The Degree of Regularity of HFE Systems

Vivien Dubois[1] and Nicolas Gama[2]

(1) DGA Rennes et (2) Université de Versailles

HFE

HFE is a public key encryption/signature scheme [Pat96].

Public key : A system of multivariate polynomials
eg : 128 polynoms of degree 2 in 128 variables over $\mathbb{F}_2$.

In general, one **cannot** efficently solve such system.

HFE

HFE is a public key encryption/signature scheme [Pat96].

Public key : A system of multivariate polynomials
eg : 128 polynoms of degree 2 in 128 variables over $\mathbb{F}_2$.

In general, one **cannot** efficently solve such system.

This system has a **hidden structure** by some **secret ismorphism** Φ,
allows to solve it efficiently.

HFE

HFE is a public key encryption/signature scheme [Pat96].

Public key : A system of multivariate polynomials
eg : 128 polynoms of degree 2 in 128 variables over $\mathbb{F}_2$.

In general, one **cannot** efficently solve such system.

This system has a **hidden structure** by some **secret ismorphism** Φ, allows to solve it efficiently.

Hidden structure = **large monovariate polynomial**
(Hidden Field Equation)

$$\left\{ \begin{array}{c} p_1(x_1, \ldots, x_n) \\ \vdots \\ p_n(x_1, \ldots, x_n) \end{array} \right. = \Phi(F)$$

Degree of regularity

A property of systems of polynomials [BFS03].
It controls the **complexity of generic algebraic attacks** on the system.

Degree of regularity

A property of systems of polynomials [BFS03].
It controls the **complexity of generic algebraic attacks** on the system.

Generic attack = combination of increasing degree of input polynomials. eg : Gröbner bases, variants of XL.

Degree of regularity

A property of systems of polynomials [BFS03].
It controls the **complexity of generic algebraic attacks** on the system.

Generic attack = combination of increasing degree of input polynomials. eg : Gröbner bases, variants of XL.

A **race** between possible combinations and the **monomial basis** of expression.

Degree of regularity

A property of systems of polynomials [BFS03].
It controls the **complexity of generic algebraic attacks** on the system.

Generic attack = combination of increasing degree of input polynomials. eg : Gröbner bases, variants of XL.

A **race** between possible combinations and the **monomial basis** of expression.

Whenever a combination in **degree** d **falls** in degree $d-1$, one obtains a new **information on the ideal***.

Degree of regularity

A property of systems of polynomials [BFS03].
It controls the **complexity of generic algebraic attacks** on the system.

Generic attack = combination of increasing degree of input polynomials. eg : Gröbner bases, variants of XL.

A **race** between possible combinations and the **monomial basis** of expression.

Whenever a combination in **degree** d **falls** in degree $d-1$, one obtains a new **information on the ideal***.

When such falls **occur by saturation** of deg d layer,
many independent falls follow.

Degree of regularity

A property of systems of polynomials [BFS03].
It controls the **complexity of generic algebraic attacks** on the system.

Generic attack = combination of increasing degree of input polynomials. eg : Gröbner bases, variants of XL.

A **race** between possible combinations and the **monomial basis** of expression.

Whenever a combination in **degree** d **falls** in degree $d-1$, one obtains a new **information on the ideal***.

When such falls **occur by saturation** of deg d layer,
many independent falls follow.

We call **degree of regularity** the degree of first fall.

Degree of regularity

New polynomials will in turn
saturate the degree $d-1$ **layer**, etc...

In the end, the last polynomials *characterize* the solutions.

The case of HFE

Experimental Fact

The degree of regularity of HFE is lower than on random quadratic systems. [Fau02,Cou01]

HFE systems **are easier to solve** using generic tools than random systems.

The case of HFE

Experimental Fact

The degree of regularity of HFE is lower than on random quadratic systems. [Fau02,Cou01]

HFE systems **are easier to solve** using generic tools than random systems.

Why on earth ? ? ?

The hidden structure doesn't seem to have a *multivariate* meaning...

The case of HFE

Experimental Fact

The degree of regularity of HFE is lower than on random quadratic systems. [Fau02,Cou01]

HFE systems **are easier to solve** using generic tools than random systems.

Why on earth ? ? ?

The hidden structure doesn't seem to have a *multivariate* meaning...

First answers [FJ03]

- Relationship between combinations of the public polynomials and **combinations on the secret univariate polynomial and *derivatives***.

The case of HFE

How bad is it ?

What is the degree of regularity of HFE ?

The case of HFE

How bad is it ?

What is the degree of regularity of HFE ?

First answers [GJS06]

- **An upper bound** on the degree of regularity **over** $\mathbb{F}_2$.
- Uses results on generic quadratic systems [BFS03].

The case of HFE

How bad is it ?

What is the degree of regularity of HFE ?

First answers [GJS06]

- **An upper bound** on the degree of regularity **over** $\mathbb{F}_2$.
- Uses results on generic quadratic systems [BFS03].

What about larger fields ? ? ? Better or Worse ? ?

Today

Precisely describe the **connection between degree of regularity** of the public system **and** the one of the **secret polynomial and derivatives**.

How to **bound the degree of regularity** of HFE systems **over any field**.

