9. 11. 2017

Věta: Nechť $G : \{0,1\}^n \to \{0,1\}^{n+1}$ je pseudonáhodný generátor. Definujeme $G_l(s_0) = b_1 b_2 \ldots b_l$, kde pro každé $i \in \{0, \ldots, l-1\}$ platí, že $s_{i+1} \parallel b_{i+1} = G(s_i)$. (Aplikací G na s_i získáme bit výstupu b_{i+1} a nový seed s_{i+1}.) Pak G_l je pseudonáhodný generátor s expanzí l pro každé $l \in \mathrm{poly}(n)$.

Důkaz: (pomocí hybridního argumentu)

Pro každé n a $0 \le j \le l$ položíme $H_n^j := U_j \parallel G_{l-j}(U_n)$, kde U_k je rovnoměrné rozdělení délky k. Speciálně platí, že $H_n^0 = G_l(U_n)$ a $H_n^l = U_l$.

Dále nechť D je PPT distinguisher pro G_l. Potřebujeme ukázat, že pro každé n platí, že

$$|\Pr[D(G(U_n)) = 1] - \Pr[D(U_l) = 1]| \le \mathrm{neg}(n).$$

Pomocí D zkonstruujeme distinguisher D' pro G.

$D'(w)$: $\qquad w \in \{0,1\}^{n+1}$

1. $j \leftarrow \{1, \ldots, l\}$, $w = s_j \parallel b_j$;
2. $b_1, \ldots, b_{j-1} \leftarrow \{0,1\}$;
3. $b_{j+1}, \ldots, b_l \leftarrow G_{l-j}(s_j)$;
4. vrať $D(b_1, \ldots, b_l)$;

Nechť D' zvolí $j = j^*$.

- Pro $w \leftarrow U_{n+1}$ dostane D distribuci odpovídající $H_n^{j^*}$. Pak platí, že

$$\Pr[D'(U_{n+1}) = 1 \mid j^* = j] = \Pr\left[D\left(H_n^{j^*}\right) = 1\right],$$

$$\Pr[D'(U_{n+1}) = 1] = \frac{1}{l} \sum_{j^*=1}^{l} \Pr\left[D\left(H_n^{j^*}\right) = 1\right].$$

- Pro $w \leftarrow G(U_n)$ dostane D distribuci odpovídající $H_n^{j^*-1}$. Potom platí, že

$$\Pr[D'(G(U_n)) = 1 \mid j^* = j] = \Pr\left[D\left(H_n^{j^*-1}\right) = 1\right],$$

$$\Pr[D'(G(U_n)) = 1] = \frac{1}{l} \sum_{j^*=1}^{l} \Pr\left[D\left(H_n^{j^*-1}\right) = 1\right] = \frac{1}{l} \sum_{j^*=0}^{l-1} \Pr\left[D\left(H_n^{j^*}\right) = 1\right].$$

Pro nějakou negligible funkci ε dostáváme, že

$$\varepsilon(n) > |\Pr[D'(G(U_n)) = 1] - \Pr[D'(U_{n+1}) = 1]| =$$

$$= \frac{1}{l} \left| \sum_{j^*=0}^{l-1} \Pr\left[D\left(H_n^{j^*}\right) = 1\right] - \sum_{j^*=1}^{l} \Pr\left[D\left(H_n^{j^*}\right) = 1\right] \right| =$$

$$= \frac{1}{l} \left| \Pr\left[D\left(H_n^0\right) = 1\right] - \Pr\left[D\left(H_n^l\right) = 1\right] \right|.$$

Tedy $\left|\Pr[D(H_n^0) = 1] - \Pr\left[D\left(H_n^l\right) = 1\right]\right| < l\varepsilon(n)$, což je stále negligible funkce.

□

Z tvrzení z minulé přednášky (PRG s expanzí 1 + OWP) a z předchozí věty dostaneme pseudonáhodný generátor G. Nechť f je OWP a b její hardcore bit. Pak položme

$$G(x) = b(x) \parallel b(f(x)) \parallel b(f(f(x))) \parallel \ldots$$

Generátor G pak má následující vlastnosti:

- efektivní online výpočet,
- nemusíme znát expanzi apriori,
- security degraduje se zvyšujícím se l.

Kolekce jednosměrných funkcí

Definice: $\mathcal{F} = \{f_{key} : D_{key} \to R_{key}\}_{key \in \mathcal{K}}$ je kolekcí OWFs, pokud

1. $\exists$ PPT $G(1^n)$, který vrací $key \in \mathcal{K}$,
2. se znalostí key lze v polynomiálním čase vybrat z rovnoměrného rozdělení na D_{key},
3. f_{key} lze vyhodnotit v polynomiálním čase $(\forall key \in \mathcal{K})(\forall x \in D_{key})$,
4. $(\forall \text{ PPT } A)(\exists \varepsilon \text{ negligible}) \Pr\left[A(1^n, k, f_k(x)) \in f_k^{-1}(f_k(x))\right] \le \varepsilon(n)$, $\forall n$, kde pravděpodobnost je přes $k \leftarrow G(1^n)$, $x \leftarrow D_k$ a náhodné mince A.

