Analysis of Multivariate Encryption Schemes: Application to Dob

Morten Øygarden[1]
joint work with Patrick Felke[2] and Håvard Raddum[1]

[1]Simula UiB

[2]University of Applied Sciences Emden-Leer

May 2021

Part I - Introduction and the Dob Encryption Scheme

Multivariate Encryption

- **public key** system of d quadratic polynomial equations in $\mathbb{F}_2[x_1, \ldots, x_d]$.
- **encryption**: evaluate the polynomials $p_1(x_1, \ldots, x_d), \ldots, p_d(x_1, \ldots, x_d)$ on plaintext $(m_1, \ldots, m_d)$ to obtain $(c_1, \ldots, c_d)$.
- **decryption**: solve the system

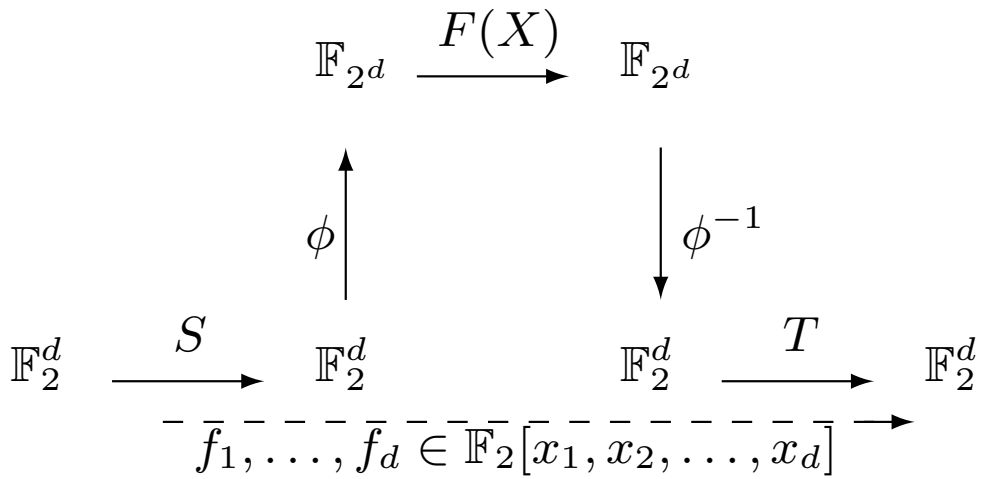
$$\begin{aligned} p_1(x_1, \ldots, x_d) &= c_1 \\ \ldots & \\ p_d(x_1, \ldots, x_d) &= c_d \end{aligned}$$

  to recover plaintext $(m_1, \ldots, m_d)$.
- **Pros**: Post-quantum secure, efficient encryption, compact ciphertext.
- **Cons**: Large public keys, inefficient decryption, unclear security.

The Dob Encryption Scheme

Macario–Rat and Patarin, 2018

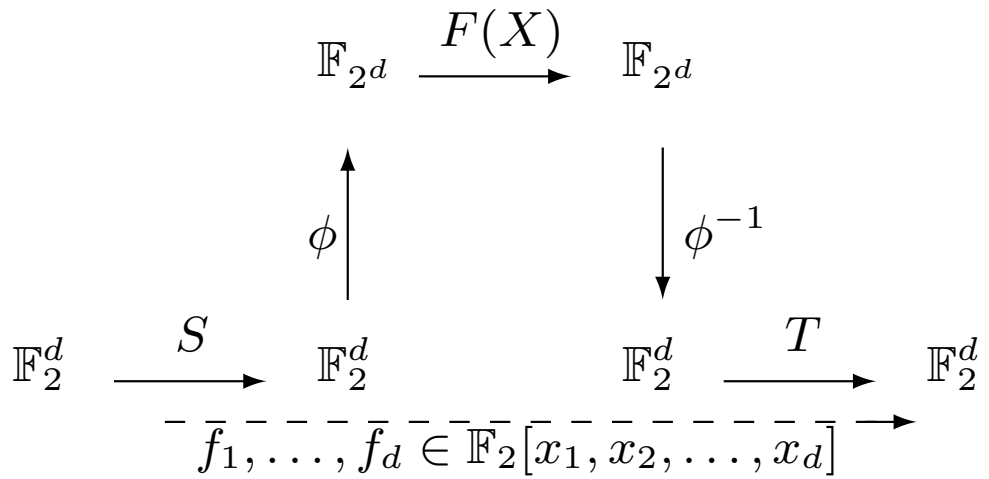
Let $S, T \in \mathbb{F}_2^{d \times d}$ be invertible, secret matrices. $\phi : \mathbb{F}_2^d \to \mathbb{F}_{2^d}$ an isomorphism.



