G r u n d s ä t z e
für die Entwicklung einer neuen Chiffrieralgorithmenklasse

1. Es sind Algorithmen bzw. Algorithmenklasse für Staatsgeheimnisse (Geheimhaltungsstufe Geheim) zu entwickeln.

2. Ein breites Einsatzspektrum ist anzustreben. Damit sin die Algorithmen der Klasse so zu gestalten, daß sich für eventuelle Dekryptierangriffe praktisch verwertbare Informationen nicht auf Bereiche auswirken können, in denen andere Algorithmen der Klasse eingesetzt sind (Einbau vom LZS)

3. Zu entwickeln ist ein 64-Bit Blockchiffrieralgorithmus gemäß ISO 8372. Damit sind Schnittstellen und Betriebsarten vom Grundsatz her definiert.

4. Für die Entwicklung des Blockchiffrieralgorithmus sind die bewährten Forderungen für solche Algorithmen, (vgl. DES Konstruktionsprinzip) wie Confusion, Diffusion, Ähnlichkeit von Chiffrierung und Dechiffrierung einzuhalten.

5. Die perfekte Sicherheit im Sinne von Shannon muß nach einer gewissen Mindestanzahl von Runden erreicht werden, wenn ein on linie Schlüssel zur Anwendung kommt.

6. Der Algorithmus muß sowohl für Softwarerealisierung in Universalrechnern als auch für Spezialgeräte (Hardware, Software und Kombinationen) günstig realisierbar sein.

7. Bzgl. Speicherplatz und Zeitverhalten müssen ähnliche Werte erreicht werden wie mit dem FEAL Algorithmus oder dem von Massey zu EUROCRYPT 90 vorgeschlagenen Algorithmus.

Es gelingt nicht klare Geschwindigkeitsanforderungen zu formulieren da diese immer von der Hardware abhängig sind.

gewisse Schallgrenzen liegen bei

9,6 Kb/s
19,2 Kb/s
48,0 Kb/s
64,0 Kb/s (ISDN Kanal)

Quellen

- ISO 8372 First edition 1987 - 08 - 15
  Information processing - Modes of operations for a 64-bit block cipher algorithmus

- Kongressmaterial EUROCRYPT 90

- Fumy, Rieß Kryptographie, R. Oldenbourg Verlag 1988

LAMBDA 64bit Blockchiffrierung

BESCHREIBUNG LAMBDA1 vom 04.04.1990

1. Einleitung

Der hier beschriebene Algorithmus LAMBDA1 kann in den standardisierten Arbeitsmoden für 64 - Bit -Blockchiffrieralgorithmen gemäß ISO 8372 angewandt werden.
Mit der LAMBDA1 Beschreibung erfolgen zugleich verbindliche Vorgaben für weitere Darstellungsvarianten des Algorithmus.

LAMBDA1 wurde aus dem DATA Encryption Standard DES abgeleitet. Folgende Änderungen wurden vorgenommen:
- Vergrößerung der effektiven Schlüssellänge von 56 Bit auf 256 Bit;
- Änderung der Art und Weise der Schlüsselfolgenerzeugung;
- Addition zweier Schlüsselvektoren nach 8 Verarbeitungszyklen;
- Änderung der Anfangspermutation IP.

Zur Anpassung an vorgesehene Realisierungen wurden gegenüber der DES-Beschreibung eine leicht modifizierte Darstellung gewählt.

2. DEFINITIONEN

2.1. Bezeichnungen

Es sei $V_m =: \{0,1\}^m$, $m \in N$, die Menge aller m-Tupel von Elementen aus $\{0,1\}$. Die Komponentenschreibweise für $X \in V_m$:
$(X(1), X(2), \ldots, X(m))$.

Operationen über V_m:

$\bigoplus: V_m \times V_m \to V_m \quad \forall (X, Y, Z) \in V^3_m:$

$$X \bigoplus Y = Z \Leftrightarrow \forall\, j \in 1,m: X(j)+Y(j) \equiv Z(j) \pmod 2.$$

$: V_m \times V_m \to V_m \quad \forall (X, Y, Z) \in V^3_m:$

$$X \; Y = Z \Leftrightarrow X(1)\bullet 2^{m-1}+X(2)\bullet 2^{m-2}+ \ldots +X(m)\bullet 2^0+ Y(1)\bullet 2^{m-1}+Y(2)\bullet 2^{m-2}+ \ldots +Y(m)\bullet 2^0 \equiv \equiv Z(1)\bullet 2^{m-1}+Z(2)\bullet 2^{m-2}+ \ldots +Z(m)\bullet 2^0 \pmod{2^m}.$$

$: V_m \times V_m \to V_m \quad \forall (X, Y, Z) \in V^3_m:$

$$X \; Y = Z \quad X = Z \quad Y.$$

Es gilt: $\forall (X,Y) \in V^2_m:$

$$X \; Y = X \quad (0,0,\ldots,0,1) \quad (Y \bigoplus (1,1,\ldots,1)). \quad (*)$$

(Im folgenden wird das jeweilige m aus dem Kontext ableitbar sein.)

Abbildungen:

$E: V_{32} \to V_{48} \quad \forall\, X \in V_{32}:$

$E(X(1),X(2),\ldots X(32)) =: (X(32),X(1),X(2),X(3),X(4),X(5),X(4),$
$X(5),X(6),X(7),X(8),X(9),X(8),X(9),X(10),X(11),X(12),X(13),$
$X(12),X(13),X(14),X(15),X(16),X(17),X(16),X(17),X(18),X(19),$
$X(20),X(21),X(20),X(21),X(22),X(23),X(24),X(25),X(24),X(25),$
$X(26),X(27),X(28),X(29),X(28),X(29),X(30),X(31),X(32),X(1)).$

$T: V_{48} \to V_{48} \quad \forall\, X \in V_{48}:$

$T(X(1),X(2),\ldots,X(48)) =: (X(48),X(1),X(2),\ldots,X(47)).$

$S=S(S_1,S_2,\ldots,S_8): V_{48} \to V_{32}$ wobei $\forall\, j \in 1,8: S_j: V_6 \to V_4.$

Für beliebige X= X(1),X(2),...,X(6)) ∈ V_6,
Y= (Y(1),Y(2),Y(3),Y(4)) ∈ V_4 und J ∈ 1,8

gilt $S_j(X)$ = Y genau dann, wenn in der j-ten Tabelle in der Ziele Nr. X(1)2 + X(6) + 1 und in der Spalte Nr.

X(2)8 + X(3)4 + X(4)2 + X(5) + 1 der Wert
Y(1)8 + Y(2)4 + Y(3)2 + Y(4) steht:

S_1

14	1	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	3	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	1	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

2.2. Abbildung G

G: V_{32} x V_{48} → V_{32} ist für eine gegebene Permutation
P: 1,32→1,32 folgendermaßen definiert:

∀ (X,Z) ∈ V^2_{32} ∀ Y ∈ V_{48}: G(X,Y) = Z genau dann, wenn
Z = S(Y⊕E(X(P(1)),X(P(2));...,X(P(32)))).

