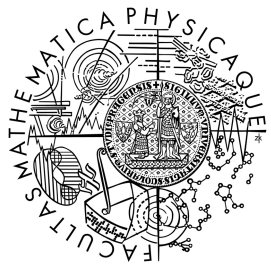
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Petr Vácha

Kryptografické využití grupy kvadratických residuí

Katedra algebry

Vedoucí bakalářské práce: Mgr. Štěpán Holub, Ph.D.
Studijní program: Matematika, Obecná matematika

2010

Děkuji vedoucímu své bakalářské práce Mgr. Štěpánu Holubovi, Ph.D. za cenné rady a konzultace.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 3. srpna 2010 Petr Vácha

Obsah

Název práce: Kryptografické využití grupy kvadratických residuí
Autor: Petr Vácha
Katedra: Katedra algebry
Vedoucí bakalářské práce: Mgr. Štěpán Holub, Ph.D.
e-mail vedoucího: holub@karlin.mff.cuni.cz

Abstrakt: V předložené práci studujeme vlastnosti grupy kvadratických zbytků a možnosti jejího použití v kryptografii. V druhé kapitole se zabýváme strukturou této grupy. Konkrétně velikostí a cykličností. Dále v práci popisujeme grupu znaménkových kvadratických zbytků, která je jakýmsi vylepšením grupy kvadratických zbytků. Ve třetí kapitole referujeme jeden z výsledků práce [1] a doplňujeme ho o podrobnosti a komentáře. Definujeme v ní asymetrický šifrovací systém využívající vlastností grupy znaménkových kvadratických zbytků popsaných v druhé kapitole a dokazujeme jeho IND-CCA bezpečnost za předpokladu, že faktorizace je obtížný problém.

Klíčová slova: kvadratické zbytky, hybridní ElGamal, asymetrická kryptografie

Title: The Group of Quadratic Residues in Cryptography
Author: Petr Vácha
Department: Department of algebra
Supervisor: Mgr. Štěpán Holub, Ph.D.
Supervisor's e-mail address: holub@karlin.mff.cuni.cz

Abstract: In the present work we study the group of quadratic residues and possibilities of its applications in cryptography. In the second chapter we deal with the structure of this group. Concretely we deduce the size of group and when this group is cyclic. Then we describe the group of signed quadratic residues which is an upgrade of the group of quadratic residues. In the third chapter we report on one of the results of the work [1] and supply details and comments. We define the asymetric encryption scheme which use the properties of the group of signed quadratic residues. Assuming that factoring is a hard problem we prove IND-CCA security of defined encryption scheme.

Keywords: quadratic residues, hybrid ElGamal, asymetric encryption

Kapitola 1

Úvod

V práci budeme studovat vlastnosti grupy kvadratických zbytků a její možné využití v kryptografii. Definujeme také grupu znaménkových kvadratických zbytků, která má oproti grupě obyčejných kvadratických zbytků jednu výhodu, její prvky se totiž dají efektivně rozpoznávat od prvků, které do ní nepatří. Dále se budeme zabývat konstrukcí asymetrického šifrovacího systému nazvaného hybridní ElGamalův šifrovací systém a provedeme důkaz jeho bezpečnosti.

Důkazy bezpečnosti kryptosystémů se většinou provádí tak, že otázka bezpečnosti systému se převede na problém řešení nějakého matematického problému, který je obecně považován za obtížný. V našem případě budeme za prolomení bezpečnosti systému považovat, pokud útočník dokáže s nezanedbatelnou pravděpodobností rozlišit dvě zašifrované zprávy vlastního výběru (tzv. IND-CCA bezpečnost). Důkaz bezpečnosti v tomto smyslu pak provedeme tak, že problém rozpoznání, která ze dvou zpráv byla zašifrována, převedeme na problém faktorizace velkých čísel.

Kapitola 2

Definice a struktura grupy kvadratických zbytků

V úvodní kapitole definujeme grupu kvadratických zbytků a seznámíme se s jejími základními vlastnostmi.

2.1 Kvadratické zbytky

Definice 2.1.1 *Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$. Řekneme, že a je kvadratickým zbytkem(residuem) modulo n, pokud existuje x přirozené takové, že $x^2 \equiv a \mod n$. V opačném případě nazýváme a kvadratickým nezbytkem.*

Lemma 2.1.2 *Buď $n \in \mathbb{N}$. Označme $\mathbb{Z}_n^*$ množinu všech invertibilních prvků okruhu $\mathbb{Z}_n$. Množina $\mathbb{QR}_n = \{a \in \mathbb{Z}_n^* \mid a$ je kvadratický zbytek modulo $n\}$ spolu s násobením stejným jako v $\mathbb{Z}_n$ (tj. násobení modulo n) tvoří grupu.*

Důkaz : Zřejmě $1 \in \mathbb{QR}_n$. Dále pokud $a, b \in \mathbb{QR}_n$, existují podle definice $x, y \in \mathbb{N}$, že $a \equiv x^2$ a $b \equiv y^2$ (mod n). Pak ale $ab \equiv x^2y^2 = (xy)^2$, tedy $ab \in \mathbb{QR}_n$. Dále platí $a^{-1} = (x^2)^{-1} = (x^{-1})^2$ a tedy také $a^{-1} \in \mathbb{QR}_n$.

□

Definice 2.1.3 *Grupu $\mathbb{QR}_n$ definovanou v předchozím lemmatu budeme dále nazývat grupou kvadratických zbytků.*

Jako důležitá se později ukáže otázka, kdy $-1 \in \mathbb{QR}_n$? To zodpovíme v následující sérii lemmat a tvrzení. Budeme však potřebovat vědět něco málo o okruhu Gaussových celých čísel a jeho prvočinitelích.

Definice 2.1.4 *Okruh Gaussových celých čísel definujeme jako podokruh komplexních čísel s nosnou množinou* $\mathbb{Z}[i] = \{a + ib |\ a, b \in \mathbb{Z}\}$. *Značit ho budeme taktéž* $\mathbb{Z}[i]$. *Dále v tomto okruhu definujeme zobrazení* $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ *předpisem* $N(a + ib) = a^2 + b^2$. *Toto zobrazení budeme nazývat normou.*

Okruh Gaussových celých čísel je Eukleidovský obor s normou N. Je to tedy také Gaussův obor. To znamená, že prvočinitelé tohoto okruhu jsou právě ireducibilní prvky, a že každý prvek $\mathbb{Z}[i]$ má až na asociovanost jednoznačný rozklad na součin prvočinitelů.

Lemma 2.1.5 *Pro každé* $\alpha, \beta \in \mathbb{Z}[i]$ *platí*
(i) $N(\alpha\beta) = N(\alpha)N(\beta)$,
(ii)pokud $\alpha|\beta$, *pak* $N(\alpha)|N(\beta)$,
(iii) pokud $N(\alpha) = 1$, *pak* α *je invertibilní v* $\mathbb{Z}[i]$,
(iv) pokud $N(\alpha) = N(\beta)$ *a* $\alpha|\beta$, *pak* $\beta|\alpha$,
(v) pokud je α *prvočinitel, pak* $N(\alpha) = p$ *nebo* $N(\alpha) = p^2$ *pro nějaké prvočíslo* p.

Důkaz :
(i) Ať $\alpha = a + ib$ a $\beta = c + id$, pak $N(\alpha\beta) = N((ac - bd) + i(ad + bc)) = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta)$.
(ii) Je snadný důsledek bodu (i). Pokud $\beta = \gamma\alpha$ pak $N(\beta) = N(\gamma)N(\alpha)$, tedy $N(\alpha)|N(\beta)$
(iii) Ať $\alpha = a+ib$, pak $1 = N(\alpha) = a^2+b^2$, tedy jedno z čísel a a b je v absolutní hodnotě 1 a druhé 0. Dostáváme tedy, že $\alpha \in \{-1, 1, i, -i\}$ a to jsou zřejmě invertibilní prvky.
(iv) $\alpha|\beta$ tedy $\beta = \gamma\alpha$ pro nějaké $\gamma \in \mathbb{Z}[i]$. Pak ale $N(\alpha) = N(\beta)N(\gamma) = N(\alpha)N(\gamma)$. Po vydělení máme $N(\gamma) = 1$, tedy γ je invertíbilní, a $\beta\gamma^{-1} = \alpha$. Odtud $\beta|\alpha$.
(v) Norma prvku je celé číslo, proto existují $p_1, p_2, \ldots, p_k$ prvočísla a $\alpha_1, \alpha_2, \ldots, \alpha_k$ přirozená čísla taková, že $N(\alpha) = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$. Zároveň ovšem platí, že $N(\alpha) = \alpha\bar{\alpha}$. Tedy

$$\alpha\bar{\alpha} = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}.$$

Protože α i $\bar{\alpha}$ jsou prvočinitelé a $\mathbb{Z}[i]$ je Gaussův, je nutně $k \leq 2$. Pokud je $k = 1$, je $\alpha_1 \leq 2$. To je v souladu se zněním lemmatu. Pokud je $k = 2$, je nutně

$\alpha_1 = \alpha_2 = 1$ a p_1 i p_2 jsou prvočinitelé v $\mathbb{Z}[i]$. Proto $p_1||\alpha$ a $p_2||\bar{\alpha}$, nebo $p_2||\alpha$ a $p_1||\bar{\alpha}$. Stačí vyřešit první možnost, ta druhá je symetrická. Podle bodu (ii) mají asociované prvky stejnou normu, proto $N(\alpha) = N(p_1) = p_1^2$. Tím je důkaz dokončen.