The Dob Encryption Scheme

Macario–Rat and Patarin, 2018

Let $S, T \in \mathbb{F}_2^{d \times d}$ be invertible, secret matrices. $\phi : \mathbb{F}_2^d \to \mathbb{F}_{2^d}$ an isomorphism.



$F(X) = X^{2^m+1} + X^3 + X$, $d = 2m - 1$, is the Dobbertin permutation.

The owner of the secret key can find a polynomial equation of low degree, which is used for decryption.

Modifications

Let $f_1, \ldots, f_d$ be the polynomials from (unmodified) Dob. There will be *degree fall polynomials* at degree 3, i.e., combinations

$$\sum_{i,j} c_{i,j} x_i f_j, \qquad c_{i,j} \in \mathbb{F}_2$$

having degree 2. This makes it vulnerable to Gröbner basis attacks.

Modifications

Let $f_1, \ldots, f_d$ be the polynomials from (unmodified) Dob. There will be *degree fall polynomials* at degree 3, i.e., combinations

$$\sum_{i,j} c_{i,j} x_i f_j, \qquad c_{i,j} \in \mathbb{F}_2$$

having degree 2. This makes it vulnerable to Gröbner basis attacks.

Solution: add modifiers.

- *internal perturbation* (*ip*): choose k linear forms $v_1, \ldots, v_k$, and add quadratic combinations of them to the public key.

$$p_i = f_i + \sum_{j,l} a_{j,l} v_j v_l, \qquad a_{j,l} \in \mathbb{F}_2$$

Modifications

Let $f_1, \ldots, f_d$ be the polynomials from (unmodified) Dob. There will be *degree fall polynomials* at degree 3, i.e., combinations

$$\sum_{i,j} c_{i,j} x_i f_j, \qquad c_{i,j} \in \mathbb{F}_2$$

having degree 2. This makes it vulnerable to Gröbner basis attacks.

Solution: add modifiers.

- *internal perturbation* (*ip*): choose k linear forms $v_1, \ldots, v_k$, and add quadratic combinations of them to the public key.

$$p_i = f_i + \sum_{j,l} a_{j,l} v_j v_l, \qquad a_{j,l} \in \mathbb{F}_2$$

- Q_+: choose t quadratic polynomials $q_1, \ldots, q_t$, and add linear combinations of them to the public key.

$$p_i = f_i + \sum_{j} a_j q_j, \qquad a_j \in \mathbb{F}_2$$

Modifications

Let $f_1, \ldots, f_d$ be the polynomials from (unmodified) Dob. There will be *degree fall polynomials* at degree 3, i.e., combinations

$$\sum_{i,j} c_{i,j} x_i f_j, \qquad c_{i,j} \in \mathbb{F}_2$$

having degree 2. This makes it vulnerable to Gröbner basis attacks.

Solution: add modifiers.

- *internal perturbation* (*ip*): choose k linear forms $v_1, \ldots, v_k$, and add quadratic combinations of them to the public key.

$$p_i = f_i + \sum_{j,l} a_{j,l} v_j v_l, \qquad a_{j,l} \in \mathbb{F}_2$$

- Q_+: choose t quadratic polynomials $q_1, \ldots, q_t$, and add linear combinations of them to the public key.

$$p_i = f_i + \sum_{j} a_j q_j, \qquad a_j \in \mathbb{F}_2$$

Suggested 80–bit parameters: $d = 129$, $t = k = 6$.

Part II - Counting Degree Fall Polynomials

Setting

- We work with homogeneous ideals and over a graded ring.
- $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle$.
- For a polynomial g, g^h will denote the leading form.
- Define the homogeneous ideal $\mathcal{P} = \langle p_1^h, \ldots, p_d^h \rangle$. ($M$ is similarly defined for the modifier polynomials).
- $\mathcal{P}_l$ denotes the degree l part of $\mathcal{P}$. E.g., $\mathcal{P}_3$ contains the combinations

$$\sum_{i,j} a_{i,j} x_i p_j^h, \qquad \text{for } a_{i,j} \in \mathbb{F}_2.$$

Let f_i^h denote a polynomial from *unmodified* Dob, p_i^h a *modified* public polynomial, and m_j^h a modifier polynomial (both Q_+ and ip):

$$p_i^h = f_i^h + \sum_j m_j^h.$$

Let f_i^h denote a polynomial from *unmodified* Dob, p_i^h a *modified* public polynomial, and m_j^h a modifier polynomial (both Q_+ and ip):

$$p_i^h = f_i^h + \sum_j m_j^h.$$

Unmodified Dob will have many degree fall polynomials, which we can write as combinations:

$$\sum_{i,j} g_i^h f_j^h = 0,$$

for some polynomials g_i^h.

