Kryptografia

Lista 2 - 18 III 2013

Problem 1 Niech G będzie generatorem pseudolosowych i $|G(s)| > 2|s|$.

1. Definiujemy $G'(s) = G(s0^{|s|})$. Czy G' jest generatorem pseudolosowym?
2. Niech $G'(s) = G(s_1 \cdots s_{n/2})$, gdzie $s = s_1 \cdots s_n$. Czy G' jest generatorem pseudolosowym?

Odpowiedź twierdzącą udowodnij (w opraciu o pseudolosowość G). Jeżeli G' nie jest generatorem pseudolosowym to znajdź "rozróżniacza" (distuinguisher'a).

Problem 2 Niech G będzie PRG, niech $G'(s)$ będzie równe wyjsciu $G(s)$ obciętym do n bitów (i $|s| = n$). Udowodnij, że $F_k(x) = G'(k) \oplus x$ nie jest generatorem pseudolosowym.

Problem 3 Niech $\Pi_1 = \langle Gen_1, Enc_1, Dec_1 \rangle$, $\Pi_2 = \langle Gen_2, Enc_2, Dec_2 \rangle$ będą dwoma schematami szyfrowania. Pokaż jak skonstułować schemat szyfrowania Π (wykorzystując Π_1 i Π_2), który również będzie *CPA-secure* przy założeniu, że co najmniej jeden ze schematów Π_1 bądź Π_2 jest *CPA-secure* (nie wiesz, który ze schematów jest bezpieczny).

Problem 4 Schemat RC4 wykorzystuje algorytm inicjalizujący KSA (key-scheduling algorithm), po którym rozpoczyna się deterministyczne (zależne od stanu S) generowanie bitów.

```
1 for i from 0 to N do
2 |   S[i] := i
3 end
4 j := 0;
5 for i from 0 to T do
6 |   j := (j + S[i] + key[i mod L]) mod N;
7 |   swap(S[i], S[j]);
8 end
```

Algorithm 1: Algorytm KSA schematu RC4, najczęściej $N = T = 256$, $5 \leq L \leq N$.

Pokaż, że RC4 nie jest bezpiecznym generatorem bitów losowych. W tym celu przeanalizuj prędkość zbieżności procesu KSA-rand do rozkładu jednostajnego. KSA-rand różni się od KSA tym, że linia 6 jest postaci:

$$j := rand(N)$$

Problem 5 Zbadaj zależności (np. równoważność) pomiędzy definicją bezpiecznego generatora pseudolosowego (definicja 6 z poprzedniej listy), a poniższą definicją 1.

Definition 1. Niech $G : \{0,1\}^n \to \{0,1\}^{2n}$ będzie różnowartościowa, oraz dla każdej pozycji $k = 1, \ldots, 2n$ istnieją takie x, y, że $G(x)|_k \neq G(y)|_k$. Powiemy, że G jest **bezpiecznym generatorem pseudolosowym** jeżeli dla każdego efektywnego testu statystycznego A:

$$Adv_{PRG[A,G]} := \left| P_{k \leftarrow \{0,1\}^n} \left[A\left(G(k)\right) = 1 \right] - P_{r \leftarrow im(G)} \left[A(r) = 1 \right] \right| < \epsilon(n),$$

dla pewnej pomijalnej funckji $\epsilon(n)$ ($im(G)$ oznacza obraz funkcji G).