Współczesna kryptografia – schematy bazujące na parowaniu punktów krzywej eliptycznej

Andrzej Chmielowiec

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

Streszczenie

Współczesna kryptografia daje duże możliwości zarówno w sferze ochrony danych jak i kontroli dostępu. Jej dynamiczny rozwój na przestrzeni ostatnich lat sprawił, że dziś dysponujemy ogromnym wachlarzem technik pozwalających na zabezpieczanie danych i autoryzację użytkowników. W artykule tym zostaną omówione nowe możliwości jakie daje kryptografia wykorzystująca mechanizm parowania punktów krzywej eliptycznej.

1 Wprowadzenie

Problem logarytmu dyskretnego (DLP) jest bardzo dokładnie badany od czasu narodzin kryptografii klucza publicznego w 1975 roku. Przypomnijmy, że problem ten definiowany jest w grupie cyklicznej $G = \langle P \rangle$ rzędu n jako problem znalezienia takiej liczby $x \in [0, n-1]$, która spełnia równanie

$$Q = xP.$$

Uważa się, że w przypadku odpowiednio dobranej grupy, problem ten jest trudny obliczeniowo. Choć nie ma na to żadnego dowodu, to za takie *odpowiednie* grupy uważamy obecnie grupę multyplikatywną ciała skończonego i grupę punktów krzywej eliptycznej zdefiniowanej nad ciałem skończonym.

Z problemem logarytmu dyskretnego związany jest problem Diffiego-Hellmana. Polega on na znalezieniu wielkości abP na podstawie P, aP i bP. 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.

Trudność problemu Diffiego-Helmana jest podstawą bezpieczeństwa klasycznego już protokołu uzgadniania kluczy. Zakładając, że mamy daną grupę $G = \langle P \rangle$ rzędu n, przebieg protokołu jest następujący:

1. Strona A losuje liczbę $a \in [0, n-1]$ i wyznacza aP, które wysyła stronie B.
2. Strona B losuje liczbę $b \in [0, n-1]$ i wyznacza bP, które wysyła stronie A.

	Strona A	Strona B
Posiada	a, bP	b, aP
Wyznacza	$K = a(bP) = abP$	$K = b(aP) = abP$

Za uzgodnioną wartość przyjmuje się element $K = abP = a(bP) = b(aP)$. Ten protokół uznawany jest za jednorundowy, gdyż każda ze stron odbiera dane od swojego partnera tylko jeden raz.

Uzgodnienie wspólnego klucza przez trzy strony jest już nieco bardziej skomplikowane i wymaga zastosowania protokołu dwurundowego. Oto jego przebieg:

1. Pierwsza runda.
   (a) Strona A losuje liczbę $a \in [0, n-1]$ i wyznacza aP, które wysyła stronie B.

(b) Strona B losuje liczbę $b \in [0, n-1]$ i wyznacza bP, które wysyła stronie C.

(c) Strona C losuje liczbę $c \in [0, n-1]$ i wyznacza cP, które wysyła stronie A.

2. Druga runda.

(a) Strona A wyznacza na podstawie a i cP wartość acP, które wysyła stronie B.

(b) Strona B wyznacza na podstawie b i aP wartość abP, które wysyła stronie C.

(c) Strona C wyznacza na podstawie c i bP wartość bcP, które wysyła stronie A.

	Strona A	Strona B	Strona C
Runda 1	a, cP	b, aP	c, bP
Runda 2	a, cP, bcP	b, aP, acP	c, bP, abP
Wyznacza	$K = a(bcP)$	$K = b(acP)$	$K = c(abP)$

Za uzgodnioną wartość przyjmuje się element $K = abcP$.

