1 Kvadratické rezíduá

Problematika kvadratických rezíduí má viaceré aplikácie v kryptografii, preto sa jej v tejto časti v nevyhnutnom rozsahu budeme venovať.

Definícia 1. Číslo $a \in \mathbb{Z}_n^*$ (teda číslo z množiny $\{1, \ldots, n-1\}$, ktoré je nesúdeliteľné s n) sa nazýva kvadratickým rezíduom modulo n (označenie QR_n), ak existuje $b \in \{1, \ldots, n-1\}$ také, že $b^2 \equiv a \pmod{n}$. Ak také b neexistuje, nazývame a kvadratickým nerezíduom modulo n (označenie QNR_n).

Príklad. Nech $n = 11$. Z tabuľky vidieť, že čísla 1, 3, 4, 5 a 9 sú QR_{11}.

x	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1

V prípade, že počítame v $\mathbb{Z}_p$, kde p je prvočíslo, je charakterizácia kvadratických rezíduí jednoduchá.

Lema 1. *Nech $p > 2$ je prvočíslo. Potom platí:*

1. *Presne polovica z čísel $\{1, \ldots, p-1\}$ sú QR_p.*
2. *Ak x je riešením rovnice $x^2 \equiv a \pmod{p}$, pre $a \in \{1, \ldots, p-1\}$, tak aj $-x$ (teda $p - x$) je jej riešením.*

Dôkaz.

1. Nech $x^2 \equiv y^2 \pmod{p}$, pre nejaké $x, y \in \mathbb{Z}_p^*$. Potom

$$p \mid (x^2 - y^2) \quad \Rightarrow \quad p \mid (x-y)(x+y).$$

Môžu nastať dva prípady:

$$\begin{aligned} p \mid (x-y) \quad &\Rightarrow \quad x = y \\ p \mid (x+y) \quad &\Rightarrow \quad x = p - y. \end{aligned}$$

V prvom prípade sú x a y rovnaké. V druhom sú rôzne (lebo p je nepárne). Teda na kvadratické rezíduum modulo p sa vždy zobrazia (umocnením na druhú) dva prvky zo $\mathbb{Z}_p^*$. Preto je práve polovica čísel z tejto množiny QR_p.

2. Počítajme: $(p-x)^2 \bmod p = (p^2 - 2px + x^2) \bmod p = x^2 \bmod p = a$, čo bolo treba dokázať.

□

Prirodzenou otázkou pri skúmaní kvadratických rezíduí je hľadanie ich druhých odmocnín, t.j. riešenie rovnice $x^2 \equiv a \pmod{n}$, kde a je QR_n. V nasledujúcej leme sa zameriame na prípad, keď n je prvočíslo v špeciálnom tvare.

Lema 2. *Nech $p \equiv 3 \pmod{4}$ je prvočíslo a nech a je QR_p. Potom riešením rovnice $x^2 \equiv a \pmod{p}$ je $x = a^{\frac{p+1}{4}} \bmod p$.*

Dôkaz. Keďže $p \equiv 3 \pmod{4}$, tak $\frac{p+1}{4}$ je celé číslo. Počítajme:

$$x^2 \equiv (a^{\frac{p+1}{4}})^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \pmod{p}. \quad (1)$$

Vieme, že a je QR_p, preto existuje b také, že $b^2 \equiv a \pmod{p}$. Odtiaľ dostávame:

$$\begin{aligned} (b^2)^{\frac{p-1}{2}} &\equiv a^{\frac{p-1}{2}} \pmod{p} \\ b^{p-1} &\equiv a^{\frac{p-1}{2}} \pmod{p} \\ 1 &\equiv a^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Posledná úprava kongruencie vyplýva z malej Fermatovej vety. Po dosadení do (1) dostávame $x^2 \equiv a \pmod{p}$. □

Lemu 2 možno použiť aj na testovanie, či nejaké $a \in \mathbb{Z}_p^*$ je QR_p, pre prvočíslo p v tvare $p \equiv 3 \pmod{4}$. Postupujeme ako keby a bolo QR_p a nájdeme $x = a^{\frac{p+1}{4}} \bmod p$. Následne vykonáme skúšku správnosti, teda overíme, či $x^2 \equiv a \pmod{p}$. Skúška dopadne úspešne práve vtedy, keď a je naozaj QR_p.

