Fachhochschule Nordwestschweiz
Hochschule für Technik

Differentielle Kryptoanalyse

Artikel Kryptographie
Windisch, 4. Juni 2020

[1]

Autoren	Gabriel Nussbaumer und Fabian von Büren
Dozent	Dr. M. Hufschmid
Modul	Kryptographie (kryg)
Hochschule	Hochschule für Technik - FHNW
Studiengang	Elektro- und Informationstechnik

1 Einleitung

Kryptosysteme sind Funktionen, welche darauf basieren mehrere Runden zu durchlaufen, somit werden sie komplexer und der Widerstand gegen Angriffe nimmt zu. Der Data Encryption Standard (DES), welcher in den 1970er-Jahren von IBM entwickelt wurde, durchläuft mehrere Runden, in denen jeweils eine Expansion-Permutation, XOR-Verknüpfungen, S-Boxen und Bit-Permutation enthalten sind. Die S-Boxen sind nichtlineare Funktionen. Einem Verschlüsselungsalgorithmus kann vertraut werden, wenn dieser nach dem Prinzip von Kerckhoffs implementiert wurde. Das Kerckhoffs'sche Prinzip lautet: Die Sicherheit des Algorithmus soll nur von der Geheimhaltung des Schlüssels, nicht von der Geheimhaltung des Algorithmus abhängen. Der gesamte Verschlüsselungsalgorithmus vom DES, also die Funktionsweise, die Permutation-Tabellen wie auch die Substitutionsboxen (S-Boxen), ist öffentlich bekannt. Die Geheimhaltung der Daten hängt also vom zufällig gewählten geheimen Schlüssel ab.

Bei der differenziellen Kryptoanalyse wird ein statischer Angriff auf den Verschlüsselungsalgorithmus durchgeführt, bei dem der Angreifer selbstgewählte Klartext- und Geheimtextpaare verwenden kann. Es handelt sich also um eine „chosen plaintext attack". Es werden Differenzen in den Klartextpaaren auf Differenzen in den Geheimtextpaaren analysiert. Diese Differenzen werden verwendet um mögliche Schlüssel-Wahrscheinlichkeiten zuzuordnen und somit den wahrscheinlichsten Schlüssel zu finden. Bei Anwendung dieser Methode auf den DES, nimmt die Komplexität der Verschlüsselung mit der Anzahl der Runden zu. Im Anwendungsfall bewehrt sich die differenzielle Kryptoanalyse bei 16 Runden von DES nicht mehr im Bezug auf eine „brute force attack". Bei der Brute-Force-Attacke, was so viel heisst wie rohe Gewalt, werden alle möglichen Schlüssel durchprobiert bis der richtige Schlüssel gefunden ist, was bei einer Schlüssellänge von 56-Bits, genau 2^{56} Operationen entspricht [2].

2 Historisches

Die differenzielle Kryptoanalyse wurde im Juli 1990 von den israelischen Wissenschaftler Eli Biham und Adi Shamir veröffentlicht. In dieser Veröffentlichung wird die Methode beschrieben wie ein „chosen plaintext"-Angriff auf den DES durchgeführt werden kann [2].

Der Data Encription Standard (DES) war in den 70 Jahren das meist verwendete Verschlüsselungssystem für die zivile Bevölkerung. Mit dem DES konnte in dieser Zeit ein grosser Widerstand gegen Angriffe bewiesen werden, und wurde im Jahre 1977 als offizieller Sicherheitsstandard für die US-Regierung vom Federal Information Processing Standard (FIBS) bestätigt.

Der Mathematiker Don Coppersmith war an der Entwicklung des DES bei der Firma IBM beteiligt, insbesondere an der Kryptoanalyse der S-Boxen. Nach der Veröffentlichung der differenziellen Kryptoanalyse von Eli Biham und Adi Shamir, gab Coppersmith bekannt, dass die S-Boxen dagegen optimiert waren [3].

