II. KRZYWE ELIPTYCZNE I ICH ZASTOSOWANIE W KRYPTOLOGII

ZASTOSOWANIE KRZYWYCH ELIPTYCZNYCH DO KONSTRUKCJI BEZPIECZNYCH ALGORYTMÓW I PROTOKOŁÓW KRYPTOGRAFICZNYCH

Mariusz Jurkiewicz, Jerzy Gawinecki, Piotr Bora, Tomasz Kijko

Wojskowa Akademia Techniczna Wydział Cybernetyki,
Instytut Matematyki i Kryptologii,
00-908 Warszawa, ul. S. Kaliskiego 2

Streszczenie. Celem artykułu jest zaprezentowanie metod doboru bezpiecznych krzywych eliptycznych stosowanych do konstruowania protokołów kryptograficznych oraz sprzętową implementacje koprocesora realizującego operacje arytmetyczne na tej rodzinie krzywych algebraicznych.

Słowa kluczowe: Krzywe eliptyczne, stopień zanurzeniowy, logarytm dyskretny, krotność punktu.

1. Wstęp

Obecnie w celu uzgodnienia kluczy kryptograficznych a także realizacji podpisu cyfrowego wykorzystywane są algorytmy klucza publicznego. Podstawą bezpieczeństwa tych algorytmów są problemy trudne obliczeniowo takie jak faktoryzacja dużych liczb (algorytm RSA) albo wyznaczanie logarytmu dyskretnego (protokół Diffiego-Hellmana). Przykładem dziedziny wykorzystującej trudność znajdowania logarytmu dyskretnego jest grupa punktów krzywej eliptycznej zdefiniowana nad ciałem skończonym. Okazuje się, że nie każda grupa punktów zapewnia odpowiedni poziom bezpieczeństwa. Podejmiemy trud opisania metod wykrywania oraz radzenia sobie z tymi problemami.

Kolejne zagadnienie dotyczy sprzętowych implementacji koprocesora realizującego operacje na krzywych eliptycznych. Wspomaganie sprzętowe obliczeń dla systemów klucza publicznego na krzywych eliptycznych musi być rozpatrywane w trzech warstwach:

- wykonywanie operacji elementarnych w ciele,
- metody reprezentacji punktu, a co za tym idzie potok obliczeń dla podwajania i dodania punktów na krzywej eliptycznej,
- metody realizacji krotności punktu na krzywej eliptycznej.

Najczęściej spotykanymi rozwiązaniami są systemy budowane na krzywych nad ciałami liczbowymi lub nad ciałami wielomianów o współczynnikach z ciała charakterystyki 2. Spośród operacji elementarnych w ciele najbardziej czaso- i elementochłonną jest mnożenie modularne. Zarówno w rozwiązaniu budowanym nad ciałem liczbowym, jak i nad ciałem wielomianów najmniej efektywnym jest rozwiązanie mnożenia modularnego tzw. podstawowe. Najczęściej przechodzi się w reprezentacji czynników działania na postać czy to residuów, czy baz normalnych. W przypadku metod reprezentacji punktu na krzywej również odchodzi się od reprezentacji bezpośredniej – afinicznej, na rzecz reprezentacji ogónie nazywanych rzutowymi. Unikamy tu częstego liczenia inwersji elementu w ciele, zostawiając ją na koniec obliczeń wyliczania krotności celem korekcji wyniku do reprezentacji we współrzędnych afinicznych.

Ostatnią grupą zagadnień są metody wyznaczania krotności punktu. Podstawowym rozwiązaniem jest metoda binarna, jednak często przechodzi się na metodę dodawań-odejmowań, okien w-szerokich, m-arną, "drabiny Montgomery'ego", metodę z dzieleniem punktu lub innych.

Dobre zestawienie operacji we wszystkich trzech warstwach obliczeń umożliwia nam uzyskanie rozwiązania sprzętowego modułu wyznaczania krotności punktu o stosunkowo małych wymaganiach sprzętowych i szybkim wyznaczaniu wyniku.

2. Wprowadzenie algebraiczne

Rozpoczniemy od zaprezentowania kilku znanych faktów algebraicznych stanowiących trzon aplikacyjny matematyki w kryptologii asymetrycznej. Szczegółowe informacje dotyczące przedstawionych tu kwestii można znaleść np. w [4], [6]. Niech dany będzie zbiór S. Dowolną funkcję $\otimes : S \times S \to S$ nazywamy działaniem w S. Działanie nazywamy:

(i) *łącznym*, gdy $a \otimes (b \otimes c) = (a \otimes b) \otimes c$, dla $a, b, c \in S$;
(ii) *z elementem neutralnym*, gdy istnieje $e \in S$, że $e \otimes a = a \otimes e = a$, dla $a \in S$;
(iii) *przemiennym*, gdy $a \otimes b = b \otimes a$, dla $a, b \in S$.
(iv) *odwracalnym*, gdy dla $a \in S$ istnieje a^{-1}, że $a \otimes a^{-1} = a^{-1} \otimes a = e$;

Zbiór S z działaniem spełniającym warunki (i), (ii), (iv) nazywamy *grupą*. Jeżeli dodatkowo spełniony jest warunek (iii) grupę nazywamy *przemienną* lub *abelową*.

Zbiór R z dwoma działaniami $+, \cdot$, nazywanymi odpowiednio *„dodawaniem"* i *„mnożeniem"*, nazywamy *pierścieniem* gdy dodawanie spełnia warunki (i)-(iv) a mnożenie (i)-(iii). Ponadto obydwa działania są związane warunkiem nazywanym *rozłącznością mnożenia względem dodawania*

(v) $a \cdot (b + c) = a \cdot b + a \cdot c$, dla $a, b, c \in R$.

Elementy neutralne względem dodawania i mnożenia nazywamy odpowiednio *zerem* i *jedynką*. Zwykle zamiast pisać $a \cdot b$ piszemy ab.

Pierścień nazywamy:

- *Pierścieniem całkowitym* jeśli równość $ab = 0$ implikuje, że $a = 0$ lub $b = 0$.
- *Ciałem* jeśli mnożenie jest odwracalne, tzn. spełnia (iv).

Podzbiór $P \subset R$ nazywamy *podpierścieniem* jeśli jest pierścieniem z działaniami z R obciętymi do P. Podpierścień $J \subset R$ nazywamy *ideałem* jeśli spełniony jest warunek $ar \in J$ dla $a \in J$ oraz $r \in R$.

