Modifikátor perturbácie MPKC

viliam.hromada

October 2022

1 Intro

V tomto dokumente sa pokúsime demonštrovať, ako funguje modifikátor navrhnutý v článku *A New Perturbation for Multivariate Public Key Schemes such as HFE and UOV*. Vysvetlenie bude pomerne voľné a pre snáď lepšiu zrozumiteľnosť bude priebežne robené na príkladoch, hoci odborný text by skôr vyžadoval viac teoretický prístup.

2 HFE

2.1 Tvorba modifikovaného HFE

Ako je známe, HFE pracuje nad 2 poliami: nejakým základným poľom $\mathbb{F}_q$ a jeho rozšírením n-tého stupňa, $\mathbb{F}_{q^n}$. Uvažujme teda, že v našom prípade bude základné pole $\mathbb{F}_2 = GF(2)$ a uvažujme jeho rozšírenie 3. stupňa, $\mathbb{F}_{2^3} = GF(2^3)$, ktoré je definované pomocou primitívneho polynómu $x^3 + x + 1$ nad poľom $GF(2)$. Len pre istotu uvádzame prvky poľa $GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1\}$.

Pripomíname, že platí známy fakt, že každý prvok nad poľom $\mathbb{F}_{2^n}$ sa dá zobraziť na nejaký n-prvkový vektor nad základným poľom $\mathbb{F}_2$. Toto zobrazenie sa niekedy nazýva aj *kanonická bijekcia*, v článku ho autori označujú ako $\Phi_n : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$. Keďže ide o bijekciu, existuje aj inverzné zobrazenie, Φ_n^{-1}, ktoré zobrazí n-rozmerný vektor nad základným poľom $\mathbb{F}_q$ na prvok z poľa $\mathbb{F}_{q^n}$. Napríklad v našom prípade:

$\Phi_3(0) = (0,0,0)$	$\Phi_3^{-1}(0,0,0) = 0$
$\Phi_3(1) = (1,0,0)$	$\Phi_3^{-1}(1,0,0) = 1$
$\Phi_3(\alpha) = (0,1,0)$	$\Phi_3^{-1}(0,1,0) = \alpha$
$\Phi_3(\alpha^2) = (0,0,1)$	$\Phi_3^{-1}(0,0,1) = \alpha^2$
$\Phi_3(1+\alpha) = (1,1,0)$	$\Phi_3^{-1}(1,1,0) = 1+\alpha$
$\Phi_3(\alpha+\alpha^2) = (0,1,1)$	$\Phi_3^{-1}(0,1,1) = \alpha+\alpha^2$
$\Phi_3(1+\alpha+\alpha^2) = (1,1,1)$	$\Phi_3^{-1}(1,1,1) = 1+\alpha+\alpha^2$
$\Phi_3(1+\alpha^2) = (1,0,1)$	$\Phi_3^{-1}(1,0,1) = 1+\alpha^2$

Keď teda máme zvolené konečné pole a jeho rozšírenie, HFE schéma funguje tak, že sa nad poľom $\mathbb{F}_{q^n}$ zvolí HFE polynóm. Ide o polynóm v jednej neurčitej

v špecifickom, HFE tvare. Vo všeobecnosti má HFE polynóm tvar:

$$H(x) = \sum_{q^i+q^j \leq d} \alpha_{i,j} x^{q^i+q^j} + \sum_{q^k \leq d} \beta_k x^{q^k} + \gamma \tag{1}$$

Parameter d udáva maximálny stupeň HFE polynómu. V praxi sa volí tak, aby nebol príliš veľký, napr. $d \leq 1024$. Autori článku uvažujú zjednodušenú verziu HFE polynómu:

$$H(x) = \sum_{q^i+q^j \leq d} \alpha_{i,j} x^{q^i+q^j} \tag{2}$$

V našom prípade uvažujme, že $d = 5$, t.j. náš HFE polynóm bude (maximálne) piateho stupňa. Keďže u nás $q = 2$, jednotlivé koeficienty HFE polynómu, ktoré sa náhodne zvolia, sa v našom prípade napríklad môžu zvoliť nasledovne:

- Pre $i = 0, j = 0$, teda pre $x^2 : \alpha_{0,0} = 0$
- Pre $i = 0, j = 1$, teda pre $x^3 : \alpha_{0,1} = \alpha^2$
- Pre $i = 0, j = 2$, teda pre $x^5 : \alpha_{0,2} = 1 + \alpha$
- Pre $i = 1, j = 1$, teda pre $x^4 : \alpha_{1,1} = 1$
- Pre $i = 1, j = 2$ sa už koeficient nezvolí, lebo $2^1 + 2^2 > 5$.

Teda náš HFE polynóm bude:

$$H(x) = \alpha^2 x^3 + (1 + \alpha)x^5 + x^4 \tag{3}$$

kde neurčitá x môže nadobúdať hodnoty akéhokoľvek prvku z poľa $\mathbb{F}_{2^3}$. Ako ste sa určite dočítali v úvode do MQ kryptografie, každý takýto HFE polynóm, resp. každý polynóm v jednej neurčitej nad nejakým n-tým rozšírením konečného poľa je možné previesť na sústavu n polynómov o n neurčitých nad základným poľom. V našom prípade teda vieme polynóm $H(x)$ nad poľom $\mathbb{F}_{2^3}$ previesť na sústavu 3 kvadratických polynómov o 3 neurčitých x_1, x_2, x_3 nad základným poľom $\mathbb{F}_2$. Výsledkom je táto sústava polynómov:

- $h_1(x_1, x_2, x_3) = x_2x_3 + x_2 + x_3$
- $h_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2$
- $h_3(x_1, x_2, x_3) = x_2x_3 + x_1 + x_3$

Modifikátor $\hat{+}$ schémy HFE funguje nasledovným spôsobom. Najprv sa zvolí parameter t, ktorým je nejaké celé číslo. Následne sa vygeneruje t náhodných kvadratických polynómov $p_1, ..., p_t$ nad základným poľom $\mathbb{F}_q$ vo všetkých $x_1, ..., x_n$ neurčitých. Nech teda v našom prípade je $t = 2$ a náhodné kvadratické polynómy p_1, p_2 sú:

- $p_1(x_1, x_2, x_3) = x_1x_3 + x_2x_3 + x_2^2$

- $p_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_1^2 + x_3^2$

V ďalšom kroku sa každý z polynómov $p_i(x_1, ..., x_n)$ prevedie na polynóm $\check{p}_i$, ktorý je ekvivalentom p_i, avšak v rozšírení $\mathbb{F}_{q^n}$. Keďže každý polynóm p_i defacto zobrazuje n-prvkový vektor $(x_1, ..., x_n)$ nad $\mathbb{F}_q$ na nejaký prvok y_i z poľa $\mathbb{F}_q$, tak polynóm $\check{p}_i$ bude zobrazovať prvok $x = x_1 + \alpha x_2 + ... + \alpha^{n-1}x_n$ z poľa $\mathbb{F}_{q^n}$ na prvok $y_i + 0 * \alpha + 0 * \alpha^2 + ... + 0 * \alpha^{n-1}$ z poľa $\mathbb{F}_{q^n}$.

V našom prípade teda ak polynóm p_1 predstavuje zobrazenie:

- $p_1(0, 0, 0) = 0$
- $p_1(1, 0, 0) = 0$
- $p_1(0, 1, 0) = 1$
- $p_1(0, 0, 1) = 0$
- $p_1(1, 1, 0) = 1$
- $p_1(0, 1, 1) = 0$
- $p_1(1, 1, 1) = 1$
- $p_1(1, 0, 1) = 1$

potom jeho ekvivalent $\check{p}_1$ v rozšírení $\mathbb{F}_{2^3}$ bude predstavovať zobrazenie:

- $\check{p}_1(0) = 0$
- $\check{p}_1(1) = 0$
- $\check{p}_1(\alpha) = 1$
- $\check{p}_1(\alpha^2) = 0$
- $\check{p}_1(1 + \alpha) = 1$
- $\check{p}_1(\alpha + \alpha^2) = 0$
- $\check{p}_1(1 + \alpha + \alpha^2) = 1$
- $\check{p}_1(1 + \alpha^2) = 1$

Podobne pre p_2 a $\check{p}_2$ bude platiť:

$p_2(0, 0, 0) = 0$	$\check{p}_2(0) = 0$
$p_2(1, 0, 0) = 1$	$\check{p}_2(1) = 1$
$p_2(0, 1, 0) = 0$	$\check{p}_2(\alpha) = 0$
$p_2(0, 0, 1) = 1$	$\check{p}_2(\alpha^2) = 1$
$p_2(1, 1, 0) = 0$	$\check{p}_2(1 + \alpha) = 0$
$p_2(0, 1, 1) = 1$	$\check{p}_2(\alpha + \alpha^2) = 1$
$p_2(1, 1, 1) = 0$	$\check{p}_2(1 + \alpha + \alpha^2) = 0$
$p_2(1, 0, 1) = 1$	$\check{p}_2(1 + \alpha^2) = 1$

Otázkou, ktorú si necháme na neskôr je, ako tieto polynómy $\check{p}_i$ nájsť. Napríklad vo vyššie uvedených prípadoch platí, že príslušné polynómy $\check{p}_1, \check{p}_2$ majú predpisy:

$$\check{p}_1(x) = (\alpha+1)x^6+(\alpha^2+1)x^5+(\alpha+1)x^4+(\alpha^2+\alpha+1)x^3+(\alpha^2+\alpha+1)x^2+(\alpha^2+1)x$$

$$\check{p}_2(x) = (\alpha^2+\alpha)x^6+\alpha x^5+(\alpha^2+1)x^4+\alpha^2x^3+(\alpha+1)x^2+(\alpha^2+\alpha+1)x$$

Potom, ako sme k náhodne zvoleným polynómom $p_1, p_2, ..., p_t$ získali polynómy $\check{p}_1, \check{p}_2, ..., \check{p}_t$, teraz ešte vyberieme t náhodne zvolených prvkov z poľa $\mathbb{F}_{q^n}$, označených ako $\beta_1, \beta_2, ..., \beta_n$ a uvažujeme polynóm $Q(x)$, ktorý vznikne ako lineárna kombinácia polynómov $\check{p}_1, ..., \check{p}_t$, kde koeficienty lineárnej kombinácie sú práve $\beta_1, ..., \beta_t$, t.j.:

$$Q(x) = \sum_{i=1}^{t} \beta_i \check{p}_i(x) \tag{4}$$

V našom prípade, kde máme $t = 2$ si náhodne zvolíme 2 prvky: nech $\beta_1 = \alpha + \alpha^2$, $\beta_2 = \alpha$ a teda v našom prípade bude polynóm $Q(x)$:

$$\begin{aligned} Q(x) &= \beta_1\check{p}_1 + \beta_2\check{p}_2 = \\ &(\alpha+\alpha^2)((\alpha+1)x^6+(\alpha^2+1)x^5+(\alpha+1)x^4+(\alpha^2+\alpha+1)x^3+(\alpha^2+\alpha+1)x^2+(\alpha^2+1)x)+ \\ &+(\alpha)((\alpha^2+\alpha)x^6+\alpha x^5+(\alpha^2+1)x^4+\alpha^2x^3+(\alpha+1)x^2+(\alpha^2+\alpha+1)x) = \\ &= (\alpha^2+\alpha)x^6+(\alpha^2+\alpha+1)x^5+(\alpha^2+\alpha+1)x^3+\alpha x^2+(\alpha^2+\alpha)x \end{aligned} \tag{5}$$

Výsledné centrálne zobrazenie (trapdoor) v tomto modifikovanom HFE vznikne tak, že vezmeme HFE polynóm $H(x)$ a pripočítame k nemu polynóm $Q(x)$, t.j. $F(x) = H(x) + Q(x)$.

$$F(x) = H(x)+Q(x) = (\alpha^2+a)x^6+\alpha^2x^5+x^4+(\alpha+1)x^3+\alpha x^2+(\alpha^2+\alpha)x \tag{6}$$

Polynóm $F(x)$ je následne polynómom, ktorý reprezentuje centrálne zobrazenie (trapdoor). K nemu prislúchajúca sústava kvadratických polynómov nad základným poľom - v článku autori túto sústavu označujú aj ako $\hat{F}$:

- $f_1(x_1, x_2, x_3) = x_2x_3 + x_2 + x_3$
- $f_2(x_1, x_2, x_3) = x_1x_3 + x_3$
- $f_3(x_1, x_2, x_3) = x_1x_3 + x_1 + x_2 + x_3$

Teda na túto sústavu by sa následne aplikovali 2 afinné transformácie S, T, aby vznikol príslušný verejný kľúč.

