext to ciphertext
  - Each key bit should be active at least 8 times
- The 528 steps comprises 8¼ cycles of the key register
- The ¼ cycle was introduced as a "nuisance" impediment to cryptanalysis

Tap Points on the Shift Register



- Latency: 1 clock period
  - Minimised to enhance diffusion of bit changes in encryption/decryption

The Non-Linear Function (NLF)

- Properties
  - 5-bit Boolean function
  - 0-1 balanced
  - Algebraic degree : 3
  - Minimum distance to affine set : 8
  - Correlation immunity : 1
  - Function resiliency : 1

Attacks on Keeloq

Attack	Data	Time	Mem	Reference
Exhaustive search	2 KP	2^{63}	Small	
Time-memory trade-off	2 CP	$2^{42.7}$	100 TB	Hellman
Slide/algebraic	2^{16} KP	$2^{51.4}$	?	[Co, Ba, Wa]
Slide/guess and determine	2^{32} KP	2^{37}	16 GB	Bogdanov
Slide/cycle structure	2^{32} KP	$2^{39.4}$	16.5 GB	[Co, Ba]
Slide/fixed points	2^{32} KP	2^{27}	>16 GB	[Co, Ba, Wa]
Slide/meet-in-the-middle	2^{16} KP	2^{45}	≈2 MB	[In, Ke, …]

Exhaustive Search

Exhaustive Search

- Computational Complexity = 2^{63}
- Time: 2 weeks using FPGA circuits

Most significant half (MSH)	Criterion	Number of ciphertexts
MAC = *f*(counter)	MSH* Satisfies MAC	2
Fixed ID (known)	MSH Equals ID	2
Fixed ID (unknown)	MSH differential	3
Random bits	16-bit counter mode	≤64

* MSH = most significant half of counter

Deduced Plaintext for Exhaustive Search Attack

- Guess the state of the binary counter
  - The date of purchase of the car and the usage pattern of the driver might give a clue
  - At a usage pattern of 10 transmissions per day, the wrap-around period is approximately 18 years
- If the top bits are determined by the serial number of the transmitter, this provides the attacker with substantial information

Cryptologists Involved

- Bogdanov: Guess-and-determine, slide, and distinguishing attacks
- Courtois, Bard and Wagner: Slide-algebraic attack
- Indesteege, Keller, Dunkelman, Biham and Preneel: Slide- and meet-in-the-middle attacks
- Eisenbarth, M & T Kasper, Moradi, Paar, Salmasizadeh, Shalmani: Power analysis

Algebraic Attack

Keeloq Algebraic Equations

- NLF(x_4,x_3,x_2,x_1,x_0) = $x_0 \oplus x_1 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0x_4 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_0x_1x_4 \oplus x_0x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$
- Add 2 variables $\alpha = x_3x_4$ and $\beta = x_0x_4$
- Assume F bits of the key are known, then for r rounds of the cipher, there are

  $3r + 64 + F$ multivariate quadratic equations in

  $3r + 96$ variables of which $64 + F$ are known
- The total number of distinct monomials is approximately $12r$

