Karlsruhe Institute of Technology

Institut für Theoretische Informatik
Jun.-Prof. Dr. D. Hofheinz

Stammvorlesung Sicherheit im Sommersemester 2014

Übungsblatt 2

Hinweis: Übungsblätter können freiwillig bei Florian Böhl, Raum 255, Geb. 50.34 („Info-Bau“) zur Korrektur abgegeben werden. Die Korrektur dient nur der Selbstkontrolle; es gibt keine Punkte und keinen Klausur-Bonus.

Aufgabe 1. Aus der Vorlesung ist bekannt, dass eine Blockchiffre im CBC-Modus IND-CPA-sicher ist, wenn $\mathsf{E} : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$, 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 (dabei wird nicht zwischen Verschlüsselungsvorgängen des Orakels und des Experiments unterschieden). Geben Sie für diese beiden Fälle jeweils einen Angreifer an, der das IND-CPA-Spiel immer gewinnt.

Aufgabe 2. Wir erweitern unsere Blockchiffre-Definition aus der Vorlesung um eine zusätzliche Eingabe $T \in \{0,1\}^t$ mit $t \in \mathbb{N}$, die wir *Tweak* nennen. Sei $\mathsf{E}_{\mathsf{TWEAK}}, \mathsf{D}_{\mathsf{TWEAK}} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^l \to \{0,1\}^l$, für $k, t, l \in \mathbb{N}$. Weiterhin sei $\mathsf{E}, \mathsf{D} : \{0,1\}^{\frac{k}{2}} \times \{0,1\}^l \to \{0,1\}^l$ eine „sichere“ Blockchiffre (beispielsweise AES) und $\mathsf{PAD} : \{0,1\}^* \to \{0,1\}^l$ eine sogenannte Padding-Funktion, die Eingaben beliebiger aber fester Länge deterministisch auf die Bitlänge l abbildet. Für einen Schlüssel $K = (K_1, K_2) \in (\{0,1\}^{\frac{k}{2}})^2$, einen Index $i \in \mathbb{N}$, einen Tweak $T := (T'||i) \in \{0,1\}^t$ (T' beliebig) und einen Klartext $M \in \{0,1\}^l$ gelte

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

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

(Mit $||$ bezeichnen wir die Konkatenation von (Bit-)Strings.) Die Entschlüsselung $\mathsf{D}_{\mathsf{TWEAK}}(K, T, M)$ sei kanonisch so definiert, dass $\mathsf{D}_{\mathsf{TWEAK}}(K, T, \mathsf{E}_{\mathsf{TWEAK}}(K, T, M)) = M$ für alle K, T, M gilt. Ein Betriebsmodus, der die oben gegebene Blockchiffre nutzt, wird XTS-Modus genannt. Dabei sieht ein Chiffrat mit $T_i := (T'||i)$ wie folgt aus:

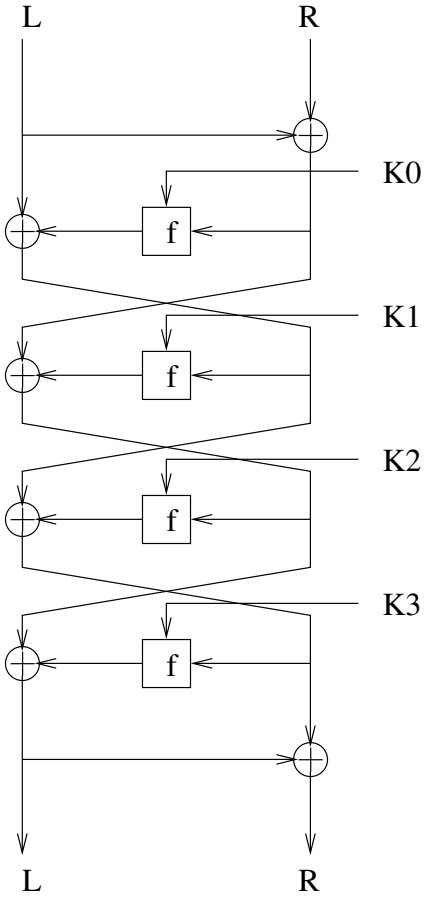
$$(C_1, C_2, \dots) = (\mathsf{E}_{\mathsf{TWEAK}}(K, T_1, M_1), \mathsf{E}_{\mathsf{TWEAK}}(K, T_2, M_2), \dots).$$

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

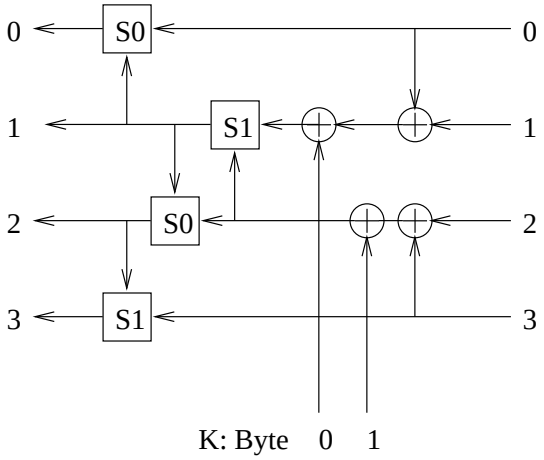
(b) Nehmen wir eine Variante des XTS-Verfahrens an, sodass $X := T'$ gilt. (T' wird also nicht unter K_2 verschlüsselt.) Was passiert, wenn Sie die zwei Chiffretexte $C_1 := \mathsf{E}_{\mathsf{TWEAK}}(K, (T'||1), \mathsf{PAD}(T'||1))$ und $C_2 := \mathsf{E}_{\mathsf{TWEAK}}(K, (T'||2), \mathsf{PAD}(T'||2))$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

(c) Zusatzaufgabe. Schreiben Sie ein Programm (beispielsweise ein Python-Skript), das den XTS-Betriebsmodus implementiert. (Hinweis: Für die ”innere“ Blockchiffre im XTS-Verfahren können Sie zum Beispiel die AES-Implementierung aus PyCrypto (`http://pythonhosted.org/pycrypto/`)) verwenden. Im AES-Fall würde $l = 128$ gelten. Als Padding-Funktion können Sie $\mathsf{PAD}(X||i) := 2^i \cdot X \bmod 2^l$ nutzen.

Aufgabe 3. Eine leicht vereinfachte Version des FEAL-4 (siehe auch `http://de.wikipedia.org/wiki/FEAL`) soll durch lineare Kryptoanalyse gebrochen werden:



Die f-Funktion und die S-Boxen ($S_i(a,b) := rot2((a+b+i) \mod 256)$ sind gegenüber dem Original nicht verändert:



Der Ausgangspunkt für eine lineare Approximationen der f-Funktion ist das jeweils letzte Bit der Addition der 4 S-Boxen, bei dem gegenüber allen anderen Bits kein Übertrag auftreten kann. Die ersten beiden S-Boxen liefern die Gleichungen:

- $F[2] = B[0] + F[8]$ und
- $F[10] = 1 + B[0] + B[8] + K[0] + B[16] + B[24] + K[8]$ (hier geht auch der Schlüssel mit ein!),

wobei $F[i]$ das i-te Ausgabebit von f ist; $B[i]$ und $K[i]$ entsprechend das i-te Eingabe- bzw. Schlüsselbit.

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

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

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

(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)?

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?