# Übung zur Vorlesung „Sicherheit“
08.05.2014 – Übungsblatt 2

Florian Böhl
florian.boehl@kit.edu

# Abgabe der Übungsblätter

# Sicherheit – Übungsblatt 2 – Aufgabe 1

Aus der Vorlesung ist bekannt, dass eine Blockchiffre im CBC-Modus IND-CPA-sicher ist, wenn $E : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$, für $k, l \in \mathbb{N}$, ununterscheidbar von einer echt zufälligen Funktion ist und der Initialisierungsvektor $IV$ für jeden Verschlüsselungsvorgang neu gleichverteilt zufällig gezogen wird. Wir betrachten nun den Fall, dass $IV$ fest und für jeden Verschlüsselungsvorgang gleich gewählt wird oder $IV$, ausgehend von einer fixen Wahl, bei jedem Verschlüsselungvorgang um 1 hochgezählt wird. Geben Sie für diese beiden Fälle jeweils einen Angreifer an, der das IND-CPA-Spiel immer gewinnt.

# Fazit

- Begriff: „IND-CPA-Sicherheit“
- Randomisierte Verschlüsselung *notwendig* für IND-CPA-Sicherheit
- Intuitiv: IND-CPA-Sicherheit schützt vor passiven Angreifern

# Sicherheit – Übungsblatt 2 – Aufgabe 2

**XTS**:

- Tweak: $T \in \{0,1\}^t$ mit $t \in \mathbb{N}$
- Blockchiffre: $\mathsf{E}, \mathsf{D} : \{0,1\}^{\frac{k}{2}} \times \{0,1\}^\ell \to \{0,1\}^\ell$
- Padding: $\mathsf{PAD} : \{0,1\}^* \to \{0,1\}^\ell$
- $\mathsf{E}_{\mathsf{TWEAK}}, \mathsf{D}_{\mathsf{TWEAK}} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^l \to \{0,1\}^\ell$, für $k, t, \ell \in \mathbb{N}$
- Für $T := (T' || i)$ und $M \in \{0,1\}^\ell$

$$X := \mathsf{E}(K_2, T')$$

$$\mathsf{E}_{\mathsf{TWEAK}}(K, T, M) := \mathsf{E}(K_1, (M \oplus \mathsf{PAD}(X||i))) \oplus \mathsf{PAD}(X||i)$$

# Sicherheit – Übungsblatt 2 – Aufgabe 2

XTS findet unter anderem mit AES als “innere” Blockchiffre im “OS X Mountain Lion“-Betriebssystem (in der ”FileVault 2“-Applikation) und im (Festplatten-)Datenverschlüsselungsverfahren TrueCrypt Anwendung. Dabei sieht ein Chiffrat, mit $T_i := (T' || i)$, wie folgt aus:

$$(C_1, C_2, \dots) = (\mathrm{E}_{\mathrm{TWEAK}}(K, T_1, M_1), \mathrm{E}_{\mathrm{TWEAK}}(K, T_2, M_2), \dots).$$

# Sicherheit – Übungsblatt 2 – Aufgabe 2

(a) Welche Vorteile hat dieses Verfahren gegenüber dem CBC-Modus, wenn wir als Anwendungszweck Festplattenverschlüsselung anschauen? (Gibt es Nachteile?)

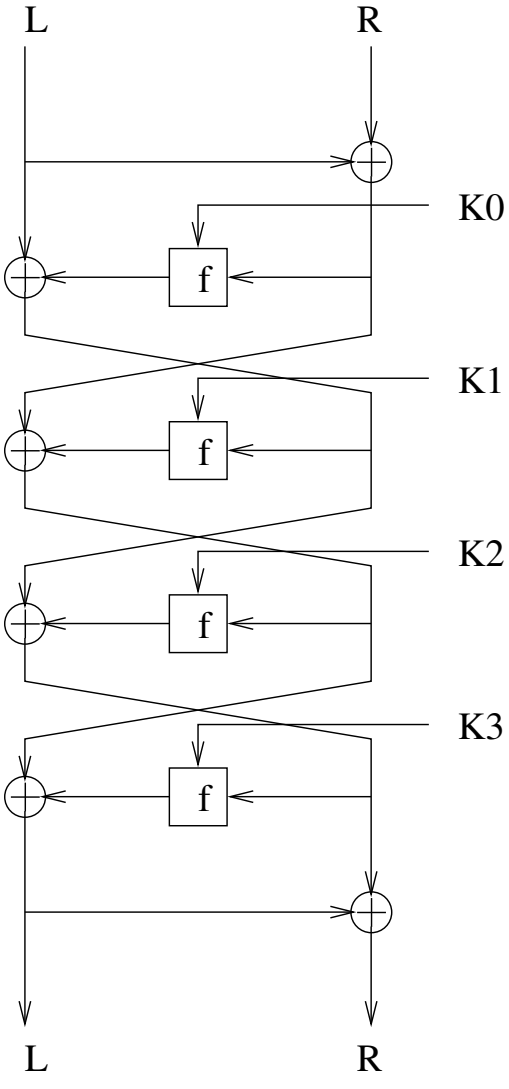
# Sicherheit – Übungsblatt 2 – Aufgabe 2

(b) Nehmen wir eine Variante des XTS-Verfahrens an, sodass $X := T'$ gilt. ($T'$ wird also nicht unter $K_2$ verschlüsselt.) Was passiert, wenn Sie die zwei Chiffretexte $C_1 := \mathrm{E}_{\mathrm{TWEAK}}(K, (T'||1), \mathrm{PAD}(T'||1))$ und $C_2 := \mathrm{E}_{\mathrm{TWEAK}}(K, (T'||2), \mathrm{PAD}(T'||2))$ XOR-verknüpfen?