Jednoduchšie testovanie, platné pre ľubovoľné prvočíslo p, poskytuje Eulerovo kritérium:

$$a \text{ je } QR_p \quad \Longleftrightarrow \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Jedna implikácia kritéria vyplýva z malej Fermatovej vety, druhú je možné ukázať cez reprezentáciu prvkov v $(\mathbb{Z}_p^*, \cdot)$ pomocou generátora tejto multiplikatívnej grupy.

Poznámka. Riešenie rovnice $x^2 \equiv a \pmod{p}$ pre prvočíslo $p \equiv 1 \pmod{4}$ a pre QR_p a je zložitejšie, hoci zvládnuteľné v pravdepodobnostnom polynomiálnom čase[1].

Nasledujúca veta sa zaoberá kryptograficky najzaujímavejším prípadom – kvadratickými rezíduami modulo n, kde n je súčin dvoch prvočísel. Presnejšie, venuje sa zložitosti hľadania druhých odmocnín QR_n.

Veta 1. *Nech $n = p \cdot q$, kde $p \neq q$ sú nepárne prvočísla. Potom sú nasledujúce tvrdenia ekvivalentné:*

1. *Existuje pravdepodobnostný polynomiálny algoritmus pre faktorizáciu n.*
2. *Existuje pravdepodobnostný polynomiálny algoritmus pre výpočet druhých odmocnín kvadratických rezíduí modulo n.*

[1] N. Koblitz: *A Course in Number Theory and Cryptography*, Springer-Verlag, 1987, strany 47–48

Dôkaz. (1 $\Rightarrow$ 2) Majme k dispozícii pravdepodobnostný polynomiálny algoritmus pre faktorizáciu n. Použijeme ho a zo zadaného n vypočítame p a q. Chceme riešiť rovnicu $x^2 \equiv a \pmod n$, kde a je QR_n. Ak by a bolo QNR_n, tak jednoducho vypočítame nekorektnú druhú odmocninu (lebo neexistuje), čo vieme následne overiť skúškou správnosti. Najskôr nájdeme druhé odmocniny a modulo p a modulo q. Ak sú $p, q \equiv 3 \pmod 4$, tak môžeme použiť lemu 2, v opačnom prípade treba použiť náročnejší postup (pozri poznámku pred vetou). Dostaneme:

$$\begin{aligned} u^2 &\equiv a \pmod p \\ v^2 &\equiv a \pmod q \end{aligned}$$

Použitím Čínskej zvyškovej vety získame hľadané riešenie ako lineárnu kombináciu u a v:

$$x = (u \cdot q \cdot (q^{-1} \bmod p) + v \cdot p \cdot (p^{-1} \bmod q)) \bmod n.$$

Ľahko môžeme overiť, že

$$\begin{aligned} x &\equiv u \pmod p \\ x &\equiv v \pmod q \end{aligned} \quad \Longrightarrow \quad \begin{aligned} x^2 &\equiv a \pmod p \\ x^2 &\equiv a \pmod q. \end{aligned}$$

Prvočísla p a q sú nesúdeliteľné, preto $x^2 \equiv a \pmod n$.

(2 $\Rightarrow$ 1) Majme k dispozícii algoritmus, ktorý rieši rovnice $x^2 \equiv a \pmod n$. Ukážeme, ako faktorizovať n.

