Anleitung zu Aufgabe 2.5

Machen Sie eine Aussage über die Sicherheit der Counter-Mode-Verschlüsselung (Aufgabe 2.3) für Mehrfachverschlüsselung, ausgehend von der PRP-Sicherheit der verwendeten Blockchiffre!

Gesucht ist eine Ungleichung zu RoR-CPA-Vorteil und PRP-Vorteil, die die folgenden Parameter zu den Anfragen des Angreifers an das Verschlüsselungsorakel berücksichtigen sollte:

- Die maximale Anzahl $q_\#$ der Anfragen;
- die jeweilige Maximallänge q_B pro Anfrage, gerechnet in Blocks zu ℓ Bits.

Als wichtiger Schritt zur Lösung betrachten Sie zunächst ein anderes Szenario: Als Verschlüsselungsschema dient die Counter-Mode-Verschlüsselung analog wie in Aufgabe 2.3 (für Details siehe die Musterlösung zu Aufgabe 2.3), jedoch ganz ohne die Blockchiffre E_K und statt dessen mit einer *gleichverteilt zufälligen Abbildung* $f\colon \{0,1\}^\ell \to \{0,1\}^\ell$.

(Das ist nur ein Gedankenexperiment, denn das lässt sich praktisch – außer für winziges ℓ – nicht realisieren. Hier können Sie $\mathrm{Func}(\{0,1\})^\ell$ als Schlüsselmenge $\mathcal{K}$ ansehen: Ein Element $f \in \mathcal{K}$ steht für sich selbst, das heißt, f als Abbildung ist die „Blockchiffre-Verschlüsselung“ zu einem „Schlüssel“ f.)

Welche obere Schranke für den RoR-CPA-Vorteil beliebiger Angreifer können wir in diesem Szenario angeben (abhängig von $q_\#$ und q_B)?

Sie können die Aufgabe zunächst vereinfacht für $q_B = 1$ angehen und annehmen, dass $\boldsymbol{A}$ nur Anfragen genau der Länge ℓ verwendet. Mit dieser Vereinfachung haben wir es mit folgendem Szenario zu tun:

- Ein Angreifer $\boldsymbol{A}$ hat Zugriff auf ein “Real”-Verschlüsselungsorakel $E_1(\cdot)$ oder ein “Random”-Verschlüsselungsorakel $E_0(\cdot)$.
- $f\colon \{0,1\}^\ell \to \{0,1\}^\ell$ ist gleichverteilt zufällig gewählt; das heißt, die Funktionswerte $f(x)$ sind gleichverteilt zufällige Elemente von $\{0,1\}^\ell$ und stochastisch unabhängig.
- Das Orakel $E_1(\cdot)$ beantwortet Anfragen $m \in \{0,1\}^\ell$, indem es $iv \in_\$ \{0,1\}^{\ell/2}$ wählt und $iv \,\|\, m \oplus f(iv \,\|\, 000\ldots000)$ zurückgibt.

  Das Orakel $E_0(\cdot)$ dagegen beantwortet Anfragen $m \in \{0,1\}^\ell$, indem es $iv \in_\$ \{0,1\}^{\ell/2}$ und $m_0 \in_\$ \{0,1\}^\ell$ wählt und $iv \,\|\, m_0 \oplus f(iv \,\|\, 000\ldots000)$ zurückgibt.
- Der Angreifer $\boldsymbol{A}$ versucht, mit höchstens $q_\#$ Anfragen an das Orakel herauszufinden, ob es sich dabei um das “Real”-Verschlüsselungsorakel handelt oder um das “Random”-Verschlüsselungsorakel. Am Ende gibt $\boldsymbol{A}$ ein Bit aus, 1 für “real” oder 0 für “random”.

Wir schreiben $\boldsymbol{A}^{E_1(\cdot)}$, um den Fall dieses Angriffsspiels zu bezeichnen, in dem $\boldsymbol{A}$ mit dem “Real”-Verschlüsselungsorakel interagiert. $\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1$ steht für das Ereignis, dass $\boldsymbol{A}$ unter dieser Voraussetzung das Bit 1 ausgibt; $\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 0$ für das Ereignis, dass $\boldsymbol{A}$ das Bit 0 ausgibt.