Degree of regularity of a quadratic system

Quadratic systems

- A system $p_1, \ldots, p_k$ of degree 2 polynomials in n variables over $\mathbb{F}_q$.
- These polynomials are seen as functions from $(\mathbb{F}_q)^n$ to $\mathbb{F}_q$.
- Variables are constrained by field equations

$$x_i^q - x_i = 0, \ (\text{or } x_i^q \to x_i) \quad i = 1, \ldots, n$$

- We work in the reduced ring

$$R_q = \mathbb{F}_q[x_1, \ldots, x_n]/\{x_1^q - x_1, \ldots, x_n^q - x_n\}$$

- Elements of R_q are vectors on the reduced monomial basis (*i.e* without powers of q).

Combinations of quadratic polynomials

- We call **combinations in degree** d :

$$\{m_1 p_1 + \cdots + m_k p_k, \quad \deg(m_i) = d-2,\ i = 1, \ldots, n\}$$

- It is the image by the linear application :

$$\begin{array}{cccccc} \sigma_d(p_1, \ldots, p_k) & : & \left((R_q)_{\leq d-2}\right)^k & \longrightarrow & (R_q)_{\leq d} \\ & & (m_1, \ldots, m_k) & \longmapsto & m_1 p_1 + \cdots + m_k p_k. \end{array}$$

Combinations of quadratic polynomials

- We call **combinations in degree** d :

$$\{m_1 p_1 + \cdots + m_k p_k, \quad \deg(m_i) = d-2,\ i = 1, \ldots, n\}$$

- It is the image by the linear application :

$$\begin{array}{rcccl} \sigma_d(p_1, \ldots, p_k) & : & \left((R_q)_{\leq d-2}\right)^k & \longrightarrow & (R_q)_{\leq d} \\ & & (m_1, \ldots, m_k) & \longmapsto & m_1 p_1 + \cdots + m_k p_k. \end{array}$$

- Its kernel is in general non zero !
  Examples :
  - $(p_2, -p_1, 0, \ldots, 0) \longrightarrow (p_2)p_1 + (-p_1)p_2 = 0$
  - $(p_1^{q-1} - 1, 0, 0, \ldots, 0) \longrightarrow (p_1^{q-1} - 1)p_1 = p_1^q - p_1 = 0$

Combinations of quadratic polynomials

- We call **combinations in degree** d :

$$\{m_1 p_1 + \cdots + m_k p_k, \quad \deg(m_i) = d-2,\ i = 1, \ldots, n\}$$

- It is the image by the linear application :

$$\begin{array}{cccccc} \sigma_d(p_1, \ldots, p_k) & : & ((R_q)_{\leq d-2})^k & \longrightarrow & (R_q)_{\leq d} \\ & & (m_1, \ldots, m_k) & \longmapsto & m_1 p_1 + \cdots + m_k p_k. \end{array}$$

- Its kernel is in general non zero !
  Examples :
  - $(p_2, -p_1, 0, \ldots, 0) \quad \longrightarrow (p_2)p_1 + (-p_1)p_2 = 0$
  - $(p_1^{q-1} - 1, 0, 0, \ldots, 0) \quad \longrightarrow (p_1^{q-1} - 1)p_1 = p_1^q - p_1 = 0$

- These $(m_1, \ldots, m_k)$ are **trivial** : they exist for any $p_1, \ldots, p_n$!

Trivial Syzygies

- We call **trivial syzygies** the elements of the kernel which exist even when the $p_1, \ldots, p_n$ are indeterminates.

Trivial Syzygies

- We call **trivial syzygies** the elements of the kernel which exist even when the $p_1, \ldots, p_n$ are indeterminates.

Formal definition

- We extend R_q with new variables $y_1, \ldots, y_k$.

$$\bar{R}_q = R_q[y_1, \ldots, y_k]/\{y_1^q - y_1, \ldots, y_k^q - y_k\}$$

Trivial Syzygies

- We call **trivial syzygies** the elements of the kernel which exist even when the $p_1, \ldots, p_n$ are indeterminates.

Formal definition

- We extend R_q with new variables $y_1, \ldots, y_k$.

$$\bar{R}_q = R_q[y_1, \ldots, y_k]/\{y_1^q - y_1, \ldots, y_k^q - y_k\}$$

- **Generic Trivial Syzygies** : the $(m_1, \ldots, m_k)$ of $\bar{R}_q$ such that

$$m_1 y_1 + \cdots + m_k y_k = 0$$

Trivial Syzygies

- We call **trivial syzygies** the elements of the kernel which exist even when the $p_1, \ldots, p_n$ are indeterminates.

Formal definition

- We extend R_q with new variables $y_1, \ldots, y_k$.

$$\bar{R}_q = R_q[y_1, \ldots, y_k]/\{y_1^q - y_1, \ldots, y_k^q - y_k\}$$

- **Generic Trivial Syzygies** : the $(m_1, \ldots, m_k)$ of $\bar{R}_q$ such that

$$m_1 y_1 + \cdots + m_k y_k = 0$$

- **Trivial Syzygies of** $(p_1, \ldots, p_k)$: the evaluations on $(p_1, \ldots, p_k)$ of the generic trivials.