$\mathcal{F}$ je kolekcí náhodných permutací, pokud f_{key} je permutací $\forall key \in \mathcal{K}$.

Značení:

- $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$.
- $\varphi(n)$ je Eulerova funkce, $\varphi(n) = |\mathbb{Z}_n^*|$.
- pro $n \in \mathbb{N}$ budeme značit $\|n\|$ délku zápisu čísla n v binární soustavě.

RSA kolekce

- prostor klíčů: $\mathcal{K} = \left\{(N, e) \mid N = pq, \text{ pro } p, q \text{ prvočísla }, \|p\| = \|q\|, e \in \mathbb{Z}_{\varphi(N)}^*\right\}$.
- generování klíčů: PPT $G(1^n)$:
  - vybere náhodná n-bitová prvočísla p a q,
  - $N = pq$,
  - vygeneruje náhodné $e \in \mathbb{Z}_{\varphi(N)}^*$,
  - vrátí (N, e).
- funkce: $f_{N,e} : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$, $f_{N,e}(x) = x^e \mod N$.

Pozorování: RSA je kolekce permutací.
Důkaz: $D_{key} = R_{key} = \mathbb{Z}_N^*$.

$e \in \mathbb{Z}_{\varphi(N)}^* \implies \left(\exists d \in \mathbb{Z}_{\varphi(N)}^*\right) ed = 1 \,(\mod \varphi(N))$.

Existuje tedy inverzní zobrazení: $y \longrightarrow y^d \mod N$.

Ověříme, že inverzní zobrazení opravdu funguje: $(f_{N,e}(x))^d \equiv (x^e)^d \equiv x^{ed} \equiv x \,(\mod N)$. Při úpravách kongruencí jsme využili Lagrangeovu větu: Pro každou grupu $(G, *)$ platí, že

$$(\forall a \in G)\underbrace{a * \cdots * a}_{n} = a^{|G|} = e.$$

□

Rabinova kolekce

- prostor klíčů: $\mathcal{K} = \{N \mid N = pq,\ \text{pro prvočísla } p, q, \|p\| = \|q\|\}$,
- generátor: PPT $G(1^n)$ generuje n-bitová prvočísla p, q,
- funkce: $f_N : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$, $f_N(x) = x^2 \mod N$.

Tvrzení: Rabinova kolekce je kolekce jednosměrných funkcí, když neexistuje efektivní algoritmus pro faktorizaci přirozených čísel.
Důkaz: (pouze „$\Leftarrow$" - Kdyby nebyla jednosměrná, tak umím faktorizovat.)

Nechť A invertuje Rabinovu kolekci s pstí $\geq \varepsilon(n)$ (non-negligible ε, pravděpodobnost přes volbu klíče a volbu náhodného x).

Zkonstruujeme $A'(n)$:

1. $x \leftarrow \mathbb{Z}_N^*$;
2. $z = x^2 \mod N$;
3. $y \leftarrow A(z, N)$;
4. vrať $gcd(x - y, N)$;

Pokud A uspěje při inverzi z:

$$x^2 - y^2 \equiv 0 \, (\mod N)\,,$$
$$(x - y)(x + y) \equiv 0 \, (\mod N)\,.$$

Pak může nastat několik možností:

1. p, q jsou netriviální faktory $(x + y)$: $N \mid x + y$,
2. p, q jsou netriviální faktory $(x - y)$: $N \mid x - y$,
3. jeden z p, q je netriviální faktor $(x + y)$ a druhý $(x - y)$

$gcd(x - y, N) \in \{p, q\}$, pokud $x \not\equiv \pm y \, (\mod N)$. Protože A invertuje bez znalosti x a z má 4 druhé odmocniny v $\mathbb{Z}_N^*$, tak s pstí $\geq \frac{1}{2}$ vrátí A „dobré" y. S pstí $\geq \frac{\varepsilon(n)}{2}$ tedy A' faktorizuje náhodné N. $\square$

Pro $p \equiv q \equiv 3 \, (\mod 4)$ je $f_N : QR_N \to QR_N$ permutací, kde QR_N jsou kvadratická residua modulo N. $(q \in QR_N \iff (\exists x)\, x^2 \equiv q \, (\mod N).)$

Modulární mocnění

- klíče: $\mathcal{K} = \left\{(p, g) \mid p \text{ je prvočíslo}, g \text{ je generátor } \mathbb{Z}_p^*\right\}$,
- generování: $G(1^n)$ zvol náhodné n-bitové prvočíslo p a g generátor $\mathbb{Z}_p^*$,
- funkce: $f_{p,g} : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$, $f_{p,g}(x) = g^x \mod p$.

Je permutací pokud ztotožníme $\mathbb{Z}_{p-1}$ s $\mathbb{Z}_p^*$.

Hardcore bity

RSA: $lsb_{N,e} : \mathbb{Z}_N^* \to \{0, 1\}$, ($lsb$ - least significant bit). Z hodnot $N, e, x^e \mod N$ neumíme spočítat $lsb_{N,e}(x)$.

Rabin: $lsb_N : \mathbb{Z}_N^* \to \{0, 1\}$

Pro modulární mocnění není lsb hardcore bit. $lsb(x) = 0 \Leftrightarrow g^x$ je čtverec mod p.