2.2 Inverzia modifikovaného HFE

Keď sme si teda ukázali, ako sa modifikuje HFE pomocou perturbačného modifikátora, musíme si vysvetliť, ako sa bude následne toto modifikované HFE invertovať. Keďže polynóm $F(x)$, ktorý vznikol z HFE polynómu $H(x)$ perturbáciou môže byť potenciálne veľkého stupňa, klasický spôsob inverzie HFE - faktorizácia polynómu cez Berlekampov algoritmus - by mal príliš veľkú zložitosť.

Ak sa teda bavíme o invertovaní modifikovaného HFE, bavíme sa o situácii, že máme nejakým spôsobom zadanú hodnotu $y \in \mathbb{F}_{q^n}$ polynómu $F(x)$, t.j. $F(x) = y$ a snažíme sa nájsť také x, ktoré po dosadení do polynómu $F(x)$ dáva práve hodnotu y. Pri polynómoch nízkeho stupňa, ako je napr. HFE polynóm $H(x)$, by sa invertovanie riešilo tak, že uvažujeme polynóm $H(x) - y = 0$, ktorý faktorizujeme Berlekampovým algoritmom. V prípade polynómu $F(x)$ je však faktorizácia príliš náročná. Autori článku preto navrhujú 2 spôsoby, ako invertovať perturbované HFE, t.j. polynóm $F(x)$. Je dôležité si uvedomiť, že predpis $F(x) = y$ sa dá prepísať na $F(x) - y = 0$, resp. v prípade perturbovaného HFE je predpisom vlastne: $H(x) + \beta_1 \check{p}_1(x) + \beta_2 \check{p}_2(x) + ... + \beta_t \check{p}_t(x) - y = 0$.

2.2.1 Prvý spôsob invertovania - prehľadávanie všetkých možností

Ak máme danú nejakú hodnotu y, pre ktorú chceme invertovať $F(x)$, t.j. hľadáme také x, že $F(x) = y$, tak prvý spôsob inverzie $F(x)$ je založený na prehľadávaní všetkých hodnôt, ktoré môžu nadobúdať polynómy $\check{p}_i$. Postup je nasledovný:

1. Uvažuj polynóm $F(x) - y = H(x) + \beta_1 \check{p}_1(x) + \beta_2 \check{p}_2(x) + ... + \beta_t \check{p}_t(x) - y = 0$.
2. Vygeneruj náhodný vektor t hodnôt $(y_1, y_2, ..., y_t)$ nad poľom $\mathbb{F}_q$.
3. Nahraď v polynóme $F(x) - y$ hodnoty $\check{p}_1(x) = y_1, \check{p}_2(x) = y_2, ..., \check{p}_t(x) = y_t$, t.j. uvažuj polynóm $H(x) + \beta_1 y_1 + \beta_2 y_2 + ... + \beta_t y_t - y = 0$
4. Keďže polynóm $H(x) + \beta_1 y_1 + \beta_2 y_2 + ... + \beta_t y_t - y = 0$ je de-facto HFE polynóm, t.j. je nízkeho stupňa, invertuj polynóm $H(x) + \beta_1 y_1 + \beta_2 y_2 + ... + \beta_t y_t - y = 0$, t.j. nájdi také x', aby platilo $H(x') = y - \beta_1 y_1 - \beta_2 y_2 - ... - \beta_t y_t$
5. Ak sa také x' nepodarilo nájsť, skoč na krok č. 2.
6. Ak sa také x' podarilo nájsť, over, či pre všetky $i = 1, ..., t$ platí, že $\check{p}_i(x') = y_i$ teda, či nájdené x' je zároveň takou hodnotou, že po dosadení do polynómu $\check{p}_i(x)$ dostávaš práve hodnotu y_i na i-tej pozícii vo vektore zvolenom v kroku č. 2.
7. Ak pre nejaké $i = 1, ..., t$ **neplatí**, že $\check{p}_i(x') = y_i$, potom skoč na krok č. 2.
8. Ak pre x' platí, že pre všetky $i = 1, ..., t$, $\check{p}_i(x') = y_i$, potom x' je hľadanou inverziou $F(x) = y$.

V prípade, že je $F(x)$, resp. perturbovaný HFE, uvažovaný ako **podpisová schéma**, tak stačí nájsť jedno x také, že platí $F(x) = y$ - preto v kroku č.

2 stačí generovať náhodný vektor t hodnôt. V prípade, že by sme uvažovali perturbovaný HFE ako **šifrovaciu schému**, musíme nájsť **všetky** x také, že $F(x) = y$, preto by sa vo vyššie uvedenom postupne mohol krok č. 2 nahradiť cyklom, v ktorom sa postupne prechádzajú **všetky** vektory t hodnôt $(y_1, ..., y_t)$, t.j. prechádza sa q^t hodnôt.

Príklad: Uvažujme teda polynóm $F(x) = (\alpha^2 + a)x^6 + \alpha^2 x^5 + x^4 + (\alpha + 1)x^3 + \alpha x^2 + (\alpha^2 + \alpha)x$ nad poľom $\mathbb{F}_{2^3}$ a uvažujme, že ho chceme invertovať pre hodnotu $y = \alpha^2 + 1$. Hľadáme teda také x, aby $F(x) = \alpha^2 + 1$.

1. Vygenerujeme vektor $t = 2$ náhodných hodnôt z $\mathbb{F}_2$ ako $(y_1, y_2) = (0, 1)$.
2. Pre túto voľbu nadobudne polynóm $H(x) + \beta_1 \check{p}_1(x) + \beta_2 \check{p}_2(x) - y$ hodnotu $\alpha^2 x^3 + (1 + \alpha)x^5 + x^4 + (\alpha + \alpha^2)0 + (\alpha)1 - (\alpha^2 + 1) = \alpha^2 x^3 + (1 + \alpha)x^5 + x^4 + (\alpha^2 + \alpha + 1)$.
3. Keďže ide o de-facto HFE polynóm, použijeme Berlekampovu faktorizáciu, čím dostaneme rozklad: $\alpha^2 x^3 + (1+\alpha)x^5 + x^4 + (\alpha^2 + \alpha + 1) = (\alpha+1)(x + \alpha^2 + \alpha + 1)(x + \alpha + 1)^2(x^2 + x + \alpha^2 + \alpha + 1)$. Z toho vidíme, že korene tohto polynómu, a teda kandidáti na potenciálne riešenie inverzie $F(x) = y$, sú:
   (a) *Len pre istotu: to, že ktoré prvky sú korene polynómu vidíme z faktorizácie podľa toho, aké prvky poľa sa nachádzajú v* ***lineárnych faktoroch****, t.j. vo faktoroch typu $(x - c)$, kde c je nejaký prvok poľa. Koreňom je potom hodnota c.*
   (b) $x' = \alpha^2 + \alpha + 1$ (toto je kvôli faktoru $(x + \alpha^2 + \alpha + 1)$, z ktorého vyplýva, že koreňom je prvok $\alpha^2 + \alpha + 1$)
   (c) $x' = \alpha + 1$ (kvôli faktoru $(x + \alpha + 1)$)
4. Teraz musíme, overiť, čí $\check{p}_1(x') = 0$ a $\check{p}_2(x') = 1$. Žiaľ, vidíme, že:
   (a) Pre $x' = \alpha^2 + \alpha + 1$, $\check{p}_1(\alpha^2 + \alpha + 1) = 1$ a $\check{p}_2(\alpha^2 + \alpha + 1) = 0$
   (b) Pre $x' = \alpha + 1$, $\check{p}_1(\alpha + 1) = 1$ a $\check{p}_2(\alpha + 1) = 0$
5. Zistili sme, že pre vektor $(0, 1) = (y_1, y_2)$ sme nedostali **žiadne riešenie** pôvodného polynómu $F(x) = y$. Skúsime teda inú voľbu (y_1, y_2).
6. Vygenerujeme vektor $t = 2$ náhodných hodnôt z $\mathbb{F}_2$ ako $(y_1, y_2) = (1, 0)$.
7. Pre túto voľbu nadobudne polynóm $H(x) + \beta_1 \check{p}_1(x) + \beta_2 \check{p}_2(x) - y$ hodnotu $\alpha^2 x^3 + (1 + \alpha)x^5 + x^4 + (\alpha + \alpha^2)1 + (\alpha)0 - (\alpha^2 + 1) = \alpha^2 x^3 + (1 + \alpha)x^5 + x^4 + (\alpha + 1)$.
8. Keďže ide o de-facto HFE polynóm, použijeme Berlekampovu faktorizáciu, čím dostaneme rozklad: $\alpha^2 x^3 + (1 + \alpha)x^5 + x^4 + (\alpha + 1) = (\alpha + 1)(x + \alpha)(x^4 + \alpha^2 x^3 + (\alpha^2 + \alpha)x^2 + (\alpha^2 + \alpha + 1)x + \alpha^2 + 1)$. Z toho vidíme, že korene tohto polynómu, a teda kandidáti na potenciálne riešenie inverzie $F(x) = y$, sú:

(a) $x' = \alpha$

9. Teraz musíme, overiť, čí $\check{p}_1(x') = 0$ a $\check{p}_2(x') = 1$. A vidíme, že naozaj:

   (a) Pre $x' = \alpha$, $\check{p}_1(\alpha) = 1$ a $\check{p}_2(\alpha) = 0$

10. Zistili sme, že pre vektor $(1, 0) = (y_1, y_2)$ sme dostali **riešenie** pôvodného polynómu $F(x) = y$ ako $x = \alpha$. Platí teda, že $F(\alpha) = \alpha^2 + 1$. Podarilo sa nám teda úspešne invertovať perturbovaný HFE polynóm.

2.2.2 Druhý spôsob invertovania - cez projekciu

Druhý spôsob inverzie perturbovaného HFE spočíva v aplikácii operátora projekcie. Definícia projekcie hovorí, že je to lineárna transformácia (resp. lineárny operátor) P na nejakom vektorovom priestore, pre ktorú platí, že $P \circ P = P$, t.j. že ak ju viackrát aplikujeme na nejaký vektor, dostaneme rovnaký výsledok, ako keby sme ju aplikovali len jeden krát, t.j. $P^2 = P$ (taká transformácia sa nazýva aj idempotent).

Pre lepšiu ilustráciu, typickou projekciou nad vektorovým priestorom je napríklad, ľudovo povedané, "tvrdé nastavenie niektorých koordinátov na nula". Predstavme si klasický trojrozmerný vektorový priestor nad $\mathbb{R}$, t.j. $\mathbb{R}^3$, klasické vektory v priestore, ktorých všeobecné vyjadrenie by bolo (x_1, x_2, x_3). Ak by sme teraz definovali zobrazenie vektorov také, že zachová len prvé dve súradnice a z tretej vždy urobí nulu, dostaneme príklad projekcie z priestoru do roviny (lebo z trojrozmerných vektorov dostaneme de facto dvojrozmerné vektory s treťou súradnicou nulovou). Takýto operátor P by mal matematické vyjadrenie ako násobenie maticou:

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

Teda napríklad $P(1, 2, 3) = (1, 2, 0)$, $P(1, 2, -10) = (1, 2, 0)$. Aplikácia tohto typu projekcie (nulovanie niektorých hodnôt) nám bude osožná pri inverzii perturbovaného HFE.

