Key Recovery Attack for ZHFE

Daniel Cabarcas[1] Daniel Smith-Tone[2,3] Javier A. Verbel[1]

[1]Universidad Nacional de Colombia, Sede Medellín, Colombia
[2] University of Louisville, USA
[3]National Institute of Standards and Technology, USA

PQCrypto June 28, 2017

Context

- MPK encryption schemes viable in PQ world
- Some of them based MQ problem
- HFE, multi HFE - broken by MinRank attack
- ZHFE

Our contribution and related work

Our contribution

- Show the existence of a low rank equivalent private key
- Show a detailed how recover a fully functional private key for ZHFE from the public key.
- Estimate the complexity of this attack

Our contribution and related work

Our contribution

- Show the existence of a low rank equivalent private key
- Show a detailed how recover a fully functional private key for ZHFE from the public key.
- Estimate the complexity of this attack

- Bettale, Faugère, Perret, (2013) "Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic"
- Zhang, Tang (2016) "On the security and key generation of the ZHFE encryption scheme"
- Perlner and Smith-Tone (2016) "Security analysis and key modification for ZHFE"

Outline

ZHFE encryption scheme

Let $\mathbb{F}$ be a field of size q and $\mathbb{K}$ an extension field of degree n of $\mathbb{F}$

HFE polynomial

$$F(X) = \sum_{0 \le i \le j < n} a_{ij} X^{q^i + q^j} + \sum_{i=0}^{n} b_i X^{q^i} + c, \quad \text{with } a_{ij}, b_i, c \in \mathbb{K}$$

ZHFE encryption scheme

Let $\mathbb{F}$ be a field of size q and $\mathbb{K}$ an extension field of degree n of $\mathbb{F}$

HFE polynomial

$$F(X) = \sum_{0 \le i \le j < n} a_{ij} X^{q^i + q^j} + \sum_{i=0}^{n} b_i X^{q^i} + c, \quad \text{with } a_{ij}, b_i, c \in \mathbb{K}$$

A low degree reduction

Let F and $\tilde{F}$ be high degree (and rank) HFE polynomials, where the following relation holds in $\mathbb{K}$

$$\begin{aligned} \Psi(X) &= X\left(\alpha_1 F^{q^0} + \cdots + \alpha_n F^{q^{n-1}} + \beta_1 \tilde{F}^{q^0} + \cdots + \beta_n \tilde{F}^{q^{n-1}}\right) \\ &+ X^q\left(\alpha_{n+1} F^{q^0} + \cdots + \alpha_{2n} F^{q^{n-1}} + \beta_{n+1} \tilde{F}^{q^0} + \cdots + \beta_{2n} \tilde{F}^{q^{n-1}}\right), \end{aligned}$$

where $\deg(\Psi) \le D$, for some small integer D.

Public and secret keys

SK A secret key is $\Pi = (G, S, T)$, where $G = (F, \tilde{F})$, $T \in End(\mathbb{F}^{2n})$, $S \in End(\mathbb{F}^n)$.

PK The public given by Π is

$$P = T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S,$$

where $\varphi : \mathbb{K} \to \mathbb{F}^n$ be the canonical $\mathbb{F}$-isomorphism and $\varphi_2 = \varphi \times \varphi$.

Public and secret keys

SK A secret key is $\Pi = (G, S, T)$, where $G = (F, \tilde{F})$, $T \in End(\mathbb{F}^{2n})$, $S \in End(\mathbb{F}^n)$.

PK The public given by Π is

$$P = T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S,$$

where $\varphi : \mathbb{K} \to \mathbb{F}^n$ be the canonical $\mathbb{F}$-isomorphism and $\varphi_2 = \varphi \times \varphi$.