Vorläufige Variante für P:

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
P(j)	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10

j	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
P(j)	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Bemerkung: Die Abbildung G unterscheidet sich in ihrer Wirkungsweise von der Abbildung f der DES-Beschreibung.
(Anwendung von P an anderer Stelle).

2.3. Schlüssel

B = (B(1),B(2),...,B(256)) ∈ V_{256} sei der verwendete Schlüssel.
Daraus werden die folgenden Vektoren gebildet:

K_1=: (B(1),B(2),...,B(48)) ∈ V_{48}
K_2=: (B(49),B(50),...,B(96)) ∈ V_{48}
K_3=: (B(97),B(98),...,B(144)) ∈ V_{48}
K_4=: (B(145),B(146),...,B(192)) ∈ V_{48}
∀ j ∈ 5,12: K_j =: $T^{11}(K_{j-4})$
∀ j ∈ 13,16: K_j =: $T^{11}(K_{25-j})$
K_{17}=: (B(193),B(194),...,B(224)) ∈ V_{32}
K_{18}=: (B(225),B(226),...,B(256)) ∈ V_{32}.

2.4. Die Folge (L_j,R_j), j=0,1,2,...,16

Für gegebene (L_0,R_0) ∈ V^2_{32} wird definiert:
∀ j ∈ 1,16: L_j ∈ $V_{32} \wedge R_j \in V_{32}$

$$\forall j \in 1,16: \begin{cases} (L_j,R_j) =: (R_{j-1},L_{j-1} \oplus G(R_{j-1},K_j)) & j \in \{8,16\} \\ (L_8,R_8) =: (R_7 \quad K_{17},(L_7 \oplus G(R_7,K_8)) \quad K_{18}) \\ (L_{16},R_{16}) =: (L_{15} \oplus G(R_{15},K_{16}),R_{15}). \end{cases}$$

2.5. Die Gesamtabbildung und deren Umkehrung

Es sei A = A(1),A(2),...,A(64)) ∈ V_{64} ein umzuformender 64-Bit-Block. Im Ergebnis der Gesamtabbildung entsteht daraus der 64-Bit-Block C = (C(1),C(2),...,C(64)) ∈ V_{64}.
Es sei (L_0,R_0) =: A.
Bilden $(L_j,R_j$ für J=1,2,...,16 gemäß 2.4.
Dann ist C = (L_{16},R_{16}).
Umkehrung: Es sei C = (C(1),C(2),...,C(64)) ∈ V_{64} gegeben.
Bilden (L'_0,R'_0) =: C und
∀ j ∈ 1,16: K'_j =: K_{17-j}
K'_{17}=: (0,0,...,0) $K_{18}=^{(*)}(0,0,...,0,1)$ $(K_{18} \oplus (1,1,...,1))$
K'_{18}=: (0,0,...,0) $K_{17}=^{(*)}(0,0,...,0,1)$ $(K_{17} \oplus (1,1,...,1))$.

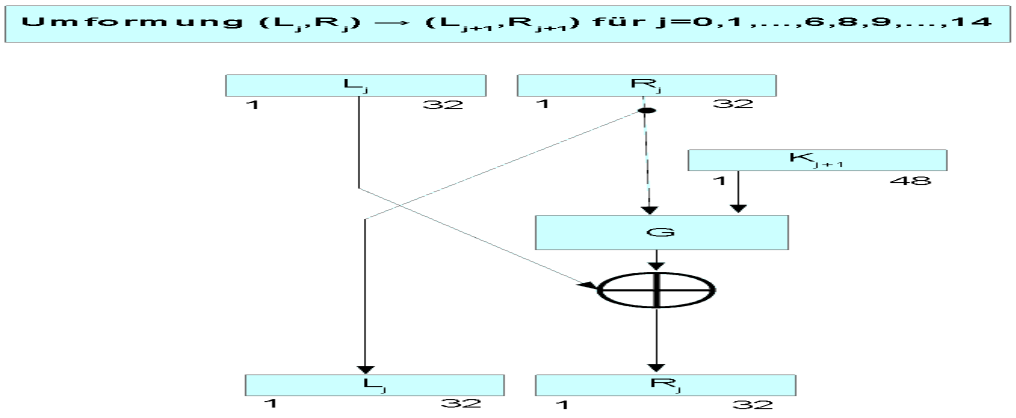
Berechnen analog zu 2.4.:

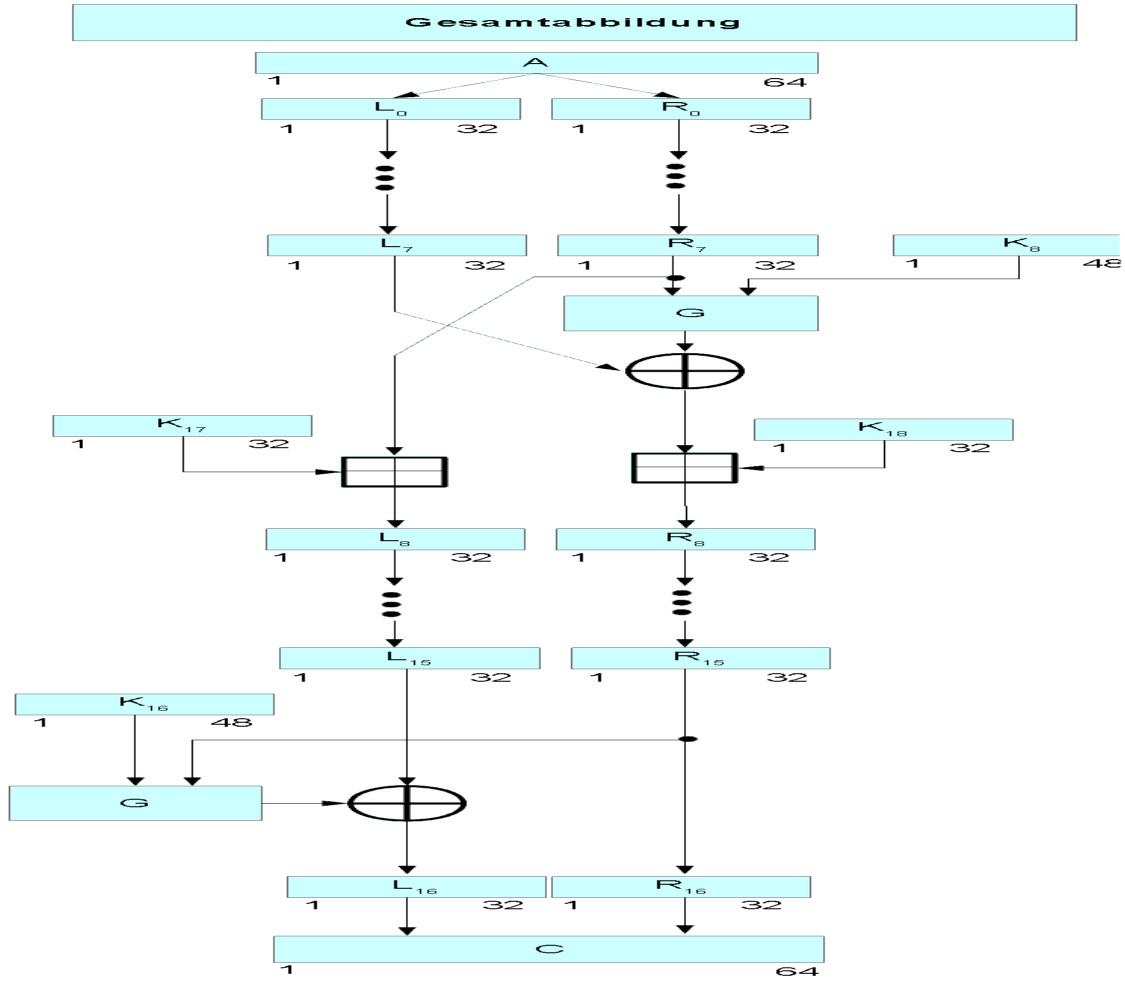
$$\forall j \in 1,16: \begin{cases} (L'_j,R'_j) =: (R'_{j-1},L'_{j-1} \oplus G(R'_{j-1},K'_j)) & j \in \{8,16\} \\ (L'_8,R'_8) =: (R'_7 \quad K'_{17},(L'_7 \oplus G(R'_7,K'_8)) & K'_{18}) \\ (L'_{16},R'_{16}) =: (L'_{15} \oplus G(R'_{15},K'_{16}),R'_{15}). \end{cases}$$