W tym miejscu rodzi się naturalne pytanie: czy istnieje protokół jednorundowy, który obsłużyłby trzy strony? Pytanie to pozostawało otwarte do 2000 roku, kiedy to Joux zaproponował nadzwyczaj proste rozwiązanie wykorzystujące odwzorowanie dwuliniowe [1]. Jego artykuł od razu znalazł się w centrum uwagi ludzi zajmujących się kryptografią. Niedługo po tym pojawiły się kolejne ciekawe propozycje oparte na odwzorowaniach dwuliniowych, a konkretnie na parowaniu punktów krzywej eliptycznej. Do najbardziej znanych należą dzisiaj

1. schemat szyfrowania oparty na identyfikatorach (Boneh i Franklin) [2],
2. schemat *krótkiego* podpisu (Boneh, Lynn i Shacham) [3].

2 Odwzorowania dwuliniowe

Przyjmijmy, że n jest liczbą pierwszą. Niech $G_1 = \langle P \rangle$ będzie grupą cykliczną rzędu n o zapisie addytywnym i elemencie neutralnym ∞, a G_T niech będzie grupą cykliczną rzędu n o zapisie multyplikatywnym i elemencie neutralnym 1. Wtedy odwzorowanie dwuliniowe możemy zdefiniować następująco:

Definicja 1 *Odwzorowaniem dwuliniowym na* (G_1, G_T) *nazywamy takie przekształcenie*

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

które spełnia następujące warunki:

1. *(Dwuliniowość) Dla każdego* $R, S, T \in G_1$, $\hat{e}(R+S, T) = \hat{e}(R, T)\hat{e}(S, T)$ *oraz* $\hat{e}(R, S+T) = \hat{e}(R, S)\hat{e}(R, T)$.
2. *(Niezdegenerowanie)* $\hat{e}(P, P) \neq 1$.
3. *(Obliczalność) Wartość* $\hat{e}(P, R)$ *może być efektywnie wyznaczona.*

□

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 $S = \infty$.

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.

Bezpieczeństwo wielu protokołów opartych na odwzorowaniach dwuliniowych opiera się na trudności obliczeniowej następującego problemu.

Definicja 2 *Jeśli $\hat{e}$ jest odwzorowaniem dwuliniowym, to dwuliniowy problem Diffiego-Hellmana definiujemy następująco: Mając dane P, aP, bP i cP należy wyznaczyć $\hat{e}(P,P)^{abc}$.* □

Zauważmy, że trudność obliczeniowa dwuliniowego problemu Diffiego-Hellmana implikuje trudność problemu Diffiego-Hellmana zarówno w grupie G_1 jak i G_T. Aby to wykazać załóżmy najpierw, że potrafimy efektywnie rozwiązać problem DH w grupie G_1. Jeżeli tak jest, to na podstawie aP i bP możemy wyznaczyć abP, co prowadzi do znalezienia $\hat{e}(abP, cP) = \hat{e}(P,P)^{abc}$. Jeśli natomiast znamy efektywną metodę rozwiązania problemu DH w grupie G_T, to obliczając $g = \hat{e}(P,P)$, $g^{ab} = \hat{e}(aP,bP)$, $g^c = \hat{e}(P,cP)$ możemy wyznaczyć $g^{abc} = \hat{e}(P,P)^{abc}$. Niestety nic więcej nie wiadomo na temat dwuliniowego problemu DH. Zakłada się jednak, że jest on w ogólności tak samo trudny jak problem DH zarówno w G_1, jak i w G_T.

Na koniec zauważmy jeszcze, że istnienie odwzorowania dwuliniowego pozwala rozwiązać decyzyjny problem DH w grupie G_1. Polega on na odpowiedzi na pytanie, czy dana czwórka elementów P, aP, bP i cP spełnia zależność $abP = cP$. Wykorzystując odwzorowanie dwuliniowe możemy zapisać $\gamma_1 = \hat{e}(P,cP) = \hat{e}(P,P)^c$ i $\gamma_2 = \hat{e}(aP,bP) = \hat{e}(P,P)^{ab}$. Oznacza to, że równość $abP = cP$ zachodzi wtedy i tylko wtedy, gdy $\gamma_1 = \gamma_2$.

