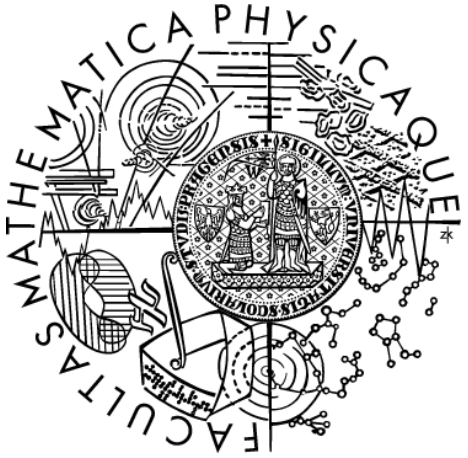
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Adolf Středa

MQ Problém

Katedra algebry

Vedoucí bakalářské práce:	Mgr. et Mgr. Jan Žemlička, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2016

Chtěl bych poděkovat svému vedoucímu bakalářské práce Mgr. et Mgr. Janu Žemličkovi, Ph.D., nejen za odborné vedení a cenné rady, ale také za trpělivost a dobře kladené dotazy, které mi umožnily v několika ohledech získat nový náhled na věc.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: MQ Problém

Autor: Adolf Středa

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. et Mgr. Jan Žemlička, Ph.D. Katedra algebry

Abstrakt: Cílem této bakalářské práce je popsat obecný MQ problém, především jeho variantu zvanou HFE, nastínit některé útoky na základní schéma založené na HFE a následně popsat nový útok na HFEz, systém vzniklý modifikací HFE, kdy se část výstupů z úvodní transformace opomene. Modifikace HFEz zajistí závislost vstupu do HFE polynomu na větším množství proměnných při zachování velikosti rozšíření tělesa. Útok na tuto modifikaci spočívá v překladu HFEz na HFE s větvením a následné aplikaci algoritmu pro separaci jednotlivých větví navrženého v [Fel06]. Separační algoritmus přes veřejný klíč vytvoří operaci, která společně se sčítáním tvoří komutativní, neasociativní algebru. Následně se aplikací několika poznatků o neasociativních algebrách za pomoci této operace spočte matice, která umožní separovat proměnné do několika sad odpovídajících jednotlivým větvím. Díky tomuto převodu můžeme následně provést útok přímo na HFE polynom neovlivněného modifikací HFEz.

Klíčová slova: MQ problém, HFE, post-kvantová kryptografie

Title: MQ Problem

Author: Adolf Středa

Department: Department Department of Algebra

Supervisor: Mgr. et Mgr. Jan Žemlička, Ph.D. Department of Algebra

Abstract: The aim of this thesis is to describe a general MQ Problem with a focus on its variant called HFE, outline several attacks on a basic scheme based on HFE and describe a new attack on HFEz, a cryptosystem based on special polynomials over finite fields with a modification, which discards a portion of the output from the initial transformation. This ensures a dependency on more variables while keeping the same size of the field. The attack starts with a translation of HFE into HFE with branches, followed by a branch separating algorithm described in [Fel06]. The separation algorithm uses the public key to derive an operation, which induces (with addition) a non-associative algebra. Utilising some properties of non-associative algebras, a matrix, which can separate variables into distinct sets according to branches, is calculated. This leads to stripping off the HFEz modification and thus allowing us to attack directly the HFE polynomial.

Keywords: MQ Problem, HFE, post-quantum cryptography

Obsah

1 Úvod

S pokrokem v oblasti kvantových počítačů je otázka post-kvantové kryptografie stále palčivější, jelikož značná část schémat pro asymetrickou kryptografii je založena na problému kvadratického rezidua, problému faktorizace anebo problému diskrétního logaritmu. Například přímou hrozbou pro RSA z oblasti kvantových počítačů je známý Shorův algoritmus [Sho97] pro faktorizaci čísel, který by měl být schopen proběhnout v polynomiálním čase.

Tuto problematiku se snažila řešit různá schémata založená na tzv. $\mathcal{MQ}$-problému – problému založeném na řešení kvadratických rovnic o více proměnných nad konečnými tělesy. Bohužel se postupně ukázalo, že mnohá navržená schémata jsou příliš snadno prolomitelná. Proto byly představeny modifikace původních schémat, které měly zvýšit odolnost schémat. Tato práce se zaměřuje na schémata s HFE trapdoorem (z anglického „Hidden Field Equations“) a jeho modifikace navržené v [Wol02], konkrétně HFEz a HFEm, s cílem se navrhnout nový potenciální algoritmus pro řešení systému s modifikací HFEz.

Prvně si v této sekci zadefinujeme základní pojmy pro práci s tělesy a transformacemi, které jsou pro $\mathcal{MQ}$-problém klíčové, abychom následně v další sekci mohli zadefinovat $\mathcal{MQ}$-problém a podívat se na HFE a některé jeho vlastnosti. Ve třetí sekci na tyto vlastnosti navážeme, abychom mohli popsat některé útoky na základní HFE schéma. Poté již budeme mít k dispozici potřebnou teorii pro modifikace, resp. útoky na ně, a provedeme útok na HFEz skrze útok na větvení popsaný v [Fel06]. Poslední sekci uzavřeme diskuzí nad několika zajímavými otevřenými problémy, které se v průběhu útoku objevují.

Při popisu HFE, modifikace HFEz a útoku na HFEz budou postupy ukázány na jednoduchých příkladech. Příklady byly vygenerovány v programu Wolfram Mathematica 10.2, zdrojový kód skriptu pro generování použitých příkladů je zveřejněn na `http://adolf.streda.matfyz.cz/MQ/example_gen.nb`. Z prostorových důvodů zde dojde k rozchodu v konvenci – napříč prací budeme pracovat s řádkovými vektory, nicméně právě u příkladů bude z důvodů prostorových vhodnější uvažovat vektory sloupcové.

1.1 Konečná tělesa

Konečná tělesa jsou základním stavebním kamenem pro schémata založená na MQ Problému, proto by bylo příhodné začít s jejich definicí a provést několik základních pozorování o jejich vlastnostech. Ještě než si připomeneme definici tělesa, bude užitečné si pro další použití připomenout i definici grupy:

Definice. *Nechť G je množina o $q \in \mathbb{N}$ prvcích a máme operaci $\cdot : G \times G \to G$. Pak $(\mathbb{G}, \cdot)$ nazveme grupou, jestliže platí následující vlastnosti:*

- *Asociativita:* $\forall a,b,c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- *Existence neutrálního prvku:* $\exists e \in G \, \forall a \in G : a \cdot e = a = e \cdot a$
- *Existence inverzního prvku:* $\forall a \in G \, \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$;

Pokud navíc platí v této grupě komutativita, $\forall a,b \in G : a \cdot b = b \cdot a$, pak takovouto grupu nazveme abelovskou grupou.

Definice. *Nechť $\mathbb{F}$ je neprázdná množina o alespoň dvou prvcích, na které máme dvě operace: sčítání $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ a násobení $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$. Pak $(\mathbb{F}, \cdot, +)$ nazveme (konečným) tělesem, jestliže $(\mathbb{F}, +)$ a $(\mathbb{F}\backslash\{0\}, \cdot)$ jsou abelovské grupy a platí distributivita: $\forall a,b,c \in \mathbb{F} : (a + b) \cdot c = a \cdot c + b \cdot c$.*

Definice. *Nechť $\mathbb{F}$ je těleso a $p \in \mathbb{F}[x]$ ireducibilní polynom stupně $n \in \mathbb{N}$ a (p) buď ideál jím generovaný v $\mathbb{F}[x]$. Pak $\mathbb{E} := \mathbb{F}[x]/(p)$ nazveme (algebraickým) rozšířením tělesa $\mathbb{F}$ stupně n, značíme $\mathbb{F} \leq \mathbb{E}$.*

Poznámka. *Nechť $\mathbb{F} \leq \mathbb{E}$ je rozšíření těles stupně $n \in \mathbb{N}$, pak nosič $\mathbb{E}$ spolu s operací sčítání a násobením prvkem z $\mathbb{F}$ je isomorfní vektorovému prostoru $\mathbb{F}^n$, označme ho jako $\mathbb{E}_{\mathbb{F}}$.*

Na ireducibilní polynomy v tělese můžeme pohlížet ještě jiným způsobem skrze jejich kořeny:

Definice. *Nechť $\mathbb{F} \leq \mathbb{E}$ je rozšíření těles, pak pro $a \in \mathbb{E}$ nazveme $m_{a,\mathbb{F}} \in \mathbb{F}[x]$ minimálním polynomem prvku a nad $\mathbb{F}$, jestliže $m_{a,\mathbb{F}}$ je monický, $m_{a,\mathbb{F}}(a) = 0$ a $\forall f \in \mathbb{F}[x] : f(a) = 0 \Rightarrow m_{a,\mathbb{F}} | f$ (tj. z hlediska dělitelnosti je minimální takový).*

Povšimněme si, že minimální polynom musí být vždy ireducibilní. Nejen proto jsou užitečným nástrojem nejen při odvozování nových těles a navíc nám umožní dát přímočaře do vztahu rozšíření tělesa $\mathbb{F}$ stupně $n \in \mathbb{N}$ a odvozeného vektorového prostoru $\mathbb{F}^n$.

Lemma 1.1. *Nechť $\mathbb{E} = \mathbb{F}[x]/(p)$, $p \in \mathbb{F}[x]$ nekonstantní ireducibilní polynom, je rozšíření těles stupně $n \in \mathbb{N}$. Pak existuje $a \in \mathbb{E}$ takové, že $p(a) = 0$ a $(1, a, \ldots, a^{n-1})$ tvoří bázi vektorového prostoru $\mathbb{E}_{\mathbb{F}}$.*

Důkaz: Buď $p(x) = k \sum_{i=0}^{n} t_i x^i, t_i, k \in \mathbb{F}$ a vezměme prvek $a \in \mathbb{E} : a = x + (p)$ & $p \| m_{a,\mathbb{F}}$. Bez újmy na obecnosti uvažme $p = m_{a,\mathbb{F}}$. Pak $\sum_{i=0}^{n} t_i a^i = 0$. Pokud by $(1, a, \ldots, a^{n-1})$ byly v $\mathbb{E}_{\mathbb{F}}$ lineárně závislé, pak existují $u_i \in \mathbb{F}$ takové, že $\sum_{i=0}^{n-1} u_i a^i = 0$, nicméně to by znamenalo, že $m_{a,\mathbb{F}}$ není minimální, a tedy dostáváme spor.

❑

Důsledek 1.2. *Nechť $\mathbb{E} = \mathbb{F}[x]/(p)$, $p \in \mathbb{F}[x]$ nekonstantní ireducibilní polynom, je rozšíření těles, pak $deg(p) = dim\mathbb{E}_{\mathbb{F}}$.*

Díky tomuto lemmatu navíc přirozeně dostaneme tzv. kanonickou bijekci. Kanonická bijekce je klíčové zobrazení, které nám umožní propojit ve schématu těleso se svým rozšíření, což se bude velmi užitečná vlastnost pro následující kapitoly.

Definice. *Zobrazení $\psi : \mathbb{E} \to \mathbb{F}^n$ pro $\mathbb{E} = \mathbb{F}[x]/(m_{a,\mathbb{F}})$, kde $m_{a,\mathbb{F}}$ je minimální polynom prvku $a \in \mathbb{E}$ nad tělesem $\mathbb{F}$, nazveme kanonickou bijekcí, jestliže toto zobrazení zobrazí libovolný prvek $x \in \mathbb{E}$ na jeho souřadnice vůči bázi $(1, a, \ldots, a^{n-1})$ vektorového prostoru $\mathbb{E}_{\mathbb{F}}$.*

Pozorování 1.3. *Kanonická bijekce je izomorfismus algeber $\mathbb{E}_{\mathbb{F}}$ a $\mathbb{E}$ se sčítáním definovaným jako ve vektorovém prostoru, resp. v tělese.*

Pozorování 1.4. *(Frobeniův automorfismus)*
Nechť $\mathbb{F}_q$ je těleso o q prvcích, pak zobrazení $\varphi : a \mapsto: a^{char\mathbb{F}_q}$, $a \in \mathbb{F}_q$, je automorfismus.

Povšimněme si jednoho zajímavého důsledku: mocnění na charakteristiku tělesa zachovává strukturu podtěles, tj. vzor i obraz leží ve stejném podtělese.