Dann erhalten wir A = (L'_{16},R'_{16}).

3. Skizzen

Die Skizzen sind kein Bestandteil der Definition.
Sie sollen lediglich den Ablauf der Umformungen veranschaulichen


Umformung $(L_j,R_j) \rightarrow (L_{j+1},R_{j+1})$ für j=0,1,...,6,8,9,...,14
L_j
1
32
R_j
1
32
K_{j+1}
1
48
G
L_j
1
32
R_j
1
32


Gesamtabbildung
A
1
64
L_0
1
32
R_0
1
32
L_7
1
32
R_7
1
32
K_8
1
48
G
K_{17}
1
32
K_{18}
1
32
L_8
1
32
R_8
1
32
L_{15}
1
32
R_{15}
1
32
K_{16}
1
48
G
L_{16}
1
32
R_{16}
1
32
C
1
64

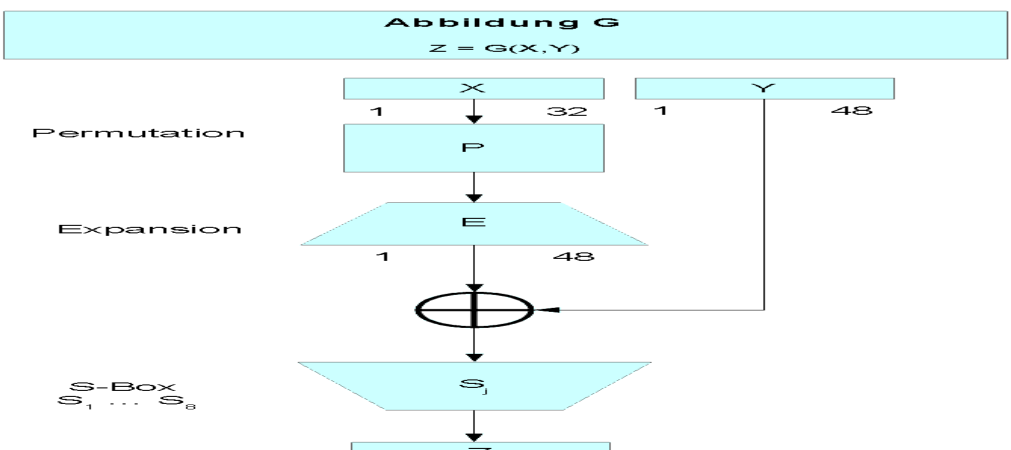


Abbildung G
Z = G(X,Y)
X
1
32
Y
1
48
Permutation
P
Expansion
E
1
48
S-Box
$S_1 \cdots S_8$
S_j

I. Verallgemeinerung der DES-like function für LAMBDA1

I.1. Allgemeine Bezeichnungen und Definitionen

a) V_n - Vektorraum der Dimension n über GF(2)

b) S_x - Gruppe aller Permutationen über eine Menge X

c) A_x - Gruppe aller geraden Permutationen über eine Menge X (alternierende Gruppe)

d) k-Funktion auf V_n

Sei $\{i_j\}_{j=1}^{k+1} \subseteq 1,n$, $f: V_k \to V_l$

Eine Funktion ς folgender Gestalt

$(a_1,...,a_{ik+1},..,a_n)\ \varsigma =$
$= (a_1,...,a_{ik+1} \oplus f(aa_1,...,a_{ik}),...,a_n)$

heißt k-Funktion.

Bemerkung: $\varsigma^2 = I$ (I-Identität).

e) $G_{k,n}$: Mit $G_{k,n}$ bezeichnet wir die Gruppe von Abbildungen, die durch die Menge der k-Funktion erzeugt wird.

f) DES-like functions:
Sie $f : V_n \to V_n$, $(X,Y) \in V^2_n$
Eine Funktion δ_f folgender Gestalt

$(X,Y)\delta_f = (Y, X \oplus f(Y))$

heißt DES-like function.
Bemerkung: δ_f kann auch wie folgt dargestellt werden: $\delta_f = \varsigma_f \bullet \Theta$, wobei

$(X,Y)\Theta = (Y,X)$,
$(X,Y)\varsigma_f = (X \oplus f(Y), Y)$.

Es gilt: $\Theta^2 = I$, $\varsigma^2_f = I$.

g) DES_{2n}: Mit DES_{2n} bezeichnen wir die Gruppe von Abbildungen, die durch die Menge der DES-like functions erzeugt wird.

h) 2-restricted DES-like function
Sei $z \in V_n$. Seien i,j_1,j_2 drei paarweise verschiedene natürlich Zahlen aus 1,n. Sie $g : V_2 \to V_1$.
Sie $f : V_n \to V_n$ eine Funktion folgender Gestalt

$f(z) = (0,...,0,g(z_{j1,j2}),0,...,0)$.
$\quad\quad\quad

Dann heißt δ 2-restricted DES-like function.

i) Abbildung $\varsigma_{i,j}^{ex}$:

Sei die Permutation $\varsigma_{i,j}^{ex} : V_{2n} \rightarrow V_{2n}$
wie folgt definiert:

$(a_1,...,a_j, ..., a_{2n}\ \varsigma_{i,j}^{ex} = (a_1,...,a_j,...,a_i,...,a_{2n}),$
wobei $(i,j) \in 1,2n$.
(Vertauschung der Bit i und j).

