Další algoritmy asymetrické kryptografie

L'ubomíra Balková

Úvod do kryptologie

22. dubna 2010

Goldwasserův-Micaliův algoritmus

- založen na obtížnosti rozlišování kvadratických reziduí a nereziduí modulo n, kde n je složené číslo
- nezná se algoritmus polynomiální v $||n||$ schopný rozhodnout, zda x je kvadratické reziduum modulo n

Kvadratická rezidua modulo prvočíslo p

Definice

Nechť $p \in \mathbb{P}$. Pak $x \in \mathbb{Z}$ nazveme kvadratické reziduum *modulo p, pokud existuje $y \in \mathbb{Z}_p^*$ tak, že*

$$y^2 \equiv x \mod p.$$

Věta

Nechť $p \in \mathbb{P}$, $p > 2$. Pro každé kvadratické reziduum x existují právě 2 různé prvky $y, z \in \mathbb{Z}_p^*$ tak, že

$$y^2 \equiv x \mod p \equiv z^2.$$

Kvadratická rezidua modulo prvočíslo p

Definice

Nechť $p \in \mathbb{P}$. Pak $x \in \mathbb{Z}$ nazveme kvadratické reziduum *modulo p, pokud existuje $y \in \mathbb{Z}_p^*$ tak, že*

$$y^2 \equiv x \mod p.$$

Věta

Nechť $p \in \mathbb{P}$, $p > 2$. Pro každé kvadratické reziduum x existují právě 2 různé prvky $y, z \in \mathbb{Z}_p^*$ tak, že

$$y^2 \equiv x \mod p \equiv z^2.$$

Důsledek

Počet kvadratických reziduí v $\mathbb{Z}_p^*$ je $\frac{p-1}{2}$.

Kvadratická rezidua modulo prvočíslo p

Definice

Nechť $p \in \mathbb{P}$. Pak $x \in \mathbb{Z}$ nazveme kvadratické reziduum *modulo p, pokud existuje $y \in \mathbb{Z}_p^*$ tak, že*

$$y^2 \equiv x \mod p.$$

Věta

Nechť $p \in \mathbb{P}$, $p > 2$. Pro každé kvadratické reziduum x existují právě 2 různé prvky $y, z \in \mathbb{Z}_p^*$ tak, že

$$y^2 \equiv x \mod p \equiv z^2.$$

Důsledek

Počet kvadratických reziduí v $\mathbb{Z}_p^*$ je $\frac{p-1}{2}$.

Legendrův symbol

Definice

Nechť $p \in \mathbb{P},\ p > 2$. Pak pro $x \in \mathbb{Z}$ definujeme

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ je kvadratické reziduum modulo } p \\ -1 & x \text{ není kvadratické reziduum modulo } p \\ 0 & p \mid x \end{cases}$$

Pozn.

$\mathbb{Z}_p^*$ je cyklická grupa řádu $p-1$, pak existuje $g \in \mathbb{Z}_p^*$ řádu $p-1$. Pak $\mathbb{Z}_p^* = \{g^0, g^1, g^2, \ldots, g^{p-2}\}$.

$$\text{Množina kvadratických reziduí} = \{g^0, g^2, g^4, \ldots, g^{p-3}\}.$$

Legendrův symbol

Definice

Nechť $p \in \mathbb{P},\ p > 2$. *Pak pro* $x \in \mathbb{Z}$ *definujeme*

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ je kvadratické reziduum modulo } p \\ -1 & x \text{ není kvadratické reziduum modulo } p \\ 0 & p \mid x \end{cases}$$

Pozn.

$\mathbb{Z}_p^*$ *je cyklická grupa řádu* $p-1$, *pak existuje* $g \in \mathbb{Z}_p^*$ *řádu* $p-1$. *Pak* $\mathbb{Z}_p^* = \{g^0, g^1, g^2, \ldots, g^{p-2}\}$.

$$\text{Množina kvadratických reziduí} = \{g^0, g^2, g^4, \ldots, g^{p-3}\}.$$

Legendrův symbol

Věta

Nechť $p \in \mathbb{P},\ p > 2$. Pak pro $x \in \mathbb{Z}$

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \mod p.$$

Pozn.

Nechť $p \in \mathbb{P},\ p > 2$. Pak pro $x, y \in \mathbb{Z}$

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right).$$

Legendrův symbol

Věta

Nechť $p \in \mathbb{P},\ p > 2$. *Pak pro* $x \in \mathbb{Z}$

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \mod p.$$

Pozn.