Zvolíme náhodne $m \in_R \mathbb{Z}_n^*$ a položíme $a = m^2 \bmod n$. Necháme si nájsť riešenie rovnice $x^2 \equiv a \pmod n$ algoritmom, ktorý máme k dispozícii. Ten vypočíta riešenie k (jedno zo 4 možných). Môže nastať jedna z nasledujúcich, rovnako pravdepodobných možností:

A	$k \equiv$	$m \pmod p$	$\wedge$	$k \equiv$	$m \pmod q$
B	$k \equiv$	$m \pmod p$	$\wedge$	$k \equiv -m$	$\pmod q$
C	$k \equiv -m$	$\pmod p$	$\wedge$	$k \equiv$	$m \pmod q$
D	$k \equiv -m$	$\pmod p$	$\wedge$	$k \equiv -m$	$\pmod q$

Tieto 4 alternatívy vyplývajú z toho, že $m^2 \equiv k^2 \pmod n$, teda $pq \mid (m+k)(m-k)$. V prípade B máme $\mathrm{nsd}(k-m, n) = p$, v prípade C $\mathrm{nsd}(k-m, n) = q$. Teda s pravdepodobnosťou $\frac{1}{2}$ dostaneme pri výpočte $\mathrm{nsd}(k-m, n)$ netriviálny faktor n. Pravdepodobnosť, že n nefaktorizujeme po l opakovaniach nášho postupu je 2^{-l}. □

2 Rabinov systém

Rabinov systém patrí medzi tie asymetrické šifrovacie systémy, o ktorých bezpečnosti sa dá dokázať, že je ekvivalentná s problémom faktorizácie. Medzi ďalšie takéto systémy patria napríklad schémy navrhnuté Williamsom[2] alebo Loxtonom[3]. Všetky však zdieľajú spoločnú slabinu: keďže dôkaz ekvivalencie s problémom faktorizácie je konštruktívny, sú neodolné voči útoku s možnosťou voľby šifrového textu (CCA).

Inicializácia. Používateľ zvolí dve veľké rôzne prvočísla p a q, pričom $p, q \equiv 3 \pmod 4$. Verejný kľúč je číslo $n = p \cdot q$. Súkromný kľúč tvorí faktorizácia n, teda prvočísla p, q.

Množina otvorených textov je $\mathbb{Z}_n$. Šifrový text v Rabinovom systéme je druhou mocninou otvoreného textu: $E(m) = m^2 \bmod n$, pre $m \in \mathbb{Z}_n$. Dešifrovanie je zložitejšie. Šifrovacia funkcia E na množine $\mathbb{Z}_n$ totiž nie je injektívna.

Ak $\mathrm{nsd}(m, n) = 1$, tak $E(m)$ je kvadratické rezíduum modulo n (QR_n, pozri časť 1). Keďže n je súčinom dvoch prvočísel, má každé QR_n, označme ho c, práve 4 druhé odmocniny. Ak $\mathrm{nsd}(m, n) \neq 1$, čo je veľmi nepravdepodobný prípad, tak buď $m = 0$ (vtedy $E(m) = 0$ a vieme jednoznačne dešifrovať) alebo $\mathrm{nsd}(m, n)$ je netriviálny faktor n (vtedy môžeme považovať náš súkromný kľúč za prezradený). V takomto prípade je druhá odmocnina jedna alebo sú dve. V ďalšej diskusii predpokladajme situáciu $\mathrm{nsd}(m, n) = 1$, a teda 4 odmocniny môžeme vypočítať takto: najskôr určíme druhé odmocniny c ($c = E(m)$) modulo p a modulo q (ak je c QR_n, tak je triviálne aj QR_p a QR_q). V oboch prípadoch sú to dve odmocniny, pozri lemu 2:

$$\begin{aligned} r_{1,2} &= \pm c^{\frac{p+1}{4}} \bmod p, \\ r_{3,4} &= \pm c^{\frac{q+1}{4}} \bmod q. \end{aligned}$$

Druhé odmocniny c modulo n dostaneme ich lineárnou kombináciou podľa Čínskej zvyškovej vety (pre korektnosť tohto postupu pozri prvú časť dôkazu vety 1):

$$\begin{aligned} M_1 &= (ar_1 + br_3) \bmod n, \\ M_2 &= (ar_1 + br_4) \bmod n, \\ M_3 &= (ar_2 + br_3) \bmod n, \\ M_4 &= (ar_2 + br_4) \bmod n, \end{aligned}$$

kde $a = q \cdot (q^{-1} \bmod p)$ a $b = p \cdot (p^{-1} \bmod q)$.