I.2. Resultate von EVEN, GOLDREICH für den DES

Lemma 1: $\forall_n > 1$: Θ ist eine gerade Permutation.

Lemma 2: $\forall_n > 1$, $\forall f: V_n \rightarrow V_n$:
ς_f ist nie eine gerade Permutation.

Beweis: siehe Artikel von EVEN, GOLDREICH.

Folgerung 1: $\forall_n > 1$, $\forall f: V_n \rightarrow V_n$:
δ_f ist eine gerade Permutation.

Folgerung 2: $DES_{2n} \subset A_{V_{2n}}$ (I)

Lemma 3: $\forall\ i \in 1,n$; $\forall\ j \in n+1,2n$:
$\varsigma_{i,h}^{ex}$ kann als eine Folge von 2 restricted DES-like functions dargestellt werden.

Lemma 4: $\forall$ >1: Jede 2-Funktion auf V_{2n} kann als eine Folge von 2-restricted DES-like functions dargestellt werden.

Beweis: siehe Artikel.

Forderung 3: $\forall_n 1$: Die Gruppe der Permutationen, die durch die 2-restricted DES-like functions erzeugt wird, fällt mit $G_{2,2n}$ zusammen.
Da die Menge der 2-restricted DES-like functions eine Untermenge der DES-like functions ist, folgt

Forderung 4: $G_{2,2n} \subset DES_{2n}$ (II)

Satz 1: (COPPERSMITH, GROSSMAN)
$\forall_n \geq 4$, $2 \leq k \leq n-2$: $G_{k,n} = A_{Vn}$. (III)

Beweis: siehe Artikel von COPPERSMITH, GROSSMAN
Aus (I), (II) und (III) folgt das gesuchte Resultat.

Satz 2: $\forall_n > 1$: $DES_{2n} = A_{V_{2n}}$

I.3. Resultate für LAMBDA1

I.3.1. Bezeichnungen/Definitionen

a) $h_{c_1c_2}$-Funktion
Sie $\forall(x,y,c_1,c_2) \in V^4{}_n$ die Funktion
h_{c_1,c_2} wie folgt definiert:

$(x,y)h_{c_1c_2} = (x\ c_1, y\ c_2)$.

b) LAMBDA-like functions
Sei δ_f eine DES-like function.
Sie $(c_1,c_2) \in V^2{}_n$.
Mit LAMBDA-like functions bezeichnen wir die Funktionen

$\gamma^f{}_{c_1,c_2} = \delta_f \circ h_{c_1,c_2}$, d. h.
$(x,y)\gamma^f{}_{c_1,c_2} = (y\ c_1(x \oplus f(y))\ c_2)$.

c) $LAMBDA_{2n}$:
Mit $LAMBDA_{2n}$ bezeichnen wir die Gruppe von Abbildungen, die durch die Menge der LAMBDA-like functions erzeugt wird.

I.3.2. Resultate

Lemma 5: $\forall(c_1,c_2)\in V^2{}_n$, $\forall_n>1$:
h_{c_1,c_2} ist eine gerade Permutation.

Beweis:
Wir stellen h_{c_1,c_2} als Hinteranderausfüllung vor vier Permutationen dar:

$h_{c_1,c_2} = h_{c_1} \circ \Theta \circ h_{c_2} \circ \Theta$, wobei
$(x,y)h_{c_1} = (x\ c_1, y)$.

Nach Lemma 1 ist Θ für alle $n>1$ eine gerade Permutation.
Die Abbildung h_{c_1} ist aber ebenfalls eine gerade Permutation (siehe Anhang, Lemma I für

$f(x) = x\ h_{c_1,c_2} = \text{const}$)

Folgerung 5: $\forall f: V_n \rightarrow V_n$, $\forall(c_1,c_2)\in V^2{}_n$:
$\gamma^f{}_{c_1,c_2}$ ist eine gerade Permutation.

Folgerung 6: $LAMBDA_{2n} \subset A_{V_{2n}}$. (IV)

Andererseits gilt: Die Menge aller DES-like functions ist eine Untermenge der Menge aller LAMBDA-like functions.
Für $c_1,c_2 \equiv 0$ fallen beide Mengen zusammen.

Folglich: $DES_{2n} \subset LAMBDA_{2n}$. (V)

Vermittels Satz 2, (IC) und (V) erhalten wir das Hauptresultat

Satz 3: $\forall_n>1$: $LAMBDA_{2n} = A_{V_{2n}}$

IV. Untersuchungen zu schwachen und Semischwachen Schlüsseln für LAMBDA1

IV.1. Allgemeine Bezeichnungen

Sei $B=: (B(1),...,B(256)) \in V_{256}$ der verwendete Schlüssel.
Daraus werden folgende Vektoren (Rundenschlüssel) gebildet:

$K_1=: (B(1),...B(48)) \in V_{48}$,
$K_2=: (B(49),...B(96)) \in V_{48}$,
$K_3=: (B(97),...B(144)) \in V_{48}$,
$K_4=: (B(145),...B(192)) \in V_{48}$,
$\forall j \in 5,12: K_j=: T^{11}(K_{j-4})$,
$\forall j \in 13,16: K_j=: T^{11}(K_{25-j})$,
$K_{17}=: (B(193),...B(224)) \in V_{32}$,
$K_{18}=: (B(225),...B(256)) \in V_{32}$.

Mit E(B,X) bezeichnen wir die Chiffrierabbildung LAMBDA1
mit den Schlüssel B für den Klartextvektor $X \in V_{64}$.
Analog sei D(B,X) die entsprechende Dechiffrierabbildung.

Laut def. soll X = D(B,E(B,X)) gelten (1)
Für gegebene $(L_0, R_0) \in V^2_{32}$ wird die
Chiffrierabbildung $E(B,(L_0,R_0)$ wie folgt definiert:

$(L_{16},R_{16}) =: E(B,(L_0,R_0))$,
$\forall_j \in 1,16: (L_j,R_j) \in V^2_{32}$,

$$\forall_j \in 1,16: \begin{cases} (L_j,R_j) =: (R_{j-1},L_{j-1} \oplus G(R_{j-1},K_j)), j \in \{8,16\}, \\ (L_8,R_8) =: (R_7 \quad K_{17},(L_7 \oplus G(R_7,K_8)) \quad K_{18}), \\ (L_{16},R_{16}) =: (L_{15} \oplus G(R_{15},K_{16}),R_{15}). \end{cases}$$

Für gegebene $(L'_0,R'_0) \in V^2_{32}$ wird die Dechiffrierabbildung

D(B,(L'_0,R'_0)) wie folgt definiert:
$(L'_{16},R'_{16}) =: D(B,(L'_0,R'_0))$,

$$\forall_j \in 1,16: \begin{cases} (L'_j,R'_j) =: (R'_{j-1},L'_{j-1} \oplus G(R'_{j-1},K'_j)), j \in \{8,16\}, \\ (L'_8,R'_8) =: (R'_7 \quad K'_{17},(L'_7 \oplus G(R'_7,K'_8)) \quad K'_{18}), \\ (L'_{16},R'_{16}) =: (L'_{15} \oplus G(R'_{15},K'_{16}),R'_{15}). \end{cases}$$

Dabei sei $\forall_j 1,16: K'_j = K_{17-j}$,
$K'_{17} = O \quad K_{18}$,
$K'_{18} = O \quad K_{17}$.