Nechť $p \in \mathbb{P},\ p > 2$. *Pak pro* $x, y \in \mathbb{Z}$

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right).$$

Kvadratická rezidua modulo složené číslo n

Definice

Nechť $n \in \mathbb{N}$. Pak $x \in \mathbb{Z}$ nazveme kvadratické reziduum *modulo n, pokud existuje $y \in \mathbb{Z}_n^*$ tak, že*

$$y^2 \equiv x \mod n.$$

Označme $x_p \equiv x \mod p$ a $x_q \equiv x \mod q$.

Věta

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q lichá. Pak x je kvadratické reziduum modulo $n \Leftrightarrow x_p$ je kvadratické reziduum modulo p a zároveň x_q je kvadratické reziduum modulo q.

Kvadratická rezidua modulo složené číslo n

Definice

Nechť $n \in \mathbb{N}$. Pak $x \in \mathbb{Z}$ nazveme kvadratické reziduum *modulo n, pokud existuje $y \in \mathbb{Z}_n^*$ tak, že*

$$y^2 \equiv x \mod n.$$

Označme $x_p \equiv x \mod p$ a $x_q \equiv x \mod q$.

Věta

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q lichá. Pak x je kvadratické reziduum modulo $n \Leftrightarrow x_p$ je kvadratické reziduum modulo p a zároveň x_q je kvadratické reziduum modulo q.

Důsledek

Pro každé kvadratické reziduum x modulo $n = pq$ existují 4 různá čísla $y_1, y_2, y_3, y_4 \in \mathbb{Z}_n^*$ tak, že $y_i^2 \equiv x \mod n$, $i \in \{1, 2, 3, 4\}$.

Kvadratická rezidua modulo složené číslo n

Definice

Nechť $n \in \mathbb{N}$. Pak $x \in \mathbb{Z}$ nazveme kvadratické reziduum *modulo n, pokud existuje $y \in \mathbb{Z}_n^*$ tak, že*

$$y^2 \equiv x \mod n.$$

Označme $x_p \equiv x \mod p$ a $x_q \equiv x \mod q$.

Věta

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q lichá. Pak x je kvadratické reziduum modulo $n \Leftrightarrow x_p$ je kvadratické reziduum modulo p a zároveň x_q je kvadratické reziduum modulo q.

Důsledek

Pro každé kvadratické reziduum x modulo $n = pq$ existují 4 různá čísla $y_1, y_2, y_3, y_4 \in \mathbb{Z}_n^*$ tak, že $y_i^2 \equiv x \mod n$, $i \in \{1, 2, 3, 4\}$.

Kvadratická rezidua modulo složené číslo n

Důsledek

Počet kvadratických reziduí modulo $n = pq$ *je* $\frac{1}{4}\#\mathbb{Z}_n^* = \frac{(p-1)(q-1)}{4}$.

Definice

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q *lichá. Definujeme* $\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right)$.

Kvadratická rezidua modulo složené číslo n

Důsledek

Počet kvadratických reziduí modulo $n = pq$ *je* $\frac{1}{4}\#\mathbb{Z}_n^* = \frac{(p-1)(q-1)}{4}$.

Definice

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q *lichá. Definujeme* $\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right)$.

Věta

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q *lichá. Pak*

1. *počet prvků ze* $\mathbb{Z}_n^*$ *s Jacobiho symbolem 1 je* $\frac{1}{2}\#\mathbb{Z}_n^*$,
2. *kvadratická rezidua modulo n mají Jacobiho symbol 1,*
3. *polovina prvků ze* $\mathbb{Z}_n^*$ *s Jacobiho symbolem 1 jsou kvadratická rezidua a polovina jsou kvadratická nerezidua.*

Kvadratická rezidua modulo složené číslo n

Důsledek

Počet kvadratických reziduí modulo $n = pq$ *je* $\frac{1}{4}\#\mathbb{Z}_n^* = \frac{(p-1)(q-1)}{4}$.

Definice

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q *lichá. Definujeme* $\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right)$.

