Cursus Cryptografie

MODERN

26-02-2017

Onderwerpen

- Blokgeheimschrift
- Feistel algoritme
- Data Encryption Standard
- Cryptoanalyse van DES
- Alternatieven voor DES
- Advanced Encryption Standard

Rekenen met Bits

		$a \oplus b$	$a \vee b$	$a \wedge b$
a	b	a XOR b	a OR b	a AND b
0	0	0	0	0
0	1	1	1	0
1	0	1	1	0
1	1	0	1	1
complement NOT 0 = 1 en NOT 1 = 0				
XOR = exclusive or				

Blokgeheimschrift

Een *n*-bits klaartekst → *n*-bits cijfertekst blok = *n* bits

Een *n*-bits → *n*-bits bijectieve afbeelding

Maximaal $2^n!$ vercijfersleutels voor *n*-bits vercijfering

Meestal minder 64-bits sleutel, 64 bits blok → $2^{64} << 2^{64}!$

blok n = 2 bits, 2^2 = 4 waarden, 4! = 4x3x2x1 = 24 sleutels

klaar	sleutel-1	sleutel-3	sleutel-4	…	sleutel-24
↓	↓	↓	↓	↓	↓
00	00	01	10	…	11
01	01	10	11	…	10
10	10	11	00	…	01
11	11	00	01	…	00

Blokgeheimschrift

- Periodiek bij herhaling $M \rightarrow C \rightarrow C^2 \rightarrow \ldots \rightarrow C^{periode} = M$
  - fixed point $E(M,K) = M$
  - antifixed point $E(M,K) = \text{complement}(M)$
  - zwakke sleutel $E(E(M,K),K) = M$
- Maskeren door whitening $M \oplus W_{in} = M' \rightarrow C' \oplus W_{uit} = C$
- Maskeren door Block Chaining

Electronic Code Book

```
* MYSTERY PROGRAM                                                    00000010
* D.E.KNUTH                                                          00000020
* THE ART OF COMPUTER PROGRAMMING, VOL I                             00000030
* EXERCISE 1.3.2 # 8                                                00000040
PRINTER   EQU   18                                                  00000050
BUF       ORIG  *+3000                                              00000060
1H        ENT1  1                                                   00000070
          ENT2  0                                                   00000080
          LDX   4F                                                  00000090
2H        ENT3  0,1                                                 00000100
```

ECB

```
\BKF<&bm/qKI5¨Uz}eKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rb?X
\BK=pw<s+m AbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rb@X
\BKM+w.i/lKH)RQw*h!M(%.x/grK$ [q+_Wx9¨ZH&8KxbR.H\8KxbR.H\8KxbR.HlH[)rbAX
\BK>;w`k&kpxs`AVn8NxzR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbBX
\h}B1'Sz\8K>4(.H\IcxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbCX
\Z!?bR.H\8KH5{UH\BV,rb>H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbDX
\IsxbR.H\8K>1'?H\IKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbEX
\8KxbR.H\8K>1'@H\HKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbFX
\8KxbR.H\8KE'+.H\LqxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbGX
\JsxbR.H\8K>1'AH\HW*bR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rc>X
```

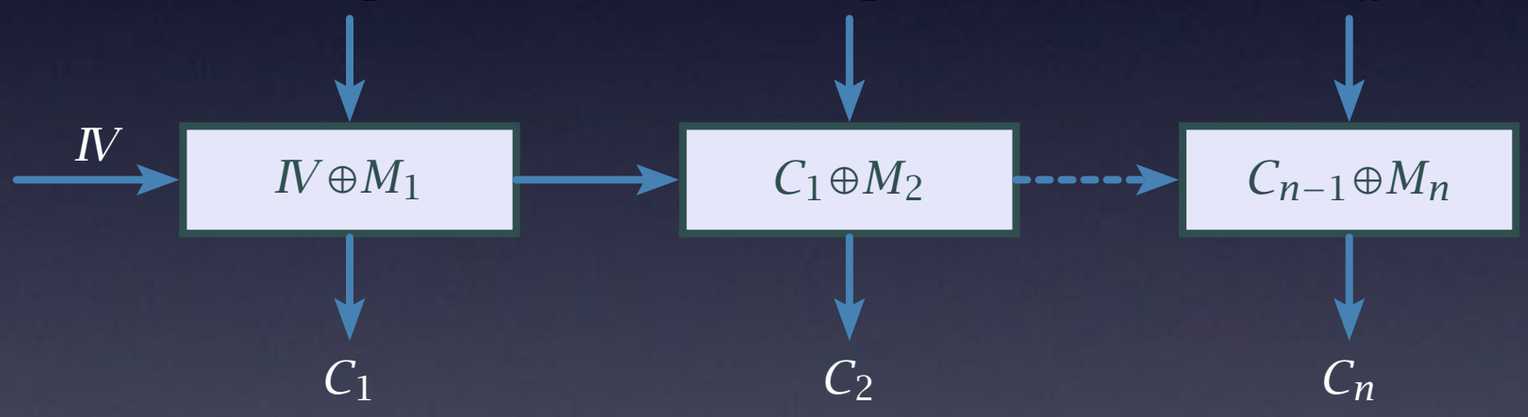
Remedie tegen structuur:
Cipher Block Chaining of Counter Mode

Cipher Block Chaining

ECB

```
\BKF<&bm/qKI5¨Uz}eKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rb?X
\BK=pw<s+m AbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rb@X
\BKM+w.i/lKH)RQw*h!M(%.x/grK$ [q+_Wx9¨ZH&8KxbR.H\8KxbR.H\8KxbR.HlH[)rbAX
\BK>;w`k&kpxs`AVn8NxzR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbBX
\h}B1'Sz\8K>4(.H\IcxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbCX
\Z!?bR.H\8KH5{UH\BV,rb>H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbDX
\IsxbR.H\8K>1'?H\IKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbEX
\8KxbR.H\8K>1'@H\HKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbFX
\8KxbR.H\8KE'+.H\LqxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbGX
\JsxbR.H\8K>1'AH\HW*bR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rc>X
```