□

Lemma 2.1.6 *Buď $p \in \mathbb{Z}$ liché prvočíslo, pak p je prvočinitel v $\mathbb{Z}[i]$ právě když $p \equiv 3 \mod 4$.*

Důkaz :

"$\Leftarrow$": Nechť $p = 4k + 3$. Pro spor předpokládejme, že existuje prvočinitel $\pi \in \mathbb{Z}[i]$ neasociovaný s p takový, že $\pi|p$. Podle předchozího lemmatu (bod (v)) existuje prvočíslo q splňující $N(\pi) = q$ nebo $N(\pi) = q^2$. Protože $\pi|p$, tak podle bodu (ii) předchozího lemmatu také $N(\pi)|N(p) = p^2$. Tedy $q|p^2$, proto $p = q$. Je tedy $N(\pi) = p$, nebo $N(\pi) = p^2$. Obě tyto možnosti nyní dovedeme ke sporu. Ať $\pi = a + ib$. Pokud $N(\pi) = p$, je $a^2 + b^2 = p = 4k + 3$. Tato rovnost ale nemůže být splněna. Budeme-li ji totiž uvažovat modulo 4, dostaneme na levé straně 0, 1, nebo 2 zatímco na pravé straně máme 3. Pokud je $N(\pi) = p^2$, dostáváme $\pi\bar{\pi} = p^2$. To ovšem znamená, že $\pi||p$ a to je spor s úvodním předpokladem.

"$\Rightarrow$": Pro spor předpokládejme, že p je prvočinitel v $\mathbb{Z}[i]$ a zároveň existuje $k \in \mathbb{Z}$ tak, že $p = 4k + 1$. Podle Fermatovy věty platí $a^{p-1} \equiv 1 \mod p$ pro každé nenulové $a \in \mathbb{Z}_p$. Pak $a^{4k} - 1 \equiv 0 \mod p$. Položíme-li $x = a^{2k}$, dostaneme $x^2 - 1 \equiv 0 \mod p$, tedy $p|(x^2 - 1)$ v celých číslech, a proto $p|(x - i)(x + i)$ v $\mathbb{Z}[i]$. Z toho ale plyne, že $p|i$, tedy p je invertibilní. To je ale spor s předpokladem, že p je prvočinitel.

□

Lemma 2.1.7 *Buď p prvočíslo, pak $-1 \in \mathbb{QR}_p$, právě když $p \equiv 1 \mod 4$, nebo $p = 2$.*

Důkaz :

"$\Leftarrow$": Pokud $p = 2$, je $1 \equiv -1 \mod 2$ tedy $-1 \in \mathbb{QR}_2$. Pokud $p > 2$, existuje $k \in \mathbb{N}$ takové, že $p = 4k + 1$. Podle Fermatovy věty platí $a^{p-1} \equiv 1 \mod p$ pro každé nenulové $a \in \mathbb{Z}_p$. Pak $a^{4k} + 1 \equiv 0 \mod p$ a to můžeme rozložit na $(a^{2k} - 1)(a^{2k} + 1) \equiv 0 \mod p$. Protože $\mathbb{Z}_p$ je obor integrity, musí být aspoň

jeden z činitelů nulový(v $\mathbb{Z}_p$). Ale první činitel je polynom stupně $2k$, má tedy nejvýše $2k$ kořenů. Protože ale rovnice platí pro každé $a \in \mathbb{Z}_p$, musí existovat $b \in \mathbb{Z}_p$ takové, že je kořenem druhého činitele, tedy $(b^{2k}+1) \equiv 0 \mod p$. Pokud položíme $c = b^k$, dostáváme $c^2 \equiv -1 \mod p$, tedy $-1 \in \mathbb{QR}_p$.

"$\Rightarrow$": Pro spor předpokládejme, že $p \equiv 3 \mod 4$ a zároveň existuje $x \in \mathbb{N}$ takové, že $x^2 \equiv -1 \mod p$. Pak $x^2 + 1 \equiv 0 \mod p$, tedy existuje l celé, že $x^2+1 = lp$. Uvažujeme-li celá čísla jako podokruh $\mathbb{Z}[i]$, pak platí $(x+i)(x-i) = lp$ v $\mathbb{Z}[i]$. Tedy $p|(x+i)(x-i)$, ale dle předchozího lemmatu je p prvočinitel v $\mathbb{Z}[i]$, tedy $p|(x+i)$ nebo $p|(x-i)$. Protože p má nulovou imaginární část, dostáváme, že $p|i$. To ale znamená, že p je invertibilní. Dostali jsme spor s tím, že p je prvočinitel, tedy lemma je dokázáno.

□

Lemma 2.1.8 *Buďte $m, n \in \mathbb{N}$ taková, že $m|n$. Ať a je kvadratický zbytek modulo n. Pak a je kvadratický zbytek modulo m.*

Důkaz : Dle předpokladu existují $x \in \mathbb{N}$ a $r \in \mathbb{Z}$ taková, že $x^2 - a = 0 \mod n$ a $n = rm$. Tedy existuje $s \in \mathbb{Z}$, že $x^2 - a = sn$. Odtud máme $x^2 - a = srm$, tedy $x^2 - a \equiv 0 \mod m$. Odtud vidíme, že a je kvadratický zbytek modulo m.

□

Lemma 2.1.9 *Nechť n je liché přirozené číslo a nechť $a \in \mathbb{Z}$. Pak pro $\alpha \in \mathbb{N}$ platí $(a \mod n) \in \mathbb{QR}_n$ právě když $(a \mod n^\alpha) \in \mathbb{QR}_{n^\alpha}$.*

Důkaz : Implikace zprava doleva plyne z předchozího lemmatu, neboť $n|n^\alpha$. Nechť tedy $(a \mod n) \in \mathbb{QR}_n$. To znamená, že a je nesoudělné s n a existuje $x \in \mathbb{Z}$ takové, že $x^2 - a \equiv 0 \mod n$. Nyní ukážeme, že existuje k celé tak, že $(x+kn)^2 - a \equiv 0 \mod n^2$. Protože a je nesoudělné s n, platí totéž i pro x(pokud by x bylo soudělné, je i $a = x^2$ soudělné). Tedy lineární rovnice $u+lx \equiv 0 \mod n$ s neznámou l má řešení pro každé $u \in \mathbb{Z}$. Speciálně tedy existuje $k \in \mathbb{Z}$, že platí

$$\frac{x^2 - a}{n} + 2kx \equiv 0 \mod n.$$

Vynásobením n dostáváme

$$(x^2 - a) + 2knx \equiv 0 \mod n^2$$

a protože $k^2n^2 \equiv 0 \mod n^2$, máme

$$x^2 + 2knx + k^2n^2 - a \equiv 0 \mod n^2,$$

tedy

$$(x + kn)^2 - a \equiv 0 \mod n^2.$$

Zatím jsme tedy dokázali tvrzení pro $\alpha = 2$. Obecný případ už však lze získat snadno. Protože n je liché, je n^2 také liché a opět můžeme aplikovat tvrzení pro případ $\alpha = 2$. Tak dostaneme důkaz pro $\alpha = 4$. Dalším aplikováním již dokázaného tedy dostaneme důkaz pro libovolnou mocninu dvojky. Buď nyní α libovolné. Buď e nejmenší takové, že $2^e > \alpha$. Lemma platí pro 2^e tj. existuje y, že $y^2 - a \equiv 0 \mod n^{2^e}$. Protože ale $n^\alpha | n^{2^e}$ dostáváme s použitím předchozího lemmatu, že $y^2 - a \equiv 0 \mod n^\alpha$. Tedy $(a \mod n^\alpha) \in \mathbb{QR}_{n^\alpha}$.

□

Důsledek 2.1.10 *Speciálaní případ předchozího lemmatu dává: Pro n liché celé a pro α přirozené platí $-1 \in \mathbb{QR}_n$ právě když $-1 \in \mathbb{QR}_{n^\alpha}$.*

Lemma 2.1.11 *Buď $e \in \mathbb{N}$, pak $-1 \in \mathbb{QR}_{2^e}$ právě když $e = 1$.*

Důkaz : Pokud $e = 1$ pak $-1 \equiv 1 \mod 2^e$. Nechť tedy $e \geq 2$. Pokud by platilo $-1 \in \mathbb{QR}_{2^e}$, pak existuje $x \in \mathbb{Z}$ tak, že $x^2 + 1 \equiv 0 \mod 2^e$, tedy existuje $k \in \mathbb{Z}$, že $x^2 + 1 = k2^e$ tj. $x^2 + 1 = 4k2^{e-2}$. Poslední rovnost platí v celých číslech, tedy musí platit i pokud ji uvažujeme modulo 4. Ale kvadratické zbytky modulo 4 jsou pouze 1 a 0, tedy dostáváme buď $1 + 1 \equiv 0 \mod 4$, nebo $0 + 1 \equiv 0 \mod 4$. Nic z toho zřejmě neplatí, tedy dostáváme spor s tím, že $-1 \in \mathbb{QR}_{2^e}$ a lemma je tím dokázáno.

□

Tvrzení 2.1.12 *Buď $n \in \mathbb{N}$ takové, že $n = 2^e p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kde p_i jsou po dvou různá lichá prvočísla. Pak $-1 \in \mathbb{QR}_n$ právě když $e \leq 1$ a $p_i \equiv 1 \mod 4$ pro každé $i \in \{1, 2, \dots, k\}$.*

Důkaz : Důkaz dostaneme aplikací čínské věty o zbytcích a předchozích dvou lemmat. Podle čínské věty o zbytcích jsou okruhy $\mathbb{Z}_n$ a $\mathbb{Z}_{2^e} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$ izomorfní(v druhém se sčítá a násobí po složkách). Řešení rovnice $x^2 + 1 \equiv 0$

mod n tedy existuje právě když existuje řešení všech rovnic $x_i^2 + 1 \equiv 0 \mod p_i^{\alpha_i}$ a $x_0^2 + 1 \equiv 0 \mod 2^e$. Tato řešení podle předchozích dvou lemmat a lemmatu 2.1.7 existují, právě když jsou splněny předpoklady tohoto tvrzení.

□

Definice 2.1.13 *Přirozené číslo n nazveme 3-složené, pokud se v jeho prvočíselném rozkladu vyskytují pouze prvočísla dávající zbytek 3 po dělení čtyřmi.*

Tvrzení 2.1.14 *Buď $n \in \mathbb{N}$. Definujme zobrazení*

$$\begin{aligned} \rho : \mathbb{QR}_n &\longrightarrow \mathbb{QR}_n \\ x &\longmapsto x^2 \end{aligned}$$

Pokud n je 3-složené, pak je zobrazení ρ automorfismem grupy $\mathbb{QR}_n$.