G sei eine Abbildung: $G:V_{32} X\ V_{48} \rightarrow V_{32}$.

Setzen wir $(L'_0,R'_0) = (L_{16},R_{16})$, ist dann in der Tat(1) erfüllt.
Wir führen weiter noch folgende Bezeichnungen ein:

Sei $0_n(0,..,0) \in V_n$ der Nullvektor und
$1_n = (1,...,1) \in V_n$ der Einsvektor aus dem Vektorraum V_n.

IV.2. Schwache Schlüssel

Definition 1:

Ein Schlüssel B heißt schwacher Schlüssel, genau dann,
wenn $\forall X \in V_{64}$: D(B,X) = E(B,X).

Folgerung 1:
Für einen schwachen Schlüssel B gilt:

$\forall X \in V_{64}$: $E(B,E(B,X)) = X$.

Beweis:
Sei $X \in V_{64}$, beliebig, aber fixiert.

Sei $g = E(B,X)$, laut Definition: $X = D(B,g)$.

Wegen $D(B,X) = E(B,X)$, $\forall X \in V_{64}$,
folgt dann:

$\forall X \in V_{64}$: $X = D(B,g) = E(B,g) = E(B,E(B,X))$.

Satz 1:
Sei B derart, daß

$'\forall i \in 1,16$: $K_i = K_{17-i}$, und $K_{17}\ K_{18} := 0_{32}$.

Dann ist B ein schwacher Schlüssel.

Beweis: Offensichtlich $\forall i \in 1,16$: $K_i = K_{17-i} = K'_{17-i}$.
$\Rightarrow \forall i \in 1,16$: $K_i = K'_i$ und $K'=0_{32}\ K_{18}$, $K'_{18}=0_{32}\ K_{17}$.
Sei $(L_0,R_0) = (L'_0,R'_0) \in V^2_{32}$, beliebig.
Dann gilt laut Definition:

$(L_1,R_1) = (R_0,L_0 \oplus G(R_0,K_1)) = (R'_0,L'_0 \oplus G(R'_0,K'_1)) = (L'_1,R'_1)$
.
.
.
$(L_7,R_7) = (R_6,L_7 \oplus G(R_6,K_7)) = (R'_6,L'_6 \oplus G(R'_6,K'_7)) = (L'_7,R'_7)$
$(L_8,R_8) = (R_6\ K_{17},(L_7 \oplus G(R_7,K_8))\ K_{18}) = (R_7\ K_{18},(L_7 \oplus G(R_7,K_8))\ K_{17}) =$
$= (R'_7\ K'_{17},(L'_7 \oplus G(R'_7,K'_8))\ K'_{18}) = (L'_8,R'_8)$
.
.
.
$(L_{16},R_{16}) = (L_{15} \oplus G(R_{15}K_{16}),R_{15}) = (L'_{15} \oplus G(R'_{15},K'_{16}),R'_{15}) = (L'_{16},R'_{16})$.

Da $(L_0,R_0) \in V^2_{32}$ beliebig gewählt werden kann, folgt sofort
$\forall X \in V_{64}$: $D(B,X) = E(B,X)$ und damit die Behauptung des Satzes.

Definition 2: Alle schwachen Schlüssel $B \in V_{256}$, die den Bedingungen von Satz 1 genügen, nennen wir schwache Schlüssel mit palindromischer Struktur.

Satz 2: Es gibt genau 2^{34} schwache Schlüssel mit palindromischer Struktur

Beweis: Wir betrachten zunächst die Bedingung
$\forall i \in 1,16$: $K_i = K_{17-i}$.
Mit den Formeln für die Schlüsselgenerierung erhalten wir

$K_1 = K_{16} = T^{33}K_1$
$K_2 = K_{15} = T^{33}K_2$

$K_3 = K_{14} = T^{33}K_3$
$K_4 = K_{13} = T^{33}K_4$
$T^{11}K_1 = K_5 = K_{12} = T^{22}K_4$
$T^{11}K_2 = K_6 = K_{11} = T^{22}K_3$
$T^{11}K_3 = K_7 = K_{10} = T^{22}K_2$
$T^{11}K_4 = K_8 = K_9 = T^{22}K_1$
$T^{22}K_1 = K_9 = K_8 = T^{22}K_4$
$T^{22}K_2 = K_{10} = K_7 = T^{22}K_3$
$T^{22}K_3 = K_{11} = K_6 = T^{22}K_2$
$T^{22}K_4 = K_{12} = K_5 = T^{22}K_1$
$T^{33}K_4 = K_{13} = K_4$
$T^{33}K_3 = K_{14} = K_3$
$T^{33}K_2 = K_{15} = K_2$
$T^{33}K_1 = K_{16} = K_1$.

Wie man leicht sieht, sind die letzten acht Gleichungen identisch zu den ersten acht. Aus letzteren erhalten wir:

a) $K_1 = T^{33}K_1$ e) $T^{11}K_1 = T^{22}K_4$
b) $K_2 = T^{33}K_2$ f) $T^{11}K_2 = T^{22}K_3$
c) $K_3 = T^{33}K_3$ g) $T^{11}K_3 = T^{22}K_2$
d) $K_4 = T^{33}K_4$ h) $T^{11}K_4 = T^{22}K_1$.

Aus e) und h) folgt sofort: (Man beachte: $T^{48} = I$)

$$\left.\begin{array}{l} K_1 = T^{11}K_4 \\ K_1 = T^{-11}K_4 \end{array}\right\} K_4 = T^{22}K_4$$

Andererseits

$$\left.\begin{array}{l} K_4 = T^{-11}K_1 \\ K_4 = T^{11}K_1 \end{array}\right\} K_1 = T^{22}K_1.$$

Analoge Gleichungen erhält man vermittels f) und g) auch für K_2, K_3.
Unter Beachtung von a) - d) folgt daraus die notwendige Bedingung:

$\forall i \in 1,4: K_i = T^{22}K_i = T^{33}K_i$
$\Rightarrow \forall i \in 1,4: K_i = T^{11}K_i$
$\Rightarrow \forall i \in 1,4: K_i = 0_{48}$ oder
$K_i = 1_{48}$.