CBC

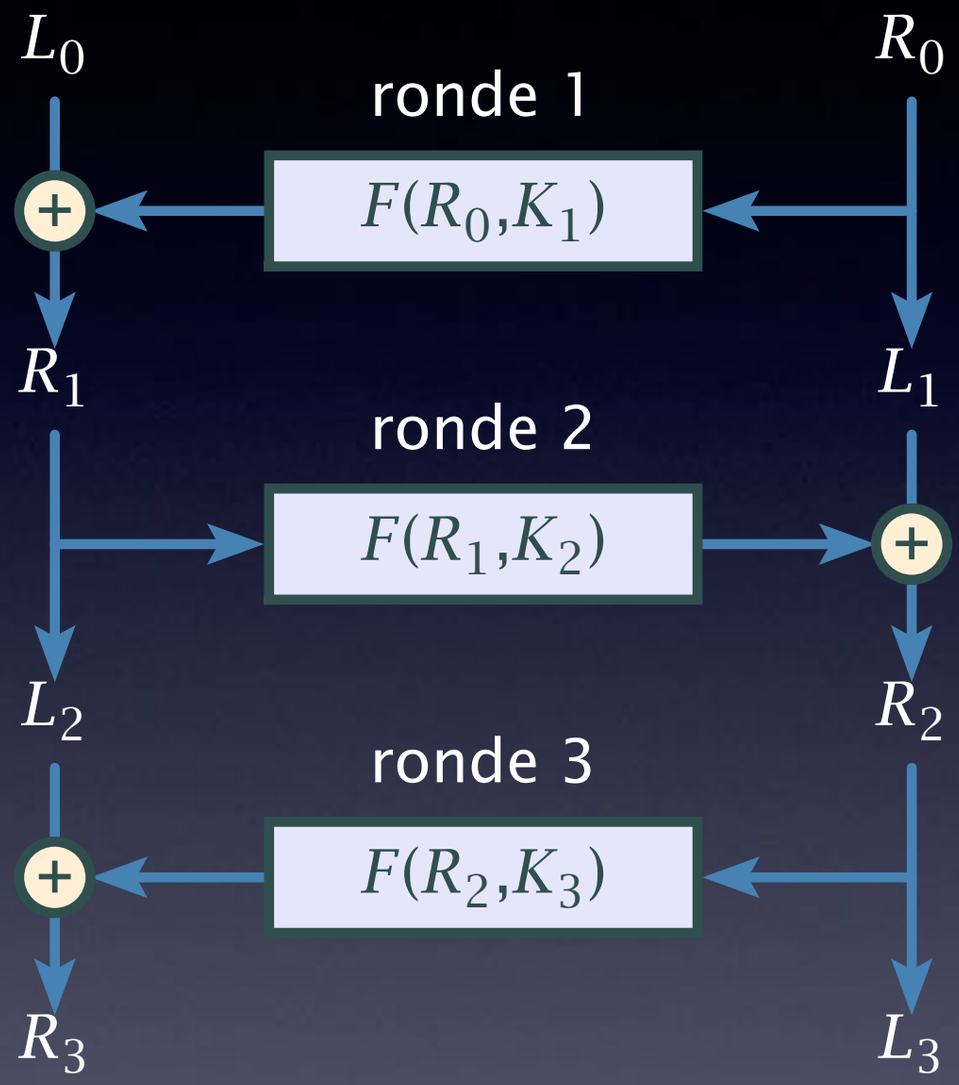



```
\BKF<&bm,T70qHX)JZ#It;'qG3nbw.UZDkZ{z!$CADF5}sR,>|2N!f!t;U}g$YO]H>y17\/V
E!enHtkjp/&PKg:SmgqiNZh<j@]#QM7%gxI<T@emdQ5UW34Va*!nZ&b?^bl(]x1(kKhQp{q!
h.T?<4@+8;@(e'2CbDau.L`\2LtaRl\n]Llz,/WW$%X4/¨&@!]DM2tT)}6Of5g#q+ ,0Hjdj
(awn$#evNm)(8$Gm]FwASvuVZ cZViD?WWOsY\r(T0;-\OApQh'F_BoYNAr_b5>B[*n)u8!;
X3-kG_tVUkxJ{(C?RU|c zq(O.h|¨m@pLfT6%`nYI?@O(S=BFw,h+Fk+CPw¨.9:sP9sKA<}l
M45+D/LUJl!syKB>GOw@-N!'D(cYOAOoA`Or34}X>9;,6'LA;q'E9yz*8Jr^<lIrE3n(Oo.k
B|#ARb\T?Un $*<=<?Z9'|j&9wFR*o9n6P2k-bgW3)}%OU6@Oai>3Hd)-:UW6;3q:#Q!I>xj
7[=:L1GS44)x}X(<1|t2!KV%.U`K$>%m+.Ld'1SV(f8}*$¨?%?$7-vP(¨woPOi p/`kyClei
,9W3F_4R)qCxm+b;&^U2p}1$#7AKsp_l o-dvc.U|Hx}yV\>y!d7|I+'vYPP <Yo$BLy3?Ah
!-`362oQ}eLqgYQ:zND<jL #w'OUm?Nkt_{np2|Tq8g(s%K=npSAvwy&kI?ZyjHnx2;$-n'g
```

Feistel schema

$$E(M,K): \quad L_1,R_1 = R_0,L_0 \oplus F(R_0,K_1)$$
$$L_2,R_2 = R_1,L_1 \oplus F(R_1,K_2)$$
$$L_3,R_3 = R_2,L_2 \oplus F(R_2,K_3)$$

$$D(M,K): \quad L_2,R_2 = R_3,L_3 \oplus F(R_3,K_3)$$
$$L_1,R_1 = R_2,L_2 \oplus F(R_2,K_2)$$
$$L_0,R_0 = R_1,L_1 \oplus F(R_1,K_1)$$



Voordelen
Geen bijzondere eisen aan functie
Meer stappen i.h.a. meer veiligheid

Gebalanceerd: #L = #R

Data Encryption Standard

1973 Initiatief National Bureau of Standards (nu NIST)

1975 IBM enig inzender voor DES

1978 Hearings US Senate Committee on Intelligence

1980 Hellman Time Memory Tradeoff e.a.

1991 Biham en Shamir Differential Cryptanalysis

1993 Matsui Linear Cryptanalysis

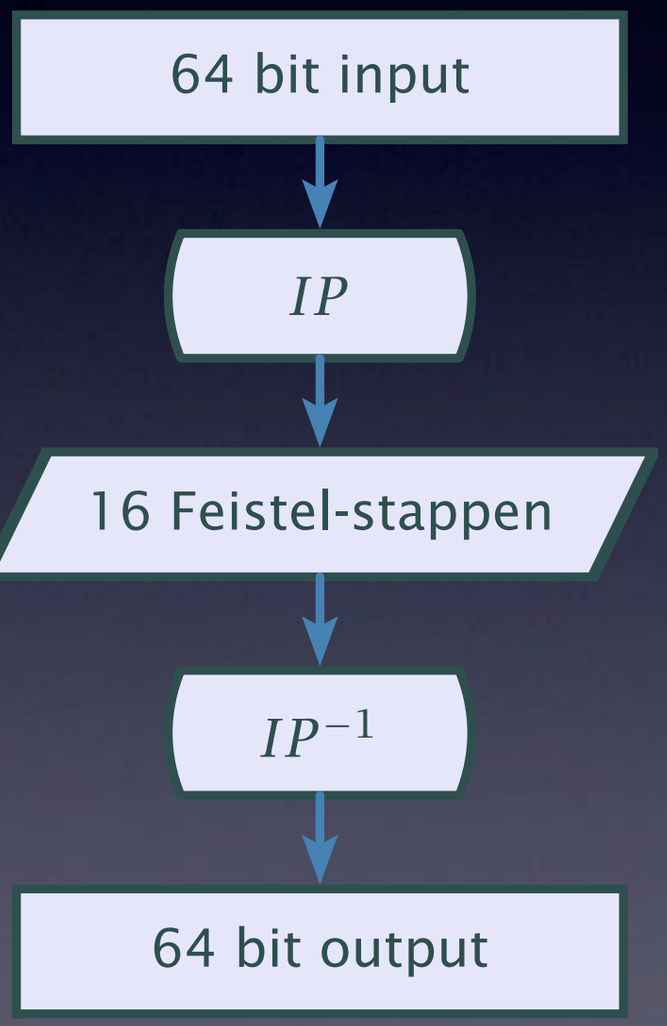
1997 Software brute force – NIST start AES op

1998 Hardware brute force

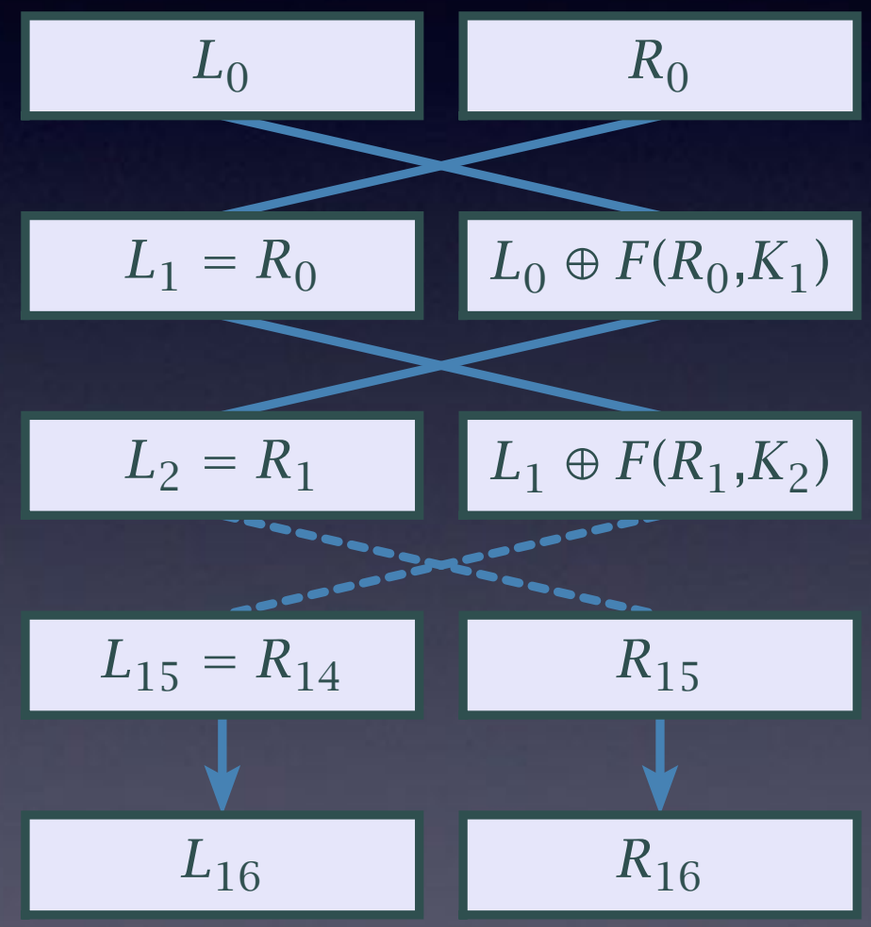
1999 DES voor het laatst verlengd als standaard

