

Ein neues iteratives Kryptosystem

Andreas Klein

1 Einführung

Iterative Kryptosysteme sind eine Klasse kryptographisch starker Funktionen, die aus kryptographisch schwachen Funktionen durch n-fache Iteration gewonnen werden. Jeder Iterationschritt wird eine Runde und das Kryptosystem ein n-Runden Kryptosystem genannt. Normalerweise werden die Schlüssel für die verschiedenen Runden aus einem Hauptschlüssel durch einen key-scheduling Algorithmus berechnet. Das bekannteste iterative Kryptosystem ist DES.

Die von Biham und Shamir entwickelte differentielle Kryptoanalyse [2] ist ein Angriff mit wählbaren Klartext gegen iterative Kryptosysteme. Differentielle Kryptoanalyse kann mit Erfolg auf eine große Klasse von Kryptosystemen angewandt werden, darunter sind DES [6, 5, 11], LOKI [4, 10] und Feal [3]. Zusammen mit der 1993 von Matsui vorgestellten linearen Kryptoanalyse [13], einem Angriff mit bekannten Klartext, bildet sie den besten bekannten Angriff gegen iterative Kryptosysteme.

In diesem Artikel wird ein neues iteratives Kryptosystem vorgestellt, das durch eine kleine Modifikation der E-Funktion gegen die gewöhnliche differentielle Kryptoanalyse immun ist. Andere Möglichkeiten um iterative Kryptosysteme gegen differentielle Kryptoanalyse zu schützen werden in [1, 8, 15] vorgestellt.

2 Das Kryptosystem

Verschlüsselung

Dieses Kryptosystem ist wie DES und die meisten anderen iterativen Kryptosysteme eine Feistel-Chiffre. Pro Durchgang werden 24 Bit verschlüsselt. Die 24 Bit werden in zwei Datenstränge zu je 12 Bit geteilt. Die beiden Datenstränge seien L_0 und R_0 . Die Ausgabe in Runde i wird berechnet als

$$R_i = L_{i-1} \text{ und } L_i = R_{i-1} \oplus F(R_i, K_i)$$

für $1 < i \leq 16$ und

$$R_1 = R_0 \text{ und } L_1 = L_0 \oplus F(R_1, K_1).$$

Das System hat 16 Runden die Ausgabe ist $L_{16}R_{16}$. Es werden unabhängige Teilschlüssel verwendet, d.h. das System verwendet 16 Schlüssel zu je 24 Bit insgesamt also

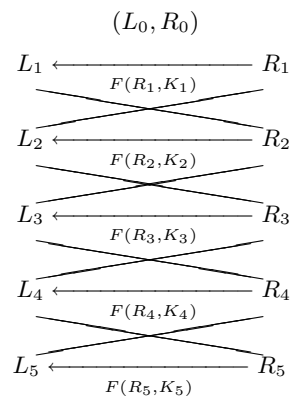


Abbildung 1: Ein fünf Runden System

2 Das Kryptosystem

einen 384 Bit Schlüssel. Die Abbildung 1 zeigt die schematische Darstellung eines fünf Runden Systems.

Entschlüsselung

Wie bei allen Feistel-Chiffren kann zum Entschlüsseln der gleiche Algorithmus wie zum Verschlüsseln verwendet werden. Doch diesmal ist der Schlüssel der ersten Runde K_{16} , der Schlüssel der zweiten Runde K_{15} usw. Der Schlüssel für die letzte Runde ist dann K_1 .

Die F-Funktion

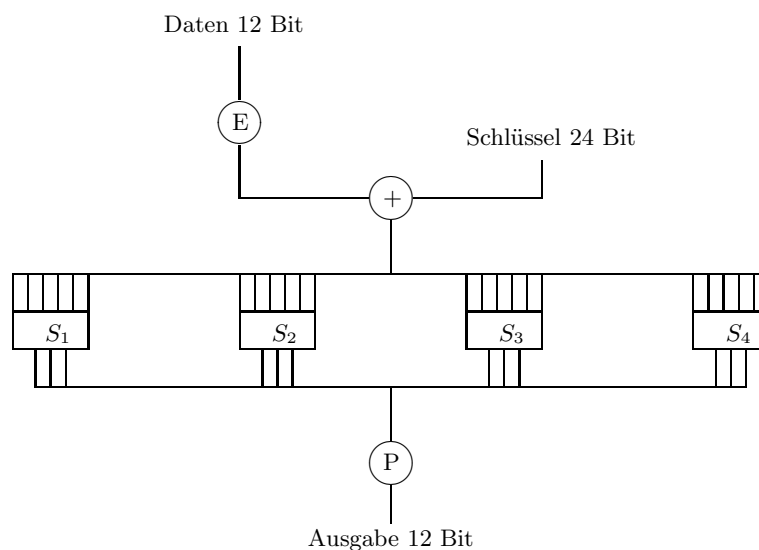


Abbildung 2: Die F-Funktion

Ein Überblick über die F-Funktion gibt Abbildung 2. Die Funktion E erhält eine 12 Bit Eingabe und liefert 24 Bit als Ausgabe. Dabei werden alle 12 Bit nach der folgenden Tafel verdoppelt:

| | | | | | |
|----|----|----|----|----|----|
| 1 | 2 | 3 | 1 | 2 | 3 |
| 4 | 5 | 6 | 4 | 5 | 6 |
| 7 | 8 | 9 | 7 | 8 | 9 |
| 10 | 11 | 12 | 10 | 11 | 12 |

Tabelle 1: Die E-Funktion

Danach wird $E(R) \oplus K$ berechnet. Dieses Ergebnis dient als Eingabe der S-Boxen. Jede der vier S-Boxen S_1, S_2, S_3 und S_4 bekommt als Eingabe einen 6-Bit Block und liefert als Ausgabe einen 4-Bit Block. Die Funktionsweise der S-Boxen wird hier am Beispiel von S_1 erklärt. Die Tafeln der anderen S-Boxen finden sich in A.1 auf Seite 13.

