Fachhochschule Nordwestschweiz
Hochschule für Technik

Differentielle Kryptoanalyse

Artikel Kryptographie
Windisch, 23. Mai 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

Inhaltsverzeichnis

1 Einleitung

Kryptosysteme sind Funktionen, welche darauf basieren mehrere Runden zu durchlaufen. Bei einer Runde von DES sind verschiedene Funktionen enthalten. Es gibt eine Bit-Permutation, arithmetische Operationen, XOR-Verknüpfungen und die S-Boxen. Die S-Boxen sind nichtlineare Übersetzungstabellen. Der gesamte Verschlüsselungsalorythmus, die Permutations-Tabellen wie auch die Übersetzungstabellen der S-boxen sind öffentlich bekannt. Die Geheimhaltung der Daten hängt also vom zufällig gewählten geheimen Schlüssel ab. Bei der Differenziellen Kryptoanalyse wird ein statischer Angriff auf den Verschlüsselungsalgorythmus durchgeführt, bei dem der Angreifer selbstgewählte Klartext und Geheimtextpaare verwenden kann. Es handelt sich also um eine chosen plaintext attack.

Wird ein Klartextangriff durchgeführt, kann die Komplexität der DES Verschlüsselung in einer Runde um die Hälfte reduziert werden, da die Symmetrie durch Komplementierung genutzt werden kann.

Es werden Differenzen in den Klartextpaaren auf Differenzen in den Geiheimtextpaaren analysiert. Diese Differenzen werden verwendet um mögliche Schlüssel Wahrscheindlichkeiten zuzuordnen und den wahrscheinlichsten Schlüssel zu finden. Bei Anwendung dieser Methode auf den DES nimmt die Komplexität der Verschlüsselung mit der Anzahl der Runden zu, wobei sich die Differenziellekryptoanalyse nicht mehr bewehrt bei 16 Runden, im Bezug auf eine brute-force attack.

$$T = DES(P, K)$$

$$\bar{T} = DES(\bar{P}, \bar{K})$$

Somit entspricht der Wert X dem Bitweise komplementierten Wert $\bar{X}$. Die Eigenschaft wird bei der Kryptonanalyse ausgenutzt indem zwei Klartext-Textpaare P_1, T_1 und P_2, T_2 zur Verfügung stehen und es gilt $P_1, \bar{T}_2$ oder $P_2, \bar{T}_1$. Der Angreifer verschlüsselt P_1 unter allen 2^{55} Schlüsseln K, deren niederwertigstes Bit Null ist. Wenn im Geheimtext der Wert T gleich dem Wert T_1 ist, dann ist der entsprechende Schlüssel K wahrscheinlich der echte Schlüssel. Ist T gleich dem Wert $\bar{T}_2$ dann ist der Schlüssel wahrscheinlich $\bar{K}$.

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.

Der Data Encription Standard (DES) war in den 70 Jahren das damals 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.

Du, ich glaube dass ist ein anderes Verfahren welches eine Brutforce attacke einfach doppelt so schnell macht bei wenig Runden. Aber das beschreibt nicht die Differenzielle Analyse ;) Ich glaube diesen Teil kann man weglassen.

3 Funktionsweise

Folglich soll die Funktionsweise einer differenziellen Kryptoanalyse auf eine Runde vom Data Encryption Standard (DES) erläutert werden (Es wird nur die rechte Seite einer DES-Runde betrachtet). 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. Die Abbildung 3.1 zeigt wie sich eine Differenz durch das Netzwerk verhält.