3 Funktionsweise

Folglich soll die Funktionsweise einer differenziellen Kryptoanalyse auf eine Runde vom Data Encryption Standard erläutert werden. Es wird nur die rechte Seite (R_0) einer DES-Runde betrachtet, womit die verwendeten Klartexte 32 Bit lang sind. Wie der Name es schon andeutet, wird bei diesem Verfahren die Differenz aus zwei Klartexten, in diesem Beispiel mit P_1 und P_2 bezeichnet, verwendet. Die Differenz wird üblicherweise mit P' bezeichnet und folgt aus einer XOR-Verknüpfung der Klartexte, also $P' = P_1 \oplus P_2$. Funktionen wie Expansionen, Permutationen oder XOR-Verknüpfen haben keine Einfluss auf die Differenz der Texte. Die Differenz kann also fast durch die gesamte Feistelstruktur beobachtet werden, wie in der Abbildung 3.1 zu erkennen ist. Eine DES-Runde beinhaltet am Ende der Runde noch eine Ausgangspermutation und die XOR-Verknüpfung mit der linken Seite (L_0). Diese Elemente wurden nicht in der Abbildung 3.1 dargestellt, da sie bei einer 1-Runden-Analyse von DES nicht von Bedeutung sind.

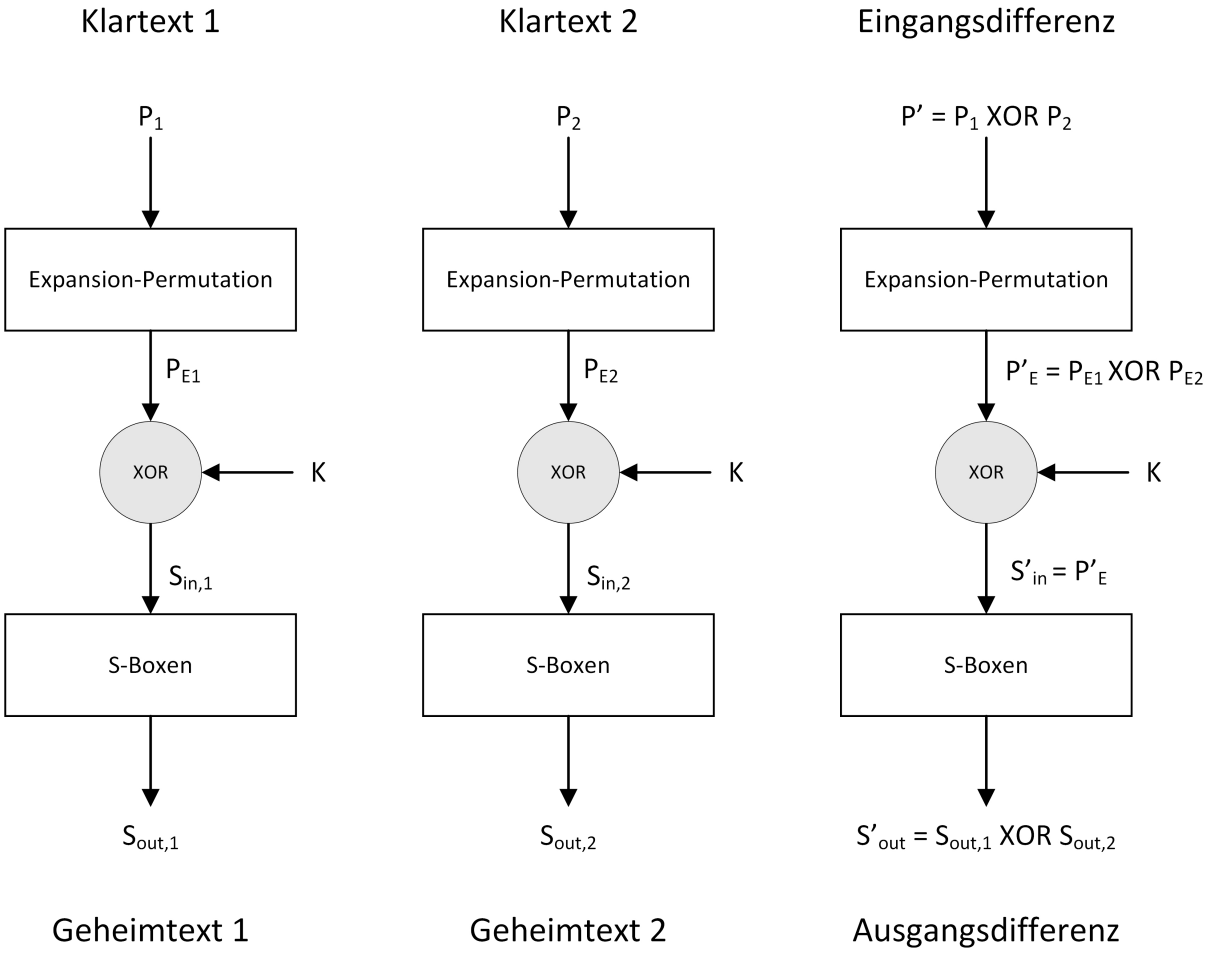

Abbildung 3.1: Verhalten von Klartext 1, 2 und der Differenz davon durch die Feistelstruktur einer Runde von DES [4]

Die Eingangswerte $S_{in,1}$ und $S_{in,2}$ der S-Boxen sind ohne Schlüssel nicht bekannt. Bei der Spalte „Differenz“ ist dieser Eingang S'_{in} aber bekannt. Eine doppelte XOR-Verknüpfung mit dem Schlüssel hebt sich auf. Mit anderen Worten ist:

$$S'_{in} = S_{in,1} \oplus S_{in,2} = (P_{E,1} \oplus K) \oplus (P_{E,2} \oplus K) = P_{E,1} \oplus P_{E,2} = P'_E \tag{3.1}$$