3 Differentielle Kryptoanalyse des Systems

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 7 | 1 | 5 | 2 | 6 | 0 | 3 |
| 0 | 4 | 2 | 6 | 1 | 5 | 3 | 7 |
| 3 | 6 | 0 | 2 | 5 | 1 | 7 | 4 |
| 2 | 0 | 6 | 4 | 3 | 7 | 5 | 1 |
| 1 | 5 | 7 | 0 | 4 | 3 | 6 | 2 |
| 7 | 2 | 4 | 3 | 6 | 0 | 1 | 5 |
| 6 | 3 | 5 | 1 | 7 | 4 | 2 | 0 |
| 5 | 1 | 3 | 7 | 0 | 2 | 4 | 6 |

Tabelle 2: S-Box 1

Die ersten 3 Bit der Eingabe von S_1 geben an in welcher Zeile der Tabelle die Ausgabe abgelesen werden muß. Die nächsten drei Bit bestimmen die Spalte. Ist die Eingabe zum Beispiel 101110_2 , so ist die 101_2 -te Zeile und 110_2 -te Spalte zu wählen, d.h. die Ausgabe ist 1.

Die Funktion P permutiert die 12 Ausgabebits der S-Boxen nach der in Tabelle 3 dargestellten Regel. P setzt also das 10. Bit an die erste Stelle, danach kommt das 8. usw.

| | | |
|----|----|----|
| 10 | 8 | 6 |
| 1 | 11 | 9 |
| 4 | 2 | 12 |
| 7 | 5 | 3 |

Tabelle 3: P Permutation

3 Differentielle Kryptoanalyse des Systems

In diesem Abschnitt betrachten wir Varianten des Systems mit weniger Runden und ihre differentielle Kryptoanalyse. Dabei werden die für dieses System spezifischen Schwierigkeiten deutlich. Dafür rufen wir uns zunächst die Grundprinzipien der differentiellen Kryptoanalyse ins Gedächtnis.

Definition 1 (XOR-Tabelle)

Eine S-Box hat $64 \cdot 64$ mögliche Eingabepaare. Jedes von ihnen hat einen Eingabe-XOR und einen Ausgabe-XOR. Eine Tabelle, die die Verteilung von Eingabe-XOR und Ausgabe-XOR zeigt, heißt XOR-Tabelle der S-Box. In dieser Tabelle entspricht jede Zeile einem bestimmten Eingabe-XOR und jede Spalte einem Ausgabe-XOR. Die Einträge geben an wieviel Paare mit diesem Eingabe-XOR und diesem Ausgabe-XOR existieren.

Die Funktion E stellt sicher, daß jede S-Box nur 8 verschiedene Eingabe-XOR-Werte erhalten kann, nämlich solche, bei denen der XOR-Wert der ersten drei Bits gleich dem XOR-Wert der letzten drei Bits ist. Wir sagen daher manchmal auch kurz, die S-Box erhält den XOR 1 als Eingabe statt ausführlich den XOR 11_8 usw. Die XOR-Tabellen finden sich in A.2 auf Seite 13.

3 Differentielle Kryptoanalyse des Systems

Die Einträge in den XOR-Tabellen geben die Wahrscheinlichkeit an, daß bei festgehaltenen Daten und zufälligen Schlüssel, der Ausgabe-XOR einen bestimmten Wert hat.

Beispiel 2

Die Eingaben 1 und 6 (d.h nach E-Funktion 11_8 und 66_8) für die erste S-Box haben den XOR-Wert $1 \oplus 6 = 7$. Die 20 in der XOR-Tabelle für S1 in der 7ten Zeile und der 0ten Spalte sagt aus, daß mit Wahrscheinlichkeit $\frac{20}{64}$ die Ausgabe der S-Box 1 für die Eingaben 1 und 6 die gleiche sein wird. Dies gilt für zufällige, gleichverteilte Schlüssel für die erste S-Box.

Es ist möglich, aus der Kenntnis zweier Eingaben und des Ausgabe-XORs einer S-Box auf den verwendeten Schlüssel zu schließen.

Beispiel 3

Angenommen die Eingaben (Daten) zu S1 sind 4 und 5 und der Ausgabe-XOR ist 0. Die XOR-Tabelle zu S1 sagt uns, daß es nur 4 Paare mit Eingabe-XOR 1 und Ausgabe-XOR 0 gibt. Diese Paare sind (14,7), (7,14), (9,0) und (0,9). Zu jedem dieser Paare gehört auch ein möglicher Schlüssel. Nämlich 52_8 , 43_8 , 55_8 bzw. 44_8 . Betrachtet man nun andere Eingaben für S1 erhält man neue Möglichkeiten für den Schlüssel. Der richtige Schlüssel ist dann der, unter dem alle Übergänge möglich sind.

Eine mögliche Analyse kann daher wie folgt ablaufen:

1. Wähle einen geeigneten Eingabe-XOR.
2. Erzeuge eine geeignete Menge von Klartextpaaren mit diesem XOR-Wert. Verschlüssele sie und behalte nur den XOR der beiden verschlüsselten Werte.
3. Zu jedem Paar leite den wahrscheinlichen Ausgabe-XOR von möglichst vielen S-Boxen in der letzten Runde ab. (Beachte, daß die Eingaben für die S-Boxen in der letzten Runde bekannt sind, da sie im Geheimtext auftauchen!)
4. Für jeden möglichen Schlüssel zähle die Anzahl der Paare, die den erwarteten Ausgabe-XOR mit diesem Schlüssel erzeugen.
5. Der richtige Schlüssel ist (hoffentlich) der einzige Schlüssel, der am häufigsten gezählt wurde.