Najmniejszym ideałem pierścienia R, zawierającym element $a \in R$ jest ideał postaci $(a) = \{ra \mid r \in R\}$. Ideał $J \subset R$ nazywa się *głównym* jeśli istnieje $a \in R$, że $J = (a)$. Wtedy mówi się czasem, że J jest ideałem głównym *generowanym* przez a. Jeśli w dziedzinie całkowitości każdy ideał jest główny, nazywamy go *dziedziną ideałów głównych*.

Niech R oraz J będą odpowiednio, pierścieniem i jego ideałem. Wprowadzamy następującą relację w R:

$$a \equiv b \pmod{J} \text{ wtedy i tylko wtedy, gdy } a - b \in J.$$

Z łatwością można pokazać, że powyższa relacja jest relacją równoważności, dzielącą R na klasy abstrakcji oznaczane symbolem $[a] := a + J$. Zbiór wszystkich klas abstrakcji powyższej relacji oznacza się przez R/J. Jeśli w zbiorze R/J określimy działania $\oplus$ oraz $\odot$

$$(a + J) \oplus (b + J) = (a + b) + J \text{ oraz } (a + J) \odot (b + J) = ab + J,$$

to okaże się, że po pierwsze są dobrze zdefiniowane a po drugie wprowadzają w R/J strukturę pierścienia. Pierścień ten nazywamy *pierścieniem ilorazowym* lub dokładniej *pierścieniem ilorazowym pierścienia R modulo J*. W dalszy ciągu zamiast symboli $\oplus, \odot$ będziemy używać zwykłego plusa i kropki.

Element $a \in R$ nazywamy *dzielnikiem* $b \in R$ jeśli istnieje $c \in R$, że $ac = b$. Elementy odwracalne w R nazywa się *dzielnikami jedynki*. Elementy $a, b \in R$ nazywamy *stowarzyszonymi* jeśli istnieje dzielnik jedynki ϵ, że $a = \epsilon b$. Element $p \in R$ nazywa się *pierwszym* jeśli nie jest dzielnikiem jedynki oraz jego jedynymi dzielnikami są dzielniki jedynki oraz elementy z nim stowarzyszone.

Twierdzenie 1. *Niech R będzie dziedziną ideałów głównych, wtedy $R/(p)$ jest ciałem wtedy i tylko wtedy, gdy c jest elementem pierwszym pierścienia R.*

Wniosek 1. $\mathbb{Z}/(p)$ jest ciałem wtedy i tylko wtedy, gdy p jest liczbą pierwszą. Oczywiście jest to ciało skończone $\#\mathbb{Z}/(p) = p$, oznacza się je również symbolem $\mathbb{Z}_p$ lub uniwersalnym symbolem $\mathbb{F}_p$.

Niech F będzie ciałem. Zbiór wszystkich wielomianów o współczynnikach z F z działaniami dodawania i mnożenia wielomianów jest pierścieniem, który oznaczamy symbolem $F[x]$. Wielomiany stałe utożsamiamy z elementami ciała F. Łatwo stwierdzić, że jedynymi dzielnikami jedynki w $F[x]$ są niezerowe elementy F. Wielomian nazywamy *unormowanym* jeśli współczynnikiem przy najwyższej potędze jest jedynka. Elementami pierwszymi w $F[x]$ są wielomiany nierozkładalne, nazywane czasem *nieprzywiedlnymi*. Trzeba podkreślić, że nieprzywiedlność jest ściśle związana z ciałem F. Klasyczny przykład to $x^2 - 2$ który jest nieprzywiedlny nad $\mathbb{Q}$ oraz rozkładalny nad $\mathbb{R}$.

Okazuje się, że $F[x]$ *jest dziedziną ideałów głównych*, dokładniej dla dowolnego ideału $J \neq (0)$ istnieje jednoznacznie wyznaczony wielomian unormowany $f \in F[x]$ taki, że $J = (f)$. Stąd oraz twierdzenia 1, dostajemy

Twierdzenie 2. *Dla $f \in F[x]$ pierścień ilorazowy $F[x]/(f)$ jest ciałem wtedy i tylko wtedy, gdy f jest wielomianem nieprzywiedlnym nad F.*

Dla dowolnego $f \in F[x]$ przyjrzymy się elementom pierścienia $F[x]/(f)$. Jak wiadomo z wcześniejszych rozważań elementy pierścienia ilorazowego mają postać $g + (f)$. Okazuje się jednak, że każda klasa zawiera jednoznacznie wyznaczonego reprezentanta $r \in F[x]$ czyniącego zadość warunkowi $\deg r < \deg f$, jest to zwyczajnie reszta z dzielenia g przez f. Ostatnia uwaga ma ciekawe konsekwencje, mianowicie dla $F = \mathbb{F}_p$, gdzie p jest liczbą pierwszą oraz f wielomianem nieprzywiedlnym takim, że $\deg f = n \geq 0$, liczba elementów ciała $\mathbb{F}_p[x]/(f)$ jest równa liczbie wielomianów w $\mathbb{F}_p[x]$ stopni mniejszych od n, zatem $\#\mathbb{F}_p[x]/(f) = p^n$.

Twierdzenie 3. *Niech $\mathbb{F}_p$ będzie ciałem skończonym*

(i) Dla każdego $n \geq 1$ istnieje nieprzywiedlny wielomian $f \in \mathbb{F}_p[x]$ stopnia n.

(ii) Dla każdego $n \geq 1$ istnieje ciało skończone zawierające p^n elementów.

(iii) Jeśli $\mathbb{F}$ oraz $\mathbb{F}'$ są ciałami skończonymi o takiej samej liczbie elementów wtedy są izomorficzne.

Jeżeli $G \subseteq F$ jest ciałem to nazywamy je *podciałem* ciała F jeśli dodatkowo $G \neq F$ to mówimy, że G jest podciałem *właściwym*. Ciało F nazywa się również *rozszerzeniem*ciała G. Łatwo stwierdzić, że iloczyn rodziny wszystkich podciał ciała F jest również jego podciałem, które nazywamy *podciałem prostym*. Zatem podciało proste nie zawiera żadnych podciał właściwych. Okazuje się, że każde podciało proste jest izomorficzne z $\mathbb{F}_p$ lub $\mathbb{Q}$. To uzasadnia następną definicję. *Charakterystyką* ciała F nazywamy rząd jego podciała prostego. Widać, że charakterystyka ciała może być zerem lub liczbą pierwszą.