1.2 Afinní transformace

Afinní transformace hrají klíčovou roli v budování schémat pro asymetrickou kryptografii založených na $\mathcal{MQ}$ problému – hrají úlohu v tzv. trapdooru, což je nutná podmínka pro vybudování efektivní asymetrické kryptografie nad $\mathcal{MQ}$ problémem. Právě použité afinní transformaci umožní skrýt jednoduše invertovatelný polynom a převést problematiku jeho invertování na úroveň NP-úplného problému.

Definice. *Nechť $n \in \mathbb{N}$, $\mathbb{F}$ je těleso, $\vec{v} \in \mathbb{F}^n$ a $f : \mathbb{F}^n \mapsto \mathbb{F}^n$ je lineární bijektivní zobrazení. Pak zobrazení $g(\vec{x}) := \vec{v} + f(\vec{x})$, $x \in \mathbb{F}^n$, nazýváme afinní transformací.*

Definice. *Nechť $n \in \mathbb{N}$, $\mathbb{F}$ je těleso, $A \in \mathbb{F}^{n\times n}$ a $\vec{v} \in \mathbb{F}^n$. Pak $S(\vec{x}) = A\vec{x} + \vec{v}$, $x \in \mathbb{F}^n$, nazýváme maticovou reprezentací afinní transformace.*

Definice. *Nechť $n \in \mathbb{N}$ a $\mathbb{F}$ je těleso. Pak, definujeme-li $f_i(\vec{x}) := \sum_{j=0}^{n-1} \alpha_{i,j}x_j + \alpha_i$ pro $\alpha_{i,j}, \alpha_i \in \mathbb{F}$, $i = 0, \ldots, n-1$, nazýváme $f(\vec{x}) = (f_0(\vec{x}), \ldots, f_{n-1}(\vec{x}))$ reprezentací afinní transformace pomocí polynomů více proměnných.*

Pozorování 1.5. *Z definice násobení matic a sčítání vektorů ve vektorovém prostoru zřejmě vyplývá, že $\alpha_{i,j} = (A)_{i,j}$ a $\vec{v} = (\alpha_0, \ldots, \alpha_{m-1})^\top$, tj. reprezentace polynomy o více proměnných je jen formální rozpis maticové reprezentace.*

Lemma 1.6. *Afinní transformace z $\mathbb{F}^n$ do $\mathbb{F}^n$, pro $\mathbb{F}$ těleso a $n \in \mathbb{N}$, tvoří s operací skládání grupu. Tuto grupu označme $Aff(\mathbb{F}^n)$.*

Důkaz: Díky Pozorování 1.5 uvažme bez újmy na obecnosti transformace v maticové reprezentaci.

Neutrálním prvkem grupy je identita. Máme-li afinní transformaci v maticové reprezentaci $S(\vec{x}) = A\vec{x} + \vec{v}$, pak jejím inverzním prvkem je $A^{-1}(\vec{x} - \vec{v}) = A^{-1}\vec{x} - A^{-1}\vec{v}$, což je opět afinní transformace složená z lineárního zobrazení definovaného maticí A^{-1} a vektoru $A^{-1}\vec{v}$. Analogicky uzavřenost na skládání: $(g \circ f)(\vec{x}) = B(A\vec{x} + \vec{v_1}) + \vec{v_2} = BA\vec{x} + (B\vec{v_1} + \vec{v_2})$.

❑

Pokud dáme do souvislosti lineárně algebraické reprezentace afinních transformací a rozšíření těles, pak dostaneme další reprezentaci. Nová reprezentace vychází z bijekce mezi rozšířením těles a vektorovým prostorem odpovídající dimenze nad rozšiřovaným tělesem. Právě zde se nám bude hodit kanonická bijekce z předchozí kapitoly.

Definice. *Nechť $\mathbb{F}_p \leq \mathbb{F}_{p^n}$, $n \in \mathbb{N}$, je rozšíření těles, pak pro $X \in \mathbb{F}_{p^n}$ polynom $P(X) = \sum_{i=0}^{n-1} A_i X^{p^i} + A$, $A_i, A \in \mathbb{F}_{p^n}$ nazveme afinní transformací reprezentovanou polynomem o jedné proměnné.*

Lemma 1.7. *Každé afinní transformaci v maticové reprezentaci nad $\mathbb{F}_q^n$ odpovídá právě jeden polynom jedné proměnné tvaru $P(X) = \sum_{i=0}^{n-1} A_i X^{q^i} + A$, $A_i, A, X \in \mathbb{F}_{q^n}$, $0 \leq i < n$, tj. je-li ψ kanonická bijekce, pak pro všechny $L \in Aff(\mathbb{F}_q^n)$ existují koeficienty $A_i, A \in \mathbb{F}_{q^n}$ určující P takové, že $\forall X \in \mathbb{F}_{q^n} : \psi P(X) = L(\psi(X))$*

Důkaz: Bez újmy na obecnosti uvažujme lineární transformaci – díky kanonické bijekci můžeme translační složku afinní transformace převést samostatně.

Zřejmě tato transformace je lineárním zobrazením nad $\mathbb{F}_q^n$ a podobně je i polynom $\sum_{i=0}^{n-1} A_i X^{q^i}$ určuje lineární zobrazením nad $\mathbb{F}_{q^n}$. Navíc díky kanonické bijekci máme jednoznačnou korespondenci mezi prvky $\mathbb{F}_q^n$ a $\mathbb{F}_{q^n}$.

Nyní se pokusíme spočítat počty lineárních zobrazení nad $\mathbb{F}_q^n$ a lineárních zobrazení nad $\mathbb{F}_{q^n}$. V prvním případě počet lineárních zobrazení odpovídá počtu matic nad daným tělesem, tj. $q^{n \cdot n} = q^{n^2}$. V druhém případě máme q^n možností jak zvolit koeficient u jednoho monočlenu, tj. celkem $(q^n)^n = q^{n^2}$ možností jak zvolit koeficienty v celém polynomu. Každé dva takovéto polynomy nad $\mathbb{F}_{q^n}$ reprezentují jiné zobrazení, jinak jejich rozdíl by měl q^n kořenů při stupni nižším jak q^n. Tímto početním argumentem dostáváme vzájemně jednoznačnou korespondenci mezi těmito množinami zobrazení, a tedy i transformacemi.

❑

Tento důkaz je spíše technický, bylo by možné sestrojit i konstruktivní variantu s využitím algoritmu pro tento převod – interpolací polynomů o více proměnných popsanou například v [MI88]. Nicméně, jelikož toto lemma v této práci použijeme jen pro technickou nadstavbu tohoto lemmatu pro kvadratické polynomy více proměnných, pak postačí i tato nekonstruktivní varianta.

Toto lemma je velmi užitečné v několika ohledech. Nejenže dává přímou korespondenci mezi afinními zobrazeními, ale navíc v kombinaci s vlastnostmi faktorových okruhů umožní najít podobnou korespondenci i u jedné skupiny nelineárních zobrazení. Právě díky tomuto přechodu můžeme využít specifika rozšíření těles u této skupiny zobrazení, ale zároveň můžeme do jisté míry aplikovat nástroje pro práci s vektorovými prostory anebo polynomy o více proměnných.

2 MQ problém

Nyní můžeme konečně popsat obecné schéma založené na problému řešení soustavy kvadratických rovnic více proměnných nad konečnými tělesy. Nechť tedy máme systém $m \in \mathbb{N}$ rovnic o $n \in \mathbb{N}$ neznámých nad tělesem $\mathbb{F}$. Pak uvažme polynomy

$$p_1(x_0, \ldots, x_{n-1}) = \sum_{(i,j)\in\mathbb{Z}_n^2} \alpha_{1,i,j} x_i x_j + \sum_{i=0}^{n-1} \beta_{1,i} x_i + \gamma_1$$

$$p_2(x_0, \ldots, x_{n-1}) = \sum_{(i,j)\in\mathbb{Z}_n^2} \alpha_{2,i,j} x_i x_j + \sum_{i=0}^{n-1} \beta_{2,i} x_i + \gamma_2$$

$$\vdots$$

$$p_m(x_0, \ldots, x_{n-1}) = \sum_{(i,j)\in\mathbb{Z}_n^2} \alpha_{m,i,j} x_i x_j + \sum_{i=0}^{n-1} \beta_{m,i} x_i + \gamma_m$$

$$\alpha_{k,i,j},\ \beta_{k,j},\ \gamma_k \in \mathbb{F} \text{ pro } 0 \leq i, j \leq n \text{ a } 0 \leq k \leq m$$

Množinu všech takovýchto možných polynomiálních vektorů $(p_1, p_2, \ldots, p_m)$ označme $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$, resp. pro případ $m = n$ zkráceně $\mathcal{MQ}(\mathbb{F}^n)$.

Uvážíme-li rovnice odvozené z těchto polynomiálních vektorů

$$y_1 = p_1(x_0, \ldots, x_{n-1})$$
$$y_2 = p_2(x_0, \ldots, x_{n-1})$$
$$\vdots$$
$$y_m = p_m(x_0, \ldots, x_{n-1})$$

pak obecně najít vyhovující $x_0, x_2, \ldots, x_{n-1}$ pro zadaná $y_1, y_2, \ldots, y_n$ je dokonce NP-úplný problém (viz str. 33 [Wol02]) – nazvěme ho $\mathcal{MQ}$ problém (dle anglického Multivariate Quadratic). Nicméně to by bylo pro vybudování asymetrické kryptografie nedostačující – potřebujeme ještě tzv. trapdoor, který nám s dodatečnou informací umožní tyto vzory spočítat ideálně v polynomiálním čase. K tomuto poslouží afinní transformace z předchozí sekce. Vezměme si trojici funkcí $(S,\mathcal{P}',T) \in \mathrm{Aff}(\mathbb{F}^n) \times \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m) \times \mathrm{Aff}(\mathbb{F}^m)$, kde $\mathcal{P}'$ je speciálně konstruovaný polynomiální vektor, aby ho bylo možné výpočetně efektivně invertovat pro konkrétní vstup. Pak trojice $(S,\mathcal{P}',T)$ bude tvořit privátní klíč a $\mathcal{P} = T \circ \mathcal{P}' \circ S$ bude příslušný veřejný klíč. Konkrétní význam „efektivního invertování“ záleží na použitém schématu, pro tento popis se zatím spokojme s intuitivní představou – tj, že dokážeme invertovat polynom řádově efektivněji než-li útočník řešící soustavu bez těchto dodatečných informací. Jedním z možných způsobů, jak takovýto trapdoor zkonstruovat je například HFE.

2.1 Hidden Field Equations (HFE)

HFE vzniklo jako zobecnění MIA (taktéž známé jako Matsumoto-Imai Schema A nebo C* pro variantu s větvením), které uvažovalo speciálně volený monočlen nad nadtělesem. HFE uvažuje navíc i součty monočlenů definovaných v MIA. Formálně definujme polynomiální vektor HFE-tvaru následovně:

Definice. *Nechť $\mathbb{F}_q$ je konečné těleso, $\mathbb{E}$ je jeho nadtěleso konečného stupně $n \in \mathbb{N}$. Uvážíme-li kanonickou bijekci $\psi : \mathbb{E} \to \mathbb{F}^n$, kterou jsme dostali jako důsledek Lemmatu 1.1, pak řekneme, že polynomiální vektor $\mathcal{P}$ je HFE-tvaru jestliže existuje polynom*

$$P(X) = \sum_{i,j=0}^{d} A_{i,j} X^{q^i+q^j} + \sum_{i=0}^{d} B_i X^{q^i} + C,\ A_{i,j}, B_i, C \in \mathbb{E},\ X \in \mathbb{E}$$

takový, že $\mathcal{P} = \psi \circ P \circ \psi^{-1}$, $d \in \mathbb{N}$. Takovýto polynom P nazveme HFE polynomem, členy $A_{i,j}X^{q^i+q^j}$ nazveme kvadratickými členy, $B_iX^{q^i}$ členy lineárními a C konstantním členem HFE polynomu.

Důsledkem zobecnění je možnost volit polynomy menšího stupně, nicméně za cenu toho, že pro práci s HFE polynomem musíme použít jiné algoritmy a mohou se objevit problémy s případnou nesurjektivitou definovaného zobrazení. Na druhou stranu útoky na toto zobecnění je možné využít i pro útoky na MIA, byť s možným snížením efektivity. Bohužel dle očekávání podobný vztah druhým směrem k dispozici není.