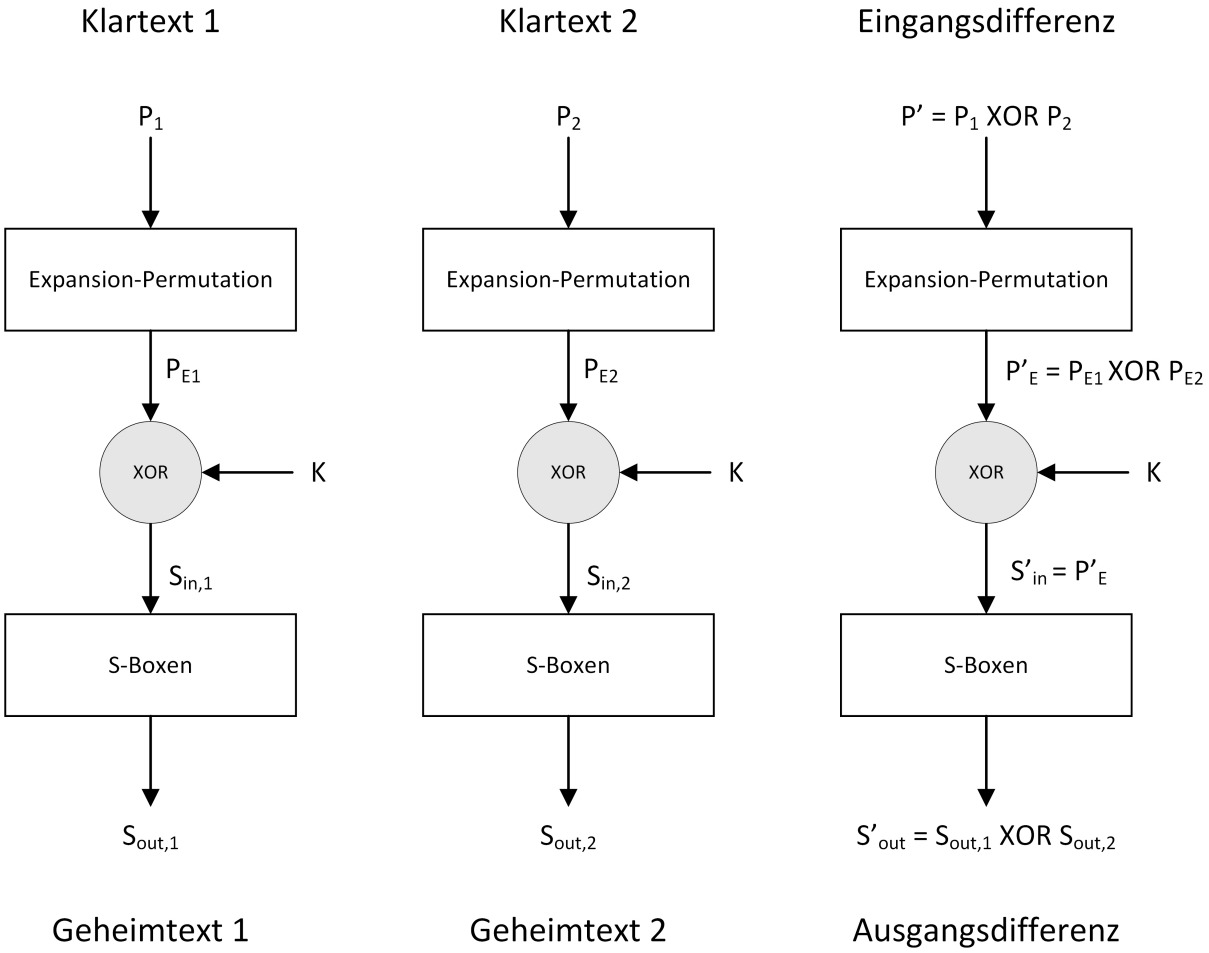

Abbildung 3.1: Verhalten von Klartext 1, 2 und der Differenz davon durch die Feistelstruktur einer Runde von DES [2]

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 aufhebt 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 können die S-Boxen genauer analysiert werden. Wie bereits in der Einleitung erwähnt, sind die S-Boxen nicht-lineraren Funktion. Um diese zu umgehen kann mit

Wahrscheinlichkeiten gearbeitet werden. Anhand der öffentlich zugänglichen S-Boxen kann eine Differenzenverteilungstabelle aufgestellt werden. In dieser wird für jede Eingangsdifferenz die Zahl Wertepaar gegeben welche eine bestimmte Ausgangsdifferenz erzeugen. Es gibt bei DES $2^6 = 64$ verschieden mögliche Eingangsdifferenzen pro S-Box. 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 [3][4].

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.

4 Anwendung

In der Funktionsweise wurde bis jetzt lediglich eine Runde von DES durchgelaufen. Es braucht nur wenige Klartext-Geheimtext Paare damit der Schlüssel für eine Runde ermittelt werden kann. Biham und Shamir haben weiter gezeigt, dass die Differenzielle Kryptoanalyse auf 2 Runden und mehr erweitert werden kann, doch umso höher die Anzahl Runden desto schwieriger die Entschlüsselung. Es muss mit den Wahrscheinlichkeiten aus der Differenzenverteilungstabelle weiter gerechnet werden. Bei 16 Runden wird die Wahrscheinlichkeit den richtigen Schlüssel zu finden so klein, dass ein Brut-force Attacke genau so schneller wäre. Die differenzielle Kryptoanalyse ist hingegen effizient bei anderen DES-ähnliche 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 [4].

5 Schluss

Literatur

[1] Thirah. (). Vorhängeschloss-schlüssel-computer-icons, cleanpng.com. Library Catalog: de.cleanpng.com, [Online] Available: `https://de.cleanpng.com/png-qhshuq/` (Abrufdatum 1. Mai 2020).

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

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

[4] 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).