Mit dieser Eigenschaft gelingt es die S-Boxen genauer zu analysieren. Wie bereits in der Einleitung erwähnt, sind die acht S-Boxen nichtlineraren Funktion. Um diese zu umgehen, wird mit Wahrscheinlichkeiten gearbeitet werden. Anhand der öffentlich zugänglichen S-Boxen kann eine Differenzenverteilungstabelle aufgestellt werden. In dieser wird für jede Eingangsdifferenz die Anzahl Wertepaar gegeben, welche eine bestimmte Ausgangsdifferenz erzeugen. Es gibt bei DES pro S-Box $2^6 = 64$ verschieden mögliche Eingangsdifferenzen. Jede Eingangsdifferenz kann mit 64 verschiedenen Wertepaare erzeugt werden. Als Beispiel: für eine Eingangsdifferenz von 34_h (Hexadezimalzahl) gibt es laut Differenzenverteilungstabelle nur zwei von den 64 Wertepaar die, beim Durchqueren der S-Boxen 1, eine Ausgangsdifferenz von 04_h erzeugen. Die anderen 62 Wertepaare mit der Differenz 34_h geben eine Ausgangsdifferenz ungleich 04_h heraus.

Da bei einer „chosen plaintext attack“ die Ausgangsdifferenz bekannt ist, können die möglichen Eingangswertepaare $(S_{in,1}, S_{in,2})$ in einer weiteren Tabelle abgelesen werden. Entsprechend der Differenzenverteilungstabelle gibt es mehr oder weniger solche möglichen Eingangspaar. Für das Beispiel mit der Eingangsdifferenz 34_h und der Ausgangsdifferenz 04_h gibt es die 2 Wertepaare $(S_{in,1}, S_{in,2}) = (13_h, 27_h)$ oder $(S_{in,1}, S_{in,2}) = (27_h, 13_h)$. Wäre die Ausgangsdifferenz 02_h bei einer Eingangsdifferenz von 34_h würde es 16 mögliche Wertepaare geben.

Da nun die Eingangswerte bekannt sind, kann der Schlüssel wie folgt berechnet werden:

$$K = P_{E,1} \oplus S_{in,1} = P_{E,2} \oplus S_{in,2} \tag{3.2}$$

Weil nicht mit Sicherheit gesagt werden kann welches Wertepaar $(S_{in,1}, S_{in,2})$ das richtige ist, gibt es bei diesem Beispiel zwei mögliche Schlüssel. Es müssten die anderen S-Boxen betrachtet oder mehrere Durchgänge durchgeführt werden, um den falschen Schlüssel auszuschliessen. [2][5]

