New Practical Multivariate Signatures from a Nonlinear Modifier

Daniel Smith-Tone[1,2]

[1]University of Louisville
[2]National Institute of Standards and Technology

20 July, 2021

Small Field Schemes

$$\mathbb{F}_q^n \xrightarrow{U} \mathbb{F}_q^n \xrightarrow{F} \mathbb{F}_q^m \xrightarrow{T} \mathbb{F}_q^m$$

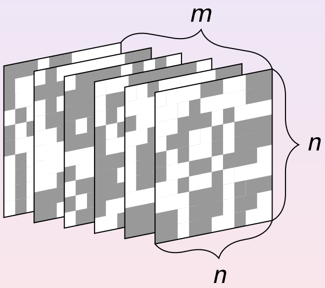
$$P = T \circ F \circ U : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Visualizing Homogeneous Quadratic Maps

$$f_\ell(\mathbf{x}) = \sum_{1\leq i\leq j\leq n} a_{ij\ell}x_ix_j$$

$$\Updownarrow$$

$$\begin{bmatrix} a_{11\ell} & a_{12\ell}/2 & \cdots & a_{1n\ell}/2 \\ a_{12\ell}/2 & a_{22\ell} & \cdots & a_{2n\ell}/2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n\ell}/2 & a_{2n\ell}/2 & \cdots & a_{nn\ell} \end{bmatrix}$$



Nonzero coefficients shaded

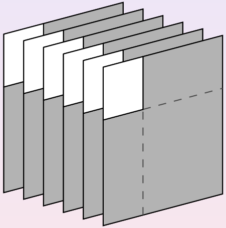
Unbalanced Oil and Vinegar (UOV)

For $0 \leq k < o$, define

$$F_k(\mathbf{x}) = \sum_{\substack{o<i<n \\ 0\leq j<n}} a_{ijk}x_i x_j + \sum_{0\leq i<n} b_{ik}x_i + c_k.$$

$$P(\mathbf{x}) = F \circ L(\mathbf{x}),$$

where L is linear.



UOV homogeneous quadratic part

~~Un~~balanced Oil and Vinegar (UOV)

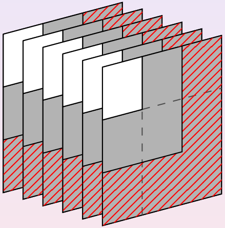
For $0 \leq k < o$, define

$$F_k(\mathbf{x}) = \sum_{\substack{o \leq i < n \\ 0 \leq j < n}} a_{ijk} x_i x_j + \sum_{0 \leq i < n} b_{ik} x_i + c_k.$$

$$P(\mathbf{x}) = F \circ L(\mathbf{x}),$$

where L is linear.

If $n \approx 2o$, this is bad



UOV homogeneous quadratic part

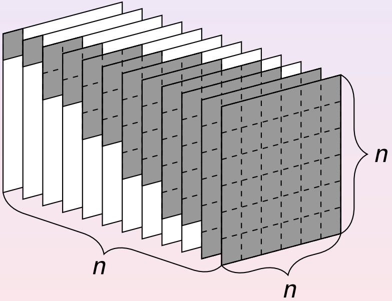
Step-wise Triangular System (STS)

Set $0 = u_0 < u_1 < \ldots < u_k = n$.
For all $u_{s-1} \leq \ell < u_s$, define

$$F_\ell = \sum_{0 \leq i,j < u_s} a_{ij\ell} x_i x_j + \sum_{0 \leq i < u_s} b_{i\ell} x_i + c_\ell.$$

$$P(\mathbf{x}) = T \circ F \circ U(\mathbf{x}),$$

where T, U are linear.



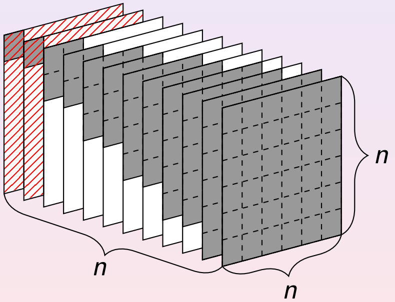
Step-wise Triangular System (STS)

Set $0 = u_0 < u_1 < \ldots < u_k = n$.
For all $u_{s-1} \leq \ell < u_s$, define

$$F_\ell = \sum_{0\leq i,j<u_s} a_{ij\ell}x_ix_j + \sum_{0\leq i<u_s} b_{i\ell}x_i + c_\ell.$$

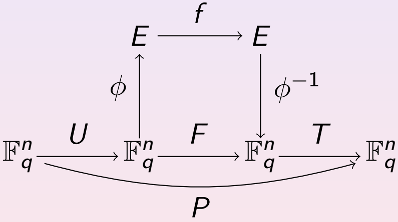
$$P(\mathbf{x}) = T \circ F \circ U(\mathbf{x}),$$

where T, U are linear.



