Współczesna kryptografia – schematy bazujące na parowaniu punktów krzywej eliptycznej

Andrzej Chmielowiec

Centrum Modelowania Matematycznego Sigma,
andrzej.chmielowiec@cmmsigma.eu

26 maja 2010

Logarytm dyskretny

Niech G będzie grupą cykliczną, w której element g jest generatorem. Logarytmem dyskretnym z elementu $h \in G$ nazywamy taką liczbę x, dla której spełnione jest równanie

$$g^x = h.$$

Znalezienie logarytmu dyskretnego jest w ogólności zadaniem obliczeniowo trudnym. W szczególności najszybsza metoda pozwalająca na jego wyznaczenie w grupie punktów krzywej eliptycznej ma złożoność

$$2^{r/2},$$

gdzie r jest największym dzielnikiem pierwszym rzędu generatora.

Uzgadnianie klucza metodą Diffiego-Hellmana

A		B
g^a	$\longrightarrow$	
	$\longleftarrow$	g^b
$h = \left(g^b\right)^a = g^{ab}$		$h = \left(g^a\right)^b = g^{ab}$

Problem Diffiego-Hellmana

Z problemem logarytmu dyskretnego związany jest problem Diffiego-Hellmana. Polega on na znalezieniu wielkości g^{ab} na podstawie g, g^a i g^p. Można wykazać, że dla dowolnej grupy problem logarytmu dyskretnego jest wielomianowo redukowalny do problemu Diffiego-Hellmana (problem logarytmu dyskretnego nie jest łatwiejszy obliczeniowo niż problem Diffiego-Hellmana). Odwrotna redukowalność została wykazana tylko w niektórych przypadkach.

Trójstronne uzgadnianie klucza

Runda pierwsza

$$\begin{array}{ccccc} A, a, g^a & \rightarrow & g^a & \rightarrow & B, b, g^b \\ \uparrow & & & & \downarrow \\ g^c & \leftarrow & C, c, g^c & \leftarrow & g^b \end{array}$$

Runda druga

$$\begin{array}{ccccc} A, a, g^a, g^c & \rightarrow & g^{ac} & \rightarrow & B, b, g^b, g^a \\ \uparrow & & & & \downarrow \\ g^{bc} & \leftarrow & C, c, g^c, g^b & \leftarrow & g^{ab} \end{array}$$

Definicja odwzorowania dwuliniowego

Odwzorowaniem dwuliniowym na (G_1, G_T) nazywamy takie przekształcenie

$$\hat{e} : G_1 \times G_1 \to G_T,$$

które spełnia następujące warunki:

1. (Dwuliniowość) Dla każdego $R, S, T \in G_1$ mamy

$$\hat{e}(R + S, T) = \hat{e}(R, T)\hat{e}(S, T),$$

$$\hat{e}(R, S + T) = \hat{e}(R, S)\hat{e}(R, T).$$

2. (Niezdegenerowanie) $\hat{e}(P, P) \neq 1$.
3. (Obliczalność) Wartość $\hat{e}(P, R)$ może być efektywnie wyznaczona.

Własności odwzorowania dwuliniowego (1)

Można wykazać, że odwzorowania dwuliniowe mają następujące własności:

1. $\hat{e}(S, \infty) = 1$ i $\hat{e}(\infty, S) = 1$.
2. $\hat{e}(S, -T) = \hat{e}(-S, T) = \hat{e}(S, T)^{-1}$.
3. $\hat{e}(aS, bT) = \hat{e}(S, T)^{ab}$ dla wszystkich $a, b \in \mathbb{Z}$.
4. $\hat{e}(S, T) = \hat{e}(T, S)$.
5. Jeśli $\hat{e}(S, R) = 1$ dla wszystkich $R \in G_1$, to $S = \infty$.

