4 czerwca 2024

Zadania z kryptografii, lista nr 10

1. Niech $p, q, s : p = 2q + 1, q = 2s + 1$ będą liczbami pierwszymi i $a \in \mathbb{Z}_p, b \in \mathbb{Z}_q$ będą rzędu odpowiednio q i s. Dana jest następująca wersja protokołu, w którym $\mathcal{P}$ dowodzi znajomości dla zadanego z takiego x, że $a^{b^x} = z$.

   - $\mathcal{P}$ losuje $r \in \mathbb{Z}_s$ i przesyła $t = a^{b^r}$,
   - $\mathcal{V}$ wybiera $c \in \{0, 1\}$,
   - $\mathcal{P}$ odsyła $y = r - cx$.

   Kiedy $\mathcal{V}$ akceptuje y? Pokaż, że protokół jest dowodem wiedzą zerową znajomości x przez $\mathcal{P}$.

2. Niech $p, q : p = 2q + 1$ będą liczbami pierwszymi i $a, b, z \in \mathbb{Z}_p^*$ będzie rzędu q. Dana jest następująca wersja protokołu, w którym $\mathcal{P}$ dowodzi znajomości $x \in \{0, 1\}, X \in \mathbb{Z}_q$, takich że $a^x b^X = z$.

   - $\mathcal{P}$ przesyła $t_0 = b^{r_0}, t_1 = ab^{r_1}$, takie że $r_0, r_1 \in_R \mathbb{Z}_q$,
   - $\mathcal{V}$ wybiera $c \in \mathbb{Z}_q$,
   - $\mathcal{P}$ odsyła y_0, y_1, c_0, c_1 i $\mathcal{V}$ sprawdza warunki: $b^{y_0} = t_0 z^{c_0}, b^{y_1} = t_1 z^{c_0}/a, c_0 + c_1 = c$.

   W jaki sposób $\mathcal{P}$ może wyliczyć wymagane $t_0, t_1, y_0, y_1, c_0, c_1$? Pokaż, że protokół ten jest dowodem z wiedzą zerową uczciwego weryfikatora znajomości x i X przez $\mathcal{P}$.

3. Pokaż, że protokół Okamoto ma wiedzę zerową uczciwego weryfikatora konstruując odpowiedni symulator.

4. Załóżmy, że tylko TA zna rozkład liczby $n = pq$. Użytkownicy posługują się protokołem Guillou-Quisquatera. W jaki sposób może być przeprowadzane generowanie kluczy, aby kluczem jawnym każdego użytkownika był jego identyfikator (nazwa). Na jakim kryptograficznym założeniu bazuje niemożliwość odtworzenia klucza tajnego z jawnego przez osobę różną od TA?

5. Załóżmy, że Alicja używa protokołu Schnorra do dowodzenia swojej tożsamości. W pewnym momencie Oskar zapragnął podszyć się pod Alicję przed Bobem. W tym celu nawiązał łączność z Bobem jako Alicja i jednocześnie zażądał od Alicji uwierzytelnienia.

   (a) pokaż w szczegółach jak Oskar może przeprowadzić swój atak,

   (b) pokaż jak Oskar może używając losowych czynników zamaskować komunikację z Alicją tak aby była losową trójką wymienioną w prawidłowo przeprowadzonym protokole (w ten sposób Oskar unika ew. nieprzyjemności, bo taka trójka nie może być skojarzona z jego komunikacją z Bobem),

   (c) pokaż jak metoda maskowania z poprzedniego podpunktu może służyć do otrzymywania ślepych podpisów Schnorra.

6. Pokaż, że następujący protokół jest protokołem z obliczeniową wiedzą zerową dowodzącym znajomości cyklu Hamiltona w grafie G.

   - Alicja losuje G' izomorficzny z G. Alicja przekazuje Bobowi zobowiązania bitowe b dla każdej pary wierzchołków $\{v, u\}$ równe 1 gdy $\{v, u\} \in E(G')$ i 0 w przeciwnym razie.
   - Bob wybiera $c \in \{0, 1\}$.
   - Jeśli $c = 0$, to Alicja odkrywa zobowiązania bitowe krawędzi cyklu Hamiltona, a gdy $c = 1$ odkrywa zobowiązania wszystkich krawędzi i ujawnia izomorfizm między G a G'.

7. Skonstruuj dowód z obliczeniową wiedzą zerową znajomości w grafie kliki zadanego rozmiaru k.