Vulnerable to rank attacks unless $u_s - u_{s-1}$ is large.

Big Field Schemes

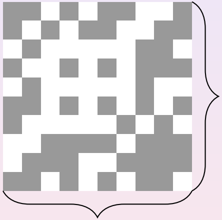


Visualizing Homogeneous Big Field Quadratic Maps

$$f(X) = \sum_{1 \le i \le j \le n} \alpha_{ij} X^{q^i + q^j}.$$

$$\Updownarrow$$

$$\begin{bmatrix} \alpha_{00} & \alpha_{01}/2 & \cdots & \alpha_{0(n-1)}/2 \\ \alpha_{01}/2 & \alpha_{11} & \cdots & \alpha_{1(n-1)}/2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{0(n-1)}/2 & a_{1(n-1)}/2 & \cdots & a_{(n-1)(n-1)} \end{bmatrix}$$



n

n

Nonzero coefficients shaded

C^* (Slightly Generalized)

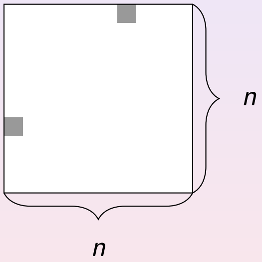
$$f(X) = \alpha X^{q^\theta + 1}.$$

$$P(\mathbf{x}) = T \circ \phi^{-1} \circ f \circ \phi \circ U(\mathbf{x}),$$

with T, U are linear and

$$\phi : F_q^n \to E$$

is an F_q-vector space isomorphism.



Nonzero coefficients shaded

C^* (Slightly Generalized)

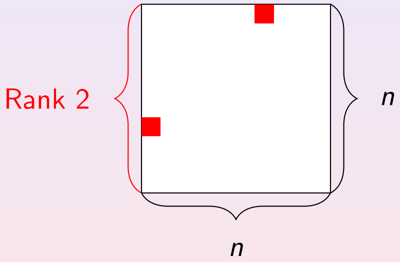
$$f(X) = \alpha X^{q^\theta + 1}.$$

$$P(\mathbf{x}) = T \circ \phi^{-1} \circ f \circ \phi \circ U(\mathbf{x}),$$

with T, U are linear and

$$\phi : F_q^n \to E$$

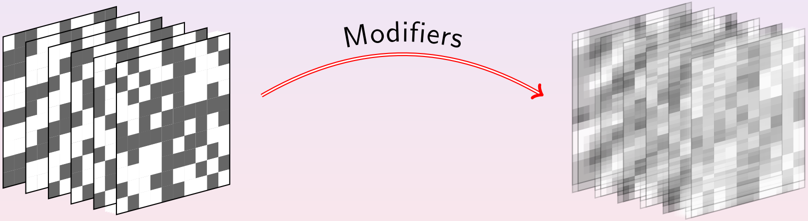
is an F_q-vector space isomorphism.



Nonzero coefficients shaded

Vulnerable to rank and differential attacks including Patarin's linearization equations.

Changing the Structure of Equations



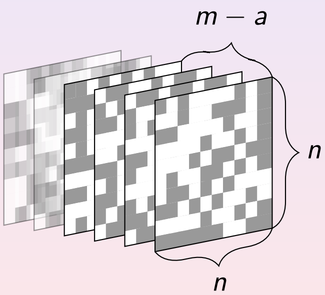
Minus (-)

Remove a public equations.

$$P_\Pi = \Pi \circ P,$$

where Π is a projection onto an $(m-a)$-dimensional subspace.

Public Map



Nonzero coefficients shaded

Projection (p)

Fix p input values.

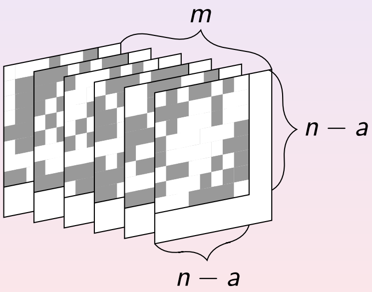
$$P_\Pi = P \circ \Pi,$$

where

$$\Pi : F_q^{n-p} \to F_q^n$$

is a linear embedding.

