Pokročilá kryptologie

Eliptické křivky a jejich vlastnosti

prof. Ing. Róbert Lórencz, CSc.

České vysoké učení technické v Praze, Fakulta informačních technologií
Katedra informační bezpečnosti

Obsah přednášky

- Úvod
- Historie
- Matematický základ
- Eliptická křivka nad tělesem GF(p)
- ECC a problém diskrétního logaritmu
- Šifrování s ECC

Úvod

- Základní úlohou kryptografie je zajištění bezpečného a utajeného přenosu informace prostřednictvím veřejného kanálu. Základní cíle jsou:
  - Ochrana osobních údajů
  - Autentizace
- Kryptografické systémy z hlediska bezpečnosti jsou:
  - Bezpodmínečně bezpečné: Odolné jakémukoliv útoku bez ohledu na množství použitých výpočtů. Typickým příkladem je One-time pad (Vernamova šifra).
  - Podmíněně bezpečné: Je výpočetně nemožné je prolomit. ALE v případě neomezené vypočetní sily ANO. V podstatě moderní kryptografické systémy jsou konstruovány na základě principu podmíněné bezpečnosti.

Úvod - motivace

- Důležitost kryptografických algoritmů veřejného klíče (asymetrické systémy) je zřejmá:
  - Správa klíčů
  - Autentizace uživatele
  - Elektronické podpisy
  - Certifikáty
- Kryptografické systémy veřejného klíče jsou založený těžce řešitelných matematických problémech
  - RSA je založené na faktorizace velkých čísel
  - DH a ElGamal na problému diskrétního logaritmu
- Hlavním problémem konvenčních kryptografických systémů s veřejným klíčem je velikost klíče, která musí být dostatečně velká, aby splňovala vysokou úroveň bezpečnosti
  - To má za následek nižší rychlost, větší prostorovou a implementační složitost
  - Možným východiskem jsou kryptografické systémy založené na eliptických křivkách (**ECC - Elliptic Curve Cryptography**)

Historie

- V. Miller a N. Koblitz přišli nezávisle na sobě na možnost použití eliptických křivek v rámci kryptosystému veřejného klíče (1985).
- V současnosti jsou eliptické kryptosystémy v řadě světových standardů a jsou komerčně akceptovány.
- Použití hlavně v prostředích s omezenými zdroji, jako jsou ad-hoc wireless networks, mobilní sítě, atd.
- Konvenční kryptografické systémy veřejného klíče jsou postupně nahrazovány systémy ECC. S rostoucím výpočetním výkonem je třeba dramaticky zvýšit velikost klíčů konvenčních systémů.
- Dále ECC má výhodu v rychlosti a menší náročnosti na hardware.
- Zkoumáním vlastností eliptických křivek se zabýval německý matematik K. T. W. Weierstrass (1815 — 1897).
- Studiem eliptických křivek se zabývali matematici dlouhodobě taktéž v takových oblastech jako důkaz Velké Fermatovy věty nebo Teorie strun.

Matematický základ 1

Eliptická křivka E nad R (reálná čísla) je definována Weierstrassovou rovnicí

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

kde $a_1, a_2, a_3, a_4, a_5 \in R$ a $\triangle \neq 0$. $\triangle$ je diskriminant křivky E a je definovaný:

$$\begin{aligned}
\triangle &= -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \\
d_2 &= a_1^2 + 4a_2 \\
d_4 &= 2a_4 + a_1 a_3 \\
d_6 &= a_3^2 + 4a_6 \\
d_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2
\end{aligned}$$

Body

V případě, že obě souřadnice bodu $P \in E$ nebo $P = \infty$ (bod v nekonečnu nebo tzv. nulový bod $\mathcal{O}$), pak množina bodu na E je:

$$E' = \{(x, y) \in R \times R : y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0\} \cup \{\mathcal{O}\}$$