Důkaz : Dle předpokladu existují prvočísla $p_1, p_2, \ldots, p_k$ a $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ taková, že $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ a $\forall i \in \{1, 2, \ldots, k\}$ platí $p_i \equiv 3 \mod 4$. Zřejmě ρ je homomorfismus, neboť $(ab)^2 = a^2 b^2$. Protože $\mathbb{QR}_n$ je konečná, stačí ukázat, že ρ je prostý. Ukážeme tedy, že $Ker(\rho) = \{1\}$. Ať tedy $a^2 = 1$, pak máme $a^2 - 1 = 0$, z toho $(a-1)(a+1) = 0$. Protože $\mathbb{Z}_n$ nemusí být obor integrity, může odvozená rovnost nastat třemi způsoby.
(i) $a = 1$
(ii) $a = -1$
(iii) existují $r, s \in \mathbb{N}$ taková, že $r = p_1^{\mu_1} p_2^{\mu_2} \ldots p_k^{\mu_k}$, $s = p_1^{\nu_1} p_2^{\nu_2} \ldots p_k^{\nu_k}$ kde všechny exponenty jsou nezáporné a platí: $\forall i \in \{1, 2, \ldots, k\}$ je $\alpha_i = \mu_i + \nu_i$ a navíc $s|(a-1)$ a zároveň $r|(a+1)$.
Vyloučením případů (ii) a (iii) dostaneme požadované tvrzení. Zřejmě (ii) nastat nemůže, neboť $a \in \mathbb{QR}_n$ a tedy $a = -1$ je ve sporu s $-1 \notin \mathbb{QR}_n$, což platí podle předchozího tvrzení. Nechť nyní platí (iii). Dostáváme, že $a \equiv -1 \mod r$. Ale r je dělitel čísla n(a tudíž je také 3-složené), tedy podle tvrzení 2.1.12 platí $-1 \notin \mathbb{QR}_r$ a podle lemmatu 2.1.8 je $a \in \mathbb{QR}_r$ a to je opět spor s $a \equiv -1 \mod r$. Tedy může nastat pouze případ (i) a tím je tvrzení dokázáno.

□

Definice 2.1.15 *Buď p prvočíslo, pro $a \in \mathbb{Z}$ definujme Legendrův symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{pokud } (a \mod p) \in \mathbb{QR}_p \\ -1 & \text{pokud } (a \mod p) \notin \mathbb{QR}_p \text{ a zároveň } p \nmid a \\ 0 & \text{pokud } p|a \end{cases}$$

Stejné označení jako pro Legendrův symbol budeme používat i pro tzv. Jacobiho symbol, který definujeme následovně:

Definice 2.1.16 *Buď n přirozené číslo. Mějme $p_1, p_2, \ldots, p_k$ po dvou různá prvočísla a $\alpha_1, \alpha_2, \ldots, \alpha_k$ přirozená čísla taková, že $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Pro $a \in \mathbb{Z}$ definujeme Jacobiho symbol předpisem*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Je vidět, že stejné značení pro oba symboly je oprávněné. Je-li totiž n prvočíslo, pak oba symboly mají stejnou hodnotu. Zajímavé je, že Jacobiho symbol se dá velice rychle počítat a to i bez znalosti faktorizace čísla n [3].

2.2 Velikost $\mathbb{QR}_n$

Lemma 2.2.1 *Buď p liché prvočíslo a buď $\alpha \in \mathbb{N}$. Pokud $a \in \mathbb{QR}_{p^\alpha}$, pak a má právě 2 různé odmocniny v $\mathbb{Z}^*_{p^\alpha}$ tj. existují právě dvě různá $u, v \in \mathbb{Z}^*_{p^\alpha}$, že $u^2 = a$ a $v^2 = a$.*

Důkaz : Hledáme všechna $k \in \mathbb{Z}^*_{p^\alpha}$ taková, že $a = k^2$ v $\mathbb{Z}^*_{p^\alpha}$. Víme, že existuje $x \in \mathbb{Z}^*_{p^\alpha}$, že $x^2 = a$. Tedy budeme řešit rovnici $x^2 = k^2$ v $\mathbb{Z}^*_{p^\alpha}$. Úpravou dostaneme $(x-k)(x+k) = 0$. Dvě řešení jsou hned vidět, sice $k = \pm x$. Poslední možnost, jak by rovnost mohla nastat je, že existuje $\beta < \alpha$ tak, že $p^\beta|(x-k)$ a $p^{\alpha-\beta}|(x+k)$. Z toho ale plyne, že $p|(x-k)$ a $p|(x+k)$, tedy musí dělit i součet obou závorek. Dostáváme proto $p|2x$, to je ale spor s $x \in \mathbb{Z}^*_{p^\alpha}$. Tedy $k = \pm x$ jsou jediná dvě řešení.

□

Lemma 2.2.2 *Buď $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_l^{\alpha_l}$ pro $\alpha_i \in \mathbb{N}$ a pro p_i po dvou různá lichá prvočísla. Ať $a \in \mathbb{QR}_n$, pak a má v $\mathbb{Z}^*_n$ právě 2^l různých odmocnin.*

Důkaz : $a \in \mathbb{QR}_n$, tedy existuje $x \in \mathbb{Z}_n^*$, že $a = x^2$. Opět hledáme všechna $k \in \mathbb{Z}_n^*$ taková, že $x^2 = k^2$. Protože podle čínské zbytkové věty jsou okruhy $\mathbb{Z}_n$ a $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_l^{\alpha_l}}$ izomorfní, řešení existuje právě když existuje řešení ve všech složkách. Tj. pokud x odpovídá l-tici $(x_1, x_2, \ldots, x_l)$, pak hledáme všechny l-tice $(k_1, k_2, \ldots, k_l)$ takové, že $\forall i \in \{1, 2, \ldots, l\}$ je $x_i^2 = k_i^2$. Podle předchozího lemmatu dostáváme v každé složce právě dvě řešení. Libovolná kombinace řešení v jednotlivých složkách odpovídá vždy jednomu řešení rovnice $x^2 = k^2$ v $\mathbb{Z}_n^*$. Tedy počet všech různých řešení je 2^l.

□

Tvrzení 2.2.3 *Pokud má $n \in \mathbb{N}$ v rozkladu právě k různých prvočísel, pak*

$$|\mathbb{QR}_n| = \frac{\phi(n)}{2^k}.$$

kde $\phi(n)$ je Eulerova funkce udávající velikost $\mathbb{Z}_n^*$

Důkaz : Definujme zobrazení

$$\begin{array}{rcl} \sigma : \mathbb{Z}_n^* & \longrightarrow & \mathbb{QR}_n \\ x & \longmapsto & x^2 \end{array}$$

σ je zřejmě grupový homomorfismus. Podle předchozího tvrzení má každý prvek z $\mathbb{QR}_n$ právě 2^k různých odmocnin v $\mathbb{Z}_n^*$. Speciálně i jednotka. Tedy $|Ker(\sigma)| = |\{x \in \mathbb{Z}_n^* : x^2 = 1\}| = 2^k$. σ je zřejmě na, proto je podle první věty o izomorfismu $\mathbb{Z}_n^*/Ker(\sigma) \simeq Im(\sigma) = \mathbb{QR}_n$, tedy $|\mathbb{Z}_n^*/Ker(\sigma)| = |\mathbb{QR}_n|$, proto $|\mathbb{QR}_n| = \phi(n)/2^k$.

□

Jako důsledek tohoto tvrzení teď odvodíme snadno vyčíslitelný vzorec pro výpočet odmocniny ležící v $\mathbb{QR}_n$.

Důsledek 2.2.4 *Buď n přirozené 3-složené číslo, které má v rozkladu právě k různých prvočísel. Pro $a \in \mathbb{QR}_n$ označme x jedinou odmocninu, která leží v $\mathbb{QR}_n$. Pak*

$$x = a^{\frac{\phi(n)+2^k}{2^{k+1}}}.$$

Důkaz : Pokud je pravá strana dobře definovaná, pak ověření rovnosti je snadné

$$\left(a^{\frac{\phi(n)+2^k}{2^{k+1}}}\right)^2 = a^{\frac{\phi(n)+2^k}{2^k}} = a \cdot a^{\frac{\phi(n)}{2^k}} = a.$$

Poslední rovnost platí protože podle předchozího tvrzení je $\frac{\phi(n)}{2^k}$ řád grupy $\mathbb{QR}_n$, a proto $a^{\frac{\phi(n)}{2^k}} = 1$ v $\mathbb{QR}_n$. Zbývá tedy ospravedlnit, že pravá strana je dobře definovaná, tj. ukázat, že $\frac{\phi(n)+2^k}{2^{k+1}}$ je celé číslo, tedy že $2^{k+1}|(\phi(n)+2^k)$.

$$\phi(n) = \frac{n}{p_1 p_2 \dots p_k}(p_1-1)(p_2-1)\dots(p_k-1),$$

kde p_i jsou prvočísla z rozkladu n. Zřejmě $2^k|(p_1-1)(p_2-1)\dots(p_k-1)$. Označme tedy $r = \frac{(p_1-1)(p_2-1)\dots(p_k-1)}{2^k}$, pak

$$\phi(n) + 2^k = \frac{n}{p_1 p_2 \dots p_k} \cdot r \cdot 2^k + 2^k = 2^k\left(\frac{n}{p_1 p_2 \dots p_k} \cdot r + 1\right).$$

Číslo r je liché(protože p_i je tvaru $4k_i + 3$ pro každé i, a proto $(p_i - 1)/2$ je liché), totéž platí i pro $\frac{n}{p_1 p_2 \dots p_k}$, proto poslední závorka v rovnosti je sudá. Tím je důsledek dokázán.

□

2.3 Cykličnost $\mathbb{QR}_n$

Pro účely třetí kapitoly budeme potřebovat odvodit podmínku, za které je grupa $\mathbb{QR}_n$ cyklická. To provedeme v této části.

Lemma 2.3.1 *Buď G konečná komutativní grupa a p prvočíslo. Pokud pro každé $g \in G$ platí $g^p = 1$, pak $|G| = p^k$ pro nějaké k přirozené.*

Důkaz : Budeme postupovat sporem. Ať existuje $n > 1$ nesoudělné s p takové, že $|G| = np^k$. Ukážeme, že pak nutně $n = 1$. To ukážeme indukcí podle k.