Unter Beachtung von e) - h) folgen dann genau vier Möglichkeiten für die Wahl von $K_1,\ldots,K_4$:

i / No.	K_1	K_2	K_3	K_4
1	0_{48}	0_{48}	0_{48}	0_{48}
2	0_{48}	1_{48}	1_{48}	0_{48}
3	1_{48}	0_{48}	0_{48}	1_{48}
4	1_{48}	1_{48}	1_{48}	1_{48}

Sei nun $K_{17} \in V_{32}$ beliebig, aber fest.
Aus der Bedingung $K_{17}\ K_{18} = 0$, folgt dann sofort der Wert für K_{18}.

Damit gibt es genau 2^{32} Möglichkeiten für die Wahl von
K_{17} und K_{18}.
Damit erhalten wir genau $4 \cdot 2^{32} = 2^{34}$ schwache
Schlüssel mit Palindromstruktur.

Frage: Gibt es auch schwache Schlüssel mit komplizierter Struktur?

IV.3. Semischwache Schlüssel

Definition 3: Ein Schlüssel B heißt semischwacher Schlüssel,
genau dann wenn

$\exists B^* \in V_{256}$, so daß
$\forall X \in V_{64}$: $D(B,X) = E(B^*,X)$.

Folgerung 2: Sei B ein semischwacher Schlüssel.
Dann gilt $\forall X \in V_{64}$:

1) $D(B^*,X) = E(B,X)$
   (d. h. B^* ist ebenfalls ein semischwacher Schlüssel.)
2) $X = E(B^*,E(B,X))$.

Beweis:

1) Es gilt $\forall X \in V_{64}$: $E(B^*,X) = D(B,X)$
$\Rightarrow \forall X \in V_{64}$ $X = D(B^*,E(B^*,X)) = D(B^*,D(B,X))$.
   Andererseits
$\Rightarrow \forall X \in V_{64}$ $X = E(B,D(B,X)) = E(B,E(B^*,X))$.
$\Rightarrow \forall X \in V_{64}$ $D(B^*,D(B,X)) = E(B,E(B^*,X))$.
  Sei $g = D(B,X) = E(B^*,X)$.

Aufgrund der Eineindeutigkeit der Chiffrenabbildungen
folgt dann:

$\forall g \in V_{64}$: $D(B^*,g) = E(B,g)$.

2) Sei $\forall X \in V_{64}$: $D(B^*,X) = E(B,X)$.
$\Rightarrow \forall X \in V_{64}$: $X = E(B^*,D(B^*,X)) = E(B^*,E(B,X))$.

Satz 3: Seien $(B,B^*) \in V^2{}_{64}$ derart, daß

$\forall i \in 1,16$: $K_i = K^*_{17-i}$
und $K_{17} = 0_{32}\ K^*_{18}$,
$K_{18} = 0_{32}\ K^*_{17}$,

Dann sind B und B* semischwache Schlüssel.

Beweis: Der Beweis verläuft analog dem Beweis von Satz 1.
Offensichtlich gilt $\forall i \in 1,16$:

$K_i = K'_{17-i} = K^*{}'_{17-i} = K^*{}'_i$,

und

$K_{17} = 0_{32}\ K^*_{18} = K^*{}'_{17}$,

$K_{18} = 0_{32}\ \ K^*_{17} = K^{*\prime}_{18}$.

Sei nun $(L_0,R_0) = (L^{*\prime}_0,R^{*\prime}_0) \in V^2_{32}$ beliebig.
Dann gilt laut Definition

$(L_1,R_1) = (R_0,L_0 \oplus G(R_0,K_1)) =$
$= (R^{*\prime}_0,L^{*\prime}_0 \oplus G(R^{*\prime}_0,K^{*\prime}_1)) = (L^{*\prime}_1,R^{*\prime}_1)$.
.
.
.
$(L_7,R_7) = (R_6,L_6 \oplus G(R_6,K_7)) =$
$= (R^{*\prime}_6,L^{*\prime}_6 \oplus G(R^{*\prime}_6,K^{*\prime}_7)) = (L^{*\prime}_7,R^{*\prime}_7)$.
$(L_8,R_8) = (R_7\ \ K_{17},(L_7,K_8))\ \ K_{18}) =$
$= (R^{*\prime}_7\ \ K^{*\prime}_{17},(L^{*\prime}_7 \oplus G(R^{*\prime}_7,K^{*\prime}_8))\ \ K^{*\prime}_{18})$
$= (L^{*\prime}_8,R^{*\prime}_8)$
.
.
.
$(L_{16},R_{16}) = (L_{15} \oplus G(R_{15},K_{15}),R_{15}) =$
$= (L^{*\prime}_{15} \oplus G(R^{*\prime}_{15},K^{*\prime}_{16})R^{*\prime}_{15}) = L^{*\prime}_{16},R^{*\prime}_{16})$.

Da $(L_0,R_0) \in V^2_{32}$ beliebig gewählt wurden kann,
folgt sofort $\forall X \in V_{64}$: $D(B^*,X) = E(B,X)$
und damit die Behauptung des Satzes.

Definition 4: Alle semischwachen Schlüssel $B \in V_{256}$,
die den Bedingungen von Satz 3 genügen, nennen wir semischwache
Schlüssel mit Palindromstruktur.

Satz 4: Es gibt genau 2^{68} semischwache Schlüssel
mit Palindromstruktur.

Beweis: Wir betrachten zunächst die Bedingung

$\forall\ i \in 1,16$: $K_i = K^*_{17-i}$.

Mittels der Formel für die Schlüsselgenerierung erhalten wir:

$K_1 = K^*_{16} = T^{3\,3}K^*_1$
$K_2 = K^*_{15} = T^{3\,3}K^*_2$
$K_3 = K^*_{14} = T^{3\,3}K^*_3$
$K_4 = K^*_{13} = T^{3\,3}K^*_4$
$T^{1\,1}K_1 = K_5 = K^*_{12} = T^{2\,2}K^*_4$
$T^{1\,1}K_2 = K_6 = K^*_{11} = T^{2\,2}K^*_3$
$T^{1\,1}K_3 = K_7 = K^*_{10} = T^{2\,2}K^*_2$
$T^{1\,1}K_4 = K_8 = K^*_9 = T^{2\,2}K^*_1$
$T^{2\,2}K_1 = K_9 = K^*_8 = T^{2\,2}K^*_4$
$T^{2\,2}K_2 = K_{10} = K^*_7 = T^{2\,2}K^*_3$
$T^{2\,2}K_3 = K_{11} = K^*_6 = T^{2\,2}K^*_2$
$T^{2\,2}K_4 = K_{12} = K^*_5 = T^{2\,2}K^*_1$
$T^{3\,3}K_4 = K_{13} = K^*_4$
$T^{3\,3}K_3 = K_{14} = K^*_3$
$T^{3\,3}K_2 = K_{15} = K^*_2$
$T^{3\,3}K_1 = K_{16} = K^*_1$.