Encryption and decryption

- To encrypt a plaintext $\underline{x} \in \mathbb{F}^n$, evaluate $P(\underline{x})$
- To decrypt $P(\underline{x})$, the map G needs to be inverted. So, if $G(X) = (Y_1, Y_2)$ then the following relation holds:

$$\begin{aligned} \Psi(X) &= X\left(\alpha_1 Y_1 + \alpha_2 Y_1^q + \cdots + \alpha_n Y_1^{q^{n-1}} + \beta_1 Y_2 + \cdots + \beta_n Y_2^{q^{n-1}}\right) \\ &+ X^q\left(\alpha_{n+1} Y_1 + \alpha_{n+2} Y_1^q + \cdots + \alpha_{2n} Y_1^{q^{n-1}} + \beta_{n+1} Y_2 + \cdots + \beta_{2n} Y_2^{q^{n-1}}\right). \end{aligned}$$

A low rank equivalent key

Let L be the function from $\mathbb{K}^2$ to $\mathbb{K}^2$ given by

$$L(X,Y) = \left(\sum_{i=1}^{n} \alpha_i X^{q^{i-1}} + \sum_{i=1}^{n} \beta_i Y^{q^{i-1}},\ \sum_{i=1}^{n} \alpha_{n+i} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{n+i} Y^{q^{i-1}} \right).$$

A low rank equivalent key

Let L be the function from $\mathbb{K}^2$ to $\mathbb{K}^2$ given by

$$L(X,Y) = \left(\sum_{i=1}^{n} \alpha_i X^{q^{i-1}} + \sum_{i=1}^{n} \beta_i Y^{q^{i-1}},\ \sum_{i=1}^{n} \alpha_{n+i} X^{q^{i-1}} + \sum_{i=1}^{n} \beta_{n+i} Y^{q^{i-1}} \right).$$

So, If $(H, \tilde{H}) := L \circ (F, \tilde{F})$ and $r = \lceil \log_q D \rceil$, then

$$\mathrm{Rank}(\mathbf{H}) \leq r+1 \qquad \mathrm{Rank}(\tilde{\mathbf{H}}) \leq r+1$$

$$\mathbf{H} = \begin{pmatrix} * & * & * & & * & & & \\ * & * & * & \cdots & * & * & \cdots & * \\ * & * & * & & * & & & \\ & \vdots & & \ddots & & & & \\ * & * & * & & * & & & \\ & * & & & & & & \\ & \vdots & & & & & & \\ & * & & & & & & \end{pmatrix} \qquad \tilde{\mathbf{H}} = \begin{pmatrix} * & * & * & & * & * & \cdots & * \\ * & * & * & \cdots & * & & & \\ * & * & * & & * & & & \\ & \vdots & & \ddots & & & & \\ * & * & * & & * & & & \\ * & & & & & & & \\ \vdots & & & & & & & \\ * & & & & & & & \end{pmatrix}$$

- If $(H, \tilde{H}) = L \circ (F, \tilde{F})$
- and L non-singular (happen with high probability), then

$$T \circ \varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S = (T \circ R) \circ \varphi_2 \circ \left(H, \tilde{H}\right) \circ \varphi^{-1} \circ S,$$

  where $R = \varphi_2 \circ L^{-1} \circ \varphi_2^{-1}$.

- $\left((F, \tilde{F}), S, T)\right)$ and $\left((H, \tilde{H}), S, (T \circ R)\right)$ are equivalent

Private key and fundamental equation

Suppose $P = T \circ \varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S$ is a ZHFE public key.

Fundamental equation

$$\sum_{i=0}^{2n-1} u_{i,0}\mathbf{P}_{i+1} = \mathbf{W}\mathbf{F}\mathbf{W}^{\top}, \text{ and } \sum_{i=0}^{2n-1} u_{i,n}\mathbf{P}_{i+1} = \mathbf{W}\tilde{\mathbf{F}}\mathbf{W}^{\top},$$

- where $\mathbf{W} := \mathbf{S}\mathbf{M}_n$, $\mathbf{U} := \mathbf{T}^{-1}\mathbf{M}_{2n} = [u_{ij}]$
- $\mathbf{M}_n = \rho \circ \varphi$ and $\mathbf{M}_{2n} = \mathrm{Diag}(\mathbf{M}_n, \mathbf{M}_n)$,
- $\rho : \mathbb{K} \to \mathbb{K}^n$, $\rho(a) = (a, a^q, ..., a^{q^{n-1}})$.