3 Protokoły wykorzystujące odwzorowania dwuliniowe

3.1 Jednorundowe uzgodnienie klucza przez trzy strony

Załóżmy, że dysponujemy efektywnym obliczeniowo odwzorowaniem dwuliniowym na grupach G_1 i G_T, w którym dwuliniowy problem DH jest trudny. Takie odwzorowanie może stanowić podstawę następującego jednorundowego protokołu uzgadniania klucza dla trzech uczestników:

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.

Zobaczmy teraz, że po tej rundzie wszyscy uczestnicy są w stanie wygenerować wspólny sekret.

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

Naturalnym pytaniem, które nasuwa się po przeanalizowaniu powyższego schematu, jest pytanie o możliwość zastosowania odwzorowań wieloliniowych $\hat{e}_l : G_1^{l-1} \to G_T$. Takie odwzorowania dawałyby możliwość jednorundowego uzgodnienia klucza przez l uczestników protokołu. Kwestia istnienia odwzorowań wieloliniowych pozostaje nadal otwarta.

3.2 Kryptografia oparta na identyfikatorach

W roku 1984 Shamir [4] przedstawił koncepcję kryptografii opartej na identyfikatorach, której zadaniem było rozwiązanie problemów powstających podczas zarządzania certyfikatami. Propozycja Shamira zakładała, że:

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).

Koncepcja Shamira doczekała się praktycznej realizacji dopiero w roku 2001, kiedy to Boneh i Franklin [2] zaproponowali identyfikatorowy schemat szyfrowania oparty na odwzorowaniach dwuliniowych. Schemat ten zakłada, że:

1. Dysponujemy dwuliniowym odwzorowaniem $\hat{e} : G_1 \to G_T$, dla którego dwuliniowy problem DH jest obliczeniowo trudny.
2. Istnieją funkcje skrótu H_1 i H_2 takie, że:
$$H_1 : \{0,1\}^* \to G_1 \setminus \{\infty\} \quad \text{i} \quad H_2 : G_T \to \{0,1\}^l.$$
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 T jest powszechnie dostępny).

Gdy użytkownik A potrzebuje klucza prywatnego d_A, wtedy zaufana trzecia strona (ZTS) tworzy identyfikator ID_A, wyznacza klucz $d_A = tQ_A = tH_1(ID_A)$ i przesyła go zabezpieczonym kanałem do użytkownika. Zauważmy, że klucz prywatny d_A można traktować jako podpis ZTS pod identyfikatorem ID_A.

Aby zaszyfrować wiadomość $m \in \{0,1\}^l$ przy użyciu schematu Boneha-Franklina musimy wykonać następujące czynności:

1. Wyznaczamy klucz publiczny na podstawie identyfikatora $Q_A = H_1(ID_A)$.
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:

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

Aby odzyskać wiadomość m z szyfrogramu (R, c) należy wyznaczyć $\hat{e}(Q_A, T)^r$ na podstawie (P, Q_A, T, R), a to jest dwuliniowy problem DH.

Należy podkreślić, że opisana metoda zapewnia co prawda ochronę przed biernym atakiem, ale jest podatna na atak z wybranym szyfrogramem. Istnieją jednak modyfikacje, które eliminują ten problem.

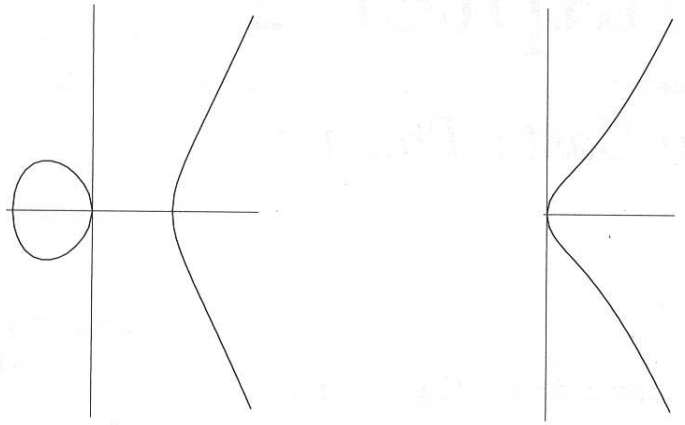
4 Krzywe eliptyczne

Krzywa eliptyczna E nad ciałem K zdefiniowana jest przez nieosobliwe równanie Weierstrassa:

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

gdzie $a_1, a_2, a_3, a_4, a_6 \in K$. Zbiór $E(K)$ jest zbiorem punktów K-wymiernych krzywej i składa się z punktu w nieskończoności ∞ oraz tych punktów $(x, y) \in K \times K$, które spełniają równanie krzywej. Jeśli K jest ciałem skończonym $\mathbb{F}_q$ charakterystyki p, to twierdzenie Hassego daje ograniczenie na liczbę punktów K-wymiernych:

$$(\sqrt{q} - 1)^2 \leq |E(K)| \leq (\sqrt{q} + 1)^2.$$



Rysunek 1: Przykłady krzywych eliptycznych na płaszczyźnie rzeczywistej

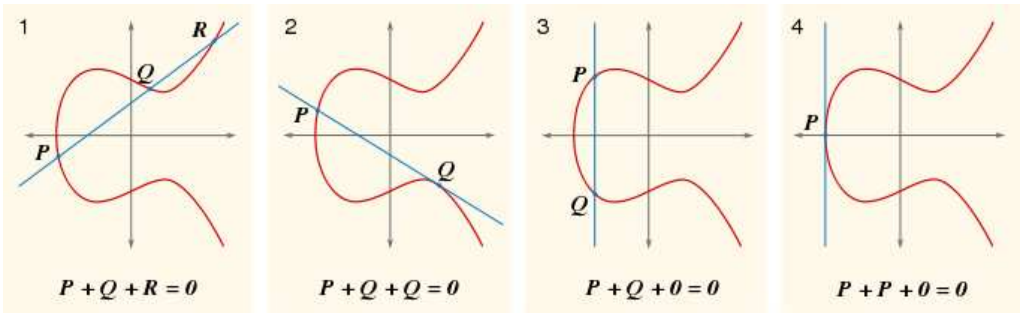
Dlatego możemy przyjąć, że $|E(K)| = q + 1 - t$, gdzie $|t| \leq 2\sqrt{q}$. Jeśli $p \mid t$, to mówimy, że krzywa E jest *superosobliwa*.

W przypadku, gdy $p > 3$, to równanie Weierstrassa można uprościć stosując liniową zamianę zmiennych do postaci:

$$E : Y^2 = X^3 + aX + b,$$

gdzie $a, b \in K$ i $4a^3 + 27b^2 \neq 0$. Podobne uproszczone formuły można również wyprowadzić dla przypadku $p = 2$ i $p = 3$.

Metoda siecznej i stycznej pokazuje w jaki sposób definiowane jest działanie grupowe na punktach krzywej eliptycznej. Działanie grupowe na punktach krzywej zdefiniowanej nad ciałem liczb rzeczywistych zostało zilustrowane na rysunku 2.



Rysunek 2: Operacje na punktach krzywej eliptycznej

Załóżmy teraz, że punkt $P \in E(\mathbb{F}_q)$ spełnia następujące warunki:

1. jest punktem rzędu n,
2. jego rząd jest liczbą pierwszą,
3. liczby n i q są względnie pierwsze.

Wtedy problem logarytmu dyskretnego w grupie $\langle P \rangle$ definiujemy następująco:

> Mając dany punkt P i punkt $Q \in \langle P \rangle$ należy znaleźć taką liczbę całkowitą l, która spełnia równanie $lP = Q$.