Public Map



Nonzero coefficients shaded

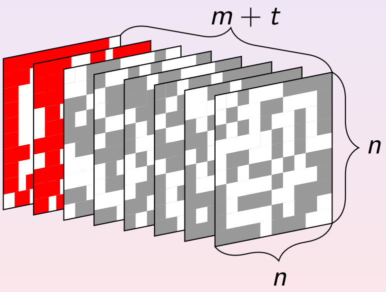
Plus (+)

Add t random equations.

$$F_+ = F \| Q,$$

where Q is a system of t random quadratic formulae in $\mathbf{x}$.

Private Map



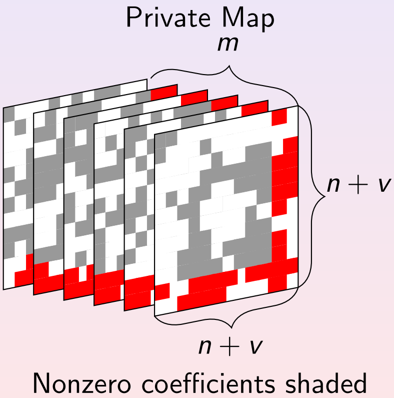
Nonzero coefficients shaded

Vinegar (v)

Add v extra variables.

$$F_v(\mathbf{x},\mathbf{v}) = F(\mathbf{x}) + Q(\mathbf{x},\mathbf{v}),$$

where Q is quadratic with the property that $F_v(\mathbf{x},\mathbf{c})$ is easy to invert for any constant $\mathbf{c}$.



Relinearization

Given a system of quadratic equations

$$P(\mathbf{x}) = \mathbf{c},$$

introduce new variables of the form

$$y_{ij} = x_i x_j.$$

Introduce equations in the new unknowns (for example) of the form

$$y_{ij} y_{k\ell} = y_{ik} y_{j\ell}$$

or

$$x_k y_{ij} = x_i y_{jk}.$$

The Q Modifier

Given a multivariate quadratic function $F : F_q^m \to F_q^m$, define a vector of auxiliary variables

$$\mathbf{w} = \begin{bmatrix} w_1 & \cdots & w_\ell \end{bmatrix}.$$

Multiply terms of F by these variables in SOME WAY to form $\widetilde{F} : F_q^{m+\ell} \to F_q^m$.
Define the vector of new variables $\mathbf{z} = \mathbf{x} \otimes \mathbf{w}$, i.e. $z_{ik} = x_i w_k$.
For each monomial in $\widetilde{F}$ randomly choose a substitution

$$x_i x_j w_k \to x_i z_{jk} \text{ or } x_i x_j w_k \to x_j z_{ik}.$$

For all equations, (i, j, k) and (i, j, r, s), randomly select $a, b \in F_q$ and add

$$a x_i z_{jk} - a x_j z_{ik} \text{ and } b z_{ij} z_{rs} - b z_{is} z_{rj},$$

forming $\widehat{F} : F_q^{(\ell+1)m} \to F_q^m$.

Inversion of $\widehat{F}$

How to solve $\mathbf{y} = \widehat{F}(\mathbf{x})$.

Step 1: Select constants

$$\mathbf{w} = \begin{bmatrix} w_1 & \cdots & w_\ell \end{bmatrix} = \begin{bmatrix} c_1 & \cdots & c_\ell \end{bmatrix}.$$

Step 2: Invert the intermediate map $\mathbf{y} = \widetilde{F}(\mathbf{u}, \mathbf{w})$.

Step 3: Compute the preimage of $\widehat{F}$,

$$\mathbf{x} = \mathbf{u} \oplus (\mathbf{u} \otimes \mathbf{w}).$$

Inversion of $\widehat{F}$

How to solve $\mathbf{y} = \widehat{F}(\mathbf{x})$.

Step 1: Select constants

$$\mathbf{w} = \begin{bmatrix} w_1 & \cdots & w_\ell \end{bmatrix} = \begin{bmatrix} c_1 & \cdots & c_\ell \end{bmatrix}.$$

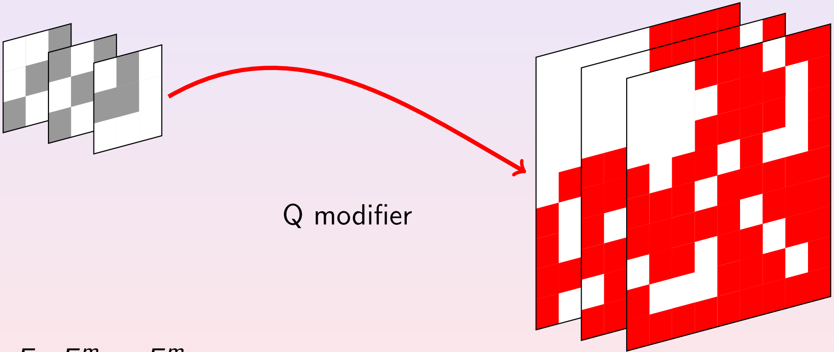
Step 2: Invert the intermediate map $\mathbf{y} = \widetilde{F}(\mathbf{u}, \mathbf{w})$.