Diese Gleichungen fassen wir wie folgt zusammen:

a) $K_1 = T^{33}K^*_1 \wedge T^{33}K_1 = K^*_1$,
b) $K_2 = T^{33}K^*_2 \wedge T^{33}K_2 = K^*_2$,
c) $K_3 = T^{33}K^*_3 \wedge T^{33}K_3 = K^*_3$,
d) $K_4 = T^{33}K^*_4 \wedge T^{33}K_4 = K^*_4$,
e) $T^{11}K_1 = T^{22}K^*_4 \wedge T^{22}K_1 = T^{11}K^*_4$,
f) $T^{11}K_2 = T^{22}K^*_3 \wedge T^{22}K_2 = T^{11}K^*_3$,
g) $T^{11}K_3 = T^{22}K^*_2 \wedge T^{22}K_3 = T^{11}K^*_2$,
h) $T^{11}K_4 = T^{22}K^*_1 \wedge T^{22}K_4 = T^{11}K^*_1$.

Vermittels a) und e) erhalten wir

$$\left.\begin{array}{l} K^*_1 = T^{-33}K_1 \\ K^*_1 = T^{33}K_1 \\ K^*_4 = T^{-11}K_1 \\ K^*_4 = T^{-11}K_1 \end{array}\right\} K_1 = T^{22}K_1 = T^{66}K_1$$

Unter Beachtung von $T^{66} = T^{18}$ erfolgt
$K_1 = T^{18}K_1 = T^{22}K_1$.

Auf analoge Art und Weise erhält man:

$\forall i \in 1,4$: $K_i = T^{18}K_i = T^{22}K_i$ (2)
und $K^*_i = T^{18}K^*_i = T^{22}K_i$.

Durch Vergleich der entsprechenden Schlüsselbits erhält man,
daß (2) nur genau für die vier Vektoren

$0_{48} = (0,...,0) \in V_{48}$,
$01_{48} = (0,1,0,1,...,0,1,0,1) \in V_{48}$
$10_{48} = (1,0,1,0,...,1,0,1,0) \in V_{48}$
$1_{48} = (1,...,1) \in V_{48}$

erfüllt ist, d. h.

$\forall i \in 1,4$: $K_i = 0_{48} \vee K_i = 10_{48} \vee K_i = 10_{48} \vee K_i = 1_{48}$,
$K^*_i = 0_{48} \vee K^*_i = 10_{48} \vee K^*_i = 10_{48} \vee K^*_i = 1_{48}$.

Aus a), d) und h) erhält man weiter

$K_1 = T^{33}K^*_1 = T^{22}K_4 = T^7K^*_4$.

Analog

$K_2 = T^{33}K^*_2 = T^{22}K_3 = T^7K^*_3$.

Daraus erhalten wir für die Wahl von K_1, K^*_1, K_4, K^*_4
lediglich folgende vier Möglichkeiten:

K_1	K^*_1	K_4	K^*_4
0_{48}	0_{48}	0_{48}	0_{48}
01_{48}	10_{48}	01_{48}	10_{48}
10_{48}	01_{48}	10_{48}	01_{48}
1_{48}	1_{48}	1_{48}	1_{48}

Eine analoge Tabelle erhält man für die Wahl von K_2, K^*_2, K_3, K^*_4.
Damit gibt es genau $16=2^4$ Möglichkeiten für die Wahl von

K_i, K^*_i, $i \in 1,4$.

Wählt am nun $(K_{17}\ K_{18}) \in V^2_{32}$ beliebig,
aber fest, dann erhält man vermittels

$K^*_{18} = 0_{32} \ K_{17}$ und $K^*_{17} = 0_{32} \ K_{18}$

sofort die Werte für K^*_{17} und K^*_{18}.

Damit gibt es also genau $2^2 \cdot 2^{32} \cdot 2^{32} \cdot = 2^{68}$
verschiedene Möglichkeiten für semischwache Schlüssel mit Palindromstruktur.

Frage: Gibt es auch semischwache Schlüssel komplizierter Struktur?

Abteilung 2 Berlin, 22, Juni 1990
Referat 21

Sachbestandsbericht LAMBDA1

1. Gegentand des Berichtes

Anfang März 1990 ergab sich die dringende Notwendigkeit, umgehend einen neuen Chiffrieralgorithmus hoher Sicherheit bereitzustellen. Die Übergabe des Algorithmus für die technische Realisierung erfolgte bereits am 12. 3. 1990 /3/. Um das Einsatzrisiko möglichst gering zu halten, eine gründliche und umfassende Analyse war nicht möglich, erfolgte der Rückgriff auf bewährte Grundstrukturen (Feistelchiffren).

Eine modifizierte Version des amerikanischen Data Encryption Standard DES /1/ erschien aus verschiedenen Gründen für den vorgesehenen Einsatz in den Geräten T316 und T325 geeignet. Die vorgenommenen Modifizierungen erfolgte mit dem Ziel, die aus der offenen Literatur und durch eigene Untersuchungen bekannten bzw. vermuteten Schwachstellen des DES zu vermeiden. Der Bericht beinhaltet die wesentlichsten, seit März, erzielten Analyseergebnisse zu der mit LAMBDA1 bezeichneten modifizierten DES-Version.

2. Der LAMBDA1 Algorithmus

LAMBDA1 kann in standardisierten Arbeitsmodi für 64-Bit Blockchiffrieralgorithmen gemäß ISO 8372 /2/ eingesetzt werden. Die exakte Beschreibung des Algorithmus findet man in /3/. Im Vergleich zum DES wird
- die effektive Schlüssellänge von 56 auf 256 Bit vergrößert,
- der als Schwäche bzw. als trapdoor vermutete Zusammenhang zwischen S-Boxen und Schlüsselfolgeerzeugung ist aufgehoben,
- nach 8 Verarbeitungszyklen (Runden) wird ein Schlüsselvektor mit einer Länge von 64 Bit im Algorithmus verarbeitet, um analytische Zusammenhänge entscheidend zu verändern,
- die Anfangs- und Endpermutationen IP bzw. IP^{-1} wurden im Interesse einer effektiven Implementierung geändert.

3. Methodik der Untersuchungen

Die im nachhinein durchzuführende kryptologische Analyse verläuft

in 2 Phasen:
In der ersten Phase erfolgen auf der Basis der ausgewerteten Veröffentlichungen zur DES-Analyse, analoge Untersuchungen zu LAMBDA1 (ca. 70 Quellen).

Dazu wurde die vorhandene Literaturübersicht zur Analyse von Blockchiffren (insbesondere zum DES) vervollständigt und zielgerichtet ausgewertet.

Tiefergehende Arbeiten sind in der zweiten Phase als Paralleluntersuchungen zu den Analysearbeiten für die Algorithmen der DELTA-Klasse /4/ vorgesehen.

4. Eingesetzte Kräfte/Kapazitäten

Mitte März begann die kryptologische Analyse. An ihr sind 9 Diplommathematiker beteiligt. Wobei alle Mitarbeiter nur ca. 30 % ihrer Arbeitszeit für diese Arbeiten verwenden.

Für experimentelle Untersuchungen stehen ESER PC und ein AT zur Verfügung.

