Mathematical Problems in Multivariate Public Key Cryptography

Timothy Hodges

University of Cincinnati

January 15, 2015
Overview

1. Multivariate Public Key Cryptosystems

2. Solving Systems of Polynomial Equations

3. First Fall Degree and HFE-systems

4. Semi-regular systems
Outline

1 Multivariate Public Key Cryptosystems
2 Solving Systems of Polynomial Equations
3 First Fall Degree and HFE-systems
4 Semi-regular systems
Multivariate Public Key Cryptosystems

$\mathbb{F}$ a finite field with $|\mathbb{F}| = q$

\[ \mathbb{F}^n \xrightarrow{\{p_1, \ldots, p_n\}} \mathbb{F}^m \]

\[ p_i(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]/\langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle = \text{Fun}(\mathbb{F}^n, \mathbb{F}) \]

Solving

\[ p_1(x_1, \ldots, x_n) = y_1 \]

\[ \vdots \]

\[ p_m(x_1, \ldots, x_n) = y_m \]

is a hard problem.

**Problem**

Design a trapdoor that retains this level of security.
Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q$.

Let $\mathbb{F}^n \xrightarrow{\{p_1, \ldots, p_n\}} \mathbb{F}^m$.

$p_i(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]/\langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle = \text{Fun}(\mathbb{F}^n, \mathbb{F})$.

Solving

$$p_1(x_1, \ldots, x_n) = y_1$$
$$\vdots$$
$$p_m(x_1, \ldots, x_n) = y_m$$

is a hard problem.

**Problem**

*Design a trapdoor that retains this level of security.*
Multivariate Public Key Cryptosystems

$\mathbb{F}$ a finite field with $|\mathbb{F}| = q$

$$\mathbb{F}^n \xrightarrow{\{p_1, \ldots, p_n\}} \mathbb{F}^m$$

$$p_i(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]/\langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle = \text{Fun}(\mathbb{F}^n, \mathbb{F})$$

Solving

$$p_1(x_1, \ldots, x_n) = y_1$$

$$\vdots$$

$$p_m(x_1, \ldots, x_n) = y_m$$

is a hard problem.

**Problem**

*Design a trapdoor that retains this level of security.*
Multivariate Public Key Cryptosystems

\[ F \text{ a finite field with } |F| = q \]

\[ F^n \xrightarrow{\{p_1, \ldots, p_n\}} F^m \]

\[ p_i(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]/\langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle = \text{Fun}(F^n, F) \]

Solving

\[ p_1(x_1, \ldots, x_n) = y_1 \]

\[ \vdots \quad \vdots \]

\[ p_m(x_1, \ldots, x_n) = y_m \]

is a hard problem.

Problem

*Design a trapdoor that retains this level of security.*
Multivariate Public Key Cryptosystems

\( \mathbb{F} \) a finite field with \(|\mathbb{F}| = q\)

\[
\mathbb{F}^n \xrightarrow{\{p_1, \ldots, p_n\}} \mathbb{F}^m
\]

\( p_i(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n] / \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle = \text{Fun}(\mathbb{F}^n, \mathbb{F}) \)

Solving

\[
p_1(x_1, \ldots, x_n) = y_1
\]

\[
\vdots
\]

\[
p_m(x_1, \ldots, x_n) = y_m
\]

is a hard problem.

**Problem**

*Design a trapdoor that retains this level of security.*
Hidden Field Systems: Matsumoto-Imai

Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1) t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t} \alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$\mathbb{K}$ $\xrightarrow{P} \mathbb{K}$ $\sigma$ $\uparrow$ $\tau$ $\downarrow$

$\mathbb{F}^n \xrightarrow{\{p_1,\ldots,p_n\}} \mathbb{F}^n$ $\sigma, \tau$ invertible affine linear maps

Private Key

Public Key
Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P: \mathbb{K} \rightarrow \mathbb{K}$, 

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n - 1} = 1$ by Lagrange's Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t} \alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X \cdot X^{q^s}$ is quadratic

