Kryptografia

Lista nr 7, 3 VI

1. Dla schematu zobowiązań Pedersena z parametrami $p = 37, g = 13, h = 35$, opublikowano zobowiązanie $c(x, r) = g^x h^r \bmod p = 29$. Do jakiej wartości x jest to zobowiązanie?
2. Dla schematu zobowiązań wykorzystujących problem dyskretnego logarytmu w Z_p, z parametrami $p = 37, g = 13$ opublikowano zobowiązanie $c(x) = g^x \bmod p = 29$. Do jakiej wartości x jest to zobowiązanie?
3. Uczestnik protokołu ($\mathbf{P_i}$) posiada sekret s_i, którym chce się podzielić. W tym celu wybiera liczbę pierwszą p, a następnie niezależnie i jednostajnie losuje $r_{i,1}, r_{i,2} \in Z_p$, oraz oblicza wartość
$$r_{i,3} = s_i - r_{i,1} - r_{i,2} \bmod p.$$
$\mathbf{P_i}$ przesyła $r_{i,a}, r_{i,b}$ (dla $a, b \neq j$ do $\mathbf{P_j}$ (w szczególności $\mathbf{P_1}$ przesyła $r_{1,1}, r_{1,3}$ do $\mathbf{P_2}$).
Uzasadnij, że ani $\mathbf{P_2}$ ani $\mathbf{P_3}$ nie poznają żadnej informacji na temat s_1.
W jaki sposób dowolni dwaj uczestnicy protokołu mogą zrekonstruować s_i?
Zakładając, że s jest kluczem tajnym dla podpisów ElGamal'a (a kluczem publicznym jest $g, h = g^s \bmod p, p$) pokaż jak $\mathbf{P_i}$ i $\mathbf{P_j}$ mogą wspólnie podpisać wiadomość m.
4. Przyjmij, że każdy uczestnik $\mathbf{P_i}$ protokołu dokonał podziału swojej wartości s_i tak jak opisano w zadaniu 3 (przy wspólnej wartości p). W jaki sposób uczestnicy protokołu mogą obliczyć wartość $s = s_1 + s_2 + s_3 \bmod p$? Zadbaj, aby Twoja propozycja nie ujawniała s_i innym uczestnikom protokołu.
5. Jak wykorzystać protokół z poprzedniego zadania do głosowania? Załóż, że jedynymi opcjami głosowania są tak/nie.
Jak przekształcić protokół "tak/nie" na protokół głosowania na jednego z n kandydatow?
6. Zaproponuj schemat obliczania iloczynu $s = s_1 s_2 \bmod p$ przez trzech uczestników ($\mathbf{P_3}$ uczestniczy w protokole, ale "nie ma wejścia") w taki sposób, że uczestnik i zna jedynie s oraz s_i (zarówno przed jak i po wykonaniu protokołu).
7. Twoim zadaniem jest opracowanie protokołu dla aplikacji mobilnej realizującej funkcjonalność zbliżoną do opowiedzianej w bajce "Tinderella", z tą różnicą, że serwer ma nie poznawać preferencji użytkowników. Dokładniej: celem protokołu jest stwierdzenie, czy uczestnicy $\mathbf{P_1}, \mathbf{P_2}$ są sobą zainteresowani ($s_i = 1$) czy nie ($s_i = 0$), rezultatem protokołu jest bit $b = 1$ wtedy i tylko wtedy gdy $s_1 = s_2 = 1$, w pozostałych przypadkach $b = 0$.
W szczególności z przebiegu protokołu uczestnik $\mathbf{P_1}$, który nie jest zainteresowany uczestnikiem $\mathbf{P_2}$ nie może się dowiedzieć wartości s_2.
8. Protokół z zadania 4 nie jest optymalny. Zaproponuj rozwiązanie, w którym sekret dzielony jest na dwa a nie trzy składniki.
9. Rozpatrz następujące sytuacje podczas wykonywania protokołu z zadania 4:
   - $\mathbf{P_i}$ wybierze wartości w ten sposób, że $s_{i,1} \neq r_{i,1} + r_{i,2} + r_{i,3}$,
   - $\mathbf{P_1}$ prześle do $\mathbf{P_2}$: $r_{1,1}, r_{1,3}$, a do $\mathbf{P_3}$: $r'_{1,1}, r_{1,2}$ gdzie $r_{1,1} \neq r'_{1,1}$.

   Jak można wykryć/jak można zapobiec takim sytuacjom?