Degree falls and degree of regularity

- We call **degree fall** an **Homogeneous** $(m_1, \ldots, m_k)$ of degree $d-2$ such that $[m_1 p_1 + \cdots + m_k p_k]_d = 0$.
- It is the kernel of

$$\begin{array}{rccccl} \sigma_d^h(p) & : & ((R_q)_{d-2})^k & \longrightarrow & (R_q)_d \\ & & (m_0, \ldots, m_{k-1}) & \longmapsto & [m_0 p_0 + \cdots + m_{k-1} p_{k-1}]_d. \end{array}$$

Degree falls and degree of regularity

- We call **degree fall** an **Homogeneous** $(m_1, \ldots, m_k)$ of degree $d-2$ such that $[m_1 p_1 + \cdots + m_k p_k]_d = 0$.
- It is the kernel of
$$\begin{array}{rcccl} \sigma_d^h(p) & : & ((R_q)_{d-2})^k & \longrightarrow & (R_q)_d \\ & & (m_0, \ldots, m_{k-1}) & \longmapsto & [m_0 p_0 + \cdots + m_{k-1} p_{k-1}]_d. \end{array}$$
- (Unfortunately) Homogeneous parts of degree $d-2$ of trivial Syzygies in degree $d-2$ are solutions !

  ... We call them **trivial degree falls**.

Degree falls and degree of regularity

- We call **degree fall** an **Homogeneous** $(m_1, \ldots, m_k)$ of degree $d-2$ such that $[m_1 p_1 + \cdots + m_k p_k]_d = 0$.
- It is the kernel of

$$\begin{array}{cccccc} \sigma_d^h(p) & : & ((R_q)_{d-2})^k & \longrightarrow & (R_q)_d \\ & & (m_0, \ldots, m_{k-1}) & \longmapsto & [m_0 p_0 + \cdots + m_{k-1} p_{k-1}]_d . \end{array}$$

- (Unfortunately) Homogeneous parts of degree $d-2$ of trivial Syzygies in degree $d-2$ are solutions !

  . . . We call them **trivial degree falls**.
- We call **degree of regularity** the smallest degree at which there exists *non-trivial* degree falls.

Degree falls and degree of regularity

- We call **degree fall** an **Homogeneous** $(m_1, \dots, m_k)$ of degree $d-2$ such that $[m_1 p_1 + \cdots + m_k p_k]_d = 0$.
- It is the kernel of

$$\begin{array}{cccccc} \sigma_d^h(p) & : & ((R_q)_{d-2})^k & \longrightarrow & (R_q)_d \\ & & (m_0, \dots, m_{k-1}) & \longmapsto & [m_0 p_0 + \cdots + m_{k-1} p_{k-1}]_d. \end{array}$$

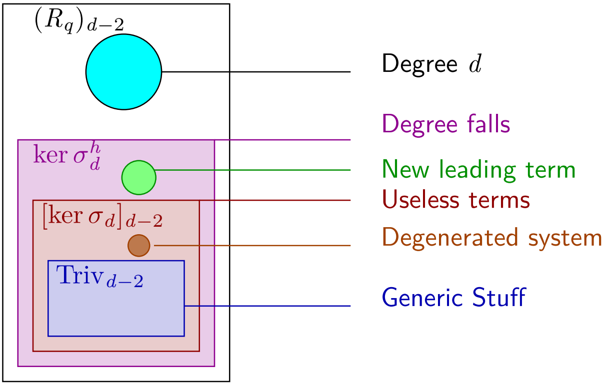
- (Unfortunately) Homogeneous parts of degree $d-2$ of trivial Syzygies in degree $d-2$ are solutions !

  ... We call them **trivial degree falls**.
- We call **degree of regularity** the smallest degree at which there exists *non-trivial* degree falls.

Remarks on the definition of degree of regularity

- Defined in [BFS03] by a *set theoretic* property.
- Here : it is an *algebraic* relying on trivial degree falls.

Degree of regularity vs Degree of computation



Degree of regularity vs Degree of computation

One always has

$$\ker(\sigma_d^h) \supseteq [\ker(\sigma_d)]_{d-2} \supseteq [\mathrm{Triv}]_{d-2}$$

- Degree of first useful fall : Smallest d such that $\ker(\sigma_d^h) \neq [\ker(\sigma_d)]_{d-2}$
- Degree of regularity : Smallest d such that $\ker(\sigma_d^h) \neq [\mathrm{Triv}]_{d-2}$
  - implies : Up to the degree of regularity, there are only trivials in $\ker(\sigma_d^h)$.
  - (Hopefully) on most systems, the first equality will fail first.
  - Example of a very bad system : $\{P, P, \ldots\}$.

Construction of HFE Systems

From the small field to the (secret) large one

- $\mathbb{F}_{q^n}$: extension of degree n of $\mathbb{F}_q$, it is a vector space over $\mathbb{F}_q$.
- Choose an arbitrary basis $S = (s_1, \ldots, s_n)$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
- S is viewed as a bijection : $(\mathbb{F}_q)^n \longrightarrow \mathbb{F}_{q^n}$

From the small field to the (secret) large one

- $\mathbb{F}_{q^n}$: extension of degree n of $\mathbb{F}_q$, it is a vector space over $\mathbb{F}_q$.
- Choose an arbitrary basis $S = (s_1, \ldots, s_n)$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
- S is viewed as a bijection : $(\mathbb{F}_q)^n \to \mathbb{F}_{q^n}$
- S induces a linear bijection : $\{\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}\} \longrightarrow \{(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n\}$

$$\Psi_S \; : P \quad \longmapsto \quad S^{-1} \circ P \circ S$$

From the small field to the (secret) large one

- $\mathbb{F}_{q^n}$: extension of degree n of $\mathbb{F}_q$, it is a vector space over $\mathbb{F}_q$.
- Choose an arbitrary basis $S = (s_1, \ldots, s_n)$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
- S is viewed as a bijection : $(\mathbb{F}_q)^n \to \mathbb{F}_{q^n}$
- S induces a linear bijection : $\{\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}\} \longrightarrow \{(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n\}$

$$\Psi_S \ : P \quad \longmapsto \quad S^{-1} \circ P \circ S$$

- Remark : $\{\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}\}$ is an algebra but not $\{(\mathbb{F}_q)^n \to (\mathbb{F}_q)^n\}$.