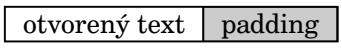
Takže po dešifrovaní dostávame potenciálne 4 otvorené texty. Pokiaľ je očakávaný otvorený text kontextovo závislý (má nejakú štruktúru), je jednoduché odlíšiť ho od ostatných. V opačnom prípade je potrebné k textu pred šifrovaním pridávať vhodnú hlavičku alebo tzv. „padding“ (pozri ďalej).

Ľahko vidieť, že bezpečnosť Rabinovho systému je založená na probléme počítania druhých odmocnín modulo n, kde n je súčin dvoch veľkých prvočísel. Tento problém je ekvivalentný problému faktorizácie n, podľa vety 1.

[2] H.C. Williams: *A modification of the RSA public-key procedure*, IEEE Transactions on Information Theory IT-26, 1980.
[3] J.H. Loxton, D.S.P. Khoo, G.J. Bird, J. Seberry: *A cubic RSA code equivalent to factorization*, Journal of Cryptology, Vol. 5, 1992.

Nepríjemnou, už vyššie avizovanou vlastnosťou Rabinovho systému je neodolnosť voči útoku s možnosťou voľby šifrového textu (CCA). Predstavme si, že protivník si môže zvoliť šifrový text c, ktorý mu majiteľ tajného kľúča dešifruje. Teda protivník dostane na požiadanie jednu zo štyroch druhých odmocnín modulo n. CCA prebieha nasledovne: protivník zvolí náhodné $m \in_R \mathbb{Z}_n^*$ a nechá si dešifrovať $c = m^2 \bmod n$. Po zistení k, $k^2 \equiv c \pmod n$, môžu nastať 4 prípady – rovnaké ako pri dôkaze vety 1. Útočník následným výpočtom $\mathrm{nsd}(k - m, n)$ faktorizuje n s pravdepodobnosťou $\frac{1}{2}$. Pri l pokusoch je pravdepodobnosť úspešného útoku protivníka (teda faktorizácie n) $1 - 2^{-l}$. Rabinov systém je preto možné použiť len v takom prostredí (v takých protokoloch), kde nie je možné realizovať CCA.

Padding (vypchávka)
Padding je doplnenie otvoreného textu pred šifrovaním (šifrovacou transformáciou), najčastejšie reťazcom bitov pevnej dĺžky. Doplnenie môže byť realizované náhodným reťazcom, konštantou, prípadne kontrolným súčtom. Padding znižuje mohutnosť množiny otvorených textov. Na druhej strane, pomáha riešiť niektoré bezpečnostné alebo praktické problémy spojené s použitím konkrétneho asymetrického systému. Napríklad náhodný padding pri RSA pomáha, ak je počet potenciálnych správ malý.



V Rabinovom systéme má zmysel uvažovať o konštantnom paddingu alebo o paddingu s kontrolným súčtom z nasledujúcich dôvodov:

1. Umožní sa jednoznačné dešifrovanie, vďaka schopnosti odlíšiť správny otvorený text. Po dešifrovaní totiž očakávame (a skontrolujeme) definovaný padding.
2. Zamedzí sa realizácii CCA útoku, keď po dešifrovaní skontrolujeme padding. Ak žiadny zo štvorice textov nevyhovuje, bude výsledok dešifrovania prázdny. Podotknime, že v takto upravenom Rabinovom systéme už nie sme schopní dokázať ekvivalenciu rozbitia systému a problému faktorizácie.