

Securitatea Sistemelor Informatice



- Curs 10.5 - Criptografia bazată pe curbe eliptice

Adela Georgescu

Facultatea de Matematică și Informatică
Universitatea din București
Anul universitar 2022-2023, semestrul I

Grupuri ciclice pentru uz criptografic

- ▶ În cursul precedent am discutat despre grupuri ciclice și am subliniat faptul că sunt de preferat, pentru criptografie, grupurile ciclice de ordin prim;

Grupuri ciclice pentru uz criptografic

- ▶ În cursul precedent am discutat despre grupuri ciclice și am subliniat faptul că sunt de preferat, pentru criptografie, grupurile ciclice de ordin prim;
- ▶ Am menționat că, de obicei, se lucrează în grupul \mathbb{Z}_p^* cu p prim iar un subgrup de ordin prim al lui este format din mulțimea resturilor pătratice modulo p ;

Grupuri ciclice pentru uz criptografic

- ▶ În cursul precedent am discutat despre grupuri ciclice și am subliniat faptul că sunt de preferat, pentru criptografie, grupurile ciclice de ordin prim;
- ▶ Am menționat că, de obicei, se lucrează în grupul \mathbb{Z}_p^* cu p prim iar un subgrup de ordin prim al lui este format din mulțimea resturilor pătratice modulo p ;
- ▶ În continuare introducem o altă clasă de grupuri care constă din **punctele unei curbe eliptice**;

Grupuri ciclice pentru uz criptografic

- ▶ În cursul precedent am discutat despre grupuri ciclice și am subliniat faptul că sunt de preferat, pentru criptografie, grupurile ciclice de ordin prim;
- ▶ Am menționat că, de obicei, se lucrează în grupul \mathbb{Z}_p^* cu p prim iar un subgrup de ordin prim al lui este format din mulțimea resturilor pătratice modulo p ;
- ▶ În continuare introducem o altă clasă de grupuri care constă din **punctele unei curbe eliptice**;
- ▶ Aceste grupuri sunt folosite în criptografie pentru că, spre deosebire de \mathbb{Z}_p^* , nu se cunoaște deocamdată nici un algoritm sub-exponențial pentru rezolvarea DLP în aceste grupuri.

Curbe eliptice

Definiție

O curbă eliptică peste \mathbb{Z}_p , $p > 3$ prim, este mulțimea perechilor (x, y) cu $x, y \in \mathbb{Z}_p$ așa încât

$$y^2 = x^3 + Ax + B \bmod p$$

împreună cu punctul la infinit \mathcal{O} unde

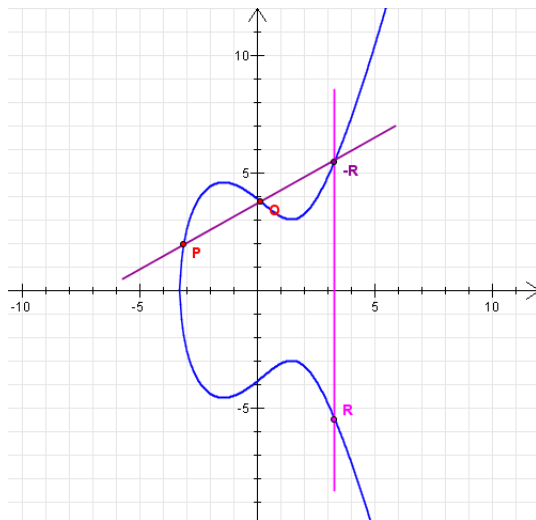
$A, B \in \mathbb{Z}_p$ sunt constante care respectă $4A^3 + 27B^2 \neq 0 \bmod p$

- ▶ Vom nota cu $E(\mathbb{Z}_p)$ o curbă eliptică definită peste \mathbb{Z}_p

Curbe eliptice

O curbă eliptică peste spațiul numerelor reale \mathbb{R}

$$E(\mathbb{R}) : y^2 = x^3 - x + 1$$



Grupul punctelor de pe o curbă eliptică

- Pentru a arăta că punctele de pe o curbă eliptică formează un grup ciclic, definim o operație de grup peste aceste puncte:

Grupul punctelor de pe o curbă eliptică

- ▶ Pentru a arăta că punctele de pe o curbă eliptică formează un grup ciclic, definim o operație de grup peste aceste puncte:
- ▶ Definim operația binară aditivă " $+$ " astfel:

Grupul punctelor de pe o curbă eliptică

- ▶ Pentru a arăta că punctele de pe o curbă eliptică formează un grup ciclic, definim o operație de grup peste aceste puncte:
- ▶ Definim operația binară aditivă "+" astfel:
 - ▶ punctul la infinit \mathcal{O} este element neutru: $\forall P \in E(\mathbb{Z}_p)$ definim

$$P + \mathcal{O} = \mathcal{O} + P = P.$$

Grupul punctelor de pe o curbă eliptică

- ▶ Pentru a arăta că punctele de pe o curbă eliptică formează un grup ciclic, definim o operație de grup peste aceste puncte:
- ▶ Definim operația binară aditivă "+" astfel:
 - ▶ punctul la infinit \mathcal{O} este element neutru: $\forall P \in E(\mathbb{Z}_p)$ definim

$$P + \mathcal{O} = \mathcal{O} + P = P.$$

- ▶ fie $P = (x_1, y_1)$ și $Q = (x_2, y_2)$ două puncte de pe curbă; atunci:

Grupul punctelor de pe o curbă eliptică

- ▶ Pentru a arăta că punctele de pe o curbă eliptică formează un grup ciclic, definim o operație de grup peste aceste puncte:
- ▶ Definim operația binară aditivă "+" astfel:
 - ▶ punctul la infinit \mathcal{O} este element neutru: $\forall P \in E(\mathbb{Z}_p)$ definim

$$P + \mathcal{O} = \mathcal{O} + P = P.$$

- ▶ fie $P = (x_1, y_1)$ și $Q = (x_2, y_2)$ două puncte de pe curbă; atunci:
- ▶ dacă $x_1 = x_2$ și $y_2 = -y_1$, $P + Q = \mathcal{O}$

Grupul punctelor de pe o curba eliptică

- ▶ altfel, $P + Q = R$ de coordonate (x_3, y_3) care se calculează astfel:

$$\begin{aligned}x_3 &= [m^2 - x_1 - x_2 \bmod p] \\ y_3 &= [m(x_1 - x_3) - y_1 \bmod p]\end{aligned}$$

- ▶ iar m se calculează astfel:

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p & \text{dacă } P \neq Q \\ \frac{3x_1^2 + A}{2y_1} \bmod p & \text{dacă } P = Q \end{cases}$$

Grupul punctelor de pe o curba eliptică

- ▶ altfel, $P + Q = R$ de coordonate (x_3, y_3) care se calculează astfel:

$$\begin{aligned}x_3 &= [m^2 - x_1 - x_2 \bmod p] \\ y_3 &= [m(x_1 - x_3) - y_1 \bmod p]\end{aligned}$$

- ▶ iar m se calculează astfel:

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p & \text{dacă } P \neq Q \\ \frac{3x_1^2 + A}{2y_1} \bmod p & \text{dacă } P = Q \end{cases}$$

- ▶ dacă $P = Q$ și $y_1 = 0$, atunci $P + Q = 2P = \mathcal{O}$

Grupul punctelor de pe o curba eliptică

- ▶ Geometric, suma a două puncte P și Q se obține trasând o linie prin cele două puncte și găsind cel de-al treilea punct R de intersecție al liniei cu E ;

Grupul punctelor de pe o curba eliptică

- ▶ Geometric, suma a două puncte P și Q se obține trasând o linie prin cele două puncte și găsind cel de-al treilea punct R de intersecție al liniei cu E ;
- ▶ În această situație, m reprezintă panta dreptei care trece prin P și Q ;

