

КРИПТОГРАФИЈА

- ШЕСТИ ДЕО -

ДОЦ. ДР ДРАГАН ЂОКИЋ

Математички факултет, Универзитет у Београду

`dragan.djokic@matf.bg.ac.rs`

14. март 2024.

КОДИРАЊЕ И ДЕКОДИРАЊЕ ПОМОЋУ ЕК

Ако је $q = p$ прост број:

▶ Кодирање:

▶ Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$

КОДИРАЊЕ И ДЕКОДИРАЊЕ ПОМОЋУ ЕК

Ако је $q = p$ прост број:

- ▶ Кодирање:
 - ▶ Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
 - ▶ Порука која треба да се кодира се по потреби се дели на блокове максималне величине N тд. $Nk < q$

КОДИРАЊЕ И ДЕКОДИРАЊЕ ПОМОЋУ ЕК

Ако је $q = p$ прост број:

▶ Кодирање:

- ▶ Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- ▶ Порука која треба да се кодира се по потреби се дели на блокове максималне величине N тд. $Nk < q$
- ▶ Прво се блок m преведе у нумерички еквивалент M који треба кодирати тачком (x_0, y_0) са криве $E : y^2 = x^3 + ax + b$ (над \mathbb{Z}_p)

КОДИРАЊЕ И ДЕКОДИРАЊЕ ПОМОЋУ ЕК

Ако је $q = p$ прост број:

▶ Кодирање:

- ▶ Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- ▶ Порука која треба да се кодира се по потреби се дели на блокове максималне величине N тд. $Nk < q$
- ▶ Прво се блок m преведе у нумерички еквивалент M који треба кодирати тачком (x_0, y_0) са криве $E : y^2 = x^3 + ax + b$ (над \mathbb{Z}_p)
- ▶ Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0

КОДИРАЊЕ И ДЕКОДИРАЊЕ ПОМОЋУ ЕК

Ако је $q = p$ прост број:

▶ Кодирање:

- ▶ Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- ▶ Порука која треба да се кодира се по потреби се дели на блокове максималне величине N тд. $Nk < q$
- ▶ Прво се блок m преведе у нумерички еквивалент M који треба кодирати тачком (x_0, y_0) са криве $E : y^2 = x^3 + ax + b$ (над \mathbb{Z}_p)
- ▶ Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0
- ▶ Уколико претх. нема решења покушавамо даље са $Mk + 1$, $Mk + 2, \dots, Mk + k - 1$ све док не пронађемо (x_0, y_0)

КОДИРАЊЕ И ДЕКОДИРАЊЕ ПОМОЋУ ЕК

Ако је $q = p$ прост број:

▶ Кодирање:

- ▶ Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- ▶ Порука која треба да се кодира се по потреби се дели на блокове максималне величине N тд. $Nk < q$
- ▶ Прво се блок m преведе у нумерички еквивалент M који треба кодирати тачком (x_0, y_0) са криве $E : y^2 = x^3 + ax + b$ (над \mathbb{Z}_p)
- ▶ Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0
- ▶ Уколико претх. нема решења покушавамо даље са $Mk + 1, Mk + 2, \dots, Mk + k - 1$ све док не пронађемо (x_0, y_0)

▶ Декодирање:

- ▶ M добијамо као $\left[\frac{x_0}{k} \right]$

КОДИРАЊЕ И ДЕКОДИРАЊЕ ПОМОЋУ ЕК

Ако је $q = p$ прост број:

▶ Кодирање:

- ▶ Овај метод ће радити успешно са вероватноћом $1 - \frac{1}{2^k}$, при чему k сами бирамо, у пракси $k \in [30, 50]$
- ▶ Порука која треба да се кодира се по потреби се дели на блокове максималне величине N тд. $Nk < q$
- ▶ Прво се блок m преведе у нумерички еквивалент M који треба кодирати тачком (x_0, y_0) са криве $E : y^2 = x^3 + ax + b$ (над \mathbb{Z}_p)
- ▶ Покуша се са $x_0 = Mk$, уколико $y^2 = x_0^3 + ax_0 + b$ има решења, изаберемо једно такво y_0
- ▶ Уколико претх. нема решења покушавамо даље са $Mk + 1, Mk + 2, \dots, Mk + k - 1$ све док не пронађемо (x_0, y_0)