Nechť $k = 1$. Tedy $|G| = np$. Vezměme libovolný nejednotkový prvek g z G a označme $H = \langle g \rangle$ podgrupu generovanou tímto prvkem. Dle předpokladu je $|H| = p$. H je zřejmě normální, proto má smysl uvažovat faktorgrupu G/H. Je $|G/H||H| = |G|$, tedy $|G/H| = n$. Ale pro libovolné $hH \in G/H$ je $(hH)^p = h^pH = 1H = H$. Tedy G/H obsahuje prvky řádu p. To je ale spor s tím, že n a p jsou nesoudělná. Ať nyní $k > 1$. Opět označme $H = \langle g \rangle$ pro nějaký nejednotkový prvek z G. Pak $|G/H| = np^{k-1}$ a dle indukčního překpokladu je $n = 1$.

□

Lemma 2.3.2 *Buď G komutativní grupa taková, že $|G| = n = p_1 p_2 \dots p_k$ pro nějaká různá prvočísla. Pak G je cyklická.*

Důkaz : Pro každé $i \in \{1, 2, \dots, k\}$ označme $G_i = \{g \in G : g^{p_i} = 1\}$. Pak G_i je zřejmě podgrupa v G pro každé i. Označme $H = G_1 \times G_2 \times \dots \times G_k$. Ukážeme, že $G \simeq H$ a že G_i jsou netriviální. Pro $g \in G$ existují $\alpha_{1,g}, \alpha_{2,g}, \dots, \alpha_{k,g}$ tak, že $o(g) = p_1^{\alpha_{1,g}} p_2^{\alpha_{2,g}} \dots p_k^{\alpha_{k,g}}$, kde $o(g)$ je řád prvku g v G. Pro každé i a $g \in G$ položme $q_{i,g} = o(g)/p_i^{\alpha_{i,g}}$. Protože všechna q_i jsou nesoudělná, existují celá čísla $r_{1,g}, r_{2,g}, \dots, r_{k,g}$ taková, že $q_{1,g}r_{1,g} + q_{2,g}r_{2,g} + \dots + q_{k,g}r_{k,g} = 1$. Definujme homomorfismy

$$\begin{aligned} \phi : G &\longrightarrow H \\ g &\longmapsto (g^{r_{1,g}q_{1,g}}, g^{r_{2,g}q_{2,g}}, \dots, g^{r_{k,g}q_{k,g}}) \end{aligned}$$

$$\begin{aligned} \psi : H &\longrightarrow G \\ (g_1, g_2, \dots, g_k) &\longmapsto g_1 \cdot g_2 \cdot \dots \cdot g_k \end{aligned}$$

Pak pro $g \in G$ je

$$\psi(\phi(g)) = \prod_{i=1}^{k} g^{r_{i,g}q_{i,g}} = g^{q_{1,g}r_{1,g} + q_{2,g}r_{2,g} + \dots + q_{k,g}r_{k,g}} = g.$$

Protože $q_{1,g}r_{1,g} + q_{2,g}r_{2,g} + \dots + q_{k,g}r_{k,g} = 1$, je $q_{i,g}r_{i,g} \equiv 1 \mod p_i$ pro každé i.

Pokud nyní $(g_1, g_2, \dots, g_k) \in H$ a pokud označíme $g = g_1 \cdot g_2 \cdot \dots \cdot g_k$, dostáváme

$$\begin{aligned} \phi(\psi((g_1, g_2, \dots, g_k))) &= (g^{r_{1,g}q_{1,g}}, g^{r_{2,g}q_{2,g}}, \dots, g^{r_{k,g}q_{k,g}}) \\ &= (g_1^{r_{1,g}q_{1,g}}, g_2^{r_{2,g}q_{2,g}}, \dots, g_k^{r_{k,g}q_{k,g}}) \\ &= (g_1^{(r_{1,g}q_{1,g} \mod p_1)}, g_2^{(r_{2,g}q_{2,g} \mod p_2)}, \dots, g_k^{(r_{k,g}q_{k,g} \mod p_k)}) \\ &= (g_1, g_2, \dots, g_k). \end{aligned}$$

Druhá rovnost platí, neboť pro každé i, j takové, že $i \neq j$ platí $g_i^{r_{j,g}q_{j,g}} = 1$. U třetí rovnosti můžeme exponenty brát modulo p_i, neboť $g_i^{p_i} = 1$ dle definice G_i. Tedy $\psi\phi$ je identita na G a $\phi\psi$ je identita na H, proto $G \simeq H$. Pak $|G| = |H|$, a protože každá G_i má podle předchozího lemmatu velikost $p_i^{k_i}$ pro nějaké k_i, je $|G_i| = p_i$ pro každé i. Pro každé i tedy existuje $f_i \in G$ prvek řádu p_i. Pak $f = f_1 \cdot f_2 \cdot \dots \cdot f_k$ je prvek řádu n a tedy generátor grupy G. Proto G je cyklická.

□

Důsledek 2.3.3 *Buď n přirozené číslo složené z k faktorů. Pokud $\phi(n)/2^k$ neobsahuje ve svém prvočíselném rozkladu čtverec, pak je grupa $\mathbb{QR}_n$ cyklická a má právě*

$$\phi\left(\frac{\phi(n)}{2^k}\right)$$

generátorů.

Důkaz : Cykličnost plyne z předchozího lemmatu, neboť podle tvrzení 1.2.3 je $|\mathbb{QR}_n| = \phi(n)/2^k$. Protože každá konečná cyklická grupa je izomorfní grupě $(\mathbb{Z}_m, +)$ pro vhodné m, je

$$\left(\mathbb{QR}_n, \cdot\right) \simeq \left(\mathbb{Z}_{\frac{\phi(n)}{2^k}}, +\right).$$

Odtud snadno dostáváme počet generátorů $\mathbb{QR}_n$.

□

2.4 Jednoduchý šifrovací systém

V následující části ukážeme, že počítání odmocnin v grupě kvadratických zbytků bez znalosti rozkladu čísla n je obtížné. Už víme, že v určitých případech a se znalostí hodnoty $\phi(n)$ je počítání odmocnin snadné. Nyní konkrétně ukážeme, že bez znalosti prvočíselného rozkladu čísla n je výpočet odmocnin stejně obtížný jako faktorizace n, což je obecně pokládáno za obtížný problém. Na základě toho pak definujeme jednoduchý šifrovací systém s veřejným klíčem.

V této části budeme uvažovat n takové, že $n = pq$ kde p, q jsou prvočísla dávající zbytek 3 po dělení čtyřmi.

Definice 2.4.1 *Přirozené číslo n nazveme Blumovo, pokud existují p, q prvočísla taková, že $p \equiv 3 \mod 4$, $p \equiv 3 \mod 4$ a $n = pq$.*

Poznámka 2.4.2 *Blumova přirozená čísla jsou zřejmě 3-složená.*

Tvrzení 2.4.3 *Buď $n = pq$ Blumovo. Pro $a \in \mathbb{QR}_n$ je*

$$x = a^{\frac{(p-1)(q-1)+4}{8}} \mod n$$

jediná odmocnina z a ležící v $\mathbb{QR}_n$.

Důkaz : Jedná se jen o speciální případ důsledku 2.2.4.

□

Následuje tvrzení již zmíněné a dokázané v [2].

Tvrzení 2.4.4 *Nechť $n = pq$ je Blumovo přirozené číslo. Pokud existuje algoritmus A pro nalezení libovolné odmocniny z $m \in \mathbb{QR}_n$ potřebující $F(n)$ kroků, pak existuje algoritmus B který na vstupu n a po $2(F(n) + \log n)$ krocích spočítá čísla p, q.*

Důkaz : Algoritmus B sestrojíme následovně: Zvolíme náhodné číslo k, že $1 < k < n$. Pokud $NSD(n, k) \neq 1$, tak jsme vyhráli a máme faktor čísla n. To se ale v drtivé většině případů nestane. Ať tedy $NSD(n, k) = 1$. Položíme $m := k^2 \mod n$. Necháme pracovat algoritmus A na vstupu m, ten po $F(n)$ krocích vrátí l splňující $l^2 = m$. Různé odmocniny z m jsou podle lemmatu 2.2.2 právě 4. Protože k jsme na začátku zvolili náhodně, pravděpodobnost že $l = \pm k$ je $1/2$. Tedy s pravděpodobností $1/2$ se algoritmus B trefil do jedné z druhých dvou odmocnin. Tedy s pravděpodobností $1/2$ dostaneme

$$k \equiv l \mod p \quad \text{a zároveň} \quad k \equiv -l \mod q$$

nebo

$$k \equiv -l \mod p \quad \text{a zároveň} \quad k \equiv l \mod q.$$

V obou případech stačí spočítat $NSD(k - l, n)$ a dostaneme jeden z faktorů čísla n. Umíme tedy rozložit n s pravděpodobností $1/2$. Tedy abychom uspěli potřebujeme celou proceduru zopakovat průměrně dvakrát. Tedy algoritmus B definujeme jako dvakrát zopakovanou popsanou proceduru. Odtud dostáváme časovou složitost algoritmu B. Je to $2(F(n) + \log n)$ kroků, kde $F(n)$ je za opakování algoritmu A a $\log n$ je maximální počet kroků výpočtu $NSD(k - l, n)$ na konci.

□

Na základě dokázaného tedy můžeme definovat jednoduchý asymetrický šifrovací systém. Ten, kdo chce dešifrovat nebo podepisovat si zvolí dvě velká prvočísla p, q taková, že $n = pq$ je Blumovo. Veřejný klíč bude číslo n a soukromý klíč bude dvojice (p, q). Prostor otevřených i šifrových textů bude stejný, sice $\mathbb{QR}_n$. Pak šifrování $m \in \mathbb{QR}_n$ probíhá jako $E(m) = m^2 \mod n$ a dešifrování podle tvrzení 2.4.3 jako $D(c) = c^{\frac{(p-1)(q-1)+4}{8}} \mod n$ pro $c \in \mathbb{QR}_n$.