Matematický základ 2

Zjednodušené Weierstrassové rovnice

Pokud uděláme nasledující substituci v obecné Weierstrassové rovnici

$$(x, y) \rightarrow (x - \frac{a_2}{3}, y - \frac{a_1 x + a_3}{2})$$

a dosadíme $a_1 = 0, a_3 = 0,$

$$a = \frac{1}{9}a_2^2 + a_4, b = \frac{2}{27}a_2^3 - \frac{1}{3}a_2 a_4 a_6$$

dostáváme zjednodušenou Weierstrassové rovnici

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

Pokud uděláme jinou substituci v obecné Weierstrassové rovnici

$$(x, y) \rightarrow (a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3})$$

dostáváme další zjednodušenou Weierstrassové rovnici

$$E : y^2 + xy = x^3 + ax^2 + b$$

Matematický základ 4

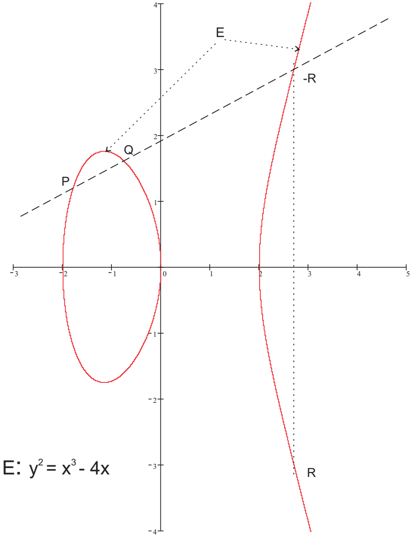
Doplňující pravidla platící pro body eliptické křivky E

- Identita $P + \mathcal{O} = \mathcal{O} + P = P \quad \forall P \in E$
- Inverse $P + (-P) = \mathcal{O} \quad \forall P \in E$
- Asociativita $P + (R + Q) = (P + R) + Q \quad \forall P, Q, R \in E$
- Komutativita $P + Q = Q + P \quad \forall P, Q \in E$

Při platnosti těchto doplňujících pravidel body křivky E vytváří Abelovskou grupu.

Sčítaní bodů

- Eliptická křivka E je množina bodů v rovině, která vyhovuje rovnici
$$E : y^2 = x^3 + ax + b.$$
- Součtem 2 různých bodů P a Q z E bude opět bod ležící na E, a tedy také vyhovující rovnici pro E.
- Geometrické interpretace součtu: Spojíme body $P = [x_P, y_P]$ a $Q = [x_Q, y_Q]$ přímkou, ta protne křivku E v bodě $-R$.
- Výsledkem sčítání je potom bod R, který je symetrický k $-R$ podle osy x. Body symetrické podle osy x nazýváme *opačné*.



Matematický základ 5

- Směrnice přímky, která spojuje dva různé body P a Q je rovná

$$s = \frac{y_Q - y_P}{x_Q - x_P}.$$

- Pro souřadnice bodu $R = [x_R, y_R]$ platí

$$x_R = s^2 - x_P - x_Q \quad \text{a} \quad y_R = s(x_P - x_R) - y_P.$$

- Když $P = Q \Rightarrow$ jejich spojnice je tečna k E a její směrnice je rovná

$$s = \frac{3{x_P}^2 + a}{2y_P}.$$

- Sčítáním 2 opačných bodů ($P = -Q$) měli bychom dostat bod $\mathcal{O}$.
- Taková přímka nám E už neprotne, resp. ji protne v ∞. Pak dle inverse: $P + (-P) = \mathcal{O}$.
- Takto je možné provádět sčítání pro $\forall$ dvojice bodů na E včetně $\mathcal{O}$.

Eliptická křivka nad tělesem GF(p)a GF(2^m)

Eliptické křivky v oboru reálných čísel

- Výpočet je pomalý
- Nepřesnosti způsobené zaokrouhlováním
- Nekonečý prostor řešení

U kryptografických algoritmů vyžadujeme rychlost a přesnost.

Při využití eliptických křivek pro šifrování pracujeme v oblasti diskrétních hodnot (celých čísel, bitových řetězců).

- Uvažujeme těleso GF(2^m), kde m je kladné celé číslo a těleso GF(p), kde p je prvočíslo.
- Obě tělesa jsou v praxi využívaná.
- Eliptická křivka nad tělesem GF(p) je definována jako bod $\mathcal{O}$ v ∞ společně s množinou bodů $P = [x, y]$, kde x a y jsou z tělesa GF(p) a vyhovují rovnici $y^2 = x^3 + ax + b$ v GF(p), tj.