$\sigma, \tau$ invertible affine linear maps
Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \to \mathbb{K}$,

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n - 1} = 1$ by Lagrange’s Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1) t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n - 1)t + 1} = \alpha^{-(q^n - 1)t} \alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^{q^s}$ is quadratic

$\sigma, \tau$ invertible affine linear maps
Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \rightarrow \mathbb{K}$, 

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n-1) = 1$,

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n-1} = 1$ by Lagrange’s Theorem. Since $\gcd(\theta, q^n-1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1)t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t} \alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X.X^q^s$ is quadratic

$\sigma, \tau$ invertible affine linear maps
Hidden Field Systems: Matsumoto-Imai

Identify (secretly) \( \mathbb{F}^n \) with an extension field \( \mathbb{K} \), where \( \dim_{\mathbb{F}} \mathbb{K} = n \). So \( |\mathbb{K}| = q^n \)

The map \( P : \mathbb{K} \rightarrow \mathbb{K} \)

\[ P(X) = X^\theta \]

is invertible with inverse \( P^{-1}(X) = X^s \) if \( \gcd(\theta, q^n - 1) = 1 \),

For all \( 0 \neq \alpha \in \mathbb{K} \), \( \alpha^{q^n - 1} = 1 \) by Lagrange’s Theorem. Since \( \gcd(\theta, q^n - 1) = 1 \), then there exist \( s, t \in \mathbb{Z} \) such that \( \theta s + (q^n - 1)t = 1 \) so

\[ (\alpha^\theta)^s = \alpha^{-(q^n-1)t+1} = \alpha^{-(q^n-1)t} \alpha = \alpha \]

Take \( q = 2^t \) and \( \theta = 1 + q^s \), \( P(X) = X.X^{q^s} \) is quadratic

\[ \begin{array}{c c c}
\mathbb{K} & \xrightarrow{P} & \mathbb{K} \\
\uparrow{\sigma} & \uparrow & \downarrow{\tau} \\
\mathbb{F}^n & \xrightarrow{\{p_1, \ldots, p_n\}} & \mathbb{F}^n \\
\end{array} \]

\( \sigma, \tau \) invertible affine linear maps
Identify (secretly) $\mathbb{F}^n$ with an extension field $\mathbb{K}$, where $\dim_{\mathbb{F}} \mathbb{K} = n$. So $|\mathbb{K}| = q^n$

The map $P : \mathbb{K} \rightarrow \mathbb{K}$,

$$P(X) = X^\theta$$

is invertible with inverse $P^{-1}(X) = X^s$ if $\gcd(\theta, q^n - 1) = 1$.

For all $0 \neq \alpha \in \mathbb{K}$, $\alpha^{q^n - 1} = 1$ by Lagrange’s Theorem. Since $\gcd(\theta, q^n - 1) = 1$, then there exist $s, t \in \mathbb{Z}$ such that $\theta s + (q^n - 1) t = 1$ so

$$(\alpha^\theta)^s = \alpha^{-(q^n - 1) t + 1} = \alpha^{-(q^n - 1) t} \alpha = \alpha$$

Take $q = 2^t$ and $\theta = 1 + q^s$, $P(X) = X \cdot X^{q^s}$ is quadratic

$$\mathbb{K} \xrightarrow{P} \mathbb{K}$$

Private Key

$$\mathbb{F}^n \xrightarrow{\{p_1, \ldots, p_n\}} \mathbb{F}^n$$

Public Key

\(\sigma, \tau\) invertible affine linear maps
Patarin’s HFE System

$P(X)$ is

- of low total degree, $D$ (efficient decryption).
- quadratic over $\mathbb{F}$ so that $p_i(x_1, \ldots, x_n)$ are quadratic (efficient encryption)

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

where $a_{ij}, b_i, c \in \mathbb{K}$. 
Patarin’s HFE System

\[ P(X) \] is

- of low total degree, \( D \) (efficient decryption).
- quadratic over \( \mathbb{F} \) so that \( p_i(x_1, \ldots, x_n) \) are quadratic (efficient encryption).