Das Problem ist daher aus der Kenntnis des Eingabe-XORs auf den Ausgabe-XOR der S-Boxen der letzten Runde zu schließen, ohne diesen null zu setzen. Ist nämlich der Eingabe-XOR 0, so muß auch der Ausgabe-XOR 0 sein, und wir erhalten keine Information. Dies geschieht mittels Charakteristiken des Kryptosystems.

Definition 4 (Charakteristik)

Eine n -Runden Charakteristik besteht aus $n+1$ Paaren $(L_0^*, R_0^*) \dots (L_n^*, R_n^*)$ mit $R_1^* = R_0^*$ und $R_i^* = L_{i-1}^*$ für $1 < i \leq n$. Dabei stehen L_i^* und R_i^* für den XOR-Wert entsprechender Werte des Kryptosystems.

3.1 Das Vier-Runden-System

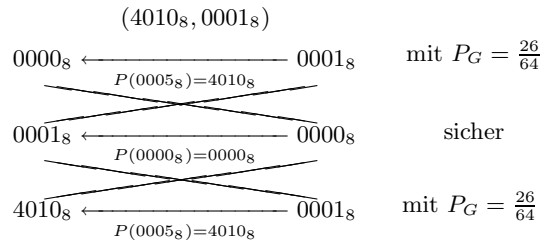


Abbildung 3: Eine drei Runden Charakteristik

Beispiel 5

Abbildung 3 zeigt eine drei Runden Charakteristik. Die Zahlen sind wie folgt zu lesen. Wenn zwei Eingaben (L_0, R_0) und (L'_0, R'_0) den XOR $(4010_8, 0001_8)$ haben (Die 8 deutet an, daß die Zahlen im Oktalsystem geschrieben sind.), so haben die Zwischenergebnisse (L_1, R_1) und (L'_1, R'_1) nach der ersten Runde mit Wahrscheinlichkeit $\frac{18}{64}$ den XOR $(0000_8, 0001_1)$. Entsprechend haben die Zwischenergebnisse nach der zweiten Runde den XOR $(0001_8, 0000_8)$ mit Wahrscheinlichkeit $\frac{18}{64} \cdot 1$. (Die Angaben rechts sind bedingte Wahrscheinlichkeiten!). Insgesamt sagt die Charakteristik also aus, daß mit Wahrscheinlichkeit $(\frac{18}{64})^2$ der Eingabe-XOR $(4010_8, 0001_8)$ zu dem Ausgabe-XOR $(4010_8, 0001_8)$ wird. Die Zahlen unter den Pfeilen geben jeweils den Ausgabe-XOR der F-Funktion an.

Eine Charakteristik ist also die Vermutung über die Entwicklung des Eingabe-XORs über die Runden. Die Wahrscheinlichkeit einer Charakteristik wird in der folgenden Definition präzisiert.

Definition 6

Unter der Wahrscheinlichkeit eines Übergangs $X \rightarrow Y$ für eine S-Box verstehen wir die Wahrscheinlichkeit, daß bei zufälligen Daten mit XOR X und zufälligem Schlüssel der Ausgaben-XOR Y ist. Diese Wahrscheinlichkeit kann man, wie in Beispiel 2 auf der vorherigen Seite erläutert, aus den XOR-Tabellen ablesen. Die Wahrscheinlichkeit eines Übergangs $I \rightarrow P(Z) = O$ für die F-Funktion ist das Produkt der Wahrscheinlichkeiten der entsprechenden Übergänge für die einzelnen S-Boxen. Die Wahrscheinlichkeit einer n -Runden Charakteristik ist das Produkt der Wahrscheinlichkeiten der n , von der Charakteristik geforderten, Übergänge für die F-Funktion. Wir werden diese Wahrscheinlichkeiten auch Grundwahrscheinlichkeiten nennen im Gegensatz zu den später definierten Korrektheitswahrscheinlichkeiten. (Bezeichnung: P_G .)

3.1 Das Vier-Runden-System

Wie bei DES ist das Vier-Runden-System sehr schwach, da eine deterministische Charakteristik verwandt werden kann.

Wir benutzen die Charakteristik aus Abbildung 4. Da $R_0 = R'_0$, folgt $L_1 = L'_1$. Da somit R_2 und R'_2 sich nur in der Eingabe für die erste S-Box unterscheiden, sind die Ausgaben der S-Boxen S_2, S_3 und S_4 für L_2 und L'_2 und damit auch in R_3 und R'_3 gleich.

3.2 Das Fünf-Runden-System

$$\begin{array}{ccc}
 & (0001_8, 0000_8) & \\
 1000_8 & \xleftarrow{P(0000_8)=0000_8} & 0000_8 \quad \text{sicher}
 \end{array}$$

Abbildung 4: Eine ein Runden Charakteristik

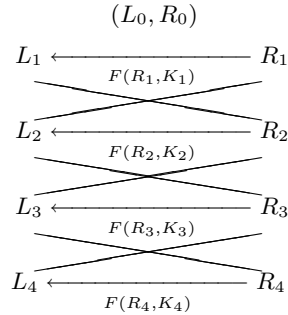


Abbildung 5: Ein vier Runden System

Aus $L_4 = R_3 \oplus F(R_4, K_4)$ und $L'_4 = R'_3 \oplus F(R'_4, K_4)$, folgt

$$F(R_4, K_4) \oplus F(R'_4, K_4) = (L_4 \oplus L'_4) \oplus (R_3 \oplus R'_3) .$$

Da L_4 und L'_4 als Ausgaben des 4-Runden Systems bekannt sind und R_3 und R'_3 für die Ausgaben von S_2, S_3 und S_4 den gleichen Wert haben, läßt sich also der Ausgabe-XOR der S-Boxen 2 bis 4 in der vierten Runde bestimmen. Da auch die Eingaben R_4 und R'_4 der F-Funktion in der vierten Runde als Ausgaben des Systems bekannt sind, läßt sich wie in Beispiel 3 auf Seite 4 der Schlüssel K_4 für die S-Boxen 2 bis 4 bestimmen. Im allgemeinen genügen 6 Klartextpaare, um die 18 bit von K_4 für die S-Boxen 2 bis 4 zu bestimmen. (Im folgenden werden wir nicht genauer auf die benötigte Anzahl von Klartextpaaren eingehen, siehe dazu [14, 12].)