Example

- $C(X) = aX^{3q^2}$
- set $X = x_1 s_1 + \cdots + x_n s_n$
- then $X^{q^2} = x_1 s_1^{q^2} + \cdots + x_n s_n^{q^2}$
- $C(X) = \sum_{i,j,k} x_i x_j x_k \cdot a s_i^{q^2} s_j^{q^2} s_k^{q^2}$
- $S^{-1}(C(X)) = \sum_{i,j,k} x_i x_j x_k \cdot S^{-1}(a s_i^{q^2} s_j^{q^2} s_k^{q^2}) = \begin{cases} c_1(x_1, \ldots, x_n) \\ c_2(x_1, \ldots, x_n) \\ c_3(x_1, \ldots, x_n) \end{cases}$
- $\psi_S(C) = (c_1, c_2, c_3)$ are homogeneous of degree 3.

Transfering the multivariate degree

- More generally : X^a, with $a = (a_0, \ldots, a_{n-1})$ in basis q.
- X^a is the product of $a_0 + \cdots + a_{n-1}$ Frobenius with multiplicity.
- It is mapped by ψ_S to a (homogeneous) system of degree $a_0 + \cdots + a_{n-1}$ over $\mathbb{F}_q$.

Transfering the multivariate degree

- More generally : X^a, with $a = (a_0, \ldots, a_{n-1})$ in basis q.
- X^a is the product of $a_0 + \cdots + a_{n-1}$ Frobenius with multiplicity.
- It is mapped by ψ_S to a (homogeneous) system of degree $a_0 + \cdots + a_{n-1}$ over $\mathbb{F}_q$.
- We call q-**degree** the value : $q\text{-deg}(X^a) = a_0 + \cdots + a_{n-1}$

Transfering the multivariate degree

- More generally : X^a, with $a = (a_0, \ldots, a_{n-1})$ in basis q.
- X^a is the product of $a_0 + \cdots + a_{n-1}$ Frobenius with multiplicity.
- It is mapped by ψ_S to a (homogeneous) system of degree $a_0 + \cdots + a_{n-1}$ over $\mathbb{F}_q$.
- We call q-**degree** the value : $q\text{-deg}(X^a) = a_0 + \cdots + a_{n-1}$

Property

ψ_S is a bijection from $(\mathcal{R}_{q^n})_{q:d}$ to $((R_q)_d)^n$.

Proof : q-deg d implies degree $\leq d$ of the vector.
Then cardinality arguments.

HFE Functions

- One chooses $P(X)$ of q-deg 2,
- **and** one bounds powers of q by a parameter D :

$$P(X) = \sum_{i,j \leq D} a_{ij} X^{q^i + q^j} + \sum_{k \leq D} b_k X^{q^k} + c$$

HFE Functions

- One chooses $P(X)$ of q-deg 2,
- **and** one bounds powers of q by a parameter D :

$$P(X) = \sum_{i,j \leq D} a_{ij} X^{q^i + q^j} + \sum_{k \leq D} b_k X^{q^k} + c$$

- HFE functions are functions of q-deg 2 and degree $\leq 2q^D$.
- Small degree : For all a, finding the roots of $P(X) - a$ is efficient.
- The degree is a property in $\mathcal{R}_{q^n}$ viewed as an algebra.
- Its interpretation in $\mathcal{R}_{q^n} \simeq (R_q)^n$ is not clear.

HFE Functions

- One chooses $P(X)$ of q-deg 2,
- **and** one bounds powers of q by a parameter D :

$$P(X) = \sum_{i,j \leq D} a_{ij} X^{q^i + q^j} + \sum_{k \leq D} b_k X^{q^k} + c$$

- HFE functions are functions of q-deg 2 and degree $\leq 2q^D$.
- Small degree : For all a, finding the roots of $P(X) - a$ is efficient.
- The degree is a property in $\mathcal{R}_{q^n}$ viewed as an algebra.
- Its interpretation in $\mathcal{R}_{q^n} \simeq (R_q)^n$ is not clear.

The cryptosystem

- The link with the field structure is secret : $S \to S$.
- The polynomial itself is secret : $P \to P$.
- $+$ a linear permutation T on the $p_1, \ldots, p_n$ (transparent for us).

Combinations of HFE polynomials

Transfering combinations of $\mathcal{R}_{q^n}$

- $p_1, \ldots, p_n$ the elements of R_q obtained from $(p_1, \ldots, p_n) = \psi_S(P)$.
- One considers combinations $m_1 p_1 + \cdots + m_n p_n$ de $p_1, \ldots, p_n$.
- These are **linear** combinations with coefficients over R_q.