DES - schema

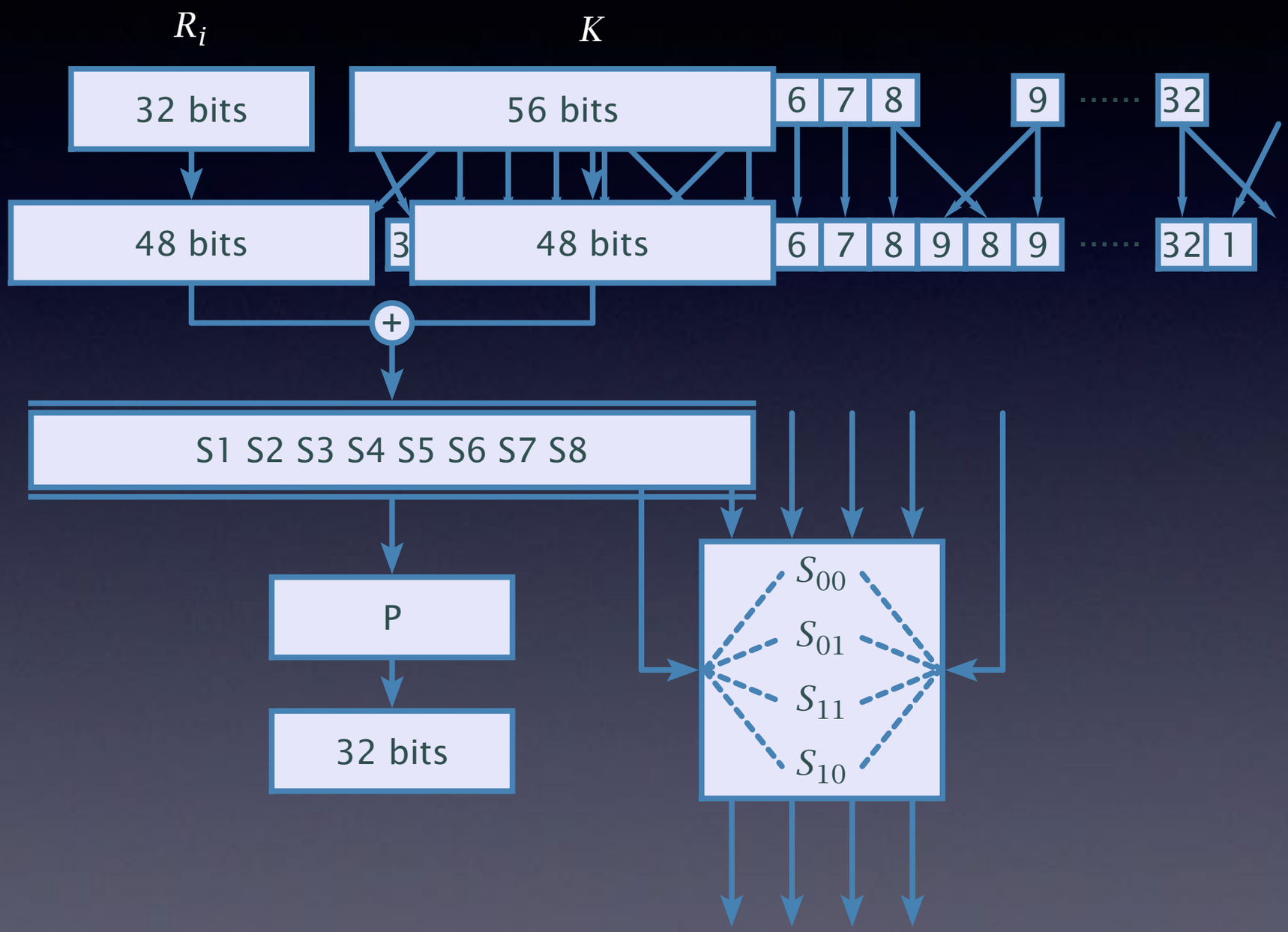
Hoofdschema



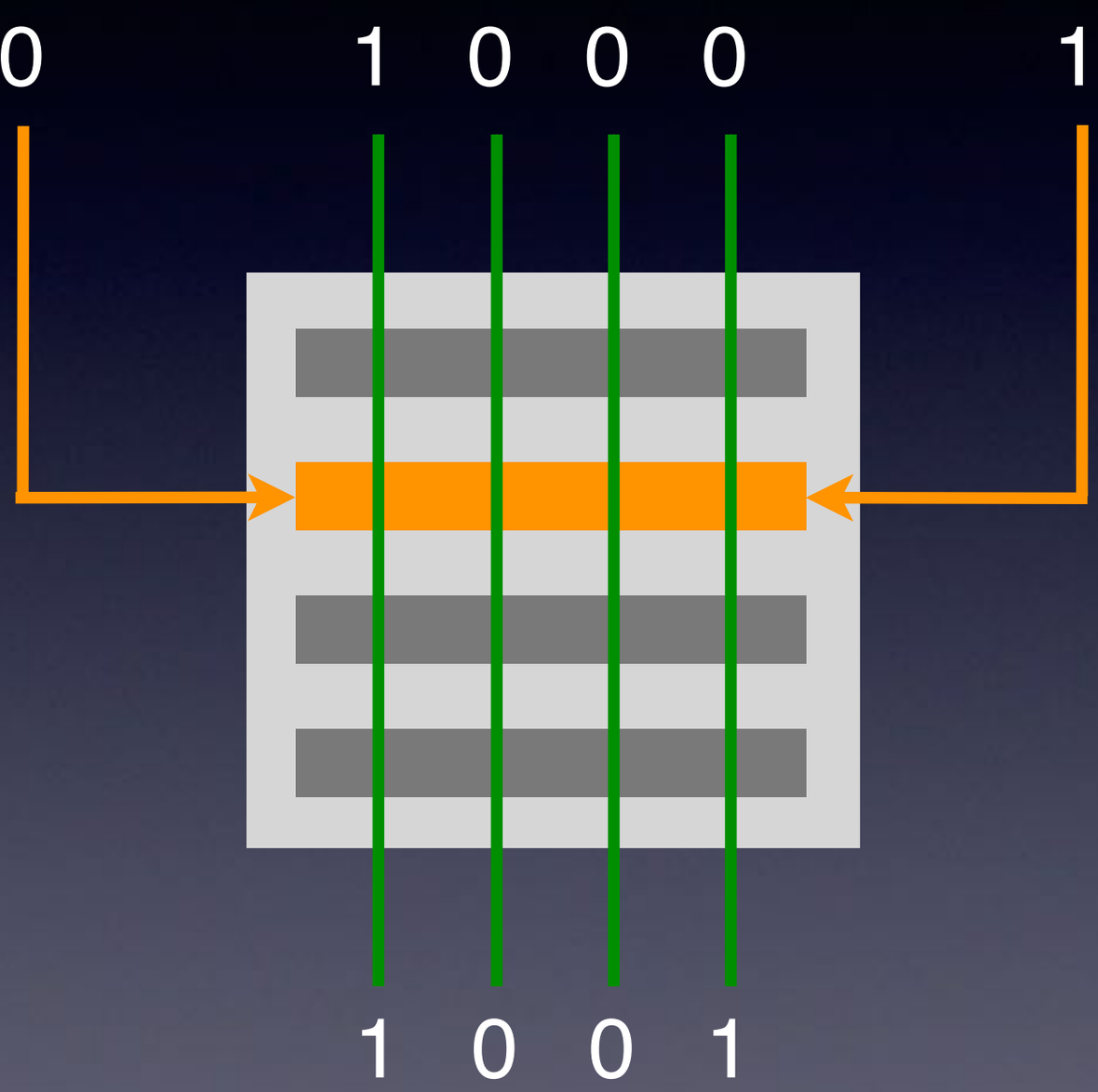
Rondetransformaties



Transformatie

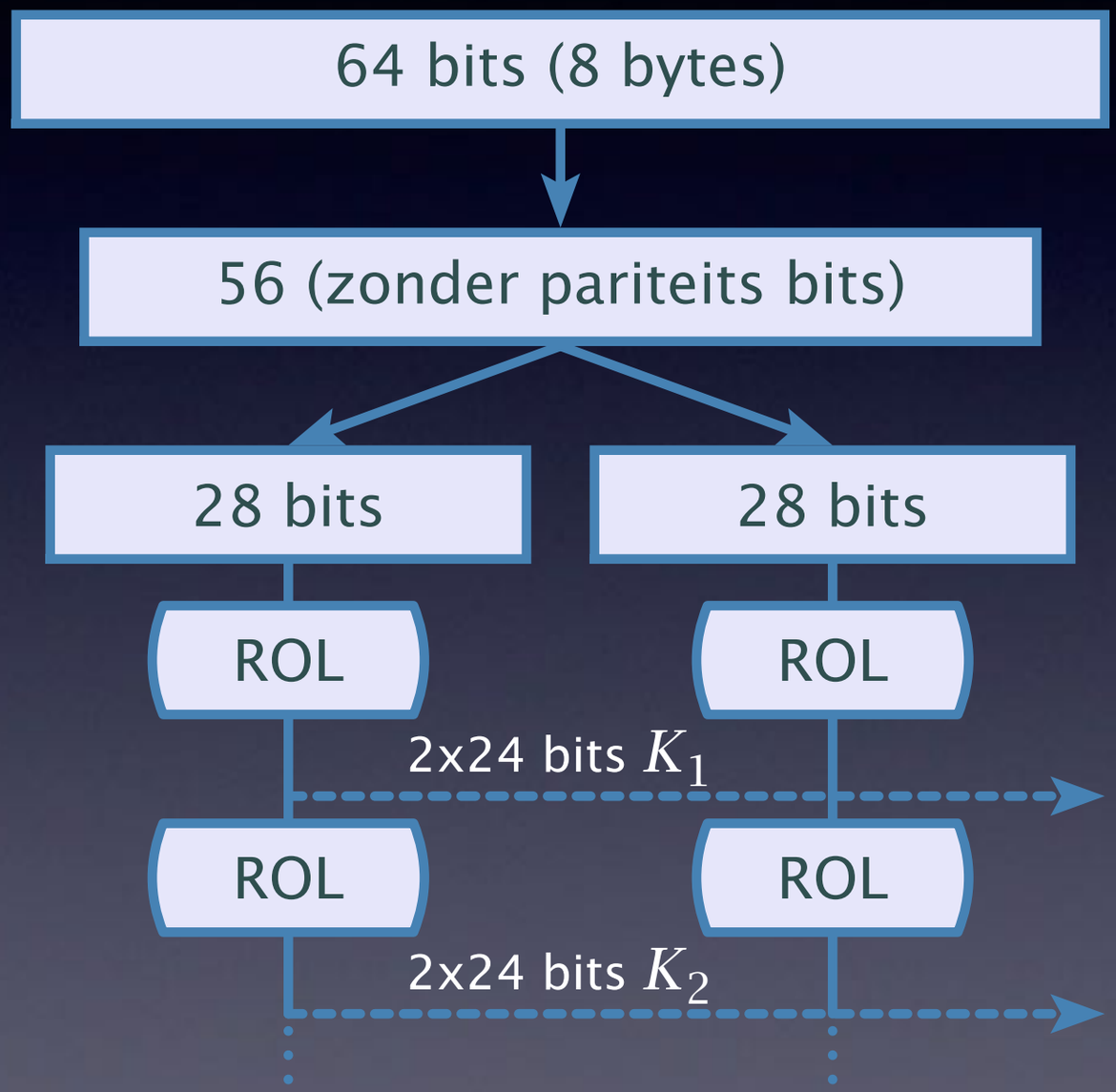


S-doos operatie



0000	1111
0001	0001
0010	0100
0011	1110
0100	0110
0101	1011
0110	0011
0111	0100
1000	1001
1001	0111
1010	0010
1011	1101
1100	1100
1101	0000
1110	0101
1111	1010

Sleutelschema



- 64 → 56 bits - pariteitsbits
- rotaties 1122222212222221
- 4 zwakke sleutels
  (00…)(11…)
  M = *E(E(M,K),K)*
- 12 halfzwakke sleutels
  (0101…)(1010…)
  M = *E(E(M,K′),K)*

Triple DES

- 56 bit DES niet langer veilig genoeg is 2-maal DES een 112 bits sleutel?
- 2-maal DES is *niet* 2x56 = 112 bits maar effectief slechts 57 bits reden meet in the middle aanval
- 3-maal DES met EDE schema
  Triple DES = $E_{K3}(D_{K2}(E_{K1}(M)))$
- Triple DES mogelijkheden
  1. $K_1 \neq K_2 \neq K_3$
  2. $K_1 = K_3 \neq K_2$
  3. $K_1 = K_2 = K_3$ compatibility mode

Meet in the Middle		
E_1		D_1
E_2	$= D_6$	D_2
E_3		D_3
E_4		D_4
E_5		D_5
E_6	$E_2 =$	D_6
E_7		D_7
…		…

Cryptoanalyse van DES

- De “DES controverse” DES door NSA te breken?
- Brute force = uitputtend zoeken
  - software
  - hardware
- Fysische methoden (Side Channel Analyse)