\[
P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c
\]

where \( a_{ij}, b_i, c \in \mathbb{K}. \)
Patarin’s HFE System

\[ P(X) \] is

- of low total degree, \( D \) (efficient decryption).
- quadratic over \( \mathbb{F} \) so that \( p_i(x_1, \ldots, x_n) \) are quadratic (efficient encryption).

\[
P(X) = \sum_{q^j + q^i \leq D} a_{ij} X^{q^j + q^i} + \sum_{q^i \leq D} b_i X^{q^i} + c
\]

where \( a_{ij}, b_i, c \in \mathbb{K} \).
Patarin’s HFE System

\( P(X) \) is

- of low total degree, \( D \) (efficient decryption).
- quadratic over \( \mathbb{F} \) so that \( p_i(x_1, \ldots, x_n) \) are quadratic (efficient encryption)

\[
P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c
\]

where \( a_{ij}, b_i, c \in \mathbb{K} \).
Outline

1 Multivariate Public Key Cryptosystems

2 Solving Systems of Polynomial Equations

3 First Fall Degree and HFE-systems

4 Semi-regular systems
Systems with a unique solution

Suppose the system

\[ p_1(x_1, \ldots, x_n) = 0 \]
\[ p_2(x_1, \ldots, x_n) = 0 \]
\[ \vdots \]
\[ p_n(x_1, \ldots, x_n) = 0 \]

If the system has the unique solution,

\[ x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n \]

then

\[ (p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)) = (x_1 - a_1, x_2 - a_2 \ldots x_n - a_n) \]

\[ x_i - a_i = \sum_{i-1}^{n} g_j(x_1, \ldots, x_n)p_j(x_1, \ldots, x_n) \]

So \( x_i - a_i \) can be found by exhaustive search of all combinations of the form \( \sum_{i-1}^{n} g_j(x_1, \ldots, x_n)p_j(x_1, \ldots, x_n) \) or by Gröbner basis algorithms.
Systems with a unique solution

Suppose the system

\[\begin{align*}
    p_1(x_1, \ldots, x_n) &= 0 \\
    p_2(x_1, \ldots, x_n) &= 0 \\
    & \quad \vdots \\
    p_n(x_1, \ldots, x_n) &= 0
\end{align*}\]

If the system has the unique solution,

\[x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n\]

then

\[\begin{pmatrix}
    p_1(x_1, \ldots, x_n) \\
    \vdots \\
    p_n(x_1, \ldots, x_n)
\end{pmatrix} = \begin{pmatrix}
    x_1 - a_1 \\
    x_2 - a_2 \\
    \vdots \\
    x_n - a_n
\end{pmatrix}\]

So \(x_i - a_i\) can be found by exhaustive search of all combinations of the form

\[
\sum_{i=1}^{n} g_j(x_1, \ldots, x_n)p_j(x_1, \ldots, x_n)
\]

or by Gröbner basis algorithms.
Systems with a unique solution

Suppose the system

\[
P_1(x_1, \ldots, x_n) = 0 \\
P_2(x_1, \ldots, x_n) = 0 \\
\vdots \\
P_n(x_1, \ldots, x_n) = 0
\]

If the system has the unique solution,

\[
x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n
\]

then

\[
(p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)) = (x_1 - a_1, x_2 - a_2 \ldots x_n - a_n)
\]

\[
x_i - a_i = \sum_{i-1}^{n} g_j(x_1, \ldots, x_n)p_j(x_1, \ldots, x_n)
\]

So \(x_i - a_i\) can be found by exhaustive search of all combinations of the form \(\sum_{i-1}^{n} g_j(x_1, \ldots, x_n)p_j(x_1, \ldots, x_n)\) or by Gröbner basis algorithms.
Let $A = \mathbb{F}[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$; set $x_i = \bar{X}_i$.

$$A_k = \{ \text{elements expressible as polynomials of degree } \leq k \}$$

Let

$$l = (p_1(x_1, \ldots, x_n), \ldots, p(x_1, \ldots, x_n)) = \sum_i A p_i(x_1, \ldots, x_n)$$

where $\deg p_i = d_i$. Note that $\dim A/l$ equals the number of solutions of the system.