Při dešifrování však nastává drobný problém. Neexistuje totiž známý algoritmus, který rozliší kvadratické zbytky od nezbytků(problém známý jako Problém kvadratických zbytků). Tedy dešifrovací orákulum nemůže poznat, zda vstup, který dostalo k dešifrování je platný šifrový text.

Tento problém se však dá vyřešit definicí podobné grupy jako je grupa kvadratických zbytků. Budeme se jí věnovat v následující části.

2.5 Grupa znaménkových kvadratických zbytků

Grupa, kterou definujeme v této části je odvozená od grupy kvadratických zbytků, má většinu jejích vlastností a jestě jednu vlastnost navíc. Sice že existuje efektivní algoritmus, který dokáže rozhodnout, zda vstup ze $\mathbb{Z}_n^*$ je nebo není jejím prvkem. Následují definice již uvedené v [1].

Definice 2.5.1 *Buď n liché přirozené číslo. Pro $x \in \mathbb{Z}_n$ definujeme absolutní hodnotu jako absolutní hodnotu z čísla které odpvídá x pokud prvky $\mathbb{Z}_n$ reprezentujeme jako {-(n-1)/2,. . . ,0,. . . ,(n-1)/2)}.*

Příklad 2.5.2 *$5 \in \mathbb{Z}_7$, pětce při znaménkové reprezentaci odpovídá -2, tedy $|5| = 2$.*

Definice 2.5.3 *Buď n liché přirozené číslo. Pro G podgrupu grupy $\mathbb{Z}_n^*$ definujeme znaménkovou grupu jako $G^+ = \{|x| : x \in G\}$ s operací „absolutní hodnota ze součinu“. Tj. pokud operaci v G^+ označíme jako $\circ$, pak $x \circ y = |xy \mod n|$ pro $x, y \in G^+$.*

Lemma 2.5.4 *G^+ s definovanou operací je opravdu grupa.*

Důkaz : G^+ je podmnožina $\mathbb{Z}_n^*$, proto stačí ověřit existenci inverzních prvků a uzavřenost vzhledem k operaci $\circ$.

Ať $g, h \in G^+$, pak podle definice G^+ existují $g_0, h_0 \in G$ takové, že $|g_0| = g$ a $|h_0| = h$. Pak $g \circ h = |gh \mod n| = ||g_0||h_0| \mod n| = ||g_0 h_0| \mod n|$, a proto $g \circ h \in G^+$. Označme $f = |g_0^{-1}|$, kde g_0^{-1} je inverzní prvek ke g_0 v grupě G. Jistě

$f \in G^+$. Pak $g \circ f = |gf \mod n| = ||g_0||g_0^{-1}| \mod n| = 1$, tedy f je inverzní prvek ke g v G^+, a proto je G^+ grupou.

□

Lemma 2.5.5 *Buď G podgrupa $\mathbb{Z}_n^*$. Pokud $-1 \notin G$, pak $|G^+| = |G|$. Pokud $-1 \in G$, pak $|G^+| = |G|/2$.*

Důkaz : Pokud $-1 \notin G$, pak je homomorfismus

$$\begin{aligned} |\cdot| : G &\longrightarrow G^+ \\ x &\longmapsto |x| \end{aligned}$$

prostý. Proto $|G| = |G^+|$. Pokud naopak $-1 \in G$ pak homomorfismus $|\cdot|$ má jádro $\{-1, 1\}$, a proto $|G^+| = |G|/2$.

□

Grupa, kterou se budeme od této chvíle zabývat je $\mathbb{QR}_n^+$. Nazýváme ji grupou znaménkových kvadratických zbytků. Pro definici šifrovacího systém jako v [1] potřebujeme znát, za jakých podmínek je $\mathbb{QR}_n^+$ cyklická. K tomu poslouží následující lemma.

Lemma 2.5.6 *Je-li n 3-složené, je $|\mathbb{QR}_n^+| = |\mathbb{QR}_n|$.*

Důkaz : Protože n je 3-složené, platí $-1 \notin \mathbb{QR}_n$ a s použitím předchzího lemmatu je důkaz dokončen.

□

Jako důsledek posledního lemmatu tedy dostáváme, že i pro $\mathbb{QR}_n^+$ platí důsledek 2.3.3 se stejnými předpoklady.

Podmnožina $\mathbb{Z}_n^*$ tvořená prvky, které mají Jacobiho symbol 1 tvoří s operací násobení modulo n grupu. Tuto grupu budeme dále značit $\mathbb{J}_n$. Teď odvodíme jak velká je grupa $\mathbb{J}_n$ a z toho vyplyne jeden, pro pozdější účely důležitý fakt.

Lemma 2.5.7 *Buď $n \in \mathbb{N}$. Pak $|\mathbb{J}_n| = |\mathbb{Z}_n^*|/2$*

Důkaz : Ať $m \in \mathbb{Z}_n^* \setminus \mathbb{J}_n$. Protože $\mathbb{Z}_n^*$ je grupa, je zobrazení $\gamma : x \longmapsto mx$ automorfismem $\mathbb{Z}_n^*$. Ale pro každé $x \in \mathbb{Z}_n^* \setminus \mathbb{J}_n$ je $mx \in \mathbb{J}_n$ a naopak pro každé $y \in \mathbb{J}_n$ je $my \in \mathbb{Z}_n^* \setminus \mathbb{J}_n$. Proto je zobrazení γ bijekcí množin $\mathbb{J}_n$ a $\mathbb{Z}_n^* \setminus \mathbb{J}_n$, tedy $|\mathbb{J}_n \setminus \mathbb{Z}_n^*| = |\mathbb{J}_n|$. Proto $|\mathbb{J}_n| = |\mathbb{Z}_n^*|/2$

□

Lemma 2.5.8 *Pokud je $n = pq$ Blumovo, pak $\mathbb{QR}_n^+ = \mathbb{J}_n^+$*

Důkaz : Z definice Jacobiho symbolu a s použitím lemmatu 2.1.8 dostáváme, že $\mathbb{QR}_n \subseteq \mathbb{J}_n$. Tedy platí i $\mathbb{QR}_n^+ \subseteq \mathbb{J}_n^+$. Víme, že $|\mathbb{QR}_n^+| = |\mathbb{QR}_n| = (p-1)(q-1)/4$ a dle předchozího lemmatu je $|\mathbb{J}_n| = (p-1)(q-1)/2$. Protože ale $-1 \in \mathbb{J}_n$(neboť $-1 \notin \mathbb{QR}_p$ a zároveň $-1 \notin \mathbb{QR}_q$) je podle lemmatu 2.5.5 $|\mathbb{J}_n^+| = |\mathbb{J}_n|/2 = (p-1)(q-1)/4$. Dostali jsme tedy, že $\mathbb{QR}_n^+ \subseteq \mathbb{J}_n^+$ a $|\mathbb{J}_n^+| = |\mathbb{QR}_n^+|$. To však znamená, že $\mathbb{J}_n^+ = \mathbb{QR}_n^+$.

□

V posledním lemmatu je předpoklad, že n je Blumovo, opravdu nutný. Velikost $\mathbb{J}_n$ je totiž vždy $\phi(n)/2$, ale velikost $\mathbb{QR}_n$ záleží na počtu faktorů čísla n. Proto by pro obecné 3-složené n náš důkaz neprošel.

Nyní už tedy dokážeme efektivně rozeznávat prvky $\mathbb{QR}_n^+$ od prvků z $\mathbb{Z}_n^* \setminus \mathbb{QR}_n^+$. Protože $\mathbb{J}_n^+ = \mathbb{QR}_n^+$, stačí u prvku, kterému chceme dosvědčit členství v $\mathbb{QR}_n^+$, spočítat Jacobiho symbol (to lze efektivně počítat [3]) a pokud tento vyjde 1, pak daný prvek leží v $\mathbb{QR}_n^+$.

Kapitola 3

Hybrydní ElGamalův šifrovací systém

V této kapitole si konečně ukážeme, že grupa znaménkových kvadratických zbytků má skutečně nějaké praktické využití. Definujeme zde asymetrický šifrovací systém. Jedná se o hybridní ElGamalův šifrovací systém(HEG) [1] používající asymetrickou metodu pro zašifrování klíče, který se následně použije pro symetrickou šifru. A právě ona asymetrická metoda bude definována nad grupou znaménkových kvadratických zbytků.

Nejprve popíšeme schéma systému a potom dokážeme jeho bezpečnost za podmínky obtížnosti faktorizace.

3.1 Definice schématu

Jak už jsme zmínili výše, budeme pro definici schématu potřebovat symetrickou šifru. Pro bezpečnostní parametr k mějme tedy symetrickou šifru $SE = (E, D)$, kde E je šifrovací transformace šifrující zprávy z množiny $\mathcal{M}(k)$ pomocí klíčů z $\mathcal{K}(k)$. D je potom dešifrovací transformace inverzní k E. Tedy platí $D_K(E_K(m)) = m$ pro každé $m \in \mathcal{M}(k)$.

Dále ať $\mathcal{H}_k$ značí množinu hashovacích funkcí definovaných na $\mathbb{QR}_n^+ \times \mathbb{QR}_n^+$.

Dále definujeme generátor RSA modulu jako algoritmus RSAgen, který pro $0 \leq \delta < 1/2$, parametr k a pro funkci $n(k)$ vygeneruje trojici (n, p, q) takovou, že $n = pq$ je $n(k)$-bitové Blumovo přirozené číslo a faktory $\phi(n)/4$ jsou po dvou různá a aspoň $\delta n(k)$-bitová čísla. Podmínka, že faktory $\phi(n)/4$ jsou po dvou různé zajišťuje podle důsledku 2.3.3, že $\mathbb{QR}_n^+$ bude cyklická. Podmínka na velikost faktorů $\phi(n)/4$ zase říká, že generátorů $\mathbb{QR}_n^+$ je hodně. Konkrétně, že ná-

hodně zvolený prvek z $\mathbb{QR}_n^+$ je generátorem s pravděpodobností $1 - O(2^{-\delta n(k)})$ (to ukážeme později v lemmatu 3.3.1).

Nyní už můžeme definovat celé schéma.

