Using a CCZ-transformation in a multivariate scheme

Irene Villa
joint work with Marco Calderini and Alessio Caminata

University of Genoa and University of Trento

BFA 2024

Multivariate Cryptography

A standard multivariate cryptosystem:

- a public finite field $\mathbb{F}_q$
- m private (quadratic) polynomials in n variables

  $$\mathcal{F} = \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix} : \mathbb{F}_q^n \to \mathbb{F}_q^m \text{ (computationally feasible to invert)}$$
- two private affine/linear invertible maps $\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$
- the public map $\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$,
  look like m random (quadratic) polynomials

`Encrypt` $\quad a \in \mathbb{F}_q^n \xrightarrow{\mathcal{P}} b = \mathcal{P}(a) \in \mathbb{F}_q^m$ $\quad$ `(Verify)`

`Decrypt` $\quad b \in \mathbb{F}_q^m \xrightarrow{\mathcal{S}^{-1}} w \in \mathbb{F}_q^m \xrightarrow{\mathcal{F}^{-1}} z \in \mathbb{F}_q^n \xrightarrow{\mathcal{T}^{-1}} a \in \mathbb{F}_q^n$ $\quad$ `(Sign)`

A classical example: MI scheme

Matsumoto-Imai cryptosystem (1988)

- Consider $\mathbb{F}_q^n$, $\mathbb{F}_{q^n}$ and $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ standard isomorphism
- Take $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ $\boxed{F(x) = x^{q^i+1}}$ s.t. $\gcd(q^n - 1, q^i + 1) = 1$
  F bijection easy to invert
- Then $\mathcal{F} = \phi \circ F \circ \phi^{-1} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$

Linearization attack by Patarin (1995)

- If $y = F(x) = x^{q^i+1}$, then $\boxed{y^{q^i} x = y x^{q^{2i}}}$
- Bilinear relation between input-output of F
- It exists also a bilinear relation between input-output of $\mathcal{P}$

A more general transformation for $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$?

⋆ **EA-transformation** $G = A_1 \circ F \circ A_2 + A$

- only affine maps involved

A more general transformation for $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$?

⋆ **EA-transformation** $G = A_1 \circ F \circ A_2 + A$

- only affine maps involved

⋆ **CCZ-transformation** $\mathcal{A}(\Gamma_F) = \Gamma_G$ for $\mathcal{A}$ aff. bij. of $\mathbb{F}_q^{n+m}$, and $\Gamma_F = \{(z, F(z)) : z \in \mathbb{F}_q^n\}$

- not preserved the algebraic degree (and the bijectivity)
- difficult to construct a random CCZ-transformation

A more general transformation for $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$?

⋆ **EA-transformation** $G = A_1 \circ F \circ A_2 + A$

- only affine maps involved

⋆ **CCZ-transformation** $\mathcal{A}(\Gamma_F) = \Gamma_G$ for $\mathcal{A}$ aff. bij. of $\mathbb{F}_q^{n+m}$, and $\Gamma_F = \{(z, F(z)) : z \in \mathbb{F}_q^n\}$

- not preserved the algebraic degree (and the bijectivity)
- difficult to construct a random CCZ-transformation

⋆ Towards a random CCZ construction

- **The t-twist**: for $t \leq \min(n, m)$, $F : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t \times \mathbb{F}_q^{m-t}$

$$F(x,y) = \begin{pmatrix} T(x,y) \\ U(x,y) \end{pmatrix} = \begin{pmatrix} T_y(x) \\ U(x,y) \end{pmatrix}, \quad G(x,y) = \begin{pmatrix} T_y(x)^{-1} \\ U(T_y(x)^{-1}, y) \end{pmatrix}$$

  with $T_y(x)$ invertible for every y
- CCZ = EA + t-twist + EA [Canteaut-Perrin 2019 for $q = 2$]
- if $\deg(F) = 2$, then $\deg(G) \leq 2 \cdot \deg(T_y(x)^{-1})$

CCZ Signature scheme

$$F(x,y) = \begin{pmatrix} T_y(x) \\ U(x,y) \end{pmatrix}, \quad G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x), y) \end{pmatrix}$$