Es bleiben noch die ersten 6 Bit von K_4 zu bestimmen. Dafür benutzen wir die Charakteristik aus Abbildung 6.

$$\begin{array}{ccc}
 & (0001_8, 0000_8) & \\
 1000_8 & \xleftarrow{P(0000_8)=0000_8} & 0000_8 \quad \text{sicher}
 \end{array}$$

Abbildung 6: Eine ein Runden Charakteristik

Mit dieser Charakteristik lassen sich die noch fehlenden Bits von K_4 bestimmen.

3.2 Das Fünf-Runden-System

Zur Analyse des Fünf-Runden-Systems benötigt man eine zwei Runden Charakteristik. Die zwei Runden Charakteristik mit der höchsten Wahrscheinlichkeit, ist die Charakteristik aus Abbildung 7 mit Wahrscheinlichkeit $P_G = \frac{26}{64}$.

3.2 Das Fünf-Runden-System

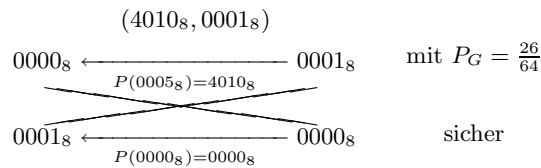


Abbildung 7: Eine zwei Runden Charakteristik

Dabei ergibt sich jedoch das Problem, daß der Übergang $0001_8 \rightarrow 1040_8$ erfordert, daß die Eingaben (Daten \oplus Schlüssel) aus folgender Menge sind:

$$\{77_8, 76_8, 74_8, 73_8, 60_8, 55_8, 52_8, 50_8, 35_8, 34_8, 33_8, 32_8, 30_8, \dots\}$$

Es folgt, daß der XOR der ersten drei Bit und der letzten drei Bit der Eingaben in folgender Menge enthalten ist:

$$\{0, 1, 3, 4, 5, 6, 7\}$$

Da zu diesem XOR-Wert nur der Schlüssel einen Beitrag liefert, folgt, daß auch der XOR der entsprechenden Schlüsselbits einen dieser Werte haben muß. Ist also $K_1 = b_1 b_2 b_3 \dots b_{24}$, so folgt, daß der Übergang

$$0001_8 \xrightarrow{F} P(0005_8) = 4010_8$$

wie von der Charakteristik gefordert nur stattfinden kann, wenn

$$b_{19} b_{20} b_{21} \oplus b_{22} b_{23} b_{24} \neq 2$$

ist.

Ein Analyseversuch mit Hilfe der Charakteristik aus Abbildung 7 kann also nur Erfolg haben, wenn der Schlüssel K_1 von dieser speziellen Form ist. Wir müssen daher die differentielle Kryptoanalyse so abwandeln, daß wir nicht von vornherein Annahmen über die Gestalt des Schlüssels machen. Zunächst führen wir folgende Begriffe ein:

Definition 7

Ein Übergang $X \rightarrow Y$ für eine S-Box S heißt korrekt für den Schlüssel K , wenn es Daten D_1 und D_2 gibt mit

$$D_1 \oplus D_2 = X$$

und

$$S(E(D_1) \oplus K) \oplus S(E(D_2) \oplus K) = Y .$$

Entsprechend heißt der Übergang $I \rightarrow O$ für die F-Funktion korrekt für den Schlüssel K , wenn es Daten D_1 und D_2 gibt mit

$$D_1 \oplus D_2 = I$$

und

$$F(D_1, K) \oplus F(D_2, K) = O .$$

Das Verhältnis der Anzahl aller Schlüssel, für die ein Übergang korrekt ist, zur Anzahl aller möglichen Schlüssel heißt die Korrektheitswahrscheinlichkeit P_K des Übergangs.

3.2 Das Fünf-Runden-System

Die Korrektheitswahrscheinlichkeit eines Übergangs läßt sich als die Wahrscheinlichkeit, daß bei zufällig gewähltem Schlüssel dieser Übergang stattfinden kann, interpretieren. Hat demnach ein Übergang in einer Charakteristik eine Korrektheitswahrscheinlichkeit kleiner als 1, so kann die Analyse mit dieser Charakteristik nicht bei allen Schlüsseln Erfolg haben.

Beispiel 8

Der oben untersuchte Übergang $0001_8 \xrightarrow{F} P(0005_8) = 4010_8$ ist korrekt für alle Schlüssel $K = b_1b_2b_3 \dots b_{24}$ mit $b_{19}b_{20}b_{21} \oplus b_{22}b_{23}b_{24} \neq 2$ aber nicht korrekt für $b_{19}b_{20}b_{21} \oplus b_{22}b_{23}b_{24} = 2$. Die Korrektheitswahrscheinlichkeit dieses Übergangs ist daher $\frac{7}{8}$.

In dem von uns betrachteten Kryptosystem hängt die Korrektheit eines der 2^6 Schlüssel, die für eine S-Box möglich sind, nur davon ab, welchen Wert der XOR der ersten drei Bits mit den letzten drei Bits hat. Es gibt also acht in diesem Sinn verschiedene Klassen von Schlüsseln. Die Tabellen in A.3 auf Seite 14 zeigen für jede S-Box und jeden Übergang $X \rightarrow Y$ mit $X \neq 0$ für wie viele dieser Klassen dieser Übergang korrekt ist. Dabei bestimmt, wie im Fall der XOR-Tabellen, X die Zeile und Y die Spalte. Wir nennen diese Tabellen *Korrektheitstabellen*.