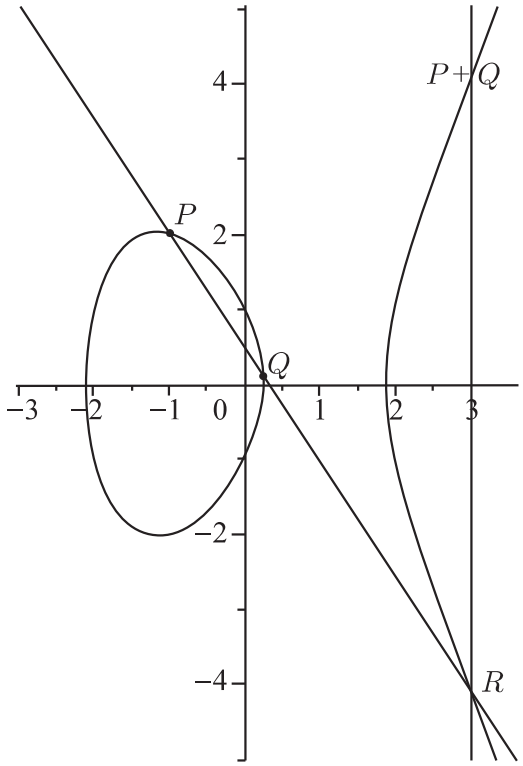
3. Krzywe eliptyczne

Rozpoczniemy od koncepcji krzywej eliptycznej (patrz np. [5], [17]). Przez chwilę będziemy poruszać się w znanym środowisku jakim są przestrzenie euklidesowe. Nazwijmy *krzywą eliptyczną* w $\mathbb{R}^2$ zbiór rozwiązań równania

$$y^2 = x^3 + ax + b. \tag{1}$$

Równania tego typu nazywa się *równaniami Weierstrassa*. Najbardziej zadziwiającą cechą krzywych eliptycznych jest możliwość zdefiniowania działania „dodawania" punktów krzywej indukującego strukturę grupy. Weźmy dwa różne punkty, powiedzmy P i Q, leżące na krzywej eliptycznej, wtedy przechodząca przez nie prosta przecina krzywą w dokładnie trzech różnych punktach $\{P, Q, -R\}$. Przyjmujemy, że wynikiem dodawania będzie punkt R krzywej, symetryczny do $-R$ względem osi odciętych.

W przypadku gdy $P = Q$ rozważamy styczną do krzywej w punkcie P i powtarzamy powyższą procedurę. Jest tu jednak pewien istotny problem, mianowicie w jaki sposób dodać punkty symetryczne względem osi odciętych lub podwoić punkt leżący dodatkowo na osi odciętych? Odpowiednia prosta będzie wówczas równoległa do osi rzędnych i oczywiście nie przetnie krzywej eliptycznej w żadnym innym punkcie. Okazuje się, że ten pozorny problem tak naprawdę jest dobrodziejstwem pozwalającym wtopić aparat algebraiczny w pojęcie krzywej. Zmienimy na chwilę punkt widzenia. Wyobraśmy sobie zanurzoną w przestrzeni płaszczyznę i stojącą na niej sferę



Rysunek 1. Dodawanie punktów na krzywej eliptycznej

jednostkową w taki sposób, że ich jedynym punktem wspólnym są odpowiednio zero i „biegun południowy" sfery. Dla dowolnego punktu płaszczyzny rozważmy prostą łączącą go z „biegunem północnym", wtedy nie licząc „bieguna" taka prosta przetnie sferę w dokładnie jednym punkcie. Oznacza to, że istnieje bijekcja pomiędzy płaszczyzną a sferą bez punktu (tzn. bez „bieguna północnego"). Pomysł polega na przypisaniu nieskończoności do tego punktu, nazywając „biegun północny" *punktem w nieskończoności* który oznaczać będziemy symbolem $\mathcal{O}$. ([1]) Wróćmy do krzywej, rzutując ją na sferę w opisany powyżej sposób widać, że każda prosta równoległa do osi rzędnych przejdzie przez punkt w nieskończoności. Dokładniej, dla punktów symetrycznych względem osi odciętych łącząca je prosta jest krzywą zamkniętą przechodzącą przez obrazy tych punktów oraz punkt w nieskończoności, analogicznie w przypadku podwajania. Nietrudno odnieść wrażenia, że punkt w nieskończoności zachowuje się jak element neutralny działania na punktach krzywej. Naturalnym pomysłem jest przeto rozszerzenie prostej o ten punkt, wtedy krzywa eliptyczna z punktem w nieskończoności oraz opisanym działaniem „dodawania punktów" staje się grupą abelową. Poniżej uściślimy zaprezentowane intuicje.

[1] Jest to tzw. jednopunktowe uzwarcenie w sensie Aleksandrowa a cała przedstawiona konstrukcja nazywa się rzutem stereograficznym.

Definicja 1. Krzywą eliptyczną nad $\mathbb{R}$ *nazywamy zbiór rozwiązań równania (1) wraz z punktem w nieskończoności* $\mathcal{O}$*, o ile stałe* a, b *spełniają dodatkowy warunek*

$$\Delta_E = -16 \cdot (4a^3 + 27b^2) \neq 0.$$

Zbiór ten oznaczamy symbolem $E(\mathbb{R})$.

Zatem krzywa eliptyczna to zbiór $E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$

Wyrażenie Δ_E nazywa się *dyskryminantem* krzywej $E(\mathbb{R})$. Warunek $\Delta_E \neq 0$ oznacza, że wielomian $x^3 + ax + b$ nie posiada pierwiastków wielokrotnych. Krzywe dla których dyskryminant się zeruje posiadają osobliwości i działanie „dodawania" przestaje zachowywać się właściwie.

Opisany powyżej sposób dodawania punktów na krzywej eliptycznej w wersji algebraicznej przyjmuje postać następującego twierdzenia:

Twierdzenie 4. (Algorytm dodawania punktów na krzywej eliptycznej) *Niech* $E(\mathbb{R})$ *będzie krzywą eliptyczną oraz* $P_1, P_2 \in E(\mathbb{R})$*, wtedy:*

- *Jeśli* $P_1 = \mathcal{O}$ *to* $P_1 + P_2 = P_2$
- *W przeciwnym wypadku, jeśli* $P_2 = \mathcal{O}$ *to* $P_1 + P_2 = P_1$
- *W przeciwnym wypadku, niech* $P_1 = (x_1, y_1)$ *oraz* $P_2 = (x_2, y_2)$
  - ▷ *Jeśli* $x_1 = x_2$ *oraz* $y_1 = -y_2$*, wtedy* $P_1 + P_2 = \mathcal{O}$
  - ▷ *W przeciwnym wypadku, określmy*

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \text{dla} P_1 \neq P_2 \\ \\ \dfrac{3x_1^2 + a}{2y_1} \text{dla} P_1 = P_2 \end{cases}$$

i niech $x_3 = \lambda^2 - x_1 - x_2$ *oraz* $y_3 = \lambda(x_1 - x_3) - y_1$*. Wtedy* $P_1 + P_2 = (x_3, y_3)$.