Grupul punctelor de pe o curba eliptică

- ▶ Geometric, suma a două puncte P și Q se obține trasând o linie prin cele două puncte și găsim cel de-al treilea punct R de intersecție al liniei cu E ;
- ▶ În această situație, m reprezintă panta dreptei care trece prin P și Q ;
- ▶ Se poate arăta că mulțimea de puncte $E(\mathbb{Z}_p)$ împreună cu operația aditivă definită formează un grup abelian;

Grupul punctelor de pe o curba eliptică

- ▶ Geometric, suma a două puncte P și Q se obține trasând o linie prin cele două puncte și găsim cel de-al treilea punct R de intersecție al liniei cu E ;
- ▶ În această situație, m reprezintă panta dreptei care trece prin P și Q ;
- ▶ Se poate arăta că mulțimea de puncte $E(\mathbb{Z}_p)$ împreună cu operația aditivă definită formează un grup abelian;
- ▶ Există o teoremă de structură pentru $E(\mathbb{Z}_p)$ care exprimă condițiile în care grupul este ciclic.

Grupul punctelor de pe o curba eliptică

Grupul punctelor de pe o curba eliptică

- În practică, sunt căutate acele curbe eliptice pentru care ordinul grupului ciclic generat este prim;

Grupul punctelor de pe o curba eliptică

- ▶ În practică, sunt căutate acele curbe eliptice pentru care ordinul grupului ciclic generat este prim;
- ▶ Pentru criptografie, sunt de interes curbe eliptice de ordin mare

Grupul punctelor de pe o curbă eliptică

- ▶ În practică, sunt căutate acele curbe eliptice pentru care ordinul grupului ciclic generat este prim;
- ▶ Pentru criptografie, sunt de interes curbe eliptice de ordin mare
- ▶ O curbă eliptică definită peste \mathbb{Z}_p are aproximativ p puncte. Mai precis [**Teorema lui Hasse**]:

$$p + 1 - 2\sqrt{p} \leq \text{card}(E(\mathbb{Z}_p)) \leq p + 1 + 2\sqrt{p}$$

Grupul punctelor de pe o curba eliptică

- ▶ În practică, sunt căutate acele curbe eliptice pentru care ordinul grupului ciclic generat este prim;
- ▶ Pentru criptografie, sunt de interes curbe eliptice de ordin mare
- ▶ O curbă eliptică definită peste \mathbb{Z}_p are aproximativ p puncte. Mai precis [**Teorema lui Hasse**]:

$$p + 1 - 2\sqrt{p} \leq \text{card}(E(\mathbb{Z}_p)) \leq p + 1 + 2\sqrt{p}$$

- ▶ Există mai multe clase de curbe eliptice slabe d.p.d.v. criptografic, iar ele trebuiesc evitate.

Grupul punctelor de pe o curbă eliptică

- ▶ În practică, sunt căutate acele curbe eliptice pentru care ordinul grupului ciclic generat este prim;
- ▶ Pentru criptografie, sunt de interes curbe eliptice de ordin mare
- ▶ O curbă eliptică definită peste \mathbb{Z}_p are aproximativ p puncte. Mai precis [**Teorema lui Hasse**]:

$$p + 1 - 2\sqrt{p} \leq \text{card}(E(\mathbb{Z}_p)) \leq p + 1 + 2\sqrt{p}$$

- ▶ Există mai multe clase de curbe eliptice slabe d.p.d.v. criptografic, iar ele trebuiesc evitate.
- ▶ De pildă, curbe eliptice peste \mathbb{Z}_p cu $\text{card}(E(\mathbb{Z}_p)) = p$