Let f_i^h denote a polynomial from *unmodified* Dob, p_i^h a *modified* public polynomial, and m_j^h a modifier polynomial (both Q_+ and ip):

$$p_i^h = f_i^h + \sum_j m_j^h.$$

Unmodified Dob will have many degree fall polynomials, which we can write as combinations:

$$\sum_{i,j} g_i^h f_j^h = 0,$$

for some polynomials g_i^h.

Using p_j^h in place of f_j^h, we now get:

$$\sum_{i,j} g_i^h p_j^h = \sum_{i,j} g_i^h m_j^h \in M.$$

As a result, one way to estimate the number of degree fall polynomials at degree ν is given by:

$$N_\nu^{(0,0)} = \dim((\mathcal{S}(\mathcal{F}))_\nu) - \dim(M_\nu) + \dim((\mathcal{P}_M)_\nu),$$

where

- $\mathcal{S}(\mathcal{F})$ is the (non trivial) syzygies in the unmodified Dob system.
- M the ideal generated by the modifiers.
- $\mathcal{P}_M$ a "correction component".

All of these components can be computed (at least for smaller degrees).

Different estimates can be found by considering certain subsets of the degree fall polynomials. We denote these estimates $N_\nu^{(i,j)}$, $i, j \geq 0$. (See the paper for more information).

We expect the number of first fall polynomials at degree ν to be the largest of these estimates (0 if all are negative).

Example

d: degree of field extension. n: number of variables. t: $\#Q_+$ modifiers. k: $\#ip$ modifiers.

$$N_3^{(0,0)} = \overbrace{2d}^{\dim(\mathcal{S}(\mathcal{F})_3)} - \underbrace{\overbrace{\left((n-k)\binom{k}{2} + \binom{k}{3}\right)}^{ip} - \overbrace{nt}^{Q_+}}_{\dim(M_3)}.$$

Example

d: degree of field extension. n: number of variables. t: $\#Q_+$ modifiers. k: $\#ip$ modifiers.

$$N_3^{(0,0)} = \overbrace{2d}^{\dim(\mathcal{S}(\mathcal{F})_3)} - \underbrace{\overbrace{\left((n-k)\binom{k}{2} + \binom{k}{3}\right)}^{ip} - \overbrace{nt}^{Q_+}}_{\dim(M_3)}.$$

$$N_4^{(0,0)} = \overbrace{(2n-1)d}^{\dim(\mathcal{S}(\mathcal{F})_4)}$$

$$- \underbrace{\overbrace{\left(t\binom{n}{2} - \binom{t}{2} - t\right)}^{Q_+} - \overbrace{\left(\binom{k}{2}\binom{n-k}{2} + \binom{k}{3}(n-k) + \binom{k}{4}\right)}^{ip} + \overbrace{t\binom{k}{2}}^{Q_+ \cap ip}}_{\dim(M_4)}$$

$$+ \underbrace{d\left(t + \binom{k}{2}\right)}_{\dim((\mathcal{P}_{M^{(2,1)}})_4)}$$

Experiments

d: degree of field extension. n: number of variables. t: $\#Q_+$ modifiers. k: $\#ip$ modifiers.

d	n	t (+)	k *(ip)*	N (predicted)	N (Magma)
53	53	0	0	$N_3^{(0,0)}$: 106	106
53	53	0	3	$N_4^{(0,0)}$: 1999	1999
53	53	3	0	$N_4^{(0,0)}$: 1596	1596
59	29	0	7	$N_4^{(1,0)}$: 21	21
37	25	2	3	$N_4^{(0,0)}$: 692	692
31	29	0	8	$N_5^{(1,1)}$: 478	478
31	30	0	8	$N_5^{(2,1)}$: 264	264
39	37	1	7	$N_5^{(2,1)}$: 136	136
57	38	4	6	$N_5^{(1,1)}$: 2086	2086
57	37	4	6	$N_5^{(1,1)}$: 2847	2847
129	50	6	6	$N_5^{(0,0)}$: 64024	64024

Part III - Attack on Dob

Observation 1

Recall at degree 4:

$$N_4^{(0,0)} = \dim((\mathcal{S}(\mathcal{F}))_4) - \dim(M_4) + \dim((\mathcal{P}_M)_4),$$

where $\dim((\mathcal{P}_M)_4) = d\left(t + \binom{k}{2}\right)$.