Własności odwzorowania dwuliniowego (2)

Jedną z konsekwencji istnienia odwzorowania dwuliniowego jest to, że problem logarytmu dyskretnego w grupie G_1 może być efektywnie zredukowany do problemu logarytmu dyskretnego w grupie G_T. Jeśli bowiem szukamy rozwiązania równania

$$Q = xP$$

w grupie G_1, to szukana liczba x jest również rozwiązaniem równania

$$\hat{e}(P, Q) = \hat{e}(P, xP) = \hat{e}(P, P)^x$$

w grupie G_T.

Dwuliniowy problem Diffiego-Hellmana

Jeśli $\hat{e}$ jest odwzorowaniem dwuliniowym, to dwuliniowy problem Diffiego-Hellmana definiujemy następująco:

Mając dane P, aP, bP i cP należy wyznaczyć $\hat{e}(P,P)^{abc}$.

Własności dwuliniowego problemu DH

Trudność obliczeniowa dwuliniowego problemu DH implikuje trudność problemu DH zarówno w grupie G_1 jak i G_T.

Jeżeli na podstawie aP i bP możemy wyznaczyć abP, to możemy również wyznaczyć

$$\hat{e}(abP, cP) = \hat{e}(P, P)^{abc}.$$

Jeżeli na podstawi $g^{ab} = \hat{e}(aP, bP)$ i $g^c = \hat{e}(P, cP)$ możemy wyznaczyć g^{abc} to znajdziemy

$$g^{abc} = \hat{e}(P, P)^{abc}.$$

Jednorundowe uzgodnienie klucza przez trzy strony (1)

1. Strona A losuje liczbę $a \in [0, n-1]$, wyznacza aP i wysyła stronom B, C.
2. Strona B losuje liczbę $b \in [0, n-1]$, wyznacza bP i wysyła stronom A, C.
3. Strona C losuje liczbę $c \in [0, n-1]$, wyznacza cP i wysyła stronom A, B.

Jednorundowe uzgodnienie klucza przez trzy strony (2)

	Strona A	Strona B	Strona C
Posiada	a, bP, cP	b, aP, cP	c, aP, bP
Wyznacza	$K = \hat{e}(bP, cP)^a = \hat{e}(P, P)^{abc}$	$K = \hat{e}(aP, cP)^b = \hat{e}(P, P)^{abc}$	$K = \hat{e}(aP, bP)^c = \hat{e}(P, P)^{abc}$

Kryptografia oparta na identyfikatorach (1)

W roku 1984 Shamir przedstawił koncepcję kryptografii opartej na identyfikatorach:

1. Kluczem publicznym użytkownika będzie jego identyfikator (na przykład adres e-mail).
2. Będzie istniała zaufana trzecia strona odpowiedzialna za tworzenie kluczy prywatnych dla użytkowników.
3. Szyfrowanie będzie można wykonać nawet przed wygenerowaniem klucza prywatnego użytkownika (operacja szyfrowania wymagać będzie jedynie identyfikatora użytkownika i klucza publicznego zaufanej trzeciej strony).

Kryptografia oparta na identyfikatorach (2)

Schemat Boneha-Franklina zakłada, że:

1. Dysponujemy dwuliniowym odwzorowaniem $\hat{e} : G_1 \longrightarrow G_T$.
2. Istnieją funkcje skrótu H_1 i H_2 takie, że:

$$H_1 : \{0,1\}^* \longrightarrow G_1 \setminus \{\infty\} \quad \text{i} \quad H_2 : G_T \longrightarrow \{0,1\}^l.$$

   gdzie l jest liczbą bitów tekstu jawnego.
3. Zaufana trzecia strona dysponuje swoim kluczem prywatnym $t \in [0, n-1]$ oraz kluczem publicznym $T = tP$.

Klucz prywatny d_A, wyznaczany jest na podstawie identyfikatora ID_A:

$$d_A = tQ_A = tH_1(ID_A).$$

Kryptografia oparta na identyfikatorach (3)

Szyfrowanie wiadomości $m \in \{0,1\}^l$:

1. Wyznaczamy klucz publiczny $Q_A = H_1(ID_A)$.
2. Wybieramy losowo liczbę $r \in [0, n-1]$ i obliczamy $R = rP$.
3. Tworzymy szyfrogram $c = m \oplus H_2(\hat{e}(Q_A, T)^r)$.
4. Wysyłamy parę (R, c) do odbiorcy.