Set

$$J_k = \sum_i A_{k-d_i} p_i \subset A_k$$

Then

$$J_1 \subset J_2 \subset \cdots \subset J_N = l$$

When $\dim A_k - \dim J_k < q$ we can find a univariate polynomial in $J_k$ which can be solved by univariate root-finding algorithms to find $a_i$. 
XL algorithm

Let \( A = \mathbb{F}[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n) \); set \( x_i = \bar{X}_i \).

\[ A_k = \{ \text{elements expressible as polynomials of degree } \leq k \} \]

Let

\[ I = (p_1(x_1, \ldots, x_n), \ldots, p(x_1, \ldots, x_n)) = \sum_i A p_i(x_1, \ldots, x_n) \]

where \( \deg p_i = d_i \). Note that \( \dim A/I \) equals the number of solutions of the system.

Set

\[ J_k = \sum_i A_{k-d_i} p_i \subset A_k \]

Then

\[ J_1 \subset J_2 \subset \cdots \subset J_N = I \]

When \( \dim A_k - \dim J_k < q \) we can find a univariate polynomial in \( J_k \) which can be solved by univariate root-finding algorithms to find \( a_i \).
Let $A = \mathbb{F}[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$; set $x_i = \bar{X}_i$.

$$A_k = \{\text{elements expressible as polynomials of degree } \leq k \}$$

Let

$$l = (p_1(x_1, \ldots, x_n), \ldots, p(x_1, \ldots, x_n)) = \sum_i A p_i(x_1, \ldots, x_n)$$

where $\deg p_i = d_i$. Note that $\dim A/l$ equals the number of solutions of the system.

Set

$$J_k = \sum_i A_{k-d_i} p_i \subset A_k$$

Then

$$J_1 \subset J_2 \subset \cdots \subset J_N = l$$

When $\dim A_k - \dim J_k < q$ we can find a univariate polynomial in $J_k$ which can be solved by univariate root-finding algorithms to find $a_i$. 
Operational Degree of XL algorithm

**Definition**

The operational degree of the XL algorithm is the highest degree of polynomials that occur in the calculations before the algorithm terminates.

**Conjecture (or Definition (Yang-Chen-Courtois))**

If there are no non-trivial relations between the $f_i$ of degree less than or equal to $k$, then

$$\dim A_k - \dim J_k = [t^k] \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i q})} \right)$$

**Rationale ($m = 1$, $J_k = A_{k-d} f$):** since $(1 - f^{q-1})f = f - f^q = 0$

$$0 \rightarrow \cdots \rightarrow A_{k-2q d} \xrightarrow{1-f^{q-1}} A_{k-(q+1)d} \xrightarrow{f} A_{k-q d} \xrightarrow{1-f^{q-1}} A_{k-d} \xrightarrow{f} A_k \rightarrow A_k/J_k \rightarrow 0$$

So $\dim A_k/J_k = \sum_j (\dim A_{k-j q d} - \dim A_{k-(j q+1) d})$.
Operational Degree of XL algorithm

**Definition**

The *operational degree* of the XL algorithm is the highest degree of polynomials that occur in the calculations before the algorithm terminates.

**Conjecture (or Definition (Yang-Chen-Courtois))**

*If there are no non-trivial relations between the $f_i$ of degree less than or equal to $k$, then*

$$\dim A_k - \dim J_k = \lceil t^k \rceil \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i q})} \right)$$

**Rationale** ($m = 1$, $J_k = A_{k-d} f$): since $(1 - f^{q-1}) f = f - f^q = 0$

$$0 \rightarrow \cdots \rightarrow A_{k-2qd} \xrightarrow{1-f^{q-1}} A_{k-(q+1)d} \xrightarrow{f} A_{k-qd} \xrightarrow{1-f^{q-1}} A_{k-d} \xrightarrow{f} A_k \rightarrow A_k/J_k \rightarrow 0$$

So $\dim A_k/J_k = \sum_j (\dim A_{k-jqd} - \dim A_{k-(jq+1)d})$
Operational Degree of XL algorithm

**Definition**

The operational degree of the XL algorithm is the highest degree of polynomials that occur in the calculations before the algorithm terminates.