Grupul punctelor de pe o curbă eliptică

- ▶ În practică, sunt căutate acele curbe eliptice pentru care ordinul grupului ciclic generat este prim;
- ▶ Pentru criptografie, sunt de interes curbe eliptice de ordin mare
- ▶ O curbă eliptică definită peste \mathbb{Z}_p are aproximativ p puncte. Mai precis [**Teorema lui Hasse**]:

$$p + 1 - 2\sqrt{p} \leq \text{card}(E(\mathbb{Z}_p)) \leq p + 1 + 2\sqrt{p}$$

- ▶ Există mai multe clase de curbe eliptice slabe d.p.d.v. criptografic, iar ele trebuiesc evitate.
- ▶ De pildă, curbe eliptice peste \mathbb{Z}_p cu $\text{card}(E(\mathbb{Z}_p)) = p$
- ▶ În practică, se folosesc curbe eliptice standardizate

Curbe eliptice folosite în practică

Curbe eliptice standardizate, folosite în practică, sigure și cu implementări eficiente:

- ▶ *curba eliptică P-256* (sau *secp256r1*) este o curbă eliptică peste \mathbb{Z}_p cu p pe 256 biți de forma $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$. Această curbă are ecuația $y^2 = x^3 - 3x + B \pmod{p}$ iar p -ul ales astfel permite o implementare eficientă. Curbele *P-384* (*secp384r1*) și *P-521* (*secp521r1*) sunt definite în mod analog
- ▶ *curba eliptică 25519* este definită peste \mathbb{Z}_p cu p pe 255 biți de forma $p = 2^{255} - 19$ și permite o implementare eficientă. Grupul acestei curbe eliptice nu are ordin prim dar se poate lucra într-un subgrup de ordin mare prim

Curbe eliptice folosite în practică

Curbe eliptice standardizate, folosite în practică, sigure și cu implementări eficiente:

- ▶ *secp256k1* este o curbă eliptică de ordin prim peste \mathbb{Z}_p cu p pe 256 biți de forma $p = 2^{256} - 2^{232} - 2^{29} - 2^{28} - 2^{27} - 2^{26} - 2^{24} - 1$ și are ecuația $y^2 = x^3 + 7 \pmod{p}$. Aceasta curbă eliptică este folosită în Bitcoin.

ECDLP - Problema logaritmului discret pe curbe eliptice

► ECDLP = Elliptic Curve Discrete Logarithm Problem

ECDLP - Problema logaritmului discret pe curbe eliptice

- ▶ ECDLP = Elliptic Curve Discrete Logarithm Problem
- ▶ Putem defini acum DLP în grupul punctelor unei curbe eliptice (ECDLP):

ECDLP - Problema logaritmului discret pe curbe eliptice

- ▶ **ECDLP** = **E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem
- ▶ Putem defini acum DLP în grupul punctelor unei curbe eliptice (ECDLP):
- ▶ Fie E o curbă eliptică peste \mathbb{Z}_p , un punct $P \in \mathbb{Z}_p$ de ordin n și Q un element din subgrupul ciclic generat de P :

$$Q \in [P] = \{sP \mid 1 \leq s \leq n-1\}$$

ECDLP - Problema logaritmului discret pe curbe eliptice

- ▶ ECDLP = Elliptic Curve Discrete Logarithm Problem
- ▶ Putem defini acum DLP în grupul punctelor unei curbe eliptice (ECDLP):
- ▶ Fie E o curbă eliptică peste \mathbb{Z}_p , un punct $P \in \mathbb{Z}_p$ de ordin n și Q un element din subgrupul ciclic generat de P :

$$Q \in [P] = \{sP \mid 1 \leq s \leq n-1\}$$

- ▶ Problema ECDLP cere găsirea unui k așa încât $Q = kP$;

ECDLP - Problema logaritmului discret pe curbe eliptice

- ▶ **ECDLP** = **E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem
- ▶ Putem defini acum DLP în grupul punctelor unei curbe eliptice (ECDLP):
- ▶ Fie E o curbă eliptică peste \mathbb{Z}_p , un punct $P \in \mathbb{Z}_p$ de ordin n și Q un element din subgrupul ciclic generat de P :

$$Q \in [P] = \{sP \mid 1 \leq s \leq n-1\}$$

- ▶ Problema ECDLP cere găsirea unui k așa încât $Q = kP$;
- ▶ Notăție: $\underbrace{P + P + \dots + P}_{s \text{ ori}} = sP$.