Ako bolo už viackrát spomínané, centrálne zobrazenie perturbovaného HFE je tvorené polynómom $F(x) = H(x) + Q(x)$, ktorý je tvorený súčtom HFE polynómu $H(x)$ a polynómu $Q(x)$, ktorý predstavuje lineárnu kombináciu $Q(x) = \beta_1\check{p}_1 + ... + \beta_t\check{p}_t$. Pokúsme sa teraz nájsť taký špeciálny operátor projekcie, ktorý označíme Π_t, ktorý bude spĺňať dôležitú vlastnosť, a síce $\Pi_t(F(x)) = \Pi_t(H(x))$. Z uvedeného vyplýva:

1. Pôjde o také lineárne zobrazenie (projekciu), ktorú keď aplikujeme na výsledné hodnoty polynómov $H(x)$ alebo $F(x)$, dostaneme vždy tú istú hodnotu, teda $\Pi_t(F(x)) = \Pi_t(H(x))$.

2. Keďže má platiť $\Pi_t(F(x)) = \Pi_t(H(x))$ a $F(x) = H(x)+Q(x)$ a zároveň Π_t má byť lineárny operátor, tak z rovnosti $\Pi_t(F(x)) = \Pi_t(H(x) + Q(x)) = \Pi_t(H(x))$ vyplýva, že $\Pi_t(Q(x)) = 0$.

3. Projekcia $\Pi_t(x)$ bude teda také zobrazenie, ktoré **všetky potenciálne hodnoty** ktoré môže nadobúdať polynóm $Q(x)$ bude **zobrazovať na nulu**.

V našom prípade bude projekcia $\Pi_t(x)$ **polynóm** nad rozšírením $\mathbb{F}_{q^n}$. Keďže má mať tento polynóm vlastnosť, že **všetky možné výsledky** $Q(x)$ **zobrazuje na nulu**, položme si otázku, ako takýto polynóm $\Pi_t(x)$ nájsť.

Ak chceme nájsť polynóm, ktorý pre **vybrané vstupy** nadobúda nulové hodnoty, takýto polynóm zostrojíme pomerne jednoducho. Nech hodnoty, pre ktoré má polynóm nadobúdať nulové hodnoty, sú $\{c_1, c_2, ..., c_n\}$. Potom polynóm $f(x)$, ktorý vznikne ako:

$$f(x) = (x - c_1)(x - c_2)...(x - c_n)$$

je polynómom n-tého stupňa, pre ktorý určite $f(c_1) = ... = f(c_n) = 0$.

V našom prípade hľadáme polynóm $\Pi_t(x)$, ktorý bude nadobúdať nulové hodnoty pre všetky možné výstupy $Q(x)$. Keď si uvedomíme, že $Q(x)$ je definovaný ako:

$$Q(x) = \beta_1\check{p}_1(x) + \beta_2\check{p}_2(x) + ... + \beta_t\check{p}_t(x)$$

kde β_i sú pevne dané a každý polynóm $\check{p}_i(x)$ môžu nadobúdať len q hodnôt z poľa $\mathbb{F}_q$, tak potom **všetkých hodnôt**, ktoré môže nadobúdať $Q(x)$, je (maximálne) q^t. Všetky hodnoty, ktoré môže nadobúdať $Q(x)$ sú vlastne všetky lineárne kombinácie prvkov $\beta_1, ..., \beta_t$, t.j. prvky, ktoré dostaneme, keď v predpise

$$\beta_1\check{p}_1(x) + \beta_2\check{p}_2(x) + ... + \beta_t\check{p}_t(x)$$

dosadíme ako hodnoty polynómov $\check{p}_1(x), ..., \check{p}_t(x)$ všetky možné hodnoty - ktorých je q^t, pretože prvý polynóm môže nadobudnúť q hodnôt, druhý polynóm môže nadobudnúť q hodnôt, ..., t-ty (posledný polynóm) môže nadobudnúť q hodnôt.

Keď týmto spôsobom vypočítame všetkých q^t prvkov, označme ich $c_1, ..., c_{q^t}$, následne z nich vyrobíme polynóm

$$\Pi_t(x) = (x - c_1)(x - c_2)...(x - c_{q^t}) = \prod_{j=1}^{q^t}(x - c_j) \tag{7}$$

Príklad: Pre pripomenutie, v našom prípade máme HFE polynóm $H(x) = \alpha^2x^3 + (1 + \alpha)x^5 + x^4$, prvky $\beta_1 = \alpha + \alpha^2, \beta_2 = \alpha$ a polynómy $\check{p}_1(X), \check{p}_2(x)$:

$$\check{p}_1(x) = (\alpha{+}1)x^6{+}(\alpha^2{+}1)x^5{+}(\alpha{+}1)x^4{+}(\alpha^2{+}\alpha{+}1)x^3{+}(\alpha^2{+}\alpha{+}1)x^2{+}(\alpha^2{+}1)x$$

$$\check{p}_2(x) = (\alpha^2 + \alpha)x^6 + \alpha x^5 + (\alpha^2 + 1)x^4 + \alpha^2x^3 + (\alpha + 1)x^2 + (\alpha^2 + \alpha + 1)x$$

teda výsledné centrálne zobrazenie $F(x) = H(x) + Q(x) = H(x) + \beta_1\check{p}_1(x) + \beta_2\check{p}_2(x) =$

$$F(x) = (\alpha^2 + a)x^6 + \alpha^2x^5 + x^4 + (\alpha + 1)x^3 + \alpha x^2 + (\alpha^2 + \alpha)x$$

Keď teraz chceme pomocou vyššie uvedeného postupu nájsť polynóm projektie $\Pi_t(x)$, musíme najprv nájsť **všetky** lineárne kombinácie prvkov β_1, β_2, kde koeficienty lineárnej kombinácie sú prvky poľa $\mathbb{F}_q = \mathbb{F}_2$. V našom prípade teda hľadáme všetky prvky podľa predpisu:

$$\beta_1 p_1 + \beta_2 p_2$$

kde $p_1, p_2 \in \mathbb{F}_2$. Dokopy teda dostaneme 4 prvky:

1. $p_1 = 0, p_2 = 0 \rightarrow (\alpha + \alpha^2) * 0 + (\alpha) * 0 = 0$
2. $p_1 = 1, p_2 = 0 \rightarrow (\alpha + \alpha^2) * 1 + (\alpha) * 0 = 0 = \alpha + \alpha^2$
3. $p_1 = 0, p_2 = 1 \rightarrow (\alpha + \alpha^2) * 0 + (\alpha) * 0 = 1 = \alpha$
4. $p_1 = 1, p_2 = 1 \rightarrow (\alpha + \alpha^2) * 1 + (\alpha) * 0 = 1 = \alpha^2$

Následne zostrojíme polynóm $\Pi_t(x)$ podľa prepisu (7), kde za $c_1 = 0, c_2 = \alpha + \alpha^2, c_3 = \alpha, c_4 = \alpha^2$, t.j.:

$$\Pi_t(x) = (x - 0)(x - (\alpha + \alpha^2))(x - \alpha)(x - \alpha^2)$$

čo po vynásobení dáva výsledok:

$$\Pi_t(x) = x + x^2 + x^4$$

Ľahko sa presvedčíme (napr. dosadením a vyhodnotením), že tento polynóm nadobúda nulové hodnoty pre prvky $0, \alpha + \alpha^2, \alpha, \alpha^2$.

Všimnite si, že tento polynóm $\Pi_t(x)$ je závislý len na prvkoch $\beta_1, ..., \beta_t$ a teda sa jeho predpis nemení pre rôzne inverzie toho istého centrálneho zobrazenia, t.j. sa dá vypočítať len jeden krát - pri generovaní kľúča. Ak teda chceme invertovať perturbované zobrazenie $F(x) = y$ pre dané y a máme k dispozícii projekciu $\Pi_t(x)$, tak potom môžeme využiť vlastnosť $\Pi_t(F(x)) = \Pi_t(H(x)) = \Pi_t(y)$, konkrétne fakt, že $\Pi_t(H(x)) = \Pi_t(y)$. Výraz $\Pi_t(H(x))$ je totižto polynóm, ktorý je stupňa maximálne $q^t d$, teda síce väčšieho stupňa ako $H(x)$, avšak potenciálne oveľa menšieho ako $F(x)$. To znamená, že ak vyjadríme $\Pi_t(H(x))$ ako polynóm, t.j. vypočítame zloženie polynómov $\Pi_t(x) \circ H(x)$, a zároveň vypočítame hodnotu $\Pi_t(y)$, tak sa môžeme pokúsiť o nájdenie riešenia vzťahu $\Pi_t(H(x)) - \Pi_t(y) = 0$ pomocou faktorizácie polynómu $\Pi_t(H(x)) - \Pi_t(y)$ Berlekampovým algoritmom, z ktorej vidíme korene $\Pi_t(H(x)) - \Pi_t(y)$ (a teda hodnoty pre ktoré $\Pi_t(H(x)) - \Pi_t(y) = 0$). Medzi faktormi, resp. koreňmi, sa bude nachádzať aj hľadané riešenie pôvodného systému $F(x) = y$. To, ktoré riešenie je správne, je nutné overiť podľa vzťahu $F(x) = y$.

Príklad Ak sme teda zistili, že projekčný polynóm $\Pi_t(x) = x + x^2 + x^4$ a chceme invertovať $F(x) = y$ pre dané $y = 1 + \alpha^2$, teda hľadáme také x, aby $F(x) = 1 + \alpha^2$, tak najprv vypočítame $\Pi_t(H(x))$, čiže do polynómu $\Pi_t(x)$ dosadíme za $x = H(x) = \alpha^2 x^3 + (1 + \alpha)x^5 + x^4$, teda:

$$\Pi_t(H(x)) = (\alpha^2 x^3 + (1+\alpha)x^5 + x^4) + (\alpha^2 x^3 + (1+\alpha)x^5 + x^4)^2 + (\alpha^2 x^3 + (1+\alpha)x^5 + x^4)^4$$

Z čoho po úpravách dostávame polynóm:

$$\Pi_t(H(x)) = x^6 + x^5 + x^4 + x^3 + x^2 + x$$

Poznámka: Pri úpravách polynómu musíme zohľadniť 2 veci:

1. Keďže sme v poli $\mathbb{F}_{2^3}$, ktoré vzniklo ako rozšírenie poľa $\mathbb{F}_2$ pomocou ireducibilného polynómu $1 + x + x^3$, tak nesmieme zabudnúť, že $\alpha^3 = \alpha + 1$
2. Keďže sme v poli $\mathbb{F}_{2^3}$, t.j. v poli, ktoré má 8 prvkov, tak platí identita: $X^8 = X$, kde X je ľubovoľný prvok poľa $\mathbb{F}_{2^3}$. Preto aj výsledný polynóm $\Pi_t(H(x))$ je menšieho stupňa ako 8, keďže každý člen aspoň 8 stupňa môžeme redukovať, $X^8 = X, X^9 = X^2, ...$

Keď aplikujeme projekčný polynóm na y dostaneme $\Pi_t(y) = \Pi_t(1 + \alpha^2) = 1$. Uvažujeme teda faktorizáciu polynómu $\Pi_t(H(x)) - \Pi_t(y)$, čo podľa napríklad Berlekampovho algoritmu:

$$x^6+x^5+x^4+x^3+x^2+x-1 = (x+\alpha)(x+\alpha+1)(x+\alpha^2)(x+\alpha^2+1)(x+\alpha^2+\alpha)(x+\alpha^2+\alpha+1)$$

Dostávame teda dokopy 6 kandidátov na inverziu perturbovaného HFE, t.j. $F(x) = 1 + \alpha^2$. Hľadáme takého, pre ktorého platí, že $F(x) = 1 + \alpha^2$:

1. $\alpha, F(\alpha) = \alpha^2 + 1$
2. $\alpha + 1, F(\alpha + 1) = 1$
3. $\alpha^2, F(\alpha^2) = \alpha^2 + \alpha + 1$
4. $\alpha^2 + 1, F(\alpha^2 + 1) = \alpha^2 + 1$
5. $\alpha^2 + \alpha, F(\alpha^2 + \alpha) = \alpha + 1$
6. $\alpha^2 + \alpha + 1, F(\alpha^2 + \alpha + 1) = 1$

Vidíme, že sa nám podarilo nájsť 2 kandidátov, ktorý túto vlastnosť spĺňajú, konkrétne α a $\alpha^2 + 1$. Obe hodnoty by teda boli rovnocenné riešenia inverzie centrálneho zobrazenia $F(x) = 1 + \alpha^2$.