Idea: private quadratic map $F \xrightarrow{t-twist} G \xrightarrow{aff-transf} \mathcal{P}$ public map

sk A_1, A_2, T, U pk $\mathcal{P} = A_1 \circ G \circ A_2$

CCZ Signature scheme

$$F(x,y) = \begin{pmatrix} T_y(x) \\ U(x,y) \end{pmatrix}, \quad G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x), y) \end{pmatrix}$$

Idea: private quadratic map $F \xrightarrow{t-twist} G \xrightarrow{aff-transf} \mathcal{P}$ public map

sk A_1, A_2, T, U pk $\mathcal{P} = A_1 \circ G \circ A_2$

Sign `s:=Sign(d,sk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow \mathcal{P}(\mathtt{s}) = h$?

Verify `Ver(d,s,pk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow$ check $\mathcal{P}(\mathtt{s}) = h$

CCZ Signature scheme

$$F(x,y) = \begin{pmatrix} T_y(x) \\ U(x,y) \end{pmatrix}, \quad G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x),y) \end{pmatrix}$$

Idea: private quadratic map $F \xrightarrow{t-twist} G \xrightarrow{aff-transf} \mathcal{P}$ public map

sk A_1, A_2, T, U pk $\mathcal{P} = A_1 \circ G \circ A_2$

Sign `s:=Sign(d,sk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow \mathcal{P}(\mathtt{s}) = h$?

1. $A_1^{-1}(h) = (w_T, w_U) \in \mathbb{F}_q^t \times \mathbb{F}_q^{m-t}$, so

$$\begin{pmatrix} w_T \\ w_U \end{pmatrix} = G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x),y) \end{pmatrix} = \begin{pmatrix} T_y^{-1}(x) \\ U(w_T,y) \end{pmatrix}$$

Verify `Ver(d,s,pk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow$ check $\mathcal{P}(\mathtt{s}) = h$

CCZ Signature scheme

$$F(x,y) = \begin{pmatrix} T_y(x) \\ U(x,y) \end{pmatrix}, \quad G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x), y) \end{pmatrix}$$

Idea: private quadratic map $F \xrightarrow{t-twist} G \xrightarrow{aff-transf} \mathcal{P}$ public map

sk A_1, A_2, T, U pk $\mathcal{P} = A_1 \circ G \circ A_2$

`Sign` `s:=Sign(d,sk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow \mathcal{P}(\mathtt{s}) = h$?

1. $A_1^{-1}(h) = (w_T, w_U) \in \mathbb{F}_q^t \times \mathbb{F}_q^{m-t}$, so

$$\begin{pmatrix} w_T \\ w_U \end{pmatrix} = G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x), y) \end{pmatrix} = \begin{pmatrix} T_y^{-1}(x) \\ U(w_T, y) \end{pmatrix}$$

2. $Y = \{y \in \mathbb{F}_q^{n-t} : w_U = U(w_T, y)\}$

`Verify` `Ver(d,s,pk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow$ check $\mathcal{P}(\mathtt{s}) = h$

CCZ Signature scheme

$$F(x,y) = \begin{pmatrix} T_y(x) \\ U(x,y) \end{pmatrix}, \quad G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x), y) \end{pmatrix}$$

Idea: private quadratic map $F \xrightarrow{t-twist} G \xrightarrow{aff-transf} \mathcal{P}$ public map

sk A_1, A_2, T, U pk $\mathcal{P} = A_1 \circ G \circ A_2$

Sign `s:=Sign(d,sk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow \mathcal{P}(\mathtt{s}) = h$?