3.1 Mehrere Runden von DES

Bis jetzt wurde lediglich eine Runde von DES betrachtet. Es braucht nur wenige Klartext-Geheimtext-Paare damit der Schlüssel für eine Runde ermittelt werden kann. Bei mehr als 2 Runden von DES können nicht mehr alle wichtigen Differenzen in der Feistelstruktur ermittelt werden. An dieser Stelle kommt die Runden-Charakteristik ins Spiel. Da die Zwischenresultate nicht zur Verfügung stehen, werden sich wiederholende Strukturen gesucht, sogenannte iterative Charakteristiken. Diese können sich nach einer oder mehrere Runden wiederholen. Die Abbildung 3.2 zeigt eine Zweirunden-Charakteristik.

Die Wahrscheinlichkeiten (im Bild 3.2 auf der rechten Seite: $p_1 = 1 =$ always und $P_2 = 1/234$) stammen aus den Differenztabellen für alle 8 S-Boxen. Anders gesagt, es gibt ein Eingangswertepaar von 234, dessen Eingangsdifferenz am Ausgang invertiert erscheint. Die anderen Wertepaare, auch „falsche Paare“ genannt, liefern eine unbrauchbare Ausgangsdifferenz ($S'_{out} = S_{out,1} \oplus S_{out,1} \neq$ 19600000 00000000). Erst bei einem gefundenen „richtigen Paar“ kann die differenzielle Kryptoanalyse angewendet werden und der Schlüssel oder Teile des Schlüssels ermittelt werden. Die Schwierigkeit bei mehreren Runden von DES liegt darin Klartext- /Geheimtextpaare zu finden wobei deren Differenz in eine sich wiederholende Struktur passt. Es gibt andere Eingangsdifferenzen welche sich nach zwei Runden wiederholen, entsprechend nicht nur $\Omega_P =$ 19600000 00000000, jedoch sind diese eher selten. Die meisten davon sind gut bei wenig Runden von DES (siehe [2]). Das Beipiel in Abbildung 3.2 kann bis 15 Runden von DES gebraucht werden. Umso mehr Runden der Verschlüsselungsalgorithmus hat, desto unwahrscheinlicher ist es ein richtiges Paar zu finden. Die Wahrscheinlichkeiten der Charakteristiken werden miteinander Multipliziert. Bei 16 Runden wird die Wahrscheinlichkeit ein richtiges Paar zu finden so klein, dass ein Brut-Force-Attacke genau so schneller wäre. Die differenzielle Kryptoanalyse