Complexity of Algebraic Attack

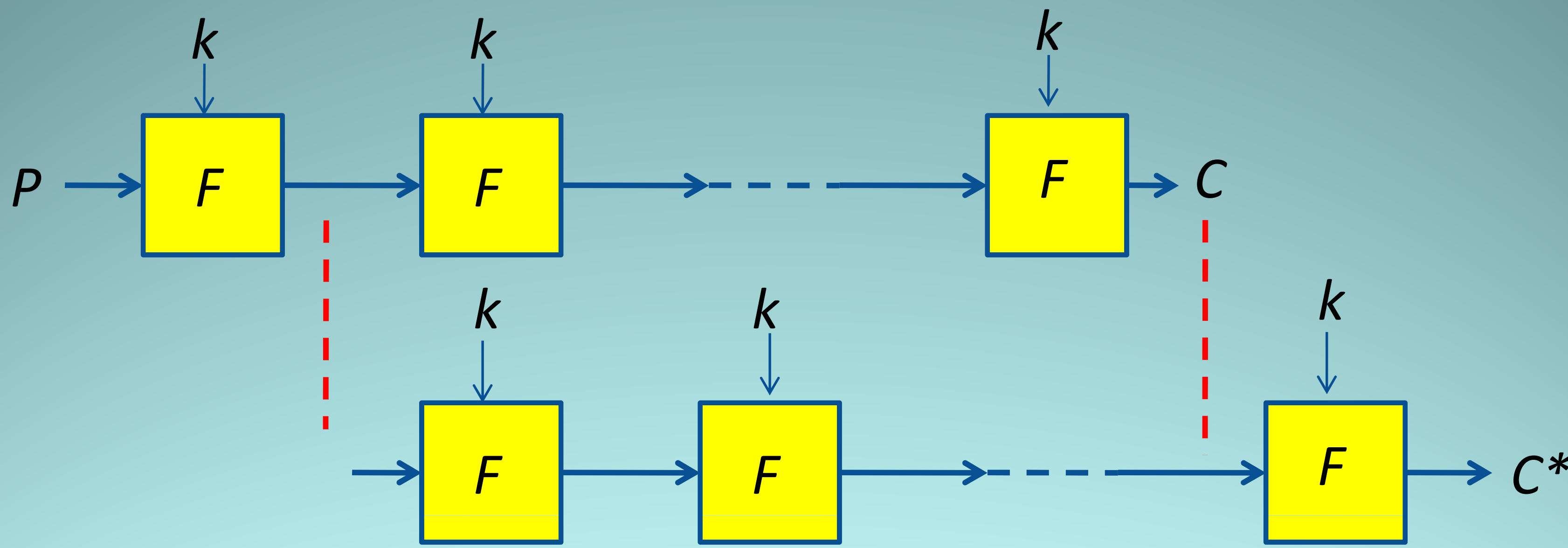
- Faster than exhaustive search on reduced Keeloq:
  - With $r = 128$, 2 known plaintexts, 30 bits guessed, the remaining 34 bits are recovered in 150 s by the program MiniSat 2.0
  - With $r = 160$ rounds, 2 plaintexts in counter mode, 30 bits guessed, the remaining 34 bits are recovered in 233 s by the program MiniSat 2.0

Linear Slide Attacks

Linear Slide Attacks

- Data requirement: 2^{32} known plaintexts (Full code book)
- Basis of attack:
  - Self-similar key schedule (supports slide attack)
  - Efficient linear approximation to the NLF
  - Existence of linear relations within the algorithm

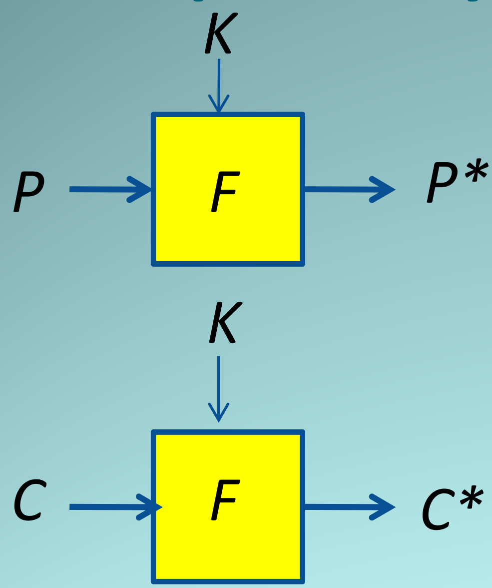
Slide Attack



A pair (P,C), (P^*,C^*) is called a *slid pair* if

$F(P) = P^*$ and $F(C) = C^*$

Complexity of the Slide Attack



- Assume that P and P^* is a slid pair, then so is C and C^*
- Use this information to solve for K
- Verify the solution by checking additional plaintext-ciphertext pairs

Complexity

1. The attacker is searching for collisions, which, due to the birthday paradox, have a high probability after $2^{n/2}$ pairs have been searched
2. Solving for K should be $<< 2^K$

Linear Approximation to NLF

$NLF(x_4, x_3, x_2, x_1, x_0) = x_0 \oplus x_1 \oplus x_0x_1 \oplus x_0x_3 \oplus x_0x_4 \oplus x_1x_2 \oplus$
$x_2x_3 \oplus x_2x_4 \oplus x_0x_1x_4 \oplus x_0x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$

- The best linear approximation, used in the slide-determine attack, is $x_0 \oplus x_1$.