K invertování polynomů v HFE-tvaru potřebujeme především algoritmus pro hledání kořenů polynomu – pro efektivní invertování průchodu systémem za pomoci privátního klíče se nabízí například von zur Gathenův-Shoupův algoritmus [vzGS92]. Další algoritmy pro hledání vzorů můžeme nalézt např. v rozšířené verzi [Pat96b] v sekci 5.

Pozorování 2.1. *Bez újmy na obecnosti můžeme uvažovat pouze polynomy bez konstantního členu, jelikož zahrnutím konstantního členu do druhé afinní transformace získáme ekvivalentní privátní polynom se stejným veřejným klíčem. Stačí si totiž uvědomit, že lineární zobrazení tvořící závěrečnou afinní transformaci lze právě kvůli linearitě aplikovat separátně na všechny monočleny, tj. můžeme přesunout konstantní člen do translační složky této transformace.*

Bohužel jak definice $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$, tak definice HFE polynomu dává relativně velký prostor pro nejednoznačnost a duplicity – zaveďme si tedy na těchto množinách ekvivalenci, abychom dokázali tuto nejednoznačnost vymezit a mohli následně pracovat s pevně danou jednoznačností (právě jednoznačnost až na tuto ekvivalenci „$\sim$“).

Definice. *Nechť máme dva HFE polynomy:*

$$P(X) = \sum_{i,j=0}^{d} A_{i,j} X^{q^i+q^j} + \sum_{i=0}^{d} B_i X^{q^i} + C$$

$$G(X) = \sum_{i,j=0}^{d'} D_{i,j} X^{q^i+q^j} + \sum_{i=0}^{d'} E_i X^{q^i} + F$$

pak řekneme, že P, Q jsou v relaci $\sim \Leftrightarrow \forall i,j \leq max(d,d') : A_{i,j} + A_{j,i} = D_{i,j} + D_{j,i}$ (jestliže předpis neobsahuje $A_{i,j}$, resp. $D_{i,j}$, pro nějaké dvojice i j, pak uvažme pro tyto indexy koeficient nulový). Analogicky si zavedeme relaci „$\sim$“ na $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Vezměme si dva polynomiální vektory $\mathcal{P}, \mathcal{Q} \in \mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Pak řekneme, že $\mathcal{P} \sim \mathcal{Q} \Leftrightarrow$ pro všechny souřadnice polynomiálních vektorů platí $\forall i,j \leq n$: součet koeficientů $x_i x_j$ a $x_j x_i$ je u obou polynomiálních vektorů stejný.

Pozorování 2.2. *Relace „$\sim$“ je zřejmě ekvivalencí na obou množinách – reflexivitu a symetrii dostáváme triviálně, tranzitivitu z tranzitivity $=$.*

Tato relace „$\sim$“ umožňuje na obou množinách vytvořit třídy ekvivalence, které shlukují polynomy, resp. polynomiální vektory, které popisují stejnou funkci. Pak nahlédněme, že tato ekvivalence má nepříjemný dopad na případná šifrovací nebo podpisová schémata. Ekvivalence dvou polynomů totiž znamená i ekvivalenci příslušných veřejných a privátních klíčů, a tedy obě sady popisují stejné funkce. Ve skutečnosti tedy případný útočník nemusí zjišťovat původní privátní klíč, ale stačí mu najít klíč k němu ekvivalentní.

Jak souvisí HFE polynomy s polynomiálními vektory, které jsme si definovali v rámci množiny $\mathcal{MQ}$? Na první pohled může být překvapivé, že existuje jednoznačná, až na ekvivalenci „$\sim$“, korespondence mezi kvadratickými polynomy více proměnných a HFE polynomy. S uvážením vztahů mezi reprezentacemi afinních transformací a poněkud trikovým rozložením HFE polynomu na součty a součiny afinních zobrazení (resp. transformací, pokud opomeneme členy s nulovými koeficienty) tento vztah dostaneme technickým rozborem v následujícím lemmatu.

Lemma 2.3. *Nechť $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ je rozšíření těles a nechť máme HFE polynom*

$$P(X) = \sum_{i,j=0}^{d} A_{i,j} X^{q^i+q^j} + \sum_{i=0}^{d} B_i X^{q^i} + C \text{ pro } C, B_i, A_{i,j}, X \in \mathbb{F}_{q^n}$$

Pak existuje právě jeden polynomiální vektor, až na ekvivalenci $\sim$, $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n)$ takový, že $\forall X \in \mathbb{F}_{q^n} : \psi P(X) = \mathcal{P}(\psi^{-1}(X))$, pro ψ kanonickou bijekci z $\mathbb{F}_{q^n}$ na $\mathbb{F}_q^n$.

Důkaz: Prvně se toto tvrzení pokusíme dokázat pro kvadratické členy. Vezměme si tedy polynom $P(X) = CX^{q^i+q^j}$, C,$X \in F_{q^n}, 0 \leq i,j \in \mathbb{N}$ a $C \neq 0$ (pro $C = 0$ odpovídající polynom najdeme snadno).

Bez újmy na obecnosti můžeme pracovat s $i,j < n$, jelikož $\forall X \in F_{q^n} : X^{q^n} = 1$, tj. $q^{\lfloor \frac{i}{n} \rfloor n}$ můžeme vytknout, čímž nám zbude i' požadované velikosti (pro j funguje stejný postup). Provedeme následující rozdělení $P(X) = X^{q^i} \cdot CX^{q^j}$.

Pokud takto rozdělíme P na součin dvou monočlenů U, V, které odpovídají afinní transformaci, pak můžeme na tyto monočleny převést pomocí Lemmatu 1.7 (s Pozorováním 1.5). Nyní s použitím kanonické bijekce ψ se podívejme na tento převod z pohledu tělesa jako faktorového okruhu $\mathbb{F}_q[x]/(p)$ pro $p \in F_q[x]$ ireducibilní polynom stupně n z definice používaného nadtělesa:

$$\mathcal{U}(x_1, \ldots, x_n) = \psi(U(\psi^{-1}(x_1, \ldots, x_n))) = \psi(\sum_{i=1}^{n} x^{i-1} u_i(x_1, \ldots, x_n))$$

kde $\mathcal{U}$ je reprezentace afinní transformace v polynomech o více proměnných, U je reprezentace tatáž transformace v reprezentaci polynomem jedné proměnné

a u_i jsou jednotlivé složky polynomiálního vektoru $\mathcal{U}$. Toto analogicky provedeme i pro V – pokud vzniklé polynomy vynásobíme $(\sum_{i=1}^{n} x^{n-1} u_i(x_1, \ldots, x_n)) \cdot (\sum_{i=1}^{n} x^{n-1} v_i(x_1, \ldots, x_n))$ a provedeme redukci modulo $p(x)$, pak po aplikaci ψ dostaneme kýžený součin $\psi(U \cdot V)$. Nyní jsme schopni převést kvadratické členy HFE polynomu.

Stále potřebujeme dokázat jednoznačnost. Povšimněme si, že mezi prvky v třídě ekvivalence relace „$\sim$“ můžeme v $\mathbb{F}_{q^n}$ snadno přecházet vytýkáním a roznásobením.

$$AX^{q^i} \cdot BX^{q^j} = (AB)X^{q^i} \cdot X^{q^j} \text{ (asociativita násobení)}$$

Pokud se na tyto koeficienty podíváme skrze kanonickou bijekci jako na lineární kombinaci prvků báze $\mathbb{F}_q^n$, pak $AX^{q^i} \cdot BX^{q^j}$ i $(AB)X^{q^i} \cdot X^{q^j}$ vyjádřené jako vektory polynomů o více proměnných musí být stejné díky komutativitě a asociativitě násobení ve faktorovém okruhu (nahlížíme-li na rozšíření tělesa jako na faktorový okruh). Po převodu záleží, jak rozdělíme koeficienty u $x_i x_j$ a $x_j x_i$, nicméně to je opět v rámci třídy ekvivalence relace „$\sim$“, tj. máme požadovanou jednoznačnost na úrovni třídy ekvivalence.

Lineární členy převedeme přímočaře díky Lemmatu 1.7, člen konstantní pak pomocí kanonické bijekce. Zde máme jednoznačnost zřejmou.

Díky homomorfnosti kanonické bijekce vůči sčítání můžeme tento postup aplikovat i na součty monočlenů – ať už kvadratických, lineárních nebo konstantních, a tedy jsme schopni převést celý HFE polynom.

❑

Tímto jsme si zároveň ověřili, že stále pracujeme s polynomy, které patří do množiny $\mathcal{MQ}(\mathbb{F}_q^n)$.

Důsledek 2.4. *Polynomiální vektory v HFE-tvaru jsou podmnožinou $\mathcal{MQ}(\mathbb{F}_q^n)$ a lze nad nimi stavět schémata založená na $\mathcal{MQ}$-problému.*

Důkaz: K tomuto tvrzení chybí už jen zohlednit případné afinní transformace, které budou modifikovat náš HFE polynom. Ovšem díky Frobeniovu automorfismu (mocnění lze aplikovat člen po členu) a důsledku mocnění v transformaci reprezentované polynomem o jedné proměnné $(X^{q^k})^{q^i+q^j} = X^{q^{i+k}+q^{j+k}}$ je možné nahlédnout, že dojde jen ke změně koeficientů. Aplikací transformací tedy dostaneme opět HFE polynom.

❑

Ještě překvapivější je, že platí i obrácený vztah – dokážeme interpretovat libovolný polynom z $\mathcal{MQ}(\mathbb{F}_q^n)$ jako HFE polynom.

Poznámka. *Nechť $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ je rozšíření těles a máme polynomiální vektor $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}_q^n)$. Pak existuje právě jeden, až na ekvivalenci „$\sim$“, HFE polynom P takový, že máme-li ψ kanonickou bijekci, pak platí $\forall X \in \mathbb{F}_{q^n} : \psi(P(X)) = \mathcal{P}(\psi(X))$.*

Důkaz: V důkaze se budeme muset vypořádat se dvěma případy, jelikož v případě $\mathbb{F}_2$ nastává rovnost u $X^{2^i+2^i} = X^{2^i}$.

Nechť tedy máme $q \neq 2$. Prvně vyčíslíme počet HFE polynomů nad $\mathbb{F}_{q^n}$. Počet koeficientů u kvadratických členů je $\binom{n}{2} + n$, n je počet koeficientů u lineárních

členů a dále máme jeden konstantní člen. Dohromady máme $(q^n)^{\frac{n\cdot(n-1)}{2}+n+n+1} = (q^n)^{\frac{n^2+3n+2}{2}}$ *možností, jak zvolit koeficienty. Pokud se podíváme na počet možných koeficientů polynomiálního vektoru z* $\mathcal{MQ}(\mathbb{F}_q^n)$*, pak máme celkem* $\binom{n}{2} + n$ *koeficientů u kvadratických členů,* n *u lineárních a opět jeden u konstantního – opět dostáváme počet možných voleb koeficientů* $(q^n)^{\frac{n^2+3n+2}{2}}$*. Díky Lemmatu 2.3 dokážeme každému z HFE polynomů přiřadit jeden polynom z* $\mathcal{MQ}(\mathbb{F}_q^n)$ *tak, aby po aplikaci kanonické bijekce oba popisovaly stejnou funkci. Pokud by dva HFE polynomy z různých tříd ekvivalence relace „*$\sim$*“ popisovaly stejnou funkci, pak by jejích rozdíl měl* q^n *kořenů, ovšem to by bylo ve sporu se stupněm polynomu, který je menší než-li* q^n*. Pro dvojici* $X^{q^i+q^j}$ *a* $X^{q^j+q^i}$ *máme* q^n *možností, jak přidělit koeficienty, aby její součet popisoval stále stejnou funkci. Analogicky pro* x_ix_j *a* x_jx_i *máme* q *možností, jak rozdělit koeficienty v jedné souřadnici, tj.* q^n *možností celkem. Nyní máme dvě stejně veliké množiny a prosté zobrazení z jedné množiny do druhé, a tedy je toto zobrazení nutně bijektivní. Dokonce zachovává i třídy ekvivalence „*$\sim$*“, čímž dostáváme jednoznačnost v požadovaném rozsahu.*

Pokud se nyní podíváme na případ $q = 2$*, pak důkaz projde analogicky – jen je zapotřebí si povšimnout, že popisovaný speciální případ odstraní na obou stranách právě* n *koeficientů (*n *možností, jak dostat prvek tvaru* $X^{2^i+2^i}$*, resp.* x_ix_i*).*

❑

Podobné tvrzení je možné rozšířit i na polynomy z $\mathcal{MQ}(\mathbb{F}_q^n, \mathbb{F}_q^m)$ – důkaz je téměř stejný, jedinou velkou změnou je nutnost vyjádřit redukci anebo projekci do prostoru jiné dimenze jako lineární zobrazení, čímž situaci převedeme na výše popsaný případ.