1. $A_1^{-1}(h) = (w_T, w_U) \in \mathbb{F}_q^t \times \mathbb{F}_q^{m-t}$, so

$$\begin{pmatrix} w_T \\ w_U \end{pmatrix} = G(x,y) = \begin{pmatrix} T_y^{-1}(x) \\ U(T_y^{-1}(x), y) \end{pmatrix} = \begin{pmatrix} T_y^{-1}(x) \\ U(w_T, y) \end{pmatrix}$$

2. $Y = \{y \in \mathbb{F}_q^{n-t} : w_U = U(w_T, y)\}$
3. get $\bar{y} \in Y$, $\bar{x} = T_{\bar{y}}(w_T)$, then $\bar{\mathtt{s}} = A_2^{-1}(\bar{x}, \bar{y})$ is a valid signature

Verify `Ver(d,s,pk)`: $h = \mathcal{H}(\mathtt{d}) \in \mathbb{F}_q^m \longrightarrow$ check $\mathcal{P}(\mathtt{s}) = h$

The choice of T and U

$$x = (x_1, \ldots, x_t) \; y = (y_1, \ldots, y_{n-t})$$

$T : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$
$T(x, y)$ invertible for every fixed y

$U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$
$U(x, y)$: fixed x it must be "easy" to get a preimage with respect to y ($\bar{y} \in Y$)

The choice of T and U

$$x = (x_1, \ldots, x_t)\ y = (y_1, \ldots, y_{n-t})$$

$T : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$
$T(x, y)$ invertible for every fixed y

- $T(x, y) = \ell(x) + \mathfrak{q}(y)$, ℓ linear bijection, $\mathfrak{q}$ random quadratic
- w.l.o.g.

$$T(x, y) = x + \mathfrak{q}(y)$$
$$T_y^{-1}(x) = x - \mathfrak{q}(y)$$

- $\deg(G) \leq 4$

$U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$
$U(x, y)$: fixed x it must be "easy" to get a preimage with respect to y $(\bar{y} \in Y)$

The choice of T and U

$$x = (x_1, \dots, x_t) \; y = (y_1, \dots, y_{n-t})$$

$T : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$
$T(x, y)$ invertible for every fixed y

- $T(x, y) = \ell(x) + \mathfrak{q}(y)$, ℓ linear bijection, $\mathfrak{q}$ random quadratic
- w.l.o.g.

$$T(x, y) = x + \mathfrak{q}(y)$$
$$T_y^{-1}(x) = x - \mathfrak{q}(y)$$

- $\deg(G) \leq 4$

$U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$
$U(x, y)$: fixed x it must be "easy" to get a preimage with respect to y ($\bar{y} \in Y$)

- use Oil-and-Vinegar (OV) maps

(OV)

$$f(z) = \sum_{j,k \in V} \alpha_{jk} z_j z_k + \sum_{j \in V} \sum_{k \in O} \beta_{jk} z_j z_k + \sum_{j \in V} \gamma_j z_j + \sum_{j \in O} \gamma_j z_j + \delta$$

The choice of T and U

$$x = (x_1, \dots, x_t) \; y = (y_1, \dots, y_{n-t})$$

$T : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$
$T(x, y)$ invertible for every fixed y

- $T(x, y) = \ell(x) + \mathfrak{q}(y)$, ℓ linear bijection, $\mathfrak{q}$ random quadratic
- w.l.o.g.

$$T(x, y) = x + \mathfrak{q}(y)$$
$$T_y^{-1}(x) = x - \mathfrak{q}(y)$$

- $\deg(G) \leq 4$

$U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$
$U(x, y)$: fixed x it must be "easy" to get a preimage with respect to y ($\bar{y} \in Y$)

- use Oil-and-Vinegar (OV) maps
- fix $0 \leq s \leq n - t$, U is a system of $m - t$ OV equations with $\{x_1, \dots, x_t, y_1, \dots, y_s\}$ vinegar and $\{y_{s+1}, \dots, y_{n-t}\}$ oil

(OV) $$f(z) = \sum_{j,k \in V} \alpha_{jk} z_j z_k + \sum_{j \in V} \sum_{k \in O} \beta_{jk} z_j z_k + \sum_{j \in V} \gamma_j z_j + \sum_{j \in O} \gamma_j z_j + \delta$$