▶ Декодирање:

- ▶ M добијамо као $\left[\frac{x_0}{k} \right]$
 - ▶ Објашњење: $\left[\frac{x_0}{k} \right] = \left[M + \frac{j}{k} \right] = M$ (не знамо шта је j , само знамо да је из $[0, k - 1]$)

ДИФИ-ХЕЛМАНОВО УСАГЛАШАВАЊЕ КЉУЧА ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ над \mathbb{F}_q и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$

ДИФИ-ХЕЛМАНОВО УСАГЛАШАВАЊЕ КЉУЧА ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ над \mathbb{F}_q и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$

ДИФИ-ХЕЛМАНОВО УСАГЛАШАВАЊЕ КЉУЧА ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ над \mathbb{F}_q и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- ▶ Затим рачунају јавне кључеве $a_AP, a_BP \in E(\mathbb{F}_q)$ и размењују их (објављују)

ДИФИ-ХЕЛМАНОВО УСАГЛАШАВАЊЕ КЉУЧА ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ над \mathbb{F}_q и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- ▶ Затим рачунају јавне кључеве $a_AP, a_BP \in E(\mathbb{F}_q)$ и размењују их (објављују)
- ▶ Усаглашени кључ ће бити $K = (a_A a_B) P \in E(\mathbb{F}_q)$

ДИФИ-ХЕЛМАНОВО УСАГЛАШАВАЊЕ КЉУЧА ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ над \mathbb{F}_q и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- ▶ Затим рачунају јавне кључеве $a_AP, a_BP \in E(\mathbb{F}_q)$ и размењују их (објављују)
- ▶ Усаглашени кључ ће бити $K = (a_A a_B) P \in E(\mathbb{F}_q)$
- ▶ Алиса може да израчуна K као $K = a_A(a_BP)$. И слично Бобан долази до K

ДИФИ-ХЕЛМАНОВО УСАГЛАШАВАЊЕ КЉУЧА ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ над \mathbb{F}_q и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Алиса и Бобан бирају своје тајне кључеве $a_A, a_B < |E(\mathbb{F}_q)|$
- ▶ Затим рачунају јавне кључеве $a_AP, a_BP \in E(\mathbb{F}_q)$ и размењују их (објављују)
- ▶ Усаглашени кључ ће бити $K = (a_A a_B) P \in E(\mathbb{F}_q)$
- ▶ Алиса може да израчуна K као $K = a_A(a_BP)$. И слично Бобан долази до K
- ▶ Цица види само a_AP и a_BP , не и K

Zadatak *Eliptička kriva koja se koristi za problem usaglašavanja ključeva Diffie-Helman protokola je $E : y^2 = x^3 + 3x + 8$ nad poljem \mathbb{F}_{13} . Ako se koristi generator $P = (2, 3)$, tajni ključevi $a_A = 4$, $a_B = 5$, odrediti tačku koja se dobija kao rezultat usaglašavanja.*

 Save  Copy  Run  SageMath 10.1

```
E=EllipticCurve(GF(13), [3,8])
P=E([2,3])
a_A=4
a_B=5
a_AP=a_A*P
a_BP=a_B*P
AlisinK=a_A*a_BP
BobanovK=a_B*a_AP
P, a_AP, a_BP, AlisinK, BobanovK
```

$((2 : 3 : 1), (1 : 5 : 1), (1 : 8 : 1), (12 : 11 : 1), (12 : 11 : 1))$

ЕЛГАМАЛОВ КРИПТОСИСТЕМ ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$

ЕЛГАМАЛОВ КРИПТОСИСТЕМ ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$

ЕЛГАМАЛОВ КРИПТОСИСТЕМ ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- ▶ За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k

ЕЛГАМАЛОВ КРИПТОСИСТЕМ ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- ▶ За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k
- ▶ Бобан тачку keP може добити тако што kP помножи са e

ЕЛГАМАЛОВ КРИПТОСИСТЕМ ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- ▶ За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k
- ▶ Бобан тачку keP може добити тако што kP помножи са e
- ▶ Бобан сабира тачке $M \oplus keP$ и $\ominus keP$ и долази до M