Diese Untersuchungen sind unter den gegebenen Bedingungen sehr aufwendig.

Für einen Versuch benötigt man auf dem ESER PC ca. 10 Stunden. Auf dem zur Verfügung stehenden AT, der unter heutigen Bedingungen als Einsteiger-Hardware einzustufen ist, werden pro Versuch nur ca. 2 Stunden benötigt.

Die Programme laufen hauptsächlich auf ESER PC. Die insgesamt bisher verbrauchte Rechenzeit beträgt ca. 400 Stunden. Die Nutzung der Rechner in einer Nachtschicht trägt zwar zur Entspannung der Situation bei, ist aber unter Berücksichtigung der oben aufgeführten Zeitrelationen unbefriedigend.

Mit durchaus handelsüblicher schneller 16-Bit Technik lägen die Zeiten bei etwa 10 - 15 Minuten. Somit erweist sich die Leistungsfähigkeit der zur Verfügung stehenden Rechner als ein entscheidender Engpaß, der sich generell hemmend für die Analyse (auch im Rahmen der DELTA-Analyse) auswirkt. Die rechentechnichen Kapazitäten der Abteilung 2 sind durch die Programmierarbeiten am Chiffrierverfahren KRAKE und die mathematisch-kryptologische Analyse überfordert.

5. Ergebnisse

5.1. In Anlehnung an die in /5/ untersuchten DES-like functions, ergaben Untersuchungen der Gruppe der LAMBDA1-like functions, daß auch hier die alternierende Gruppe vorliegt.
5.2. Alle schwachen und semischwachen Schlüssel mit Palindromcharakter /6/ wurden eindeutig bestimmt. In Relation zum Schlüsselumfang von $2^{2^{56}}$ ist ihr Auftreten jedoch um Größenordnungen geringer als beim DES.
5.3. Automorphismen
Es wurden Aussagen bewiesen, die die Anzahl und die Art der Automorphismen in einem grundlegenden Automatenmodell wesentlich einschränken. Damit sind mehrere Klassen

kryptologisch evtl. verwendbarer algebraischer Strukturen ausgeschlossen.

5.4. Zweifache Transitivität
Die zweifache Transitivität ist eine wesentliche algebraische Eigenschaft für Gruppen von Abbildungen, die in Blockchiffren verwendet werden. Die Überprüfung dieser Eigenschaft ist auch für die Analyse von LAMBDA1 von Interesse. Die theoretischen Grundlagen für eine rechnergestützte Prüfung wurden ausgearbeitet.

5.5. In der Literatur gibt es eine Reihe verschiedener statistischer Untersuchungen, mit denen versucht wird, unerwünschte Gesetzmäßigkeiten im Chiffrieralgorithmus zu entdecken. /7/
Geplant und zum Teil begonnen wurden Experimente zum Avalanche-Effekt und zum strikten Avalanch-Effekt und der Testung spezieller Bitabhängigkeiten. Aufgrund der geringen Leistungsfähigkeit der zur Verfügung stehenden Rechner, konnte bisher nur wenige Versuche durchgeführt werden, eine endgültige Wertung ist z. Zt. nicht möglich. Die bisherigen Versuche zeigen jedoch keine Auffälligkeiten.

6. Wertungen

Alle Aussagen/Wertungen sind durch die sehr kurze Zeit für die Analysearbeiten zu relativieren. In der Regel sind für solche komplizierten Arbeiten mindestens 2 Jahre vorzusehen. - Mit dem Einsatz ist nach wie vor ein gewisses Risiko verbunden. Daraus ergibt sich die Notwendigkeit, die Analyse weiterzuführen.

6.1. Es wurden bisher keine kryptologisch schlechten Eigenschaften gefunden.

6.2. Man kann davon ausgehen, daß praktisch nutzbare Schwachstellen, falls sie existieren, nur mit großem Aufwand auffindbar sind.

6.3. Mit den durchgeführten bzw. noch vorgesehenen Analysearbeiten wird das Niveau der in der offenen Literatur dargelegten Analyseergebnisse zum DES erreicht. Arbeiten zu Automorphismen und zur 2-fachen Transitivität gehen darüber hinaus.

6.4. Alle bisherigen Analyseergebnisse unterstützen die These, daß der LAMBDA1 Algorithmus nicht schlechter als der DES ist.

7. Schlußfolgerungen

7.1. In Übereinstimmung mit dem in /3/ enthaltenen Vorschlag gibt es aus heutiger Sicht keine Einwände für den bis I/91 begrenzten Einsatz von LAMBDA1 in Datenchiffriertechnik bis zum Geheimhaltungsgrad GVS.

7.2. Für das III. Quartal 1990 sind folgende Arbeiten geplant:
+ Prüfung, ob weitere Aussagen aus der offenen Literatur auf LAMBDA1 übertragbar sind.
+ die Weiterführung der begonnen Experimente zum Avalanche-Effekt.
+ Arbeiten zum Nachweis der 2-fachen Transitivität der Gruppe des Automaten und darauf aufbauend der Nachweis, daß die alternierende Gruppe erzeugt wird.
+ Suche nach möglichen Automorphismen.

7.3. Die Analyse ist langfristig parallel zur Entwicklung des neuen Blockchiffrieralgorithmus weiterzuführen. Ergebnisse

sind zum Termin I/91 in einem Dokument zusammenzufassen und zu werten.

7.4. Es ist durch die hierfür verantwortlichen Mitarbeiter der Verwaltung zu prüfen, ob für die vorgesehenen Experimente (auch und insbesondere zur Algorithmenklasse DELTA) leistungsfähigere Rechentechnik (z. B. AT mit 80386 Prozessor) zur Verfügung gestellt und die angespannte Situation bzgl. der rechentechnischen Kapazität in der Abteilung 2 entspannt werden kann.

In diesem Zusammenhang möchte ich auf unser Schreiben vom 08. 05. 1990, zu benötigter Hardware, hinweisen.

Quellen

/1/ Federal Inforamtion Processing Standard (FIPS) Publication No. 46, January 1977
Data Encryption Standard

/2/ International Stndard ISO 8372
1987 - 08 - 15
Information processing - Modes of operation for a 64-bit block cipher algorithm

/3/ Schreiben Leiter Abt. 2 vom 12. 3. 1990
Vorlage eines Datenchiffrieralgorithmus
(Anlage)

/4/ Vorläufige Beschreibung der Chiffrieralgorithmusklasse DELTA

/5/ Even S., Goldreich O.
DES-like function can generate the alternating group - IEEE Trans. Inf. Theory, 1983, Vol. IT-29, No. 6, pp. 863-865

/6/ Simmons G. J., Moore J. H.
Cycle Structure of the DES for keys having palindromic (or anti-palindromic) sequences of rounds keys. - IEEE Trans. Software Eng., 1987, Vol. SE-13, No. 2, pp. 262-273

/7/ A. K. Leung, S.E. Tavares
Sequence complexity as a test for cryptographic systems