We already know...

$$
\begin{array}{ccc}
\text{Secret} & & \text{Public} \\
P & \xrightarrow{\psi_S} & (p_0, \ldots, p_{n-1}) \\
q\text{-deg} & \longrightarrow & \text{deg} \\
q\text{-Homogeneous} & \longrightarrow & \text{Homogeneous} \\
\text{Combinations} & \longrightarrow & ??
\end{array}
$$

Transfering combinations of $\mathcal{R}_{q^n}$

Secret		Public
P	$\xrightarrow{\psi_S}$	$(p_0, \ldots, p_{n-1})$
$\sum_{i=0}^{n-1} M_i P^{q^i}$	$\xrightarrow{\psi_S}$	$\underbrace{\psi_S^*(M_0, \ldots, M_{n-1})} \cdot \begin{pmatrix} p_0 \\ \vdots \\ p_{n-1} \end{pmatrix}$
$(M_0, \ldots, M_{n-1})$	$\xrightarrow{\psi_s^*}$	$\begin{pmatrix} m_{0,0} & \cdots & m_{0,n-1} \\ \vdots & \ddots & \vdots \\ m_{n-1,0} & \cdots & m_{n-1,n-1} \end{pmatrix}$
$q\text{-deg}(M_i)$	$\xrightarrow{\psi_s^*}$	$\deg(m_{i,j})$
???	$\xrightarrow{??}$	deg falls
???	$\xrightarrow{??}$	trivials

Transfering degree falls

- Degree falls on $p_1, \ldots, p_n$ are the kernel of the map

$$\begin{array}{rcccl} \sigma_d^h(p_1, \ldots, p_n) & : & \left((R_q^h)_{d-2}\right)^n & \longrightarrow & (R_q^h)_d \\ & & (m_1, \ldots, m_n) & \longmapsto & [m_1 p_1 + \cdots + m_n p_n]_d. \end{array}$$

Transfering degree falls

- Degree falls on $p_1, \ldots, p_n$ are the kernel of the map

$$\begin{array}{rcccl} \sigma_d^h(p_1,\ldots,p_n) & : & \left((R_q^h)_{d-2}\right)^n & \longrightarrow & (R_q^h)_d \\ & & (m_1,\ldots,m_n) & \longmapsto & [m_1p_1+\cdots+m_np_n]_d. \end{array}$$

- Similarly, one has the map

$$\begin{array}{rcccl} \Sigma_d^h(P) & : & \left((\mathcal{R}_{q^n}^h)_{d-2}\right)^n & \longrightarrow & (\mathcal{R}_{q^n}^h)_d \\ & & (M_0,\ldots,M_{n-1}) & \longmapsto & [M_0P+M_1P^q+\cdots+M_{n-1}P^{q^{n-1}}]_d. \end{array}$$

Transfering degree falls

- Degree falls on $p_1, \ldots, p_n$ are the kernel of the map

$$\begin{array}{rcrcl} \sigma_d^h(p_1, \ldots, p_n) & : & \left((R_q^h)_{d-2}\right)^n & \longrightarrow & (R_q^h)_d \\ & & (m_1, \ldots, m_n) & \longmapsto & [m_1 p_1 + \cdots + m_n p_n]_d. \end{array}$$

- Similarly, one has the map

$$\begin{array}{rcrcl} \Sigma_d^h(P) & : & \left((\mathcal{R}_{q^n}^h)_{d-2}\right)^n & \longrightarrow & (\mathcal{R}_{q^n}^h)_d \\ & & (M_0, \ldots, M_{n-1}) & \longmapsto & [M_0 P + M_1 P^q + \cdots + M_{n-1} P^{q^{n-1}}]_d. \end{array}$$

- We prove that $\ker \Sigma_d^h$ is in bijection by ψ_S^* with $\ker \sigma_d^h$

Transfering degree falls

- Degree falls on $p_1, \ldots, p_n$ are the kernel of the map

$$\begin{array}{rcrcl} \sigma_d^h(p_1, \ldots, p_n) & : & \left((R_q^h)_{d-2}\right)^n & \longrightarrow & (R_q^h)_d \\ & & (m_1, \ldots, m_n) & \longmapsto & [m_1 p_1 + \cdots + m_n p_n]_d. \end{array}$$

- Similarly, one has the map

$$\begin{array}{rcrcl} \Sigma_d^h(P) & : & \left((\mathcal{R}_{q^n}^h)_{d-2}\right)^n & \longrightarrow & (\mathcal{R}_{q^n}^h)_d \\ & & (M_0, \ldots, M_{n-1}) & \longmapsto & [M_0 P + M_1 P^q + \cdots + M_{n-1} P^{q^{n-1}}]_d. \end{array}$$

- We prove that $\ker \Sigma_d^h$ is in bijection by ψ_S^* with $\ker \sigma_d^h$

$\Rightarrow$ **kernels have the same dimension !** (over their respective fields)