Observation 1

Recall at degree 4:

$$N_4^{(0,0)} = \dim((\mathcal{S}(\mathcal{F}))_4) - \dim(M_4) + \dim((\mathcal{P}_M)_4),$$

where $\dim((\mathcal{P}_M)_4) = d\left(t + \binom{k}{2}\right)$.

If we add a randomly chosen quadratic polynomial, p_R, to the system $\mathcal{P}$, we expect this effect to increase to $(d+1)\left(t + \binom{k}{2}\right)$.
The increase is due to the combinations $m_i^h p_R$.

Observation 1

This means that we can compute degree fall polynomials (syzygies), which will be of the form[a]:

$$\sum_{i,j} g_i^h p_j^h + \sum_l m_l^h p_R = 0.$$

[a] slight simplification

Observation 1

This means that we can compute degree fall polynomials (syzygies), which will be of the form[a]:

$$\sum_{i,j} g_i^h p_j^h + \sum_l m_l^h p_R = 0.$$

In particular, we learn something about the secret modifiers by inspecting what we multiplied with p_R.

[a] slight simplification

Observation 1

This means that we can compute degree fall polynomials (syzygies), which will be of the form[a]:

$$\sum_{i,j} g_i^h p_j^h + \sum_l m_l^h p_R = 0.$$

In particular, we learn something about the secret modifiers by inspecting what we multiplied with p_R.

Still difficult to compute directly, due to a high degree and a large number of variables.

[a] slight simplification

Observation 2

Setting variables to zero greatly simplifies the system.

Observation 2

Setting variables to zero greatly simplifies the system.

Let $W_1 = \{x_{1_1}, \ldots, x_{1_r}\}$ be a set of variables. The same observation hold for the projected system:

$$\sum_{i,j} g_i^h|_{W_1=0}\, p_j^h|_{W_1=0} + \sum_l m_l^h|_{W_1=0}\, p_R|_{W_1=0} = 0.$$

Observation 2

Setting variables to zero greatly simplifies the system.

Let $W_1 = \{x_{1_1}, \ldots, x_{1_r}\}$ be a set of variables. The same observation hold for the projected system:

$$\sum_{i,j} g_i^h|_{W_1=0}\, p_j^h|_{W_1=0} + \sum_l m_l^h|_{W_1=0}\, p_R|_{W_1=0} = 0.$$

We can "glue" together several local polynomials $m^h|_{W_1=0}, \ldots, m^h|_{W_\rho=0}$, to recover the (global) modifier polynomial m^h.

Simplified Overview of the Attack

1) Choose appropriate sets of variables $W_1, \ldots, W_\rho$.

Simplified Overview of the Attack

1) Choose appropriate sets of variables $W_1, \ldots, W_\rho$.

2) Form $\{\mathcal{P}, p_R\}$, by including a randomly chosen polynomial p_R.

Simplified Overview of the Attack

1) Choose appropriate sets of variables $W_1, \ldots, W_\rho$.

2) Form $\{\mathcal{P}, p_R\}$, by including a randomly chosen polynomial p_R.

3) For each W_i, find degree fall polynomials for the projected polynomial set $\{\mathcal{P}, p_R\}|_{W_i=0}$. This yields the projected modifiers $m_j^h|_{W_i=0}$.

Simplified Overview of the Attack

1) Choose appropriate sets of variables $W_1, \ldots, W_\rho$.

2) Form $\{\mathcal{P}, p_R\}$, by including a randomly chosen polynomial p_R.

3) For each W_i, find degree fall polynomials for the projected polynomial set $\{\mathcal{P}, p_R\}|_{W_i=0}$. This yields the projected modifiers $m_j^h|_{W_i=0}$.

4) Glue together the various $m_j^h|_{W_i=0}$ to find the quadratic form of the secret modifiers, m_j^h.

Effect on the Suggested Parameters for 80–bit security.

$d = 129$, $t = k = 6$

The new attack retrieves the (quadratic form of) the secret modifiers after 2^{63} operations.

With this information, we can decrypt ciphertexts using somewhere between 2^{67} and 2^{77} operations (depending on ω). This second step might be improved further.

Conclusions and Further Work

- The attack breaks the suggested parameters for the Dob encryption scheme, and we do not see any way to make this secure and efficient.
- The presented ideas might be applied to other central maps (e.g., C^* and HFE), and other modifiers (e.g., minus, vinegar and projection).
- The attack is effective against encryption schemes, while signature schemes can be secured against it.