Následující příklad popisuje velice jednoduchou, nicméně názornou ukázku, jak z privátního klíče spočítat klíč veřejný. Aby nedošlo k nechtěné záměně symbolů a indexů, tak v ukázce použiji trochu jiné značení než-li v definici – těleso budeme konstruovat jako faktorový okruh nad polynomy s proměnnou t místo x.

Příklad. *Uvažme* $\mathbb{F} := \mathbb{F}_2$ *a* $\mathbb{E} := \mathbb{F}_{2^3}$ *(*$\mathbb{E} = \mathbb{F}_q[t]/(t^3 + t^2 + 1)$*) a následující privátní klíč:*

$$S(\vec{x}) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \vec{x} + \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 + x_3 + 1 \\ x_2 + 1 \\ x_2 + x_3 \end{pmatrix}$$

$$T(\vec{x}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \vec{x} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 + x_2 \\ x_2 + x_3 + 1 \end{pmatrix}$$

$$P'(X) = tX + (t^2 + 1)X^2 + X^{2+1}$$

Pro vypočítání veřejného klíče z klíče privátního potřebujeme prvně převést první transformaci do nadtělesa, složit s polynomem a provést modulo ireducibilním polynomem $t^3 + t^2 + 1$*. Pro převod prvku z vektorového prostoru* $\mathbb{F}_2^3$ *do* $\mathbb{F}_8$ *musíme postupně roznásobit souřadnici vektoru s příslušným vektorem báze – jelikož díky Lemmatu 1.1 víme, že jde o nultou až* $n-1$ *mocninu kořene polynomu* $t^3 + t^2 + 1$ *a navíc převod proběhne oběma směry, takže nemusíme vybrat konkrétní kořen,*

ale postačí v tomto výpočtu uvažovat pro oba směry konverze ten samý, tj. na začátku výpočtu i na konci pracujeme se souřadnicemi vůči stejné bázi.

$$\mathfrak{S}(t) = t^2\left(x_1 + x_3 + 1\right) + t\left(x_2 + 1\right) + x_2 + x_3$$

$$\Rightarrow \mathfrak{S}^3(t) + (t^2+1)\mathfrak{S}^2(t) + t\mathfrak{S}(t) =$$

$$= t^6\left(x_1 + x_3 + 1\right) + t^5\left(x_2x_1 + x_1 + x_2 + x_2x_3 + x_3 + 1\right) +$$

$$+t^4\left(x_3x_1 + x_1 + x_3 + 1\right) + t^3\left(x_2 + 1\right) + t^2\left(x_1x_2 + x_2 + x_1x_3 + x_3\right) +$$

$$+t\left(x_2x_3 + x_3\right) + x_2 + x_3 \equiv$$

$$\equiv t^2\left(x_1x_2 + x_3 + 1\right) + t\left(x_2x_1 + x_3x_1 + x_1 + x_2 + 1\right) + x_1x_2 + x_2 + x_1x_3 + x_2x_3 + x_3 + 1$$

Zbývá poslední překlad – tentokrát do vektorového prostoru, a tedy vyjádření polynomu jako souřadnic vůči symbolické bázi, a složení s další transformací:

$$\mathfrak{Q}(x_1,\, x_2,\, x_3) = \begin{pmatrix} x_1x_2 + x_3x_2 + x_2 + x_1x_3 + x_3 + 1 \\ x_2x_1 + x_3x_1 + x_1 + x_2 + 1 \\ x_1x_2 + x_3 + 1 \end{pmatrix}$$

$$\mathfrak{P} = T(\mathfrak{Q}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \mathfrak{Q} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1x_2 + x_3 + 1 \\ x_1 + x_2x_3 + x_3 \\ x_3x_2 + x_2 + x_1x_3 + 1 \end{pmatrix}$$

Polynomiální vektor $\mathfrak{P}$ je veřejným klíčem k zadanému privátnímu klíči.

Šifrování a dešifrování

Proces šifrování probíhá analogicky jako u tradičních schémat pro asymetrickou kryptografii. Jediným problémem může být situace, kdy použitý klíč nedefinuje bijektivní zobrazení (ať už z důvodu velikosti vstupních anebo výstupních dimenzí nebo kvůli tvaru samotného HFE polynomu) – v tomto případě při šifrování musíme ke zprávě přidat redundantní informaci, která nám pomůže vzor zrekonstruovat. K tomuto účelu mohou pomoci například samoopravné kódy, nicméně ty přidávají do zprávy redundanci, která může následně pomoci útočníkovi. Proto pro tento účel jsou vhodnější kryptograficky bezpečné hashovací funkce, které s pravděpodobností alespoň $1 - 2^{-k}$, pro k bitová délka výstupu z hashovací funkce, zajistí unikátní dešifrování. Alternativní strategií by bylo využít padding (doplnění šifrovaného textu na předepsanou délku) předepsaného tvaru a vybrat pouze zprávu vyhovující tomuto paddingu, nicméně tato informace, podobně jako samoopravné kódy, může opět prozradit útočníkovi informaci o šifrovaném textu.

Máme-li tedy veřejný klíč $\mathcal{P} \in \mathcal{MQ}(\mathbb{F}^n,\mathbb{F}^m)$ a hashovací funkci h s výstupem o délce k-bitů, pak šifrování můžeme obecně zapsat jako funkci

$$E : \mathbb{F}_q^n \to \mathbb{F}_q^n \times \mathbb{F}_2^k$$

$$E : x \mapsto (\mathbb{P}(x), h(x))$$

Přirozeně v případě, že $\mathcal{P}$ je bijektivní, pak funkci h můžeme vynechat.

V případě dešifrování vezměme příslušný privátní klíč $(\mathcal{P}', S, T)$ pro $\mathcal{P}'$ skrytý HFE polynom a S, T afinní transformace. Nechť $(y, h(x))$ je přijatá zašifrovaná zpráva. Pak prvně na y aplikujeme T^{-1}, následně spočteme množinu vzorů pro

$T^{-1}y$, tj. množinu $\{X' \in \mathbb{F}_{q^n} | \psi \circ \mathcal{P}'(X') = y\}$. Na všechny prvky této množiny aplikujeme $S^{-1} \circ \psi$ a z obrazu vybereme prvek takový, aby výstup z hashovací funkce příslušný tomuto prvku odpovídal přiloženému $h(x)$.

$$D : \mathbb{F}_q^n \times \mathbb{F}_2^k \to \mathbb{F}_q^n$$

$$D : (y,h(x)) \mapsto x_{res} \in \{S^{-1} \circ \psi \circ \mathbb{P}'^{-1} \circ \psi^{-1} \circ T^{-1}(y) | h(x_{res}) = h(x)\}$$

Nyní si povšimněme, že tyto předpisy dávají velkou restrikci na konstrukci schémat založených na HFE. Průměrně musíme prohledat polovinu vzorů, než najdeme odpovídající vzor. Pokud tedy chceme klást důraz na malou náročnost výpočtu, pak si určitě nemůžeme dovolit zvolit příliš velkou množinu vzorů, kterou bychom museli pokaždé prohledávat.

Podpis a ověřování podpisu

V případě podpisu je situace jednodušší – jakožto podepisující ve skutečnosti „dešifrujeme“ podepisovaný text svým privátním klíčem a příjemce si podpis ověří jeho „zašifrováním“ za pomoci veřejného klíče, což by opět měla být identita. Oproti šifrování není redundance v základním schématu zapotřebí. Podepisujícímu stačí vybrat libovolný vzor z množiny, kterou dostane při dešifrování (viz předchozí podsekce před srovnáním s $h(x)$), a ten se pak zřejmě zobrazí po šifrování na požadovaný výsledek. Z tohoto postupu pramení další omezení – podepisovaný text musí nutně ležet v množině obrazů funkce definované veřejným klíčem.

Při podepisování tedy využijeme funkci D ve verzi bez hashovací funkce a při ověřování podpisu budeme srovnávat, jestliže přijatá zpráva (resp. její hash) odpovídá $E(y)$ pro y přijatý podpis.

Stejně jako v případě tradiční (RSA, Diffie-Hellman apod.) asymetrické kryptografie je výpočet podpisu relativně náročná operace a navíc velikost klíče limituje i délku šifrového textu, takže je někdy vhodnější nepodepisovat přímo text, ale podepsat výstup z kryptograficky bezpečné hashovací funkce aplikované na zprávu.

3 Útoky

3.1 Obecný útok – lineariace

Studium diferencí mezi šifrovaným textem a jeho vzorem umožňuje zkonstruovat velice obecný útok, který je možné aplikovat na libovolné schéma s veřejným klíčem ve tvaru $\mathcal{MQ}(\mathbb{F}^n, \mathbb{F}^m)$. Máme-li $y, y' \in \mathbb{F}_q^m$ a $x = (x_1, \ldots, x_n), \Delta = (\delta_1, \ldots, \delta_n) \in \mathbb{F}_q^m$ takové, že $\mathcal{P}(x) = y$ a $\mathcal{P}(x + \Delta) = y'$, pak odečtením těchto rovnic dostaneme vektor obsahující v každé souřadnici soustavu lineárních (v x_i) rovnic, kterou umíme spočítat např. Gaussovou eliminací v polynomiálním čase.

Podívejme se nyní na i-tou souřadnici toho vektoru (s využitím ekvivalence polynomů „$\sim$“, abychom snížili počet hledaných koeficientů):

$$y_i - y_i' = p_i(x_1, \ldots, x_n) - p_i((x_1 + \delta_1, \ldots, x_n + \delta_n))$$

$$= (\gamma_i - \gamma_i) + \sum_{k=0}^{n-1} \beta_{i,k}(x_k - x_k - \delta_k) + \sum_{\substack{k=0,l=0 \\ k \leq l}}^{n-1} \gamma_{i,k,l}(x_k x_l - x_k x_l - x_k \delta_l - x_l \delta_k - \delta_k \delta_l)$$

$$= -\sum_{k=0}^{n-1} \beta_{i,k}\delta_k - \sum_{\substack{k=0,l=0 \\ k \leq l}}^{n-1} \gamma_{i,k,l}(x_k \delta_l + x_l \delta_k + \delta_k \delta_l)$$

Naštěstí lze tento útok jednoduše zmařit např. přidáním náhodného paddingu ke vstupu, který tyto vztahy naruší. Ačkoliv aplikace útoku v praxi může být sporná, je důležité ho zohlednit při práci se zranitelnými schématy. Tato zranitelnost pak může způsobit oslabení schématu v některých teoretických modelech nebo ve specifických aplikacích – např. při bezpečnostním experimentu s orákulem, které umožňuje šifrovat vybraný text, je tato vlastnost fatálním nedostatkem.

3.2 Relinearizace

V roce 1999 se v [KS99] objevil velice elegantní útok na HFE, omezíme-li se na systémy s lineárními transformacemi namísto afinních (což v případě $\mathbb{F}_q \neq \mathbb{F}_2$ nemusí být nutně problém za použití algoritmu z [Fel06] pro eliminaci translací) a HFE polynomy s pouze kvadratickými členy. Základní myšlenka spočívá v přepisu centrálního polynomu do bilineární formy, která nám dá soustavu kvadratických rovnic, kterou budeme linearizovat.

