13. Bezpieczeństwo semantyczne schematu szyfrowania

Def.

Funkcja f: N -> R nazywamy zaniedbywalną, jeżeli $\forall_E > 0$, $\exists_{K=KC}$ i $\forall_{k>kc} \quad | f(k) | < k^{-c}$

Def.

Powiemy, że funkcja F: N->e jest wielomianem ograniczonym, jeśli istnieje wielomian p: N ->R o współczynnikach rzeczywistych, taka że $\forall_{i \in N} \quad | f(i) | \leq | p(i) |$

Def.

Funkcja f: NxR->R nazywamy rozszerzoną funkcją zaniedbywalną jeśli dla każdej wielomianowo ograniczonej funkcji n zaniedbywalną jest funkcja g:N->R określona następująco: g(x)=f(x,n(x))

A(wejście)=wyjście

W dalszym ciągu będziemy zakładać, że A jest pewnym wielomianowym algorytmem probabilistycznym. Dla zdarzenia Z, pr(Z) oznacza jego prawdopodobieństwo. Podobnie jeśli x to zmienna losowa, to prawdopodobieństwo, że x przyjmuje wartość d ozn. Pr[x=d].

Schemat szyfrowania:

Szyfr asymetryczny to trójka probabilistycznych algorytmów E=(Ekg,E,D) działających w czasie wielomianowym od parametru bezpieczeństwa k, takim że :

1. Ekg(1^k) = (e,d) = Ke x Kd; e,d to odpowiedni klucz publiczny i prywatny. Zbiór K = {(e',d') : $\exists_K : pr[EKg(1^k) = (e', d') > 0]$ nazywamy przestrzenią kluczy.

2. E Ke x M -> C Algorytm E nazywamy algorytmem szyfrującym, M i C to przestrzeń wiadomości i kryptogramów.
3. D Kd x C ->M Algorytm D nazywamy algorytmem deszyfującym.
4. Dla dowolnej pary (e,d) $\in K$ zachodzi równość

   $\forall_{m \in M}\ pr[D(d, E(e,m)) = m] = 1 - E(k)$ dla pewnej funkcji zaniedbywalnej E.

Własności schematy szyfrującego:

A – przeciwnik

Eksperyment $Exp_{E,A}^{(k)}$

1. $Ekg(1^k) \rightarrow (p_k, s_k)$
   $A(p_k) \rightarrow (m_0, m_1, state)$
   $A(E_{pk}(m_b), state) \rightarrow d \quad d=\{0,1\}$

Wynikiem eksperymentu jest 1, gdy d=b.
Niech $Exp_{E,A}^{(k)}$ oznacza eksperyment, w którym w pierwszym kroku losujemy wartość b={0,1} z rozkładem jednostajnym. Wtedy prawdopodobieństwo sukcesu wynosi

$pr[Exp_{E,A}^{(k)}=1] =$

$$= \sum_{x,y \in \{01\}} pr[\mathrm{Exp}_{E,A}(k) = 1, b = x, d = y] = \sum_{z \in \{0,1\}} pr[b = z, d = z] = \sum_{z \in \{0,1\}} 1/4 = 1/4 = 1/2$$

Def.
Przewagą przeciwnika w eksperymencie $Exp_{E,A}^{(k)}$ jest wartość

$$Adv_{E,A}(k) = |\ pr[Exp_{E,A} = 1] - pr[Exp_{E,A} = 1]\ |$$

Def.
Schemat szyfrowania jest semantycznie bezpieczny (ma własność nieodróżnialności) jeśli dla wszystkich algorytmów probabilistycznych A o złożoności wielomianowej $Adv_{E,A}(k)$ jest funkcją zaniedbywalną.