Transfering generic trivial syzygies

Trivial syzygies of the small field

- One extends R_q with indeterminates $y_1, \ldots, y_n$:

$$\bar{R}_q = R_q[y_1, \ldots, y_n]/\{y_1^q - y_1, \ldots, y_k^q - y_n\}$$

- Trivial Syzygies : $(m_1, \ldots, m_n)$ over $\bar{R}_q$ su that

$$m_1 y_1 + \cdots + m_n y_n = 0$$

- Notion of degree on the elements of $\bar{R}_q$: $(1,2)$-degree : $d_x + 2d_y$

Transfering generic trivial syzygies

Trivial syzygies of the small field

- One extends R_q with indeterminates $y_1, \ldots, y_n$:

$$\bar{R}_q = R_q[y_1, \ldots, y_n]/\{y_1^q - y_1, \ldots, y_k^q - y_n\}$$

- Trivial Syzygies : $(m_1, \ldots, m_n)$ over $\bar{R}_q$ su that

$$m_1 y_1 + \cdots + m_n y_n = 0$$

- Notion of degree on the elements of $\bar{R}_q$: $(1,2)$-degree : $d_x + 2d_y$

Similarly, on the large field

- Extend $\mathcal{R}_{q^n}$ with indeterminate Y : $\bar{\mathcal{R}}_{q^n} = \mathcal{R}_{q^n}[Y]/\{Y^q - Y\}$
- Trivial Syzygies : the $(M_0, \ldots, M_{n-1})$ over $\bar{\mathcal{R}}_{q^n}$ such that

$$M_0 Y + \cdots + m_n Y^{q^{n-1}} = 0$$

- Notion of degree on $\bar{\mathcal{R}}_{q^n}$: $(1,2)$-q-degree.

Transfering generic trivial syzygies

Like before,

- We extend the bijection $\bar{\psi}_S^*$ which maps combinations of $\bar{\mathcal{R}}_{q^n}$ and $(\bar{R}_q)^n$ and preserves the $(1, 2)$-degree.
- **Thus : Generic trivials are in bijection.**

Transfering generic trivial syzygies

Like before,

- We extend the bijection $\bar{\psi}_S^*$ which maps combinations of $\bar{\mathcal{R}}_{q^n}$ and $(\bar{R}_q)^n$ and preserves the $(1,2)$-degree.
- **Thus : Generic trivials are in bijection.**

Transfering trivial syzygies

- Trivial syzygies in degree d of $(p_1, \ldots, p_n)$ are the evaluations in $(p_1, \ldots, p_n)$ of the generic trivial syzygies of $(1,2)$-degree d.
- They are associated to the trivial syzygies of P in q-degree d.
- Similarly : Their highest degree homogeneous part are associated.

Transfering the degree of regularity

$$\begin{array}{rcccl} \Sigma_d^h(P) & : & \left((\mathcal{R}_{q^n}^h)_{d-2}\right)^n & \longrightarrow & (\mathcal{R}_{q^n}^h)_d \\ & & (M_0, \ldots, M_{n-1}) & \longmapsto & [M_0 P + M_1 P^q + \cdots + M_{n-1} P^{q^{n-1}}]_d. \end{array}$$

The **degree of regularity** of $(p_1, \ldots, p_n) = \psi_S(P)$ is the smallest d such that the kernel of $\Sigma_d^h(P)$ contains non-trivial elements.

Multivariate rewriting of $\mathcal{R}_{q^n}$

$$\mathcal{R}_{q^n} = \mathbb{F}_{q^n}[X]/(X^{q^n} - X)$$

- One rewrites Frobenius as multivariate variables [GJS06] : $X_0, \ldots, X_{n-1}$ with $X_i = X^{q^i}$.

Multivariate rewriting of $\mathcal{R}_{q^n}$

$$\mathcal{R}_{q^n} = \mathbb{F}_{q^n}[X]/(X^{q^n} - X)$$

- One rewrites Frobenius as multivariate variables [GJS06] : $X_0, \ldots, X_{n-1}$ with $X_i = X^{q^i}$.
- One then has the rewriting rules $X_i^q \to X_{i+1}$.
- $\mathcal{R}_{q^n}$ is identified with the multivariate ring

$$\mathbb{F}_{q^n}[X_0, \ldots, X_{n-1}]/\{X_0^q - X_1, \ldots, X_{n-1}^q - X_0\}.$$

- The q-degree becomes degree in multivariate notation.

Multivariate rewriting of $\mathcal{R}_{q^n}$

$$\mathcal{R}_{q^n} = \mathbb{F}_{q^n}[X]/(X^{q^n} - X)$$

- One rewrites Frobenius as multivariate variables [GJS06] : $X_0, \ldots, X_{n-1}$ with $X_i = X^{q^i}$.
- One then has the rewriting rules $X_i^q \to X_{i+1}$.
- $\mathcal{R}_{q^n}$ is identified with the multivariate ring
$$\mathbb{F}_{q^n}[X_0, \ldots, X_{n-1}]/\{X_0^q - X_1, \ldots, X_{n-1}^q - X_0\}.$$
- The q-degree becomes degree in multivariate notation.
- Similarly, on writes $P_0, \ldots, P_{n-1}$ the Frobenius of P.
- The definition of trivial Syzygies rewrites easily.

Multivariate rewriting of $\mathcal{R}_{q^n}$

$$\mathcal{R}_{q^n} = \mathbb{F}_{q^n}[X]/(X^{q^n} - X)$$

- One rewrites Frobenius as multivariate variables [GJS06] : $X_0, \ldots, X_{n-1}$ with $X_i = X^{q^i}$.
- One then has the rewriting rules $X_i^q \to X_{i+1}$.
- $\mathcal{R}_{q^n}$ is identified with the multivariate ring
$$\mathbb{F}_{q^n}[X_0, \ldots, X_{n-1}]/\{X_0^q - X_1, \ldots, X_{n-1}^q - X_0\}.$$
- The q-degree becomes degree in multivariate notation.
- Similarly, on writes $P_0, \ldots, P_{n-1}$ the Frobenius of P.
- The definition of trivial Syzygies rewrites easily.