Suppose $P = T \circ \varphi_2 \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S$ is a ZHFE public key.

Fundamental equation

$$\sum_{i=0}^{2n-1} u_{i,0}\mathbf{P}_{i+1} = \mathbf{W}\mathbf{F}\mathbf{W}^{\top}, \text{ and } \sum_{i=0}^{2n-1} u_{i,n}\mathbf{P}_{i+1} = \mathbf{W}\tilde{\mathbf{F}}\mathbf{W}^{\top},$$

$$\mathbf{F} = \begin{pmatrix} * & * & * & & * & & & \\ * & * & * & \cdots & * & * & \cdots & * \\ * & * & * & & * & & & \\ & \vdots & & \ddots & & & & \\ * & * & * & & * & & & \\ & * & & & & & & \\ & \vdots & & & & & & \\ & * & & & & & & \end{pmatrix} \qquad \tilde{\mathbf{F}} = \begin{pmatrix} * & * & * & & * & * & \cdots & * \\ * & * & * & \cdots & * & & & \\ * & * & * & & * & & & \\ & \vdots & & \ddots & & & & \\ * & * & * & & * & & & \\ * & & & & & & & \\ \vdots & & & & & & & \\ * & & & & & & & \end{pmatrix}$$

$\mathbf{u} = [u_{i,0}]_i$ and $\mathbf{v} = [u_{i,n}]_i$ are solution to the MinRank problem associated with $(\mathbf{P}_1, ..., \mathbf{P}_{2n})$ and $r + 1$.

Too many equivalent keys

Too many equivalent keys

A big set of equivalent keys

- Let $\mathcal{A} : \mathbb{K}^2 \to \mathbb{K}^2$ be a non-singular linear transformation represented by $A^* = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}$
- $\text{Frob}_k : \mathbb{K} \to \mathbb{K}$, $\text{Frob}_k(a) = a^{q^k}$,
- If

$$\begin{aligned} G' &= \text{Frob}_k \circ \mathcal{A} \circ (F, \tilde{F}) \circ \text{Frob}_{n-k}, \\ T' &= T \circ \varphi_2 \circ \mathcal{A}^{-1} \circ \text{Frob}_{n-k} \circ \varphi_2^{-1}, \\ S' &= \varphi \circ \text{Frob}_k \circ \varphi^{-1} \circ S, \end{aligned}$$

- $T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S = T' \circ \varphi_2 \circ G' \circ \varphi^{-1} \circ S'$
- (G, S, T) and (G', S', T') are equivalent, where $G = (F, \tilde{F})$,

Given a private key (G', S', T'), if $G' := (H, \tilde{H})$,

$$\mathbf{U}' := \mathbf{T}'^{-1}\mathbf{M}_{2n}, \quad \mathbf{W}' := \mathbf{S}'\mathbf{M}_n,$$

$$\sum_{i=0}^{2n-1} u'_{i,0}\mathbf{P}_{i+1} = \mathbf{W'HW'}^{\top}, \text{ and } \sum_{i=0}^{2n-1} u'_{i,n}\mathbf{P}_{i+1} = \mathbf{W'\tilde{H}W'}^{\top}.$$

Given a private key (G', S', T'), if $G' := (H, \tilde{H})$,

$$\mathbf{U}' := \mathbf{T}'^{-1}\mathbf{M}_{2n}, \quad \mathbf{W}' := \mathbf{S}'\mathbf{M}_n,$$

$$\sum_{i=0}^{2n-1} u'_{i,0}\mathbf{P}_{i+1} = \mathbf{W'HW'}^{\top}, \text{ and } \sum_{i=0}^{2n-1} u'_{i,n}\mathbf{P}_{i+1} = \mathbf{W'\tilde{H}W'}^{\top}.$$