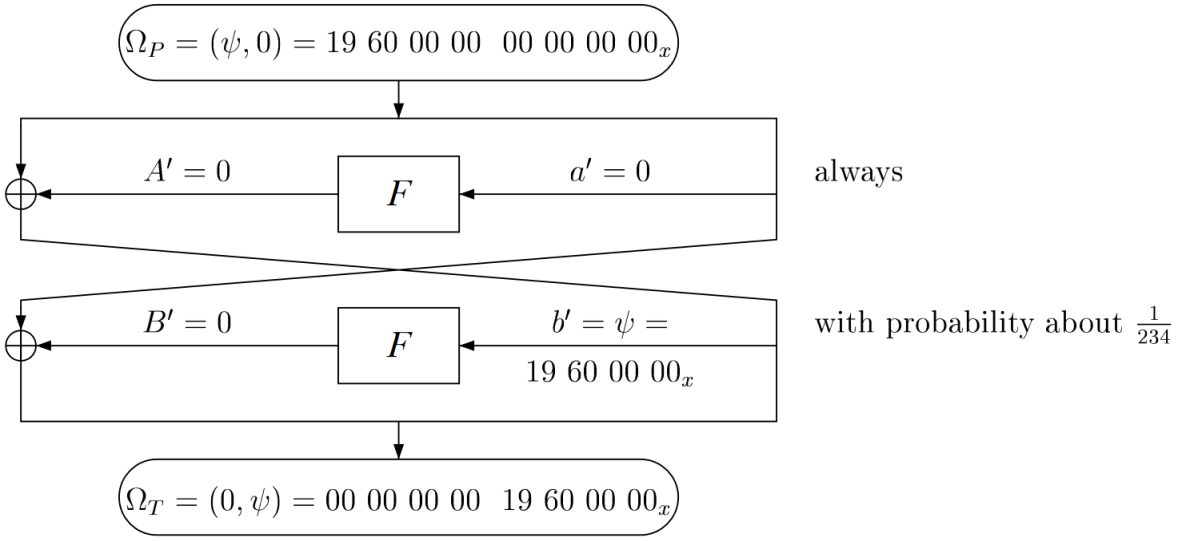

Abbildung 3.2: Dies ist eine Zweirunden-Charakteristik für die differenzielle Kryptoanalyse bei mehr als zwei Runden von DES. Die Eingangsdifferenz wiederholt sich nach zwei Runden in der Feistelstruktur [2].

ist hingegen effizient bei anderen DES-ähnlichen Kryptosysteme. Verschlüsselungsverfahren wie die Achtrunden-Variante von Lucifer (Verschlüsselungsverfahren entworfen durch IBM vor DES) oder FEAL-4 / FEAL-8 können zum Beispiel mit der vorgestellten Methode gebrochen werden. FEAL mit weniger als 32 Runden können teilweise gebrochen werden. [2]

4 Schluss

Mit der differenziellen Kryptoanalyse wurde von Hiham und Shamir eine Methode veröffentlicht mit der ein statischer Angriff auf ein Verschlüsselungsalgorithmus durchgeführt werden kann. Wird der Angriff am Verschlüsselungsalgorithmus von Data Encryption Standart (DES) angewendet, wird in einem ersten Schritt der geheime Schlüssel durch zweifacher Anwendung der XOR-Verknüpfung aufgehoben. Nun können die nichtlinearen Funktionen (S-Boxen) analysiert werden. Mit den öffentlich zugänglichen S-Boxen werden Differenzentabellen erstellt in denen die Anzahl mögliche Wertepaare definiert sind, für die mit der Eingangsdifferenz eine bestimmte Ausgangsdifferenz erzeugt werden kann. Aus den Eingangswertepaaren, welche die Ausgangsdifferenz erfüllen, können nun mögliche Schlüssel mit XOR-Verknüpfungen, an Stelle wo der Schlüssel eingesetzt wird, berechnet werden. Mit mehreren Runden von DES können nicht mehr alle wichtigen Differenzen ermittelt werden, da die Zwischenresultate nicht zur Verfügung stehen. Es werden sich wiederholende Strukturen gesucht. Die Wahrscheinlichkeit den richtigen Schlüssel zu finden nimmt ab. Bei 16 Runden wird die Wahrscheinlichkeit das richtige Paar zu finden so klein, dass eine Brut-Force-Attacke genauso schnell wäre. Bei anderen Verschlüsselungssysteme wie Lucifer oder FEAL kann die differenzielle Kryptoanalyse effizient angewendet werden. Seit dem die Methode der differenzielle Kryptoanalyse publiziert wurde, muss beim Entwurf eines Verschlüsselungsalgorithmus darauf geachtet werden, dass diese Methode nicht wirkungsvoll eingesetzt werden kann.

Literatur

[1] Thirah. (). Vorhängeschloss-Schlüssel-Computer-Icons, [Online] Available: `https://de.cleanpng.com/png-qhshuq/` (Abrufdatum 1. Mai 2020).

[2] E. Biham und A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, 19. Juli 1990. [Online] Available: `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.31.2000&rep=rep1&type=pdf` (Abrufdatum 23. Mai 2020).

[3] C. D, *The Data Encryption Standard (DES) and its strength against attacks*, Mai 1994. [Online] Available: `https://ieeexplore.ieee.org/abstract/document/5389567`.

[4] T. M. Tutoials. (24. Dez. 2016). Kryptographie #98 - differentielle Kryptoanalyse von DES, [Online] Available: `https://www.youtube.com/watch?v=JoNP1U0leao&t=499s` (Abrufdatum 23. Mai 2020).

[5] *Differenzielle kryptoanalyse*, in *Wikipedia*, 1. Mai 2019. [Online] Available: `https://de.wikipedia.org/w/index.php?title=Differenzielle_Kryptoanalyse&oldid=188123152` (Abrufdatum 23. Mai 2020).