  - foutinjectie
  - tijdsduur operaties
  - analyse stroomverbruik
- Time Memory Tradeoff
- Differentiële cryptoanalyse
- Lineaire cryptoanalyse

DES controverse

- National Security Agency is betrokken bij ontwikkeling DES
- Voorganger Lucifer 128 bits DES 56 verzwakt door NSA?
- Is 16 ronden Feistel wel genoeg?
- Ontwikkelcriteria i.h.b. van S-dozen zijn geheim verdacht?
- Structuur in S-dozen én ontwerp geheim valluik ingebouwd?
- Hardware brute force binnen capaciteit NSA?
- Onderzoek US Senate Committee on Intelligence in 1978:
  - DES is more than adequate for its intended applications
  - IBM invented and designed DES
  - NSA did not tamper with the design
  - NSA certified DES free of known statistical/mathematical weakness
  - overtuigend?

Brute Force

Hardware

1984: DES-crips gaat 256 coderingen per seconde

1998: Deep Crack gebouwd voor $250.000

37.050 DES-chips parallel

2.500.000 encrypties per seconde

alle sleutels in ± 9 dagen

Unicity Distance DES ≈ 16 bytes

$(70/256)^{16} \times 2^{56} \approx 70.000.000$ vals alarm

1997 Rocke Verser internet programma zoals SETI

78.000 deelnemers

maximaal 14.000 machines tegelijk

18 feb – 17 juni → Eureka

Hoe een goede sleutel te herkennen?