The matrices representing G' are

$$\mathbf{H} = \mathrm{Frob}_k(a_{00}\mathbf{F} + a_{01}\tilde{\mathbf{F}}),$$
$$\tilde{\mathbf{H}} = \mathrm{Frob}_k(a_{10}\mathbf{F} + a_{11}\tilde{\mathbf{F}}),$$

Moreover, $\mathrm{Rank}(\mathbf{H}), \mathrm{Rank}(\tilde{\mathbf{H}}) \leq r + 1$

Have the shape,

$$\begin{pmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \end{pmatrix}$$

Given a private key (G', S', T'), if $G' := (H, \tilde{H})$,

$$\mathbf{U}' := \mathbf{T}'^{-1}\mathbf{M}_{2n}, \quad \mathbf{W}' := \mathbf{S}'\mathbf{M}_n,$$

$$\sum_{i=0}^{2n-1} u'_{i,0}\mathbf{P}_{i+1} = \mathbf{W'HW'}^{\top}, \text{ and } \sum_{i=0}^{2n-1} u'_{i,n}\mathbf{P}_{i+1} = \mathbf{W'\tilde{H}W'}^{\top}.$$

The matrices representing G' are

$$\mathbf{H} = \mathrm{Frob}_k(a_{00}\mathbf{F} + a_{01}\tilde{\mathbf{F}}),$$
$$\tilde{\mathbf{H}} = \mathrm{Frob}_k(a_{10}\mathbf{F} + a_{11}\tilde{\mathbf{F}}),$$

Moreover, $\mathrm{Rank}(\mathbf{H}), \mathrm{Rank}(\tilde{\mathbf{H}}) \leq r + 1$

Have the shape,

$$\begin{pmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \end{pmatrix}$$

The first and $(n+1)$-th column of $\mathbf{U}'$ are solutions to the MinRank problem associated with $\mathbf{P}_1, ..., \mathbf{P}_{2n}$ and $r + 1$.

Given a private key (G', S', T'), if $G' := (H, \tilde{H})$,

$$\mathbf{U}' := \mathbf{T}'^{-1}\mathbf{M}_{2n}, \quad \mathbf{W}' := \mathbf{S}'\mathbf{M}_n,$$

$$\sum_{i=0}^{2n-1} u'_{i,0}\mathbf{P}_{i+1} = \mathbf{W'HW'}^{\top}, \text{ and } \sum_{i=0}^{2n-1} u'_{i,n}\mathbf{P}_{i+1} = \mathbf{W'\tilde{H}W'}^{\top}.$$

$$\mathbf{U}' = \left(\begin{array}{c|c|c|c|c|c|c|c} \mathbf{u}' & \mathbf{u}'^{q} & \cdots & \mathbf{u}'^{q^{n-1}} & \mathbf{v}' & \mathbf{v}'^{q} & \cdots & \mathbf{v}'^{q^{n-1}} \end{array} \right),$$

$$\mathbf{u}' := [u'_{i,0}] = a_{00}\mathbf{u}^{q^k} + a_{01}\mathbf{v}^{q^k} \quad \mathbf{v}' := [u'_{i,n}] = a_{10}\mathbf{u}^{q^k} + a_{11}\mathbf{v}^{q^k}$$

Given a private key (G', S', T'), if $G' := (H, \tilde{H})$,

$$\mathbf{U}' := \mathbf{T}'^{-1}\mathbf{M}_{2n}, \quad \mathbf{W}' := \mathbf{S}'\mathbf{M}_n,$$

$$\sum_{i=0}^{2n-1} u'_{i,0}\mathbf{P}_{i+1} = \mathbf{W'HW'}^{\top}, \text{ and } \sum_{i=0}^{2n-1} u'_{i,n}\mathbf{P}_{i+1} = \mathbf{W'\tilde{H}W'}^{\top}.$$

$$\mathbf{W}' = \left(\begin{array}{c|c|c|c} & & & \\ \mathbf{w} & \mathbf{w}^q & \cdots & \mathbf{w}^{q^{n-1}} \\ & & & \end{array} \right)$$