$$y^2 \equiv x^3 + ax + b \pmod{p} .$$

Eliptická křivka nad tělesem GF(p) 1

- Koeficienty a a b jsou také prvky tělesa GF(p) a musí splňovat podmínku
$$|4a^3 + 27b^2|_p \neq 0.$$
- Takto definovaná množina bodů tvoří grupu, koeficienty a a b volíme libovolně (veřejné parametry příslušného kryptosystému).
- V této grupě definujeme opačný bod k $\mathcal{O}$ jako $\mathcal{O} = -\mathcal{O}$ a pro ostatní nenulové body $P = [x_P, y_P] \in$ E definujeme $-P = [x_P, |-y_P|_p]$, dále pro všechny body $P \in E$ definujeme $P + -P = \mathcal{O}$ a $P + \mathcal{O} = P$.
- Bod $\mathcal{O}$ nazýváme také nulovým bodem, vzhledem k jeho roli při sčítání v grupě E. Sčítání stejných nenulových bodů $P + P$ definujme jako $R = P + P = [x_R, y_R]$, kde směrnice s je rovná
$$s = \left|\frac{3{x_P}^2 + a}{2y_P}\right|_p$$

Eliptická křivka nad tělesem GF(p) 2

- a souřadnice bodu R

$$x_R = \left| s^2 - x_P - x_Q \right|_p \quad \text{a} \quad y_R = \left| s(x_P - x_R) - y_P \right|_p .$$

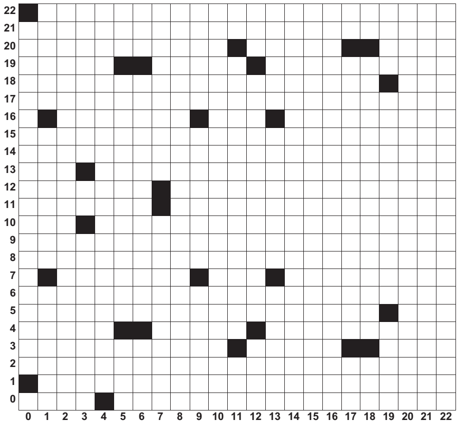
- Sčítáním různých nenulových a vzájemně neinverzních bodů P = [x_P, y_P] a Q = [x_Q, y_Q] křivky E definujeme jako $P + Q = R$ = [x_R, y_R], kde směrnice s je rovná

$$s = \left| \frac{y_Q - y_P}{x_Q - x_P} \right|_p$$

- a souřadnice bodu R

$$x_R = \left| s^2 - x_P - x_Q \right|_p \quad \text{a} \quad y_R = \left| s(x_P - x_R) - y_P \right|_p .$$

Eliptická křivka nad tělesem GF(p) 3



(0,1)	(6,4)	(12,19)	(0,22)
(6,19)	(13,7)	(1,7)	(7,11)
(13,16)	(1,16)	(7,12)	(17,3)
(3,10)	(9,7)	(17,20)	(3,13)
(9,16)	(18,3)	(4,0)	(11,3)
(18,20)	(5,4)	(11,20)	(19,5)
(5,19)	(12,4)	(19,18)	O

28 bodů eliptické křivky $y^2 = x^3 + x + 1$ nad $GF(23)$

Eliptická křivka nad tělesem GF(p) 4

Příklad:

$E: y^2 \equiv x^3 + 2x + 2 \pmod{17}, \quad P = [5,1], \quad 2P = ?$

$2P = P + P = [5,1] + [5,1]$

$s = \left|\frac{3x_P^2+2}{2y}\right|_{17} = \left|(2\cdot 1)^{-1}\cdot(3\cdot 5^2+2)\right|_{17} = \left|9\cdot 9\right|_{17} = \left|81\right|_{17} = 13$

$x_{2P} = \left|s^2 - x_P - x_P)\right|_{17} = \left|13^2 - 5 - 5\right|_{17} = \left|159\right|_{17} = 6$

$y_{2P} = \left|s(x_P - x_{2P}) - y_P\right|_{17} = \left|13(5-6) - 1\right|_{17} = \left|-14\right|_{17} = 3$

$2P = [6,3]$

Zkouška:

$3^2 \equiv 6^3 + 2\cdot 6 + 2 \pmod{17}$

$9 \equiv 12 + 12 + 2 \pmod{17}$

$9 = 9$

Reprezentace bodů na ECC

- Souřadnice (x, y) jsou označovány jako afinní souřadnice. Počítání s takto definovanými body má nevýhody při provádění sčítání a zdvojnásobování bodů na křivce E. Jedná se zejména o drahé inverzní operace.
- Souřadnice (x, y) mohou být reprezentovány trojici (X, Y, Z), která se nazývá projektivní souřadnice. Vztah mezi (x, y) a (X, Y, Z) je následovní:
$$\begin{aligned} (X, Y, Z) &= (\lambda^c x, \lambda^d y, \lambda) \\ (x, y) &= (X/Z^c, Y/Z^d) \\ \text{kde:}\lambda &\neq 0 \end{aligned}$$
- Existuje řada typů souřadnicových systémů s různými hodnotami c a d (standardní, Jacobian, Lopez-Dahab).
- Při použití projektívních souřadnicových systémů nahradíme "drahé" operace inverze v GF operacemi násobení. Pokud složitost prováděných inverzí v porovnání se složitostí násobení je velký, pak je výhodné použít vybraný projektívní souřadnicový systém.

ECC a problém diskrétního logaritmu 1

- Pro pochopení podstaty šifrování a podepisování v ECC je důležité využití tzv. problému diskrétního logaritmu.
- Pro určitý bod P na křivce E postupně vypočítáme body 2P, 3P, 4P, 5P, 6P atd., čímž dostaneme obecně různé body xP na E.
- Protože křivka má konečný počet bodů, označíme ho #P, po určitém kroku m se nám musí tato posloupnost opakovat.
- V bodě opakování mP tak platí mP = nP, kde nP je některý z předešlých bodů. Odtud dostáváme mP – nP = O ⇒
- existuje nějaké $r = m - n$, $r < m$ takové, že rP = O, z toho plyne, že v posloupnosti P, 2P, 3P, 4P, 5P,... se vždy dostaneme k bodu O, a poté cyklus začína znovu od bodu P, protože $(r+1)$P = rP +P = O + P = P.
- Nejmenší takové r, pro které je rP = O, nazýváme *řád bodu* P.

ECC a problém diskrétního logaritmu 2

- Lze dále dokázat, že řád bodu dělí řád křivky, přičemž *řádem křivky* nazýváme počet bodů na křivce #E.
- Různé body na křivce E mají různý řád. V kryptografické praxi vybíráme takové body, jejichž řád je roven největšímu prvočíslu v rozkladu čísla #E nebo jeho násobku, který nazýváme *kofaktor*.
- U bodu řádu r máme zaručeno, že dojde k opakování v posloupnosti P, 2P, 3P,... až po r-tém kroku.
- V případě, že r je velké číslo, např. 2^{256}, je to skutečně dlouhá posloupnost.
- Právě při šifrování a elektronickém podepisování se využívá tak velké posloupnosti a to právě v souvislosti s tzv. problémem diskrétního logaritmu.
- V případě, že si zvolíme jako náš privátní klíč číslo k a vypočteme Q = kP, potom body P a Q můžeme zveřejnit jako součást veřejného klíče.

ECC a problém diskrétního logaritmu 3

- Problém diskrétního logaritmu je úloha, jak z bodů P a Q získat tajné číslo k tak, aby platilo Q = kP.
- Je zřejmé, že pro malý řád bodu P je úloha triviální. Pro velká r je to úloha, která se nedá řešit efektivně, tj. v polynomiálním čase. Z tohoto důvodu mohou být body P a Q zveřejněné.
- Dosud nejúčinnější metodou pro řešení takto definovaného problému diskrétního logaritmu eliptických křivek je tzv. Pollardova ρ metoda, jejíž složitost je řádově $\sqrt{\frac{\pi r}{2}}$ kroků. Má exponenciální složitost.
- Pokud máme $r = 2^{256}$, dostáváme $\approx 2^{128}$ kroků, což je zhruba na úrovni luštitelnosti symetrické blokové šifry se 128 bitovým klíčem.
- Pro nás je to z výpočetního hlediska neřešitelné, a tedy příslušná šifra je výpočetně bezpečná.

Bezpečnost kryptosystémů veřejného klíče 1

- Kryptosystémy veřejného klíče jsou navrženy na základě obtížné řešitelnosti některých matematických problémů.
  - RSA bezpečnost závisí na obtížnosti faktorizace velkých čísel
  - DH a ElGamal bezpečnost je založena na obtížnosti řešení diskrétního logaritmu
  - ECC bezpečnsot vychází z obtížnosti řešení diskrétního logaritmu eliptických křivek (ECDLP).
- Přímá cesta vedoucí k prolomení systémů s veřejným klíčem je získat tajný klíč z veřejného klíče. Ale výpočetní cena je ekvivalentní řešení těžkého matematického problému, na kterém je bezpečnost šifry postavená.
- Pro řešení faktorizace velkých čísel a řešení problému diskrétního logaritmu je nerychlejší algoritmus GNFS (General Number Field Sieve) se subexponenciální složitosti

$$L_n[1/3, 1.923] = O(e^{1.923(\log n)^{1/3}(\log\log n)^{2/3}})$$

Srovnání velikosti klíčů kryptosystémů veřejného klíče

Symetrické alg.	RSA a DH	ECC
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