UOV-CCZ Scheme

- n, m, t, s with $t \leq \min(n, m)$ and $s \leq n - t$
- $\mathfrak{q} : \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$ **random quadratic**, so $T(x, y) = x + \mathfrak{q}(y)$
- $U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$ **random OV maps** with $t + s$ vinegar variables (x_i, y_j, $j \leq s$) and $n - t - s$ oil variables (y_j, $j > s$)
- A_1, A_2 **random affine bijections** of $\mathbb{F}_q^m$, $\mathbb{F}_q^n$
- $G(x, y) = (x - \mathfrak{q}(y), U(x - \mathfrak{q}(y), y))$

pk $\mathcal{P} = A_1 \circ G \circ A_2$ sk $\mathfrak{q}, U, A_1, A_2$

UOV-CCZ Scheme

- n, m, t, s with $t \leq \min(n, m)$ and $s \leq n - t$
- $\mathfrak{q} : \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$ **random quadratic**, so $T(x, y) = x + \mathfrak{q}(y)$
- $U : \mathbb{F}_q^t \times \mathbb{F}_q^{n-t} \to \mathbb{F}_q^{m-t}$ **random OV maps** with $t + s$ vinegar variables (x_i, y_j, $j \leq s$) and $n - t - s$ oil variables (y_j, $j > s$)
- A_1, A_2 **random affine bijections** of $\mathbb{F}_q^m$, $\mathbb{F}_q^n$
- $G(x, y) = (x - \mathfrak{q}(y), U(x - \mathfrak{q}(y), y))$

pk $\mathcal{P} = A_1 \circ G \circ A_2$ sk $\mathfrak{q}, U, A_1, A_2$

a.k.a. Pesto scheme

Like in the Pesto Sauce, we try to fully mix the variables (ingredients) using a CCZ transformation (mortar and pestle).

Key Sizes

Theorem

The public key consists of $m\binom{n+4}{4}$ *coefficients over* $\mathbb{F}_q$*, and the secret key consists of*

$$m^2+m+n^2+n+t\binom{n-t+2}{2}+(m-t)\binom{t+s+2}{2}+(m-t)(n-t-s)(t+s+1)$$

coefficients over $\mathbb{F}_q$*.*

Amount of coefficients of $\mathbb{F}_q$ to store

n	m	t	s	amount for pk	amount for sk
5	4	2	1	504	106
6	5	2	2	1050	177
10	8	3	2	8008	545

Linearization attack for $s = 0$

Linearization Equation (LE) $\mathcal{R} : \mathbb{F}_q^n \times \mathbb{F}_q^m \to \mathbb{F}_q$

$$\mathcal{R}(z, w) = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} z_i w_j + \sum_{i=1}^{n} \beta_i z_i + \sum_{j=1}^{m} \gamma_j w_j + \delta \in \mathbb{F}_q[z, w]$$

s.t. $\forall \bar{z} \in \mathbb{F}_q^n$, $\mathcal{P}(\bar{z}) = \bar{w}$, $\mathcal{R}(\bar{z}, \bar{w}) = 0$.

- Fixed the output $\bar{w} \in \mathbb{F}_q^m$, $\mathcal{R}(z, \bar{w})$ is *linear* in z (input)
- Higher Order LE (HOLE): relation $\mathcal{R}$ only linear in the input

Linearization attack for $s = 0$

Linearization Equation (LE) $\mathcal{R} : \mathbb{F}_q^n \times \mathbb{F}_q^m \to \mathbb{F}_q$

$$\mathcal{R}(z, w) = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} z_i w_j + \sum_{i=1}^{n} \beta_i z_i + \sum_{j=1}^{m} \gamma_j w_j + \delta \in \mathbb{F}_q[z, w]$$

s.t. $\forall \bar{z} \in \mathbb{F}_q^n$, $\mathcal{P}(\bar{z}) = \bar{w}$, $\mathcal{R}(\bar{z}, \bar{w}) = 0$.