Twierdzenie 5. *Krzywa eliptyczna* $E(\mathbb{R})$ *wraz z wyżej określonym działaniem „dodawania" jest grupą abelową.*

Powyżej przedstawiliśmy intuicyjną definicję krzywej eliptycznej nad $\mathbb{R}$, jednak chcąc znaleść zastosowanie krzywych eliptycznych w kryptologii jesteśmy zmuszeni zmienić scenę. Dokładniej, interesować nas będą analogony powyższych definicji jednak z tą różnicą, że tym razem współczynniki krzywej będą elementami ciała $\mathbb{F}_p$. Zatem,

Definicja 2. Krzywą eliptyczną nad $\mathbb{F}_p$ *nazywamy zbiór*

$$E(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\} \tag{3}$$

przy założeniu, że dyskryminant spełnia warunek

$$\Delta_E = -16 \cdot (4a^3 + 27b^2) \neq 0 \pmod{\text{char}(\mathbb{F}_p)}. \tag{4}$$

Uwaga 1. Z powodów które podamy poniżej zakładamy, że $p \geq 3$.
Jest rzeczą zdumiewającą, że geometrycznie określone działanie „dodawania" punktów krzywej eliptycznej nad $\mathbb{R}$ przenosi się bez zmian oraz z zachowaniem wszystkich zasadniczych własności na przypadek ciała skończonego o charakterystyce większej niż dwa.

Twierdzenie 6. *Niech $P, Q \in E(\mathbb{F}_p)$, wtedy:*

(i) Algorytm dodawania opisany w twierdzeniu 4 zastosowany do P i Q zwraca element z $E(\mathbb{F}_p)$.

(ii) Zbiór $E(\mathbb{F}_p)$ wraz z działaniem dodawania punktów krzywej eliptycznej jest (skończoną) grupą abelową.

Na podstawie poprzedniego twierdzenia wiemy, że krzywa eliptyczna nad ciałem skończonym (z chwilowym ograniczeniem na charakterystykę) jest grupą abelową. Naturalne pytanie dotyczy ilości elementów tej grupy. Spróbujmy z grubsza oszacować ten problem. Ustalając $x_0 \in \mathbb{F}_p$, dostaniemy trzy możliwości w odniesieniu do wartości wyrażenia $x_0^3 + ax + b$. Po pierwsze może się zdarzyć, że wielkość ta da się spierwiastkować modulo p, co da nam dwa punkty z $E(\mathbb{F}_p)$. W przybliżeniu taka sytuacja występuje w około 50% wypadków. Drugi przypadek to brak możliwości spierwiastkowania, co zdarza się również w około połowie sytuacji. Na koniec wartość wyrażenia może być równa zero, wtedy otrzymamy dokładnie jeden punkt z $E(\mathbb{F}_p)$. Jednak taki przypadek może zajść dla co najwyżej trzech elementów $\mathbb{F}_p$. Podsumowując możemy oczekiwać, że $\#E(\mathbb{F}_p) \approx 50\% \cdot 2 \cdot p + 1 = p + 1$ (1 odpowiada za punkt w nieskończoności).

Znane twierdzenie Hassego, później uogólnione przez Weil'a i Deligne'a mówi, że nasze oczekiwania są spełnione z dokładnością do pewnych losowych wielkości.

Twierdzenie 7. (Hasse) *Niech $E(\mathbb{F}_p)$ będzie krzywą eliptyczną. Wtedy*

$$\#E(\mathbb{F}_p) = p + 1 - t_p, \quad \text{przy czym } |t_p| \leq 2\sqrt{p}.$$

Wielkość

$$t_p = p + 1 - \#E(\mathbb{F}_p)$$

nazywa się śladem Frobeniusa dla $E(\mathbb{F}_p)$.

Twierdzenie Hassego pozwala nam oszacować $\#E(\mathbb{F}_p)$, jednak nie dostarcza narzędzi do wyznaczenia tej wielkości. Oczywiście można zastosować metodę typu podstaw i sprawdź, jednak jest ona ekstremalnie nie efektywna zajmuje czas $O(p)$. W pracy [15] Schoof pokazał algorytm wyznaczania $\#E(\mathbb{F}_p)$ w czasie $O((\ln p)^8)$. Algorytm Schoof'a został następnie ulepszony przez Elkies'a i Atkin'a, zyskując znaczenie praktyczne (złożoność $O((\ln p)^6)$) i jest aktualnie znany jako SEA (patrz [16]).

Powróćmy do definicji 2 z której wynika, że wszystko dobrze działa dopóki dyskryminant nie jest zerem. Jednak z (4) dostajemy natychmiast, że w ciałach postaci $\mathbb{F}_{2^k}$ równość $\Delta_E = 0$ jest zawsze prawdziwa, gdyż $\mathrm{char}(\mathbb{F}_{2^k}) = 2$, co można czytać $2 = 0$. W tej sytuacji konieczne jest uogólnienie pojęcia krzywej eliptycznej:

Definicja 3. Krzywą eliptyczną *nazywamy zbiór rozwiązań* uogólnionego równania Weierstrassa

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5}$$

wraz z punktem w nieskończoności $\mathcal{O}$. *Współczynniki* $a_1, \ldots a_6$ *muszą czynić zadość równości* $\Delta \neq 0$, *gdzie* dyskryminant Δ *definiujemy następująco*

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6,$$

gdzie

$$d_2 = a_1^2 + 4a_2, \quad d_4 = 2a_4 + a_1a_3, \quad d_6 = a_3^2 + 4a_6,$$
$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Równanie (5) ma najogólniejszą postać i w przypadku ciała o charakterystyce większej niż dwa[2] można ją sprowadzić do krzywej postaci (3) za pomocą trywialnego przekształcenia. Zmiany polegają na tym, że pracując z postacią (5) zmianie ulega algorytm dodawania punktów. Dokładniej odbicie względem osi odciętych $(x, y) \mapsto (x, -y)$ wynikające z definicji geometrycznej trzeba zastąpić bardziej technicznym warunkiem $(x, y) \mapsto (x, -y - a_1x - a_3)$. Jest to jednocześnie formuła opisująca punkt przeciwny do danego.