- Generování klíče: Nejprve pomocí RSAgen(k) vygenerujeme (n, p, q). Náhodně zvolíme generátor g grupy $\mathbb{QR}_n^+$. Dále náhodně volíme $x \in \{1, 2, \ldots, (p-1)(q-1)/4\}$ a hashovací funkci $H \in \mathcal{H}_k$. Položíme $X = g^x \in \mathbb{QR}_n^+$. Pak veřejný klíč bude $pk = (n, g, X, H)$ a soukromý klíč $sk = (n, x, H)$.

- Šifrování: Ať m je zpráva, kterou chceme zašifrovat. Zvolíme náhodně $y \in \{1, 2, \ldots, \lceil n/4 \rceil\}$, položíme $Y = g^y$, $K = H(Y, X^y)$ a $\psi = E_K(m)$. Výsledný šifrový text bude $(Y, \psi) \in \mathbb{QR}_n^+ \times \{0,1\}^*$

- Dešifrování: Pokud jsme přijali šifrový text tvaru (Y, ψ), nejprve ověříme zda $Y \in \mathbb{QR}_n^+$. Pokud ano, spočítáme $K = H(Y, Y^x)$ a původní zprávu m dostaneme jako $D_K(\psi)$.

Jak už bylo zmíněno výše, velikost $\mathbb{QR}_n^+$ je $(p-1)(q-1)/4$. Proto by vypadalo rozumně volit při šifrování $y \in \{1, 2, \ldots, (p-1)(q-1)/4\}$, neboť pak by náhodná veličina Y měla rovnoměrné rozdělení. To by ovšem znamenalo, že hodnota $(p-1)(q-1)/4$ musí být veřejná, tedy bychom dávali útočníkovi k dispozici nějakou netriviální informaci o hodnotách p, q. A to právě nechceme. Proto je exponent y volen z množiny $\{1, 2, \ldots, \lceil n/4 \rceil\}$. Při tomto výběru tedy nemá Y přesně rovnoměrné rozdělelí, ale moc se od něj neliší, protože rozdíl hodnot $\lceil n/4 \rceil$ a $(p-1)(q-1)/4$ je vzhledem k velikosti n dost malý. Tím jsme tedy dosáhli toho, že hodnoty p, q se použijí pouze při generování klíčů, a pak už se v celém schématu nikde nevyskytují.

Při dešifrování se uplatňuje výhoda použití grupy znaménkových kvadratických zbytků oproti použití obyčejné grupy kvadratických zbytků. Pokud bychom totiž použily grupu kvadratických zbytků, pro ověření zda $Y \in \mathbb{QR}_n$ při dešifrování bychom potřebovali znát p a q. Když ale použijeme grupu znaménkových kvadratických zbytků, dokážeme podle závěru druhé kapitoly toto ověření efektivně provést i bez znalosti hodnot p, q, a tedy o nich neposkytujeme útočníkovi žádnou informaci.

3.2 Několik základních pojmů

Abychom mohli dokazovat bezpečnost systému, musíme nejprve upřesnit, jaký druh bezpečnosti chceme a čím bude bezpečnost schématu podmíněna. Proto

nyní definujeme dva matematické problémy a jednu metodu posuzování bezpečnosti kryptosystémů.

Definice 3.2.1 *Ať $f : \mathbb{N} \to \mathbb{R}$ je funkce. Řekneme, že f je zanedbatelná, pokud roste pomaleji než libovolný inverzní polynom. Tj. pro každé $c \in \mathbb{N}$ existuje $k_0 \in \mathbb{N}$ takové, že pro každé $k \geq k_0$ platí*

$$f(k) < \frac{1}{k^c}.$$

Efektivním útočníkem budeme v celém textu rozumět pravděpodobnostní algoritmus pracující v polynomiálním čase.

Definice 3.2.2 *Řekneme, že platí podmínka obtížnosti faktorizace vzhledem k RSAgen, pokud*

$$Adv^{fac}_{A,RSAgen}(k) = Pr[(p,q) \leftarrow A(n) : (n,p,q,) \leftarrow RSAgen(k)]$$

je zanedbatelná funkce pro každého efektivního útočníka A. Přičemž zápis na pravé straně značí pravděpodobnost, že algoritmus A na vstupu n spočítá (p,q) za podmínky, že trojice (n,p,q) byla vygenerována náhodně pomocí RSAgen definovaného v předchozí části.

Další podmínka, kterou budeme používat je tzv. *silný Diffie-Hellmanův předpoklad (SDH)*, který vychází ze známého Diffie-Hellmanova problému tj. pro g generátor grupy a pro dva náhodné prvky X, Y spočítat $DH_g(X,Y) = g^{(dlog_g X)(dlog_g Y)}$, kde $dlog_g$ značí diskrétní logaritmus o základu g. V silném Diffie-Hellmanově problému má útočník za úkol totéž, tedy spočítat $DH_g(X,Y)$, ale má navíc přístup k tzv. Diffie-Hellmanovu rozhodovacímu orákulu pro pevná g a X ($DDH_{g,X}$), to je definováno následovně: $DDH_{g,X}(\hat{Y},\hat{Z}) = 1$ pokud $\hat{Y}^{dlog_g X} = \hat{Z}$ a $DDH_{g,X}(\hat{Y},\hat{Z}) = 0$ jinak.

Definice 3.2.3 *Řekneme, že silný Diffie-Hellmanův předpoklad platí vzhledem k RSAgen, pokud*

$$Adv^{SDH}_{A,RSAgen}(k) = Pr\left[Z = DH_g(X,Y) : \begin{array}{l}(n,p,q) \leftarrow RSAgen(k)\\ g \leftarrow \mathbb{QR}^+_n,\ \text{že } g \text{ je generáror } \mathbb{QR}^+_n\\ X,Y \leftarrow \mathbb{QR}^+_n\\ Z \leftarrow A^{DDH_{g,X}}(n,g,X,Y)\end{array}\right]$$

je zanedbatelná funkce pro každého efektivního útočníka A. Přičemž pravá strana značí pravděpodobnost, že útočník A komunikující s orákulem $DDH_{g,X}$ spočte

správně $DH_g(X,Y)$ za předpokladu, že (n,p,q) jsme generovali náhodně pomocí RSAgen, generátor g jsme vybrali náhodně z množiny všech generátorů $\mathbb{QR}_n^+$ a X,Y byla zvolena také náhodně.

Nyní definujeme pojem bezpečnosti pro asymetrickou šifru. Mějme tedy asymetrickou šifru $PKE = (Kg, Enc, Dec)$ (PKE značí public key encryption), kde Kg pravděpodobnostní algoritmus pro generování dvojice klíčů (pk, sk). Enc je šifrovací algoritmus a Dec značí dešifrovací transformaci.

Definice 3.2.4 *Řekneme, že asymetrický systém PKE=(Kg,Enc,Dec) je IND-CCA(indistinguishability against chosen-ciphertext attack) bezpečný, pokud*

$$Adv^{CCA}_{PKE,A} = \left| Pr\left[\hat{b} = b : \begin{array}{l} (pk, sk) \leftarrow Kg(k) \\ (m_0, m_1, St) \leftarrow A_1^{Dec(sk,\cdot)}(pk) \\ b \leftarrow \{0,1\}, c := Enc(pk, m_b) \\ \hat{b} \leftarrow A_2^{Dec(sk,\cdot)}(c, St) \end{array}\right] - \frac{1}{2}\right|$$

je zanedbatelná funkce pro každého efektivního útočníka $A = (A_1, A_2)$. Přičemž navíc A_2 nesmí při komunikaci s $Dec(sk,\cdot)$ položit dotaz na dešifrování šifrového textu c.

Popsáno slovy to znamená, že žádný efektivní útočník, který si vybere dvě zprávy, nedokáže rozpoznat, která z nich byla zašifrována. A to i přesto, že má přístup k dešifrovacímu orákulu $Dec(sk,\cdot)$. Výskyt proměnné St v definici nám pouze říká, že algoritmy A_1 a A_2 spolu mohou komunikovat, tj. A_1 může předat algoritmu A_2 nějakou informaci o svých výpočtech. Analogicky definujeme IND-CCA bezpečnost symetrické šifry SE.

V důkazech bezpečnosti systémů, ve kterých se vyskytují hashovací funkce, nastává problém jak tyto funkce modelovat. My budeme pro jednoduchost používat model náhodného orákula. Náhodné orákulum je jakási dokonalá hashovací funkce, která splňuje následující vlastnosti:

- na různé vstupy dává různé výstupy
- na stejný vstup odpovídá vždy stejným výstupem
- při dotazu na vstup, na který jsme se jestě nezeptali dává výstup náhodně vybraný ze všech hodnot, které nejsou obrazem žádného dosud položeného dotazu

První podmínka říká, že je bezkolizní, druhá zajišťuje, že je to opravdu funkce a poslední hovoří o náhodnosti funkce.

3.3 Důkaz bezpečnosti v modelu náhodného orákula

Nyní už tedy můžeme přistoupit k samotnému důkazu bezpečnosti hybridního ElGamalova šifrovacího systému ve smyslu IND-CCA a to za předpokladu obtížnosti faktorizace. Nejprve ukážeme, že nad grupou znaménkových kvadratických zbytků je předpoklad obtížnosti faktorizace podmíněn platností silného Diffie-Hellmanova předpokladu[1]. A nakonec ukážeme, že IND-CCA bezpečnost zmiňovaného systému plyne z platnosti silného Diffie-Hellmanova předpokladu[1].