ЕЛГАМАЛОВ КРИПТОСИСТЕМ ПОМОЋУ ЕК

- ▶ Јавни кључ: коначно поље \mathbb{F}_q , елиптичка крива $E : y^2 = x^3 + ax + b$ и тачка $P = (x_0, y_0) \in E(\mathbb{F}_q)$, односно параметри (q, a, b, x_0)
 - ▶ Пожељно је да P буде генератор групе $(E(\mathbb{F}_q), \oplus)$
- ▶ Бобан бира свој тајни кључ $e < |E(\mathbb{F}_q)|$ и помоћу њега рачуна јавни кључ $eP \in E(\mathbb{F}_q)$
- ▶ За сваки кодирани блок поруке $M \in E(\mathbb{F}_q)$ Алиса генерише случајан број $k < |E(\mathbb{F}_q)|$ и шаље Бобану тачке kP и $M \oplus keP$, где keP добија множећи тачку eP (коју је добила од Бобана) са k
- ▶ Бобан тачку keP може добити тако што kP помножи са e
- ▶ Бобан сабира тачке $M \oplus keP$ и $\ominus keP$ и долази до M
- ▶ Цица види само eP и kP , $M \oplus keP$ и мора да реши проблем дискретног логаритма да би дошла до поруке M

Zadatak Za sistem El Gamal koristi se eliptička kriva $E : y^2 = x^3 + 3x + 8$ nad poljem \mathbb{F}_{13} . Generator je $P = (2, 3)$. Ako su tajni ključ $e = 5$, prikazati postupak šifrovanja poruke $M = (12, 11)$ (koristi se slučajan broj $k = 4$), a zatim postupak dešifrovanja šifrata.

 Save Copy Run SageMath 10.1

```
E=EllipticCurve(GF(13),[3,8])
P=E([2,3])
e=5
M=E([12,11])
k=4
eP=e*P
kP=k*P
kriptM=M+k*eP
dekriptM=kriptM-e*kP
eP, kP, kriptM, dekriptM
```

```
((1 : 8 : 1), (1 : 5 : 1), (1 : 5 : 1), (12 : 11 : 1))
```

Хоћемо да факторишемо број n за који верујемо да је сложен

Хоћемо да факторишемо број n за који верујемо да је сложен

- ▶ Претпоставимо супротно: n је прост

Хоћемо да факторишемо број n за који верујемо да је сложен

- ▶ Претпоставимо супротно: n је прост
- ▶ Онда је \mathbb{Z}_n поље

Хоћемо да факторишемо број n за који верујемо да је сложен

- ▶ Претпоставимо супротно: n је прост
- ▶ Онда је \mathbb{Z}_n поље
- ▶ Изаберемо неку елиптичку криву $E(\mathbb{Z}_n)$ и неку тачку P са те криве

ФАКТОРИЗАЦИЈА ПОМОЋУ ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

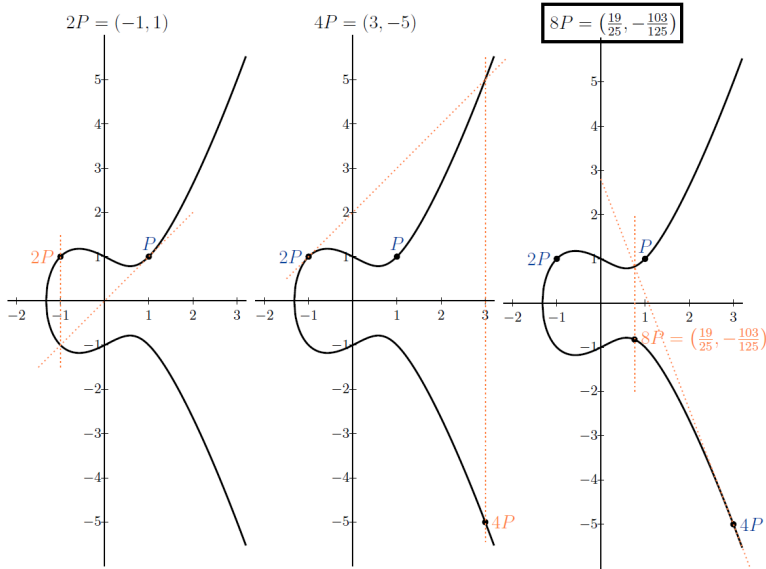
- ▶ Претпоставимо супротно: n је прост
- ▶ Онда је \mathbb{Z}_n поље
- ▶ Изаберемо неку елиптичку криву $E(\mathbb{Z}_n)$ и неку тачку P са те криве
- ▶ Кренемо да рачунамо $2P, 3P, 4P, \dots$ (или $2P, 4P, 8P, \dots$) и негде ће се појавити проблем са дељењем (нпр. у формули за сабирање тачака)
 - ▶ Практично рачунамо све у \mathbb{Q} , па редукујемо $\text{mod } n$