[2] Zakwalifikowanie krzywych eliptycznych nad ciałem charakterystyki 3 do klasy analizowanych równaniem (3) ma charakter czysto teoretyczny, gdyż istnieją takie krzywe dla których dyskryminant jest niezerowy. Jednak w praktyce przypadek ten włącza się do sytuacji opisywanej równaniem (5), gdyż wtedy jesteśmy w stanie ogarnąć znacznie większą liczbę krzywych.

4. Praktyczne zastosowania krzywych eliptycznych

4.1. Problem logarytmu dyskretnego

Bieżącą sekcję zakończymy opisując jeden z głównych powodów uzasadniających użycie krzywych eliptycznych w kryptologii. Podobnie jak wyżej wróćmy na krótki moment do zbioru liczb rzeczywistych. Wyobraźmy sobie sytuację w której dwoje głównych aktorów sceny kryptologicznej, Alicja i Bob ustalają pewną liczbę rzeczywistą $g \geq 1$, następnie Alicja wybiera w sekrecie liczbę n, możemy spokojnie założyć, że będzie to liczba naturalna i publikuje liczbę $q = g^n$. Aktualnie abstrahujemy od pytania w jakim celu to robi. Adwersarz na podstawie informacji o postaci g oraz q musi odkryć n. Natychmiast widać, że $n = \log_g q$, czyli problem sprowadza się do rozwiązania klasycznego równania logarytmicznego znanego z podstawowego kursu matematyki, co naturalnie w rozważanym przypadku nie stanowi najmniejszego problemu.

Wróćmy do krzywych eliptycznych i spróbujmy powtórzyć powyższą konstrukcję, zobaczymy czy w tym przypadku rozwiązanie jest równie trywialne. Rozważmy grupę punktów krzywej eliptycznej $E(\mathbb{F}_p)$, gdzie jak wiadomo p jest liczbą pierwszą lub potęgą liczby pierwszej. Alicja wybiera punkt $P \in E(\mathbb{F}_p)$ oraz $n \in \mathbb{N}$ i oblicza

$$Q = \underbrace{P + P + \ldots P}_{n-1 \text{ dodawań w } \mathrm{E}(\mathbb{F}_p)} = [n]P,$$

następnie publikuje P oraz Q. Na podstawie tych danych przeciwnik musi wyznaczyć n, czyli rozwiązać proste na pierwszy rzut oka równanie. Jednak tym razem równanie już proste nie jest. Mianowicie, okazuje się, że techniczna trudność definicji dodawania punktów krzywej eliptycznej wraz z arytmetyką modularną w ciele $\mathbb{F}_p$, czyni ten problem niezwykle trudnym obliczeniowo, przynajmniej dla dużych p. *Najszybszy znany algorytm rozwiązuje opisany problem w grupie punktów krzywej eliptycznej $E(\mathbb{F}_p)$ o rzędzie r (r – liczba pierwsza) w nie mniej niż $O(\sqrt{r})$ krokach.*

Definicja 4. *Niech $E(\mathbb{F}_p)$ będzie krzywą eliptyczną nad ciałem skończonym $\mathbb{F}_p$ oraz niech $P, Q \in E(\mathbb{F}_p)$.* Problemem logarytmu dyskretnego na krzywej eliptycznej (ECDLP) nazywamy problem znalezienia liczby naturalnej n takiej, że $Q = [n]P$. W analogii do klasyki szukaną liczbę oznaczamy

$$n = \log_P Q,$$

i mówimy, że n jest dyskretnym logarytmem eliptycznym o podstawie P z Q.

Zwróćmy uwagę na fakt, że w powyższa definicja zawiera pewną lukę, mianowicie mogą istnieć punkty P, Q leżące na krzywej takie, że Q nie jest wielokrotnością P. Wtedy oczywiście wyrażenie $\log_P Q$ nie jest określone. Z praktycznego punktu widzenia nie jest to żadne ograniczenie, gdyż mając opublikowane P oraz Q wiadomo, że odpowiadający im ECDLP jest rozwiązywalny. Druga sprawa którą chcemy podkreślić jest niejednoznaczność rozwiązania. Dokładniej jeżeli istnieje n takie, że $n = \log_P Q$ wówczas takich rozwiązań jest nieskończenie wiele, w związku ze skończonością grupy $E(\mathbb{F}_p)$. Tak naprawdę wartość $\log_P Q$ jest elementem zbioru $\mathbb{Z}/(s)$, gdzie s jest rzędem punktu P, co więcej jeśli n_0 jest jakimkolwiek rozwiązaniem ECDLP to również są nimi wszystkie liczby postaci $n = n_0 + ks$, $k \in \mathbb{N}$. Zaletą spojrzenia na opisywane zagadnienie w ten sposób jest to, że dyskretny logarytm eliptyczny spełnia równanie:

$$\log_P(Q_1 + Q_2) = \log_P(Q_1) + \log_P(Q_2), \quad \text{dla} Q_1, Q_2 \in E(\mathbb{F}_p).$$

Należy zwrócić uwagę na fakt, że znaki plus po dwóch stronach równości oznaczają dwa różne działania w różnych strukturach algebraicznych, odpowiednio w $E(\mathbb{F}_p)$ oraz $\mathbb{Z}/(s)$. Dodatkowo zdefiniujemy w tym miejscu pojęcia stopnia zanurzeniowego i anomalnej krzywej eliptycznej, które będą wykorzystywane przy omawianiu wymagań stawianych bezpiecznym kryptograficznie krzywym eliptycznym.

Definicja 5. Niech E będzie krzywą eliptyczną nad ciałem $\mathbb{F}_q$, gdzie $q = p^m$, gdzie p jest liczbą pierwszą. Dodatkowo niech r będzie największym dzielnikiem pierwszym $\#E(\mathbb{F}_q)$. Stopniem zanurzeniowym (embeded degree, MOV) krzywej eliptycznej $E(\mathbb{F}_q)$ nazywamy najmniejsza liczbę naturalną l taką, że zachodzi

$$r|(q^l - 1).$$

Należy zwrócić uwagę, że dla $r = p$ stopień zanurzeniowy nie istnieje.