Tekst ~ [a...zA...Z0...9...] →

± 70 uit 256 plausibel

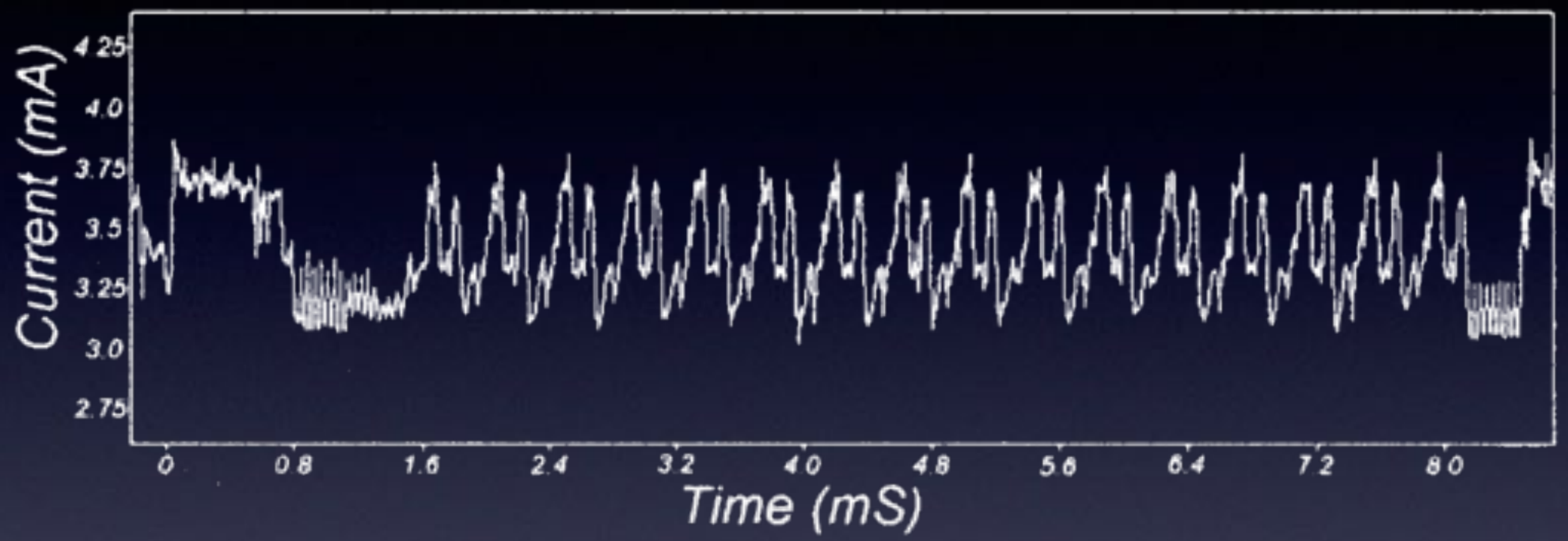
ciphertext-only

Unicity Distance DES ≈ 8 bytes → 2^{16} vals alarm

Software

known-plaintext

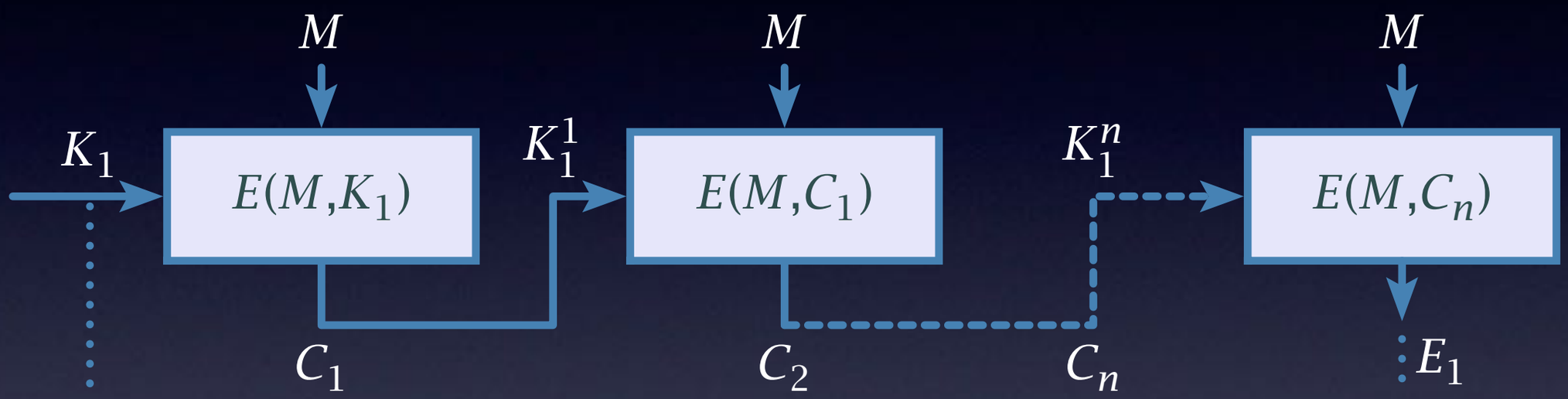
Side Channel Analyse



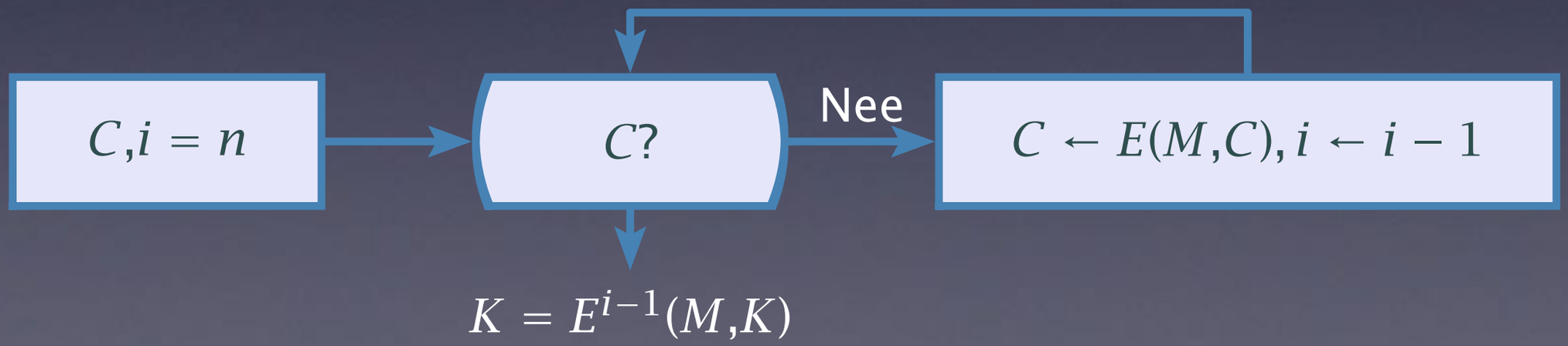
- Stroomverbruik toont processor acties
- Foutinjectie geeft verschillende uitkomsten
- Timing analyse door verschil in processor instructies

Time Memory Tradeoff

Voorbereidingsfase



Analysefase



Differentiële Cryptoanalyse

Chosen-plaintext analyse van Biham en Shamir 1991

kies paren klaartekst met constant verschil:

$$\Delta M = M \oplus M^* = constant \quad C = E(M,K) \quad C^* = E(M^*,K)$$

dan geldt in elke ronde:

$$(R_{i-1} \oplus K_i) \oplus (R^*_{i-1} \oplus K_i) = R_{i-1} \oplus R^*_{i-1} = \Delta R$$

onderzoek per S-doos:

(R_{i-1}, R^*_{i-1}) met $\Delta R = constant$

Voorbeeld 1e substitutie van S_1:

$$\Delta_{in} = 1000_2 \begin{cases} (A,2)(2,A) \\ (6,E)(E,6) \end{cases} \xrightarrow{S_1} \Delta_{uit} = 1011_2 \begin{cases} (6,D)(D,6) \\ (B,0)(0,B) \end{cases}$$

Statistische verschillen S_1

Δ	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
0010	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
0011	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
0100	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
0101	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
0110	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
0111	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
1000	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
1001	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
1010	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
1011	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
1100	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
1101	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
1110	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
1110	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

- niet alle verschillen zijn aanwezig
- verschillen komen niet even vaak voor

Δ_{in} 1000
0010 ⊕ 1010 S_1 → 1101 ⊕ 0110 = 1011 = B
1010 ⊕ 0010 S_1 → 0110 ⊕ 1101 = 1011 = B
0110 ⊕ 1110 S_1 → 1011 ⊕ 0000 = 1011 = B
1110 ⊕ 0110 S_1 → 0000 ⊕ 1011 = 1011 = B
→ 4 in rij 1000-kolom B
0001 ⊕ 1001 S_1 → 0100 ⊕ 1010 = 1110 = E
1001 ⊕ 0001 S_1 → 1010 ⊕ 0100 = 1110 = E
→ 2 in rij 1000-kolom E
…

Karakteristiek verschil

4 Feistel-stappen: $L_4, R_4 = R_3, \underbrace{L_1 \oplus f(R_1, K_2)}_{L_3 = R_2} \oplus f(R_3, K_4)$

$$\Delta_{uit} = f(R_3, K_4) \oplus f(R_3^*, K_4) = \Delta L_1 \oplus \underbrace{f(R_1, K_2) \oplus f(R_1^*, K_2)}_{\text{uit gekozen } \Delta M} \oplus \Delta R_4$$

De gekozen ΔM heet een *karakteristiek*.
ΔM verdeelt zich over meerdere uitvoerverschillen.
Per ΔM dus slechts een *kans* op de gewenste karakteristiek.

$S \to p \leq 14/64 \quad \Delta M = 1960000000000000 \to p = 0.004274$
Herhaald over de benodigde 13 ronden $p \approx 2^{-47}$.
Plus andere trucs → iets beter dan uitputtend zoeken.