- Fixed the output $\bar{w} \in \mathbb{F}_q^m$, $\mathcal{R}(z, \bar{w})$ is *linear* in z (input)
- Higher Order LE (HOLE): relation $\mathcal{R}$ only linear in the input

Attack for $s = 0$ (in U $\{x_i\}$ vinegar and $\{y_i\}$ oil)

1. $\begin{pmatrix} w_T \\ w_U \end{pmatrix} = G(x, y) \Rightarrow \boxed{w_U = U(w_T, y)}$ quadratic HOLEs
2. we have quadratic HOLEs for $\mathcal{P} = A_1 \circ G \circ A_2$
3. reconstruct the coefficients (by considering enough input-output pairs)
4. given a targeted output, we have $m - t$ linear equations in the input

Differential attack via linear structures

$$\mathcal{P} = A_1 \circ \begin{bmatrix} x - \mathfrak{q}(y) \\ U(x - \mathfrak{q}(y), y) \end{bmatrix} \circ A_2, \text{ with } x - \mathfrak{q}(y) = \begin{pmatrix} x_1 - \mathfrak{q}_1(y) \\ \vdots \\ x_t - \mathfrak{q}_t(y) \end{pmatrix}$$

- $\mathcal{P}$ has (at least) $q^t - 1$ quadratic components ($\mathcal{P}_\lambda = \lambda \cdot \mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q$)
- For $f = x_i - \mathfrak{q}_i(y)$, $\mathcal{LS}(f) = \{a \in \mathbb{F}_q^n \mid f(z+a) - f(z) \text{ const}\}$, then $\mathcal{LS}(f) \supseteq \mathbb{F}_q^t \times \{0_{n-t}\}$ ($a = (a', 0_{n-t})$ with $a' \in \mathbb{F}_q^t$)

Idea of the attack:

- recover Δ the quadratic components of $\mathcal{P}$ (assume $|\Delta| = q^t - 1$)
- $\exists$ t-dimensional vector subspace of $V \subseteq \mathbb{F}_q^n$ s.t. $V \subseteq \bigcap_{f \in \Delta} \mathcal{LS}(f)$
- then $L_2(V) = \mathbb{F}_q^t \times \{0_{n-t}\}$, with $A_2(\cdot) = L_2(\cdot) + const$

In V there are t linearly independent vectors which form the first t columns of L_2^{-1}

A variant in univariate form $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$

Set $q = 2,\ Tr_n(x) = x + x^2 + \cdots + x^{2^{n-1}}$.
Examples of $\mathcal{A} : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, $\mathcal{A}(\Gamma_F) = \Gamma_G$

$$\mathcal{A}_1 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + \gamma_1 Tr_n(\theta x + \lambda y) \\ \gamma_1 Tr_n(\theta x) + y \end{pmatrix}, \quad \mathcal{A}_2 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + \gamma_2 Tr_n(\lambda y) \\ y \end{pmatrix}$$

under some restriction on the parameters

- Not UOV-CCZ instances
- If F is easily invertible, $\mathcal{P}$ constructed with (one of) these transformations can be used in a cryptographic scheme
- $\deg(\mathcal{P}) \leq 3$

To conclude

We proposed a scheme which "hides" the central map F via a CCZ-transformation and we performed a preliminary security analysis.

We believe that more interesting results can come out by connecting further the theory of Boolean functions with the theory of multivariate cryptography.

To conclude

We proposed a scheme which "hides" the central map F via a CCZ-transformation and we performed a preliminary security analysis.

We believe that more interesting results can come out by connecting further the theory of Boolean functions with the theory of multivariate cryptography.

Thank you for your attention

Some references

L. Budaghyan, M. Calderini, I. Villa. On relations between CCZ-and EA-equivalences. Cryptography and Communications 12 (2020): 85-100.

M. Calderini, A. Caminata, I. Villa, A new multivariate primitive from CCZ equivalence. arXiv:2405.20968, 2024.

A. Canteaut, L. Perrin. On CCZ-equivalence, extended-affine equivalence, and function twisting. Finite Fields and Their Applications. 2019 Mar 1;56:209-46.

J. Jeong, N. Koo, S. Kwon. On the Functions Which are CCZ-equivalent but not EA-equivalent to Quadratic Functions over $\mathbb{F}_{p^n}$. arXiv preprint arXiv:2306.13718, (2023).

T. Matsumoto, H. Imai. Public quadratic polynomial-tuples for efficient signature verification and message-encryption, in EUROCRYPT 1988. LNCS, vol. 330 (Springer, 1988), pp. 419-553.

J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88, in CRYPTO 1995. LNCS, vol. 963 (Springer, 1995), pp. 248-261.