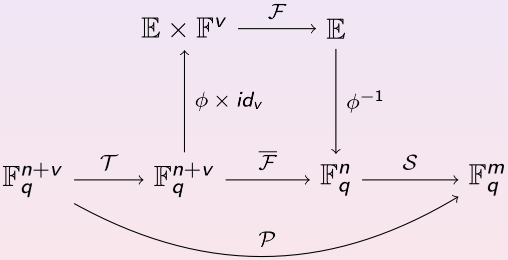
Gui

Daniel Smith-Tone

National Institute of Standards and Technology

2 February, 2018

Gui Diagram


$\mathbb{E} \times \mathbb{F}^v$
$\mathcal{F}$
$\mathbb{E}$
$\phi \times id_v$
ϕ^{-1}
$\mathbb{F}_q^{n+v}$
$\mathcal{T}$
$\mathbb{F}_q^{n+v}$
$\overline{\mathcal{F}}$
$\mathbb{F}_q^n$
$\mathcal{S}$
$\mathbb{F}_q^m$
$\mathcal{P}$

Parameters

- $\mathbb{F} = \mathbb{F}_q$, where $q = 2^e$.
- $\mathbb{E} = \mathbb{F}_q^n$, degree n extension of $\mathbb{F}$.
- $\phi : \mathbb{F}^n \rightarrow \mathbb{E}$, $\mathbb{F}$-vector space isomorphism.
- D a degree bound, and $r = \lfloor \log_q(D-1) \rfloor + 1$.
- a number of equations removed
- v number of vinegar variables
- k repetition factor
- $m = n - a$ number of equations.

Public and Private Keys

Private Key

- $\mathcal{S} : \mathbb{F}^n \to \mathbb{F}^{n-a}$ affine transformation of full rank.
- $\mathcal{T} : \mathbb{F}^{n+v} \to \mathbb{F}^{n+v}$ invertible affine transformation.
- Central map $\mathcal{F} : \mathbb{E} \times \mathbb{F}^v \to \mathbb{E}$, defined by

$$\mathcal{F}(X, \overline{v}) = \sum_{0 \le i \le j}^{q^i + q^j \le D} \alpha_{i,j} X^{q^i + q^j} + \sum_{0 \le i}^{q^i \le D} \beta_i(\overline{v}) X^{q^i} + \gamma(\overline{v}),$$

where the $\beta_i : \mathbb{F}^v \to \mathbb{E}$ are affine and $\gamma : \mathbb{F}^v \to \mathbb{E}$ is quadratic.

Public Key

$$\mathcal{P} = \mathcal{S} \circ \phi^{-1} \circ \mathcal{F} \circ (\phi \times id_v) \circ \mathcal{T}.$$

A Relevant Algebra

Let $\Phi : \mathbb{E} \rightarrow \mathbb{A}$ be the representation defined by
$\Phi(X) = (X, X^q, \ldots, X^{q^{n-1}})$.
WLOG specify ϕ by choosing a primitive element $\theta \in \mathbb{E}$.
Define the composition $\Phi \circ \phi$ as right multiplication by

$$\mathbf{M}_n = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^q & \cdots & \theta^{q^{n-1}} \\ \theta^2 & \theta^{2q} & \cdots & \theta^{2q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1} & \theta^{(n-1)q} & \cdots & \theta^{(n-1)q^{n-1}} \end{bmatrix}.$$

Then $(\Phi \circ \phi) \times id_v : \mathbb{F}^{n+v} \rightarrow \mathbb{E} \times \mathbb{F}^v$ is given by

$$\widetilde{\mathbf{M}}_n = \begin{bmatrix} \mathbf{M}_n & \mathbf{0}_{n\times v} \\ \mathbf{0}_{v\times n} & I_v \end{bmatrix},$$ where I_v is the identity matrix.

HFE Part of Central Map

(Odd Characteristic Case, for Simplicity)

$$\begin{bmatrix} X & X^q & \cdots & X^{q^{n-1}} \end{bmatrix} \begin{bmatrix} \alpha_{0,0} & \frac{\alpha_{0,1}}{2} & \cdots & \frac{\alpha_{0,r-1}}{2} & 0 & \cdots & 0 \\ \frac{\alpha_{0,1}}{2} & \alpha_{1,1} & \cdots & \frac{\alpha_{1,r-1}}{2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{0,r-1}}{2} & \frac{\alpha_{r,r-1}}{2} & \cdots & \alpha_{r-1,r-1} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} X \\ X^q \\ \vdots \\ X^{q^{n-1}} \end{bmatrix}$$

Example

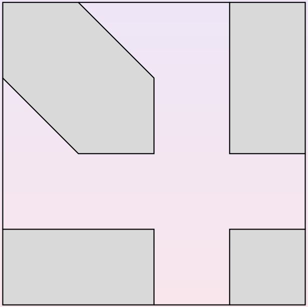


Figure: The shape of the matrix representation of the central map of HFEv- over $\mathbb{A} \times \mathbb{F}^v$. The shaded areas represent possibly nonzero entries.