Aby sme zhrnuli tento spôsob inverzie perturbovaného HFE, ak máme danú nejakú hodnotu y, pre ktorú chceme invertovať $F(x)$, t.j. hľadáme také x, že $F(x) = y$, tak druhý spôsob inverzie $F(x)$ je založený na aplikácii tzv. projekcie Π_t. Postup je nasledovný:

1. Pre dané hodnoty $\beta_1, \beta_2, .., .\beta_t$ vypočítaj všetky ich lineárne kombinácie pomocou t koeficientov z poľa $\mathbb{F}_q$, t.j. urč všetky hodnoty tvaru $\sum_{i=1}^{t} \beta_i p_i$, $p_i \in \mathbb{F}_q$. Inak napísané, vypočítaj množinu C prvkov poľa $\mathbb{F}_{q^n}$, ktorá je daná ako $C = \{c_j \mid c_j = \sum_{i=1}^{t} \beta_i p_i,\ p_i \in \mathbb{F}_q\}$
2. Vypočítaj projekčný polynóm $\Pi_t(x) = \prod_{j \in C} (x - c_j) = (x - c_1)...(x - c_{q^t})$

3. Vypočítaj aplikáciu projekčného polynómu na HFE polynóm, $\Pi_t(H(x))$.
4. Vypočítaj aplikáciu projekčného polynómu na hodnotu y, $\Pi_t(y)$.
5. Vyrieš systém $\Pi_t(H(x)) - \Pi_t(y) = 0$, napr. nájdením koreňov polynómu $\Pi_t(H(x)) - \Pi_t(y)$ pomocou faktorizácie Berlekampovym algoritmom.
6. Korene $\Pi_t(H(x)) - \Pi_t(y)$ označ ako x'. Platí pre ne, že $\Pi_t(H(x')) = \Pi_t(y)$
7. Z množiny nájdených x' nájdi také, pre ktoré platí $F(x') = y$. To je potom hľadanou inverziou systému $F(x) = y$.

V prípade, že je $F(x)$, resp. perturbovaný HFE, uvažovaný ako **podpisová schéma**, tak stačí nájsť jedno x také, že platí $F(x) = y$ - preto v kroku č. 7 stačí zobrať prvú hodnotu, kde $F(x') = y$. V prípade, že by sme uvažovali perturbovaný HFE ako **šifrovaciu schému**, musíme nájsť **všetky** x' také, že $F(x') = y$.

2.3 Tvorba $\check{p}_i$ polynómu z polynómu p_i

V tejto sekcii sa ešte pristavíme pri tom, ako k polynómu $p_i(x_1, ..., x_n)$ nad poľom $\mathbb{F}_q$ vyrobíme polynóm $\check{p}_i$ nad poľom $\mathbb{F}_{q^n}$.

2.3.1 Lagrangeov interpolačný polynóm

Prvou metódou, ktorou je možné k polynómu $p_i(x_1, ..., x_n)$ nad poľom $\mathbb{F}_q$ vyrobiť polynóm $\check{p}_i$ nad poľom $\mathbb{F}_{q^n}$, ktorý realizuje de-facto to isté zobrazenie, je pomocou Lagrangeovho interpolačného polynómu - pravdepodobne ste sa s ním stretli na niektorom z predmetov počas štúdia na FEI STU.

Vo všeobecnosti, (Lagrangeov) interpolačný polynóm je metóda interpolácie, t.j. ak máme daných n párov hodnôt $\{(x_i, y_i)\}_{i=0}^{n}$, potom interpolačný polynóm $f(x)$ je taký polynóm, pre ktorý platí $f(x_i) = y_i$ pre $i = 0, ..., n$. V ľudskej reči interpoláciou vznikne taký polynóm, ktorý má tú vlastnosť, že pre zadané páry hodnôt (x_i, y_i) vždy pre x_i nadobúda hodnoty y_i. Lagrangeov interpolačný polynóm potom pre n párov hodnôt $\{(x_i, y_i)\}_{i=0}^{n}$ vytvorí takýto polynóm podľa nasledovného predpisu:

$$f(x) = \sum_{i=0}^{n} \left(y_i * \left(\prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{x - x_j}{x_i - x_j} \right) \right) \tag{8}$$

V našom prípade ho teda vieme využiť tak, že ak vieme, že chceme nájsť taký polynóm $\check{p}_1(x)$ nad poľom $\mathbb{F}_{2^3}$, ktorý predstavuje zobrazenie:

- $\check{p}_1(0) = 0$
- $\check{p}_1(1) = 0$
- $\check{p}_1(\alpha) = 1$

- $\check{p}_1(\alpha^2) = 0$
- $\check{p}_1(1+\alpha) = 1$
- $\check{p}_1(\alpha+\alpha^2) = 0$
- $\check{p}_1(1+\alpha+\alpha^2) = 1$
- $\check{p}_1(1+\alpha^2) = 1$

tak si vytvoríme množinu párov hodnôt $\{(0,0),(1,0),(\alpha,1),(\alpha^2,0),(1+\alpha,1),(\alpha+\alpha^2,0),(1+\alpha+\alpha^2,1),(1+\alpha^2,1)\}$ pre ktoré následne pomocou interpolácie podľa vzťahu (8) nájdeme polynomiálny predpis, ktorý tvorí práve $\check{p}_1(x)$:

$$\check{p}_1(x) = 0*(\frac{x-1}{0-1}*\frac{x-\alpha}{0-\alpha}*\frac{x-\alpha^2}{0-\alpha^2}*\frac{x-(1+\alpha)}{0-(1+\alpha)}*\frac{x-(\alpha+\alpha^2)}{0-(\alpha+\alpha^2)}*\frac{x-(1+\alpha+\alpha^2)}{0-(1+\alpha+\alpha^2)}*\frac{x-(1+\alpha^2)}{0-(1+\alpha^2)})+$$
$$0*(\frac{x-0}{1-0}*\frac{x-\alpha}{1-\alpha}*\frac{x-\alpha^2}{1-\alpha^2}*\frac{x-(1+\alpha)}{1-(1+\alpha)}*\frac{x-(\alpha+\alpha^2)}{1-(\alpha+\alpha^2)}*\frac{x-(1+\alpha+\alpha^2)}{1-(1+\alpha+\alpha^2)}*\frac{x-(1+\alpha^2)}{1-(1+\alpha^2)})+$$
$$1*(\frac{x-0}{\alpha-0}*\frac{x-1}{\alpha-1}*\frac{x-\alpha^2}{\alpha-\alpha^2}*\frac{x-(1+\alpha)}{\alpha-(1+\alpha)}*\frac{x-(\alpha+\alpha^2)}{\alpha-(\alpha+\alpha^2)}*\frac{x-(1+\alpha+\alpha^2)}{\alpha-(1+\alpha+\alpha^2)}*\frac{x-(1+\alpha^2)}{\alpha-(1+\alpha^2)})+$$
$$\dots$$
$$1*(\frac{x-0}{(1+\alpha^2)-0}*\frac{x-1}{(1+\alpha^2)-1}*\frac{x-\alpha}{(1+\alpha^2)-\alpha}*\frac{x-\alpha^2}{(1+\alpha^2)-\alpha^2}*\frac{x-(1+\alpha)}{(1+\alpha^2)-(1+\alpha)}*$$
$$*\frac{x-(\alpha+\alpha^2)}{(1+\alpha^2)-(\alpha+\alpha^2)}*\frac{x-(1+\alpha+\alpha^2)}{(1+\alpha^2)-(1+\alpha+\alpha^2)}) =$$
$$= (\alpha+1)x^6+(\alpha^2+1)x^5+(\alpha+1)x^4+(\alpha^2+\alpha+1)x^3+(\alpha^2+\alpha+1)x^2+(\alpha^2+1)x$$

2.3.2 Hľadanie koeficientov $\check{p}_i(x)$ cez lineárnu algebru

Hľadanie polynómu $\check{p}_i(x)$ je možné aj alternatívne - pomocou lineárnej algebry riešením špeciálnej sústavy lineárnych rovníc. Tento spôsob je efektívnejší než počítanie pomocou Lagrangeovho polynómu, pretože potrebuje menší počet párov $(x, y = \check{p}(x))$, pretože využíva fakt, že ak $p(x_1, x_2, ..., x_n)$ je kvadratický polynóm o n neurčitých nad základným poľom $\mathbb{F}_q$, tak potom príslušný polynóm $\check{p}(x)$ nad rozšírením $\mathbb{F}_{q^n}$ bude určite tvaru:

$$\check{p}_i(x) = \sum_{\substack{0\le i\le j\\ q^i+q^j<n}} A_{i,j}x^{q^i+q^j} + \sum_{\substack{0\le i\\ q^i<n}} B_i x^{q^i} + C,$$

kde $A_{i,j}, B_i, C \in \mathbb{F}_{q^n}$. Špeciálne, v prípade polí charakteristiky 2 (čo je aj náš prípad) má polynóm $\check{p}(x)$ o niečo jednoduchší tvar:

$$\check{p}_i(x) = \sum_{\substack{0\le i< j\\ 2^i+2^j<n}} A_{i,j}x^{2^i+2^j} + \sum_{\substack{0\le i\\ 2^i<n}} B_i x^{2^i} + C,$$

kde $A_{i,j}, B_i, C \in \mathbb{F}_{2^n}$. Rozdiel je v tom, že členy $A_{i,j}$ môžu mať v prvom prípade $i = j$, v prípade polí charakteristiky 2 táto situácia nie je relevantná (pretože člen $A_{i,i}x^{2^i+2^i} = A_{i,i}x^{2*2^i} = A_{i,i}x^{2^{i+1}}$ je de facto členom typu $B_{i+1}x^{2^{i+1}}$).

V ďalšom texte budeme uvažovať polia charakteristiky 2, avšak úvahy sú rovnako aplikovateľné aj na iné konečné polia. Ak máme teda kvadratický polynóm $p(x_1, x_2, ..., x_n)$ nad poľom $\mathbb{F}_2$ a chceme nájsť jeho ekvivalentnú reprezentáciu $\check{p}(x)$ nad poľom $\mathbb{F}_{2^n}$, stačí nám uvedomiť si, že vlastne hľadáme **koeficienty** $A_{i,j}, B_i, C$ polynómu v tvare

$$\check{p}_i(x) = \sum_{\substack{0 \le i < j \\ 2^i + 2^j < n}} A_{i,j} x^{2^i+2^j} + \sum_{\substack{0 \le i \\ 2^i < n}} B_i x^{2^i} + C, \tag{9}$$

Ak si teda vygenerujeme dostatočný počet párov hodnôt nad základným poľom $\mathbb{F}_2$, $((x_1, x_2, ..., x_n), p(x_1, x_2, ..., x_n))$, resp. k nim prislúchajúcich hodnôt v $\mathbb{F}_{2^n}$ vo všeobecnosti v tvare $(x, y = \check{p}(x))$, vieme hľadať koeficienty $A_{i,j}, B_i, C$ riešením jednoduchej sústavy lineárnych rovníc. Stačí, ak totiž do predpisu (9) dosadíme nejaký známy pár (x, y) a dostaneme lineárnu rovnicu v neznámych $A_{i,j}, B_i, C$.