Step 3: Compute the preimage of $\widehat{F}$,

$$\mathbf{x} = \mathbf{u} \oplus (\mathbf{u} \otimes \mathbf{w}).$$

Family of efficiently invertible functions

Q for Quadratic



$$F : F_q^m \to F_q^m$$

$$\widehat{F} : F_q^{(\ell+1)m} \to F_q^m$$

Example

Consider the function F over F_7 whose coordinates are given by

$$\begin{aligned} y_1 &= 2x_1x_2 + 3x_1x_3 + x_2x_3 \\ y_2 &= x_1^2 + 5x_1x_3 + 2x_2x_3 \\ y_3 &= x_1x_3 + 3x_2^2 + 6x_2x_3. \end{aligned}$$

Step 1: We produce $\widetilde{F} : F_q^5 \to F_q^3$,

$$\begin{aligned} y_1 &= 2x_1x_2w_2 + 3x_1x_3w_1 + 3x_1x_3w_2 + x_2x_3w_1 \\ y_2 &= x_1^2w_1 + x_1^2w_2 + 5x_1x_3w_2 + 2x_2x_3w_1 \\ y_3 &= x_1x_3w_1 + x_1x_3w_2 + 3x_2^2w_2 + 6x_2x_3w_2. \end{aligned}$$

Example, cont'd

At this point $\widetilde{F} : F_q^5 \to F_q^3$ is given by:

$$\begin{aligned} y_1 &= 2x_1x_2w_2 + 3x_1x_3w_1 + 3x_1x_3w_2 + x_2x_3w_1 \\ y_2 &= x_1^2w_1 + x_1^2w_2 + 5x_1x_3w_2 + 2x_2x_3w_1 \\ y_3 &= x_1x_3w_1 + x_1x_3w_2 + 3x_2^2w_2 + 6x_2x_3w_2. \end{aligned}$$

We construct the vector $\mathbf{z} = \mathbf{x} \otimes \mathbf{w}$.
Step 2: We produce $\widehat{F} : F_q^9 \to F_q^3$, by substitutions and random additions of cancelling terms (in parentheses for emphasis):

$$\begin{aligned} y_1 &= 2x_2z_{12} + 3x_1z_{31} + 3x_1z_{32} + x_3z_{21} + (4z_{12}z_{31} + 3z_{11}z_{32} + x_1z_{22} + 6x_2z_{12}) \\ y_2 &= x_1z_{11} + x_1z_{12} + 5x_3z_{12} + 2x_2z_{31} + (x_3z_{12} + 6x_1z_{32} + 4z_{22}z_{11} + 3z_{12}z_{21}) \\ y_3 &= x_1z_{31} + x_3z_{12} + 3x_2z_{22} + 6x_2z_{32} + (2x_1z_{21} + 5x_2z_{11} + 3z_{32}z_{11} + 4z_{12}z_{31}). \end{aligned}$$

QC^*

Let $f(X) = X^{q^\theta+1}$ be a C^* map. Define $\widetilde{F} : F_q^{m+\ell} \to F_q^m$ by

$$\widetilde{F}(\mathbf{x}, \mathbf{w}) = \phi^{-1}(\phi(B(\mathbf{w}))f(\phi(\mathbf{x}))),$$

where $\phi : F_q^m \to E$ is an F_q-vector space isomorphism and $B : F_q^\ell \to F_q^m$ is linear.

Note that $\widetilde{F}(\cdot, \mathbf{w})$ is a C^* map with a coefficient other than 1. Easily invertible.

$$P(\mathbf{x}) = T \circ \widehat{F} \circ U.$$

QC^*: Inversion of $\widehat{F}$

For small ℓ, we can store linearization equations $L_i^{\mathbf{w}}$ for the C^* map $\widetilde{F}(\cdot, \mathbf{w})$ for all $\mathbf{w}$.