Definicja 6. Krzywą eliptyczną E zdefiniowaną nad $\mathbb{F}_q$ nazywamy anomalną, gdy największy dzielnik pierwszy r rzędu grupy punktów $\#E(\mathbb{F}_q)$ jest równy charakterystyce ciała $\mathbb{F}_q$.

4.2. Wymagania bezpieczeństwa

Wszystkie kryptosystemy oparte o krzywe eliptyczne bazują na trudności obliczenia logarytmu dyskretnego w grupie punktów krzywej eliptycznej ECDLP. Dlatego też wymagania bezpieczeństwa w ogromnym stopniu

są związane z istniejącymi algorytmami służącymi do wyznaczania logarytmu dyskretnego na krzywych eliptycznych. Część z tych algorytmów pozwala także na obliczanie logarytmu dyskretnego w grupie multiplikatywnej ciała skończonego i w addytywnej grupie jaką jest jakobian krzywej hipereliptycznej. Warto w tym miejscu opisać krótko wybrane algorytmy, gdyż ich charakterystyka posłuży nam do zdefiniowania wymaganych własności jakimi powinna cechować się bezpieczna krzywa eliptyczna.

1. *Pełne przeszukanie (atak brutalny).* Jeżeli szukamy takiej wartości całkowitej α, dla której zachodzi $Q = [\alpha]P$, to możemy dla kolejnych β od 1 obliczać punkty na krzywej $R = [\beta]P$ i sprawdzać, czy $R = Q$. Jeśli równość zajdzie, to szukana wartość α jest równa aktualnej wartości β. Atak ten wymaga w najgorszym przypadku wyznaczenia wszystkich elementów grupy generowanej przez punkt P.
2. *Meroda ρ-Pollarda.* Metoda ta została przedstawiona przez Pollarda (patrz [12]). Opiera się ona na paradoksie dnia urodzin. W algorytmie tym dwa elementy grupy B (w naszym przypadku dwa punkty krzywej eliptycznej) poruszają się z różną „prędkością" po pseudolosowej trajektorii, aż do momentu znalezienia się w cyklu i dogonienia elementu „wolniejszego" przez element „szybszy"[3]. Metoda ta wymaga w przybliżeniu pierwiastka z $\#B$ operacji w grupie. Przyjmując założenie, że 2^{128} operacji nie uda się wykonać w rozsądnym czasie, to wymagamy, aby $\#B > 2^{256}$.
3. *Metoda Pohliga-Hellmana.* Metoda ta pozwala na zredukowanie problemu obliczenia logarytmu dyskretnego w grupie $E(\mathbb{F}_q)$, której rząd rozkłada się na czynniki pierwsze postaci $\#E(\mathbb{F}_q) = \prod p_i^{a_i}$ do wyznaczenia logarytmu dyskretnego w podgrupach o rzędach równych p_i (patrz [9]). Wynika z tego, że problem logarytmu dyskretnego w grupie $E(\mathbb{F}_q)$ jest tak trudny, jak problem logarytmu dyskretnego w podgrupie rzędu r, gdzie r jest równe największemu p_i. Dlatego też zalecane jest aby $\#E(\mathbb{F}_q)$ był liczbą pierwszą, albo $\#E(\mathbb{F}_q) = k \cdot r$, gdzie r jest liczbą pierwszą a k jest małe (np. mniejsze niż 5).
4. *Metoda wykorzystująca anomalne krzywe eliptyczne.* W 1998 Semaev przedstawił metodę o złożoności wielomianowej (patrz [14]) pozwalającą na sprowadzenie problemu logarytmu dyskretnego w grupie $E(\mathbb{F}_q)$ krzywej anomalnej do problemu wyznaczenia wielokrotności w addytywnej grupie ciała $\mathbb{F}_q$. Ruck rozwiną tę metodę dla przypadku krzywych hipereliptycznych ([13]). Należy więc unikać stosowania krzywych anomalnych.

[3] Opis dotyczy jednej z wersji tego algorytmu (wersji nie wymagającej pamiętania trajektorii). Istnieją wersje tego algorytmu w których po pseudolosowej trajektorii porusza się tylko jeden punkt, jednak wymagają one pamiętania punktów na trajektorii.

5. *Atak MOV i Freya-Rucka.* Menezes, Okamoto i Vanstone (patrz [8]) oraz Frey i Ruck (patrz [3]) pokazali, że jeżeli dla krzywej eliptycznej $E(\mathbb{F}_q)$ o rzędzie podzielnym przez dużą liczbę pierwszą r istnieje stopień zanużeniowy l, to istnieje homomorfizm grup z podgrupy $E(\mathbb{F}_q)$ o rzędzie r w podgrupę grupy multiplikatywnej ciała $\mathbb{F}_{q^l}$. W przypadku, gdy l jest małe (nie większe niż 50), zamiast wyznaczać logarytm dyskretny w $E(\mathbb{F}_q)$, to po przekształceniu szybciej otrzymamy rezultat dla podgrupy grupy $\mathbb{F}^*_{q^l}$.
6. *Ataki typu „cover".* Ataki tego typu bazują na zaproponowanej przez Freya (patrz [2]) idei, że dla pewnych (nie wszystkich) krzywych eliptycznych $E(\mathbb{F}_{q^m})$ istnieją krzywe hipereliptyczne $C(\mathbb{F}_q)$ takie, że grupa punktów $E(\mathbb{F}_{q^m})$ jest homomorficzna z jakobianem krzywej $C(\mathbb{F}_q)$. W przypadku, gdy genus krzywej C jest nieco większy od m, to obliczeniowo opłacalne jest przejście (przy pomocy homomorfizmu) z grupy punktów krzywej E do jakobianu krzywej C, i w tej grupie wyznaczenie logarytmu dyskretnego. Aby uniknąć takiej sytuacji zalecane jest, aby unikać krzywych eliptycznych (w ogólnym przypadku hipereliptycznych), dla których stopień rozszerzenia ciała bazowego m jest mały. Sugerowane jest aby stosować krzywe zdefiniowane nad ciałem prostym $\mathbb{F}_p$ albo nad $\mathbb{F}_{2^m}$ z m będącym liczbą pierwszą.

Podsumowując powyższe rozważania można określić, jakimi parametrami powinna charakteryzować się bezpieczna kryptograficznie krzywa eliptyczna. Są nimi:

1. q powinna być liczbą pierwszą ($q = p$) albo$q = 2^m$ i m jest liczbą pierwszą.
2. Liczba r powinna być liczbą większą niż 2^{256}.
3. Liczba r nie może dzielić q.
4. Stopień zanurzenia l powinien być większy od 50.

