Stefan Sokołowski

KRYPTOGRAFIA

wykład 6

Inst. Informatyki Stosowanej, ANS
Elbląg, 2026/2027

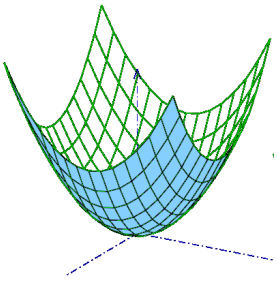
Matematyka krzywych eliptycznych

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

Jak wygladają wykresy tak zadanych funkcji?

Wykresami funkcji dwóch zmiennych są powierzchnie; np.

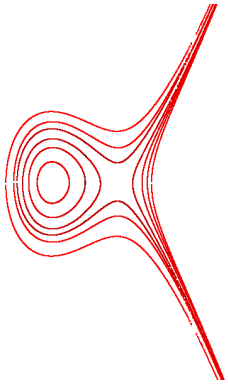
$$\left.\begin{array}{l} F : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ F(x,y) \stackrel{\text{def}}{=} x^2 + y^2 \end{array}\right\} \quad \text{paraboloida} \longrightarrow$$



Krzywe są przekrojami tych powierzchni na zadanej wysokości.

Z przekrojów na różnych wysokościach powstaje *mapa poziomicowa* powierzchni. Dla **naszej** krzywej wygląda ona tak:

$$\left.\begin{array}{l} F : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ F(x,y) \stackrel{\text{def}}{=} y^2 - x^3 - ax \end{array}\right\} \longrightarrow$$



stefan.info.pl/Dydaktyka/Krypto/Slajdy/Programy/WykresXY

Matematyka krzywych eliptycznych

Kiedy taki wykres nie wyznacza krzywej?

por. stefan.info.pl/Dydaktyka/Krypto/Slajdy/Programy/WykresXY/plaska

Jeśli $\frac{dF(x_0,y_0)}{dx} = \frac{dF(x_0,y_0)}{dy} = 0$, to w punkcie (x_0, y_0) powierzchnia wyznaczona funkcją F ma „płaskowyż" — jest całkiem pozioma; poziomica przestaje być linią.

Dla naszej funkcji $F(x,y) \stackrel{\text{def}}{=} y^2 - x^3 - ax$ to się dzieje dla takich (x,y), że

$$\begin{cases} 0 = \frac{dF(x,y)}{dx} = \frac{d(y^2-x^3-ax)}{dx} = -3x^2 - a & \text{więc } x = \left(\frac{-a}{3}\right)^{\frac{1}{2}} \\ 0 = \frac{dF(x,y)}{dy} = \frac{d(y^2-x^3-ax)}{dy} = 2y & \text{więc } y = 0 \end{cases}$$

czyli na takich punktach krzywej $y^2 = x^3 + ax + b$, że

$$0 = \left(\frac{-a}{3}\right)^{\frac{3}{2}} + a\left(\frac{-a}{3}\right)^{\frac{1}{2}} + b$$

DALEJ

Matematyka krzywych eliptycznych

Kiedy taki wykres nie wyznacza krzywej?

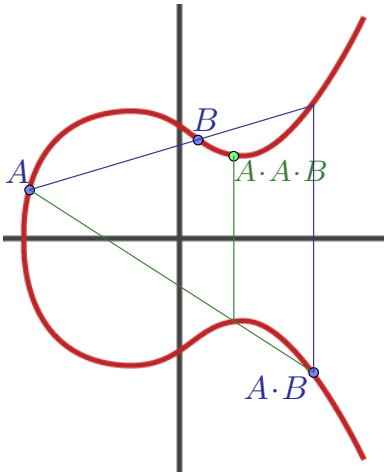
$$\begin{aligned} 0 &= \left(\frac{-a}{3}\right)^{\frac{3}{2}} + a\left(\frac{-a}{3}\right)^{\frac{1}{2}} + b \\ b^2 &= \left(\frac{-a}{3}\right)^{3} + 2\cdot\left(\frac{-a}{3}\right)^{\frac{3}{2}}\cdot a\left(\frac{-a}{3}\right)^{\frac{1}{2}} + a^2\left(\frac{-a}{3}\right) \\ b^2 &= \frac{-a^3}{27} + 2a\cdot\left(\frac{-a}{3}\right)^{2} + \frac{-a^3}{3} \\ b^2 &= \frac{-a^3}{27} + \frac{2a^3}{9} - \frac{a^3}{3} \\ b^2 &= \frac{-a^3}{27} + \frac{6a^3}{27} - \frac{9a^3}{27} \\ 27b^2 &= -4a^3 \\ \boxed{4a^3+27b^2 = 0} & \end{aligned}$$