ФАКТОРИЗАЦИЈА ПОМОЋУ ЕК

Хоћемо да факторишемо број n за који верујемо да је сложен

- ▶ Претпоставимо супротно: n је прост
- ▶ Онда је \mathbb{Z}_n поље
- ▶ Изаберемо неку елиптичку криву $E(\mathbb{Z}_n)$ и неку тачку P са те криве
- ▶ Кренемо да рачунамо $2P, 3P, 4P, \dots$ (или $2P, 4P, 8P, \dots$) и негде ће се појавити проблем са дељењем (нпр. у формули за сабирање тачака)
 - ▶ Практично рачунамо све у \mathbb{Q} , па редукујемо $\text{mod } n$
- ▶ Када се у имениоцу појави број g који није инвертибилан по модулу n , онда ће НЗД(g, n) > 1 бити прави делилац n

Пример: За растављање 35 користимо ЕК $y^2 = x^3 - x + 1$ над \mathbb{Z}_{35} (није поље) и $P = (1, 1)$



$\text{НЗД}(35, 25) = 5$ је делилац 35

Example

We want to factor 4453. Let E be the elliptic curve $y^2 = x^3 + 10x - 2 \pmod{4453}$ and let $P = (1, 3)$. Let's try to compute $3P$. First, we compute $2P$. The slope of the tangent line at P is

$$\frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

We used the fact that $\gcd(6, 4453) = 1$ to find $6^{-1} \equiv 3711 \pmod{4453}$. Using this slope, we find that $2P = (x, y)$, with

$$x \equiv 3713^2 - 2 \equiv 4332, \quad y \equiv -3713(x - 1) - 3 \equiv 3230.$$

To compute $3P$, we add P and $2P$. The slope is

$$\frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

But $\gcd(4331, 4453) = 61 \neq 1$. Therefore, we cannot find $4331^{-1} \pmod{4453}$, and we cannot evaluate the slope. However, we have found the factor 61 of 4453, and therefore $4453 = 61 \cdot 73$.

- ▶ У примерима смо имали среће да међу mP -овима брзо наиђемо на проблем са дељењем, генерално то није случај

ЛЕНСТРИН МЕТОД

- ▶ У примерима смо имали среће да међу mP -овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- ▶ претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B -гладак број за неко мало B (инспирисано Полардовим $(p - 1)$ -методом)

ЛЕНСТРИН МЕТОД

- ▶ У примерима смо имали среће да међу mP -овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- ▶ претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B -гладак број за неко мало B (инспирисано Полардовим $(p-1)$ -методом)
- ▶ не погађати које m ради већ покушати са $m = \text{НЗС}(1, 2, \dots, B)$ или $m = B!$ (m не зависи ни од n ни од p)

ЛЕНСТРИН МЕТОД

- ▶ У примерима смо имали среће да међу mP -овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- ▶ претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B -гладак број за неко мало B (инспирисано Полардовим $(p-1)$ -методом)
- ▶ не погађати које m ради већ покушати са $m = \text{НЗС}(1, 2, \dots, B)$ или $m = B!$ (m не зависи ни од n ни од p)
- ▶ знамо да $|E(\mathbb{Z}_p)|$ дели ове m , па ће бити $mP = \mathcal{O}$ на $E(\mathbb{Z}_p)$ тј. појавиће се именилац g који је дељив са p

ЛЕНСТРИН МЕТОД

- ▶ У примерима смо имали среће да међу mP -овима брзо наиђемо на проблем са дељењем, генерално то није случај