ECDLP - Securitate

- ▶ Alegând cu grijă curbele eliptice, cel mai bun algoritm pentru rezolvarea ECDLP este considerabil mai slab decât cel mai bun algoritm pentru rezolvarea problemei DLP în \mathbb{Z}_p^* ;

ECDLP - Securitate

- ▶ Alegând cu grijă curbele eliptice, cel mai bun algoritm pentru rezolvarea ECDLP este considerabil mai slab decât cel mai bun algoritm pentru rezolvarea problemei DLP în \mathbb{Z}_p^* ;
- ▶ De exemplu, algoritmul de calcul al indicelui nu este deloc eficient pentru ECDLP;

ECDLP - Securitate

- ▶ Alegând cu grijă curbele eliptice, cel mai bun algoritm pentru rezolvarea ECDLP este considerabil mai slab decât cel mai bun algoritm pentru rezolvarea problemei DLP în \mathbb{Z}_p^* ;
- ▶ De exemplu, algoritmul de calcul al indicelui nu este deloc eficient pentru ECDLP;
- ▶ Pentru anumite curbe eliptice, singurii algoritmi de rezolvare sunt algoritmi generici pentru DLP, adică metoda baby-step giant-step și metoda Pollard rho;

ECDLP - Securitate

- ▶ Alegând cu grijă curbele eliptice, cel mai bun algoritm pentru rezolvarea ECDLP este considerabil mai slab decât cel mai bun algoritm pentru rezolvarea problemei DLP în \mathbb{Z}_p^* ;
- ▶ De exemplu, algoritmul de calcul al indicelui nu este deloc eficient pentru ECDLP;
- ▶ Pentru anumite curbe eliptice, singurii algoritmi de rezolvare sunt algoritmi generici pentru DLP, adică metoda baby-step giant-step și metoda Pollard rho;
- ▶ Cum numărul de pași necesari pentru un astfel de algoritm este de ordinul rădăcinii păturate a cardinalului grupului, se recomandă folosirea unui grup de ordin cel puțin 2^{160} .

ECDLP - Securitate

- ▶ O consecință a teoremei lui Hasse este că dacă avem nevoie de o curbă eliptică cu 2^{160} elemente, trebuie să folosim un număr prim p pe aproximativ 160 biți;

ECDLP - Securitate

- ▶ O consecință a teoremei lui Hasse este că dacă avem nevoie de o curbă eliptică cu 2^{160} elemente, trebuie să folosim un număr prim p pe aproximativ 160 biți;
- ▶ Deci, dacă folosim o curbă eliptică $E(\mathbb{Z}_p)$ cu p pe 160 biți, un atac generic asupra ECDLP are 2^{80} complexitate timp;

ECDLP - Securitate

- ▶ O consecință a teoremei lui Hasse este că dacă avem nevoie de o curbă eliptică cu 2^{160} elemente, trebuie să folosim un număr prim p pe aproximativ 160 biți;
- ▶ Deci, dacă folosim o curbă eliptică $E(\mathbb{Z}_p)$ cu p pe 160 biți, un atac generic asupra ECDLP are 2^{80} complexitate timp;
- ▶ Un nivel de securitate de 80 biți oferă securitate pe termen mediu;

ECDLP - Securitate

- ▶ O consecință a teoremei lui Hasse este că dacă avem nevoie de o curbă eliptică cu 2^{160} elemente, trebuie să folosim un număr prim p pe aproximativ 160 biți;
- ▶ Deci, dacă folosim o curbă eliptică $E(\mathbb{Z}_p)$ cu p pe 160 biți, un atac generic asupra ECDLP are 2^{80} complexitate timp;
- ▶ Un nivel de securitate de 80 biți oferă securitate pe termen mediu;
- ▶ În practică, curbe eliptice peste \mathbb{Z}_p cu p până la 256 biți sunt folosite, cu un nivel de securitate pe 128 biți.