Príklad Vezmime náš príklad, t.j. pole $\mathbb{F}_2$, jeho rozšírenie $\mathbb{F}_{2^3}$ a polynóm nad základným poľom $p_1(x_1, x_2, x_3) = x_1x_3 + x_2x_3 + x_2^2$, tak hľadáme polynóm $\check{p}_1(x)$, pre ktorý vieme, že musí platiť:

- $\check{p}_1(0) = 0$
- $\check{p}_1(1) = 0$
- $\check{p}_1(\alpha) = 1$
- $\check{p}_1(\alpha^2) = 0$
- $\check{p}_1(1 + \alpha) = 1$
- $\check{p}_1(\alpha + \alpha^2) = 0$
- $\check{p}_1(1 + \alpha + \alpha^2) = 1$
- $\check{p}_1(1 + \alpha^2) = 1$

Taktiež vieme, že predpis polynómu $\check{p}_1(x)$ bude vo všeobecnosti, podľa predpisu (9):

$$\check{p}_1(x) = A_{0,1}x^3 + A_{0,2}x^5 + A_{1,2}x^6 + B_0x + B_1x^2 + B_2x^4 + C$$

Pomocou známych párov hodnôt $(x, y = \check{p}_1(x))$ vieme postupne získať množinu lineárnych rovníc tak, že $y = \check{p}_1(x)$ tvorí pravú stranu rovnice a x dosadíme do predpisu:

- Zo vzťahu $\check{p}_1(0) = 0$ dostaneme rovnicu:

$$0 = C$$

- Zo vzťahu $\check{p}_1(1) = 0$ dostaneme rovnicu:

  $$0 = A_{0,1} + A_{0,2} + A_{1,2} + B_0 + B_1 + B_2 + C$$

- Zo vzťahu $\check{p}_1(\alpha) = 1$ dostaneme rovnicu:

  $$1 = A_{0,1}\alpha^3 + A_{0,2}\alpha^5 + A_{1,2}\alpha^6 + B_0\alpha + B_1\alpha^2 + B_2\alpha^4 + C$$

- $\check{p}_1(\alpha^2) = 0$

  $$0 = A_{0,1}\alpha^6 + A_{0,2}\alpha^{10} + A_{1,2}\alpha^{12} + B_0\alpha^2 + B_1\alpha^4 + B_2\alpha^8 + C$$

- $\check{p}_1(1 + \alpha) = 1$

  $$1 = A_{0,1}(1+\alpha)^3 + A_{0,2}(1+\alpha)^5 + A_{1,2}(1+\alpha)^6 + B_0(1+\alpha) + B_1(1+\alpha)^2 + B_2(1+\alpha)^4 + C$$

- $\check{p}_1(\alpha + \alpha^2) = 0$

  $$0 = A_{0,1}(\alpha+\alpha^2)^3 + A_{0,2}(\alpha+\alpha^2)^5 + A_{1,2}(\alpha+\alpha^2)^6 + B_0(\alpha+\alpha^2) + B_1(\alpha+\alpha^2)^2 + B_2(\alpha+\alpha^2)^4 + C$$

- $\check{p}_1(1 + \alpha + \alpha^2) = 1$

  $$1 = A_{0,1}(1+\alpha+\alpha^2)^3 + A_{0,2}(1+\alpha+\alpha^2)^5 + A_{1,2}(1+\alpha+\alpha^2)^6 + B_0(1+\alpha+\alpha^2) + B_1(1+\alpha+\alpha^2)^2 + B_2(1+\alpha+\alpha^2)^4 + C$$

  V tomto momente máme 7 lineárnych rovníc o 7 neznámych. Ich riešením dostaneme hodnoty $A_{0,1}, A_{0,2}, A_{1,2}, B_0, B_1, B_2, C$

- $\check{p}_1(1 + \alpha^2) = 1$

  Ak by nám predchádzajúca sústava nedávala jednoznačné riešenie, môžeme ešte pridať rovnicu z tohto páru:

  $$1 = A_{0,1}(1+\alpha^2)^3 + A_{0,2}(1+\alpha^2)^5 + A_{1,2}(1+\alpha^2)^6 + B_0(1+\alpha^2) + B_1(1+\alpha^2)^2 + B_2(+\alpha^2)^4 + C$$

Celkovo teda dostávame lineárnu sústavu 7 rovníc o 7 premenných nad poľom $\mathbb{F}_{2^3}$ - len pre istotu, to znamená, že hodnoty (koeficienty) rovníc sú prvky $\mathbb{F}_{2^3}$, t.j. $0, 1, \alpha, ..., \alpha^2 + \alpha + 1$:

$$0 = C$$

$$0 = A_{0,1} + A_{0,2} + A_{1,2} + B_0 + B_1 + B_2 + C$$

$$1 = A_{0,1}\alpha^3 + A_{0,2}\alpha^5 + A_{1,2}\alpha^6 + B_0\alpha + B_1\alpha^2 + B_2\alpha^4 + C$$

$$0 = A_{0,1}\alpha^6 + A_{0,2}\alpha^{10} + A_{1,2}\alpha^{12} + B_0\alpha^2 + B_1\alpha^4 + B_2\alpha^8 + C$$

$$1 = A_{0,1}(1+\alpha)^3 + A_{0,2}(1+\alpha)^5 + A_{1,2}(1+\alpha)^6 + B_0(1+\alpha) + B_1(1+\alpha)^2 + B_2(1+\alpha)^4 + C$$

$$1 = A_{0,1}(1+\alpha+\alpha^2)^3 + A_{0,2}(1+\alpha+\alpha^2)^5 + A_{1,2}(1+\alpha+\alpha^2)^6 + B_0(1+\alpha+\alpha^2) + B_1(1+\alpha+\alpha^2)^2 + B_2(1+\alpha+\alpha^2)^4 + C$$

$$0 = A_{0,1}(\alpha+\alpha^2)^3 + A_{0,2}(\alpha+\alpha^2)^5 + A_{1,2}(\alpha+\alpha^2)^6 + B_0(\alpha+\alpha^2) + B_1(\alpha+\alpha^2)^2 + B_2(\alpha+\alpha^2)^4 + C$$

Riešením tejto sústavy by sme dostali nasledovné hodnoty premenných:

- $C = 0$
- $B_0 = \alpha^2 + 1$
- $B_1 = \alpha^2 + \alpha + 1$
- $B_2 = \alpha + 1$
- $A_{0,1} = \alpha^2 + \alpha + 1$
- $A_{0,2} = \alpha^2 + 1$
- $A_{1,2} = \alpha + 1$

To znamená, že sme **našli koeficienty** polynómu $\check{p}_1(x)$. Výsledný polynóm by teda bol:

$$\check{p}_1(x) = (\alpha+1)x^6+(\alpha^2+1)x^5+(\alpha+1)x^4+(\alpha^2+\alpha+1)x^3+(\alpha^2+\alpha+1)x^2+(\alpha^2+1)x$$

čo je rovnaký výsledok ako v predchádzajúcej sekcii, takže postup bol úspešný.

2.3.3 Hľadanie koeficientov $\check{p}_i(x)$ podľa KS

Hľadanie polynómu $\check{p}_i(x)$ je možné aj ďalším spôsobom, podľa postupu, ktorý navrhujú Kipnis a Shamir v článku *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*. Podľa experimentov je však tento spôsob menej efektívny než predchádzajúci, preto ho tu neuvádzame a necháme na čitateľke, aby si hov prípade záujmu našla v príslušnej literatúre.

3 UOV

3.1 Tvorba modifikovaného UOV

Ako je známe, HFE pracuje nad nejakým konečným poľom $\mathbb{F}_q$. Uvažujme teda, že v našom prípade bude základné pole $\mathbb{F}_{2^3} = GF(2^3)$. Toto konečné pole vzniklo z poľa $GF(2)$ pomocou primitívneho polynómu $x^3 + x + 1$ nad $GF(2)$. Len pre istotu uvádzame prvky poľa $GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1\}$. Naschvál neuvažujeme ako základné pole len $GF(2)$, ale trochu komplikovanejšie pole $GF(2^3)$, pretože aj autori článku o perturbovanom UOV odporúčajú pracovať nad poliami typu $GF(p^n)$.

Keď teda máme zvolené konečné pole, nad ktorým vytvoríme UOV, tak sa zvolia 2 parametre: h a v, udávajúce počet olejových a octových neurčitých. Spolu bude teda $n = h + v$ neurčitých, ktoré sa rozdelia do 2 skupín:

1. h-neurčitých $x_1, x_2, ..., x_h$, tzv. olejové neurčité,

2. v-neurčitých $x'_1, x'_2, ..., x'_v$, tzv. octové neurčité.

Štandardný UOV systém je potom tvorený h kvadratickými polynómami nad poľom $\mathbb{F}_q$ v $h + v$ neurčitých v tvare:

$$\begin{aligned} y_1 &= \sum_{1 \leq i \leq j \leq v} a_{1ij} x'_i x'_j + \sum_{\substack{1 \leq i \leq h \\ 1 \leq j \leq v}} b_{1ij} x_i x'_j \\ &... \\ y_h &= \sum_{1 \leq i \leq j \leq v} a_{hij} x'_i x'_j + \sum_{\substack{1 \leq i \leq h \\ 1 \leq j \leq v}} b_{hij} x_i x'_j \end{aligned} \tag{10}$$

teda členy (termy) jednotlivých polynómov sú v takých tvaroch, že obsahujú medzi sebou vynásobené alebo octové neurčité, alebo octovú a olejovú neurčitú; neobsahujú členy tvorené súčinom olejových neurčitých. Koeficienty termov sú z príslušného poľa $\mathbb{F}_q$.

V našom prípade uvažujme, že $h = v = 3$, t.j. náš UOV systém bude obsahovať 3 polynómy o 3 olejových a 3 octových neurčitých. Keďže u nás $q = 2^3$, jednotlivé koeficienty polynómov budú z poľa $\mathbb{F}_{2^3}$. Napríklad nech takýto UOV systém je nasledovný:

1. $y_1 = \alpha {x'_1}^2 + (\alpha+1) x'_1 x'_3 + \alpha^2 x'_2 x'_3 + {x'_3}^2 + \alpha x'_1 x_1 + x'_3 x_1 + x'_2 x_2 + \alpha^2 x'_1 x_3 + (\alpha^2 + 1) x'_2 x_3 + x'_3 x_3$

2. $y_2 = \alpha x'_1 x'_2 + (\alpha + 1) x'_1 x'_3 + (\alpha^2 + \alpha) x'_2 x'_3 + (\alpha^2 + 1) {x'_3}^2 + x'_1 x_1 + (\alpha + 1) x'_2 x_1 + \alpha^2 x'_1 x_2 + \alpha x'_3 x_2 + (\alpha + 1) x'_2 x_3$

3. $y_3 = \alpha {x'_2}^2 + x'_1 x'_3 + \alpha {x'_3}^2 + \alpha x'_2 x_2 + x'_3 x_2 + \alpha^2 x'_1 x_3 + \alpha^2 x'_2 x_3 + \alpha x'_3 x_3$

Autori článku o perturbácii označujú takýto UOV systém ako $y = U(x, x')$, resp. ako homogénny $(h+v, h)$ polynomiálny systém druhého stupňa (*homogénny* znamená, že všetky členy sú rovnakého stupňa - v našom prípade druhého stupňa). V označení $(h + v, h)$ je prvé číslo $h + v$ počet neurčitých, druhé číslo h počet polynómov.

Modifikátor $\hat{+}$ schémy UOV funguje nasledovným spôsobom. Najprv sa zvolí parameter t, ktorým je nejaké celé číslo. Následne sa vygeneruje t náhodných kvadratických polynómov $z_1, ..., z_t$ nad základným poľom $\mathbb{F}_q$ v **olejových** x_1, ... , x_h neurčitých. Nech teda v našom prípade je $t = 2$ a náhodné kvadratické polynómy z_1, z_2 nad poľom $\mathbb{F}_{2^3}$ sú:

- $z_1(x_1, x_2, x_3) = x_1 x_3 + (1 + \alpha) x_2 x_3 + \alpha^2 x_2^2$
- $z_2(x_1, x_2, x_3) = (1 + \alpha + \alpha^2) x_1 x_2 + (1 + \alpha^2) x_1 x_3 + x_1^2 + \alpha x_3^2$

Takýto systém 2 polynómov o 3 neurčitých by sa v duchu značenia autorov označil ako $(h, t) = (3, 2)$ polynomiálny systém. Autori ho v článku označujú aj

ako $z = Q(x)$, t.j. polynómy z_1, z_2 tvoria systém označený ako Q a ich výstupné 2 hodnoty vektor z.

