Jak krzywe eliptyczne chronią twoje dane?

Kryptografia krzywych eliptycznych

Jan Kocierz

10 maja 2026

Politechnika Krakowska
Studenckie Koło Naukowe Matematyków PK



Plan prezentacji

Motywacja - klasyczny protokół Diffiego–Hellmana

Matematyka krzywych eliptycznych

Krzywe eliptyczne nad ciałem skończonym

Bezpieczeństwo krzywych eliptycznych

Zastosowanie krzywych eliptycznych - ECDH

Krzywe stosowane w praktyce

Podsumowanie

Co z ECC w erze postkwantowej?

Motywacja - klasyczny protokół Diffiego–Hellmana

Klasyczny protokół Diffiego-Hellmana - grupa $\mathbb{Z}_p^*$

Parametry publiczne: p, g.

Alicja

- Wybiera tajne $a \in \{1, \ldots, p-2\}$,
- Oblicza $A = g^a \pmod{p}$,
- Wysyła A,
- Odbiera B,
- **Sekret:** $K = B^a \pmod{p}$.

Bob

- Wybiera tajne $b \in \{1, \ldots, p-2\}$,
- Oblicza $B = g^b \pmod{p}$,
- Wysyła B,
- Odbiera A,
- **Sekret:** $K = A^b \pmod{p}$.

$$K = (g^b)^a = \mathbf{g^{ab}} = (g^a)^b \pmod{p}$$

Definicja

Niech g będzie generatorem grupy multiplikatywnej $\mathbb{Z}_p^*$ (gdzie p jest liczbą pierwszą). Dla danego $h \in \mathbb{Z}_p^*$, **logarytm dyskretny** z h przy podstawie g to liczba całkowita $x \in \{0, 1, \ldots, p-2\}$ taka, że

$$g^x \equiv h \pmod{p}.$$

Oznaczamy:

$$x = \log_g h \pmod{p}.$$

Matematyka krzywych eliptycznych

Krzywe eliptyczne nad $\mathbb{R}$

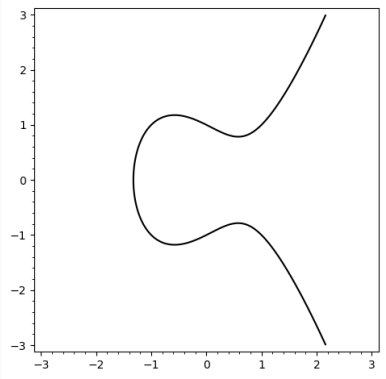
Definicja

Niech $a, b \in \mathbb{R}$ będą takie, że $4a^3 + 27b^2 \neq 0$. Krzywą eliptyczną nad $\mathbb{R}$ nazywamy zbiór $\mathcal{E}$ rozwiązań $(x, y) \in \mathbb{R}^2$ równania

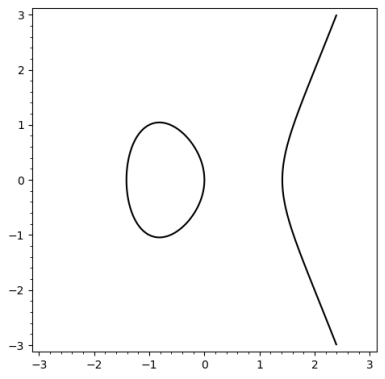
$$y^2 = x^3 + ax + b,$$

wraz ze specjalnym punktem $\mathcal{O}$ nazywanym punktem w nieskończoności.

Przykłady krzywych eliptycznych



Rysunek 1: Krzywa $y^2 = x^3 - x + 1$.
Opracowanie własne.



Rysunek 2: Krzywa $y^2 = x^3 - 2x$.
Opracowanie własne.