**Conjecture (or Definition (Yang-Chen-Courtois))**

If there are no non-trivial relations between the \( f_i \) of degree less than or equal to \( k \), then

\[
\text{dim } A_k - \text{dim } J_k = [t^k] \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i (1 - t^{d_i}) \right)
\]

Rationale \((m = 1, J_k = A_{k-d} f)\): since \((1 - f^{q-1})f = f - f^q = 0\)

\[
0 \rightarrow \cdots \rightarrow A_{k-2qd} \xrightarrow{1-f^{q-1}} A_{k-(q+1)d} \xrightarrow{f} A_{k-qd} \xrightarrow{1-f^{q-1}} A_{k-d} \xrightarrow{f} A_k \rightarrow A_k/J_k \rightarrow 0
\]

So \(\text{dim } A_k/J_k = \sum_j (\text{dim } A_{k-jqd} - \text{dim } A_{k-(jq+1)d})\)
Yang-Chen formula

Let

\[ s_d = [t^d] \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i (1 - t^{d_i}) \right) \]

Typical behavior for a set of 20 quadratic polynomials in 20 variables over \( \mathbb{F}_3 \).

<table>
<thead>
<tr>
<th>( d )</th>
<th>( \dim A_d )</th>
<th>( \dim J_d )</th>
<th>( \dim A_d - \dim J_d )</th>
<th>( s_d )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>21</td>
<td>20</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>2</td>
<td>231</td>
<td>420</td>
<td>211</td>
<td>211</td>
</tr>
<tr>
<td>3</td>
<td>1771</td>
<td>4430</td>
<td>1331</td>
<td>1331</td>
</tr>
<tr>
<td>4</td>
<td>10626</td>
<td>31030</td>
<td>5776</td>
<td>5776</td>
</tr>
<tr>
<td>5</td>
<td>53110</td>
<td>161350</td>
<td>17480</td>
<td>17480</td>
</tr>
<tr>
<td>6</td>
<td>229810</td>
<td>661030</td>
<td>33650</td>
<td>33650</td>
</tr>
<tr>
<td>7</td>
<td>883410</td>
<td>2089394</td>
<td>18470</td>
<td>18470</td>
</tr>
<tr>
<td>8</td>
<td>2089395</td>
<td>2089394</td>
<td>1</td>
<td>-125740</td>
</tr>
</tbody>
</table>

Conjecture (Y-C-C)

The operational degree of the XL algorithm on the system \( f_1, \ldots, f_m \) is at most

\[ \text{Ind} \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i (1 - t^{d_i}) \right) = \min \{ d \mid s_d \leq 0 \} \]
Yang-Chen formula

Let

\[ s_d = [t^d] \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i q})} \right) \]

Typical behavior for a set of 20 quadratic polynomials in 20 variables over \( \mathbb{F}_3 \).

<table>
<thead>
<tr>
<th>( d )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \dim A_d )</td>
<td>1</td>
<td>21</td>
<td>231</td>
<td>1771</td>
<td>10626</td>
<td>53110</td>
<td>229810</td>
<td>883410</td>
<td>2089395</td>
</tr>
<tr>
<td>( \dim J_d )</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>420</td>
<td>4430</td>
<td>31030</td>
<td>161350</td>
<td>661030</td>
<td>2089394</td>
</tr>
<tr>
<td>( \dim A_d - \dim J_d )</td>
<td>1</td>
<td>21</td>
<td>211</td>
<td>1331</td>
<td>5776</td>
<td>17480</td>
<td>33650</td>
<td>18470</td>
<td>1</td>
</tr>
<tr>
<td>( s_d )</td>
<td>1</td>
<td>21</td>
<td>211</td>
<td>1331</td>
<td>5776</td>
<td>17480</td>
<td>33650</td>
<td>18470</td>
<td>-125740</td>
</tr>
</tbody>
</table>

Conjecture (Y-C-C)

The operational degree of the XL algorithm on the system \( f_1, \ldots, f_m \) is at most

\[ \text{Ind} \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i q})} \right) = \min\{d \mid s_d \leq 0\} \]
Yang-Chen formula

Let

\[ s_d = [t^d] \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_{i} \frac{(1 - t^{d_i})}{(1 - t^{d_i} q)} \right) \]

Typical behavior for a set of 20 quadratic polynomials in 20 variables over \( \mathbb{F}_3 \).