Beispiel 9

Bei dem schon untersuchten Übergang $1 \xrightarrow{S_4} 5$ gibt es sieben Klassen von Schlüsseln, für die dieser Übergang korrekt ist. In der Tabelle S_4 steht daher in der ersten Zeile und fünften Spalte eine 7.

Wie man an Hand der Korrektheitstabellen ablesen kann, gibt es keinen Übergang verschieden von dem trivialen Übergang $0 \rightarrow 0$ mit Korrektheitswahrscheinlichkeit 1. Deshalb ist es unmöglich, ein System mit mehr als 4 Runden mit nur einer Charakteristik zu analysieren. Bei DES war dies möglich.

Wir müssen daher mehrere Charakteristiken gleichzeitig benutzen, um alle Möglichkeiten für die Schlüssel abzudecken. Dies kann wie folgt geschehen:

Definition 10

Eine Menge M von Charakteristiken heißt korrekt, wenn für alle möglichen Schlüssel es eine Charakteristik aus M gibt, so daß alle von der Charakteristik geforderten Übergänge für diesen Schlüssel korrekt sind.

Die beiden Charakteristiken in Abbildung 8 bilden eine korrekte Menge von drei Runden Charakteristiken:

Mit dieser Menge von Charakteristiken lassen sich nun bei einem fünf Runden Kryptosystem, die 18 Bit von K_5 , die in die S-Boxen 1 bis 3 eingehen, bestimmen.

Wir betrachten abwechselnd Klartextpaare für jede der beiden Charakteristiken und leiten die wahrscheinlichen Schlüssel ab. Für jede Charakteristik und jeden Schlüssel zählen wir, wie oft dieser Schlüssel von der Charakteristik vorgeschlagen wurde. Sobald einer der Zähler einen vorher festgelegten Schwellenwert übersteigt, brechen wir ab und nehmen den zu diesem Zähler gehörenden Schlüssel als den wahrscheinlichsten Schlüssel.

3.3 Mehr-Runden-Systeme

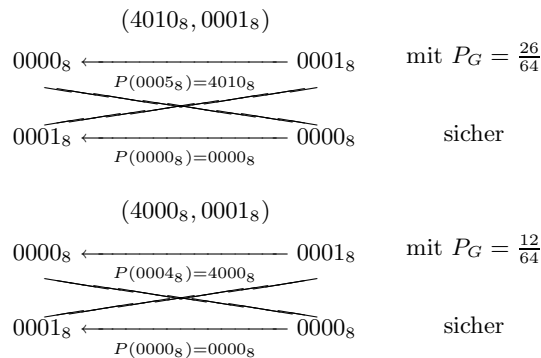


Abbildung 8: Eine korrekte Menge von zwei Runden Charakteristiken

Die entsprechende Charakteristik ist für den aktuellen Schlüssel mit hoher Wahrscheinlichkeit korrekt. Wenn weitere Analysen zur Bestimmung von anderen Teilen des Schlüssels durchgeführt werden, sollten daher vorzugsweise Charakteristiken mit diesen Übergängen benutzt werden.

In der Praxis hat sich ein Schwellenwert von 12 als geeignet erwiesen. Dabei wird der richtige Schlüssel in über 95% der Fälle mit ungefähr 200 gewählten Klartexten gefunden.

3.3 Mehr-Runden-Systeme

Bei einer Charakteristik können keine zwei aufeinanderfolgende Übergänge gleich dem trivialen Übergang $0 \rightarrow 0$ sein, da in diesem Fall alle Übergänge gleich dem trivialen Übergang sein müssten und wir so keine Information über das System erhielten.

Bei einer Analyse des 16-Runden Systems müssen wir also 13 Runden Charakteristiken mit mindestens sechs von dem trivialen Übergang verschiedenen Übergängen verwenden. Da jeder nichttriviale Übergang eine Korrektheitswahrscheinlichkeit kleiner 1 hat, muß eine korrekte Menge von 13 Runden Charakteristiken aus mindestens $2^6 = 64$ verschiedenen Charakteristiken bestehen. Abgesehen von dem Problem, daß eine solche Menge zunächst konstruiert werden muß, müssten wir bei einer Analyse aus den 64 Charakteristiken die korrekte herausfinden, was eine unrealistisch hohe Anzahl von gewählten Klartexten erfordern würde.

Für weniger Runden läßt sich allerdings noch eine Analyse durchführen. Als Beispiel zeigt Abbildung 9 auf der nächsten Seite eine korrekte Menge von vier Runden Charakteristiken, die zur Analyse des 7 Runden Systems verwandt werden können. Im Vergleich zu der Menge aus Abbildung 8 zeigen sich jedoch mehrere Besonderheiten:

1. Die zweite und dritte Charakteristik lassen sich durch den trivialen Übergang zu fünf Runden Charakteristiken erweitern.
2. Bei der Analyse werden, je nachdem welche Charakteristik korrekt ist, verschiedene Teile des Schlüssels K_7 gefunden. Bei der ersten Charakteristik sind es die Schlüsselbits für S_1 , S_2 und S_4 , bei der zweiten und dritten die für S_1 , S_3 und S_4 und bei der vierten die für S_1 , S_2 und S_3 .