To solve $\mathbf{y} = \widehat{F}(\mathbf{x})$, find an element $\mathbf{u}$ in the left kernel of the block matrix

$$\begin{bmatrix} L_1^{\mathbf{w}}\mathbf{y}^\top & \cdots & L_m^{\mathbf{w}}\mathbf{y}^\top \end{bmatrix}.$$

Then we have that

$$\mathbf{y} = \widehat{F}(\mathbf{u} \oplus (\mathbf{u} \otimes \mathbf{w})),$$

so that $\mathbf{x} = \mathbf{u} \oplus (\mathbf{u} \otimes \mathbf{w})$ is a preimage of $\mathbf{y}$.

QC^* Efficiency

Inversion requires

1) $m+1$ matrix-vector products,
2) an $m\ell$-dimensional Kronecker product, and
3) solving a linear system.

A total of $m^3 + m^\omega + m^2(\ell+1)^2 + m\ell$ multiplications in F_q.

(If you do not want to store q^ℓ linearization systems, inversion will cost one more matrix-vector multiplication.)

QSTS

Let $F(\mathbf{x})$ be an STS map. Define $\widetilde{F} : F_q^{m+\ell} \rightarrow F_q^m$ by multiplying every term in F by a random linear form in $\mathbf{w}$.

Note that for all fixed $\mathbf{w}$ that $\widetilde{F}(\cdot, \mathbf{w})$ is an STS map. Easily invertible.

$$P(\mathbf{x}) = T \circ \widehat{F} \circ U.$$

QSTS Efficiency

Inversion requires

1) 2 matrix-vector products,
2) an $m\ell$-dimensional Kronecker product, and
3) inversion of a triangular map.

A total of $m^3 + 2\binom{m+2}{3} + m^2(\ell+1)^2 + m\ell$ multiplications in F_q.

UOV Attacks

Notice that any Q system can be inverted as a UOV scheme; thus, any UOV attack is applicable.

1) Invariant Attack (à la OV).

2) UOV reconciliation attack.

Direct Attack

Any UOV preimage is valid, so the solving degree of P is not the same as F.

Using a hybrid approach and Thomae's trick we find the semi-regular degree

$$d_{sr} = \min\{d : [t^d]S(t) \leq 0\}, \text{ where } S(t) = \frac{(1-t^2)^{m-\ell-1}}{(1-t)^{m-\ell-1-k}}.$$

This produces a complexity of

$$\mathcal{O}\left(q^k \binom{m-\ell-1-k+d_{sr}}{d_{sr}}^{\omega}\right).$$

Q Kernel Attack

Note that monomials of the form $z_{ik}z_{jk}$ never occur in $\widehat{F}$. Thus, the assignment

$$\begin{bmatrix} x_1 & \cdots & x_n & z_{11} & \cdots & z_{1\ell} & \cdots z_{\ell\ell} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & 0 & \cdots & c_1 & \cdots c_\ell \end{bmatrix},$$

makes $\widehat{F} = 0$. Hence there exists a linear injection $M : F_q^\ell \to F_q^{m(\ell+1)}$ such that

$$\mathbf{M}\mathbf{P}_i\mathbf{M}^\top = \mathbf{0}_{\ell\times\ell}, \forall 1 \leq i \leq m.$$

Assuming $\mathbf{M}$ in echelon form, $m\binom{\ell}{2}$ equations in $m\ell^2$ variables.

Forms an ℓ^2-dimensional ideal, but $\ell << m$, so harder to solve than the direct attack.

Rank Attacks

Both C^* and STS have severe rank weaknesses.

Note that for all linear injections $M : F_q^m \to F_q^{m(\ell+1)}$

$$P \circ M \neq P',$$

where P' is a C^* or STS public key.

Thus QC^* and QSTS have no rank defect.

Differential Attack

Recall that many variants of C^* are vulnerable to differential attacks.

Since there is no linear injection M such that $P \circ M$ has the C^* shape, QC^* is not susceptible.

Parameters and Performance

Experiments using the MAGMA Computer Algebra System[1].

	q	m	ℓ	# Eqs.	# Vars.	sig. (B)	pk (B)	sign (ms)	ver. (ms)
Q-schemes	2^8	44	3	44	176	176	677600	0.6	2.9
UOV	2^8			44	176	176	677600	3.7	2.9

[1] Any mention of commercial products does not indicate endorsement by NIST

Future Directions

1) More security analysis.

2) Study case $\mathbf{w} = \begin{bmatrix} w_1 & \cdots & w_\ell & 1 \end{bmatrix}$.

3) Examine Q applied to other schemes. (QOV?)