<table>
<thead>
<tr>
<th>( d )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>dim ( A_d )</td>
<td>1</td>
<td>21</td>
<td>231</td>
<td>1771</td>
<td>10626</td>
<td>53110</td>
<td>229810</td>
<td>883410</td>
<td>2089395</td>
</tr>
<tr>
<td>dim ( J_d )</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>420</td>
<td>4430</td>
<td>31030</td>
<td>161350</td>
<td>661030</td>
<td>2089394</td>
</tr>
<tr>
<td>dim ( A_d - \dim J_d )</td>
<td>1</td>
<td>21</td>
<td>211</td>
<td>1331</td>
<td>5776</td>
<td>17480</td>
<td>33650</td>
<td>18470</td>
<td>1</td>
</tr>
<tr>
<td>( s_d )</td>
<td>1</td>
<td>21</td>
<td>211</td>
<td>1331</td>
<td>5776</td>
<td>17480</td>
<td>33650</td>
<td>18470</td>
<td>-125740</td>
</tr>
</tbody>
</table>

Conjecture (Y-C-C)

The operational degree of the XL algorithm on the system \( f_1, \ldots, f_m \) is at most

\[ \text{Ind} \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_{i} \frac{(1 - t^{d_i})}{(1 - t^{d_i} q)} \right) = \min \{ d \mid s_d \leq 0 \} \]
Yang-Chen formula

Let

\[ s_d = [t^d] \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i}q)} \right) \]

Typical behavior for a set of 20 quadratic polynomials in 20 variables over \( \mathbb{F}_3 \).

<table>
<thead>
<tr>
<th>( d )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \dim A_d )</td>
<td>1</td>
<td>21</td>
<td>231</td>
<td>1771</td>
<td>10626</td>
<td>53110</td>
<td>229810</td>
<td>883410</td>
<td>2089395</td>
</tr>
<tr>
<td>( \dim J_d )</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>420</td>
<td>4430</td>
<td>31030</td>
<td>161350</td>
<td>661030</td>
<td>2089394</td>
</tr>
<tr>
<td>( \dim A_d - \dim J_d )</td>
<td>1</td>
<td>21</td>
<td>211</td>
<td>1331</td>
<td>5776</td>
<td>17480</td>
<td>33650</td>
<td>18470</td>
<td>1</td>
</tr>
<tr>
<td>( s_d )</td>
<td>1</td>
<td>21</td>
<td>211</td>
<td>1331</td>
<td>5776</td>
<td>17480</td>
<td>33650</td>
<td>18470</td>
<td>-125740</td>
</tr>
</tbody>
</table>

**Conjecture (Y-C-C)**

The operational degree of the XL algorithm on the system \( f_1, \ldots, f_m \) is at most

\[
\text{Ind} \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i}q)} \right) = \min \{ d \mid s_d \leq 0 \} 
\]
Asymptotics of the Index

**Definition**

The index of a power series $\sum_i a_i t^i$, denoted $\text{Ind}(\sum_i a_i t^i)$ is the first $k$ such that $a_k \leq 0$.

**Problem**

Understand the behavior of

$$\text{Ind} \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i q})} \right)$$

**Theorem**

(The case when $q = 2$, $n = m$ and $d_1 = \cdots = d_n = 2$). Asymptotically,

$$\text{Ind} \left( \frac{(1 - t^2)^n}{(1 - t)^{n+1}} \left( \frac{1 - t^2}{1 - t^{2q}} \right)^n \right) \sim 0.09n$$
Asymptotics of the Index

**Definition**

The index of a power series $\sum_i a_i t^i$, denoted $\text{Ind}(\sum_i a_i t^i)$, is the first $k$ such that $a_k \leq 0$.