- Hodnoty jsou v bitech a jsou to hodnoty doporučené NIST,
- Je vidět, že hodnoty kopírují subexponencialni složitost algoritmu (GNFS) pro faktorizaci a DLP vs exponenciální složitost pro ECDLP (Pollardova ρ-metoda.).

Šifrování s ECC

- Podstatu šifrování pomocí ECC si ukážeme na analogii Diffie-Hellmanova schématu výměny klíče.
- Strana *i* a *j*, si chtějí vyměnit tajnou informaci přes veřejný kanál.
- Každá strana má důvěryhodnou cestou získaný veřejný klíč protistrany. V případě ECC ještě navíc předpokládáme, že oba sdílejí stejnou křivku E a její bod P.
- Označme po řadě d_i a Q_i privátní a veřejný klíč strany *i*, a obdobně d_j a Q_j pro stranu *j*, potom si obě strany mohou ustanovit společný klíč – bod Z na křivce E, aniž spolu komunikují.
- Strana *i* vypočte bod Z jako $d_i Q_j$ a strana *j* jako $d_j Q_i$. Tyto body jsou ve skutečnosti stejné, protože $Z = d_i Q_j = d_i(d_j P) = (d_i d_j)P$ a současně $Z = d_j Q_i = d_j(d_i P) = (d_j d_i)P$.
- Tedy každá strana vezme bod veřejný klíč — bod protistrany a sečte ho *n*-krát, kde *n* je privátní klíč. Protože obě strany vycházejí ze stejného bodu P, dospějí do stejného bodu Z.

Double-and-Add algoritmus pro násobení bodu I

Algoritmus Double-and-Add

- Algoritmus násobení bodu na EC je analogické algoritmu modulárného umocňování.
- Můžeme přímo převzít Square-and-Multiply algoritmus pro vytvoření algoritmu pro násobení bodu na EC.
- Jediny rozdíl je v tom, že umocňování se převede na zdvojnásobení bodů a násobení se převede na sčítaní bodu P.
- Pro náhodné číslo d ($T = dP$) délky $t + 1$ bitů vyžaduje algoritmus v průměru $1,5t$ bodových zdvojnásobení a sčítaní.
- Algoritmus vykonává prohlíží bitovou reprezentaci d z leva doprava a podle hodnot jednotlivých bitů vykonává zdvojení v každé iteraci a sčítaní pokud hodnota právě prohlíženého bitů má hodnotu 1.

Double-and-Add algoritmus pro násobení bodu II

Double-and-Add algoritmus pro násobení bodu

Vstup: eliptická křivka E, bod $P \in E$, $d = \sum_{i=0}^{t} d_i 2^i$, kde $d_i \in \{1, 0\}$, $d_t = 1$ a modul n. .

Výstup: $T = dP$

Inicializace: $T = P$

Algoritmus:

1. FOR $i = t - 1$ DOWNTO 0
   1. $T = T + T \bmod n$
   2. IF $d_i = 1$ THEN $T = T + P \bmod n$
2. RETURN (T)

Příklad

Uvažujme násobení $26P$, které má následující binární reprezentaci

$$26P = (11010_2)P = (d_4 d_3 d_2 d_1 d_0)P$$

Double-and-Add algoritmus pro násobení bodu III

Algoritmus prohlíží hodnotu d od msb - d_4 až po lsb d_0.