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ A fost inventată independent în 1987 de Neal Koblitz și în 1986 de Victor Miller;

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ A fost inventată independent în 1987 de Neal Koblitz și în 1986 de Victor Miller;
- ▶ La începutul anilor 1990 se făceau foarte multe speculații despre securitatea și practicalitatea ECC, mai ales comparativ cu RSA;

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ A fost inventată independent în 1987 de Neal Koblitz și în 1986 de Victor Miller;
- ▶ La începutul anilor 1990 se făceau foarte multe speculații despre securitatea și practicalitatea ECC, mai ales comparativ cu RSA;
- ▶ După cercetări intensive, ECC pare foarte sigură, la fel de sigură precum RSA sau schemele bazate pe DLP;

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ A fost inventată independent în 1987 de Neal Koblitz și în 1986 de Victor Miller;
- ▶ La începutul anilor 1990 se făceau foarte multe speculații despre securitatea și practicalitatea ECC, mai ales comparativ cu RSA;
- ▶ După cercetări intensive, ECC pare foarte sigură, la fel de sigură precum RSA sau schemele bazate pe DLP;
- ▶ Încrederea a crescut după ce în 1999 și 2001 au fost standardizate, pentru domeniul bancar, semnături digitale și schimburi de chei bazate pe curbe eliptice.

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ Curbele eliptice sunt folosite pe larg și în standardele comerciale precum IPsec sau TLS;

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ Curbele eliptice sunt folosite pe larg și în standardele comerciale precum IPsec sau TLS;
- ▶ ECC este adesea preferată în fața criptografiei cu cheie publică pentru sistemele încorporate precum dispozitivele mobile...

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ Curbele eliptice sunt folosite pe larg și în standardele comerciale precum IPsec sau TLS;
- ▶ ECC este adesea preferată în fața criptografiei cu cheie publică pentru sistemele încorporate precum dispozitivele mobile...
- ▶ ...din motive de performanță;

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ Curbele eliptice sunt folosite pe larg și în standardele comerciale precum IPsec sau TLS;
- ▶ ECC este adesea preferată în fața criptografiei cu cheie publică pentru sistemele încorporate precum dispozitivele mobile...
- ▶ ...din motive de performanță;
- ▶ implementările pentru ECC sunt considerabil mai mici și mai rapide decât cele pentru RSA;

Criptografia pe curbe eliptice - ECC (Elliptic Curve Cryptography)

- ▶ Curbele eliptice sunt folosite pe larg și în standardele comerciale precum IPsec sau TLS;
- ▶ ECC este adesea preferată în fața criptografiei cu cheie publică pentru sistemele încorporate precum dispozitivele mobile...
- ▶ ...din motive de performanță;
- ▶ implementările pentru ECC sunt considerabil mai mici și mai rapide decât cele pentru RSA;
- ▶ ECC cu chei pe 160-250 biți oferă cam același nivel de securitate precum RSA sau sistemele bazate pe DLP cu chei pe 1024-3072 biți.

Comparație între ECC, criptografia simetrică și asimetrică

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Figure: [Understanding cryptography, Christoph Paar, Jan Pelzl, Springer 2010]

Comparație între ECC, criptografia simetrică și asimetrică

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Figure: [Understanding cryptography, Christoph Paar, Jan Pelzl, Springer 2010]

- Un algoritm are nivelul de securitate "security level" pe n biți dacă cel mai bun atac necesită 2^n pași.

Important de reținut!

- ▶ Curbele eliptice oferă un suport bun pentru criptografie;
- ▶ ECDLP este dificilă.