Krzywych eliptycznych $y^2 = x^3 + ax + b$ takich, że parametry a i b spełniają **ten** warunek, należy zabronić.

Kryptografia krzywych eliptycznych — przypominajka

Krzywa eliptyczna:

$y^2 = x^3 + a \cdot x + b$



- przecina oś y w pktach $\sqrt{b}$ i $-\sqrt{b}$;
- symetryczna względem osi x;
- dowolną prostą przecina w $\leqslant 3$ punktach;
- niech A i B leżą na krzywej w taki sposób, że ma ona jeszcze jeden punkt przecięcia z prostą AB; przez $A \cdot B$ rozumiemy punkt krzywej symetryczny do niego wzgl. osi x;
- operację $\cdot$ można stosować wielokrotnie:
  $A \cdot B$
  $A \cdot A \cdot B$
  $A \cdot A \cdot A \cdot B$
  $\ldots$

Łatwe: znając krzywą, jej punkty A i B oraz $n \in \mathbb{N}$, obliczyć $\underbrace{A \cdot \ldots \cdot A}_{n} \cdot B$

Trudne: znając krzywą, jej punkty A i B oraz $\underbrace{A \cdot \ldots \cdot A}_{n} \cdot B$, znaleźć $n \in \mathbb{N}$

Matematyka krzywych eliptycznych

Łatwe?

Znamy:
krzywą $\boldsymbol{y^2 = x^3 + ax + b}$
punkt $A = (x_A, y_A)$ na tej krzywej
punkt $B = (x_B, y_B)$ na tej krzywej

Szukamy:
trzeci punkt przecięcia
$C = (x_C, y_C)$
prostej AB z krzywą

Taki punkt musi spełniać:

- równanie prostej AB:
  $\boldsymbol{y} = \lambda \cdot (\boldsymbol{x} - x_A) + y_A$
  gdzie $\lambda = \dfrac{y_B - y_A}{x_B - x_A}$
- równanie krzywej eliptycznej:
  $\boldsymbol{y}^2 = \boldsymbol{x}^3 + a \cdot \boldsymbol{x} + b$

Czyli:

$$\begin{aligned}
(\lambda \cdot (\boldsymbol{x} - x_A) + y_A)^2 &= \boldsymbol{x}^3 + a \cdot \boldsymbol{x} + b \\
\lambda^2 \cdot (\boldsymbol{x}^2 - 2x_A\boldsymbol{x} + x_A^2) + 2\lambda y_A(\boldsymbol{x} - x_A) + y_A^2 &= \boldsymbol{x}^3 + a \cdot \boldsymbol{x} + b \\
\lambda^2\boldsymbol{x}^2 + (-2\lambda^2 x_A + 2\lambda y_A)\boldsymbol{x} + (2\lambda y_A(-x_A) + \lambda^2 x_A^2 + y_A^2) &= \boldsymbol{x}^3 + a \cdot \boldsymbol{x} + b \\
\boldsymbol{x}^3 - \lambda^2 \cdot \boldsymbol{x}^2 + (2\lambda^2 x_A - 2\lambda y_A + a) \cdot \boldsymbol{x} + (2\lambda x_A y_A - \lambda^2 x_A^2 - y_A^2 + b) &= 0
\end{aligned}$$

Matematyka krzywych eliptycznych

Współrzędna x punktu przecięcia krzywej z prostą musi być pierwiastkiem równania stopnia 3

$$x^3 - \lambda^2 \cdot x^2 + (2\lambda^2 x_A - 2\lambda y_A + a) \cdot x + (2\lambda x_A y_A - \lambda^2 x_A^2 - y_A^2 + b) = 0$$

Jak je rozwiązać? — ogólnie to jest trudne... ale w tym przypadku znamy już jego 2 pierwiastki: x_A i x_B.