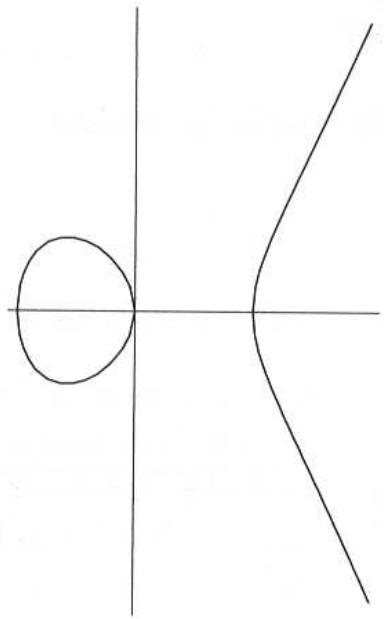
W celu odszyfrowania wiadomości użytkownik wykorzystuje swój klucz prywatny d_A i wyznacza tekst jawny $m = c \oplus H_2(\hat{e}(d_A, R))$. Proces deszyfrowania wiadomości działa poprawnie, ponieważ prawdziwa jest następująca równość:

$$\hat{e}(d_A, R) = \hat{e}(tQ_A, rP) = \hat{e}(Q_A, P)^{tr} = \hat{e}(Q_A, tP)^r = \hat{e}(Q_A, T)^r.$$

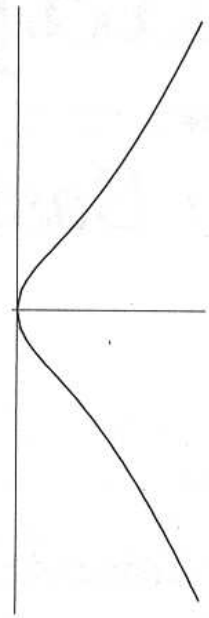
Krzywa eliptyczna

Jednorodne równanie Weierstrassa:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$