Po vygenerovaní polynómov $z_1, ..., z_t$ teraz ku každému polynómu $y_1, ..., y_h$ pôvodného UOV pripočítame **náhodnú lineárnu kombináciu** polynómov $z_1, ..., z_t$. Formálne sa to zapíše ako:

$$\begin{aligned} y_1 &= \sum_{1\leq i\leq j\leq v} a_{1ij}x'_ix'_j + \sum_{\substack{1\leq i\leq h\\ 1\leq j\leq v}} b_{1ij}x_ix'_j + \sum_{1\leq i\leq t}\lambda_{1i}z_i \\ &... \\ y_h &= \sum_{1\leq i\leq j\leq v} a_{hij}x'_ix'_j + \sum_{\substack{1\leq i\leq h\\ 1\leq j\leq v}} b_{hij}x_ix'_j + \sum_{1\leq i\leq t}\lambda_{hi}z_i \end{aligned} \tag{11}$$

V našom prípade, kde máme $t = 2$ teda ku každému polynómu v UOV pripočítame nejakú lineárnu kombináciu polynómov z_1 a z_2. Jednotlivé koeficienty λ zvolíme napríklad takto:

1. $\lambda_{11} = 1, \lambda_{12} = \alpha$ (koeficienty pre lineárnu kombináciu pre súčet k polynómu y_1
2. $\lambda_{21} = 1 + \alpha^2, \lambda_{22} = \alpha + \alpha^2$ (koeficienty pre lineárnu kombináciu pre súčet k polynómu y_2
3. $\lambda_{31} = 0, \lambda_{32} = \alpha^2$ (koeficienty pre lineárnu kombináciu pre súčet k polynómu y_3

To znamená, že výsledné perturbované UOV zobrazenie, t.j. UOV$\hat{+}$ zobrazenie, bude mať podobu:

$$\begin{aligned} y_1 &= \alpha x_1'^2 + (\alpha+1)x'_1x'_3 + \alpha^2x'_2x'_3 + x_3'^2 + \\ &\quad \alpha x'_1x_1 + x'_3x_1 + x'_2x_2 + \alpha^2x'_1x_3 + (\alpha^2+1)x'_2x_3 + x'_3x_3 + \\ &\quad x_1x_3 + (1+\alpha)x_2x_3 + \alpha^2x_2^2 + \\ &\quad \alpha((1+\alpha+\alpha^2)x_1x_2 + (1+\alpha^2)x_1x_3 + x_1^2 + \alpha x_3^2) \\ y_2 &= \alpha x'_1x'_2 + (\alpha+1)x'_1x'_3 + (\alpha^2+\alpha)x'_2x'_3 + (\alpha^2+1)x_3'^2 + \\ &\quad x'_1x_1 + (\alpha+1)x'_2x_1 + \alpha^2x'_1x_2 + \alpha x'_3x_2 + (\alpha+1)x'_2x_3 \\ &\quad (1+\alpha^2)(x_1x_3 + (1+\alpha)x_2x_3 + \alpha^2x_2^2) + \\ &\quad (\alpha+\alpha^2)((1+\alpha+\alpha^2)x_1x_2 + (1+\alpha^2)x_1x_3 + x_1^2 + \alpha x_3^2) \\ y_3 &= \alpha x_2'^2 + x'_1x'_3 + \alpha x_3'^2 + \\ &\quad \alpha x'_2x_2 + x'_3x_2 + \alpha^2x'_1x_3 + \alpha^2x'_2x_3 + \alpha x'_3x_3 \\ &\quad (\alpha^2)((1+\alpha+\alpha^2)x_1x_2 + (1+\alpha^2)x_1x_3 + x_1^2 + \alpha x_3^2) \end{aligned}$$

Výsledkom je teda sústava h polynómov o $h + v$ neurčitých, t.j. $(h + v, h)$ polynomiálny systém. Pripočítanie lineárnych kombinácií polynómov $z_1, ..., z_t$

spôsobí, že sa stratí UOV štruktúra, t.j. polynómy už budú obsahovať aj termy, ktoré obsahujú vynásobené olejové neurčité. Výsledný systém, t.j. UOV$\hat{+}$ autori označujú aj ako $F(x, x')$, t.j. ako polynomiálny systém obsahujúci octové x' a olejové x neurčité - avšak, ako sme neraz zdôraznili, teraz už obsahuje aj členy s len olejovými neurčitými. To, že tento systém vznikol z pôvodného UOV systému $U(x, x')$ pripočítaním lineárnych kombinácií $z_1, ..., z_t$ autori označujú aj ako $F(x, x') = U(x, x') + \Lambda(Q(x))$, kde Λ predstavuje nejaký (t, h) homogénny lineárny polynomiálny systém (v podstate to len formálne popisuje h lineárnych kombináciu $z_1, ..., z_t$).

Teda na túto sústavu $F(x, x')$ by sa následne aplikovali 2 afinné transformácie S, T, aby vznikol príslušný verejný kľúč.

3.2 Inverzia modifikovaného UOV

Keď sme si teda ukázali, ako sa modifikuje UOV pomocou perturbačného modifikátora, musíme si vysvetliť, ako sa bude následne toto modifikované UOV invertovať. Keďže systém $F(x, x')$, ktorý vznikol z UOV systému polynómu $U(x, x')$ perturbáciou už neobsahuje štruktúru, kde by po dosadení octových neurčitých vznikol lineárny systém v olejových neurčitých, klasický spôsob inverzie UOV nebude fungovať.

Ak sa teda bavíme o invertovaní modifikovaného UOV, bavíme sa o situácii, že máme nejakým spôsobom zadaných h hodnôt $(y_1, ..., y_h)$ z poľa $\mathbb{F}_q$ a snažíme sa nájsť také hodnoty premenných $(x_1, ..., x_h, x'_1, ..., x'_v)$, ktoré po dosadení do systému $F(x, x')$ dávajú práve hodnoty $(y_1, ..., y_h)$. Pri systémoch UOV štruktúry by sa invertovanie riešilo tak, že náhodne priradíme hodnoty octovým premenným $x'_1, ..., x'_v$ a po dosadení dostaneme lineárny systém v $x_1, ..., x_h$, ktorý vyriešime. V prípade systému $F(x, x')$ je však tento postup nie vhodný, keďže aj po dosadení by sme stále mali kvadratický systém. Autori článku preto navrhujú 2 spôsoby, ako invertovať perturbované UOV.

3.2.1 Prvý spôsob invertovania - prehľadávanie všetkých možností

Ak máme daný nejaký vektor h hodnôt $y = (y_1, ..., y_h)$, pre ktorý chceme invertovať $y = F(x, x')$, t.j. hľadáme také $(x_1, ..., x_h, x'_1, ..., x'_v)$, že $F(x, x') = y$, tak prvý spôsob inverzie $F(x)$ je založený na prehľadávaní všetkých hodnôt, ktoré môžu nadobúdať polynómy z_i. V podstate ide o to, že tipujeme, aké hodnoty budú nadobúdať polynómy $z_1, z_2, ..., z_t$ pre hľadané x.

Postup je nasledovný:

1. Vygeneruj vektor v náhodných hodnôt z poľa $\mathbb{F}_q$ pre octové neurčité $(x'_1, ..., x'_v)$ a dosaď do $y = F(x, x')$, t.j. vypočítaj $y = F(x, v)$. (tento krok je rovnaký, ako keby sme chceli riešiť pôvodné UOV).

2. Vygeneruj náhodný vektor t hodnôt $(u_1, u_2, ..., u_t)$ nad poľom $\mathbb{F}_q$.

3. Nahraď v systéme $F(x, v) = y$ časti predstavujúce polynómy $z_i(x_1, ..., x_h)$ hodnotami u_i. Tým v podstate odstrániš kvadratické členy pochádzajúce

z polynómov $z_1, ..., z_t$ a dostávaš lineárny systém h rovníc o h premenných $(x_1, ..., x_h)$.

4. Vyrieš príslušný lineárny systém.

5. Ak lineárny systém nemá riešenie, skoč na krok č. 2. Ak **žiaden** z možných vektorov t hodnôt $(u_1, ..., u_t)$ nevedie na nejaké riešenie, skoč na krok č. 1.

6. Ak mal lineárny systém riešenie $(x_1, ..., x_h)$, over, či pre každé $i = 1, ..., t$ platí, že $z_i(x_1, ..., x_h) = u_i$, t.j. či z_i po dosadení nájdeného riešenia nadobúda práve i-tu hodnotu vektora $(u_1, ..., u_t)$ z kroku č. 2. Ak nie, choď na krok č. 2. Ak vyčerpáš všetky vektory z kroku č. 2, skoč na krok č. 1.

7. Ak nájdené riešenie $(x_1, ..., x_h)$ lineárneho systému zároveň spĺňa podmienku, že pre každé $i = 1, ..., t$ platí, že $z_i(x_1, ..., x_h) = u_i$, potom $(x_1, ..., x_h, x'_1, ..., x'_v)$ je hľadanou inverziou $F(x, x') = y$.

V prípade, že je $F(x, x')$, resp. perturbovaný UOV, uvažovaný ako **podpisová schéma**, tak stačí nájsť jedno (x, x') také, že platí $F(x, x') = y$ - preto v kroku č. 2 stačí generovať náhodný vektor t hodnôt. Ako píšeme v postupe, môže nastať situácia, že nedostaneme riešenie lineárneho systému, resp. že riešenie lineárneho systému, ktoré dostaneme, nie je správnym riešením $F(x, x') = y$. Preto by sa vo vyššie uvedenom postupne mohol krok č. 2 nahradiť cyklom, v ktorom sa postupne prechádzajú **všetky** vektory t hodnôt $(u_1, ..., u_t)$, t.j. prechádza sa q^t hodnôt.

Príklad: Uvažujme teda perturbované UOV nad poľom $\mathbb{F}_{2^3}$:

$$
\begin{aligned}
y_1 = {} & \alpha {x'_1}^2 + (\alpha+1)x'_1x'_3 + \alpha^2 x'_2x'_3 + {x'_3}^2 + \\
& \alpha x'_1x_1 + x'_3x_1 + x'_2x_2 + \alpha^2 x'_1x_3 + (\alpha^2+1)x'_2x_3 + x'_3x_3 + \\
& x_1x_3 + (1+\alpha)x_2x_3 + \alpha^2 x_2^2 + \\
& \alpha((1+\alpha+\alpha^2)x_1x_2 + (1+\alpha^2)x_1x_3 + x_1^2 + \alpha x_3^2) \\
y_2 = {} & \alpha x'_1x'_2 + (\alpha+1)x'_1x'_3 + (\alpha^2+\alpha)x'_2x'_3 + (\alpha^2+1){x'_3}^2 + \\
& x'_1x_1 + (\alpha+1)x'_2x_1 + \alpha^2 x'_1x_2 + \alpha x'_3x_2 + (\alpha+1)x'_2x_3 \\
& (1+\alpha^2)(x_1x_3 + (1+\alpha)x_2x_3 + \alpha^2 x_2^2) + \\
& (\alpha+\alpha^2)((1+\alpha+\alpha^2)x_1x_2 + (1+\alpha^2)x_1x_3 + x_1^2 + \alpha x_3^2) \\
y_3 = {} & \alpha {x'_2}^2 + x'_1x'_3 + \alpha {x'_3}^2 + \\
& \alpha x'_2x_2 + x'_3x_2 + \alpha^2 x'_1x_3 + \alpha^2 x'_2x_3 + \alpha x'_3x_3 \\
& (\alpha^2)((1+\alpha+\alpha^2)x_1x_2 + (1+\alpha^2)x_1x_3 + x_1^2 + \alpha x_3^2)
\end{aligned}
$$