Dodawanie punktów — wzory algebraiczne

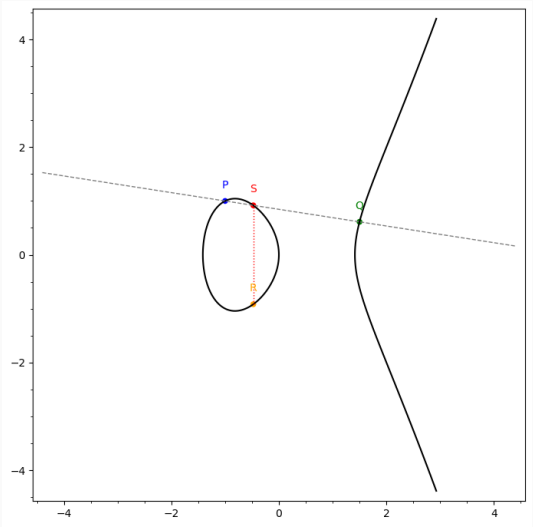
Definicja

Niech $\mathcal{E}(\mathbb{R})$ będzie krzywą eliptyczną oraz $P_1, P_2 \in \mathcal{E}(\mathbb{R})$, wtedy:

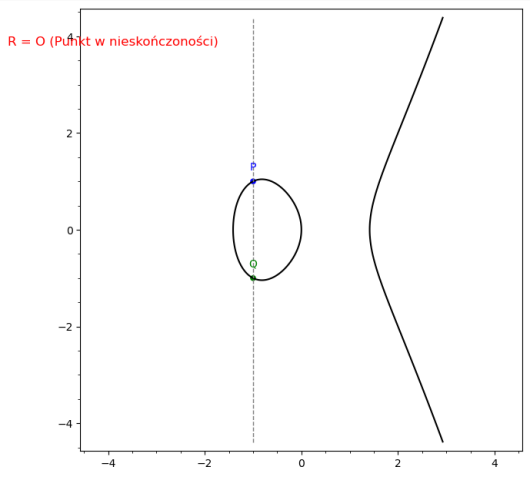
- Jeśli $P_1 = \mathcal{O}$, to $P_1 + P_2 = P_2$
- Jeśli $P_2 = \mathcal{O}$, to $P_1 + P_2 = P_1$
- W przeciwnym przypadku, niech $P_1 = (x_1, y_1)$ oraz $P_2 = (x_2, y_2)$
  - Jeśli $x_1 = x_2$ oraz $y_1 = -y_2$, wtedy $P_1 + P_2 = \mathcal{O}$
  - W przeciwnym przypadku, określmy

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

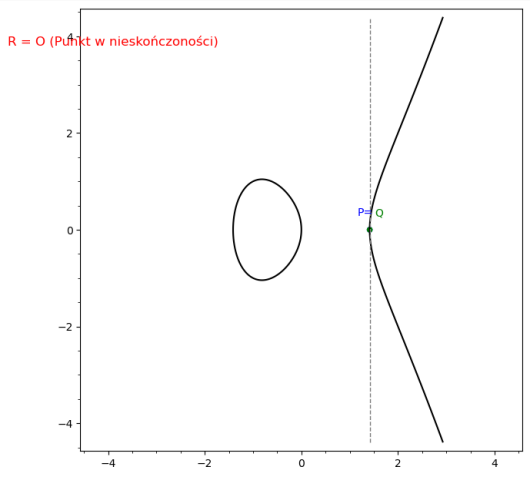
i niech $x_3 = \lambda^2 - x_1 - x_2$ oraz $y_3 = \lambda(x_1 - x_3) - y_1$. Wtedy $P_1 + P_2 = (x_3, y_3)$.



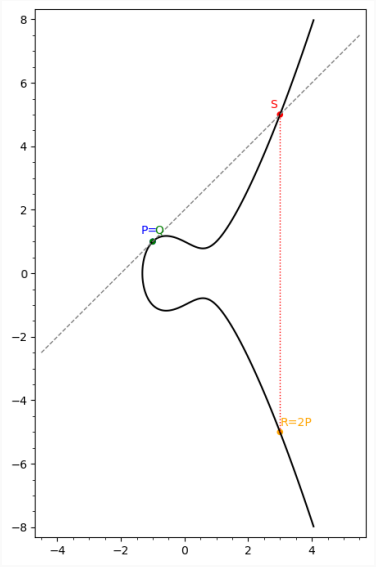
Rysunek 3: Dodawanie punktów na krzywej $y^2 = x^3 - 2x$.



