Matematyka Podpisu Elektronicznego 27.10.04

Wykład 4. Klasyczne kryptosystemy asymetryczne - cd.

Stefan Dziembowski stefan-mpe@dziembowski.net

Streszczenie.

1 Problem logarytmu dyskretnego

Nieformalnie:

dana grupa $(G, \cdot)$ i element $\alpha \in G$ (rzędu m) i element β generowany przez α.

znaleźć $a = 1, \ldots, m$ tże $\alpha^a = \beta$.

Takie a oznaczamy $\log_\alpha \beta$ i nazywamy ...

(zauważmy, że obliczeni funkcji odwrotnej jest łatwe, jeśli tylko łatwe jest wykonie operacji w grupie).

Przykład: Z_n, Z_p^*.

W wielu grupach obliczanie logarytmu dysk. (o określonych podstawach) jest uważane za trudne

2 Protokol DH uzgadaniania klucza

Niech G będzie grupą w której obliczanie logarytmu dyskretnego o podstawie $\alpha \in G$ (rzędu m) jest trudne.

1. Alicja wybiera losowe $a \in \{0, \ldots, m-1\}$ i przesyła α^a do Boba.
2. Bob wybiera losowe $b \in \{0, \ldots, m-1\}$ i przesyła α^b do Alicji.
3. Uzgodnionym kluczem jest α^{ab}.

Co widzi Ewa? α^a, α^b, ale jak ma obliczyć α^{ab}.

Rozważmy następujące stwierdzenia:

1. Problem obliczenia logarytmu dyskretnego jestr trudny
2. Protokół Diffiego-Hellmana jestr bezpieczny

Oczywiście zachodzi implikacja $2 \rightarrow 1$, ale w ogólności nie wiadomo, czy zachodzi implkacja odwrotna. W każdym razie dla wielu popularnych grup jest to problemem otwartym.

Więcej na ten temat: [GB], Rozdział 10.1.

3 Skad wziąc grupę G i odpowiednią podstawę

Pierwszym pomysłem jest Z_p^* (gdzie p jest pierwsza) i niech α będzie jej generatorem.

Ten problem jest uważany za trudny o ile $p-1$ nie ma wszystkich małych czynników (Pohlig and Hellman).

Taki generator istnieje (bo p jest pierwsza), ale jak go znaleźć?

Można to zrobić na różne sposoby:

3.1 Sposób 1.

1. bierzemy losową liczbę pierwszą q i podstawiamy $p := 2q + 1$.
2. Jeśli p nie jest pierwsza, to go to 1.
3. bierzemy losowy elelmet α
4. jeśli $\alpha^2 = 1$ albo $\alpha^q = 1$ to go to 3.

Skomentować dlaczego liczby powtórzeń w obu przypadkach są małe i dlaczego to działa.

(cwiczenie: ile jest generatorow grupy syklicznej?)

3.2 Sposób 2.

Jeśli komuś nie odpowiada, że p nie jest całkowiecie losowa, to może użyć Algorytmu Bacha (Patrz też Adam Kalai).

Są też inne pomysły na gryou (oparte na krzywych eliptycznych). O tym za moment.

Wiecej na ten temat można znaleźć w [GB], Rozdział 2.3.1.

4 Kryptosystem ElGamala

Niech Z_p będzie grupą, a α jej generatorem (te wartości mogą być ustalone i publicznie znane).

Wszystkie operacje będą wykonywane w Z_p^*.
Z_p^* — zbiór wiadmości
$Z_p^* \times Z_p^*$ — zbiór kryptogramów.
Generacja klucza:

1. Zalosuj $a \xleftarrow{\mathrm{r}} \{0, \ldots, p-1\}$.
2. KLuczem prywatnym jest a.
3. Kluczem publicznym jest $\beta := \alpha^a$ (oraz α i p).

4.1 Szyfrowanie

Niech $k \xleftarrow{\mathrm{r}} \{0, \ldots, p-1\}$

$$\mathcal{E}^{\mathrm{ElGamal}}_{\beta,\alpha,p}(x) := (\alpha^k, x\beta^k).$$

Zauważmy, że szyfrowanie jest zrandomizowane.
Jak odszyfrować? Posiadacz klucza prywatnego nie zna k...
Ponadto, w odróżnieniu od RSA, nie jest w posiadaniu żadnej tajnej informacji, któa pozwolłaby np. obliczyć logarytm dysk.
Zauważmy: $(\alpha^k, x\beta^k) = (\alpha^k, x\alpha^{ak})$. Oznaczmy $y_1 := \alpha^k$, $y_2 := x\alpha^{ak}$.
Dlatego $x := y_2 \cdot y_1^{-a}$. Stąd wzór

$$\mathcal{D}^{\mathrm{ElGamal}}(y_1, y_2) := y_2 \cdot y_1^{-a}$$

Więcej na ten temat: [MvOV97], Rozdział 8.4.

4.2 Podpis

Ponieważ szyfrowanie jest niedeterministyczne, to nie da się od razy stworzyć schematu podpisu. Istnieje jednak schemat zwany *podpisem ElGamala* – patrz Rozdział 11.5.2 [MvOV97].

5 Krzywe eliptyczne

Niech K będzie ciałem. *Krzywą eliptyczną* nad ciałem K nazywamy zbiór punktów w K^2 spełniających równanie

$$y^2 = x^3 + ax + b,$$

(gdzie $a, b \in K$ są takie, że $4a^3 + 27b^2 \neq 0$), oraz dodatkowo elememt $\mathcal{O}$ zwany *punktem w nieskończoności*.

Ćwiczenie: pokazać, że jeśli $4a^3 + 27b^2 = 0$, to równanie nie ma trzech rozwiązań. (Np. $x^3 - 3x + 2 = (x-1)^2(x+2)$).

Narysować krzywą eliptyczną nad rzeczywistymi.

Wproadzamy strukturę grupy na krzywej eliptycznej.

wytłumaczyć dodawanie dwóch punktów (x_1, y_1), (x_2, y_2)

- te same punkty

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

- punkty o tej samej współrzędnej x – punkt w nieskończoności
- punkty o różnej współrzednej x. Jak w przypadku pierwszym, ale $\lambda = \frac{3x_1^2 + a}{2y_1}$

Dodawanie $\mathcal{O}$ jest jasne ($\mathcal{O}$jest elem. neutralnym)

Łatwo spradzić, że tak zdefiniowana operacja daje nam grupę.

Więcej na ten temat: [GB], Rozdział C.11 (Strona 264).

Literatura

[GB] S. Goldwasser and M. Bellare. Lecture notes in cryptography. dostępne pod adresem `http://www.cs.ucsd.edu/users/mihir/papers/gb.html`.

[MvOV97] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997. dostępne pod adresem `http://www.cacr.math.uwaterloo.ca/hac/`.