Równanie stopnia 3 o trzech pierwiastkach rzeczywistych x_A, x_B i x_C i o współczynniku 1 przy najwyższej potędze, ma postać:

$$\begin{aligned} (x - x_A) \cdot (x - x_B) \cdot (x - x_C) &= 0 \\ (x^2 - (x_A + x_B) \cdot x + x_A x_B) \cdot (x - x_C) &= 0 \\ x^3 - (x_A + x_B + x_C) \cdot x^2 + (x_A x_B + x_A x_C + x_B x_C) \cdot x - x_A x_B x_C &= 0 \end{aligned}$$

Z przyrównania współczynników przy x^2 tu i tu mamy:

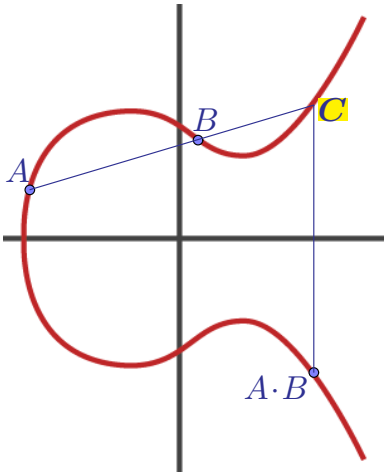
$$x_A + x_B + x_C = \lambda^2$$

więc:

$$x_C = \lambda^2 - x_A - x_B$$

Matematyka krzywych eliptycznych

$$y^2 = x^3 + a \cdot x + b$$



Punkt $C = (x_C, y_C)$ przecięcia prostej AB z krzywą $y^2 = x^3 + ax + b$ wyznaczony jest przez

$$\begin{cases} x_C = \lambda^2 - x_A - x_B \\ y_C = \lambda \cdot (x_C - x_A) + y_A \end{cases}$$

gdzie $\lambda = \dfrac{y_B - y_A}{x_B - x_A} \stackrel{?}{=} 0$

Więc potrzebny punkt $A \cdot B = (x_{A \cdot B}, y_{A \cdot B})$ wyznaczony jest przez

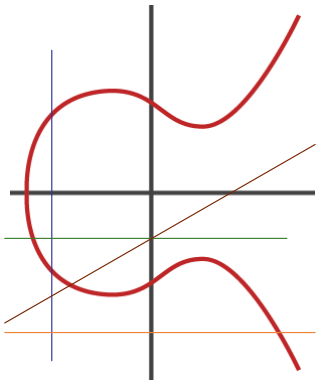
$$\begin{cases} x_{A \cdot B} = \lambda^2 - x_A - x_B \\ y_{A \cdot B} = \lambda \cdot (x_A - x_{A \cdot B}) - y_A \end{cases}$$

Ale czy to zawsze działa?

Matematyka krzywych eliptycznych

Jeśli $x_B - x_A = 0$, to prosta AB jest **pionowa** i trzeciego punktu przecięcia **nie ma**.

Trzeci punkt przecięcia nie istnieje jeszcze w kilku innych przypadkach:



— pionowa

— pozioma zbyt blisko osi x

— pozioma zbyt daleko osi x

— skośna pod zbyt małym kątem do osi x

. . . to jeszcze nie wszystko. . .

Dla tych przypadków wprowadza się specjalny
„punkt w nieskończoności”
i rozszerza się na niego operację $\cdot$ na punktach krzywej.