Věta

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q *lichá. Pak*

1. *počet prvků ze* $\mathbb{Z}_n^*$ *s Jacobiho symbolem 1 je* $\frac{1}{2}\#\mathbb{Z}_n^*$,
2. *kvadratická rezidua modulo n mají Jacobiho symbol 1,*
3. *polovina prvků ze* $\mathbb{Z}_n^*$ *s Jacobiho symbolem 1 jsou kvadratická rezidua a polovina jsou kvadratická nerezidua.*

Kvadratická rezidua modulo složené číslo n

Věta

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q lichá. Pak pro $x, y \in \mathbb{Z}$ platí

$$\left(\frac{xy}{n}\right) = \left(\frac{x}{n}\right)\left(\frac{x}{n}\right).$$

Důsledek

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q lichá. Nechť $x, x' \in QR_n$ a $y, y' \in QNR_n^{+1}$. Pak

1. $xx' \in QR_n$,
2. $yy' \in QR_n$,
3. $xy \in QNR_n^{+1}$.

Kvadratická rezidua modulo složené číslo n

Věta

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q lichá. Pak pro $x, y \in \mathbb{Z}$ platí

$$\left(\frac{xy}{n}\right) = \left(\frac{x}{n}\right)\left(\frac{x}{n}\right).$$

Důsledek

Nechť $n = pq$, $p, q \in \mathbb{P}, p \neq q$, p, q lichá. Nechť $x, x' \in QR_n$ a $y, y' \in QNR_n^{+1}$. Pak

1. $xx' \in QR_n$,
2. $yy' \in QR_n$,
3. $xy \in QNR_n^{+1}$.

Goldwasserovo-Micaliovo šifrovací schéma

- veřejný klíč = n, soukromý klíč = faktorizace $n = pq$
- šifrování bitu 0 - náhodné kvadratické reziduum modulo n,
  šifrování bitu 1 - náhodné kvadratické nereziduum modulo n
  s Jacobiho symbolem $+1$
- dešifrování = rozhodování, zda číslo je či není kvadratické reziduum modulo n při znalosti $n = pq$

Goldwasserovo-Micaliovo šifrovací schéma

Otázka: Jak odesílatel vybírá náhodná kvadratická rezidua modulo n a kvadratická nerezidua s Jacobiho symbolem $+1$?

1. vybírání náhodných kvadratických reziduí modulo n
   - vyber náhodně $y \in \mathbb{Z}_n^*$
   - polož $x \equiv y^2 \mod n$

Goldwasserovo-Micaliovo šifrovací schéma

Otázka: Jak odesílatel vybírá náhodná kvadratická rezidua modulo n a kvadratická nerezidua s Jacobiho symbolem $+1$?

1. vybírání náhodných kvadratických reziduí modulo n
   - vyber náhodně $y \in \mathbb{Z}_n^*$
   - polož $x \equiv y^2 \mod n$
2. vybírání náhodných kvadratických nereziduí s Jacobiho symbolem $+1$
   - při neznámé faktorizaci n není takový algoritmus (polynomiální v $||n||$) znám

Goldwasserovo-Micaliovo šifrovací schéma

Otázka: Jak odesílatel vybírá náhodná kvadratická rezidua modulo n a kvadratická nerezidua s Jacobiho symbolem $+1$?

1. vybírání náhodných kvadratických reziduí modulo n
   - vyber náhodně $y \in \mathbb{Z}_n^*$
   - polož $x \equiv y^2 \mod n$
2. vybírání náhodných kvadratických nereziduí s Jacobiho symbolem $+1$
   - při neznámé faktorizaci n není takový algoritmus (polynomiální v $||n||$) znám

Goldwasserovo-Micaliovo šifrovací schéma

Otázka: Jak odesílatel vybírá náhodná kvadratická nerezidua s Jacobiho symbolem $+1$?

- pomoci může příjemce, který klíče generuje
- příjemce vybírá navíc náhodné $z \in QNR_n^{+1}$ a (n, z) je pak veřejný klíč
- odesílatel vybírá náhodné $y \in QNR_n^{+1}$ tak, že $y := zx^2 \mod n$, kde $x \in \mathbb{Z}_n^*$ je voleno náhodně

Goldwasserovo-Micaliovo šifrovací schéma

Otázka: Jak odesílatel vybírá náhodná kvadratická nerezidua s Jacobiho symbolem $+1$?