Opis warunków bezpieczeństwa stawianych przed krzywymi eliptycznymi w aspekcie zastosowań kryptograficznych oraz zalecane do wykorzystania krzywe można znaleść w [1], [11].

Dodatkowo zaleca się, aby iloraz rzędu krzywej $\#E(\mathbb{F}_q)$ przez r (oznaczony przez k) nie powinien przekroczyć 4.

4.3. Przykłady bezpiecznych krzywych eliptycznych

Przedstawimy teraz przykłady krzywych eliptycznych do zastosowań kryptograficznych (spełniających wymagania bezpieczeństwa). Przykłady te zostały wyznaczone zarówno dla przypadku, gdy krzywa eliptyczna zdefiniowana jest nad ciałem charakterystyki 2 jak i ciałem prostym.

4.3.1. Krzywe eliptyczne nad ciałami charakterystyki 2

Niech $E(\mathbb{F}_{2^m})$ będzie krzywą eliptyczną na ciałem $\mathbb{F}_{2^m}$ opisaną równaniem (5). Wtedy możemy sprowadzić równanie tej krzywej do jednego z dwóch równań

$$E_1(\mathbb{F}_{2^m}) \ : \ y^2 + xy = x^3 + b_2x^2 + b_6, \qquad (\text{gdy } a_1 \neq 0),$$

albo

$$E_2(\mathbb{F}_{2^m}) \ : \ y^2 + b_3y = x^3 + b_4x + b_6, \qquad (\text{gdy } a_1 = 0).$$

Krzywe eliptyczne $E(\mathbb{F}_{2^m})$ i $E_1(\mathbb{F}_{2^m})$ (albo $E(\mathbb{F}_{2^m})$ i $E_2(\mathbb{F}_{2^m})$) są izomorficzne, a także izomorficzne są ich grupy punktów.

Na potrzeby praktycznych zastosowań szukaliśmy krzywych eliptycznych $E(\mathbb{F}_{2^{281}})$ o równaniu:

$$E(\mathbb{F}_{2^{281}}) \ : \ y^2 + xy = x^3 + b_6, \tag{6}$$

gdzie $\mathbb{F}_{2^{281}} \cong \mathbb{F}_2[t]/(f(t))$, przy czym wielomian f jest nieprzywiedlny nad $\mathbb{F}_{2^{281}}$ (patrz Twierdzenie 3) i ma postać

$$\begin{aligned} f(t) = t^{281} &+ t^{280} + t^{278} + t^{277} + t^{276} + t^{273} + t^{272} + t^{262} + t^{261} + t^{260} \\ &+ t^{257} + t^{256} + t^{230} + t^{229} + t^{228} + t^{225} + t^{224} + t^{217} + t^{216} \\ &+ t^{214} + t^{213} + t^{212} + t^{209} + t^{208} + t^{198} + t^{197} + t^{196} + t^{193} \\ &+ t^{192} + t^{153} + t^{152} + t^{150} + t^{149} + t^{148} + t^{145} + t^{144} + t^{134} \\ &+ t^{133} + t^{132} + t^{129} + t^{128} + t^{25} + t^{24} + t^{22} + t^{21} + t^{20} \\ &+ t^{17} + t^{16} + t^{6} + t^{5} + t^{4} + t + 1. \end{aligned}$$

Wyznaczone zostały trzy krzywe eliptyczne zdefiniowane nad wybranym ciałem opisane równaniem (6) przedstawione w Tabeli 1. Współczynniki b_6 w równaniach krzywych zostały zapisane w postaci heksadecymalnej[4].

4.3.2. Krzywe eliptyczne nad ciałem prostym

Na potrzeby praktycznych zastosowań szukaliśmy krzywych eliptycznych $E(\mathbb{F}_p)$ o równaniu:

$$E(\mathbb{F}_p) \ : \ y^2 = x^3 - 3x + b, \tag{7}$$

[4] Oznaczenia współczynników r i k jak w podrozdziale 4.2.

Tabela 1

Bezpieczne krzywe eliptyczne nad ciałem $\mathbb{F}_{2^{281}}$

Krzywa eliptyczna 1.	
b_6	0xC89B77ED7DAC9E3F00298E09C1ABD4546401E1EDC2\\ 219265826B6E638788C3C6BDECF
r	971334446112864535459730953411759453321203 50\\ 661220484393992280233745866707028078193 3 $\approx 2^{279}$
k	2
Krzywa eliptyczna 2.	
b_6	0x3029C1EEA22882E032CC968936E9A79CF49517B3D2\\ 230C2614A0C495D2E6C84C9A199C
r	971334446112864535459730953411759453321202 49\\ 239295095937441051901129613083551699424 7 $\approx 2^{279}$
k	2
Krzywa eliptyczna 3.	
b_6	0x23B5B7F7D2BE7EA4E097515298455DBFC7E3228A20\\ B3A37B8C8B52B76174B95E0D2147
r	971334446112864535459730953411759453321202 92\\ 775976982301563382340206871795885841918 1 $\approx 2^{279}$
k	2

gdzie $p = 2^{288} - 2^{224} - 2^{64} - 1$.

Wyznaczone zostały trzy krzywe eliptyczne zdefiniowane nad wybranym ciałem opisane równaniem (7) przedstawione w Tabeli 2.

5. Praktyczna realizacja arytmetyki na krzywych eliptycznych

Główną operacją w systemach wykorzystujących technologię klucza publicznego na krzywych eliptycznych jest wyznaczenie krotności punktu $[k]P$, gdzie P jest punktem krzywej eliptycznej a k liczbą całkowitą. Do realizacji tego zadania należy rozpatrzyć obliczenia w trzech warstwach:

- w warstwie obliczeń w ciele charakterystyki 2 lub p szybkie mnożenie w ciele,
- w warstwie reprezentacji krzywej, dla ominięcia czasochłonnego liczenia wielokrotnego inwersji elementu w ciele,
- w warstwie metod wyznaczania krotności punktu.