Aktualnie najlepszą metodą rozwiązywania tego problemu jest algorytm ρ-Pollarda [5], którego oczekiwany czas działania jest rzędu $O(\sqrt{n})$. Jeśli $n \approx q$, to czas działania wspomnianego algorytmu jest wykładniczy względem $\log q$. Należy zauważyć, że istnieją również inne metody rozwiązywania problemu logarytmu dyskretnego, które mają zastosowanie dla konkretnych rodzajów krzywych. W szczególności można zastosować iloczyn Weila i Tatea, aby przenieść problem z grupy punktów krzywej, do grupy multyplikatywnej ciała skończonego $\mathbb{F}_{q^k}$ [6]. Liczbę k nazywamy wtedy *stopniem osadzenia* krzywej i definiujemy ją następująco.

Definicja 3 *Załóżmy, że E jest krzywą eliptyczną zdefiniowaną nad ciałem $\mathbb{F}_q$, a $P \in E(\mathbb{F}_q)$ jest punktem o rzędzie pierwszym n. Jeśli* $\mathrm{nwd}(n, q) = 1$, *to stopniem osadzenia $\langle P \rangle$ nazywamy najmniejszą liczbę całkowitą k, dla której zachodzi $n \mid q^k - 1$.* □

Jeśli stopień osadzenia jest niski, to stosując iloczyn Weila możemy wykorzystać podwykładnicze algorytmy znajdowania logarytmu dyskretnego (metoda indeksu), które mogą okazać się szybsze w $\mathbb{F}_{q^k}$ niż algorytm Pollarda w $\langle P \rangle$. Z tego właśnie powodu w kryptografii opartej na problemie logarytmu dyskretnego na krzywej eliptycznej stosuje się tylko takie krzywe, których stopień osadzenia jest duży.

Ostatnio krzywe eliptyczne o niewielkim stopniu osadzenia wracają do łask. Dzieje się tak dlatego, że dają one możliwość efektywnej realizacji iloczynu Weila i Tatea, co w efekcie prowadzi do odwzorowań dwuliniowych.

5 Iloczyn Tate i algorytm Millera

Niech E będzie krzywą eliptyczną o współczynnikach z ciała $K = \mathbb{F}_q$ zadaną przez równanie Weierstrassa $r(X, Y) = 0$. Niech ponadto $\overline{K}$ będzie domknięciem algebraicznym ciała K.

Dywizorem na E nazywamy formalną sumę punktów krzywej $D = \sum_{P \in E} n_P(P)$, w której co najwyżej skończona liczba współczynników n_P jest niezerowa. Zbiór punktów $P \in E$ o niezerowych współczynnikach n_P nazywamy *nośnikiem* D. Dywizor nazwiemy *zerowym* jeśli spełnia warunek $\sum_{P \in E} n_P = 0$. Powiemy, że dywizor jest określony nad ciałem K jeśli

$$D^\sigma = \sum_P n_P(P^\sigma) = D$$

dla wszystkich automorfizmów σ ciała $\overline{K}$ będących identycznością na K. Przyjmujemy przy tym, że $P^\sigma = (\sigma(x), \sigma(y))$ jeśli $P = (x, y)$ i $\infty^\sigma = \infty$. Zbiór wszystkich dywizorów określonych nad ciałem K oznaczamy przez $\mathrm{Div}_K(E)$.

Przez $K(E)$ oznaczać będziemy ciało ułamków $K[X, Y]/r(X, Y)$. Dywizorem funkcji $f \in K(E)$ nazywamy sumę formalną $\mathrm{div}(f) = \sum_{P \in E} m_P(P)$, w której m_P jest krotnością, z jaką P wchodzi do rozkładu f na czynniki (ujemne wartości przyjmowane są w przypadku biegunów). Dywizory funkcji należących do $K(E)$ nazywamy *dywizorami głównymi*. Poniższe twierdzenie pozwala na ich dokładne określenie.