Resultaten Biham-Shamir

- Gegeven beste aanval is 16 ronden precies genoeg
- Permutatie minimaliseert kans op goede aanval
- Volgorde S-dozen $S_1S_2S_3S_4S_5S_6S_7S_8$ bijna optimaal
- Substituties binnen S-dozen optimaal
- Geen 4-substituties per S-doos verzwakt aanzienlijk
- Verwisselen expansie en subsleutel verzwakt
- Volledig onafhankelijke subsleutels maakt weinig uit

verrassende conclusie

DES optimaal beveiligd tegen differentiële cryptoanalyse

vervolgens bevestigd door Coppersmith, lid IBM-team

Lineaire Cryptoanalyse

Known-plaintext analyse van Matsui 1993

kans p dat $M[m_1,m_2,\ldots] \oplus C[c_1,c_2,\ldots] = K[k_1,k_2,\ldots]$

$M[m_1,m_2,\ldots] = \vec{X_M} \cdot \vec{M}$ ($\vec{X_M}$ is bitselector voor M)

itereerbare karakteristiek van Matsui

$$R[15] \oplus F(R,K)[7,18,24] = K[22] \qquad p = 42/64$$

$$R[29] \oplus F(R,K)[15] = K[44] \qquad p = 30/64$$

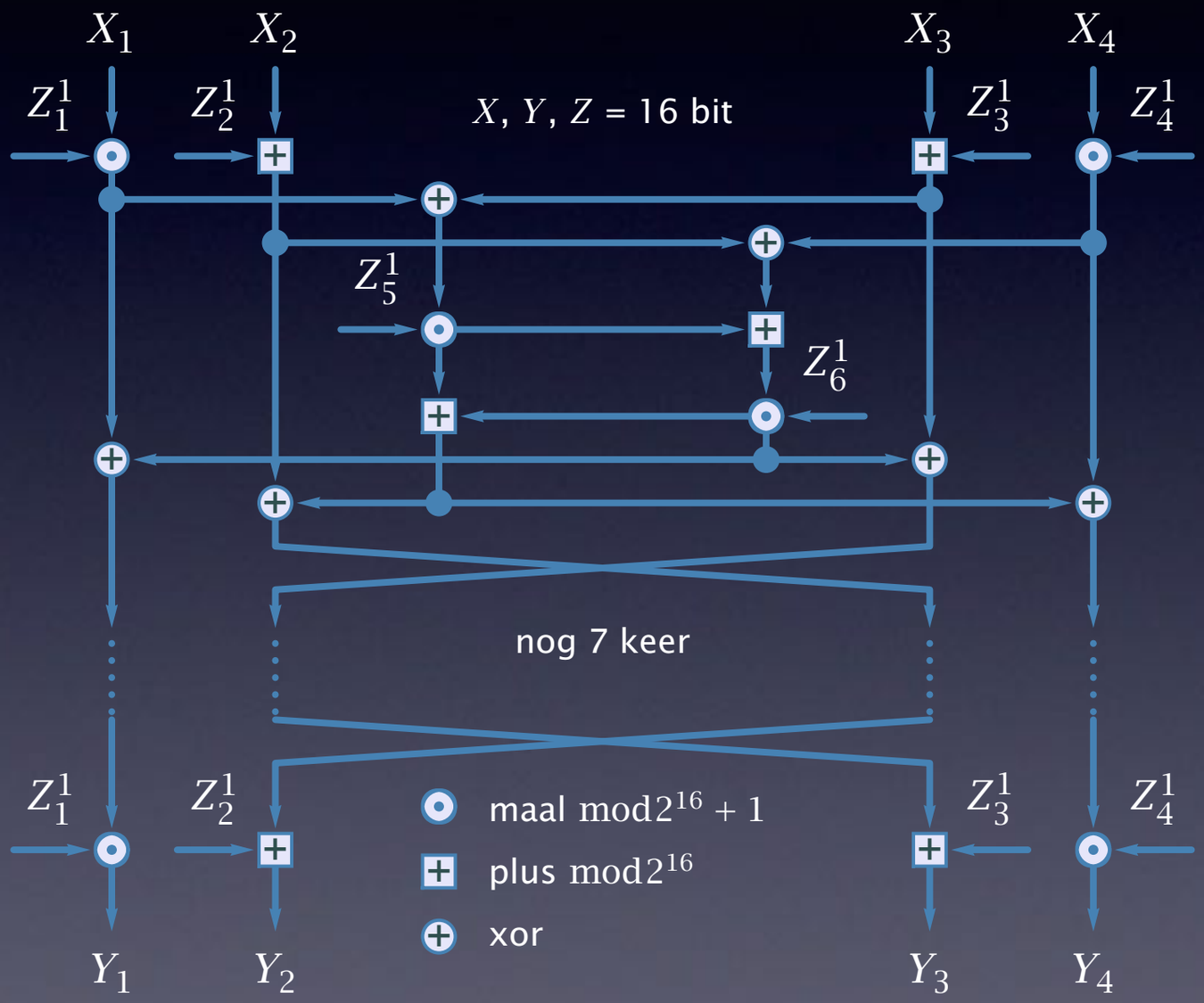
$$R[15] \oplus F(R,K)[7,18,24,29] = K[22] \qquad p = 12/64$$

totaal $p = 0{,}5 + 1.19 \times 2^{-22}$ → 2^{47} pt-ct paren nodig

DES alternatieven

- NEWDES Scott 1985 – geen variant van DES
- SKIPJACK NSA 1985 – escrowed encryption standard
- FEAL Shimizu en Miyaguchi 1987 – Japan
- IDEA Lai en Massey 1990 – ETH Zürich
- LOKI Brown, Pieprzyk, Seberry 1990 – Australië
- GOST Gosudarstvennyi Standard Soyuza – USSR
- BLOWFISH Schneier 1994 – Counterpane Inc
- RC5 Rivest 1994 – RSA Laboratories
- TEA Wheeler en Needham 1994 – Cambridge University
- enzovoorts, enzovoorts

IDEA – ingewikkeld



1990 Lai & Massey, ETH Zürich

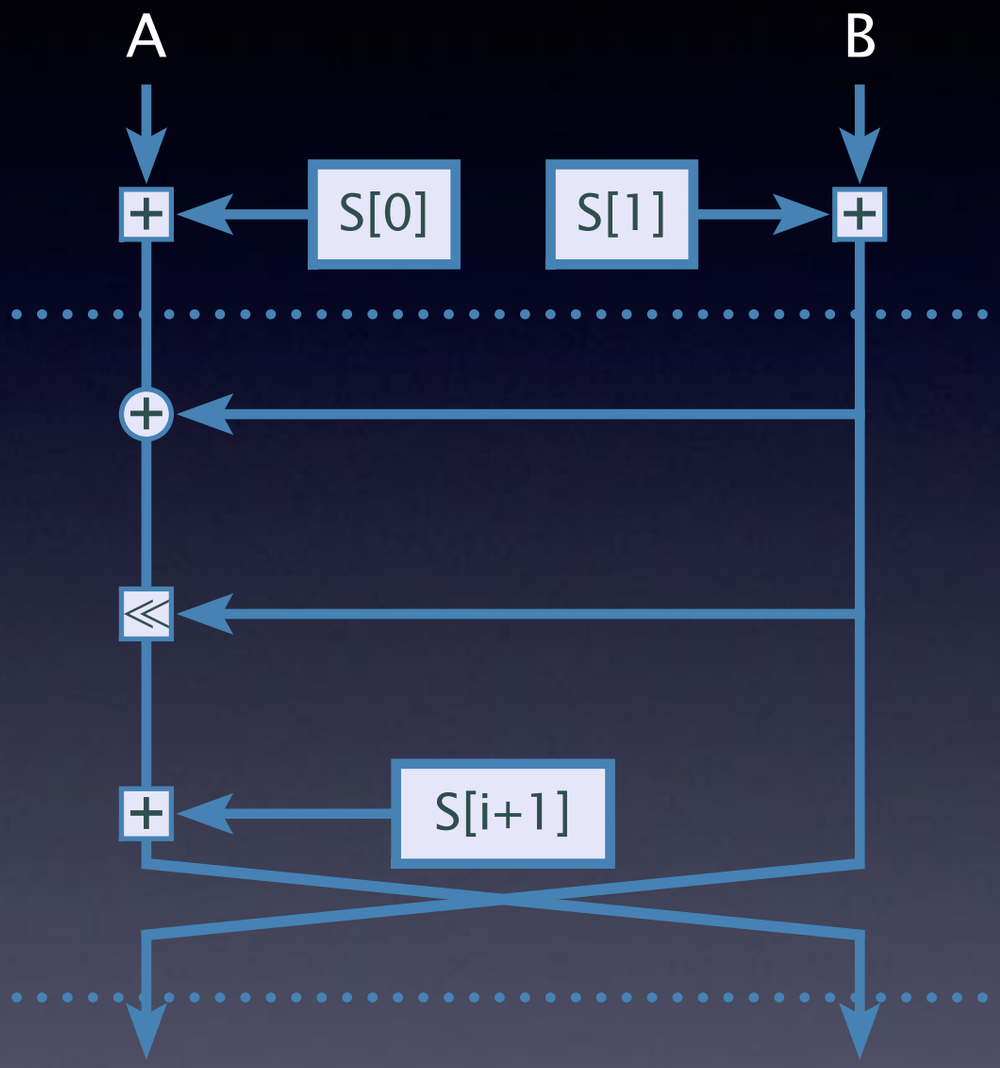
16-bits architectuur

128 bits sleutel

Cryptoanalyse tot 4-5 ronden

Daemen 1993
groepen zwakke sleutels 2^{23} 2^{51} 2^{63}

RC5 – eenvoudig



Halve ronde RC5

1990
Rivest, RSA laboratories

RC5-*w*/*r*/*b* parametrisatie
- blok 2*w* bits
- aantal rondes *r*
- sleutel *b* bits
- bv RC5-32/12/16