Mějme $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ rozšíření těles. Je-li $G(\vec{x}) = (T \circ P' \circ S)\vec{x}$ veřejný klíč, alternativně můžeme toto složení vyjádřit díky Lemmatu 2.1 jako

$$P'(X) = \sum_{i,j=0}^{d-1} P_{i,j} X^{q^i + q^j},\ P_{i,j}, X \in \mathbb{F}_{q^n}, d \leq n$$

$$G(X) = \sum_{i,j=0}^{n-1} G_{i,j} X^{q^i + q^j},\ G_{i,j}, X \in \mathbb{F}_{q^n}$$

Obvykle se z důvodů výpočetní složitosti volí n mnohem větší než d, takže uvažme dokonce případ $d << n$. Z tohoto zápisu je zřejmé, že $G(X)$ můžeme vyjádřit také jako bilineární formu:

$$G(X) = \vec{x}^\top G\vec{x}, G = (G_{i.j})_{i,j=0}^{n\times n}, \vec{x} = (X^{q^0}, \ldots, X^{q^{n-1}})^\top, X \in \mathbb{F}_{q^n}$$

Analogicky si můžeme vyjádřit $T^{-1}(X) = \sum_{i=0}^{n-1} T_i X^{q^i}$ (což bude zřejmě opět lineární transformace) a $S(X) = \sum_{i=0}^{n-1} S_i X^{q^i}$ pro S_i,$T_i, X \in \mathbb{F}_{q^n}$. Pak dle Věty 4 z [KS99] lze $T^{-1}(G(X))$ vyjádřit jako bilineární formu pro matici $W = (w_{i,j})_{i,j=0}^{n\times n}$, $w_{i,j} = S_{j-i}^{q^i}$ (dolní index uvažujme modulo n), a HFE polynom vyjádřený jako matice $P = (P_{i,j})_{i,j=0}^{n\times n}$:

$$T^{-1}(G(X)) = \sum_{i=0}^{n-1} T_i G^{i*},\ G^{i*}(X) = \sum_{k,l=0}^{n-1} (G_{k,l})^{q^i} X^{q^{i+k}+q^{i+l}}$$

$$T^{-1}(G(X)) = P(S(X)) = \sum_{i,j,u,v=0}^{n-1} X^{q^u} S_{u-i}^{q^i} P_{i,j} S_{v-j}^{q^j} X^{q^v} = \vec{x}WPW^\top\vec{x}^\top = \vec{x}G'\vec{x}^\top$$

Z těchto vztahů pro G' se budeme snažit využít předpokladu, že $d << n$, k odvození koeficientů T_i a prvků matice $G' = WPW^\top$. Pro náhodné koeficienty $T_0, \cdots, T_{n-1}$ bude očekávaná hodnost bilineární formy $WPW^\top$ velice blízká n, ovšem při správné volbě dostaneme výrazný pokles hodnosti, jelikož $P_{i,j} = 0$ je-li i nebo j alespoň d. To znamená, že hledáme-li levé jádro G' (tj. $\vec{x} : \vec{x}G' = 0$), pak při správné volbě T_i dostaneme podprostor dimenze alespoň $n - d$ (kde d je z definice velice malé oproti n a $rank(P) \leq d$). A tedy s vysokou pravděpodobností dokážeme najít $n - d$ lineárně nezávislých vektorů z levého jádra i pokud zafixujeme jejich prvních $n-d$ souřadnic na námi vybranou hodnotu. Tím pádem máme v každém vektoru d proměnných, tj. $d(n - d)$ proměnných celkem. Neznámé koeficienty T_i dají dalších n proměnných. Výpočet takovéhoto vektoru lze vyjádřit ze vztahu $\vec{x}G' = 0$ jako soustavu n rovnic. Celkem dostáváme $n(n - d)$ rovnic v $n + r(n - d)$ neznámých. Tyto rovnice jsou ale kvadratické!

To lze vyřešit pomocí vylepšení známého triku linearizace, kdy $\vec{x}_i\vec{x}_j$, $i \leq j$, substituujeme na novou proměnnou $y_{i,j}$. Ale tím, kromě hledaného řešení, dostaneme velké množství parazitických řešení. S problémem parazitických řešení se snaží vypořádat toto vylepšení zvané relinearizace. Prvním krokem je přidání lineárně (ale ne algebraicky) nezávislých rovnic v potřebném počtu. Tyto rovnice dostaneme díky možnosti rozdílného uzávorkování při linearizaci pro různé n-tice. Například pro čtveřici x_a, x_b, x_c, x_d dostaneme rovnice:

$$(x_a x_b)(x_c x_d) = (x_a x_c)(x_b x_d) = (x_a x_d)(x_b x_c) \rightarrow y_{ab}y_{cd} = y_{ac}y_{bd} = y_{ad}y_{bc}$$

Následně postupně linearizujeme zbylé alespoň kvadratické členy. Tyto substituce již povedou na soustavu lineárních rovnic. Výsledná složitost není ideální (např. pro $r = 13$ a $q = 2$ dostáváme $O(n^8)$), nicméně pořád jsme na úrovni polynomiální složitosti. Ale z tohoto dostaneme n dimenzionální prostor řešení, tj. potřebujeme zavést další restrikce. Pokud ovšem převedeme rovnice z nadtělesa do jeho podtělesa a fixují se některé hodnoty, pak pro každou fixaci se povede snížit počet řešení o q^k, pro $k < n$. Postupně se dostaneme až na úroveň, kdy se nám podaří vyřadit všechna parazitická řešení.

Z těchto informací již bude přímočaré spočíst S a P. Jelikož W je invertibilní, pak levé jádro $G' = WPW^\top$ je stejné jako levé jádro WP. Uvážíme-li bez újmy na obecnosti, že platí $rankP = d$, pak jádro P obsahuje pouze vektory, které mají prvních d souřadnic nulových. Potom ovšem vektory báze levého jádra $WPW^\top$ musí W zobrazit na právě takovéto vektory. Každý takovýto vektor nám dá z tohoto vztahu d rovnic s prvky W jako proměnnými. Nahradíme-li proměnné $w_{i,j}$ proměnnými $S_{j-i}^{q^i}$, pak každé S_i můžeme přepsat pomocí kanonické bijekce pro nějakou bázi $(a_0, \ldots, a_{n-1})$ vektorového prostoru $\mathbb{F}_q^n$ na $S_i = \sum_{j=0}^{n-1} s_{ij} a_j$, $s_{ij} \in \mathbb{F}_q$. Takto dostaneme soustavu lineárních rovnic, které poskytnou (až na multiplikativní konstantu) jednoznačné řešení.

3.3 Gröbnerovy báze

Zřejmě nejefektivnější útok na HFE (s variantami HFE+, HFE- a do určité míry HFEv) nad $\mathbb{F}_2$ se objevil v [FJ03] – útok využívá Gröbnerovy báze, které ve výsledku umožní zjistit celkovou strukturu centrálního polynomu a v některých případech dostaneme členy jeho rozkladu na lineární polynomy.

Mějme polynomy $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_n]$ a označme ideál jimi generovaný jako I. Pak řekneme, že konečná množina $G \subseteq I$ je Gröbnerovou bází I právě tehdy, když $\forall f \in I \, \exists g \in G : LT(g)|LT(f)$, kde $LT(p)$ označuje vedoucí term (vzhledem k nějakému uspořádání - např. lexikografickému).

Pro nalezení Gröbnerovy báze ideálu I existuje několik různých algoritmů z nichž je pravděpodobně nejznámější Buchbergerův algoritmus.

Poznámka. *Pro konkrétní aplikaci [FJ03] doporučují použít tzv. DRL (Degree Reverse Lexicographical order) uspořádání, které je mnohem efektivnější pro danou problematiku než klasické lexikografické uspořádání. DRL uspořádání je definováno následovně:* $x_1^{k_1} \cdots x_n^{k_n} >_{DLR} x_1^{l_1} \cdots x_n^{l_n} \Leftrightarrow ((deg(x^k) = \sum_{i=0}^{n-1} k_i > deg(x^l)$ *nebo* $deg(x^l) = \sum_{i=0}^{n-1} l_i > deg(x^k))$ *a zároveň pro nejmenší* $i \in \{0, \ldots, n-1\}$ *takové, že* $k_i - l_i$ *je nenulové, platí dokonce* $k_i - l_i < 0$.

Definujeme-li si tedy množinu $V_{\mathbb{F}_2} := \{(a \in \mathbb{F}_2^n | \forall i \in \mathbb{Z}_m : f_i(a) = 0)\}$, pak hledáme-li Gröbnerovu bázi $(f_1, \ldots, x_1^2 - x_1, \ldots, x_n^2 - x_n)$ mohou nastat různé situace. Pro HFE jsou obzvláště zajímavé dva případy: báze je triviální je-li $V_{\mathbb{F}_2}$ prázdná a pro $|V_{\mathbb{F}_2}| = 1$ dostaneme bázi ve tvaru $(x_1 - a_1, \ldots, x_n - a_n)$, kde $(a_1, \ldots, a_n)$ je právě jediný prvek $V_{\mathbb{F}_2}$.

Pokud využijeme DRL, pak i pro ostatní případy dostaneme zajímavé výsledky. Například nalezená Gröbnerova báze ideálu bude vždy obsahovat všechny nezávislé rovnice v daném ideálu nejnižšího celkového stupně (S odkazem na [CLO05] autoři konstatují, že je dokonce možné zjistit všechny algebraické vztahy mezi polynomy $f_1, \ldots, f_n$.)

Ačkoliv je počítání Gröbnerových bází v nejhorším případě problém s exponenciální složitostí, tak naštěstí pro polynomy typu HFE toto neplatí a nejvyšší stupeň polynomů ve výpočtu báze nezávisí na stupni rozšíření tělesa. Ve výsledku je s velkou pravděpodobností mnohem rychlejší – [FJ03] uvádí konkrétní experimentální odhady pro složitost výpočtu Gröbnerovy báze pro stupeň HFE polynomu ≤ 512 v rozmezí $O(n^6) - O(n^{10})$ v závislosti na tomto stupni.

Celkovou náročnost značně ovlivní i volba algoritmu pro hledání Gröbnerovy báze. Ačkoliv je Buchbergerův algoritmus velice efektivně implementovaný

v mnohém výpočetním softwaru, tak pro použití pro kryptoanalýzu HFE byly objeveny efektivnější algoritmy. [FJ03] použili algoritmus F_5, resp. jeho modifikaci pro tělesa s charakteristikou 2 pojmenovanou $F_5/2$.

Tuto modifikaci Faugère a Joux aplikovali v [FJ03] na první „HFE challenge“ uveřejněné v [Pat96b], kde prohledávání prostoru by vyžadovalo více jak 2^{80} operací, tj. mimo běžné výpočetní kapacity. Jejich algoritmus $F_5/2$ zvládl prolomit „HFE challenge“ za přibližně 2 dny a 4 hodiny na procesoru s taktem 1GHz a 4Gb operační paměti, což je velmi výrazné zlepšení.

4 Modifikace

Naneštěstí všechna základní schémata, umožňující použití trapdooru, byla již prolomena. Samotné HFE je dle [WP05] prolomeno několika různými způsoby, jak jsme si již ukázali v předchozí kapitole. Bylo tedy zapotřebí přistoupit k jejich modifikacím, které se snaží eliminovat nedostatky těchto schémat. Dvě z dostupných modifikací navrhl Christopher Wolf ve své diplomové práci [Wol02] a právě na tyto modifikace se pokusíme zaměřit.

4.1 HFEm a HFEz

První z nich se jmenuje HFEm, modifikace HFE maskováním. V původní práci se uvažovalo více variant, nicméně v pozdějším článku [WP05] se již označením HFEm označuje pouze jedna z těchto variant – HFEz. Pro tuto práci budeme tyto varianty odlišovat a používat původní značení HFEm, HFEz a HFEm'.