Attack description

Finding $\mathbf{T}'$

1. Find a vector $\mathbf{u}' = (u'_0, ..., u'_{2n-1}) \in \mathbb{K}^{2n}$ such that

$$\text{Rank}\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right) \leq r+1$$

2. Compute $\mathbf{K}' = \ker\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right)$ and find $\mathbf{v}' = (v'_0, ..., v'_{2n-1}) \in \mathbb{K}^{2n}$ such that

$$\mathbf{K}'\left(\sum_{i=0}^{2n-1} x'_i \mathbf{P}_{i+1}\right) = \mathbf{0}$$

3. Use $\mathbf{u}'$ and $\mathbf{v}'$ to compute $\mathbf{U}' = \mathbf{T}'^{-1}\mathbf{M}_{2n}$

Finding $\mathbf{S}'$

- $\sum_{i=0}^{2n-1} u_i' \mathbf{P}_{i+1} = \mathbf{W}' \mathbf{H} \mathbf{W}'^{\top}$

  $$\ker(\mathbf{H}) = \mathbf{K}' \mathbf{W}',$$

  where $\mathbf{K}' = \ker\left(\sum_{i=0}^{2n-1} u_i' \mathbf{P}_{i+1}\right)$.

- $\mathbf{w}$ the first column of $\mathbf{W}'$ is a solution of the following overdeterminate ($r(n-r-1)$ equations and n variables) linear system

$$\mathbf{x}\left[\mathbf{K}' | \mathrm{Frob}_{(n-1)}(\mathbf{K}') | \cdots | \mathrm{Frob}_{(n-r-1)}(\mathbf{K}')\right] = \mathbf{0}$$

Finding $\mathbf{S}'$

- $\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1} = \mathbf{W}' \mathbf{H} \mathbf{W}'^{\top}$

  $$\ker(\mathbf{H}) = \mathbf{K}' \mathbf{W}',$$

  where $\mathbf{K}' = \ker\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right)$.

- $\mathbf{w}$ the first column of $\mathbf{W}'$ is a solution of the following overdeterminate ($r(n-r-1)$ equations and n variables) linear system

$$\mathbf{x}\left[\mathbf{K}' | \mathrm{Frob}_{(n-1)}(\mathbf{K}') | \cdots | \mathrm{Frob}_{(n-r-1)}(\mathbf{K}')\right] = \mathbf{0}$$

Computing the core polynomials $\mathbf{H}$ and $\tilde{\mathbf{H}}$

$$\mathbf{H} = \mathbf{W}'^{-1}\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right)\mathbf{W}'^{-t} \text{ and } \tilde{\mathbf{H}} = \mathbf{W}'^{-1}\left(\sum_{i=0}^{2n-1} v'_i \mathbf{P}_{i+1}\right)\mathbf{W}'^{-t}.$$

Finding the low degree Ψ

Remember that

$$\mathbf{H}' = \begin{pmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \end{pmatrix} \qquad \tilde{\mathbf{H}}' = \begin{pmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \\ * & * & & & & & & \end{pmatrix}$$

Can we extract a low degree polynomial from those core polynomials which let us invert them?

Finding the low degree Ψ

- Note that

$$a_{11}^{q^k}\mathbf{H} - a_{01}^{q^k}\tilde{\mathbf{H}} = \det(A^*)^{q^k}\,\mathrm{Frob}_k(\mathbf{F}) \qquad -a_{10}^{q^k}\mathbf{H} + a_{00}^{q^k}\tilde{\mathbf{H}} = \det(A^*)^{q^k}\,\mathrm{Frob}_k(\tilde{\mathbf{F}})$$

- Define

$$\Psi' := X(a_{11}^{q^k}H - a_{01}^{q^k}\tilde{H}) + X^q(-a_{10}^{q^k}H + a_{00}^{q^k}\tilde{H}) = \det(A^*)^{q^k}\,\mathrm{Frob}_k(\Psi).$$

- Solving some linear systems we can recover a functional low degree Ψ'

Experimental results

The experiments were performed using Magma v2.21-1 on a server with a processor Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz, running Linux CentOS release 6.6.

