Yao's Millionaires' problem

Marcin Ostrowski

2 lipca 2021

1 Wstęp

Problem dotyczy dwóch milionerów, Alice i Boba, którzy chcą wiedzieć, który z nich jest bogatszy, bez ujawniania ich rzeczywistego bogactwa. Ten problem jest analogiczny do bardziej ogólnego problemu, w którym występują dwie liczb a i b, a celem jest ustalenie, czy nierówność $a \geqslant b$ jest prawdziwa lub fałszywa bez ujawniania rzeczywistych wartości a i b.

2 Rozwiązanie Ioannidisa i Anantha

2.1 Transfer utajniony 1-2

W transferze utajnionym 1-2, nadawca ma dwie wiadomości m_0 i m_1, a odbiorca posiada bit b. Odbiorca chce otrzymać wiadomość m_b, bez ujawniania nadawcy bitu b. Nadawca chce mieć pewność, że odbiorca otrzymuje tylko jedną z dwóch wiadomości.

Nadawca				Odbiorca		
Opis	Prywatne	Publiczne		Publiczne	Prywatne	Opis
Przygotuj wiadomości do wysłania	m_0, m_1					
Wygeneruj parę kluczy RSA i wyślij publiczną część	d	N, e	$\rightarrow$	N, e		Otrzymuje publiczny klucz
Wygeneruj i wyślij losowe wiadomości x_0, x_1		x_0, x_1	$\rightarrow$	x_0, x_1		Otrzymuje wiadomości
					k, b	Ustal bit $b \in \{0,1\}$ oraz wygeneruj losowe k
Otrzymuje zaślepioną wiadomość v		v	$\leftarrow$	$v = (x_b + k^e) \bmod N$		Dodaje czynnik losowy do wiadomości x_b tworząc zaślepioną wiadomość
Wygeneruj dwie wartości		$k_0 = (v - x_0)^d \bmod N$ $k_1 = (v - x_1)^d \bmod N$				
Połącz wiadomości z kluczami oraz wyślij je		$m'_0 = m_0 + k_0$ $m'_1 = m_1 + k_1$	$\rightarrow$	m'_0, m'_1		Otrzymuje dwie wiadomości
					$m_b = m'_b - k$	Odejmuje czynnik losowy od zaślepionej wiadomości otrzymując wiadomość m_b

2.2 Protokół

W celu opisania protokołu liczba nadawcy jest oznaczona jako a, a liczba odbiorcy jest oznacza jako b. Długość binarnych reprezentacji a oraz b jest mniejsza od $d \in \mathbf{N}$. W każdej liczbie binarnej najbardziej znaczący bit jest na końcu w binarnej reprezentacji, tj. najmniej znaczący bit jest na pozycji 0.

- Nadawca tworzy macierz K o rozmiarze $d \times 2$. Składowa K_{ij}, dla $j \in \{0,1\}$ oraz $0 \leqslant i < d$, to binarna liczba o długości k, gdzie k to długość klucza RSA wygenerowanego w transferze utajnionym.
- Nadawca losuje dwie liczby u oraz v, gdzie $0 \leqslant u < 2k$, a $v \leqslant k$.

- Niech K_{ijl} oznacza l-ty bit liczby w K_{ij}. Niech a_i oznacza i-ty bit liczby a. Dla każdego $0 \leqslant i < d$ nadawca:
  - Dla każdego bitu o indeksie $j \geqslant v$ ustawia K_{i1j} oraz K_{i2j} do losowych wartości.
  - Jeśli $a_i = 1$, to ustawiamy indeks $l = 0$, w przeciwnym razie ustawiamy indeks $l = 1$. Następnie dla każdego bitu o indeksie $0 \leqslant j \leqslant 2 \times i - 1$ ustawiamy K_{ilj} do losowej wartości.
  - Ustawiamy indeks $m = 2 \times i$, a następnie ustawiamy $K_{il(m+1)} = 1$ oraz $K_{ilm} = a_i$.
  - Generujemy losową k-bitową liczbę binarną S_i. Dla ostatniego indeksu $i = d - 1$ dwa ostatnie bity w S_{d-1} zostaną ustawione następująco: $S_{(d-1)(k-1)} = 1 \oplus \bigoplus_{j=1}^{d-2} S_{j(k-1)} \oplus \bigoplus_{j=1}^{d-1} K_{j0(k-1)}$, $S_{(d-1)(k-2)} = 1 \oplus \bigoplus_{j=1}^{d-2} S_{j(k-2)} \oplus \bigoplus_{j=1}^{d-1} K_{j0(k-2)}$.
  - Dla każdego indeksu $l \in \{0, 1\}$ ustawiamy $K'_{il} = \mathrm{rot}(K_{il} \oplus S_i, \mathrm{u})$, gdzie $\mathrm{rot}(x, t)$ oznacza obrót bitowy x w lewo o t bitów.
- Dla każdego $0 \leqslant i < d$ nadawca oraz odbiorca transferują K'_{il}, gdzie $l = b_i$, a b_i to i-ty bit w liczbie b.
- Nadawca wysyła do odbiorcy $N = \mathrm{rot}(\bigoplus_{j=0}^{d-1} S_j, u)$.
- Odbiorca xoruje wszystkie przetransferowane wiadomości oraz otrzymane N. Odbiorca skanuje wynik od lewej do prawej szukając dużej sekwencji zer. Niech c oznacza bit na prawo od takiej sekwencji. Jeśli bit na prawo od c jest 1, to $a \geqslant b$, w przeciwnym razie $a < b$.