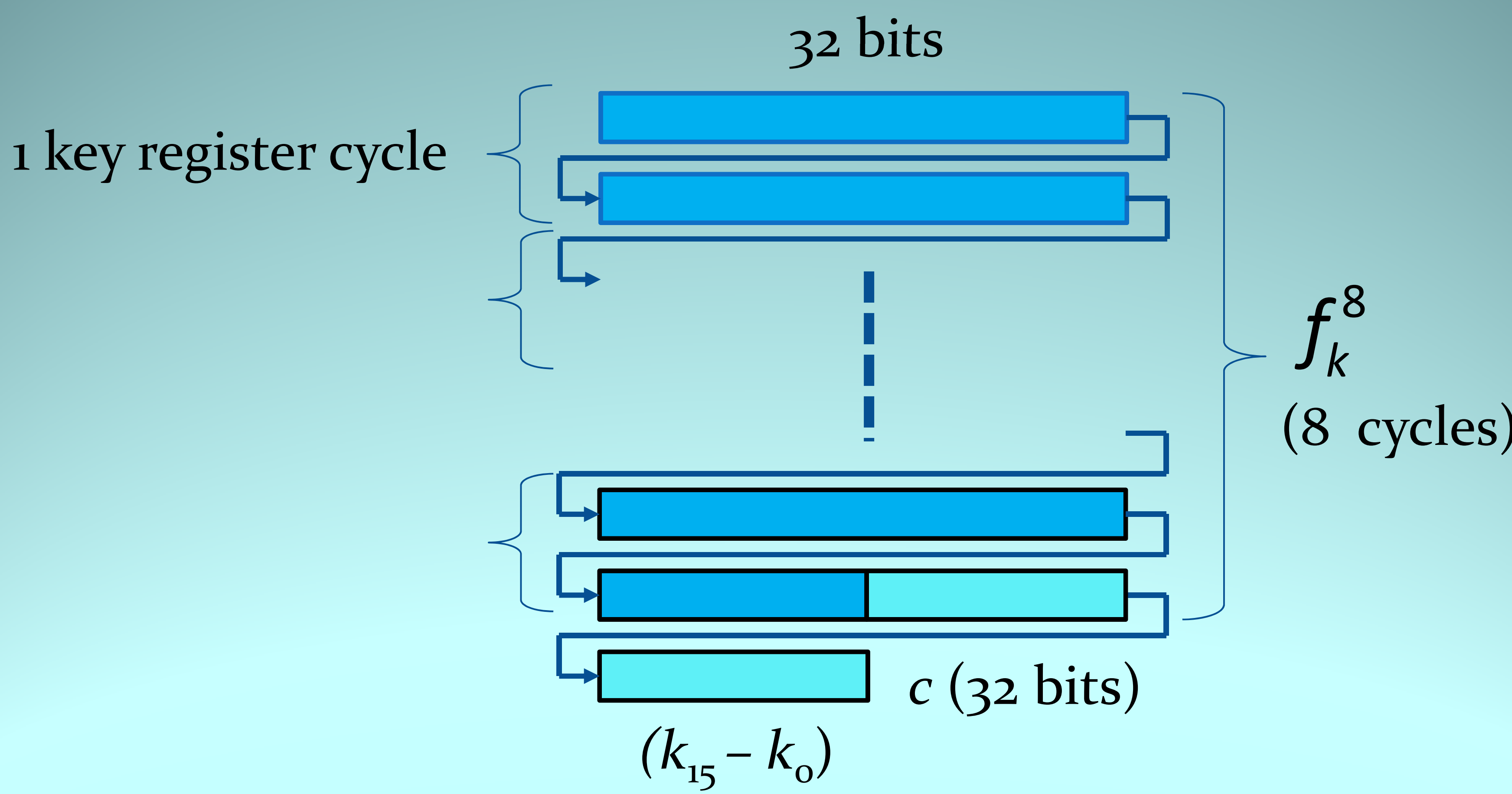
$Pr(NLF(x_4, x_3, x_2, x_1, x_0) = 0 \mid x_0 \oplus x_1 = 0) = 5/8$
$Pr(NLF(x_4, x_3, x_2, x_1, x_0) = 1 \mid x_0 \oplus x_1 = 1) = 5/8$