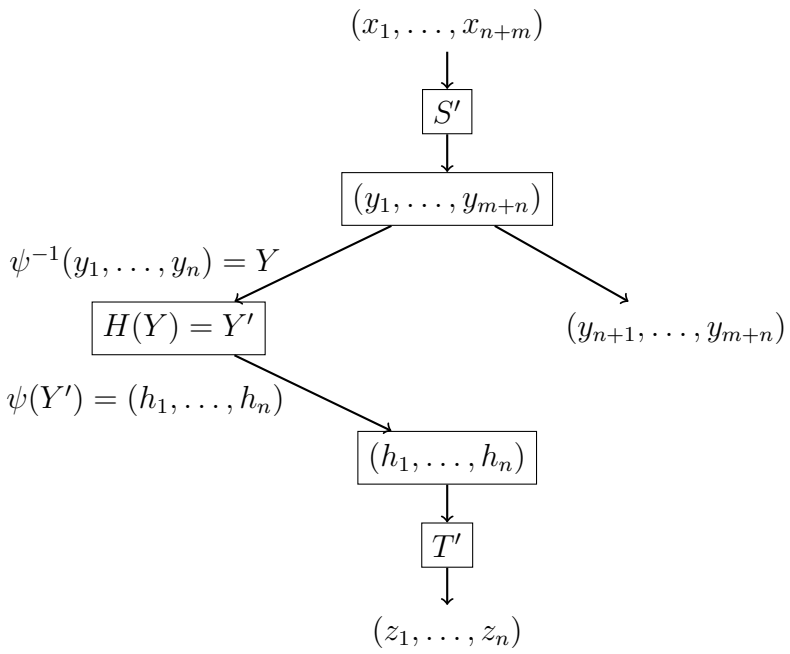
Ve schématu stále pracujeme s rozšířením stupně $n \in \mathbb{N}$. Oproti standardnímu HFE jsou afinní transformace nad $\mathbb{F}_q^{n+m}$ pro nějaké $m \in \mathbb{N}$. Po průchodu původní transformací pošleme n proměnných do složení HFE polynomu P nad $\mathbb{F}_{q^n}$, resp. do složení funkcí $\psi \circ P \circ \psi^{-1}$. Zbylých m proměnných bude vstupem pro náhodné polynomy $g_1, \ldots, g_n \in \mathbb{F}[x_{n+1}, x_{n+2}, \ldots, x_{m+n}]$. Výstup z obou částí tvoří dohromady vstup poslední afinní transformace nad $\mathbb{F}_q^n$. Při dešifrování se postupuje podobně jako v modifikaci HFEv navržené v [KPG99], kde koeficienty HFE polynomu jsou závislé na vstupu – je nutné při invertování použít v menší míře hrubou sílu, tj. invertujeme výstup tajného HFE polynomu a zkoušíme postupně hrubou silou $O(q^m)$ možností pro možné vzory u náhodných polynomů – tentokrát ovšem s mnohem menší náročností, jelikož oproti HFEv (kde je navíc zapotřebí pro každou volbu hledat znovu kořeny polynomu) stačí invertovat pouze afinní transformaci. Bohužel to taktéž znamená, že je zapotřebí v případě šifrování k nezašifrovanému textu přidat redundanci, abychom byli schopni ověřit, že jsme našli správné řešení. Při podepisování narážíme na problém, že nemůžeme jednoduše ověřit (bez aplikace veřejného klíče jako při ověření podpisu), zda-li máme správný vzor. Proto je tato modifikace vhodná spíše pro šifrovací schémata.

Druhou modifikací je HFEz (Zero Added Equations), která je speciálním případem HFEm. Oproti HFEz nevstupují do schématu náhodné polynomy, ale oněch dodatečných m proměnných, které dostaneme z první afinní transformace nebudeme brát v potaz – to se projeví pouze na poslední afinní transformaci, která je nad n dimenzionálním prostorem. Je zřejmé, že dešifrování může probíhat úplně analogicky. Díky této změně je možné s touto modifikací přímočaře vybudovat i podpisové schéma.

Obě tyto modifikace můžeme dokonce hybridizovat v modifikaci HFEm'. Tato modifikace využívá nejen náhodné polynomy, ale také vynechá z výstupu z první afinní transformace několik proměnných stejně jako v případě HFEz.

4.2 HFE⊥

Další modifikací, značně starší než předchozí, je tzv. větvení (branching), které lze nalézt v kontextu již zmiňovaného C* v [MI88]. Původním záměrem bylo umožnit snížit zátěž při dešifrování, kdy se stačí vypořádat pouze se součtem nižších stupňů nadtělesa.



Obrázek 1: Schéma HFEz

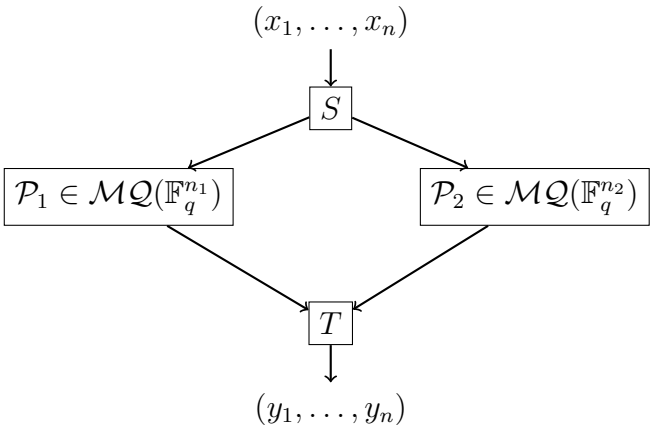
Situaci zjednodušenou na dvě větve a systém s afinními transformacemi S, T stejné dimenze popisuje schéma č. 2, kde $n = n_1 + n_2$.

V kontextu HFE budeme tuto modifikaci označovat jako HFE$\perp$.

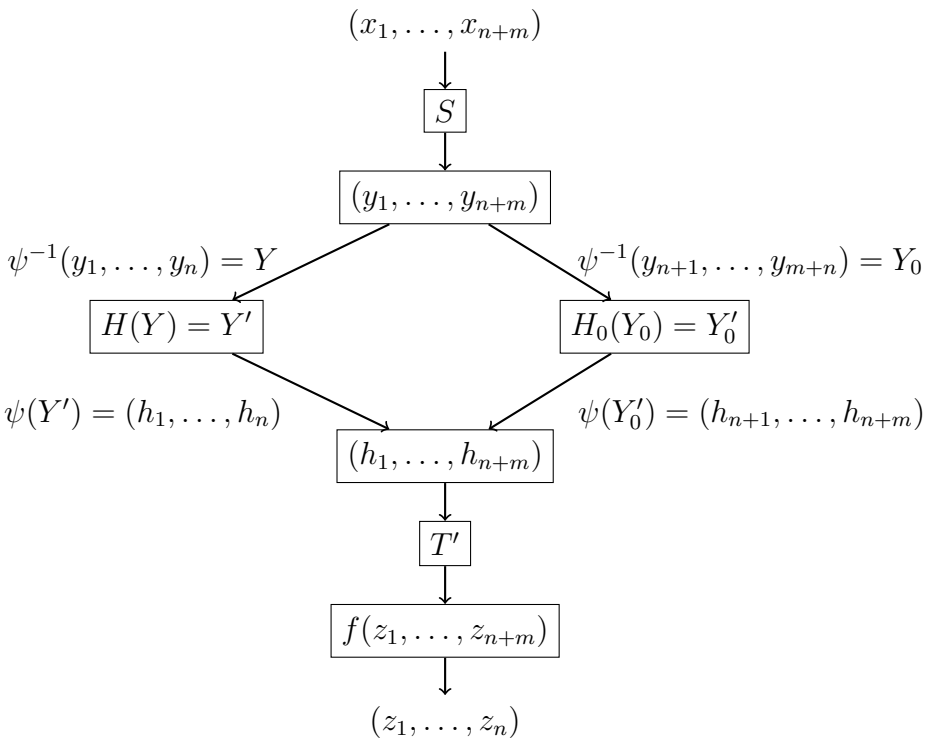
Bohužel, jak se ukázalo např. v [Fel06], je tato optimalizace za příliš velkou cenu na straně bezpečnosti. Právě kvůli existenci efektivních algoritmů pro eliminaci této modifikace se budeme snažit převést HFEz na HFE$\perp$.

4.3 Útok na HFEz

Základní myšlenkou útoku, převedení HFEz na HFE modifikované pomocí větvení (HFE$\perp$), které pak za určitých předpokladů dokážeme separovat na řešení jednotlivých větví, čímž redukujeme situaci na řešení běžného HFE a testování



Obrázek 2: Schéma HFE$\perp$



Obrázek 3: Schéma převodu HFEz na HFE⊥

možných výstupů hrubou silou, podobně jako při dešifrování.

Klíčovou myšlenkou je, že zahození proměnných a redukce výstupní afinní transformace je ekvivalentní průchodu nulovým HFE polynomem následovaným průchodem rozšířenou afinní transformací a následným zahozením posledních m proměnných ze výstupu.

Pro separaci větví využijeme algoritmus navržený v [Fel06], který by měl s vysokou pravděpodobností proběhnout s předpokládanou složitostí $O(n^6)$.

Věta 4.1. *Buď $S \in Aff(\mathbb{F}_q^{n+m})$, $T \in Aff(\mathbb{F}_q^n)$ afinní transformace, $H(X) = \sum_{i,j=0}^{n-1} \alpha_{ij} X^{q^i+q^j} + \sum_{i=0}^{n} \alpha_i X^{q^i}$, $X \in \mathbb{F}_{q^n}$, polynom v HFE-tvaru, redukční funkce $f_m : (x_1, \ldots, x_{m+n}) \mapsto (x_1, \ldots, x_n)$ pro $x_i \in \mathbb{F}_q$ a ψ kanonická bijekce z $\mathbb{F}_{q^n}$ do $\mathbb{F}_q^n$. Uvážíme-li HFEz systém $T \circ \psi \circ H \circ \psi^{-1} \circ f_m \circ S$, pak existuje $T' \in Aff(\mathbb{F}_q^{n+m})$ takové, že výstupy T, $f_m \circ T'$ se rovnají, jestliže prvních n souřadnic vstupních vektorů se rovná. Nechť navíc H_0 je nulový polynom nad $\mathbb{F}_{q^m}$, pak, složíme-li funkce dle diagramu na obrázku 3, dostaneme systém typu HFE⊥, který určuje stejné zobrazení jako původní HFEz systém.*

Důkaz: Dle obrázku 3 je zřejmé, že popsaný odvozený systém je typu HFE⊥. Nadále ho budeme označovat jako simulaci HFE⊥

Zadefinujme si prvně zobrazení

$$f_{-n} : (x_1, \ldots, x_{m+n}) \mapsto (x_{n+1}, \ldots, x_{m+n})$$

Následně se podíváme na obě situace pro fixní vstup $(x_1, \ldots, x_{n+m})$. V případě HFEz dostaneme před aplikací afinní transformace T vektor

$$\psi \circ H \circ f_m \circ S(x_1, \ldots, x_{n+m}) = (h_1, \ldots, h_n) \in \mathbb{F}_q^n$$

V případě simulace obdržíme v téže fázi mezivýsledky

$$\psi \circ H \circ f_m \circ S(x_1, \ldots, x_{n+m}) = (h_1, \ldots, h_n) \in \mathbb{F}_q^n$$

$$\psi \circ H_0 \circ f_{-n} \circ S(x_1, \ldots, x_{n+m}) = (h_{n+1}, \ldots, h_{m+n}) \in \mathbb{F}_q^n$$

Mezivýsledky simulace spojíme na $(h_1, \ldots, h_{m+n})$*. Následně modifikujeme poslední afinní transformaci* T *z* $HFEz$

$$HFEz: \ T(h_1, \ldots, h_n) = \begin{pmatrix} t_{11} & \ldots & t_{1n} \\ \vdots & \ddots & \\ t_{n1} & & t_{nn} \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} + \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = \sum_{i=1}^{n} \sum_{j=1}^{n} (t_{ij} h_j + t_j) \vec{e_i}$$

na rozšířenou verzi T' *podle následujícího předpisu:*

$$Simulace: \ T'(h_1, \ldots, h_{m+n}) = \begin{pmatrix} t_{11} & \ldots & t_{1n} & 0 & \ldots & 0 \\ \vdots & \ddots & & \vdots & \ddots & \\ t_{n1} & & t_{nn} & 0 & & 0 \\ 0 & \ldots & 0 & 1 & & 0 \\ \vdots & \ddots & & & \ddots & \\ 0 & & 0 & 0 & & 1 \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_{m+n} \end{pmatrix} + \begin{pmatrix} t_1 \\ \vdots \\ t_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Zřejmě i toto rozšíření musí být afinní transformací. Podívejme se tedy na výsledek simulace a ověřme, že splňuje podmínku $T(x_1, \ldots, x_n) = f_m \circ T'(x_1, \ldots, x_{m+n})$ *pro libovolná* $x_1, \ldots, x_{m+n} \in \mathbb{F}_q$*.*

$$\sum_{i=1}^{n} \sum_{j=1}^{n} (t_{ij} h_j + t_j) \vec{e_i} + \sum_{i=n+1}^{n+m} h_i \vec{e_i} \Rightarrow f_m \circ T'(h_1, \ldots, h_{m+n}) = \sum_{i=1}^{n} \sum_{j=1}^{n} (t_{ij} h_j + t_j) \vec{e_i}$$