- pomoci může příjemce, který klíče generuje
- příjemce vybírá navíc náhodné $z \in QNR_n^{+1}$ a (n, z) je pak veřejný klíč
- odesílatel vybírá náhodné $y \in QNR_n^{+1}$ tak, že $y := zx^2 \mod n$, kde $x \in \mathbb{Z}_n^*$ je voleno náhodně

Goldwasserovo-Micaliovo šifrovací schéma

- veřejný klíč $= (n, z)$, kde z je náhodné kvadratické nereziduum modulo n
- soukromý klíč $=$ faktorizace $n = pq$
- šifrování $m \in \{0, 1\}$:

$$c := z^m x^2 \mod n$$

- dešifrování $=$ rozhodování, zda číslo je či není kvadratické reziduum modulo n při znalosti $n = pq$
  - spočti $\left(\frac{c}{p}\right)$ a $\left(\frac{c}{q}\right)$, pokud oboje $+1$, pak $m = 0$, jinak $m = 1$

Rabinův algoritmus

založen na obtížnosti hledání modulární odmocniny, tj. řešení $x \equiv y^2 \mod n$, kde x známé, když n je složené číslo

- ekvivalentní faktorizaci $n = pq$ (při znalosti kořenů $y, y' \in \mathbb{Z}_n^*,\ y \neq \pm y'$, lze faktorizovat n v polynomiálním čase v $||n||$)
- RSA - není známo, zda řešitelné bez faktorizace
- Goldwasser-Micali - není známo, zda řešitelné bez faktorizace

Rabinův algoritmus

založen na obtížnosti hledání modulární odmocniny, tj. řešení $x \equiv y^2 \mod n$, kde x známé, když n je složené číslo

- ekvivalentní faktorizaci $n = pq$ (při znalosti kořenů $y, y' \in \mathbb{Z}_n^*,\ y \neq \pm y'$, lze faktorizovat n v polynomiálním čase v $||n||$)
- RSA - není známo, zda řešitelné bez faktorizace
- Goldwasser-Micali - není známo, zda řešitelné bez faktorizace

RSA rozšířenější z historických důvodů (výpočetní náročnost stejná, Rabin dokazatelně bezpečný)

Rabinův algoritmus

založen na obtížnosti hledání modulární odmocniny, tj. řešení $x \equiv y^2 \mod n$, kde x známé, když n je složené číslo

- ekvivalentní faktorizaci $n = pq$ (při znalosti kořenů $y, y' \in \mathbb{Z}_n^*,\ y \neq \pm y'$, lze faktorizovat n v polynomiálním čase v $||n||$)
- RSA - není známo, zda řešitelné bez faktorizace
- Goldwasser-Micali - není známo, zda řešitelné bez faktorizace

RSA rozšířenější z historických důvodů (výpočetní náročnost stejná, Rabin dokazatelně bezpečný)

Výpočet modulární odmocniny modulo prvočíslo

Věta

Nechť $p \in \mathbb{P}$, $p = 3 \mod 4$ *a* $x \in \mathbb{Z}_p^*$ *kvadratické reziduum modulo* p, *pak* $x^{\frac{p+1}{4}}$ *je modulární odmocnina* x, *tj.*

$$x = (x^{\frac{p+1}{4}})^2 \mod p.$$

Výpočet modulární odmocniny modulo složené číslo

Nechť $n = pq, p, q \in \mathbb{P},\ p = 3 \mod 4,\ q = 3 \mod 4$ a $x \in \mathbb{Z}_n^*$ kvadratické reziduum modulo n,

- spočti $x_p \equiv x \mod p$ a $x_q \equiv x \mod q$
- najdi y_p, y_q:

$$x_p \equiv y_p^2 \mod p, \quad x_q \equiv y_q^2 \mod q$$

- z Čínské zbytkové věty urči $y \in \mathbb{Z}_n^*$:

$$y \equiv y_p \mod p, \quad y \equiv y_q \mod q$$

pak y je modulární odmocnina x modulo n, tj.

$$x \equiv y^2 \mod n.$$

Rabinovo šifrovací schéma

- veřejný klíč $= n$
- soukromý klíč $=$ faktorizace $n = pq$
- šifrování $m \in \{0, 1\}$:

$$(c, c') := (y^2 \mod n,\ \mathrm{lsb}(y) \oplus m),$$

  kde y je náhodné kvadratické reziduum modulo n
- dešifrování:
  - spočti jediné $y \in QR_n$ tak, že $c \equiv y^2 \mod n$
  - spočti $m = c' \oplus \mathrm{lsb}(y)$