Degree of regularity of $(p_1, \ldots, p_n) = \psi_S(P)$ in R_q

$=$

degree of regularity of $P_0, \ldots, P_{n-1}$ in $\mathcal{R}_{q^n}$ multivariate.

Final Characterization of the degree of regularity

Finally, since one only cares about the highest degree homogeneous layer (degree falls and trivials), we can equivalently work with $X_i^q \rightarrow X_{i+1}$ or $X_i^q \rightarrow 0$.

The degree of regularity of $(p_1, \ldots, p_n) = \psi_S(P)$ in R_q

$$=$$

the degree of regularity of $\hat{P}_0, \ldots, \hat{P}_{n-1}$ in $\mathcal{R}_{q^n}$
where $\mathcal{R}_{q^n} = \mathbb{F}_{q^n}[X_0, \ldots, X_{n-1}]/\{X_0^q, \ldots, X_{n-1}^q\}$

Bounding the degree of regularity of HFE systems

Bounding the degree of regularity in general

general idea

- One assumes $\mathrm{Triv}(P_{0..k-1})_{d-2} = \ker \Sigma_d^h(P_{0..k-1})$ for $d \uparrow$
- Until contradiction,
  (like $\dim \mathrm{Triv}(P_{0..k-1})_{d-2} > \dim \ker \Sigma_d^h(P_{0..k-1})$)

Bounding the degree of regularity in general

general idea

- One assumes $\mathrm{Triv}(P_{0..k-1})_{d-2} = \ker \Sigma_d^h(P_{0..k-1})$ for $d \uparrow$
- Until contradiction,
  (like $\dim \mathrm{Triv}(P_{0..k-1})_{d-2} > \dim \ker \Sigma_d^h(P_{0..k-1})$)
- Then : we are already above the degree of regularity !
  MQ Bound

The case of HFE Systems

- Since : $P(X) = \sum_{i,j \leq D} a_{ij} X^{q^i + q^j} + \sum_{k \leq D} b_k X^{q^k} + c$

The case of HFE Systems

- Since : $P(X) = \sum_{i,j \leq D} a_{ij} X^{q^i + q^j} + \sum_{k \leq D} b_k X^{q^k} + c$
- where $D \ll n$ is a parameter, our system has the shape :

$$\begin{cases} P_0(X_0, \ldots, X_D) \\ P_1(X_1, \ldots, X_{D+1}) \\ \quad \vdots \\ P_{n-1}(X_{n-1}, \ldots, X_{D-1}). \end{cases}$$

- Each polynomial is expressed over a small subset of variables.

The case of HFE Systems

- Since : $P(X) = \sum_{i,j \leq D} a_{ij} X^{q^i + q^j} + \sum_{k \leq D} b_k X^{q^k} + c$
- where $D \ll n$ is a parameter, our system has the shape :

$$\begin{cases} P_0(X_0, \ldots, X_D) \\ P_1(X_1, \ldots, X_{D+1}) \\ \quad \vdots \\ P_{n-1}(X_{n-1}, \ldots, X_{D-1}). \end{cases}$$

- Each polynomial is expressed over a small subset of variables.

Property [GJS06]

- Contains small subsystems.
- $\mathcal{S}_k = \{P_0, \ldots, P_{k-1}\}$ is expressed on the m_k first variables,

$$m_k = \min\{D + k, n\}.$$

The case of HFE Systems

However

What is the link between degree of regularity of the system and the one of a subsystem ?

The case of HFE Systems

However

What is the link between degree of regularity of the system and the one of a subsystem ?

- With the set theoretic definition of BFS04 : OK

$\Rightarrow$ degree of regularity of subsystem $>$ of the full system.

The case of HFE Systems

However

What is the link between degree of regularity of the system and the one of a subsystem ?

- With the set theoretic definition of BFS04 : OK

$\Rightarrow$ degree of regularity of subsystem $>$ of the full system.

- With our definition :
  - Deg. fall of a subsystem $\Rightarrow$ deg. fall on the full system OK

The case of HFE Systems

However

What is the link between degree of regularity of the system and the one of a subsystem ?

- With the set theoretic definition of BFS04 : OK

$\Rightarrow$ degree of regularity of subsystem $>$ of the full system.

- With our definition :
  - Deg. fall of a subsystem $\Rightarrow$ deg. fall on the full system OK
  - Non-trivial for a subsystem $\Rightarrow$ Non-trivial for the full system ? ?

The case of HFE Systems

However

What is the link between degree of regularity of the system and the one of a subsystem ?

- With the set theoretic definition of BFS04 : OK

$\Rightarrow$ degree of regularity of subsystem $>$ of the full system.

- With our definition :
  - Deg. fall of a subsystem $\Rightarrow$ deg. fall on the full system OK
  - Non-trivial for a subsystem $\Rightarrow$ Non-trivial for the full system ? ?
  - **Lemma** : True up to the degree of regularity $\rightarrow$ OK.

The case of HFE systems

GJS Bound

- One notes d_k the degree of regularity of $\mathcal{S}_k$.
- The degree of regularity of HFE system is bounded by $\min_k\{d_k\}$
- The value of d_k is computed via MQ-bound.