Best Determine-Slide Attack

- Data: 2^{32} known plaintexts (full codebook)
- Complexity: $\approx 2^{37}$ Keeloq encryptions

Slide/Fixed Point Attacks

Cycle Structure of Keeloq



Slide-Determine Attack

- Remove the ¼ cycle by guessing the first 16 key bits and decrypting the ciphertext by 16 rounds
- Given the pair (p, c), Search for fixed points $f_k^8(p)=p$
  - About 2^{16} pairs will be found (birthday paradox)
- Store the triples $(p, c, (k_{15}, \dots, k_0))$
- Apply an algebraic attack to determine the unknown 48 key bits
- Verify solutions by checking additional plaintext-ciphertext pairs

Complexity

- Data: 2^{32} known plaintexts (full codebook)
- Version A: Average = $2^{31.1}$ Keeloq encryptions
- Version B (optimised): Average = $2^{27.7}$ Keeloq encryptions

Safe Keys

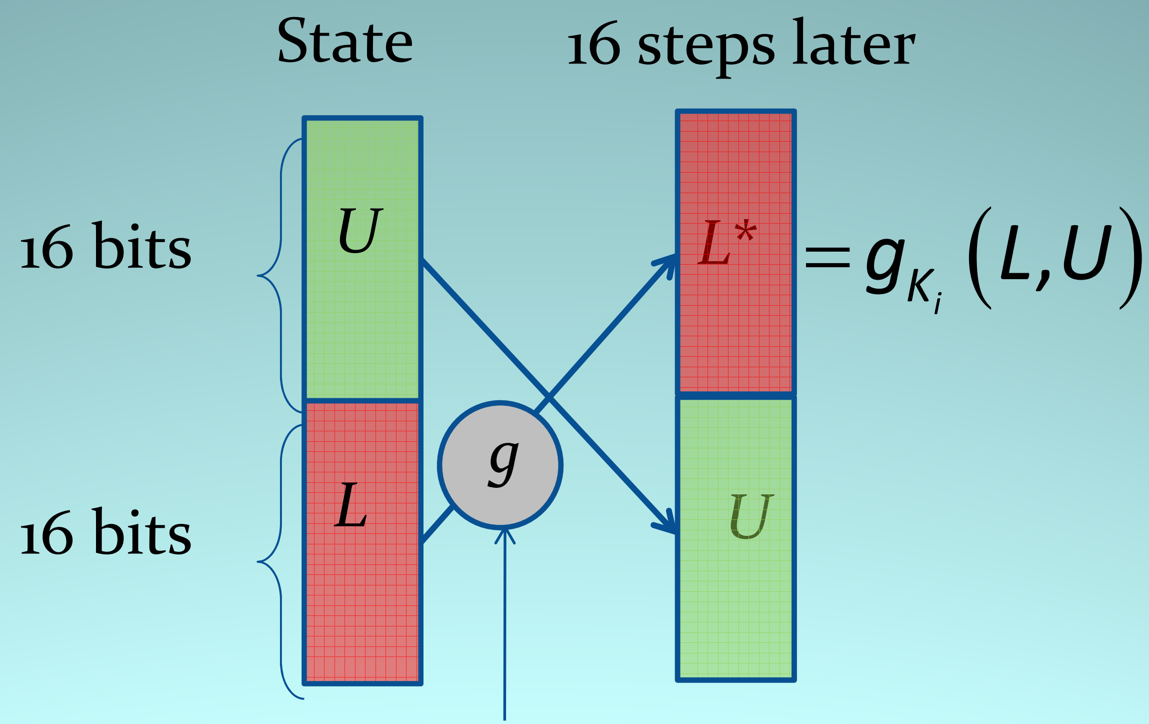
- The success of the attack depends on the existence of fixed points, and this is a function of the key
  - Version A works for about 63% of keys
  - The attack does not work for about 37% of keys
  - Optimised version A works for about 30% of keys