Ленстрин метод:

- ▶ претпоставка: n има прост чинилац p тд. кардиналност $|E(\mathbb{Z}_p)|$ је B -гладак број за неко мало B (инспирисано Полардовим $(p-1)$ -методом)
- ▶ не погађати које m ради већ покушати са $m = \text{НЗС}(1, 2, \dots, B)$ или $m = B!$ (m не зависи ни од n ни од p)
- ▶ знамо да $|E(\mathbb{Z}_p)|$ дели ове m , па ће бити $mP = \mathcal{O}$ на $E(\mathbb{Z}_p)$ тј. појавиће се именилац g који је дељив са p
- ▶ али нећемо рачунати $\text{mod } p$, већ $\text{mod } n$

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ▶ ако успемо да израчунамо mP без проблема - претпоставка о B -глаткости није испуњена, покушати са већим B или другом елиптичком кривом

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ▶ ако успемо да израчунамо mP без проблема - претпоставка о B -глаткости није испуњена, покушати са већим B или другом елиптичком кривом
- ▶ ако се као именилац појави g дељив са n - променити тачку P

Дакле, рачунамо mP на $E(\mathbb{Z}_n)$. Може да се деси:

- ▶ ако успемо да израчунамо mP без проблема - претпоставка о B -глаткости није испуњена, покушати са већим B или другом елиптичком кривом
- ▶ ако се као именилац појави g дељив са n - променити тачку P
- ▶ ако се као именилац појави g које није дељиво са n , али није ни инвертибилно по модулу n - онда је НЗД(g, n) прави делилац n

УПАРИВАЊА НА ЕЛИПТИЧКИМ КРИВАМА

ДЕФИНИЦИЈА

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \longrightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q)) e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q)) e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

ДЕФИНИЦИЈА

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \rightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q)) e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q)) e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

► Последица: За све $P, Q \in E(\mathbb{F}_q)$ и $a, b \in \mathbb{N}$ важи

$$e(aP, bQ) = e(P, Q)^{ab}$$

ДЕФИНИЦИЈА

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \rightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q)) e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q)) e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

- ▶ Последица: За све $P, Q \in E(\mathbb{F}_q)$ и $a, b \in \mathbb{N}$ важи

$$e(aP, bQ) = e(P, Q)^{ab}$$

- ▶ Дифи-Хелманов проблем над ЕК (помоћу P , aP и bP одредити abP) своди на проблем дискретног логаритма у \mathbb{F}_q

ДЕФИНИЦИЈА

За пресликавање $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \rightarrow \mathbb{F}_q \setminus \{0\}$ кажемо да је упаривање (билинеарно пресликавање) на $E(\mathbb{F}_q)$ ако важи

$$(\forall P_1, P_2, Q \in E(\mathbb{F}_q)) e(P_1 \oplus P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

$$(\forall P, Q_1, Q_2 \in E(\mathbb{F}_q)) e(P, Q_1 \oplus Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

- ▶ Последица: За све $P, Q \in E(\mathbb{F}_q)$ и $a, b \in \mathbb{N}$ важи

$$e(aP, bQ) = e(P, Q)^{ab}$$

- ▶ Дифи-Хелманов проблем над ЕК (помоћу P , aP и bP одредити abP) своди на проблем дискретног логаритма у \mathbb{F}_q
- ▶ Детаљније о упаривањима: Craig Costello: *Pairings for beginners*, Главе 4 и 5

- ▶ Кажемо да је упаривање e допуштиво ако је
 - ▶ недегенерисано:
 - ▶ $(\forall Q) e(P, Q) = 1 \implies P = \emptyset$
 - ▶ $(\forall P) e(P, Q) = 1 \implies Q = \emptyset$
 - ▶ ефективно израчунљиво

- ▶ Кажемо да је упаривање e допустиво ако је
 - ▶ недегенерисано:
 - ▶ $(\forall Q) e(P, Q) = 1 \implies P = \mathcal{O}$
 - ▶ $(\forall P) e(P, Q) = 1 \implies Q = \mathcal{O}$
 - ▶ ефективно израчунљиво
- ▶ Често се уместо на групама $E(\mathbb{F}_q)$ и $\mathbb{F}_q \setminus \{0\}$ упаривање дефинише на неким њиховим подгрупама
 - ▶ Упаривање је пресликавање $e : G_1 \times G_2 \longrightarrow G$ које задовољава претх. захтеве, где је $G_1, G_2 \leq E(\mathbb{F}_q)$ и $G \leq \mathbb{F}_q \setminus \{0\}$