The case of HFE systems

GJS Bound

- One notes d_k the degree of regularity of $\mathcal{S}_k$.
- The degree of regularity of HFE system is bounded by $\min_k\{d_k\}$
- The value of d_k is computed via MQ-bound.

Other property of HFE systems

- The P_i are written on monomials of the form $X_iX_{i+\ell}$, $\ell \leq D$.
- Their combinations are written on multiples of $X_iX_{i+\ell}$, $\ell \leq D$.
- They are contained in a proper subspace of the full image space.

The case of HFE systems

GJS Bound

- One notes d_k the degree of regularity of $\mathcal{S}_k$.
- The degree of regularity of HFE system is bounded by $\min_k\{d_k\}$
- The value of d_k is computed via MQ-bound.

Other property of HFE systems

- The P_i are written on monomials of the form $X_i X_{i+\ell}$, $\ell \leq D$.
- Their combinations are written on multiples of $X_i X_{i+\ell}$, $\ell \leq D$.
- They are contained in a proper subspace of the full image space.
- One deduces a better bound : the **HFE-bound**

Enumerations

Computation of MQ, GJS, or HFE bound :

- Dimension of $(\mathcal{R}_{q^n})_d^h$: enumerate the size of the monomial basis : Standard, Easy

Enumerations

Computation of MQ, GJS, or HFE bound :

- Dimension of $(\mathcal{R}_{q^n})^h_d$: enumerate the size of the monomial basis : Standard, Easy
- Size of the HFE monomial basis : $\approx$ Easy

Enumerations

Computation of MQ, GJS, or HFE bound :

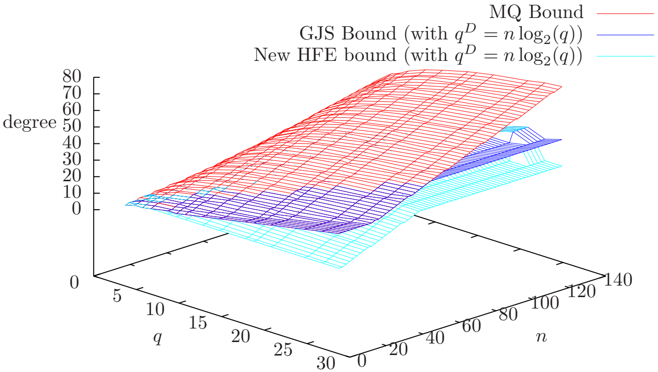
- Dimension of $(\mathcal{R}_{q^n})^h_d$: enumerate the size of the monomial basis : Standard, Easy
- Size of the HFE monomial basis : $\approx$ Easy
- Dimension of $\mathrm{Triv}(P_0, \ldots, P_k)_d$: Technical...
  We find :
  $$\tau_{k+1,d} = \tau_{k,d} + \sum_{i=1}^{q-1} \left(k \dim(\mathcal{R}_m)^h_{d-2i} - \tau_{k+1,d-2i}\right) + \dim(\mathcal{R}_m)^h_{d-2(q-1)}.$$
  With $\mathcal{R}_m = \mathbb{F}_{q^n}[X_0, \ldots, X_{m-1}]/\{X_0^{q^n}, \ldots, X_{m-1}^{q^n}\}$

Computation of MQ, GJS and HFE bounds

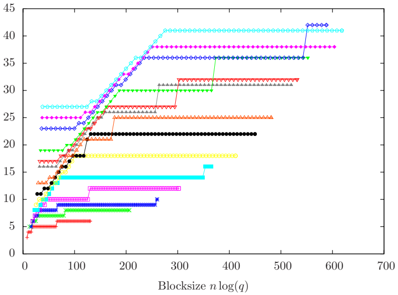
- We are now ready to compute the bounds !
- D is indexed on the blocksize to ensure polynomial decryption.

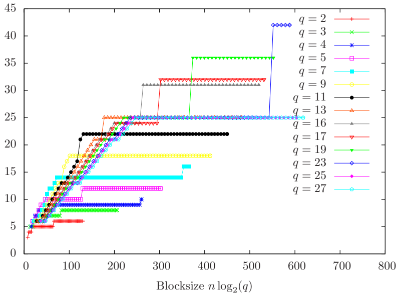
Computation of MQ, GJS and HFE bounds

- We are now ready to compute the bounds !
- D is indexed on the blocksize to ensure polynomial decryption.



Comparison of GJS and HFE bounds



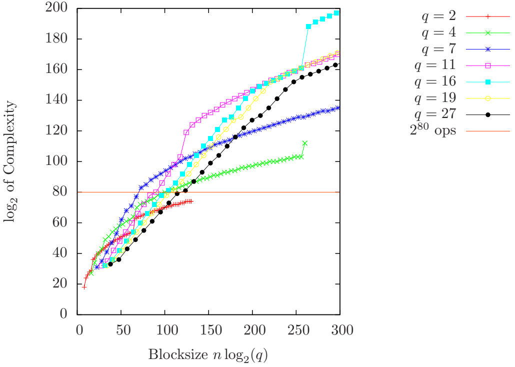


Generic Attacks on the public key

- Complexity : cost of the linear algebra at the degree of regularity.
- On obtains an **upper bound on the estimated complexity**.

Generic Attacks on the public key

- Complexity : cost of the linear algebra at the degree of regularity.
- On obtains an **upper bound on the estimated complexity**.



THANK YOU !