3.3 Mehr-Runden-Systeme

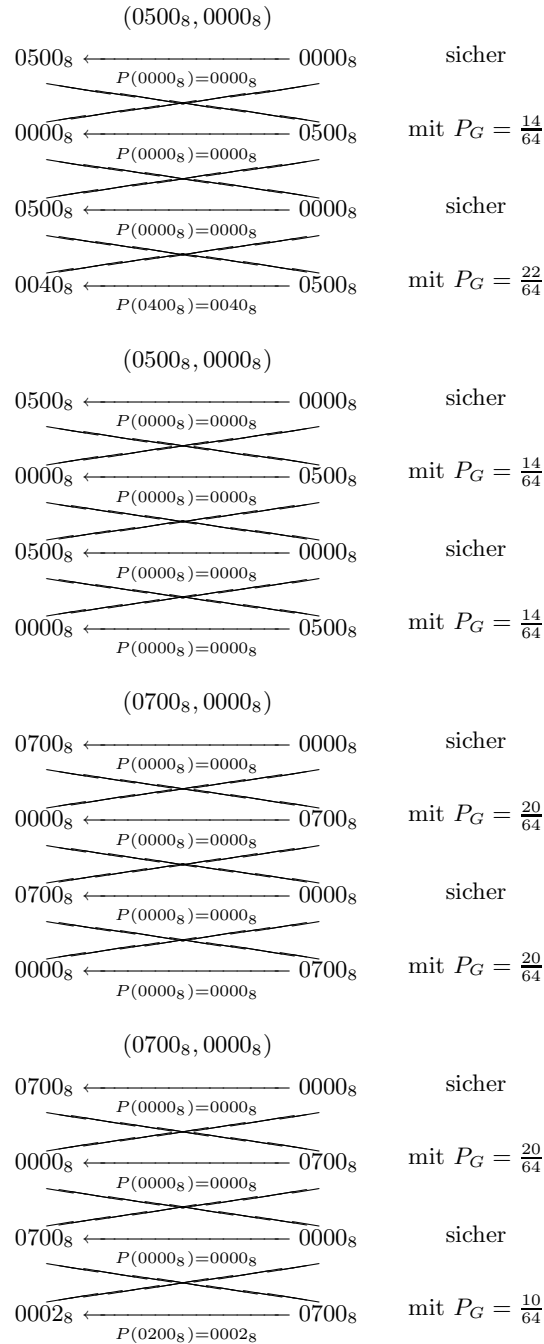


Abbildung 9: Eine korrekte Menge von vier Runden Charakteristiken

4 Designprinzipien des Systems

Bevor wir zu den Designprinzipien des Systems kommen, betrachten wir zunächst die Designprinzipien von DES. Für die S-Boxen haben Brickel, Moore und Purtill [7] folgenden Prinzipien aufgestellt:

1. Jede Zeile ist eine Permutation der ganzen Zahlen von 0 bis 15.
2. Keine S-Box ist eine lineare oder affine Funktion ihrer Eingabe.
3. Die Änderung eines Eingabebits bewirkt die Änderung von mindestens zwei Ausgabebits.
4. $S(x)$ und $S(x \oplus 001100)$ unterscheiden sich in mindestens zwei Bits.
5. $S(x) \neq S(x \oplus 11ef00)$ für alle Werte von e und f.
6. Die S-Boxen werden so gewählt, daß sie den Unterschied zwischen 1'er und 0'er in der Ausgabe einer S-Box minimieren, wenn ein Bit festgelassen wird.

Denkt man an die differentielle Kryptoanalyse, so muß man an eine S-Box folgende Forderung stellen :

Die S-Boxen werden so gewählt, daß sie die Einträge in den XOR-Tabellen minimieren.

Bei DES wurde außerdem die E-Funktion so gewählt, daß möglichst viele S-Boxen gleichzeitig von null verschiedenen Eingabe-XOR Werte erhalten. So ist zum Beispiel für ein Übergang $X \rightarrow 0$ für die F-Funktion notwendig, daß mindestens zwei S-Boxen von null verschiedene Eingabewerte erhalten.

Bei dem von uns betrachteten Kryptosystem ist jedoch die E-Funktion so gewählt, daß keine zwei S-Boxen gemeinsame Datenbits erhalten. Stattdessen erhält jede S-Box nur drei verschiedene Datenbits. Dadurch werden die Abhängigkeiten, die die Korrektheitswahrscheinlichkeiten kleiner 1 erzeugen, hervorgerufen.

An die S-Boxen stellen sich daher neue Anforderungen:

Wie bei DES sind die S-Boxen so gewählt, daß die Einträge in den XOR-Tabellen möglichst klein sind. Darüber hinaus darf kein Übergang außer dem trivialen Übergang $0 \rightarrow 0$ eine Korrektheitswahrscheinlichkeit von 1 haben.

| | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|
| i | 1 | 2 | 3 | 4 | 5 | 6 |
| h_i | 12,09 | 11,80 | 11,89 | 12,29 | 12,07 | 12,00 |
| i | 7 | 8 | 9 | 10 | 11 | 12 |
| h_i | 12,15 | 12,08 | 12,14 | 12,16 | 12,23 | 11,93 |
| i | 13 | 14 | 15 | 16 | 17 | 18 |
| h_i | 11,95 | 11,79 | 12,21 | 12,11 | 11,99 | 12,09 |
| i | 19 | 20 | 21 | 22 | 23 | 24 |
| h_i | 12,12 | 11,72 | 12,51 | 11,90 | 12,27 | 12,18 |

Tabelle 4: Der Avalanche-Effekt

Die P-Permutation wurde so gewählt, daß die Bits möglichst gut durchmischt werden. Dadurch wird erreicht, daß das Avalanche-Kriterium erfüllt wird. Nach

4 Designprinzipien des Systems

diesem Kriterium müssen sich durchschnittlich die Hälfte der Geheimtextbits ändern, wenn sich ein Klartextbit ändert. Die Tabelle 4 zeigt die durchschnittliche Anzahl h_i von geänderten Geheimtextbits, wenn das i -te Klartextbit geändert wird.

Das System ist in dieser Form nur dazu da, das Konzept der Korrektheitswahrscheinlichkeiten zu erläutern. Ein System zur praktischen Anwendung sollte mehr S-Boxen haben. Darüber hinaus sollten die S-Boxen 8-Bit nach 4-Bit abbilden und einen key-scheduling Algorithmus verwandt werden.