- ▶ Кажемо да је упаривање e допуштиво ако је
 - ▶ недегенерисано:
 - ▶ $(\forall Q) e(P, Q) = 1 \implies P = \mathcal{O}$
 - ▶ $(\forall P) e(P, Q) = 1 \implies Q = \mathcal{O}$
 - ▶ ефективно израчунљиво
- ▶ Често се уместо на групама $E(\mathbb{F}_q)$ и $\mathbb{F}_q \setminus \{0\}$ упаривање дефинише на неким њиховим подгрупама
 - ▶ Упаривање је пресликавање $e : G_1 \times G_2 \longrightarrow G$ које задовољава претх. захтеве, где је $G_1, G_2 \leq E(\mathbb{F}_q)$ и $G \leq \mathbb{F}_q \setminus \{0\}$
- ▶ Пример: Нека r дели $q - 1$ и $|E(\mathbb{F}_q)|$
 - ▶ $P \in E(\mathbb{F}_q)$ тачка реда r (тј. r је најмањи број за који важи $rP = \mathcal{O}$) и нека је $G_1 = \langle P \rangle = \{\mathcal{O}, P, 2P, \dots, (r-1)P\}$
 - ▶ $G_2 = \langle Q \rangle$, где је тачка Q реда r
 - ▶ $G = Z_r = \{\zeta \in \mathbb{F}_q \mid \zeta^r = 1\}$ група r -тих корена из јединице
 - ▶ За сваки корен $\zeta \in G$ имамо по једно упаривање $e(aP, bQ) = \zeta^{ab}$

► r -торзiona подгрупа: $E(\mathbb{F}_q)[r] = \{P \in E(\mathbb{F}_q) \mid \underbrace{rP = \mathcal{O}}_{\substack{\text{ред } P \\ \text{дели } r}}\}$

▶ r -торзиона подгрупа: $E(\mathbb{F}_q)[r] = \{P \in E(\mathbb{F}_q) \mid \underbrace{rP = \mathcal{O}}_{\substack{\text{ред } P \\ \text{дели } r}}\}$

▶ За $q = p^\alpha$ имамо Фробенијусово пресликавање

$$\pi : \mathbb{F}_q \longrightarrow \mathbb{F}_q, \pi(g) = g^p$$

▶ Ако $\mathbb{F}_p = \mathbb{Z}_p$ видимо као потпоље \mathbb{F}_q онда је π идентитет на \mathbb{Z}_p , а није на \mathbb{F}_q

▶ π индукује и пресликавање $\pi : E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_q)$,
 $\pi(x, y) = (\pi(x), \pi(y))$ и $\pi(\mathcal{O}) = \mathcal{O}$

▶ r -торзиона подгрупа: $E(\mathbb{F}_q)[r] = \{P \in E(\mathbb{F}_q) \mid \underbrace{rP = \mathcal{O}}_{\substack{\text{ред } P \\ \text{дели } r}}\}$

▶ За $q = p^\alpha$ имамо Фробенијусово пресликавање $\pi : \mathbb{F}_q \rightarrow \mathbb{F}_q$, $\pi(g) = g^p$

▶ Ако $\mathbb{F}_p = \mathbb{Z}_p$ видимо као потпоље \mathbb{F}_q онда је π идентитет на \mathbb{Z}_p , а није на \mathbb{F}_q

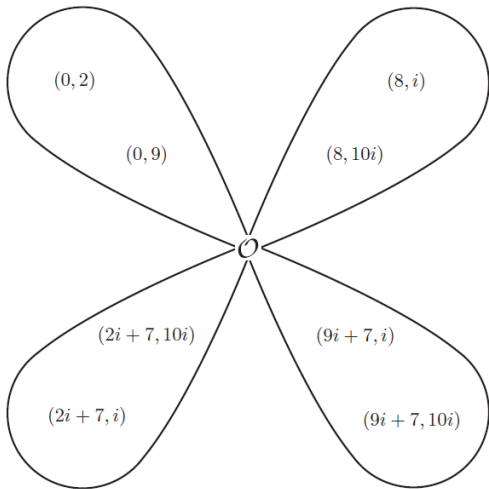
▶ π индукује и пресликавање $\pi : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_q)$, $\pi(x, y) = (\pi(x), \pi(y))$ и $\pi(\mathcal{O}) = \mathcal{O}$