❑

Příklad. *Uvažme* $\mathbb{F} := \mathbb{F}_2$ *a* $\mathbb{E} := \mathbb{F}_{2^3}$ *(*$\mathbb{E} = \mathbb{F}_q/(t^3 + t^2 + 1)$*) a následující privátní klíč:*

$$S(\vec{x}) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \vec{x} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 + x_3 + x_4 + 1 \\ x_2 + x_4 + 1 \\ x_2 + x_3 \\ x_4 \end{pmatrix}$$

$$T(\vec{x}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \vec{x} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 + x_2 \\ x_2 + x_3 + 1 \end{pmatrix}$$

$$HFE(X) = Xt + (t^2 + 1)X^2 + X^{2+1}, \ HFE_0(X) = 0 \cdot X$$

Analogicky s úvodním příkladem spočítáme veřejný klíč - jedinou změnou bude vynechání m*, v tomto případě* $m = 1$*, proměnných:*

$$\mathfrak{S}(t) = t^2 (x_1 + x_3 + x_4 + 1) + t (x_2 + x_4 + 1) + x_2 + x_3$$

$$\Rightarrow \mathfrak{S}^3(t) + (t^2 + 1)\mathfrak{S}^2(t) + t\mathfrak{S}(t) = (x_1 + x_3 + 1)t^2 + (x_1 + x_2 + 1)t + (x_1 + x_3)$$

$$= t^5 (x_2 x_1 + x_4 x_1 + x_1 + x_2 + x_2 x_3 + x_3 + x_2 x_4 + x_3 x_4 + x_4 + 1) +$$

$$+t^4\left(x_2+x_1x_3+x_1x_4+x_4+1\right)+t^3\left(x_1+x_2+x_3\right)+t^2\left(x_1x_2+x_1x_3\right)+$$
$$t\left(x_3x_2+x_4x_2+x_2+x_3x_4\right)\equiv$$
$$\equiv t^2\left(x_2x_1+x_4x_1+x_1+x_3+x_4+1\right)+t\left(x_2x_1+x_3x_1+x_1+x_2+x_3\right)+$$
$$x_1x_2+x_2+x_1x_3+x_2x_3+x_2x_4+x_3x_4$$

$$\mathfrak{Q}(x_1,\,x_2,\,x_3)=\begin{pmatrix}x_1x_2+x_3x_2+x_4x_2+x_2+x_1x_3+x_3x_4\\x_2x_1+x_3x_1+x_1+x_2+x_3\\x_2x_1+x_4x_1+x_1+x_3+x_4+1\end{pmatrix}$$

$$\mathfrak{P}(x_1,\,x_2,\,x_3)=T(\mathfrak{Q})=\begin{pmatrix}0&0&1\\1&1&0\\1&0&1\end{pmatrix}\mathfrak{Q}+\begin{pmatrix}0\\0\\1\end{pmatrix}=$$

$$=\begin{pmatrix}x_2x_1+x_4x_1+x_1+x_3+x_4+1\\x_1+x_2x_3+x_3+x_2x_4+x_3x_4\\x_3x_1+x_4x_1+x_1+x_2+x_2x_3+x_3+x_2x_4+x_3x_4+x_4\end{pmatrix}$$

$\mathfrak{P}$ *je veřejný klíč, který jakožto útočník máme k dispozici.*

Základním krokem pro Felkeho útok popsaný v [Fel06] je zadefinování dvou obecně neasociativních, komutativních algeber. První z těchto algeber je definována nad $\mathbb{F}_{q^n}$ s následující operací: pro vybraný HFE polynom $P(X)=\sum_{i,j=0}^{n-1}\alpha_{i,j}X^{q^i+q^j}+\sum_{i=0}^{n}\alpha_iX^{q^i}$ definujme operaci $M(a,b):=P(a+b)-P(a)-P(b)$, $a,b\in\mathbb{F}_{q^n}$.

Lemma 4.2. $\mathbb{F}_{q^n}$ *s násobením definovaným operací* M *tvoří komutativní algebru.*

Důkaz: Díky distributivitě v tělese se lineární části poodečítají, a tedy operaci M *lze rozepsat:* $M(a,b)=\sum_{i,j=0}^{n-1}\alpha_{i,j}(a^{q^i}b^{q^j}+a^{q^j}b^{q^i})$. *Pokud porovnáme* $M(a,b)$ *a* $M(b,a)$, *pak si povšimneme, že pouze v každém členu sumy se prohodí pořadí sčítanců v závorce a z komutativity sčítání v tělese dostáváme i komutativitu indukované algebry.*

❑

Poznámka. $\mathbb{F}_{q^n}$ *s násobením definovaným operací* M *není obecně asociativní.*

Důkaz: Uvažme následující protipříklad:

$$M(a,M(1,1))=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}\sum_{l=0}^{n-1}\alpha_{i,j}\alpha_{k,l}\left(2a^{q^i}+2a^{q^j}\right)$$

$$M(a,M(1,1))=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}\sum_{l=0}^{n-1}\alpha_{i,j}\alpha_{k,l}\left(a^{q^{i+k}}+a^{q^{i+l}}+a^{q^{j+k}}+a^{q^{j+l}}\right)$$

Nyní je vidět, že v obou situacích pro např. $i=j=0$ *a* $\alpha_{i,j}=0$, *pro všechna* $i,j\in\{2,\ldots,n-1\}$, $\alpha_{i,j}=1$ *jinak, dostaneme v prvním případě* $32a^q+32a$. *V druhém případě dostaneme součet* $16a^{q^2}+32a^q+16a$, *což se rovná právě tehdy když* $16a^{q^2}=16a$ *– to zřejmě v obecném konečném tělese nemusí platit, a tedy jsme ověřili, že obecně tato algebra není asociativní.*

❑

Nechť tedy máme těleso $\mathbb{F}_q$ a jeho rozšíření $\mathbb{F}_{q^n} = \mathbb{F}_q/(m_{\alpha,\mathbb{F}})$, pak můžeme M díky Lemmatu 2.3 (existence vyjádření HFE polynomu jako polynomiálního vektoru o více proměnných) vyjádřit také polynomy více proměnných, které vyjádří M pro konkrétní souřadnici vůči bázi $(1, \alpha, \ldots, \alpha^{n-1})$:

$$M(\sum_{i=0}^{n-1} a_i\alpha^i,\ \sum_{i=0}^{n-1} b_i\alpha^i) = \sum_{i=0}^{n-1} m_i(\vec{a},\ \vec{b})$$

Velice podobně zadefinujeme operaci $M'(a,b) := L_1(M(L_2(a), L_2(b)))$, kde L_1, L_2 jsou lineární části S, T – i tato operace generuje obecně neasociativní, komutativní algebru. Analogicky zavedeme $m'_i(\vec{a},\vec{b})$ jakožto reprezentaci $M(a,b)$ v polynomech více proměnných. Je-li S, T lineární a $(p_1, \ldots, p_n)$ polynomiální vektor – veřejný klíč – pak zřejmě můžeme spočítat $m'_i(\vec{a},\vec{b}) = p_i(\vec{a}+\vec{b}) - p_i(\vec{a}) + p_i(\vec{b})$.

Felkeho útok na větvení je založen na Coppersmith-Patarinově (viz [Pat96a]) útoku na tzv. Dragon Schemes – zde využijeme faktu, že jedinými lineárními zobrazeními nad tělesem jakožto 1-dimenzionálním vektorovým prostorem jsou násobení prvky tělesa. Pokud se na toto tvrzení podíváme z pohledu neasociativních algeber, pak lineární zobrazení L na $\mathbb{F}_{q^n}$, která splňují podmínku

$$\forall x, y \in \mathbb{F}_{q^n} : L(xy) = xL(y)$$

jsou právě prvky multiplikativního centralizátoru (viz např. [Sch66]).

Nyní si rozšiřme definici M a M' na HFEz. Nechť do větve s HFE polynomem jde n proměnných a zbylých m proměnných jde do větve s nulovým HFE polynomem. Pak definujme $M_{HFE} \times M_0$ (na prvních n proměnných provedeme M_{HFE}, na zbývajících m M_0), kde M_{HFE} je dle původní definice $M(a,b)$ a M_0 je zavedeno analogicky, ale pro nulový polynom dimenze m. Právě reprezentace M' polynomem více proměnných má z hlediska výpočtu velice zajímavou vlastnost:

Lemma 4.3. *Jsou-li S, T afinní, pak M' reprezentovanou soustavou polynomů o více proměnných získáme spočtením $m_i(\vec{a},\vec{b}) = p_i(\vec{a}+\vec{b}) - p_i(\vec{a}) + p_i(\vec{b})$, $i = 1, \ldots, n$, za pomoci veřejného klíče $(p_1, \ldots, p_n)$, kde v $m_i(\vec{a},\vec{b})$ vynecháme případné konstantní členy.*

Důkaz: Je-li S lineární, pak je implikace zřejmá při využití Pozorování 2.1, jelikož mocněním s exponentem menším než řád multiplikativní grupy tělesa (která je cyklická), násobením a sčítáním, resp. odečítáním, x_i nemohu získat (uvažujeme-li obecný prvek tělesa – v konkrétních instancích se samozřejmě konstanty mohou vyskytnout) konstantní člen. Zároveň díky tomuto pozorování konstantní člen není ani v HFE polynomu.

Je-li T lineární, pak nejjednodušší řešení nám poskytne pohled na průchod HFE polynomem skrze jemu odpovídající polynom z množiny $\mathcal{MQ}(\mathbb{F}_q^n)$, který máme díky Lemmatu 2.3 k dispozici. Tento polynom má nejvýše kvadratické členy, tj. dojde k násobení nejvýše dvou lineárních kombinací $1, x_1, \ldots, x_{m+n}$ (1 odpovídá právě konstantnímu členu afinní transformace). Což znamená, že konstantní člen se na výstupu projeví pouze ve formě lineárních a konstantních členů – lineární členy se při dosazení do definice m'_i odečtou a zbudou pouze členy konstantní.

Poslední případ, kdy jsou obě transformace afinní, získáme přímočaře kombinací předchozích případů.

❑

Definice. *Nechť máme daná M a M' (resp. jejich varianty reprezentované soustavou polynomů o více proměnných), pak definujme smíšený multiplikativní centralizátor jako množinu všech uspořádaných dvojic lineárních zobrazení (C, C'), které splňují:*

$$C'(m'_1(\vec{x},\vec{y}),\ \ldots,\ m'_{n+m}(\vec{x},\vec{y})) = (m'_1(\vec{x},C\vec{y}),\ \ldots,\ m'_{n+m}(\vec{x},C\vec{y}))$$

Povšimněme si prvně, že tato definice rozšiřuje standardní definici multiplikativního centralizátoru pro neasociativní algebry. Místo hledání lineárního zobrazení L splňujícího $\forall x, y \in \mathbb{F}_{q^n} : L(xy) = xL(y)$, hledáme dvojici lineárních zobrazení (L_1, L_2) $\forall x, y \in \mathbb{F}_{q^n} : L_1(xy) = xL_2(y)$. Triviálně pak dostáváme, že je-li L v multiplikativním centralizátoru, pak (L, L) je ve smíšeném multiplikativním centralizátoru.

Pozorování 4.4. *Podmínku v definici lze ekvivalentně přepsat na:*

$$C'B(m_1(A\vec{x},A\vec{y}),\ \ldots,\ m_{n+m}(A\vec{x},A\vec{y})) = B(m_1(A\vec{x},AC\vec{y}),\ \ldots,\ m_{n+m}(A\vec{x},AC\vec{y}))$$

kde A je lineární část afinní transformace S a B je lineární část afinní transformace T.

Náleží-li tedy (C, C') smíšenému multiplikativnímu centralizátoru, pak dvojice $(ACA^{-1},\ B^{-1}C'B)$ řeší

$$Z'((m_1,\ \ldots,m_{m+n})) = (m_1(\vec{x}, Z\vec{y}),\ \ldots, m_{m+n}(\vec{x}, Z\vec{y}))$$

Ovšem potom si můžeme taktéž zadefinovat $C := A^{-1}ZA$ a $C' := BZ'B^{-1}$ pro Z a Z' splňující tuto rovnici a nyní již lze nahlédnout, že řešení jsou vzájemně konjugována.

Smíšený centralizátor M' spočítáme přímočaře Gaussovou eliminací, kde koeficienty $c_{i,j}$, $c'_{i,j}$ matic $C\,C$ budou hledané neznámé a rovnice dostaneme z dvojic šifrových a otevřený textů, které vygenerujeme za pomoci veřejného klíče.