Matematyka krzywych eliptycznych



„Proste równoległe spotykają się w nieskończoności”

Do punktów krzywej $y^2 = x^3 + ax + b$ dorzucamy nieistniejący na rysunku punkt @ i określamy na nim działanie $\cdot$.

Matematyka krzywych eliptycznych

$A = (x_A, y_A)$, $B = (x_B, y_B)$.

$A \cdot B \stackrel{\text{def}}{=}$

- jeśli $x_A \neq x_B$ (prosta AB niepionowa), to jak poprzednio
- jeśli $x_A = x_B$ i $y_A \neq y_B$ (prosta AB pionowa), to @
- jeśli $x_A = x_B$ i $y_A = y_B = 0$ (pokrywające się punkty na osi x), to @
- jeśli $x_A = x_B$ i $y_A = y_B \neq 0$ (pokrywające się punkty poza osią x),
  to $(\boldsymbol{x}, \boldsymbol{y})$ gdzie
  $$\begin{cases} x = \left(\frac{3x_A^2 + a}{2y_A}\right)^2 - 2x_A \\ y = \frac{(x_A - x)\cdot(3x_A^2 + a)}{2y_A} - y_A \end{cases}$$
  (czyli punkt przecięcia stycznej z krzywą)
- jeśli $A = @$, to B
- jeśli $B = @$, to A

Kryptografia krzywych eliptycznych

Jeśli $\left\{ \begin{array}{c} 4a^3 + 27b^2 \neq 0 \text{ oraz} \\ A \text{ i } B \text{ leżą na krzywej } y^2 = x^3 + ax + b \end{array} \right\}$,
to potrafimy wyliczyć punkt $A \cdot B$.

Te wyliczenia wymagają tylko czterech działań arytmetycznych ($+$, $-$, $*$, $/$), więc dają się powtórzyć w dowolnym $\mathbb{Z}_p$ dla liczby pierwszej $p \geqslant 5$.

Dla dowolnego $n \in \mathbb{N}$ oraz $A \in \mathbb{Z}_p$ można stosunkowo łatwo policzyć
$A^n = \underbrace{A \cdot A \cdot \ldots \cdot A}_{n}$
Ale jest bardzo trudno, mając wynik takiego obliczenia, znaleźć użyte w nim n.

Jak tego użyć do szyfrowania?

Kryptografia krzywych eliptycznych

Jak tego użyć do szyfrowania?

Dane jawne:
liczba pierwsza $p \geqslant 5$ (wyznaczająca $\mathbb{Z}_p$)
liczby $a, b \in \mathbb{Z}_p$ t.ż. $4a^3 + 27b^2 \not\equiv_p 0$
liczba $G \in \mathbb{Z}_p$

Klucz prywatny:
losowa liczba $n \in \mathbb{Z}_p$

Klucz publiczny:
liczba G^n

Eliptyczny Diffie-Hellman (uzgodnienie klucza do szyfru symetrycznego):

Ania	Bolek
wybiera $n_A \in \mathbb{Z}_p$	wybiera $n_B \in \mathbb{Z}_p$
ogłasza G^{n_A}	ogłasza G^{n_B}
oblicza $K = (G^{n_B})^{n_A}$	oblicza $K = (G^{n_A})^{n_B}$

to jest ten sam klucz

Kryptografia krzywych eliptycznych w praktyce

- Szyfrowanie przez krzywe eliptyczne jest znacznie trudniejsze do złamania niż tradycyjne RSA czy Diffie-Hellman.
- Wobec tego wymaga mniejszych liczb.
- Przy tym samym stopniu zabezpieczenia szyfrowanie eliptyczne jest szybsze i tańsze niż tradycyjne metody.

Przykład krzywej eliptycznej używanej w szyfrowaniu:

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

$$a = 115792089210356248762697446949407573530086143415290314195533631308867097853948$$

$$b = 41058363725152142129326129780047268409114441015993725554835256314039467401291$$