ТЕОРЕМА

За свако r које дели $|E(\mathbb{F}_q)|$

1. $E(\mathbb{F}_q)[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$
2. $E(\mathbb{F}_q)[r]$ има тачно $r + 1$ подгрупу реда r
3. Рестрикција: $\pi|_{E(\mathbb{F}_q)[r]}$ има тачно две сопствене вредности 1 и p
4. Сопствени потпростори \mathcal{G}_1 и \mathcal{G}_2 који одговарају сопственим вредностима 1 и p , редом, су 2 групе са списка из дела 2.

Пример: Елиптичка крива $E : y^2 = x^3 + 4$ над пољем $\mathbb{F}_{121} = \{a + bi \mid 0 \leq a, b \leq 10\}$, где је $i^2 = -1$. Имамо 3-торзиону подгрупу $E(\mathbb{F}_{121}) [3]$ која садржи 9 тачака и која има 4 подгрупе са по 3 тачке



Горе лево је $\mathcal{G}_1: \pi(0, 2) = (0, 2), \pi(0, 9) = (0, 9)$,
 горе десно је $\mathcal{G}_2: \pi(8, i) = 3(8, i), \pi(8, 10i) = 3(8, 10i)$

- ▶ Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1, \mathcal{G}_2$ (из претх. теореме)

- ▶ Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1, \mathcal{G}_2$ (из претх. теореме)
- ▶ Најзначајнији тип (за zero knowledge proofs) је $G_1 = \mathcal{G}_1$ и $G_2 = \mathcal{G}_2$

- ▶ Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1, \mathcal{G}_2$ (из претх. теореме)
- ▶ Најзначајнији тип (за zero knowledge proofs) је $G_1 = \mathcal{G}_1$ и $G_2 = \mathcal{G}_2$
- ▶ Постоје сурјекције
 - ▶ траг $\text{Tr} : E(\mathbb{F}_q)[r] \longrightarrow \mathcal{G}_1,$
 $\text{Tr}(P) = P \oplus \pi(P) \oplus \pi^2(P) \oplus \dots \oplus \pi^{\alpha-1}(P)$
 (где је α из $q = p^\alpha$)
 - ▶ анти-траг $\text{aTr} : E(\mathbb{F}_q)[r] \longrightarrow \mathcal{G}_2, \text{aTr}(P) = (rP) \ominus \text{Tr}(P)$

- ▶ Постоји више типова упаривања - у зависности од тога да ли је нека група G_1, G_2 (из дефиниције) баш једнака $\mathcal{G}_1, \mathcal{G}_2$ (из претх. теореме)
- ▶ Најзначајнији тип (за zero knowledge proofs) је $G_1 = \mathcal{G}_1$ и $G_2 = \mathcal{G}_2$
- ▶ Постоје сурјекције
 - ▶ траг $\text{Tr} : E(\mathbb{F}_q)[r] \longrightarrow \mathcal{G}_1,$
 $\text{Tr}(P) = P \oplus \pi(P) \oplus \pi^2(P) \oplus \dots \oplus \pi^{\alpha-1}(P)$
 (где је α из $q = p^\alpha$)
 - ▶ анти-траг $\text{aTr} : E(\mathbb{F}_q)[r] \longrightarrow \mathcal{G}_2, \text{aTr}(P) = (rP) \ominus \text{Tr}(P)$
- ▶ Свако упаривање $e : \mathcal{G}_1 \times \mathcal{G}_2 \longrightarrow Z_r$ (где је Z_r група r -тих корена из 1) се може проширити до упаривања

$$\hat{e} : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)[r] \longrightarrow Z_r, \quad \hat{e}(P, Q) = e(\text{Tr}(P), \text{aTr}(Q))$$