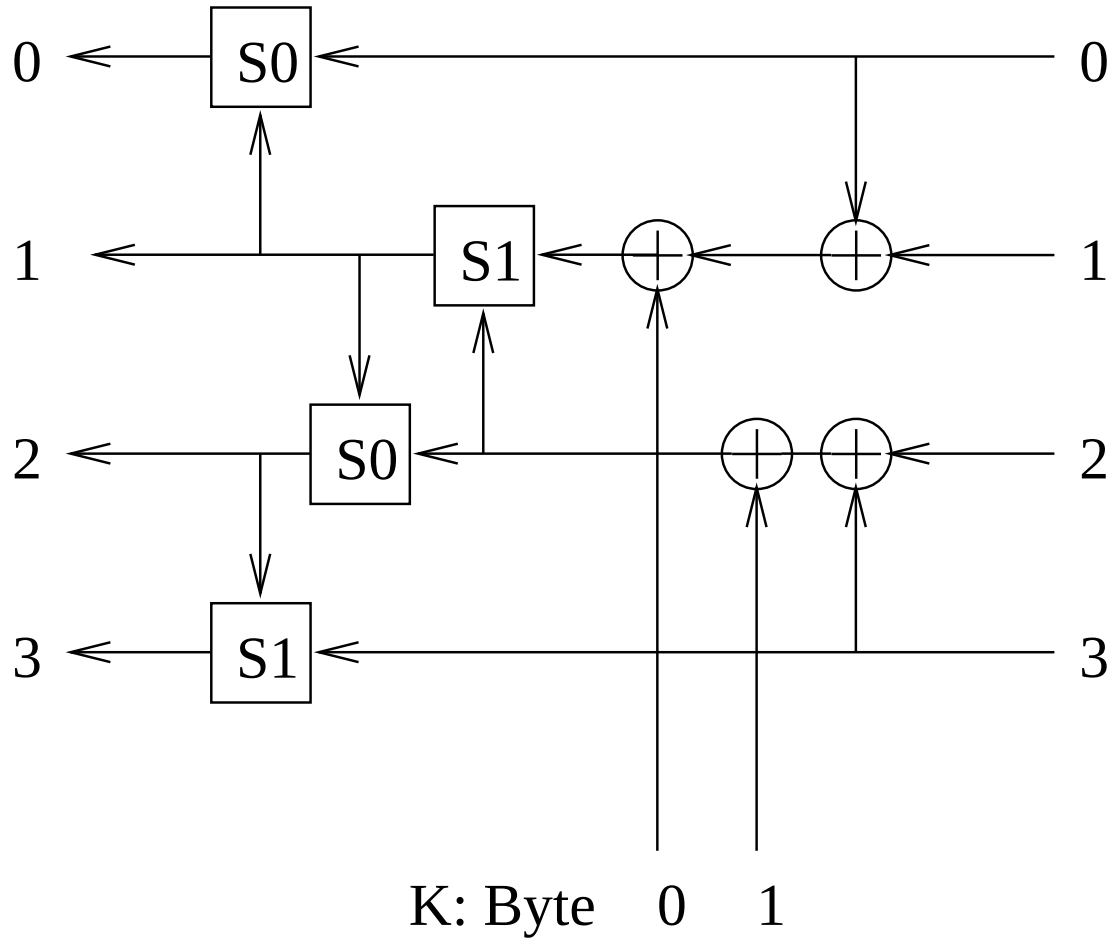
# Sicherheit – Übungsblatt 2 – Aufgabe 2

(c) Python-Skript: Siehe Musterlösung.

# Sicherheit – Übungsblatt 2 – Aufgabe 3



# Sicherheit – Übungsblatt 2 – Aufgabe 3



# Sicherheit – Übungsblatt 2 – Aufgabe 3

(a) Geben Sie die Gleichungen an, die die beiden anderen $S$-Boxen liefern.

# Sicherheit – Übungsblatt 2 – Aufgabe 3

(b) Geben Sie die 3-Runden Charakteristiken an, die sich durch die Gleichung zur ersten und dritten S-Box ergeben.

# Sicherheit – Übungsblatt 2 – Aufgabe 3

(c) Beschreiben Sie das Vorgehen der linearen Kryptoanalyse, das die vier Charakteristiken verwendet.

# Sicherheit – Übungsblatt 2 – Aufgabe 3

(d) Bei wievielen Klartext/Chiffrat-Paaren erwarten Sie einen Erfolg der Analyse?
Empirisch funktioniert der Angriff bei etwa 15 Paaren problemlos. Wie erklärt sich der Unterschied zu dem geschätzten Wert (falls er abweicht)?

# Sicherheit – Übungsblatt 2 – Aufgabe 4

Symmetrische Verschlüsselungsverfahren in der Praxis: Wählen Sie drei (verbreitete) kryptographische Protokolle bzw. drei Programme aus, in denen symmetrische Verschlüsselungsverfahren zum Einsatz kommen. Welche Chiffren werden jeweils verwendet? (Bei Blockchiffren: Welche Modi werden benutzt? Wie wird ggf. der Initialisierungsvektor gewählt?) Woher kommt der verwendete Schlüssel?