Lemma 3.3.1 *Mějme trojici (n, p, q) vygenerovanou pomocí $RSAgen(k)$. Pravděpodobnost, že náhodně vybraný prvek z $\mathbb{QR}_n^+$ je generátor této grupy je $1 - O(2^{-\delta n(k)})$.*

Důkaz : Podle definice RSAgen jsou faktory čísla $\phi(n)/4 = ((p-1)(q-1))/4$ po dvou různé a alespoň $\delta n(k)$-bitové. Označme tyto faktory $p_1, p_2, \ldots, p_c$ pro nějaké $c \in \mathbb{N}$. Ze spodního odhadu na velikost faktorů máme, že jejich počet je nejvýše $1/\delta$, tj. $c \leq 1/\delta$. Každé p_i je aspoň $\delta n(k)$-bitové, proto pro každé p_i platí, že $p_i \geq 2^{\delta n(k)-1}$. Odhadujme nyní pravděpdobnost, že náhodně vybraný prvek je generátor. Protože $\mathbb{QR}_n^+$ je cyklická, je počet jejích generátorů $\phi(|\mathbb{QR}_n^+|)$. Tedy pravděpodobnost, že náhodně vybraný prvek je generátorem je

$$\begin{aligned}
\frac{\phi(|\mathbb{QR}_n^+|)}{|\mathbb{QR}_n^+|} &= \frac{\phi(\frac{(p-1)(q-1)}{4})}{\frac{(p-1)(q-1)}{4}} = \frac{(p_1-1)(p_2-1)\ldots(p_c-1)}{p_1 p_2 \ldots p_c} = \prod_{i=1}^{c} \frac{p_i - 1}{p_i} \\
&= \prod_{i=1}^{c} 1 - \frac{1}{p_i} \geq \prod_{i=1}^{c} 1 - \frac{1}{2^{\delta n(k)-1}} = (1 - 2^{-\delta n(k)+1})^c \\
&\geq 1 - c \cdot 2^{-\delta n(k)+1} = 1 - 2 \cdot c \cdot 2^{-\delta n(k)} \geq 1 - \frac{2}{\delta} \cdot 2^{-\delta n(k)}
\end{aligned}$$

Předposlední nerovnost plyne z Bernoulliho nerovnosti($(1+x)^m \geq 1 + mx$ pro každé $m \in \mathbb{N}$ a $x \in (-1, \infty)$). $2/\delta$ už je konstanta nezávislá na k. Tím je lemma dokázáno.

□

Tvrzení 3.3.2 *Pokud platí předpoklad obtížnosti faktorizace vzhledem k RSAgen, pak nad grupou známénkových kvadratických zbytků modulo n platí i silný Diffie-Hellmanův předpoklad vzhledem k RSAgen. Přesněji: Pro každého útočníka A na*

silný Diffie-Helmanův problém existuje útočník B na problém faktorizace takový, že

$$Adv^{SDH}_{A,RSAgen}(k) \leq Adv^{fac}_{B,RSAgen} + O(2^{-\delta n(k)}).$$

Důkaz : Mějme tedy útočníka A na silný Diffie-Hellmanův problém. Sestrojíme útočníka B, který bude ve spolupráci s A řešit problém faktorizace s požadovanou pravděpodobností. Předpokládejme, že B dostal výzvu n. B bude postupovat následovně: Zvolí si náhodně u z množiny $(\mathbb{Z}^*_n)^+ \setminus \mathbb{QR}^+_n$ a položí $h = u^2$. Pak $h \in \mathbb{QR}^+_n$ a h je dle předchozího lemmatu generátorem $\mathbb{QR}^+_n$ s velkou pravděpodobností, konkrétně $1-O(2^{-\delta n(k)})$. Dále B zvolí náhodně $a, b \in \{1, 2, \ldots, \lceil n/4 \rceil\}$ a položí $g = h^2$, $X = hg^a$ a $Y = hg^b$. Z rovnosti $X = hg^a = g^{\frac{1}{2}}g^a$ dostáváme, že $dlog_g X = a + 1/2 \mod |\mathbb{QR}^+_n|$. Nyní B dá útočníkovi A výzvu (g,X,Y). A je ovšem útočník na silný Diffie-Hellmanův problém, proto B musí ještě zajistit rozhodovací Diffie-Hellmanovo orákulum. To ovšem sestrojí jednoduše, neboť

$$\hat{Y}^{dlog_g X} = \hat{Z} \Longleftrightarrow \hat{Y}^{2dlog_g X} = \hat{Z}^2 \Longleftrightarrow \hat{Y}^{2a+1} = \hat{Z}^2$$

První ekvivalence platí, neboť n je Blumovo, a proto je v $\mathbb{QR}^+_n$ mocnění na druhou bijekce (podle tvrzení 2.1.14 a důkazu lemmatu 2.5.5). Tedy B může sestrojit silné Diffie-Hellmanovo orákulum následovně:

$$DDH_{g,X}(\hat{Y}, \hat{Z}) = \begin{cases} 1 \text{ pokud } \hat{Y}^{2a+1} = \hat{Z}^2 \\ 0 \text{ jinak} \end{cases}$$

Útočník A má tedy přístup k sestrojenému orákulu a může pracovat na výzvě (g, X, Y). A s pravděpodobností $Adv^{SDH}_{A,RSAgen}(k)$ spočítá správně

$$Z = DH_g(X, Y) = g^{(dlog_g X)(dlog_g Y)} = g^{(a+1/2)(b+1/2)} = h^{2(a+1/2)(b+1/2)} = h^{2ab+a+b+1/2}$$

B však zná a i b, proto může spočítat $v = h^{1/2}$. Výpočet v provede násobením vhodnými prvky z $\mathbb{QR}^+_n$, proto $v \in \mathbb{QR}^+_n$. Protože ale u zvolené na začátku neleží v $\mathbb{QR}^+_n$, tak dostáváme dvě různé odmocniny z h modulo n. Nyní stačí, aby B spočítal $NSD(u - v, n)$ a dostává jeden z faktorů čísla n. Zbývá ukázat s jakou pravděpodobností útočník B uspěje. K neúspěchu dojde pouze v případech kdy u je zvoleno tak, že $h = u^2$ není genegátor $\mathbb{QR}^+_n$ nebo pokud A odpoví špatně. První případ nastává s pravděpodobností $O(2^{-\delta n(k)})$, proto

$$Adv^{fac}_{B,RSAgen} \geq Adv^{SDH}_{A,RSAgen}(k) - O(2^{-\delta n(k)}).$$

□

Tvrzení 3.3.3 *Pokud nad grupou znaménkových kvadratických zbytků platí silný Diffie-Hellmanův předpoklad vzhledem k RSAgen a pokud je symetrická šifra SE použitá v systému IND-CCA bezpečná, pak je i hybridní ElGamalův šifrovací systém IND-CCA bezpečný. Konkrétně platí, že pro každého útočníka A na IND-CCA bezpečnost hybridního ElGamalova systému existuje útočník B na silný Diffie-Hellmanův problém a útočník $\bar{B}$ na IND-CCA bezpečnost symetrické šifry SE tak, že*

$$Adv^{CCA}_{A,HEG} \leq Adv^{SDH}_{B,RSAgen}(k) + Adv^{CCA}_{\bar{B},SE}(k) + O(2^{-\delta n(k)})$$

.

Důkaz : Nechť $A = (A_1, A_2)$ je útočník na IND-CCA bezpečnost Hybridniho ElGamalova systému. Připomeňme původní experiment, pomocí kterého jsme definovali IND-CCA bezpečnost:

$$\left[\begin{array}{l} (pk, sk) \leftarrow Kg(k) \\ (m_0, m_1, St) \leftarrow A_1^{Dec(sk,\cdot)}(pk) \\ b \leftarrow \{0,1\}, c := Enc(pk, m_b) \\ \hat{b} \leftarrow A_2^{Dec(sk,\cdot)}(c, St) \end{array}\right]$$

V případě, o který se zajímáme (tj. případ hybridního ElGamalova systému), je $pk = (n, g, X, H)$, $sk = (n, x, H)$ a $c = (Y, \psi)$.

Nyní definujeme tři modifikace tohoto experimentu. Ať p_i značí pravděpodobnost, že v i-tém experimentu útočník A uspěl, tj. že $\hat{b} = b$.

- Experiment 1: První experiment bude přímo ten původní použitý pro definici IND-CCA bezpečnosti. Dle definice tedy platí

$$Adv^{CCA}_{A,HEG} = \left| p_1 - \frac{1}{2} \right| \tag{3.1}$$

- Experiment 2: V druhém experimentu změníme postup výpočtu šifrového textu $c = (Y, \psi)$ a postup zodpovídání dotazů na dešifrování v druhé části, tj. dešifrování dotazů od A_2. Zvolme náhodně nějaký symetrický klíč K. Ten použijeme k zašifrování příslušné zprávy m_b. Tedy $c = (Y, \psi)$, kde $\psi = E_K(m_b)$. Dotazy na dešifrovací orákulum v druhé části zodpovídáme následovně. Pokud se útočník zeptá na šifrový text tvaru (Y, ϕ) kde $\psi \neq \phi$, odpovíme textem dešifrovaným pomocí klíče K (namísto klíče $L = H(Y, Y^x)$, jak by tomu bylo v prvním experimentu). Pokud se útočník

ptá na jiné šifrové texty, odpovídáme stejně jako v prvním experimentu. Označme F událost, kdy útočník dá požadavek orákulu H na spočítání $H(Y, Y^x)$. Všiměme si, že dokud nenastane událost F, tak jde z pohledu útočníka o stejný experiment jako je ten první. Tedy

$$|p_1 - p_2| \leq Pr[F] \tag{3.2}$$

Nyní sestrojíme útočníka B na silný Diffie-Hellmanův problém jehož úspěšnost bude záviset na pravděpodobnosti události F. Předpokládejme, že B dostal výzvu (n, g, X, Y). B bude simulovat experiment 2 s veřejným klíčem $pk = (n, g, X, H)$ a šifrovým textem $c = (Y, \psi) = (Y, E_K(m_b))$ pro náhodně zvolený symetrický klíč K. B nezná tajný klíč $sk = (n, x, H)$, proto nemůže jednoduše odpovídat na dešifrovací dotazy útočníka A. Na dotaz $(\hat{Y}, \hat{\psi})$ tedy B odpoví následovně: Pokud už se někdy útočník A zeptal okákula H na hodnotu v $(\hat{Y}, \hat{Z})$ takovou, že $DDH_{g,X}(\hat{Y}, \hat{Z}) = 1$, tj. $\hat{Z} = \hat{Y}^x$, pak může B použít na dešifrování dotazu $(\hat{Y}, \hat{\psi})$ klíč $\hat{K} = H(\hat{Y}, \hat{Z})$. V opačném případě, tj. v případě, že A v minulosti neudělal na H žádný dotaz tvaru $(\hat{Y}, \hat{Z})$ kde $DDH_{g,X}(\hat{Y}, \hat{Z}) = 1$, pak hodnota $H(\hat{Y}, \hat{Y}^x)$ jestě nikde nebyla použita, a protože H modelujeme jako náhodné orákulum, tak tuto hodnotu může B zvolit libovolně. Dotaz tedy dešifruje pomocí náhodně zvoleného symetrického klíče $\bar{K} = H(\hat{Y}, \hat{Y}^x)$.