Key Gen

Algorithm 1 GuiKeyGen: Key Generation of Gui

Input: $(q, n, D, a, v), \phi$.
Output: Gui key pair (sk, pk).

repeat
$M_S \leftarrow \mathrm{Matrix}(q, n, n)$
until $\mathrm{IsInvertible}(M_S) ==$ **TRUE**
$c_S \xleftarrow{\$} \mathbb{F}^n$
$\mathcal{S} \leftarrow \mathrm{Aff}(M_S, c_S)$
$InvS \leftarrow M_S^{-1}$
repeat
$M_T \leftarrow \mathrm{Matrix}(q, n+v, n+v)$
until $\mathrm{IsInvertible}(M_T) ==$**TRUE**
$c_T \xleftarrow{\$} \mathbb{F}^{n+v}$
$\mathcal{T} \leftarrow \mathrm{Aff}(M_T, c_T)$
$InvT \leftarrow M_T^{-1}$
$\mathcal{F} \leftarrow \mathrm{HFEvmap}(q, n, D, a, v)$
$\mathcal{P} \leftarrow \mathcal{S} \circ \phi^{-1} \circ \mathcal{F} \circ (\phi \times id_v) \circ \mathcal{T}$
$sk \leftarrow (InvS, c_S, \mathcal{F}, InvT, c_T)$
$pk \leftarrow \mathcal{P}$
return (sk, pk)

GuiSign

Algorithm 2 GuiSign

Input: Gui private key $(InvS, c_S, \mathcal{F}, InvT, c_T)$, message d, repetition factor k

Output: signature $\sigma \in \mathbb{F}^{(n-a} + k \cdot (a+v)$

$\ell \leftarrow \lceil k \cdot \log_2(q) \cdot (n-a)/|\mathcal{H}| \rceil.$

$\overline{\mathbf{h}} \leftarrow \mathcal{H}(d) \| \mathcal{H}(\mathcal{H}(d)) \| \ldots \| \mathcal{H}^{\ell}(d)$

$S_0 \leftarrow \mathbf{0}^{n-a}$

for $i = 1$ to k **do**

$\quad \mathbf{d}_i \leftarrow \mathbb{F}^{n-a}!(\overline{\mathbf{h}}_{(i-1)\cdot\log_2 q\cdot(n-a)+1}, \ldots, \overline{\mathbf{h}}_{i\cdot\log_2 q\cdot(n-a)})$

$\quad (S_i, X_i) \leftarrow \mathrm{InvHFEv} - (\mathbf{d}_i \oplus S_{i-1})$

end for

$\sigma \leftarrow (S_k \| X_k \| \ldots \| X_1)$

return σ

InvHFEv-

Algorithm 3 InvHFEv-: Inversion of the HFEv- public key

Input: Gui private key $(InvS, c_S, \mathcal{F}, InvT, c_T), \phi$, vector $\mathbf{w} \in \mathbb{F}^{n-a}$
Output: vector $\mathbf{z} \in \mathbb{F}^{n+v}$ such that $\mathcal{P}(\mathbf{z}) = \mathbf{w}$.

$r_1, \ldots, r_a \overset{\$}{\leftarrow} \mathbb{F}$
$\mathbf{x} \leftarrow InvS \cdot ((\mathbf{w} \| r_1 \| \ldots \| r_a) - c_S)$
$X \leftarrow \phi(\mathbf{x})$
repeat
  $\mathbf{v} = (v_1, \ldots, v_v) \overset{\$}{\leftarrow} \mathbb{F}^v$
  $\mathcal{F}_V \leftarrow \mathcal{F}(\cdot, \mathbf{v})$
  $Y \leftarrow \gcd(\mathcal{F}_V(\widehat{Y}) - X, \widehat{Y}^{2^n} - \widehat{Y})$
until $\deg(Y) == 1$
$\mathbf{y} \leftarrow \phi^{-1}(\mathrm{root}(Y))$
$\mathbf{z} \leftarrow InvT \cdot ((\mathbf{y} \| \mathbf{v}) - c_T)$
return z

GuiVer

Algorithm 4 GuiVer: Signature Verification Process of Gui

Input: Gui public key $\mathcal{P}$, message d, repetition factor k, signature $\sigma \in \mathbb{F}^{(n-a)+k(a+v)}$

Output: boolean value **TRUE** or **FALSE**.

$\ell \leftarrow \lceil k \cdot \log_2(q) \cdot (n-a)/|\mathcal{H}| \rceil$.