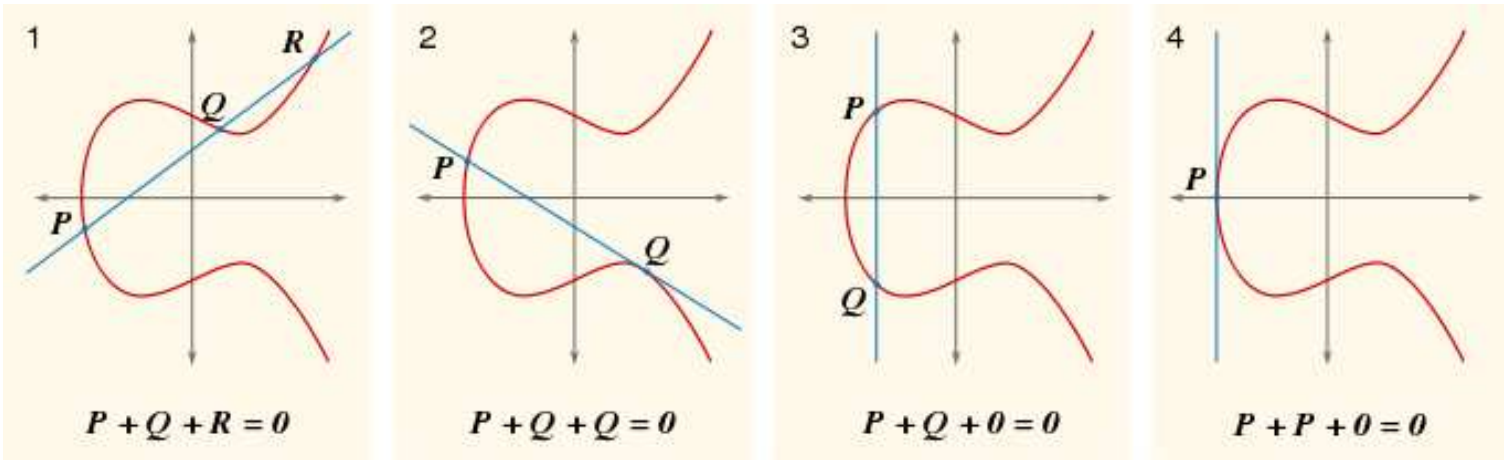
(a) $y^2 = x^3 - x$



(b) $y^2 = x^3 + x$

Grupa punktów krzywej eliptycznej

Punkty krzywej eliptycznej tworzą grupę.



Metody rozwiązywania logarytmu dyskretnego na krzywej eliptycznej

Aktualnie najlepszą metodą rozwiązywania tego problemu jest algorytm ρ-Pollarda, którego oczekiwany czas działania jest rzędu $O(\sqrt{n})$.

Istnieją również metody rozwiązywania problemu logarytmu dyskretnego, które mają zastosowanie dla konkretnych rodzajów krzywych. W szczególności można zastosować iloczyn Weila i Tate, aby przenieść problem z grupy punktów krzywej, do grupy multyplikatywnej ciała skończonego $\mathbb{F}_{q^k}$.

Stopniem osadzenia $\langle P \rangle \subset E$ nazywamy najmniejszą liczbę całkowitą k, dla której zachodzi $n \mid q^k - 1$.

Iloczyn Tate - definicja

Niech $P, Q \in E[n]$ i niech f_P będzie funkcją spełniającą warunek $\mathrm{div}(f_P) = n(P) - n(\infty)$. Przyjmijmy ponadto, że $R \in E[n]$ jest punktem spełniającym warunek $R \notin \{\infty, P, -Q, P - Q\}$ oraz D_Q jest dywizorem zdefiniowanym następująco $D_Q = (Q + R) - (R)$. Przez iloczyn Tate rozumiemy odwzorowanie:

$$e : E[n] \times E[n] \to \mu_n$$

zdefiniowane następująco:

$$e(P, Q) = f_P(D_Q)^{(q^k-1)/n} = \left(\frac{f_P(Q + R)}{f_P(R)} \right)^{(q^k-1)/n}.$$

Algorytm Millera (1)

Jeśli $P \in E[n]$, l jest linią przechodzącą przez punkty iP, jP, a v jest linią pionową przechodzącą przez punkt $iP + jP$, to

$$f_{i+j} = f_i f_j \frac{l}{v}.$$

Algorytm Millera (2)

1. $n = (n_t, \ldots, n_1, n_0)_2$, $R \in E[n] \setminus \{\infty, P, -Q, P - Q\}$.
2. Przyjmujemy $f \leftarrow 1$, $T \leftarrow P$.
3. Dla i od t do 0 wykonujemy:
   - 3.1 Wyznaczamy prostą l, styczną do krzywej w T.
   - 3.2 Wyznaczamy pionową prostą v przechodzącą przez $2T$.
   - 3.3 $T \leftarrow 2T$.
   - 3.4 $f \leftarrow f^2 \cdot \frac{l(Q+R)}{v(Q+R)} \cdot \frac{v(R)}{l(R)}$.
   - 3.5 Jeśli $n_i = 1$ to
     - 3.5.1 Wyznaczamy prostą l przechodzącą przez T i P.
     - 3.5.2 Wyznaczamy pionową prostą v przechodzącą przez $T + P$.
     - 3.5.3 $T \leftarrow T + P$.
     - 3.5.4 $f \leftarrow f \cdot \frac{l(Q+R)}{v(Q+R)} \cdot \frac{v(R)}{l(R)}$.
4. Obliczamy $f^{(q^k-1)/n}$.

Pytania

Czy mają Państwo pytania?