Operaties
- xor, plus/minus mod 2^{2w}
- data afhankelijke rotaties

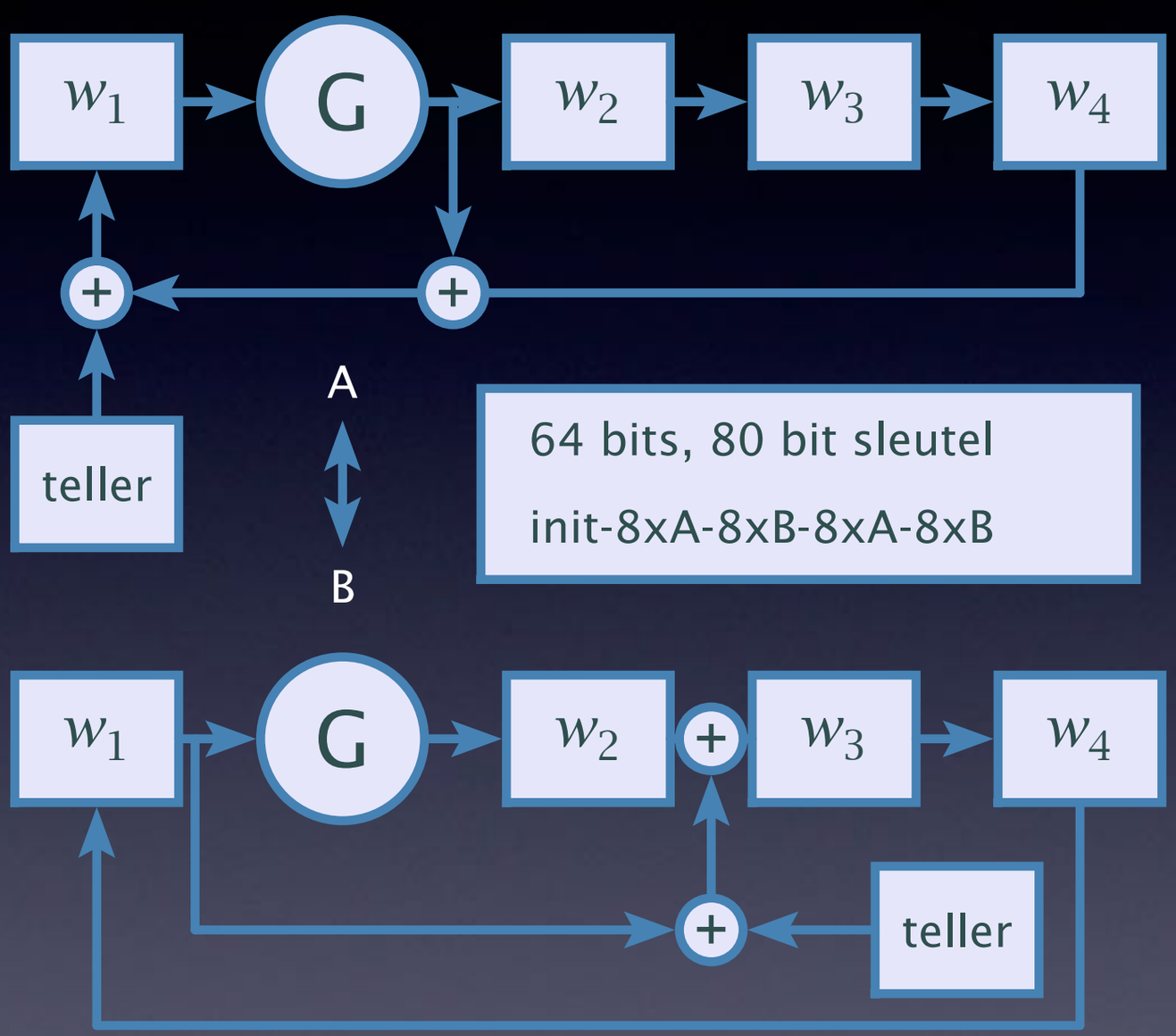
Subsleutels
K = b-bits → $S_0 \ldots S_{2r+1}$

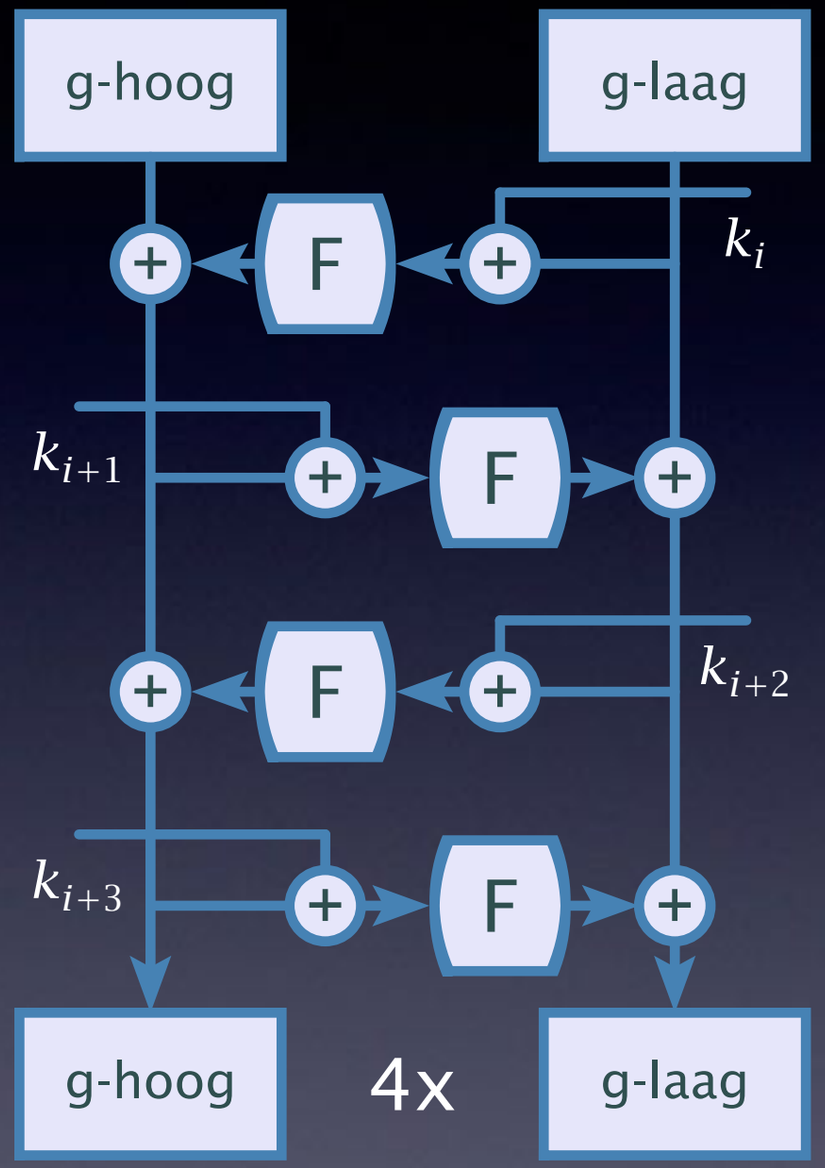
NSA = National Security Agency

Opvolger afzonderlijke Army & Navy codebrekers
24-10-1952 president Truman

NSA = “No Such Agency” 🤐

Skipjack





Declassificatie NSA in 1998 – Shamir e.a. 1999 impossible differentials

AES

12 september 1997 NIST start opvolging DES

AES = Advanced Encryption Standard

- ongeclassificeerd en publiek algoritme
- overal zonder royalties beschikbaar
- symmetrisch 128 bits blokgeheimschrift
- gebruikerskeuze voor sleutel uit 128, 192, 256 bits
- efficiënte implementatie t.b.v. smartcards, e.d.