A Tabellen

A.1 Tafeln der S-Boxen

| S1 | | | | | | | | S2 | | | | | | | |
|----|---|---|---|---|---|---|---|----|---|---|---|---|---|---|---|
| 4 | 7 | 1 | 5 | 2 | 6 | 0 | 3 | 5 | 3 | 0 | 4 | 7 | 1 | 6 | 2 |
| 0 | 4 | 2 | 6 | 1 | 5 | 3 | 7 | 6 | 5 | 7 | 1 | 0 | 4 | 2 | 3 |
| 3 | 6 | 0 | 2 | 5 | 1 | 7 | 4 | 2 | 1 | 6 | 7 | 4 | 0 | 3 | 5 |
| 2 | 0 | 6 | 4 | 3 | 7 | 5 | 1 | 7 | 6 | 1 | 5 | 2 | 3 | 4 | 0 |
| 1 | 5 | 7 | 0 | 4 | 3 | 6 | 2 | 0 | 4 | 3 | 6 | 5 | 2 | 1 | 7 |
| 7 | 2 | 4 | 3 | 6 | 0 | 1 | 5 | 3 | 7 | 5 | 2 | 1 | 6 | 0 | 4 |
| 6 | 3 | 5 | 1 | 7 | 4 | 2 | 0 | 1 | 2 | 4 | 0 | 3 | 5 | 7 | 6 |
| 5 | 1 | 3 | 7 | 0 | 2 | 4 | 6 | 4 | 0 | 2 | 3 | 6 | 7 | 5 | 1 |

| S3 | | | | | | | | S4 | | | | | | | |
|----|---|---|---|---|---|---|---|----|---|---|---|---|---|---|---|
| 4 | 5 | 2 | 7 | 3 | 6 | 1 | 0 | 7 | 6 | 0 | 3 | 1 | 4 | 2 | 5 |
| 1 | 4 | 3 | 6 | 2 | 7 | 0 | 5 | 2 | 7 | 1 | 4 | 0 | 3 | 5 | 6 |
| 0 | 6 | 1 | 3 | 7 | 2 | 5 | 4 | 5 | 4 | 2 | 1 | 3 | 0 | 6 | 7 |
| 3 | 1 | 6 | 4 | 0 | 5 | 7 | 2 | 1 | 2 | 4 | 7 | 5 | 6 | 3 | 0 |
| 2 | 7 | 5 | 1 | 4 | 0 | 6 | 3 | 0 | 3 | 6 | 2 | 7 | 5 | 4 | 1 |
| 5 | 3 | 4 | 0 | 6 | 1 | 2 | 7 | 6 | 1 | 7 | 5 | 4 | 2 | 0 | 3 |
| 6 | 0 | 7 | 2 | 5 | 4 | 3 | 1 | 4 | 5 | 3 | 0 | 6 | 7 | 1 | 2 |
| 7 | 2 | 0 | 5 | 1 | 3 | 4 | 6 | 3 | 0 | 5 | 6 | 2 | 1 | 7 | 4 |

A.2 XOR-Tabellen

| | | S1 | | | | | | | |
|---|--|----|---|----|----|----|----|----|----|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | | 64 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | | 4 | 2 | 10 | 8 | 18 | 4 | 4 | 14 |
| 2 | | 8 | 8 | 10 | 6 | 12 | 8 | 10 | 2 |
| 3 | | 4 | 4 | 16 | 4 | 6 | 10 | 10 | 10 |
| 4 | | 2 | 0 | 18 | 12 | 8 | 2 | 12 | 10 |
| 5 | | 14 | 8 | 0 | 6 | 18 | 0 | 12 | 6 |
| 6 | | 4 | 8 | 12 | 4 | 12 | 4 | 12 | 8 |
| 7 | | 20 | 6 | 2 | 8 | 2 | 12 | 12 | 2 |

| | | S2 | | | | | | | |
|---|--|----|----|----|----|----|----|----|----|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | | 64 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | | 4 | 10 | 4 | 18 | 4 | 6 | 8 | 10 |
| 2 | | 8 | 4 | 16 | 4 | 22 | 2 | 2 | 6 |
| 3 | | 4 | 6 | 6 | 16 | 2 | 8 | 8 | 14 |
| 4 | | 2 | 16 | 2 | 12 | 8 | 10 | 4 | 10 |
| 5 | | 14 | 0 | 12 | 2 | 22 | 4 | 0 | 10 |
| 6 | | 4 | 10 | 6 | 16 | 2 | 4 | 8 | 14 |
| 7 | | 20 | 2 | 10 | 4 | 8 | 2 | 14 | 4 |

A.3 Korrektheitstabellen

| | | S3 | | | | | | | |
|---|----|----|----|---|----|----|----|----|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 64 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 4 | 8 | 10 | 2 | 14 | 18 | 4 | 4 | |
| 2 | 8 | 6 | 10 | 8 | 2 | 12 | 8 | 10 | |
| 3 | 4 | 4 | 16 | 4 | 10 | 6 | 10 | 10 | |
| 4 | 2 | 12 | 18 | 0 | 10 | 8 | 2 | 12 | |
| 5 | 14 | 6 | 0 | 8 | 6 | 18 | 0 | 12 | |
| 6 | 4 | 4 | 12 | 8 | 8 | 12 | 4 | 12 | |
| 7 | 20 | 8 | 2 | 6 | 2 | 2 | 12 | 12 | |

| | | S4 | | | | | | | |
|---|----|----|----|----|----|----|----|----|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 64 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 4 | 6 | 4 | 2 | 12 | 26 | 4 | 6 | |
| 2 | 8 | 2 | 8 | 14 | 2 | 8 | 10 | 12 | |
| 3 | 4 | 8 | 12 | 8 | 2 | 14 | 10 | 6 | |
| 4 | 2 | 4 | 6 | 20 | 4 | 6 | 12 | 10 | |
| 5 | 14 | 0 | 10 | 16 | 4 | 2 | 12 | 6 | |
| 6 | 4 | 8 | 6 | 6 | 10 | 18 | 12 | 0 | |
| 7 | 20 | 12 | 6 | 2 | 2 | 2 | 12 | 8 | |

