Lemma 15

Doplnění důkazu

V práci byla IND-CPA bezpečnost zavedena pomocí experimentu RoR (Real or Random), ve kterém je cílem útočníka rozlišit mezi zašifrovanou jím zvolenou zprávou a zašifrovanou náhodně zvolenou zprávou (viz kapitola 2.2). IND-CPA bezpečnost lze zavést i pomocí jiných experimentů. Ukazuje se, že tyto různé definice jsou ekvivalentní.

Označme RoZ experiment, ve kterém je cílem útočníka rozlišit mezi zašifrovanou jím zvolenou zprávou a zašifrovanou nulovou zprávou. Pro úplnost důkazu Lemmatu 15 je třeba dokázat následující implikaci

$$\text{RoZ-IND-CPA bezpečnost} \Rightarrow \text{RoR-IND-CPA bezpečnost.}$$

Důkaz. Důkaz provedeme nepřímo. Mějme úspěšného RoR-IND-CPA útočníka $\mathcal{A}$. Ukážeme, že pak existuje simulátor $\mathcal{S}$, který bude úspěšným RoZ-IND-CPA útočníkem.

1. Buď tajně zvolen bit $b \leftarrow U(\{0,1\})$ a vygenerován klíč $(sk, pk) \leftarrow \mathsf{Gen}(1^n)$. Zveřejní se vyjádření bezpečnostního parametru 1^n a veřejný klíč pk.
2. $\mathcal{S}$ tajně zvolí bit $c \leftarrow U(\{0,1\})$.
3. $\mathcal{A}$ pošle dotaz na zprávu $m \in \mathcal{P}$.
4. $\mathcal{S}$ pošle dotaz orákulu
$$m' = \begin{cases} r, \text{ kde } r \leftarrow U(\mathcal{P}) \wedge |r| = |m|, & \text{pokud } c = 0, \\ m, & \text{pokud } c = 1. \end{cases}$$
5. $\mathcal{O}$ vrací šifrový text
$$y = \begin{cases} \mathsf{Enc}_{pk}(0^{|m'|}), & \text{pokud } b = 0, \\ \mathsf{Enc}_{pk}(m'), & \text{pokud } b = 1. \end{cases}$$
6. $\mathcal{S}$ přepošle šifrový text y.
7. $\mathcal{A}$ vypustí c^* (odhad bitu c).
8. $\mathcal{S}$ vypustí $b^* = c + c^* + 1$ (odhad bitu b).

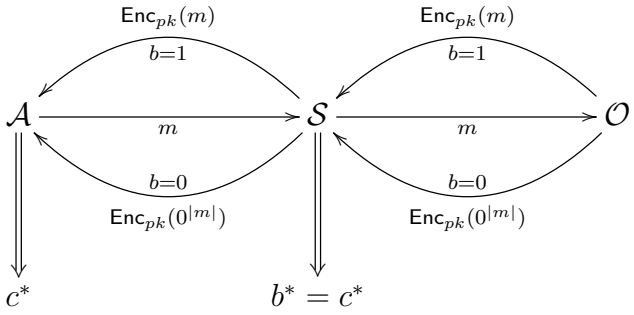
Simulace je znázorněná na Obrázcích 1,2.

Pokud $b = 1$, tak simulátor věrně simuluje RoR-IND-CPA experiment, tedy platí

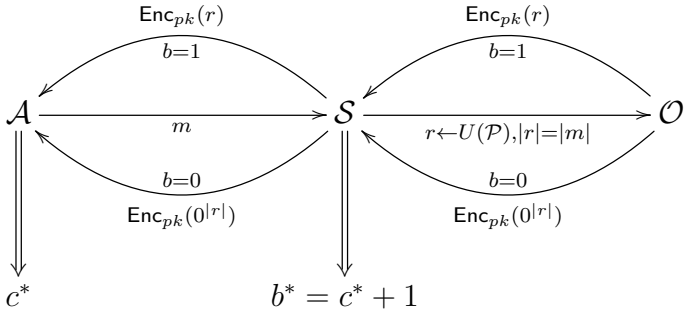
$$|\Pr[c^* = 1 \mid c = 1 \wedge b = 1] - \Pr[c^* = 1 \mid c = 0 \wedge b = 1]| = \mathrm{Adv}^{\mathrm{RoR}}(\mathcal{A}). \tag{1}$$

Pokud $b = 0$, tak útočník dostává pro obě možná c zašifrovanou nulovou zprávu stejné délky. Tedy odpověď simulátoru pro $b = 0$ nezávisí na hodnotě c. Tedy ani útočníkův odhad c^* nezávisí na hodnotě c. Tedy platí, že

$$|\Pr[c^* = 1 \mid c = 1 \wedge b = 0] - \Pr[c^* = 1 \mid c = 0 \wedge b = 0]| = \mathsf{negl}(n). \tag{2}$$



Obrázek 1: Průběh simulace v případě, že $c = 1$.



Obrázek 2: Průběh simulace v případě, že $c = 0$.

Dle definice advantege platí, že

$$\mathrm{Adv}^{\mathrm{RoZ}}(\mathcal{A}) = |\Pr[b^* = 1 \mid b = 1] - \Pr[b^* = 1 \mid b = 0]|. \tag{3}$$

Pomocí věty o úplné pravděpodobnosti (Tvrzení 1), rovností (1),(2) a toho, že $b^* = c^* + c + 1$ dostáváme vztah

$$\mathrm{Adv}^{\mathrm{RoZ}}(\mathcal{A}) = \frac{1}{2}|\mathrm{Adv}^{\mathrm{RoR}}(\mathcal{S}) - \mathrm{negl}(n)|.$$

Důkaz je podobný důkazu Lemmatu 40 v bakalářské práci. Proto zde podrobný výpočet advantage není uveden. □