Kryptografia, Lista 3

Adrian Mucha, Politechnika Wrocławska, WPPT 26.05.2020

Merkle Hellman Kryptosystem

Wstęp

Rozważmy 0-1 problem plecakowy z n przedmiotami o wartościach v_i oraz wagach w_i. Mamy znaleźć podzbiór rzeczy maksymalizujący zysk nieprzekraczając pewnej maksymalnej pojemności W. Problem jest NP-trudny, ale może zostać rozwiązany w czasie pseudo-wielomianowym z zastosowaniem programowania dynamicznego.

Problem sumy podzbioru (*subset sum problem*) jest specjalnym przypadkiem problemu plecakowego gdzie każda wartość jest równa swej wadze. Wejściem jest zbiór $A = \{a_1, \ldots, a_n \,|a_i \in \mathbb{N}_{>0}\}$ oraz liczba dodatnia S. Jeżeli istnieje podzbiór A sumujący się do S to wyjściem jest `TRUE`, `FALSE` w p.p. Ten problem również jest NP-trudny.

Łatwy problem plecakowy to taki, w którym zbiór A jest ciągiem super-rosnącym, tj

$$a_2 > a_1, a_3 > a_2 + a_1, \ldots, a_n > a_{n-1}, \ldots, a_1$$

. Przykładem takiego ciągu jest ciąg potęgowy 2^n. Z tego zbioru wybieramy podzbiór $X \subset A$ sumujący się do E, który będziemy traktować jako klucz prywatny.

Komunikacja

Alicja:

1. Generuje sekretny *klucz prywatny*
2. Generuje *klucz publiczny*, który jest dostępny dla wszystkich
3. Otrzymuje zaszyfrowaną wiadomość od Boba
4. Odszyfrowuje ją za pomocą *klucza prywatnego*

Bob:

1. Używa *klucza publicznego* Alicji do zaszyfrowania tekstu jawnego
2. Wysyła zaszyfrowany tekst do Alicji

Algorytm

Alicja:

1. Wybiera $A = \{a_1, a_2, \ldots, a_n \,|a_i > \sum_{1 \le j < i} a_j\}$ (super-rosnący ciąg), wybiera prosty problem plecakowy
2. Oblicza $E = \sum_{i=1}^{n} a_i$
3. Wybiera $M > E$
4. Wybiera W, takie że $2 \le W < M$ oraz $gcd(W, M) = 1$ by zapewnić odwracalność modulo M.
5. Oblicza publiczny (trudny) problem plecakowy $B = \{b_1, b_2, \ldots, b_n\}$, w którym

$$b_i = Wa_i \mod M$$

6. Zachowuje (ukrywa) *klucz prywatny* (A, W, M)
7. Publikuje *klucz publiczny* B

Bob:

1. Chce zaszyfrować tekst jawny P, który dzieli na k elementowych ciągów długości n, $P = \{P_1, \ldots, P_k\}$
2. Szyfruje bloki tekstu jawnego otrzymując szyfrogram $C = \{c_1, \ldots, c_n\}$

$$\forall_{P_i \in P}, \sum_{j=1}^{n} P_{ij} b_j = c_i$$

   gdzie P_{ij} oznacza j-ty znak i-tego bloku tekstu jawnego
3. Wysyła C do Alicji

Alicja:

1. Po otrzymaniu szyfrogramu of Boba, Alicja oblicza w - odwrotność W modulo M

$$wW \equiv 1 \mod M$$

2. Używa powiązania między łatwym i trudnym problemem plecakowym

$$wb_i = a_i \mod M$$

3. Aby odszyfrować szyfrogram C, obliczane jest

$$S_i = wC_i \mod M = w \sum_{j=1}^{n} P_{ij} b_j \mod M = \sum_{j=1}^{n} P_{ij} w b_j \mod M = \sum_{j=1}^{n} P_{ij} a_j$$

4. Ponieważ $S_i < M$ oraz $M > E$ to ostatecznie, szukanie tekstu jawnego sprowadza się do znalezienia rozwiązania

$$S_i = \sum_{j=1}^{n} P_{ij} a_j$$

   , które można znaleźć w czasie wielomianowym ponieważ używana jest łatwa wersja problemu plecakowego