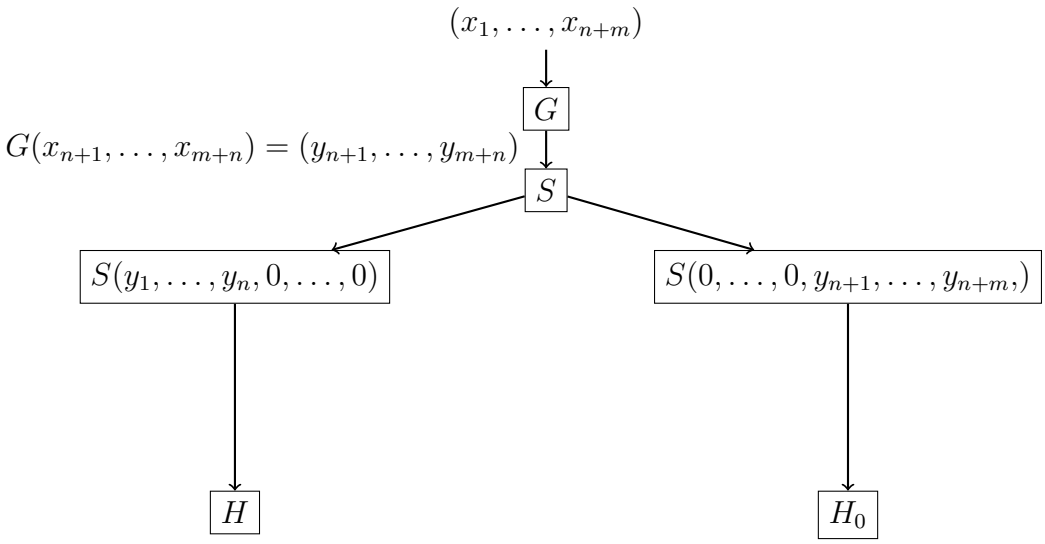
Pro speciální případy, např. pro některá tělesa charakteristiky 2, se podařilo Felkemu v [Fel06] popsat všechny prvky smíšeného centralizátoru a na základě experimentálních dat formuloval domněnku, která zobecňuje tyto speciální případy:

Domněnka 4.5. *Matice C z dvojice (C, C') ze smíšeného centralizátoru pro libovolný systém o l větvích jsou matice $A^{-1}ZA$ se Z ve tvaru*

$$Z = \begin{pmatrix} \Lambda_1 & 0 & \ldots & 0 \\ 0 & \Lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \Lambda_l \end{pmatrix}$$

kde Λ_i je bloková matice zobrazení odpovídající násobení prvkem z rozšíření tělesa příslušného stupně.

Tato hypotéza dává k dispozici velmi silný nástroj. Jestliže je matice Z dokonce v Jordanově kanonickém tvaru, pak zřejmě A bude maticí obsahující Jordanovy řetízky příslušné matici C. Tím pádem pak matici A dostaneme dokonce přímo z algoritmu pro převod do Jordanova kanonického tvaru.



Obrázek 4: Separace proměnných za pomoci matice G

Pokud jsme tedy schopni najít takovou matici $C = A^{-1}ZA$, v našem případě se dvěma bloky, pak z matice C odvodíme matici $G := A^{-1}Z$ takovou, že AG je matice tvaru

$$AG = \begin{pmatrix} W_1 & 0 \\ 0 & W_2 \end{pmatrix}$$

pro W_1 a W_2 blokové matice. Teoreticky můžeme obdržet bloků více, nicméně pořád nám jde o separaci do dvou skupin, tj. bez újmy na obecnosti můžeme teoreticky bloky pro stejnou větev sloučit v jeden blok, který bude též blokově diagonální. Následně je separace jednotlivých větví přímočará – díky blokové diagonalitě se proměnné separují podobně jako na obrázku 4.

Navažme na předchozí příklad a podívejme se na výpočet matice pro separaci větví pro dříve spočtený veřejný klíč.

Příklad. *S příkladem navážeme na předchozí příklad s veřejným klíčem*

$$\mathfrak{P}(x_1,\, x_2,\, x_3, x_4) = \begin{pmatrix} x_2x_1 + x_4x_1 + x_1 + x_3 + x_4 + 1 \\ x_1 + x_2x_3 + x_3 + x_2x_4 + x_3x_4 \\ x_3x_1 + x_4x_1 + x_1 + x_2 + x_2x_3 + x_3 + x_2x_4 + x_3x_4 + x_4 \end{pmatrix}$$

a transformací

$$S(\vec{x}) = A\vec{x} + \vec{v};\ A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Nyní využijeme připravené Lemma 4.3 pro získání polynomiálního vektoru $\vec{m}' = (m_1, m_2, m_3)$. Navíc, vynecháme-li koncovou redukci z Lemmatu 4.1, pak dostaneme systém, který má stejnou dimenzi pro vstupní i výstupní hodnoty.

$$\vec{m}'(\vec{a},\vec{b}) = \mathfrak{P}(a_1+b_1,\, a_2+b_2,\, a_3+b_3, a_4+b_4) - \mathfrak{P}(a_1,\, a_2,\, a_3, a_4) - \mathfrak{P}(b_1,\, b_2,\, b_3, b_4) + c$$

kde $c \in \mathbb{F}_q$ je konstanta, která odečte konstantní členy v polynomiálním vektoru, odstranění redukce se projeví přidáním poslední nulové souřadnice (lineární kombinace nul – výstupů z nulového polynomu – je pořád nula).

$$\vec{m}'(\vec{a},\vec{b}) = \begin{pmatrix} x_2x_1 + x_4x_1 + x_1 + x_3 + x_4 + 1 \\ x_1 + x_2x_3 + x_3 + x_2x_4 + x_3x_4 \\ x_3x_1 + x_4x_1 + x_1 + x_2 + x_2x_3 + x_3 + x_2x_4 + x_3x_4 + x_4 \\ 0 \end{pmatrix}$$

Tento vektor dosadíme do soustavy, kterou dostaneme přímou aplikací definice smíšeného multiplikativního centralizátoru. Po dosazení několika párů původních a šifrových textů (které lze vytvořit z původních textů díky veřejnému klíči) dostaneme soustavu rovnic, kterou umíme řešit například Gaussovou eliminací.

$$C'\vec{m}'(\vec{a},\vec{b}) = \vec{m}'(\vec{a},C\vec{b})$$

pro $C', C \in \mathbb{F}_q^{4\times 4}$ – hledané matice. Smíšený centralizátor vyjádříme soustavou.

$$\begin{pmatrix} c'_{11} & c'_{12} & c'_{13} & c'_{14} \\ c'_{21} & c'_{22} & c'_{23} & c'_{24} \\ c'_{31} & c'_{32} & c'_{33} & c'_{34} \\ c'_{41} & c'_{42} & c'_{43} & c'_{44} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ (a_1+a_4)(b_2+b_3) + a_3(b_1+b_2+b_4) + a_2(b_1+b_3+b_4) \\ (a_1+a_4)(b_2+b_3) + a_3(b_1+b_2+b_4) + a_2(b_1+b_3+b_4) \\ 0 \end{pmatrix} =$$

$$= \vec{m}'(\vec{a}, \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix} \cdot \vec{b})$$

Na této soustavě provedeme několik úprav a dostaneme závislosti mezi prvky matice C (ačkoliv máme k dispozici i restrikce na matici C', tak ta nás v tomto kroku již nezajímá):

$$\begin{pmatrix} c_{11} & 0 & 0 & 0 \\ c_{41} & c_{34} + c_{42} + c_{44} & c_{43} & c_{34} \\ c_{41} & c_{42} & c_{34} + c_{43} + c_{44} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}$$

zvolme tedy například následující matici C:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

vynásobme nyní ACA^{-1} (tj. dostaneme matici Z z Domněnky 4.5)

$$ACA^{-1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Což je opravdu blokově diagonální matice s bloky velikosti 3 a 1, jak tvrdí hypotéza. Nyní je zapotřebí převést matici C do Jordanova kanonického tvaru. Nicméně

povšimněme si, že předchozí krok nám dává blokově diagonální matici v Jordanově kanonickém tvaru, tj. až na pořadí vlastních čísel bude výstup z převodu do Jordanova kanonického tvaru dokonce stejný. Pokud zadefinujeme matici $G := A^{-1}C$*, pak je zřejmé, že* $A \cdot G$ *bude opět blokově diagonální matice.*

Tímto jsme obdrželi matici, která nám umožní oddělit jednotlivé větve, tj. můžeme aplikovat některý z algoritmů navrhovaný pro tradiční HFE.

5 Diskuse a závěr

Navzdory tomu, že $\mathcal{MQ}$ problém je obecně NP-úplný problém, který umožňuje vytvořit schémata pro post-kvantovou kryptografii, existují mnohé útoky proti základním schématům i proti některým jejich modifikacím. Jednou z modifikací, která měla umožnit vybudovat šifrovací schémata nad HFE, byla modifikace původně označovaná jako HFEz („Zero Added Equations“ v [Wol02]), která je v novějším článku od mj. jejího autora již označovaná jako HFEm („Masking“ v [WP05]).

V sekci 4.3 jsme ukázali, že dokážeme převést systém HFEz na systém HFE$\perp$, kde již máme k dispozici algoritmus navržený v [Fel06] pro rozdělení systému na jednotlivé větve. Tento algoritmus využívá několika poznatků o neasociativních algebrách a aplikuje je pro nalezení matice, která dokáže oddělit proměnné před úvodní transformací S na dvě a více sad podle patřičných větví. Nalezení těchto matic by podle [Fel06] mělo proběhnout s vysokou pravděpodobností, nicméně konkrétní podmínky, kdy je možné separaci provést, jsou zatím otevřenou otázkou.

Za předpokladu, že jsme schopni provést separaci, se HFEz dostává do situace, kdy existují algoritmy schopné běžet v polynomiálním čase, které umožní získat privátní klíč z veřejného klíče pro tuto modifikaci. Toto by bylo pro HFE nepříjemné, protože, jak například [Wol02] poznamenává, je relativní nedostatek modifikací, které by umožnily vybudovat nad HFE šifrovací schémata. Proto vyvstává otázka, jak se bude chovat separační algoritmus z [Fel06] pro systémy, kde existují větve s obecnými (ne nutně HFE) polynomy – jestliže by je bylo možné řešit podobně, pak by bylo možné obdobný postup vztáhnout i na obecnější HFEm, resp. HFEm'.

Literatura

[CLO05] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2nd edition, 2005.

[Fel06] Patrick Felke. *Coding and Cryptography: International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005. Revised Selected Papers*, chapter On the Affine Transformations of HFE-Cryptosystems and Systems with Branches, pages 229–241. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[FJ03] Jean-Charles Faugère and Antoine Joux. *Advances in Cryptology - CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings*, chapter Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases, pages 44–60. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. *Advances in Cryptology — EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings*, chapter Unbalanced Oil and Vinegar Signature Schemes, pages 206–222. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[KS99] Aviad Kipnis and Adi Shamir. *Advances in Cryptology — CRYPTO' 99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings*, chapter Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization, pages 19–30. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[MI88] Tsutomu Matsumoto and Hideki Imai. *Advances in Cryptology — EUROCRYPT '88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, May 25–27, 1988 Proceedings*, chapter Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption, pages 419–453. Springer Berlin Heidelberg, Berlin, Heidelberg, 1988.

[Pat96a] Jacques Patarin. *Advances in Cryptology — CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings*, chapter Asymmetric Cryptography with a Hidden Monomial, pages 45–60. Springer Berlin Heidelberg, Berlin, Heidelberg, 1996.

[Pat96b] Jacques Patarin. *Advances in Cryptology — EUROCRYPT '96: International Conference on the Theory and Application of Cryptographic Techniques Saragossa, Spain, May 12–16, 1996 Proceedings*, chapter Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms, pages 33–48. Springer Berlin Heidelberg, Berlin, Heidelberg, 1996. (Extended version).

[Sch66] R.D. Schafer. *An Introduction to Nonassociative Algebras*. Dover books on mathematics. Dover Publications, 1966.

[Sho97] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997.

[vzGS92] Joachim von zur Gathen and Victor Shoup. Computing frobenius maps and factoring polynomials. *Computational Complexity*, 2(3):187–224, 1992.

[Wol02] Christopher Wolf. Hidden Field Equations (HFE) - Variations and Attacks. Master's thesis, Universität Ulm, 2002. `http://www.christopher-wolf.de/dpl`.

[WP05] Christopher Wolf and Bart Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, 2005. `http://eprint.iacr.org/`.

Seznam obrázků