Twierdzenie 1 *Dywizor $D = \sum_{P \in E} n_P(P)$ jest dywizorem głównym wtedy i tylko wtedy, gdy*

$$\sum_{P \in E} n_P = 0 \quad i \quad \sum_{P \in E} n_P(P) = \infty.$$

Powiemy, że dwa dywizory $D_1, D_2 \in \mathrm{Div}_K(E)$ są równoważne $D_1 \sim D_2$ jeżeli istnieje taka funkcja wymierna $f \in K(E)$, że $D_1 = D_2 + \mathrm{div}(f)$. Jeśli $f \in K(E)$ i $D = \sum n_P(P) \in \mathrm{Div}_K(E)$ są takie, że mają rozdzielne nośniki, to można zdefiniować $f(D)$ jako

$$f(D) = \prod_{P \in E} f(P)^{n_P}.$$

5.1 Iloczyn Tatea

Załóżmy, że $|E(\mathbb{F}_q)| = hn$, gdzie n jest pewną liczbą pierwszą taką, że $\mathrm{nwd}(n, q) = 1$. Niech ponadto k będzie najmniejszą liczbą całkowitą, dla której zachodzi $n \mid q^k - 1$. Zbiór wszystkich punktów $P \in E(\overline{K})$ spełniających zależność $nP = \infty$ (punkty rzędu n) będziemy oznaczali przez $E[n]$ (można wykazać, że

$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$). Ponadto przez μ_n oznaczymy podgrupę rzędu n grupy $\mathbb{F}_{q^k}^{\times}$.

Zanim zdefiniujemy iloczyn Tatea, dodamy jeszcze kilka dodatkowych założeń, które uproszczą opis. Przyjmijmy, że $n \nmid q-1$ (czyli $k > 1$). Ponieważ $E[n] \subset E(\mathbb{F}_{q^k})$ i $|E[n]| = n^2$, to $n^2 \mid |E(\mathbb{F}_{q^k})|$ i $n \nmid |E(\mathbb{F}_{q^k})|/n^2$.

Definicja 4 *Niech $P, Q \in E[n]$ i niech f_P będzie funkcją spełniającą warunek $div(f_P) = n(P) - n(\infty)$ (f ma n-krotne zero w P i n-krotny biegun w ∞). 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 $D_Q = (Q+R) - (R)$ (taki wybór punktu R gwarantuje, że D_Q i $div(f_P)$ będą miały rozłączne nośniki). Przez iloczyn Tatea rozumiemy odwzorowanie*

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

zdefiniowane następująco:

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

□

Można wykazać, że tak określone odwzorowanie jest dobrze określone i nie zależy od wyboru funkcji f_P oraz punktu R. Ponadto odwzorowanie to jest niezdegenerowanym odwzorowaniem dwuliniowym.

5.2 Algorytm Millera

W tej części opiszemy algorytm Millera [7], który pozwala efektywnie wyznaczyć iloczyn Tatea. Kluczowym elementem tego algorytmu jest procedura wyznaczania funkcji f_P o dywizorze $n(P) - n(\infty)$.

Dla każdego $i \geq 1$, niech f_i będzie funkcją, której dywizor jest równy

$$\mathrm{div}(f_i) = i(P) - (iP) - (i-1)(\infty).$$

Przy takiej definicji mamy $f_1 = 1$ i $f_n = f_P$. Poniższy lemat pokazuje w jaki sposób efektywnie wyznaczyć f_n.

Lemat 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*

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

Dowód: Ponieważ linie l i v wyrażają działanie grupowe na punktach krzywej E, to możemy zapisać

$$\begin{aligned}
\mathrm{div}(f_i f_j \frac{l}{v}) &= \mathrm{div}(f_i) + \mathrm{div}(f_j) + \mathrm{div}(l) - \mathrm{div}(v) \\
&= (i(P) - (iP) - (i-1)(\infty)) + (j(P) - (jP) - (j-1)(\infty)) \\
&\quad +((iP) + (jP) + (-(i+j)(P)) - 3(\infty)) \\
&\quad -(((i+j)(P)) + (-(i+j)(P)) - 2(\infty)) \\
&= (i+j)(P) - (i+j)(P) - (i+j-1)(\infty) \\
&= \mathrm{div}(f_{i+j}).
\end{aligned}$$

■

Niech $n = (n_t, \ldots, n_1, n_0)_2$ będzie binarną reprezentacją liczby n. Funkcja f_P może być efektywnie wyznaczona metodą dodawań i podwojeń podczas przechodzenia kolejnych bitów liczby n *od lewej do prawej*.