In tegenstelling tot ’70-jaren nu
deelnemers uit alle delen van de wereld !

Deelnemers 1e ronde

CAST-256	Entrust Technologies Inc	Canada
CRYPTON	Future Systems Inc	Korea
DEAL	Outerbridge, Knudsen	Canada
DEC	Centre National Recherche Scientific	Frankrijk
E2	Nippon Telegraph and Telephone Corp	Japan
FROG	TecApro Internacional SA	Costa Rica
HPC	Schroeppel	USA
LOKI97	Brown, Pieprzyk, Seberry	Australië
MAGENTA	Deutsche Telekom AG	Duitsland
MARS	IBM	USA
RC6	RSA Laboratories	USA
RIJNDAEL	Daemen, Rijmen	België
SAFER+	Cylink Corp	USA
SERPENT	Anderson, Biham, Knudsen	Internationaal
TWOFISH	Schneier, Kelsey	USA

finalisten – tot winnaar uitgeroepen RIJNDAEL 2-10-2000 → AES

Rijndael

- Heeft SQUARE geheimschrift als voorloper
- Geen Feistel-schema maar algebra als basis
- Keuze blok/sleutel uit 128/192/256 bits
- Whitening stap voorafgaand aan vercijfering
- Afhankelijk sleutellengte 10/12/14 ronden met
  - ByteSub
  - ShiftRow
  - MixColumn
  - AddRoundKey
- Snelle vercijfering smartcards met weinig geheugen
- Cryptoanalyse nog niet gelukt t/m 2015

Rijndael schema

AddRoundKey – Whitening		
stap	startronden	slotronde
1	ByteSub	ByteSub
2	ShiftRow	ShiftRow
3	MixColumn	AddRoundKey
4	AddRoundKey	

- ByteSub = S-doos substitutie
- ShiftRow en MixColumn = lineaire menglaag
- AddRoundKey = exclusive-or met veranderende subsleutels

Basisoperaties

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

ByteSub

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

ShiftRow

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

MixColumn

Byte Substitutie

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

ByteSub

byte $B = abcdefgh$ *in* $GF(2^8)$

$$ax^7 + bx^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \quad \{0, 1\}$$

$$B_1 + B_2 = (a_1 + a_2 \bmod 2)\,x^7 + (b_1 + b_2 \bmod 2)\,x^6 \cdots$$

$$B_1 \times B_2 = (a_1 x^7 + \cdots)(a_2 x^7 + \cdots) \bmod (x^8 + x^4 + x^3 + x + 1)$$

ByteSub is in twee stappen opgebouwd:

(1) inverse $B \rightarrow B^{-1}$

(2) lineaire transformatie $M \cdot B + C$

In de praktijk wordt een tabel gehanteerd: $S[B = 0 \cdots 255]$

ShiftRow

b_0	b_4	b_8	b_{12}
b_5	b_9	b_{13}	b_1
b_{10}	b_{14}	b_2	b_6
b_{15}	b_3	b_7	b_{11}

MixColumn

kolommen zijn vectoren (b_0, b_1, b_2, b_3) *etc.*

schrijf kolomvector als polynoom $(b_0x^3 + b_1x^2 + b_2x + b_3)$

mixing is vermenigvuldig met $f = (3x^3 + x^2 + x + 2) \pmod{x^4 + 1}$

praktisch door vermenigvuldigen met een *circulant* matrix:

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

inverse met $f^{-1} = (11x^3 + 13x^2 + 9x + 14) \pmod{x^4 + 1}$

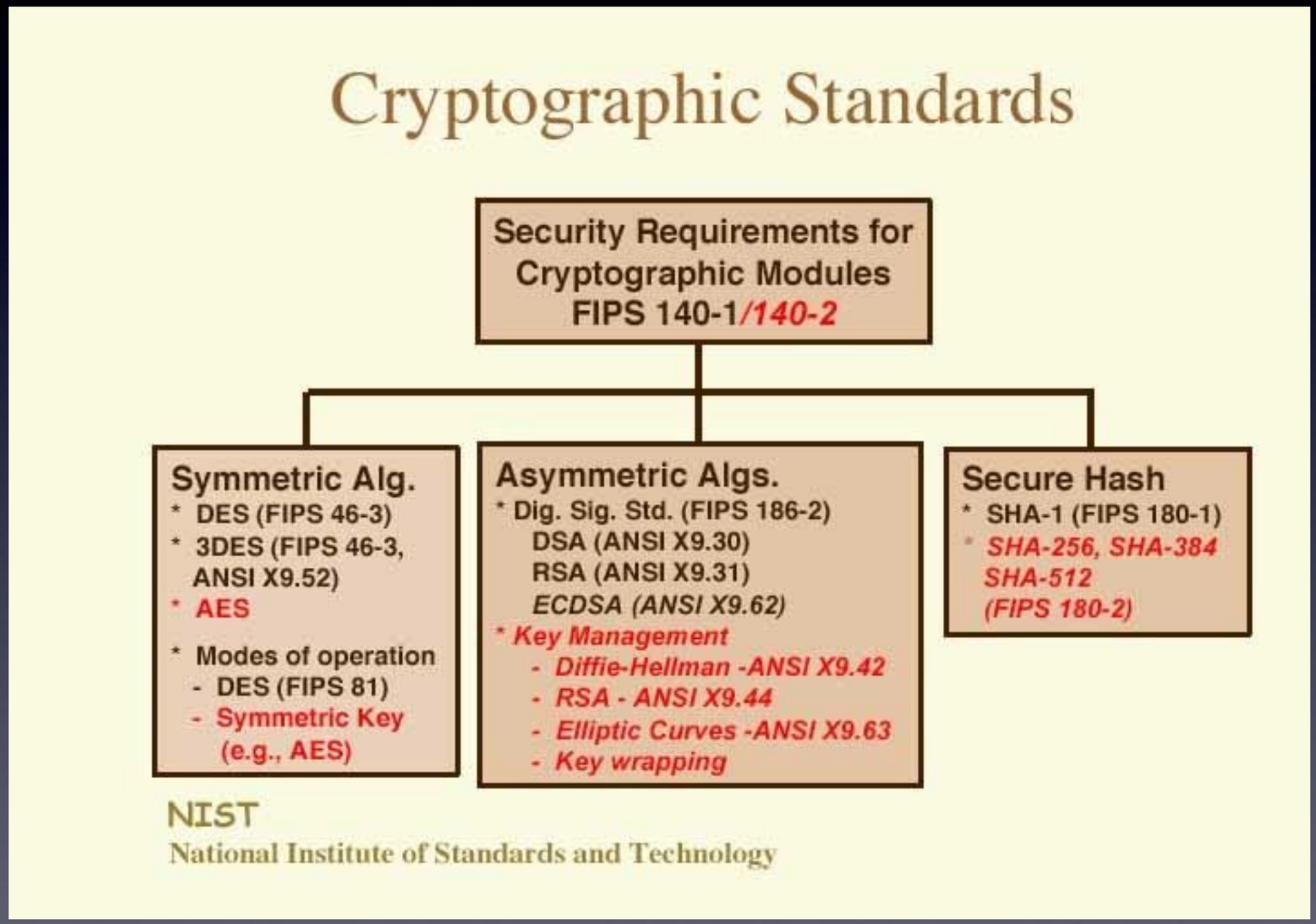
MixColumn

b_0	b_4	b_8	b_{12}
b_5	b_9	b_{13}	b_1
b_{10}	b_{14}	b_2	b_6
b_{15}	b_3	b_7	b_{11}

AddRoundKey

- 128 bits block/key + whitening → 1408 subsleutelbytes nodig
- kettingberekening maakt "on the fly" generatie mogelijk
- rekenschema $W_i = W_{i-1} \oplus W_{vorige\ ronde}$
- elke ronde aanvullende rotatie plus ByteSub substitutie en combinatie met de rondeteller
- extra bewerkingen by 256 bit sleutel

Standaarden



Lichtgewicht cryptografie

NIST sedert 2013

NISTIR 8114: Draft Report on Lightweight Cryptography
workshops in 2015, 2016

cryptosystemen voor:

- RFID tags
- embedded systemen

Bijvoorbeeld:

- DES met 1 i.p.v. 8 S-dozen
- TEA = Tiny Encryption Algorithm

`www.nist.gov/programs-projects/lightweight-cryptography`