12. 10. 2017

Tvrzení: Pokud (G, E, D) splňuje perfect secrecy, pak platí $|\mathcal{K}| \geq |\mathcal{M}|$.

Důkaz: Nechť $|\mathcal{K}| < |\mathcal{M}|$. Nechť M je rovnoměrné pravděpodobnostní rozdělení na $\mathcal{M}$. Nechť $c \in \mathcal{C}$:

$Pr[E_k(M) = c] > 0$

$\mathcal{M}(c) := \{m \mid m = D_k(c) \text{ pro } k \in \mathcal{K}\}$

Platí $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$, tedy $\exists m' \in \mathcal{M} : m' \notin \mathcal{M}(c)$.

Závěrem dostáváme: $Pr[M = m' \mid \mathcal{C} = c] = 0 \neq Pr[M = m'] = 1/|\mathcal{M}|$ □

Kde můžeme slevit v nárocích na bezpečnost? První možností je předpokládat, že Eve je stále výpočetně neomezená, což vede na statistical security.

Statistical security

Definice: Nechť X, Y jsou náhodné proměnné nad S. Řekneme, že X, Y jsou *statistically ε-indistinguishable*, pokud

$$\forall T \subseteq S : |Pr[X \in T] - Pr[Y \in T]| \leq \varepsilon.$$

T je statistický test.

Definice: (G, E, D) splňuje *statistical ε-indistinguishability*, pokud $\forall m_0 \, \forall m_1 \in \mathcal{M}$ jsou náhodné proměnné $E_k(m_0)$ a $E_k(m_1)$ statistically ε-indistinguishable, tj.

$$|Pr[E_k(m_0) \in T] - Pr[E_k(m_1) \in T]| \leq \varepsilon.$$

Adversary má pravděpodobnost $\leq \varepsilon$ nalézt m z c.

Podobně jako pro perfect secrecy platí $|\mathcal{K}| \geq (1 - \varepsilon)|\mathcal{M}|$.

Computational security

Jaká je výhoda kryptografie s důkazy? Z důkazů lze odvodit rozumný parametr, který nám dá délky klíčů, a napoví, s jakou pravděpodobností adversary prolomí protokol.

Asymptotická formalizace

- "security parameter", Alice a Bob zvolí $n \in \mathbb{N}$
- Efektivní adversary PPT (probabilistic polynomial time), pro každý security parametr má program běžící čas $poly(n)$ (neuniformní)
- (G, E, D) v fixním polynomiálním čase
- $|\mathcal{M}|$ závisí na n: $\mathcal{M} = \bigcup_n \mathcal{M}_n$, kde např. $\mathcal{M}_n = \{0, 1\}^n$

Definice: Funkce $\varepsilon : \mathbb{N} \to [0, 1]$ je *negligible (zanedbatelná)*, pokud:

$$\forall c \in \mathbb{N} \, \exists n_c \in \mathbb{N} \, \forall n > n_c : \varepsilon(n) < \frac{1}{n^c}$$

Příkladem negligible funkcí jsou 2^{-n}, $n^{-\log(n)}$, $2^{-\sqrt{n}}$.

Definice: (G, E, D) na prostoru zpráv $\mathcal{M} = \bigcup_n \mathcal{M}_n$, kde délka všech zpráv v $\mathcal{M}_n$ je stejná, splňuje *indistinguishability ciphertextů*, pokud $\forall$ PPT A $\exists$ negligible ε takové, že

$$\forall m_0, m_1 \in \mathcal{M}_n : |Pr[A(E_k(m_0)) = 1] - Pr[A(E_k(m_1)) = 1]| \leq \varepsilon(n)$$

Pravděpodobnost je přes $k \leftarrow G(1^n)$ a náhodné mince E a A. Ciphertext má vždy délku $\geq n$.

Definice, kterou nebudeme používat: (ε, t) secure, pokud $\forall A$ běžící v čase t platí podmínka.

Asymptotická vs. konkrétní definice: t ve specifickém výpočetním modelu (2^{100} cyklů CPU) (G, E, D) v čase $\ll t$, $\varepsilon \leq 2^{-100}$

Cíl: (G, E, D), kde $|\mathcal{K}| \ll |\mathcal{M}$.

Příklad, který nefunguje:

Pravděpodobnostní OTP:

$\mathcal{K} = \{0,1\}^n$ $\mathcal{M} = \{0,1\}^{2n}$

$E_k(m) = i_1, \ldots, i_{2n} \leftarrow \{1, \ldots, n\}$

$c = (i_1, \ldots, i_{2n}, m \oplus (k_{i_1}, k_{i_2}, \ldots, k_{i_{2n}})$

$G(1^n) : k \leftarrow \{0,1\}^n$

Definice: (G, E, D) nad $\mathcal{M} = \bigcup_n \mathcal{M}_n$, kde délka všech zpráv v $\mathcal{M}_n$ je stejná, splňuje *guessing indistinguishability ciphertextů*, pokud $\forall$ PPT A $\exists$ negligible ε tak, že A zvítězí v následující hře s pravděpodobností nejvýše $\frac{1}{2} + \varepsilon(n)$.

1. A zvolí $m_0, m_1 \in \mathcal{M}_n$
2. $k \leftarrow G(1^n)$ a $b \leftarrow \{0,1\}$
3. A dostane $E_k(m_b)$ a vrátí b'
4. A zvítězí, pokud $b = b'$

Tvrzení: (G, E, D) splňuje indistinguishability ciphertextů právě tehdy, když splňuje guessing indistinguishability ciphertextů.

Důkaz: "$\Leftarrow$"Mějme $\mathcal{A}_i$ pro $m_0^*, m_1^* \in \mathcal{M}$, kde

$$|Pr[\mathcal{A}_i(E_k(m_0^*)) = 1] - Pr[\mathcal{A}_i(E_k(m_1^*)) = 1]| \geq \frac{1}{p(n)}$$

pro $p \in poly(n)$.

Zkonstruujeme $\mathcal{A}_{gi}$: 1) zvol m_0^*, m_1^* 3) pro c odpověz $\mathcal{A}_i(c)$

$\mathcal{A}_{gi}$ zvítězí s pravděpodobností $\geq \frac{1}{2} + \frac{1}{2p(n)}$.

"$\Rightarrow$"Obdobně.

Definice: (G, E, D) nad $\mathcal{M} = \bigcup_n \mathcal{M}_n$, kde délka všech zpráv v $\mathcal{M}_n$ je stejná, splňuje *semantic security*, pokud $\forall$ PPT A $\exists$ PPT A' takový, že pro všechna rozdělení M nad $\mathcal{M}$ a každou funkci $f : \mathcal{M} \to \{0,1\}^*$ platí:

$$Pr[A(E_k(M)) = f(M)] \leq Pr[A'(1^n) = f(M)] + \text{negl}(n)$$

Autory definice jsou Goldwasser a Micali. f je libovolná funkce jako například $f(m) = m$ nebo $f(m) = 50.$ bit m.

Tvrzení: (Bez důkazu) (G, E, D) splňuje semantic security právě tehdy, když splňuje indistinguishability ciphertextů.