			Minors		KS	
q	r	n	CPU time [s]	Memory [MB]	CPU time [s]	Memory [MB]
7	2	8	255	4216	280	439
7	2	12	3111	59651	1272	752
7	2	16			5487	2537
17	2	8	277	5034	299	503
17	2	12	3584	68731	1330	817
17	2	16			6157	2800

Table: MinRank attack to ZHFE

Theoretical results

- A fully functional private key can be extracted from a ZHFE public key
- If $L : \mathbb{K}^2 \to \mathbb{K}^2$ is singular the attack also works
- asymptotic complexity of the attack using minors modeling is $\mathcal{O}\left(n^{(r+2)\omega}\right)$

Future work

- Is the KS modeling more efficient than the minors modeling?
- What is the complexity of the KS modeling?
- Can we make HFE or ZHFE secure by making r a function of the security parameter?

THANK YOU

What about if L is singular?

- If $P = T \circ \varphi_2 \circ G \circ \varphi^{-1} \circ S$ is the public key. Then

$$R' \circ P = \varphi_2 \circ (L \circ G) \circ \varphi^{-1} \circ S,$$

$R' = \varphi_2 \circ L \circ \varphi_2^{-1} \circ T^{-1}$.

- We can recover R' and an functional private key for $R' \circ P$.
- Given $y = P(x)$, compute $y' = R'(y)$, and use the recovered private key to find preimages for y'

Finding $\mathbf{S}''$

- $\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1} = \mathbf{W}''\mathbf{H}'\mathbf{W}''^{\top}$

  $$\ker(\mathbf{H}') = \mathbf{K}'\mathbf{W}'',$$

  where $\mathbf{K}' = \ker\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right)$. $\mathbf{K}'$ has size $(n-r-1) \times n$

- $\ker(H')$ is on the form $[\mathbf{0}_{(n-r-1)}|\mathbf{C}]$.

- $\mathbf{w}$ the first column of $\mathbf{W}''$ satisfies the next overdeterminate linear system

$$\left[\mathbf{K}'|\mathrm{Frob}_{(n-1)}(\mathbf{K}')|\cdots|\mathrm{Frob}_{(n-r-1)}(\mathbf{K}')\right]^{\top}\mathbf{w} = \mathbf{0}$$

Finding $\mathbf{S}''$

- $\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1} = \mathbf{W}''\mathbf{H}'\mathbf{W}''^{\top}$

  $$\ker(\mathbf{H}') = \mathbf{K}'\mathbf{W}'',$$

  where $\mathbf{K}' = \ker\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right)$. $\mathbf{K}'$ has size $(n-r-1) \times n$

- $\ker(H')$ is on the form $[\mathbf{0}_{(n-r-1)}|\mathbf{C}]$.

- $\mathbf{w}$ the first column of $\mathbf{W}''$ satisfies the next overdeterminate linear system

$$\left[\mathbf{K}'|\mathrm{Frob}_{(n-1)}(\mathbf{K}')|\cdots|\mathrm{Frob}_{(n-r-1)}(\mathbf{K}')\right]^{\top}\mathbf{w} = \mathbf{0}$$

Computing the core polynomials $\mathbf{H}'$ and $\tilde{\mathbf{H}}'$

$$\mathbf{H}' = \mathbf{W}''^{-1}\left(\sum_{i=0}^{2n-1} u'_i \mathbf{P}_{i+1}\right)\mathbf{W}''^{-t} \text{ and } \tilde{\mathbf{H}}' = \mathbf{W}''^{-1}\left(\sum_{i=0}^{2n-1} v'_i \mathbf{P}_{i+1}\right)\mathbf{W}''^{-t}.$$