Rysunek 4: Dodawanie punktów przeciwnych na krzywej $y^2 = x^3 - 2x$.



Rysunek 5: Wielokrotność punktu P na krzywej $y^2 = x^3 - 2x$.



Rysunek 6: Wielokrotność punktu P na krzywej $y^2 = x^3 - x + 1$.

Kluczowa obserwacja

Twierdzenie

$(\mathcal{E}, +)$, gdzie $\mathcal{E}$ to krzywa eliptyczna, a $+$ to dodawanie na niej punktów zdefiniowane jak na początku rozdziału, jest grupą abelową.

Krzywe eliptyczne nad ciałem skończonym

Krzywe eliptyczne nad ciałem skończonym

Definicja

Niech $p > 3$ będzie liczbą pierwszą oraz $a, b \in \mathbb{F}_p$ takie, że $4a^3 + 27b^2 \neq 0 \pmod{p}$. Krzywą eliptyczną nad ciałem $\mathbb{F}_p$ nazywamy zbiór

$$\mathcal{E}(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \; y^2 = x^3 + ax + b\},$$

wraz ze specjalnym punktem $\mathcal{O}$ zwanym punktem w nieskończoności.

Twierdzenie

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

Krzywe eliptyczne nad dowolnym ciałem

Definicja

Krzywą eliptyczną nazywamy zbiór rozwiązań uogólnionego równania Weierstrassa

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

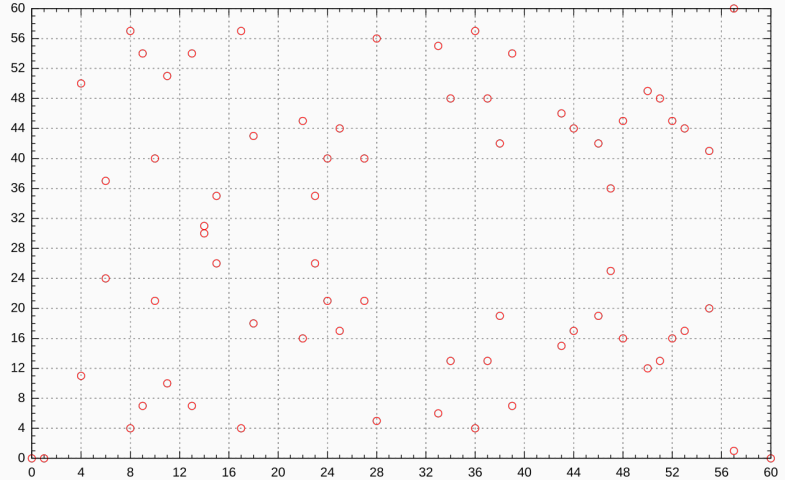
wraz z punktem w nieskończoności $\mathcal{O}$. Współczynniki $a_1, \ldots, a_6$ muszą spełniać warunek $\Delta \neq 0$, gdzie Δ definiujemy następująco

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

przy czym

$$d_2 = a_1^2 + 4a_2, \quad d_4 = 2a_4 + a_1 a_3, \quad d_6 = a_3^2 + 4a_6,$$

$$d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2.$$



Rysunek 7: Krzywa $y^2 = x^3 - x$ nad ciałem $\mathbb{F}_{61}$.

Optymalizacja obliczania nP - przykład

Chcemy obliczyć $13P$:

$$13 = (1101)_2$$

Zaczynamy od elementu neutralnego (tzn. punktu w nieskończoności): $R = \mathcal{O}$.

$$\begin{aligned}
\text{bit 1:} \quad & R = 2\mathcal{O} + P = P \\
\text{bit 1:} \quad & R = 2P + P = 3P \\
\text{bit 0:} \quad & R = 2(3P) = 6P \\
\text{bit 1:} \quad & R = 12P + P = 13P
\end{aligned}$$

Wynik:

$$\boxed{13P}$$

Bezpieczeństwo krzywych eliptycznych

Problem logarytmu dyskretnego na krzywej eliptycznej (ECDLP)