Für den Fall mit dem “Random”-Verschlüsselungsorakel schreiben wir $\boldsymbol{A}^{E_0(\cdot)}$. Also heißt $\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1$ bzw. $\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 0$, dass $\boldsymbol{A}$ im “Random”-Fall das Bit 1 bzw. das Bit 0 ausgibt.

Wir wollen eine obere Schranke finden für den ROR-CPA-Vorteil

$$\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} = \Pr\left[\boldsymbol{A}^{\mathsf{E}_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{\mathsf{E}_0(\cdot)} \Rightarrow 1\right]$$

eines beliebigen Angreifers $\boldsymbol{A}$, der das Orakel höchstens $q_\#$ mal befragt. Dafür reicht es nicht, $\Pr\left[\boldsymbol{A}^{\mathsf{E}_1(\cdot)} \Rightarrow 1\right]$ oder $\Pr\left[\boldsymbol{A}^{\mathsf{E}_0(\cdot)} \Rightarrow 1\right]$ alleine zu betrachten! Jede dieser Wahrscheinlichkeiten könnte 1 sein (z. B. bei einem Angreifer $\boldsymbol{A}$, der *immer* das Bit 1 ausgibt). Eine sinnvolle obere Schranke können wir nur für die Differenz erhalten.

Betrachten Sie dafür zunächst den Fall $q_\# = 1$. Wie ist die Orakelantwort $\mathsf{E}_1(\cdot)$ verteilt? Wie ist die Orakelantwort $\mathsf{E}_0(\cdot)$ verteilt?

In beiden Fällen haben wir eine Gleichverteilung (unabhängig von m). Warum?

Daraus folgt für $q_\# = 1$ zwangsläufig $\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} = 0$. Warum?

Betrachten Sie als nächstes $q_\# = 2$. Es kann also zwei Orakelanfragen geben mit entsprechenden Antworten, beide entweder vom "Real"-Orakel oder vom "Random"-Orakel.

Wenn nicht ein bestimmtes Ereignis C eintritt, sieht $\boldsymbol{A}$ auch hier von beiden Orakeln das gleiche Verhalten. Was macht dieses Ereignis aus? Was ist seine Wahrscheinlichkeit $\Pr[C]$?

Hier können wir folgern

$$\left|\Pr\left[\boldsymbol{A}^{\mathsf{E}_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{\mathsf{E}_0(\cdot)} \Rightarrow 1\right]\right| \leq \Pr[C].$$

Damit haben wir $\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} \leq \Pr[C]$ gezeigt! Wir haben hier also eine obere Schranke.

Gehen Sie anschließend zum allgemeinen Fall mit beliebigem $q_\#$. Auch dort können Sie ein Ereignis C angeben, dessen Wahrscheinlichkeit $\Pr[C]$ bestimmen und folgern $\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} \leq \Pr[C]$.

Wenn Sie bis hier gekommen sind, betrachten Sie auch für q_B den allgemeinen Fall! Gemäß dem Lösungsvorschlag zu Aufgabe 2.3 können wir annehmen $q_B \leq 2^{\ell/2}$. Ändert sich etwas an der obere Schranke für $\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$?

Bis hier haben wir es mit einer gleichverteilt zufälligen Abbildung $f\colon \{0,1\}^\ell \to \{0,1\}^\ell$ zu tun, nicht mit einer Blockchiffre E_K. Als Zwischenergebnis haben wir eine obere Schranke für $\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$ bei Counter-Mode-Verschlüsselung mit $f \in \mathrm{Func}(\{0,1\}^\ell)$ erhalten.

Haben Sie eine Idee, wie sich von diesem Zwischenergebnis ein Ergebnis für die eigentliche Aufgabenstellung herleiten lässt, also eine obere Schranke für $\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$ bei Counter-Mode-Verschlüsselung mit einer Blockchiffre E_K?