Krok

#0	$P = \mathbf{1_2}P$	init, bit $d_4 = 1$
#1a	$P + P = 2P = \mathbf{10_2}P$	zdvojení, bit d_3
#1b	$2P + P = 3P = 10_2P + 1_2P = \mathbf{11_2}P$	sčítaní, bit $d_3 = 1$
#2a	$3P + 3P = 6P = 2(11_2P) = \mathbf{110_2}P$	zdvojení, bit d_2
#2b		nic, bit $d_2 = 0$
#3a	$6P + 6P = 12P = 2(110_2P) = \mathbf{1100_2}P$	zdvojení, bit d_1
#3b	$12P + P = 13P = 1100_2P + 1_2P = \mathbf{1101_2}P$	sčítaní, bit $d_1 = 1$
#4a	$13P + 13P = 26P = 2(1101_2P) = \mathbf{11010_2}P$	zdvojení, bit d_0
#4b		nic, bit $d_0 = 0$

ECDSA I

ECDSA - Elliptic Curve Digital Signature Algorithm

- Kryptosystémy s eliptickými křivkami (ECC - Elliptic Curve Cryptosystem) pracující se slovem délky 160 až 256 bitů garantuji stejnou bezpečnost jako 1024 až 3072 bitové RSA.
- Kratší bitové slová umožňuji získat výsledky v kratším čase.
- Proto ECDSA byl v roce 1998 v USA stanoven ANSI (American National Signature Algorithm) normou.
- ECDSA norma je koncepčně blízka k DSA normě. Problém diskrétního logarotmu je vybudován na grupě EC.
- Aritmetické operace ECDSA jsou ale značně odlišné od aritmetických operací DSA.
- ECDSA je definován pro EC v $GF(p)$ a $GF(2^m)$. V praxi je víc upřednostňována realizace v $GF(p)$. Dále bude uvedena ECDSA varianta v $GF(p)$.

ECDSA II

Generování klíčů pro ECDSA

1. Je vybrána eliptická křivka E s nasledujícími parametry:
   - modul p,
   - koeficienty a a b,
   - bod A generující cyklickou grupu prvočísla řádu křivky q.
2. Nechť d je náhodné celé číslo a platí $0 < d < q$.
3. Vypočteme $B = dA$.
   Definujeme klíče:
   $k_{pub} = (p, a, b, q, A, B)$
   $k_{pr} = (d)$.

- Definice klíčů reprezentuje problém diskrétniho logaritmu.
- Podle doporučení ANSI hodnota q by měla být minimálně 160 bitová pro zabezpečení vyšší úrovně bezpečnosti.

ECDSA III

Podpis a ověření podpisu

- Stejně jako u DSA tak, také u ECDSA podpis se skládá z dvojice celých čísel (r, s). Každý z nich má stejnou bitovou délku jako q.
- S použitím privátního a veřejného klíče si můžeme vyjádřit proces podpisu zprávy x následujícím způsobem.

Generování podpisu pomocí ECDSA

1. Vybereme nějaké náhodné dočasné celé číslo - klíč k_E, kde $0 < k_E < q$.
2. Vypočítame $R = k_E A$.
3. Nechť $r = x_R$.
4. Vypočítame $s \equiv (h(x) + dr)k_E^{-1} \bmod q$.

- V kroku 3 je x koordináta bodu R přiřazena proměnné r.

ECDSA IV

- Zpráva x je hašovaná s použitím hašovací funkce h. Následně je vypočítaná hodnota s.
- Výstup z hašovací funkce musí být minimálně tak velký jako q.

Ověření podpisu pomocí ECDSA

1. Vypočítame pomocnou hodnotu $w \equiv s^{-1} \bmod q$.
2. Vypočítame pomocnou hodnotu $u_1 \equiv wh(x) \bmod q$.
3. Vypočítame pomocnou hodnotu $u_2 \equiv wr \bmod q$.
4. Vypočítame $P = u_1 A + u_2 B$.
5. Ověření $ver_{k_{pub}}(x, (r, s))$ plyne z:
    1. $|x_p|_q = |r|_q \Rightarrow$ platný podpis,
    2. $|x_p|_q \neq |r|_q \Rightarrow$ neplatný podpis.

- V posledním kroku je označená x_p souřadnice bodu P.

ECDSA V

- Pokud x_p neni kongruentni modulo p s hod notou r tak podpis jeneplatný.

Důkaz

- $$s \equiv (h(x) + dr)k_E^{-1} \bmod q$$

  co je ekvivalentní

  $$k_E \equiv s^{-1}h(x) + ds^{-1}r \bmod q$$

- Pravá strana kongruence může být vyjádřena pomocí pomocných proměnných u_1 a u_2.

  $$k_E \equiv u_1 + du_2 \bmod q$$

ECDSA VI

- V případě, že bod A generuje cyklickou grupu řádu q, můžeme vynásobit obě strany kongruence bodem A.

$$k_E A = (u_1 + du_2)A = u_1 A + u_2 dA = u_1 A + u_2 B$$

- Poslední výraz ukazuje, že výraz $u_1 A + u_2 B$ je rovný $k_E A$ když korektní podpis a klíč byly použitý.
- To je přesně podmínka v ověřovacím procesu, která srovnává x-souřadnici bodu $P = u_1 A + u_2 B$ a bodu $R = k_E A$.