Definicja

Niech $\mathcal{E}(\mathbb{F}_p)$ będzie krzywą eliptyczną nad ciałem skończonym $\mathbb{F}_p$ oraz niech $P, Q \in \mathcal{E}(\mathbb{F}_p)$. Problemem logarytmu dyskretnego na krzywej eliptycznej nazywamy problem znalezienia liczby $n \in \mathbb{N}$ takiej, że $Q = nP$. Szukaną liczbę oznaczamy

$$n = log_P Q$$

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

Brakujące definicje

Definicja

Podgrupą cykliczną grupy punktów na krzywej eliptycznej generowaną przez punkt P nazywamy zbiór wszystkich punktów, które możemy uzyskać przez wielokrotne dodawanie P do siebie: $\langle P \rangle = \{P, 2P, 3P, ..., sP = \mathcal{O}\}$.

Definicja

Liczbę s z poprzedniej definicji nazywamy rzędem punktu P, jest to najmniejsza z liczb całkowitych dodatnich n, dla których $nP = \mathcal{O}$.

Ataki ogólnego przeznaczenia

Niech dane będą: punkt bazowy $G \in \mathcal{E}(\mathbb{F}_p)$, $P \in \langle G \rangle$, $\#\langle G \rangle = N$ oraz $Q = nP$.

- **Baby-step, Giant-step** — algorytm deterministyczny oparty na metodzie „przecięcia połówkowego". Złożoność to $O(\sqrt{N})$ - wymaga dużych zasobów pamięciowych, więc stosowany głównie teoretycznie.
- **Pollard's** ρ — metoda probabilistyczna wykorzystująca ideę spaceru losowego po grupie, aż dwa punkty dadzą kolizję. Złożoność czasowa to $O(\sqrt{N})$.
- **Pohlig–Hellman** — wykorzystuje faktoryzację liczby N. Jeśli N ma małe czynniki pierwsze, atak rozbija ECDLP na kilka mniejszych problemów w podgrupach.

Stopień zanurzeniowy i krzywe anomalne

Definicja

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

$$r \mid (q^l - 1).$$

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

Definicja

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

Ataki specjalne

- **MOV (Menezes–Okamoto–Vanstone)** — przenosi problem logarytmu dyskretnego na krzywej eliptycznej (ECDLP) do problemu logarytmu dyskretnego (DLP) w ciele skończonym $\mathbb{F}_{q^l}$ przy użyciu parowań dwuliniowych. Skuteczny, gdy stopień zanurzeniowy l jest mały.
- **SSA (Smart-Satoh-Araki)** — atakuje krzywe anomalne, używając logarytmu p-adycznego (po podniesieniu krzywej z $\mathbb{F}_p$ do $\mathbb{Q}_p$).

Parametry bezpiecznej krzywej - podsumowanie

Aby krzywa eliptyczna była bezpieczna, należy:

1. Zapewnić duży rząd N podgrupy cyklicznej (np. 256-bitowy dla 128-bitowego bezpieczeństwa),
2. Wybrać N, które jest liczbą pierwszą lub ma duży czynnik pierwszy,
3. Unikać krzywych anomalnych i supersingularnych.

Zastosowanie krzywych eliptycznych - ECDH

Protokół Elliptic-curve Diffie–Hellman

Parametry publiczne: $q, \mathcal{E}, G, N$.

Alicja

- Wybiera tajne $a \in \{1, \ldots, N-1\}$,
- Oblicza $G_A = aG$,
- Wysyła G_A (punkt na krzywej $\mathcal{E}$),
- Odbiera G_B,
- **Sekret:** $S = aG_B$.