A.3 Korrektheitstabellen

| | | S1 | | | | | | | | | | S2 | | | | | | | |
|---|---|----|---|---|---|---|---|---|---|---|---|----|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 2 | 1 | 4 | 3 | 5 | 2 | 2 | 6 | | 1 | 2 | 3 | 2 | 5 | 1 | 3 | 4 | 4 | |
| 2 | 4 | 4 | 5 | 3 | 3 | 3 | 4 | 1 | | 2 | 4 | 2 | 5 | 2 | 4 | 1 | 1 | 3 | |
| 3 | 2 | 2 | 7 | 2 | 3 | 5 | 4 | 5 | | 3 | 2 | 3 | 2 | 6 | 1 | 3 | 3 | 5 | |
| 4 | 1 | 0 | 6 | 6 | 4 | 1 | 5 | 5 | | 4 | 1 | 5 | 1 | 5 | 4 | 3 | 2 | 4 | |
| 5 | 6 | 4 | 0 | 3 | 7 | 0 | 3 | 3 | | 5 | 6 | 0 | 5 | 1 | 7 | 1 | 0 | 5 | |
| 6 | 2 | 4 | 5 | 2 | 5 | 1 | 5 | 4 | | 6 | 2 | 3 | 3 | 5 | 1 | 1 | 3 | 5 | |
| 7 | 7 | 2 | 1 | 4 | 1 | 5 | 5 | 1 | | 7 | 7 | 1 | 4 | 2 | 3 | 1 | 5 | 1 | |

| | | S3 | | | | | | | | | | S4 | | | | | | | |
|---|---|----|---|---|---|---|---|---|---|---|---|----|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 2 | 3 | 4 | 1 | 6 | 5 | 2 | 2 | | 1 | 2 | 3 | 2 | 1 | 4 | 7 | 2 | 1 | |
| 2 | 4 | 3 | 5 | 4 | 1 | 3 | 3 | 4 | | 2 | 4 | 1 | 3 | 3 | 1 | 4 | 4 | 4 | |
| 3 | 2 | 2 | 7 | 2 | 5 | 3 | 5 | 4 | | 3 | 2 | 4 | 5 | 3 | 1 | 6 | 4 | 2 | |
| 4 | 1 | 6 | 6 | 0 | 5 | 4 | 1 | 5 | | 4 | 1 | 2 | 3 | 5 | 2 | 3 | 5 | 4 | |
| 5 | 6 | 3 | 0 | 4 | 3 | 7 | 0 | 3 | | 5 | 6 | 0 | 4 | 6 | 1 | 1 | 3 | 3 | |
| 6 | 2 | 2 | 5 | 4 | 4 | 5 | 1 | 5 | | 6 | 2 | 3 | 2 | 3 | 3 | 7 | 5 | 0 | |
| 7 | 7 | 4 | 1 | 2 | 1 | 1 | 5 | 5 | | 7 | 7 | 4 | 2 | 1 | 1 | 1 | 5 | 2 | |

Literatur

- [1] Carlisle M. Adams. On immunity against Biham and Shamir's 'differential cryptanalysis'. *Inf. Process. Lett.*, 41(2):77–80, 1992.
- [2] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.
- [3] Eli Biham and Adi Shamir. Differential cryptanalysis of Feal and N -Hash. In *EUROCRYPT '91*, number 547 in Lecture Notes in Computer Science, pages 1–16, 1991.
- [4] Eli Biham and Adi Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. In *CRYPTO '91*, number 576 in Lecture Notes in Computer Science, pages 156–171, 1992.
- [5] Eli Biham and Adi Shamir. *Differential cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, 1993.
- [6] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round DES. In *CRYPTO '92*, number 740 in Lecture Notes in Computer Science, pages 487–496, 1993.
- [7] E. F. Brickel, J. H. Moore, and M. R. Purtill. Structure in the S-Boxes of DES. In *CRYPTO '86*, Lecture Notes in Computer Science, pages 3–7, 1986.
- [8] Lawrence Brown, Matthew Kwan, Josef Pieprzyk, and Jennifer Seberry. Improving resistance to differential cryptanalysis and the redesign of LOKI. In *ASIACRYPT '91*, number 739 in Lecture Notes in Computer Science, pages 36–50, 1993.
- [9] Andreas Klein. PASCAL-Programm zur differentiellen Kryptoanalyse. Erhältlich über E-mail: Andreas.Klein@mathe.uni-giessen.de.
- [10] Lars Ramkilde Knudsen. Cryptanalysis of LOKI. In *ASIACRYPT '91*, number 739 in Lecture Notes in Computer Science, pages 22–35, 1993.
- [11] Lars Ramkilde Knudsen. Iterative characteristics of DES and s^2 -DES. In *CRYPTO '92*, number 740 in Lecture Notes in Computer Science, pages 497–511, 1993.
- [12] Matthew Kwan. Simultaneous attacks in differential cryptanalysis (getting more pairs per encryption). In *ASIACRYPT '91*, number 739 in Lecture Notes in Computer Science, pages 489–492, 1993.
- [13] M. Matsui. Linear cryptanalysis method for DES chipper. In *EUROCRYPT '93*, number 765 in Lecture Notes in Computer Science, pages 386–397, 1993.
- [14] Hiroshi Miyano. A method to estimate the number of chiphertext pairs for differential cryptanalysis. In *ASIACRYPT '91*, number 793 in Lecture Notes in Computer Science, pages 51–58, 1993.

LITERATUR

- [15] Kaisa Nyberg and Lars Ramkilde Knudson. Provable security against differential cryptanalysis. In *CRYPTO '92*, number 740 in Lecture Notes in Computer Science, pages 566–574, 1993.