Slide/Meet-in-the-Middle Attack

Slide/Meet-in-the-Middle Attack

- Participating research groups
  - Computer science department, Technion, Israel
  - Research group COSIC of the Katholieke Universiteit Leuven, Belgium
  - Math department of the Hebrew University, Israel

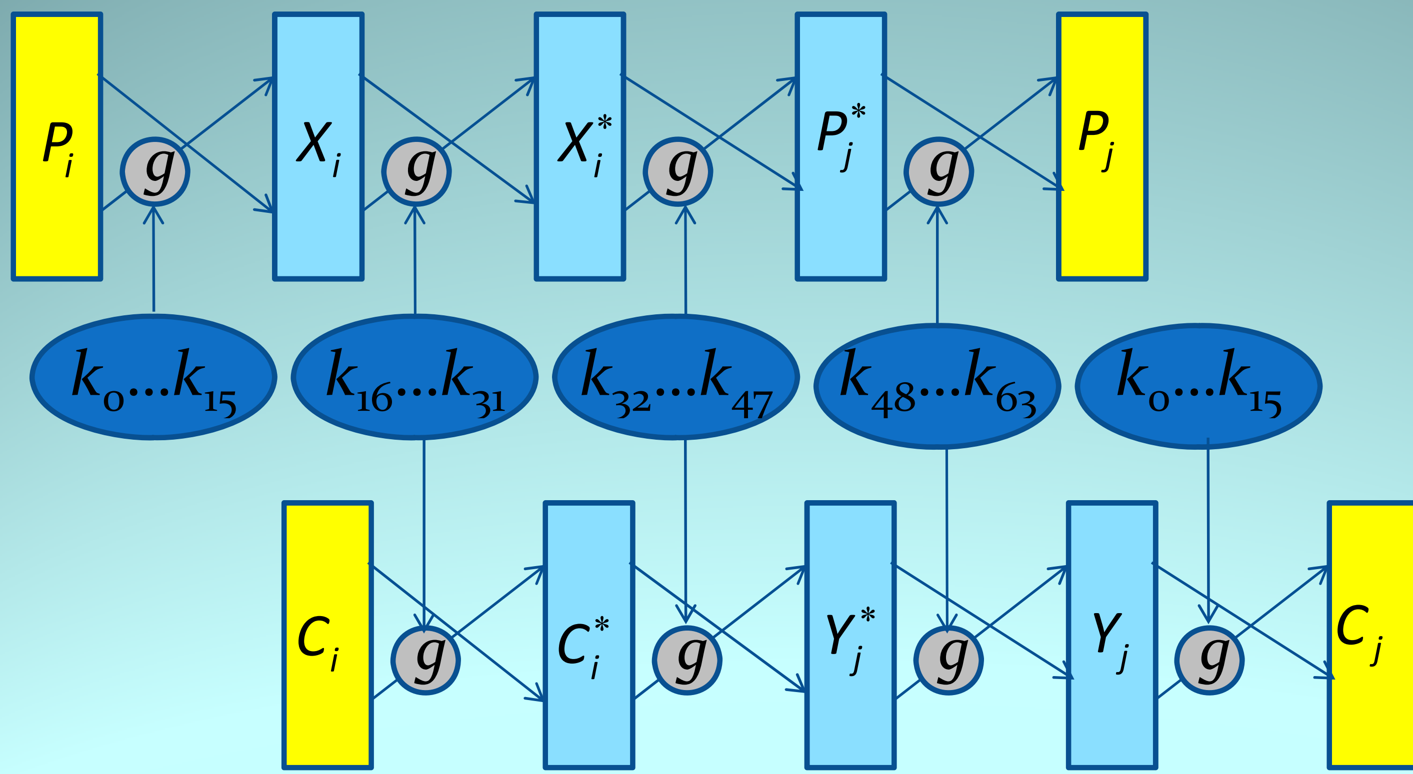
Recovering Key Bits



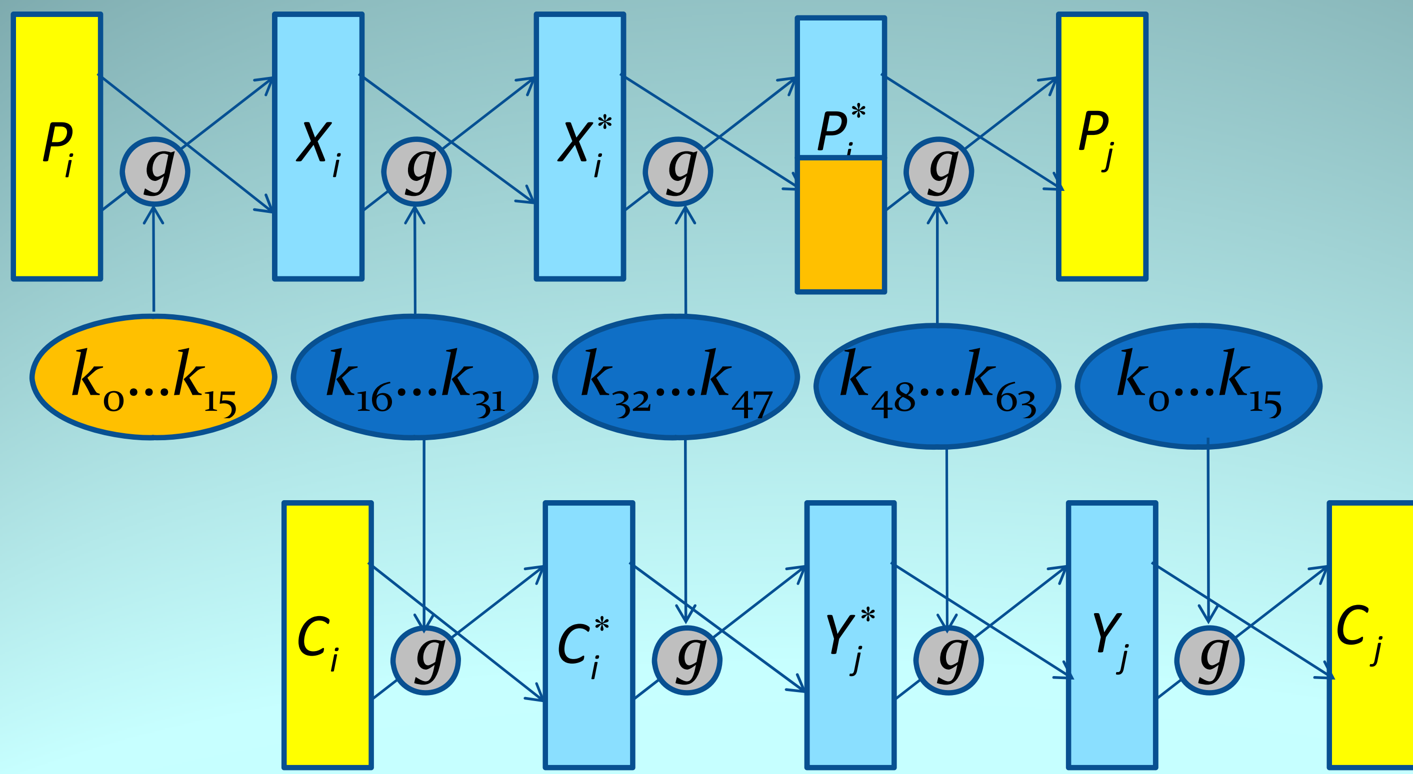
$K_i = (k_{16i} \ldots k_{16i+15})$, i = 0,1,2,3