Bob

- Wybiera tajne $b \in \{1, \ldots, N-1\}$,
- Oblicza $G_B = bG$,
- Wysyła G_B (punkt na krzywej $\mathcal{E}$),
- Odbiera G_A,
- **Sekret:** $S = bG_A$.

$$S = a(bG) = (\mathbf{ab})\mathbf{G} = b(aG)$$

Krzywe stosowane w praktyce

secp256r1 (NIST P-256): Parametry

Równanie: $y^2 = x^3 + ax + b \pmod{p}$

- **p:** `FFFFFFFF 00000001 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF` $= 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
- **a:** `...FFFFFFFC` $= p - 3$
- **b:** `5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B`
- **Gx:** `6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296`
- **Gy:** `4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5`
- **N:** `FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551`
- **h:** `1`

secp256r1 (NIST P-256): Zastosowania

Kluczowe zastosowania (protokół ECDH)

- **TLS/SSL (HTTPS):** Najpopularniejsza krzywa do uzgadniania kluczy sesji (ECDHE).
- **JSON Web Tokens:** Często używana do podpisywania tokenów autoryzacyjnych.
- **Secure Shell:** Używana do bezpiecznej wymiany kluczy.



Rysunek 8: Wygenerowano za pomocą AI (model Google Imagen)

secp256k1: Parametry

Krzywa typu Koblitza ($a = 0, b = 7$), słynna dzięki Bitcoinowi. Zoptymalizowana pod kątem wydajności obliczeń.

Równanie: $y^2 = x^3 + 7 \pmod{p}$

- **p:** `FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F` $= 2^{256} - 2^{32} - 977$
- **a:** `...00000000`
- **b:** `...00000007`
- **Gx:** `79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798`
- **Gy:** `483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8`
- **N:** `FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141`
- **h:** `1`

secp256k1: Zastosowania

Kluczowe zastosowania (protokół ECDSA)

- **Bitcoin:** Używana do generowania par kluczy i autoryzowania transakcji poprzez podpisy cyfrowe (ECDSA).
- **Ethereum:** Podobnie jak Bitcoin, używa tej krzywej do zabezpieczania kont i transakcji.



Curve25519: Parametry

Nowoczesna krzywa Montgomery'ego (postaci $y^2 = x^3 + Ax^2 + x$) zaprojektowana przez D.J. Bernsteina.

Protokół X25519 (ECDH na Curve25519)

- **p:** 7FFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFED $= 2^{255} - 19$
- **A:** 486662
- **Gx:** 9
- **N:** Rząd podgrupy $\approx 2^{252}$
- **h:** 8

Curve25519: Zastosowania

Kluczowe zastosowania (protokół X25519)

- **Signal Protocol:** Używana do ustanawiania bezpiecznych sesji.
- **TLS 1.3:** Jeden z domyślnych mechanizmów wymiany kluczy w nowym standardzie HTTPS.
- **WireGuard:** Domyślny protokół wymiany kluczy dla tego VPN.



Podsumowanie

Podsumowanie

Zastosowanie kryptografii krzywych eliptycznych zapewnia ten sam poziom bezpieczeństwa co klasyczne systemy przy drastycznie krótszych kluczach. Bezpieczeństwo opiera się na trudności problemu logarytmu dyskretnego na krzywych, który jest odporny na klasyczne ataki typu *Index Calculus*. Pełne bezpieczeństwo wymaga stosowania sprawdzonych standardów, aby uniknąć ataków matematycznych. Krzywe eliptyczne są powszechnie stosowane w cyberbezpieczeństwie - od zabezpieczania stron WWW, przez kryptowaluty, po komunikatory i IoT, więc ECC jest fundamentem nowoczesnego Internetu.

Co z ECC w erze postkwantowej?

Przyszłość: Era Postkwantowa

- Komputery kwantowe łamią problem ECDLP w czasie wielomianowym.
- **Rozwiązanie:** Kryptografia oparta na izogeniach.
- Krzywe supersingularne powracają jako bezpieczny fundament!

Bibliografia i

- NIST SP 800-57 Part 1 Rev. 5 — Recommendation for Key Management.
- E. Rescorla, RFC 8446 — The Transport Layer Security (TLS) Protocol Version 1.3.
- D. J. Bernstein, "Curve25519: new Diffie-Hellman speed records", PKC 2006.
- L. C. Washington, "Elliptic Curves: Number Theory and Cryptography".
- SECG, "SEC 2: Recommended Elliptic Curve Domain Parameters".

Dziękuję za uwagę!

Kontakt: jan.kocierz@student.pk.edu.pl