Ekvivalentná reprezentácia perturbovaného UOV by bola nasledovná (v nej sme nerozpísali $z_1(x_1, x_2, x_3), z_2(x_1, x_2, x_3)$, ale nechali sme ich tam ako polynómy):

$$
\begin{aligned}
y_1 &= \alpha {x'_1}^2 + (\alpha+1)x'_1x'_3 + \alpha^2 x'_2x'_3 + {x'_3}^2 + \\
&\quad \alpha x'_1x_1 + x'_3x_1 + x'_2x_2 + \alpha^2 x'_1x_3 + (\alpha^2+1)x'_2x_3 + x'_3x_3 + \\
&\quad z_1(x_1,x_2,x_3) + \alpha z_2(x_1,x_2,x_3) \\
y_2 &= \alpha x'_1x'_2 + (\alpha+1)x'_1x'_3 + (\alpha^2+\alpha)x'_2x'_3 + (\alpha^2+1){x'_3}^2 + \\
&\quad x'_1x_1 + (\alpha+1)x'_2x_1 + \alpha^2 x'_1x_2 + \alpha x'_3x_2 + (\alpha+1)x'_2x_3 \\
&\quad (1+\alpha^2)z_1(x_1,x_2,x_3) + (\alpha+\alpha^2)z_2(x_1,x_2,x_3) \\
y_3 &= \alpha {x'_2}^2 + x'_1x'_3 + \alpha {x'_3}^2 + \\
&\quad \alpha x'_2x_2 + x'_3x_2 + \alpha^2 x'_1x_3 + \alpha^2 x'_2x_3 + \alpha x'_3x_3 \\
&\quad (\alpha^2)z_2(x_1,x_2,x_3)
\end{aligned}
$$

Povedzme, že sú dané hodnoty $y = (y_1, y_2, y_3) = (\alpha, \alpha+\alpha^2, 1)$, pre ktoré chceme invertovať perturbované UOV, t.j. hľadáme hodnoty olejových a octových premenných $(x_1, x_2, x_3, x'_1, x'_2, x'_3)$, aby $F(x, x') = y$:

1. Vygenerujeme hodnoty octových premenných náhodne: $v = (x'_1, x'_2, x'_3) = (1, 1, \alpha)$ a dosadíme do systému $F(x, x') = F(x, v) = y$ za octové premenné. Tým sa zmení systém na $y = F(x, v)$:

$$
\begin{aligned}
\alpha &= x_2 + (\alpha+1)x_3 + (\alpha+1) + z_1(x_1,x_2,x_3) + \alpha z_2(x_1,x_2,x_3) \\
\alpha+\alpha^2 &= \alpha x_1 + (\alpha+1)x_3 + 1 + (1+\alpha^2)z_1(x_1,x_2,x_3) + (\alpha+\alpha^2)z_2(x_1,x_2,x_3) \\
1 &= (\alpha^2)x_3 + (\alpha+1) + (\alpha^2)z_2(x_1,x_2,x_3)
\end{aligned}
$$

2. Vygenerujeme vektor $t = 2$ náhodných hodnôt z $\mathbb{F}_{2^3}$ ako $(u_1, u_2) = (\alpha^2 + 1, \alpha+1)$ a nahradíme $z_1(x_1, x_2, x_3)$ za u_1 a $z_2(x_1, x_2, x_3)$ za u_2:

$$
\begin{aligned}
\alpha &= x_2 + (\alpha+1)x_3 + (\alpha+1) + (\alpha^2+1) + \alpha(\alpha+1) \\
\alpha+\alpha^2 &= \alpha x_1 + (\alpha+1)x_3 + 1 + (1+\alpha^2)(\alpha^2+1) + (\alpha+\alpha^2)(\alpha+1) \\
1 &= (\alpha^2)x_3 + (\alpha+1) + (\alpha^2)(\alpha+1)
\end{aligned}
$$

3. Tým dostávame sústavu 3 rovníc o 3 neznámych (x_1, x_2, x_3), ktorú riešime, napríklad Gaussovou eliminačnou metódou. Zistili by sme, že uvedená sústava má nasledovné riešenie:
   (a) $x_1 = 0$
   (b) $x_2 = \alpha + 1$
   (c) $x_3 = \alpha^2 + \alpha$

4. V ďalšom kroku musíme, overiť, či pre naše riešenie $x_1 = 0, x_2 = \alpha + 1, x_3 = \alpha^2 + \alpha$, ktoré sme dostali, platí, že $z_1(x_1, x_2, x_3) = u_1 = \alpha^2 + 1$ a $z_2(x_1, x_2, x_3) = u_2 = \alpha + 1$. Žiaľ, zistíme, že nie, pretože

(a) $z_1(x_1 = 0, x_2 = \alpha + 1, x_3 = \alpha^2 + \alpha) = 1 \neq \alpha^2 + 1$

(b) $z_2(x_1 = 0, x_2 = \alpha + 1, x_3 = \alpha^2 + \alpha) = \alpha^2 \neq \alpha + 1$

Keďže riešenia (x_1, x_2, x_3) nesplnili tento test, skúsime vygenerovať iné náhodné (u_1, u_2) a postup zopakovať.

5. Vygenerujeme nový vektor $t = 2$ náhodných hodnôt z $\mathbb{F}_{2^3}$ ako $(u_1, u_2) = (\alpha + 1, \alpha^2 + \alpha + 1)$ a nahradíme $z_1(x_1, x_2, x_3)$ za u_1 a $z_2(x_1, x_2, x_3)$ za u_2:

$$\begin{aligned} \alpha &= x_2 + (\alpha + 1)x_3 + (\alpha + 1) + (\alpha + 1) + \alpha(\alpha^2 + \alpha + 1) \\ \alpha + \alpha^2 &= \alpha x_1 + (\alpha + 1)x_3 + 1 + (1 + \alpha^2)(\alpha + 1) + (\alpha + \alpha^2)(\alpha^2 + \alpha + 1) \\ 1 &= (\alpha^2)x_3 + (\alpha + 1) + (\alpha^2)(\alpha^2 + \alpha + 1) \end{aligned}$$

6. Tým dostávame sústavu 3 rovníc o 3 neznámych (x_1, x_2, x_3), ktorú riešime, napríklad Gaussovou eliminačnou metódou. Zistili by sme, že uvedená sústava má nasledovné riešenie:

   (a) $x_1 = \alpha^2 + 1$

   (b) $x_2 = 1$

   (c) $x_3 = \alpha$

7. V ďalšom kroku musíme, overiť, či pre naše riešenie $x_1 = \alpha^2 + 1, x_2 = 1, x_3 = \alpha$, ktoré sme dostali, platí, že $z_1(x_1, x_2, x_3) = u_1 = \alpha + 1$ a $z_2(x_1, x_2, x_3) = u_2 = \alpha^2 + \alpha + 1$. Zistíme, že áno, pretože

   (a) $z_1(x_1 = \alpha^2 + 1, x_2 = 1, x_3 = \alpha) = \alpha + 1$

   (b) $z_2(x_1 = \alpha^2 + 1, x_2 = 1, x_3 = \alpha) = \alpha^2 + \alpha + 1$

8. Tým sa nám podarilo nájsť riešenie správne hodnoty olejových premenných $(x_1, x_2, x_3) = (\alpha^2 + 1, 1, \alpha)$. Keď k nim pridáme hodnoty octových premenných, ktoré sme zvolili na začiatku, $(x_1, x_2, x_3, x'_1, x'_2, x'_3) = (\alpha^2 + 1, 1, \alpha, 1, 1, \alpha)$ dostávame hľadané riešenie systému $F(x, x') = y$, t.j. inverziu perturbovaného UOV zobrazenia pre vektor hodnôt $y = (\alpha, \alpha + \alpha^2, 1)$.

3.2.2 Druhý spôsob invertovania - cez substitúciu z_i

Druhý spôsob inverzie perturbovaného UOV je založený na nasledovnej myšlienke. Uvažujme perturbované UOV, ktoré chceme invertovať pre nejakú danú hodnotu y a v ktorom už prebehla voľba octových premenných, t.j. uvažujme systém vyššie označený ako $F(x, v) = y$. V tomto systéme máme olejové premenné v lineárnych členoch, ako pozostatok pôvodného UOV a potom tam máme lineárne kombinácie polynómov označených ako $z_1(x_1, ..., x_h), z_2(x_1, ..., x_h), ..., z_t(x_1, ..., x_h)$, ktoré obsahujú kvadratické členy v olejových neurčitých.

Príklad: Je dané perturbované UOV, v ktorom znovu pre lepšiu ilustráciu ponecháme $z_1(x_1, x_2, x_3), z_2(x_1, x_2, x_3), z_3(x_1, x_2, x_3)$ ako polynómy a nerozpíšeme

ich:

$$\begin{aligned}
y_1 &= \alpha {x'_1}^2 + (\alpha+1)x'_1x'_3 + \alpha^2x'_2x'_3 + {x'_3}^2 + \\
&\quad \alpha x'_1x_1 + x'_3x_1 + x'_2x_2 + \alpha^2x'_1x_3 + (\alpha^2+1)x'_2x_3 + x'_3x_3 + \\
&\quad z_1(x_1,x_2,x_3) + \alpha z_2(x_1,x_2,x_3) \\
y_2 &= \alpha x'_1x'_2 + (\alpha+1)x'_1x'_3 + (\alpha^2+\alpha)x'_2x'_3 + (\alpha^2+1){x'_3}^2 + \\
&\quad x'_1x_1 + (\alpha+1)x'_2x_1 + \alpha^2x'_1x_2 + \alpha x'_3x_2 + (\alpha+1)x'_2x_3 \\
&\quad (1+\alpha^2)z_1(x_1,x_2,x_3) + (\alpha+\alpha^2)z_2(x_1,x_2,x_3) \\
y_3 &= \alpha {x'_2}^2 + x'_1x'_3 + \alpha {x'_3}^2 + \\
&\quad \alpha x'_2x_2 + x'_3x_2 + \alpha^2x'_1x_3 + \alpha^2x'_2x_3 + \alpha x'_3x_3 \\
&\quad (\alpha^2)z_2(x_1,x_2,x_3)
\end{aligned}$$

a sú dané hodnoty $y = (y_1, y_2, y_3) = (\alpha, \alpha+\alpha^2, 1)$, pre ktoré chceme zobrazenie invertovať. Povedzme, že sa zvolia octové neurčité ako: $v = (x'_1, x'_2, x'_3) = (1, 1, \alpha)$ a dosadia sa do systému $F(x, x') = F(x, v) = y$ za octové neurčité. Tým sa zmení systém na $y = F(x, v)$:

$$\begin{aligned}
\alpha &= x_2 + (\alpha+1)x_3 + (\alpha+1) + z_1(x_1,x_2,x_3) + \alpha z_2(x_1,x_2,x_3) \\
\alpha+\alpha^2 &= \alpha x_1 + (\alpha+1)x_3 + 1 + (1+\alpha^2)z_1(x_1,x_2,x_3) + (\alpha+\alpha^2)z_2(x_1,x_2,x_3) \\
1 &= (\alpha^2)x_3 + (\alpha+1) + (\alpha^2)z_2(x_1,x_2,x_3)
\end{aligned}$$

Vidíme, že po dosadení octových premenných nám zostala sústava, kde sú lineárne členy v olejových premenných a navyše tam máme lineárne kombinácie systémov $z_1(x_1, x_2, x_3)$ a $z_2(x_1, x_2, x_3)$. V predchádzajúcej časti sme si ukázali, že jedným spôsobom riešenia je náhodne tipovať, aké hodnoty bude z_1 a z_2 nadobúdať. V tejto sekcii si ukážeme alternatívne riešenie.

Zadefinujeme si t nových premenných, označíme ich ako $z_1, z_2, ..., z_t$ a **nahradíme nimi** v systéme $F(x, v) = y$ príslušné polynómy $z_1(x_1, ..., x_t)$, ..., $z_t(x_1, ..., x_t)$, t.j. položíme rovnosť: $z_1 = z_1(x_1, ..., x_t), ..., z_t = z_t(x_1, ..., x_t)$ Tým dostaneme systém h rovníc o $h + t$ premenných, ktorý **je lineárny**.