ECMQV I

ECMQV - Elliptic Curve Menezes-Qu-Vanstone je protokol pro dohodu klíči s autentizaci založený na schématu Diffie – Hellman.

- Poskytuje ochranu před aktívním útočníkem
- Samotný MQV protokol lze upravit tak, aby pracoval v libovolné konečné skupině.
- Například ve skupinách eliptických křivek – ECMQV.
- MQV původně navrhli Alfred Menezes, Minghua Qu a Scott Vanstone v roce 1995. V roce 1998 byl upraven Lawem a Solinasem.
- MQV je součástí standardu veřejného klíče IEEE P1363 a standardu NIST SP800-56A.
- Některé varianty MQV jsou nárokovány v patentech (Certicom).

ECMQV II

Generování klíčů pro ECMQV

1. Mějme EC E, bod P na křivce E, kofaktor h křivky E a modul n.
2. Alice (ID_A) má pár klíčů (A, a), kde $A = aP$.
   A je veřejný klíč a a je soukromý klíč.
3. Bob (ID_B) má pár klíčů (B, b), kde $B = bP$.
   B je veřejný klíč a b je soukromý klíč.
4. Pro $\overline{R}$ platí
   - Nechť $R = (x, y)$ je bod na eliptické křivce.
   - Pak $\overline{R} = (x \bmod 2^L) + 2^L$, kde
   - $L = \left\lceil \frac{\lfloor \log_2 l \rfloor + 1}{2} \right\rceil$.
   - l je řád bodu P.
   - Takže $\overline{R}$ je prvních L bitů x-sové souřadnice R.

ECMQV III

Generování K pomocí ECMQV s autentizaci, k-sdílený tajný klíč

1. Alice generuje dvojici klíčů (X, x) tak, že náhodně vygeneruje dočasný klíč x a vypočítá $X = xP$, kde P je bod na EC.
2. Bob generuje dvojici klíčů (Y, y) tak, že náhodně vygeneruje dočasný klíč y a vypočítá $Y = yP$, kde P je bod na EC.
3. Alice vypočítá $s_a = |x + \overline{X}a|_n$ a

   pošle Bobovi ID_A, X.
4. Bob vypočítá $s_b = |y + \overline{Y}b|_n$ a $t_B = MAC_k(2, ID_B, ID_A, Y, X)$ a

   pošle Alici ID_B, Y, t_B.
5. Alice vypočítá $K = h \cdot s_a(Y + \overline{Y}B)$ a $t = MAC_k(2, ID_B, ID_A, Y, X)$, a ověří, že $\mathbf{t} = \mathbf{t_B}$, pak vypočte $t_A = MAC_k(3, ID_A, ID_B, X, Y)$ a

   pošle t_A Bobovi.
6. Bob vypočítá $K = h \cdot s_b(X + \overline{X}A)$ a $t = MAC_k(3, ID_A, ID_B, X, Y)$ a ověří, že $\mathbf{t} = \mathbf{t_A}$.
7. Nyní mají oba nově vytvořený společný tajný klíč K.

ECMQV IV

Ověření správnosti generování klíče K

- Bob vypočítal K:

$$K = h \cdot s_b(X + \overline{X}A) = h \cdot s_b(xP + \overline{X}aP) = h \cdot s_b(x + \overline{X}a)P = h \cdot s_b s_a P$$

- Alice vypočítala K:

$$K = h \cdot s_a(Y + \overline{Y}B) = h \cdot s_a(yP + \overline{Y}bP) = h \cdot s_a(y + \overline{Y}b)P = h \cdot s_b s_a P$$

Odolnost vůči útoku “man-in-the-middle”

- Hodnota $s_a = (x + \overline{X}a)$ slouží jako implicitní podpis pro Alici, tzn. že jenom ten kdo zná hodnotu tajného klíče a může generovat s_a.
- Bob nepřímo ověří jeho platnost vztahem $(X + \overline{X}A) = (xP + \overline{X}aP) = (x + \overline{X}a)P = s_a P$
- Stejným způsobem hodnota s_b slouží jako implicitní podpis pro Boba.