K_i is easily solved if L, L^* and U are known

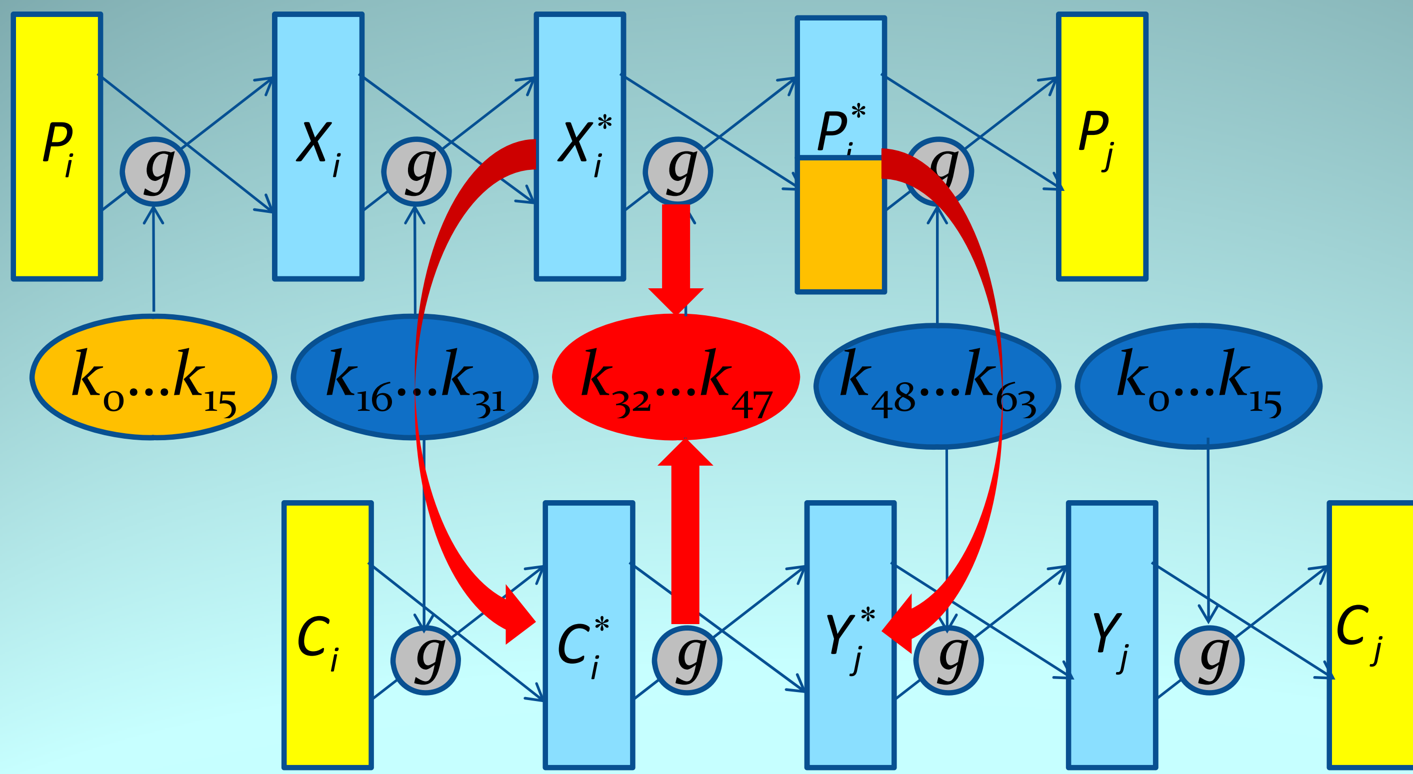
Meet-in-the-Middle Attack



Meet-in-the-Middle Attack



Meet-in-the-Middle Attack



Complexity of the Attack

$$2^{16}(32\cdot 2^{16} + 2^{16}(32\cdot 2^{16} + 2^{16}(32 + 4))) = 2^{54.0} \text{ rounds}$$

- Data: 2^{16} known plaintexts
  - 65 minutes to obtain data
- Time complexity: $2^{45.0}$ Keeloq encryptions
  - 7.8 days on 64 CPU cores
  - Variant requires 3.4 days on 64 CPU cores

Discussion

Discussion

- Keeloq has been successfully cracked, but a pure algebraic attack requires more research
- Improvements:
  - Scale up the Keeloq block and key lengths
  - Slight structural changes to the key schedule would stop slide attacks

Benefit of Hindsight

- The design team underestimated
  - The rapid progress in brute force computational capabilities
  - Discovery of new attacks, such as the slide attack


ACCESS DENIED
... should’ve attended EUROCRYPT.