Tabela 2

Bezpieczne krzywe eliptyczne nad ciałem $\mathbb{F}_p$

Krzywa eliptyczna 1.	
b	46434666704580341340259055902747977740358974\\ 54392091081371144908744414258809152977737 89
r	49732323640978664212842230147967020030578915\\ 28289128726616608518761304752515915957465 81 $\approx 2^{288}$
k	1
Krzywa eliptyczna 2.	
b	14732881112350622874811312589591370839680442\\ 43105312076444408832890195297848162721130 60
r	49732323640978664212842230147967020030578916\\ 28257463259318435905415732402897998519997 51 $\approx 2^{288}$
k	1
Krzywa eliptyczna 3.	
b	20137344272582920889432431100201652193397174\\ 49453420802303602893781644196827693905175 74
r	49732323640978664212842230147967020030578916\\ 61757216467295712663315173256463767031183 29 $\approx 2^{288}$
k	1

W warstwie obliczeń w ciele najistotniejsze jest mnożenie modularne. Dla rozwiązań nad ciałem charakterystyki 2 wykorzystuje się np. algorytm Karatsuby (patrz [7]) lub mnożenia elementów przekształconych do postaci baz normalnych. Dla rozwiązań nad ciałem charakterystyki p wykorzystuje się najczęściej przekształcenie czynników mnożenia do postaci residuów i realizacji obliczeń np. z wykorzystaniem algorytmu Montgomery'ego (patrz [10]).

W warstwie reprezentacji krzywej przechodzi się z postaci afinicznej na reprezentację krzywej w jednej z postaci rzutowych. Dla rozwiązań nad ciałem charakterystyki 2 wykorzystuje się najczęściej postać współrzędnych rzutowych Lopeza-Dahaba. Dla rozwiązań nad ciałem charakterystyki $p > 2$ postać współrzędnych rzutowych ważonych nazywana jest również jakobianowymi.

W warstwie metod wyznaczania krotności punktu spotyka się metody:

- binarną,
- dodawania-odejmowania,
- tzw. „complementary recording" (gdy wartość k zapisana w NKB posiada dużą liczbę jedynek),

- $2r$-arna,
- okna w-szerokiego,
- tzw. „drabina Montgomery'ego",
- mnożenia skalarnego Montgomery'ego,
- łańcuchów dodawania-odejmowania punktu,
- z wykorzystaniem reprezentacji Zeckendora liczby k,
- z dzieleniem punktu,
- skalarną dla obliczeń typu $[k_1]P + [k_2]Q$,
- okienek z rozwinięciem znakowym m-arnym.

Dla porównania efektywności wykorzystania powyższych rozwiązań często w literaturze spotyka się zestawienia dotyczące kosztów – ilości mnożeń dla realizacji konkretnej krotności punktu, jednak należy tu również uwzględnić bezpieczeństwo implementacji. Tu jedynie dwie ostatnie warstwy grają szczególną rolę. W warstwie reprezentacji krzywej należy wybrać rozwiązanie oferujące równowagę pomiędzy ilością operacji dla podwajania i dodania punktu na krzywej, natomiast w warstwie liczenia krotności możliwość ukrycia charakterystyki bitów obliczanej krotności. Tu szczególnie predestynowane są rozwiązania naturalnie bezpieczne, jak np. mnożenia skalarnego Montgomery'ego.

6. Podsumowanie

Z powyższych rozważań płyną naturalne wnioski dotyczące doboru krzywych eliptycznych do konstrukcji bezpiecznych algorytmów o nie opartych. W przypadku praktycznych implementacji tych algorytmów warto zwrócić uwagę na realizacje sprzętowe, gdyż

- można efektywnie realizować rozwiązania klucza publicznego oparte na krzywych eliptycznych w oparciu o platformy procesorowe lub struktury programowalne, osiągając bardzo duże przepływności,
- można wyznaczyć np. krotność punktu w czasie ok 5 ms w przypadku systemu budowanego nad ciałem $\mathbb{F}_{2^m}$ z m rzędu 400 (m musi być liczbą pierwszą) i implementację koprocesora w strukturze programowalnej,
- można realizować obliczenia w sposób bezpieczny i odporny na ataki typu „side channel".

Literatura

[1] Certicom Research. *SEC 2: Recommended Elliptic Curve Domain Parameters*, 2010.

[2] G. Frey, *How to disguise an elliptic curve (Weil descent)*, Talk at ECC'98, Waterloo, 1998.

[3] G. Frey and H.-G. Ruck, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp., 62(206):865–874, 1994.

[4] J. Gawinecki, J. Szmidt, *Zastosowanie ciał skończonych i funkcji boolowskich w kryptografii*, BelStudio, 2001.

[5] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.

[6] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, revised edition, 1994.

[7] A. Karatsuba and Y. Ofman, *Multiplication of Multidigit Numbers on Automata*, *Soviet Phys. Doklady* 7(7):595596, 1963.

[8] A.J. Menezes, T. Okamoto, and S.A. Vanstone, *Reducing elliptic curve logarithms to logarithms is a finie field*, IEEE Trans. Information Theory, 39(5):1639–1646, 1993.

[9] S.C. Pohlig and M.E. Hellman, *An improved algorithm for computing logarithms over $gf(p)$ and its cryptographic significances*, IEEE Trans. Information Theory, IT-24(1):106–110, 1978.

[10] P.L. Montgomery, *Modular multiplication without trial division*, Mathematics of Computation, 78:315–333, 1985.

[11] PKN, *PN-ISO/IEC 15946-1. Technika informatyczna – Techniki zabezpieczeń – Techniki kryptografii oparte na krzywych eliptycznych – Część 1: Postanowienia ogólne*, 2005.

[12] J.M. Pollard, *Monte carlo methods for index computation* $(\mathrm{mod}\, p)$, Math. Comp., 32(143):918–924, 1978.

[13] H.-G. Ruck, *On the discrete logarithm in the divisor class group of curves*, Math. Comp., 68(226):805–806, 1999.

[14] I. A. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp., 67(221):353–356, 1998.

[15] R. Schoof, *Elliptic curves over finite fields and the computation of square roots* $\mathrm{mod}\, p$, Math. Comp., 44(170):483–494, 1985.

[16] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théor, Nombres Bordeaux, 7(1):219–254, 1995. Les Dix-huitiémes Journées Arithmétiques (Bordeaux, 1993).

[17] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Discrete Mathematics and Its Applications. Chapman & Hall/CRC, 2003.

APPLICATIONS OF ELLIPTIC CURVES FOR CONSTRUCTION OF SECURE CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

Abstract. The main purpose of this paper is to present some methods of choosing secure ECs for construction of cryptographical protocols and hardware implementation of coprocesor that performs aritmetical operations over this set of algebraic curves.

Keywords: elliptic curve, embedding degree, discrete logarithm, point multiplication.