MIX AND MATCH - POMIESZAJ I DOPASUJ

materiały pomocnicze do seminarium kryptograficznego na podstawie artykułu A.Jakobson, M.Jakobsson - „Mix and Match - Secure Evaluation Protocol"

25 lutego 2003

1 PET- <u>P</u>laintext <u>E</u>quality <u>T</u>est

Input - kryptogramy (α_0, β_0), (α_1, β_1). Output *true* jeśli odpowiadają tym samym tekstom jawnym. W przeciwnym wypadku *false*.

1. Liczy się wspólnie $(\xi, \varrho) = \left(\frac{\alpha_0}{\alpha_1}, \frac{\beta_0}{\beta_1}\right)$ i wybiera generator h
2. Każdy z uczestników P_i losuje $z_i, r_i \epsilon_U \mathbf{Z_q}$ i publikuje $C_i = g^{z_i} h^{r_i}$
3. Każdy z uczestników P_i liczy i publikuje
$$(\xi_i, \varrho_i) = (\xi^{z_i}, \varrho^{z_i})$$
4. Każdy uczestnik udawadnia (ZK Proof), że $\xi_i = \xi^{z_i}, \varrho_i = \varrho^{z_i}$ jeśli $C_i = g^{z_i} h^{r_i}$ Jeśli P_i nie udowodni, cały Mix and Match rusza od nowa. Oczywiście już bez oszusta P_i.
5. Uczestnicy wspólnie liczą a potem deszyfrują kryptogram
$$\left(\prod_{i=1}^{n} \xi_i, \prod_{i=1}^{n} \varrho_1^i\right)$$
Jeśli wynikiem jest 1 oznacza to, żę kryptogramy odpowiadają tym samym tekstom jawnym - PET zwtaca *true*. W przeciwnym przypadku PET zwraca *false*.

2 Mix and Match - szkic protokołu

SYTUACJA: Jest n uczestników $P_1, P_2, ..., P_n$. Posiadają oni odpowiednio liczby $B_1, B_2, ..., B_n$. Gdzie $(B_i)_2 = b_1^i b_2^i ... b_n^i$
ZADANIE: policzyć $f(B_1, B_2, ..., B_n)$ „ujawnianic możliwie mało" o $B_1, B_2, ..., B_n$ W tyn celu:

1. Uzgadnia się reprezentację funkcji f w postaci układu kombinacyjnego C_f. Są to bramki $G_1, G_2, ..., G_N$. tak uprządkowane, że głębokość bramki G_i jest niewiększa niż głębokość bramki G_{i+1}
2. Dla każdej bramki G_i tworzona jest „tablica prawdy" T_i
3. Ustala teksty jawne będące reprezentacją bitów 0 i 1. Może to być na przykład g jako 1 a g^{-1} jako 0
4. Wspólnie szfrowane są elementy wszystkich N „tablic prawdy" $\{T_i\}_{i=1}^{N}$ odpowiadające bramkom $\{G_i\}_{i=1}^{N}$. Uczestnicy indywidualnie szyfują bity swoich inputów.
5. MIXING: We wszystkich tablicach T_i miesza się wiersze, re-szyfując wszystkie elementy. (podprotokołem typu MIXnet) Tak otrzymujemy tablice $\left\{\overline{T}_i\right\}_{i=1}^{N}$
6. MATCHING: Dla każdej z bramek wykonujemy następujące działania: Niech l_i,r_i oznaczają kryptogramy odpowiednio lewego i prawaego inputu. Jeśli
$$PET(l_i, \overline{T}_i[u, 1]) = PET(l_i, \overline{T}_i[u, 2]) = true$$
to $\overline{T}_i[u, 3]$ jest kryptogramem outputu tej bramki.
7. Tak otrzymany output staje się inputem kolejnej bramki. Jeśli jest wynikiem końcowym, jest wspólnie deszyfrowany.