Pokud v tomto experimetnu někdy nastane událost F, tak to znamená, že A položil dotaz na hodnotu $H(Y, Z)$ kde $Z = Y^x$. B má k dispozici rozhodovací Diffie-Hellmanovo orákulum, proto tuto skutečnost zjistí. Jako odpověď na úvodní výzvu (n, g, X, Y) může tedy B vrátit hodnotu Z. Tedy vždy když nastane událost F, útočník B uspěje. Proto

$$Pr[F] \leq Adv^{SDH}_{B,RSAgen}(k) + O(2^{-\delta n(k)}), \tag{3.3}$$

kde korekční faktor $O(2^{-\delta n(k)})$ omezuje statistickou vzdálenost rozdělení náhodné veličiny Y v experimentu 1 a náhodné veličiny Y v silném Diffie-Hellmanově experimentu. Ty totiž nejsou stejně rozdělené. V SDH experimentu má Y rovnoměrné rozdělení, zatímco v experimentu 1(tj. v IND-CCA experimentu) nikoliv. Podrobné odvození tohoto členu uvedeme po dokončení důkazu tvrzení.

- Experiment 3: Poslední experiment dostaneme modifikací toho druhého. Celý experiment bude probíhat stejně, jen ve fázi, kdy máme zašifrovat zprávu m_b, tak vybereme náhodnou zprávu r stejné délky jako jsou m_0

a m_1 a tu zašifrujeme místo příslušného m_b. Označme G událost, že v některé fázi experimentu útočník A pozná, že jsme zprávu r vybrali náhodně. Pokud tedy G nenastane, tak je experiment 3 z pohledu útočníka A totožný s experimentem 2, proto

$$|p_2 - p_3| \leq Pr[G]$$

To ovšem znamená, že umíme sestrojit útočníka $\bar{B}$ na IND-CCA bezpečnost symetrické šifry SE takového, že

$$|p_2 - p_3| \leq Pr[G] \leq Adv^{CCA}_{\bar{B},SE}(k) \tag{3.4}$$

Protože $\psi = E_K(r)$, nezávisí šifrový text (Y, ψ) na hodnotě b. Proto útočník A nemá o příslušném otevřeném textu žádnou informaci, tedy pravděpodobnost jeho úspěchu v tomto experimentu je přesně $1/2$. Tj. $p_3 = 1/2$.

A na závěr zbývá už jen poskládat všechny dílčí nerovnosti 3.1, 3.2, 3.3 a 3.4 dohromady. Dostáváme

$$\begin{aligned} Adv^{CCA}_{A,HEG} &= \left|p_1 - \frac{1}{2}\right| \leq \left|p_1 - p_2 - \frac{1}{2} + p_2\right| \\ &\leq |p_1 - p_2| + |\frac{1}{2} - p_2| \leq Pr[F] + |p_3 - p_2| \\ &\leq Adv^{SDH}_{B,RSAgen}(k) + O(2^{-\delta n(k)}) + Adv^{CCA}_{\bar{B},SE}(k) \end{aligned}$$

□

Následuje slíbené odvození podoby korekčního faktoru z nerovnice 3.3 v důkazu předchozího tvrzení:

V tvrzení je útočník A na IND-CCA bezpečnost hybridního ElGamalova systému. V IND-CCA experimentu se Y nevolí podle rovnoměrného rozdělení, ale my útočníkovi A v experimentu 2 předáváme výzvu vybranou pro SDH experiment a tam se Y volí podle rovnoměrného rozdělení. Pravděpodobnost úspěchu útočníka A v simulaci experimentu 2 nebude tedy přesně $Adv^{CCA}_{A,HEG}$, ale bude o trochu jiná.

Nejdříve se podívejme jaké rozdělení má Y v IND-CCA experimentu. Y získáme tak, že zvolíme náhodně $y \in \{1, 2, \ldots, \lceil n/4 \rceil\}$ a pak položíme $Y = g^y$, kde g je generátor $\mathbb{QR}^+_n$. Velikost $\mathbb{QR}^+_n$ je $(p-1)(q-1)/4$, to je o trochu menší než $n/4$, proto se nám $\mathbb{QR}^+_n$ rozdělí na dvě skupiny prvků. Prvky v první skupině jsou vybrány s pravděpodobností $4/n$, zatímco prvky druhé skupiny jsou

vybrány s pravděpodobností dvojnásobnou, tedy $8/n$. Druhá skupina bude mít $n/4 - (p-1)(q-1)/4 = (p+q-1)/4$ prvků, tedy na první skupinu zbývá $(p-1)(q-1)/4 - (p+q-1)/4 = (n-2p-2q+2)/4$ prvků. A je pravděpodobnostní algoritmus, proto může na stejném vstupu jednou uspět a podruhé ne. Označme si prvky $\mathbb{QR}_n^+$ jako $\{a_1, a_2, \ldots, a_{(p-1)(q-1)/4}\}$ a označme q_i pravděpodobnost, že algoritmus A na vstupu a_i uspěje. V případě, že vybíráme Y podle rovnoměrného rozdělení, spočteme celkovou pravděpodobnost úspěchu útočníka A jako

$$\sum_{i=1}^{(p-1)(q-1)/4} \frac{4}{(p-1)(q-1)} \cdot q_i = \frac{4}{(p-1)(q-1)} \sum_{i=1}^{(p-1)(q-1)/4} q_i, \tag{3.5}$$

kde $4/((p-1)(q-1))$ je pravděpodobnost výběru jednotlivých prvků při rovnoměrném rozdělení. Pokud vybíráme podle druhého rozdělení, je pravděpodobnost úspěchu

$$\sum_{i=1}^{(n-2p-2q+2)/4} \frac{4}{n} \cdot q_i + \sum_{i=((n-2p-2q+2)/4)+1}^{(p-1)(q-1)/4} \frac{8}{n} \cdot q_i, \tag{3.6}$$

přičemž tiše předpokládáme, že prvky $\{a_1, a_2, \ldots, a_{(n-2p-2q+2)/4}\}$ tvoří zmiňovanou první skupinu a zbylé prvky tvoří skupinu druhou. Naším cílem je odhadnout, o kolik se pravděpodobnosti 3.5 a 3.6 liší. Počítejme tedy:

$$\begin{aligned}
&\left| \frac{4}{(p-1)(q-1)} \sum_{i=1}^{(p-1)(q-1)/4} q_i - \sum_{i=1}^{(n-2p-2q+2)/4} \frac{4}{n} \cdot q_i - \sum_{i=((n-2p-2q+2)/4)+1}^{(p-1)(q-1)/4} \frac{8}{n} \cdot q_i \right| \\
\leq\ & \left(\frac{4}{(p-1)(q-1)} - \frac{4}{n} \right) \sum_{i=1}^{(n-2p-2q+2)/4} q_i + \\
+\ & \left(\frac{8}{n} - \frac{4}{(p-1)(q-1)} \right) \sum_{i=((n-2p-2q+2)/4)+1}^{(p-1)(q-1)/4} q_i \\
\leq\ & \left(\frac{4}{(p-1)(q-1)} - \frac{4}{n} \right) \frac{n-2p-2q+2}{4} + \left(\frac{8}{n} - \frac{4}{(p-1)(q-1)} \right) \frac{p+q-1}{4}
\end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{n-2p-2q+2}{(p-1)(q-1)} - \frac{n-2p-2q+2}{n}\right) + \left(\frac{2p+2q-2}{n} - \frac{p+q-1}{(p-1)(q-1)}\right) \\
&= \left(\frac{n-2p-2q+2}{n-p-q+1} - \frac{n-2p-2q+2}{n}\right) + \left(\frac{2p+2q-2}{n} - \frac{p+q-1}{n-p-q+1}\right) \\
&= \left(1 - \frac{p+q-1}{n-p-q+1} - 1 + \frac{2p+2q-2}{n}\right) + \left(\frac{2p+2q-2}{n} - \frac{p+q-1}{n-p-q+1}\right) \\
&= \frac{4p+4q-4}{n} - \frac{2p+2q-2}{n-p-q+1} \leq \frac{4p+4q-4}{n} - \frac{2p+2q-2}{n} \\
&= \frac{2p+2q-2}{n} \leq \frac{2p+2q}{n} = 2 \cdot \frac{p+q}{n}.
\end{aligned}
$$

n je $n(k)$-bitové číslo a p, q mají obě $n(k)/2$ bitů, proto

$$2 \cdot \frac{p+q}{n} \leq 2 \cdot \frac{2^{n(k)/2} + 2^{n(k)/2}}{2^{n(k)-1}} = 8 \cdot \frac{2^{n(k)/2}}{2^{n(k)}} = 8 \cdot 2^{-n(k)/2} \leq 8 \cdot 2^{-\delta n(k)}.$$

Tím jsme tedy odvodili podobu korekčního faktoru v nerovnosti 3.3.

Závěrem: Spojením posledních dvou tvrzení jsme tedy ukázali, že IND-CCA bezpečnost hybridního ElGamalova systému nad grupou znaménkových kvadratických zbytků plyne z předpokladu obtížnosti faktorizace vzhledem k definovanému RSAgen, což je obecně považováno za obtížný problém.

Literatura

[1] Dennis Hofheinz, Eike Kiltz: *The Group of Signed Quadratic Residues and Applications*, IACR CRYPTO 2009, 637–653 LNCS 5677 (2009).

[2] Rabin M. O.: *Digitalized signatures and public-key functions as intractable as factorization*, TM-212, Laboratory of Computer Science, MIT, 1979.

[3] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone : *Handbook of Applied Cryptography*, CRC Press, říjen 1996, strana 73.