$\overline{\mathbf{h}} \leftarrow \mathcal{H}(d) \| \mathcal{H}(\mathcal{H}(d)) \| \ldots \| \mathcal{H}^{\ell}(d)$

for $i = 1$ to k **do**

  $\mathbf{d}_i \leftarrow \mathbb{F}^{n-a}!(\overline{\mathbf{h}}_{(i-1)\cdot \log_2 q \cdot (n-a)+1}, \ldots, \overline{\mathbf{h}}_{i \cdot \log_2 q \cdot (n-a)})$

end for

for $i = k-1$ to 0 **do**

  $S_i \leftarrow \mathcal{P}(S_{i+1} \| X_{i+1}) \oplus d_{i+1}$

end for

if $S_0 = \mathbf{0}$ **then**

  return TRUE

else

  return FALSE

end if

EUF-CMA

To achieve existential unforgability under chosen message attack, instead of signing on

$$\mathbf{h} = \mathcal{H}(d)$$

they sign on

$$\mathbf{h} = \mathcal{H}(\mathcal{H}(d)||r),$$

for a random salt r of length 128-bits.

Parameters

- **Gui-184** $(q, n, D, a, v, k) = (2, 184, 33, 16, 16, 2)$
- **Gui-312** $(q, n, D, a, v, k) = (2, 312, 129, 24, 20, 2)$
- **Gui-448** $(q, n, D, a, v, k) = (2, 448, 513, 32, 28, 2)$

Key and Signature Sizes

	parameters (n, D, a, v, k)	public key size (kB)	private key size (kB)	signature size (bit)
Gui-184	$(184, 33, 16, 16, 2)$	416.3	19.1	360
Gui-312	$(312, 129, 24, 20, 2)$	1955.1	59.3	504
Gui-448	$(448, 513, 32, 28, 2)$	5789.2	155.9	664

Performance - Platform

Processor: Intel® Xeon™ CPU E3-1225 v5 3.30 GHz (Skylake)
Memory: 64GB (4x16) ECC DIMM DDR4 Synch 2133 MHz
OS: Linux 4.8.5, GCC 6.4

Performance

scheme	parameters (n, D, a, v, k)		key gen.	sign. gen.	sign. verif.
		cycles	704M	34M	169k
Gui-184	$(184, 33, 16, 16, 2)$	time(ms)	213	10.4	0.051
		memory	3.5MB	3.4MB	3.3MB
		cycles	4790M	1757M	595k
Gui-312	$(312, 129, 24, 20, 2)$	time(ms)	1452	532	0.181
		memory	5.4MB	3.6MB	5.0MB
		cycles	32247M	86086M	3385k
Gui-448	$(448, 513, 32, 28, 2)$	time(ms)	9772	26086	1.025
		memory	9.2MB	10.7MB	8.7MB

Attack #1 - Brute Force

We may first fix the values of $v + a$ variables and still expect to have a solution to

$$\mathcal{P}(\mathbf{z}) = \mathbf{w}.$$

$$\mathrm{Comp}_{\mathrm{brute;classical}} = k \cdot 2^{n-a+2} \cdot \log_2(n-a).$$

$$\mathrm{Comp}_{\mathrm{brute;quantum}} = k \cdot 2^{(n-a)/2} \cdot 2 \cdot \log_2(n-a).$$

New result: Quantum FXL over GF(2) has complexity $\approx 2^{0.45n}$.

Attack #2 - Direct Attack

A paper by Petzoldt empirically derives a formula for d_{reg},

$$d_{reg} = \lfloor \frac{a+r+v+7}{3} \rfloor,$$

and provides evidence that the "hybrid approach" is ineffective for HFEv-.

$$\mathrm{Comp}_{\mathrm{direct;classical}} = 2 \cdot k \cdot 3 \cdot \binom{n-a}{d_{reg}}^2 \cdot \binom{n-a}{2}.$$

Attack #3 - MinRank

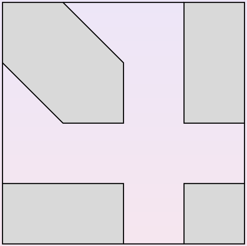


Figure: The shape of the matrix representation of the central map of HFEv- over $\mathbb{A} \times \mathbb{F}^v$. The shaded areas represent possibly nonzero entries.

$$\mathrm{Rank}\left(\sum_i t_i D\mathcal{P}_i\right) = r + a + v.$$

Attack #3 - MinRank - Complexity

$$\mathrm{Comp}_{\mathrm{MinRank;classical}} = \binom{n+r+v}{r+a+v}^{\omega},$$

where $2 \leq \omega \leq 3$ is the linear algebra constant.
They choose $\omega = 2.3$ for analysis.

Attack #4 - Distinguishing Attack

One idea is to select random projections to eliminate linear forms in the vinegar subspace.
This noticably reduces the degree of regularity.

$$\mathrm{Comp}_{\mathrm{Dist;classical}} = 2^{n-k} \cdot 3 \cdot \binom{n+v-k}{d_{reg}}^2 \cdot \binom{n+v-k}{2}.$$

$$\mathrm{Comp}_{\mathrm{Dist;quantum}} = 2^{(n-k)/2} \cdot 3 \cdot \binom{n+v-k}{d_{reg}}^2 \cdot \binom{n+v-k}{2}.$$

Attack #5 - Differential Attack

Cartor et al. proved that HFEv- is immune to differential attacks.

Advantages and Limitations

1. Very Short Signatures +
2. Security +
3. Modest computational requirements +
4. Efficiency +
5. Large Key Sizes –