Podczas wyznaczania iloczynu Tetea konieczne jest znalezienie jedynie wartości funkcji f_P w punktach $Q+R$ i R. Dlatego też algorytm Millera wyznacza w każdej swojej iteracji jedynie wartości funkcji f_i we wspomnianych punktach.

1. Niech $n = (n_t, \ldots, n_1, n_0)_2$ będzie binarną reprezentacją liczby n.
2. Wybieramy punkt $R \in E[n] \setminus \{\infty, P, -Q, P-Q\}$.

3. Przyjmujemy $f \leftarrow 1$, $T \leftarrow P$.
4. Dla i od t do 0 wykonujemy:
   (a) Wyznaczamy prostą l, styczną do krzywej w punkcie T.
   (b) Wyznaczamy pionową prostą v przechodzącą przez punkt $2T$.
   (c) $T \leftarrow 2T$.
   (d) $f \leftarrow f^2 \cdot \frac{l(Q+R)}{v(Q+R)} \cdot \frac{v(R)}{l(R)}$.
   (e) Jeśli $n_i = 1$ to
      i. Wyznaczamy prostą l przechodzącą przez punkty T i P.
      ii. Wyznaczamy pionową prostą v przechodzącą przez punkt $T + P$.
      iii. $T \leftarrow T + P$.
      iv. $f \leftarrow f \cdot \frac{l(Q+R)}{v(Q+R)} \cdot \frac{v(R)}{l(R)}$.
5. Obliczamy $f^{(q^k-1)/n}$.

Niestety iloczyn Tatea nie spełnia jednego z założeń, których wymagaliśmy od odwzorowania dwuliniowego – grupa $E[n]$ nie jest cykliczna. Aby rozwiązać ten problem należy znaleźć taki endomorfizm $\Psi : E \rightarrow E$, dla którego $\Psi(P) \notin \langle P \rangle$. Wtedy odwzorowanie $\hat{e}(Q, R) = e(Q, \Psi(Q))$ będzie spełniało wszystkie warunki definicji odwzorowania dwuliniowego.

6 Podsumowanie

W artykule zaprezentowane zostały nowe mechanizmy kryptograficzne, które można uzyskać stosując parowanie punktów krzywej eliptycznej. Okazuje się, że możliwość parowania punktów krzywej pozwala na konstrukcję takich schematów, jak:

1. Jednorundowe uzgodnienie kluczy pomiędzy trzema stronami.
2. Szyfrowanie oparte na identyfikatorach.

Należy podkreślić, że ta dziedzina kryptografii znajduje się obecnie w fazie bardzo intensywnego rozwoju. Efektem tego jest duża liczba publikacji dotyczących możliwości praktycznego wykorzystania iloczynu Tatea, algorytmu Millera oraz parowania puntów krzywej.

Literatura

[1] A. Joux, "A one round protocol for tripartite Diffie-Hellman", *Algorithmic Number Theory: 4th International Symposium*, pp. 263–267, 2000.

[2] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing", *Advances in Cryptology – CRYPTO 2001*, pp. 586–615, 2001.

[3] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing", *Advances in Cryptology – ASIACRYPT 2001*, pp. 297–319, 2001.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes", *Advances in Cryptology – CRYPTO 84*, pp. 47–53, 1984.

[5] J. Pollard, "Monte Carlo methods for index computation mod p", *Mathematics of Computation*, pp. 918–924, 1978.

[6] A. Menezes, T. Okamoto, S. Vanstone, "Reducing elliptic courve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, pp. 1639–1646, 1993.

[7] V. Miller, "The Weil pairing, and its efficient calculation", *Journal of Cryptology*, pp. 235–261, 2004.