Príklad: V našom prípade si teda vytvoríme nové premenné z_1, z_2 a nahradíme nimi v systéme $F(x, v) = y$ polynómy $z_1(x_1, x_2, x_3), z_2(x_1, x_2, x_3)$. Teda zo systému:

$$\begin{aligned}
\alpha &= x_2 + (\alpha+1)x_3 + (\alpha+1) + z_1(x_1,x_2,x_3) + \alpha z_2(x_1,x_2,x_3) \\
\alpha+\alpha^2 &= \alpha x_1 + (\alpha+1)x_3 + 1 + (1+\alpha^2)z_1(x_1,x_2,x_3) + (\alpha+\alpha^2)z_2(x_1,x_2,x_3) \\
1 &= (\alpha^2)x_3 + (\alpha+1) + (\alpha^2)z_2(x_1,x_2,x_3)
\end{aligned}$$

dostávame systém

$$\begin{aligned}
\alpha &= x_2 + (\alpha+1)x_3 + (\alpha+1) + z_1 + \alpha z_2 \\
\alpha+\alpha^2 &= \alpha x_1 + (\alpha+1)x_3 + 1 + (1+\alpha^2)z_1 + (\alpha+\alpha^2)z_2 \\
1 &= (\alpha^2)x_3 + (\alpha+1) + (\alpha^2)z_2
\end{aligned}$$

Je **veľmi dôležité** aby ste si uvedomili rozdiel medzi vyššie uvedenými systémami. V prvom systéme sú $z_1(x_1, x_2, x_3)$ a $z_2(x_1, x_2, x_3)$ **polynómy**, zatiaľ čo v druhom systéme sú z_1, z_2 **premenné**. Vidíme, že keďže sme pridali $t = 2$ nové premenné, dostávame systém $h = 3$ rovníc o $h + t = 3 + 2 = 5$ premenných, ktorý je **lineárny**.

Ak máme teraz lineárnu sústavu h rovníc o $h+t$ premenných, **pokúsime sa ju upraviť tak**, že si vyjadríme premenné $x_1, ..., x_h$, teda olejové premenné, pomocou novovytvorených premenných $z_1, ..., z_t$. V prípade, že je hodnosť systému rovná h, podarí sa nám každú olejovú premennú $x_1, ..., x_h$ vyjadriť pomocou premenných $z_1, ..., z_t$.

Príklad: V našom prípade zo systému:

$$\begin{aligned}
\alpha &= x_2 + (\alpha+1)x_3 + (\alpha+1) + z_1(x_1, x_2, x_3) + \alpha z_2(x_1, x_2, x_3) \\
\alpha + \alpha^2 &= \alpha x_1 + (\alpha+1)x_3 + 1 + (1+\alpha^2)z_1(x_1, x_2, x_3) + (\alpha+\alpha^2)z_2(x_1, x_2, x_3) \\
1 &= (\alpha^2)x_3 + (\alpha+1) + (\alpha^2)z_2(x_1, x_2, x_3)
\end{aligned}$$

dostávame po ekvivalentných úpravách nasledovné vyjadrenie olejových premenných x_1, x_2, x_3 pomocou nových premenných z_1, z_2:

$$\begin{aligned}
x_1 &= (\alpha^2 + \alpha + 1)z_1 + (\alpha^2 + \alpha + 1)z_2 + \alpha^2 \\
x_2 &= z_1 + z_2 + \alpha^2 + 1 \\
x_3 &= z_2 + \alpha^2 + 1
\end{aligned}$$

Keď sme si teraz vyjadrili olejové premenné $x_1, x_2, ..., x_h$ pomocou novodefinovaných premenných $z_1, ..., z_t$, vráťme sa do systému polynómov $z_1(x_1, ..., x_h), ..., z_t(x_1, ..., x_h)$. Uvedomte si teraz veci:

1. Novovytvorené premenné z_i boli vytvorené tak, aby platilo medzi premennou z_i a polynómom $z_i(x_1, ..., x_h)$ že $z_i = z_i(x_1, ..., x_h)$
2. Polynómy $z_i(x_1, ..., x_h)$ sú tvorené len olejovými premennými $x_1, ..., x_h$. A tie máme **teraz vyjadrené** pomocou novovytvorených premenných $z_1, ..., z_t$.

Môžeme teda uvažovať nasledovný systém rovníc (znovu upozorňujem na rozdiel medzi premennou z_i a polynómom $z_i(x_1, .., x_h)$:

$$\begin{aligned}
z_1 &= z_1(x_1, x_2, ..., x_h) \\
z_2 &= z_2(x_1, x_2, ..., x_h) \\
&... \\
z_t &= z_t(x_1, x_2, ..., x_h)
\end{aligned}$$

Uvedený systém je systém t rovníc o $t + h$ premenných $z_1, ..., z_t, x_1, ..., x_h$. Avšak, ak **využijeme to**, že máme premenné $x_1, ..., x_h$ vyjadrené **pomocou**

premenných $z_1, ..., z_t$, môžeme toto vyjadrenie dosadiť, čím dostaneme **kvadratickú sústavu** t rovníc o t premenných $z_1, ..., z_t$.

Príklad T.j. v našom prípade, po rozpísaní toho, aké **konkrétne** polynómy $z_1(x_1, x_2, x_3), z_2(x_1, x_2, x_3)$ sú:

$$z_1 = z_1(x_1, x_2, x_3) = x_1x_3 + (1 + \alpha)x_2x_3 + \alpha^2x_2^2$$
$$z_2 = z_2(x_1, x_2, x_3) = (1 + \alpha + \alpha^2)x_1x_2 + (1 + \alpha^2)x_1x_3 + x_1^2 + \alpha x_3^2$$

Po dosadení

- $x_1 = (\alpha^2 + \alpha + 1)z_1 + (\alpha^2 + \alpha + 1)z_2 + \alpha^2$,
- $x_2 = z_1 + z_2 + \alpha^2 + 1$,
- $x_3 = z_2 + \alpha^2 + 1$

a prenesení všetkých premenných na pravú stranu dostávame 2 **kvadratické** rovnice o 2 premenných z_1, z_2:

$$0 = (\alpha^2)z_1^2 + (\alpha^2)z_1z_2 + (\alpha + 1)z_1 + \alpha z_2 + 1$$
$$0 = (\alpha^2 + \alpha)z_1z_2 + (\alpha^2)z_2^2 + (\alpha^2 + \alpha)z_1 + (\alpha^2 + 1)z_2 + (\alpha^2 + \alpha + 1)$$

Týmto spôsobom sme dostali **výsledný kvadratický systém** o t rovniciach a t neznámych. Ak teraz tento systém vyriešime a **nájdeme hodnoty premenných** $z_1, z_2, ..., z_t$, tak zo známych vzťahov olejových premenných $x_1, ..., x_h$ a premenných $z_1, ..., z_t$ vieme ľahko určiť korektné hodnoty hľadaných olejových premenných dosadením. V prípade, že by **neexistovalo** riešenie t rovníc o premenných $z_1, ..., z_t$, musíme sa vrátiť späť a zvoliť iné octové neurčité a proces opakovať. Teoreticky by tento proces mal byť **rýchlejší**, než ten, v ktorom sa hodnoty polynómov $z_i(x_1, ..., x_h)$ náhodne tipujú.

Príklad Uvažujme kvadratický systém:

$$0 = (\alpha^2)z_1^2 + (\alpha^2)z_1z_2 + (\alpha + 1)z_1 + \alpha z_2 + 1$$
$$0 = (\alpha^2 + \alpha)z_1z_2 + (\alpha^2)z_2^2 + (\alpha^2 + \alpha)z_1 + (\alpha^2 + 1)z_2 + (\alpha^2 + \alpha + 1)$$

Nejakým spôsobom by sa nám podarilo zistiť, že vyššie uvedená **kvadratická** sústava má riešenie $z_1 = \alpha+1$ a $z_2 = \alpha^2+\alpha+1$. To znamená, že by sme následne olejové premenné vypočítali na základe vzťahov:

- $x_1 = (\alpha^2 + \alpha + 1)z_1 + (\alpha^2 + \alpha + 1)z_2 + \alpha^2$,
- $x_2 = z_1 + z_2 + \alpha^2 + 1$,
- $x_3 = z_2 + \alpha^2 + 1$

kde po dosadení $z_1 = \alpha + 1, z_2 = 1 + \alpha + \alpha^2$ dostávame

- $x_1 = \alpha^2 + 1$,
- $x_2 = 1$,
- $x_3 = \alpha$

To znamená, že **hľadané hodnoty olejových premenných** $x_1 = \alpha^2 + 1, x_2 = 1, x_3 = \alpha$. **Nezabúdajme**, že to celé sme počítali pre hodnoty octových premenných $(x'_1, x'_2, x'_3) = (1, 1, \alpha)$. Úspešne sa nám teda podarilo nájsť inverziu UOV perturbovaného centrálneho zobrazenia, v ktorom sme hodnoty $y = (\alpha, \alpha + \alpha^2 + 1)$ invertovali na $(x_1, x_2, x_3, x'_1, x'_2, x'_3) = (\alpha^2 + 1, 1, \alpha, 1, 1, \alpha)$.

Zhrnutie tohto spôsobu inverzie perturbovaného UOV by teda bolo nasledovné: Ak máme daný nejaký vektor h hodnôt $y = (y_1, ..., y_h)$, pre ktorý chceme invertovať $y = F(x, x')$, t.j. hľadáme také $(x_1, ..., x_h, x'_1, ..., x'_v)$, že $F(x, x') = y$, tak druhý spôsob inverzie $F(x)$ je založený na vytvorení nových t premenných $z_1, ..., z_t$ a položení rovnosti $z_1 = z_1(x_1, ..., x_h), ..., z_t = z_t(x_1, ..., x_h)$ a následnej snahe vyjadriť olejové premenné $x_1, ..., x_h$ pomocou $z_1, ..., z_t$. Postup je nasledovný:

1. Vygeneruj vektor v náhodných hodnôt z poľa $\mathbb{F}_q$ pre octové neurčité $(x'_1, ..., x'_v)$ a dosaď do $y = F(x, x')$, t.j. vypočítaj $y = F(x, v)$.
2. Vytvor nové premenné $z_1, ..., z_t$ pre ktoré platí $z_i = z_i(x_1, ..., x_h)$ pre $i = 1, .., t$.
3. Nahraď v systéme $y = F(x, v)$ polynómy $z_i(x_1, ..., x_h)$ premennými z_i, čím dostaneš systém h rovníc o $h + t$ premenných.
4. V tomto systéme vyjadri olejové premenné $x_1, ..., x_h$ pomocou premenných $z_1, ..., z_t$.
5. Vyvtor sústavu rovníc $z_i = z_i(x_1, ..., x_h)$, $i = 1, ..., t$, v ktorých následne dosaď za $x_1, ..., x_h$ vyjadrenia pomocou premenných $z_1, ..., z_t$.
6. Tým dostaneš sústavu t kvadratických rovníc o t neznámych $z_1, ..., z_t$.
7. Nájdi riešenie tejto sústavy, t.j. hodnoty premenných $z_1, ..., z_t$ a spätne tieto hodnoty dosaď do vyjadrení olejových premenných $x_1, ..., x_h$ z kroku č. 4
8. Ak táto kvadratická sústava nemá riešenie, skoč na krok č. 1.
9. Nájdené hodnoty olejových a octových premenných $(x_1, ..., x_h, x'_1, ..., x'_v)$ sú hľadanou inverziou $F(x, x') = y$.

Jedným z možných problémov tohto postupu je krok číslo 7. Totižto v ňom riešime **kvadratickú sústavu** t rovníc v premenných $z_1, ..., z_t$ - čo môže pôsobiť mätúco, keďže ako sme neraz napísali, vo všeobecnosti je riešenie kvadratickej sústavy rovníc viacerých premenných nad konečným poľom **NP-hard**. Avšak v tomto prípade je na našej strane fakt, že t je volené tak, aby bolo **malé**. Preto riešenie sústavy t kvadratických rovníc o t premenných by nemalo byť také zložité, ako keby sme povedzme chceli riešiť pôvodnú sústavu v olejových premenných, kde sme mali h rovníc o h premenných - a v praxi by určite $t << h$.

To, akým spôsobom / algoritmom riešiť samotnú sústavu t rovníc o t premenných je na samostatnú debatu. Existuje niekoľko prístupov, ktoré je možné zvoliť, od hľadania riešení hrubou silou $\mathcal{O}(q^t)$ po rôzne sofistikované algoritmy typu F4, F5 alebo XL.