**Problem**

*Understand the behavior of*

$$\text{Ind} \left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i}q)} \right)$$

**Theorem**

*(The case when $q = 2$, $n = m$ and $d_1 = \cdots = d_n = 2$). Asymptotically,*

$$\text{Ind} \left( \frac{(1 - t^2)^n}{(1 - t)^{n+1}} \left( \frac{(1 - t^2)}{(1 - t^{2q})} \right)^n \right) \sim .09n$$
Asymptotics of the Index

**Definition**

The index of a power series \( \sum_i a_i t^i \), denoted \( \text{Ind}(\sum_i a_i t^i) \) is the first \( k \) such that \( a_k \leq 0 \).

**Problem**

*Understand the behavior of*

\[
\text{Ind}\left( \frac{(1 - t^q)^n}{(1 - t)^{n+1}} \prod_i \frac{(1 - t^{d_i})}{(1 - t^{d_i,q})} \right)
\]

**Theorem**

*(The case when \( q = 2 \), \( n = m \) and \( d_1 = \cdots = d_n = 2 \)). Asymptotically,*

\[
\text{Ind} \left( \frac{(1 - t^2)^n}{(1 - t)^{n+1}} \left( \frac{(1 - t^2)}{(1 - t^{2q})} \right)^n \right) \approx .09n
\]
Conclusion

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

Problem

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC’s like Matsumoto-Imai and HFE?

Not really

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the $f_i$’s as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.
Conclusion

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

Problem

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC’s like Matsumoto-Imai and HFE?

Not really

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the $f_i$’s as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.
Conclusion

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

Problem

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC’s like Matsumoto-Imai and HFE?

Not really

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the $f_i$’s as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.
Conclusion and Applications to MPKC

**Conclusion**

If we assume the YCC Conjecture that the operational degree of XL is the index of the series and we can understand the asymptotics of this index we can determine the complexity of the algorithm on such systems.

**Problem**

Prove the YCC conjecture

Does this analysis give us useful information about applying the XL algorithm to attacking systems of equations derived from MPKC’s like Matsumoto-Imai and HFE?

*Not really*

- The systems of equations derived from such systems are qualitatively different from the ones assumed to have as few relations between the $f_i$’s as possible.
- In fact non-trivial relations occur much earlier and the XL algorithm will terminate at a much lower degree.
Outline

1. Multivariate Public Key Cryptosystems

2. Solving Systems of Polynomial Equations

3. First Fall Degree and HFE-systems

4. Semi-regular systems
First Fall Degree

**Definition**

**First Fall Degree:** Lowest degree at which non-trivial “degree falls” occur.

\[
\deg \left( \sum_i g_i p_i \right) < \max \{ \deg(g_i) + \deg(p_i) \}
\]

Trivial degree falls:

\[
p_i^{q-1} p_i = p_i^q = p_i, \quad p_j p_i - p_i p_j = 0
\]

**Example**

If \( q = 2 \) and \( p(x_1, \ldots, x_6) = x_1 x_2 + x_3 x_4 + x_5 x_6 + 1 \) then

\[
x_1 x_3 x_5 (x_1 x_2 + x_3 x_4 + x_5 x_6 + 1) = x_1 x_2 x_3 x_5 + x_1 x_3 x_4 x_5 + x_1 x_3 x_5 x_6 + x_1 x_3 x_5
\]

is a non-trivial degree fall.
First Fall Degree

**Definition**

**First Fall Degree:** Lowest degree at which non-trivial “degree falls” occur.

\[
\deg \left( \sum_i g_i p_i \right) < \max \{ \deg(g_i) + \deg(p_i) \}
\]

Trivial degree falls:

\[
p_i^{q-1} p_i = p_i^q = p_i, \quad p_j p_i - p_i p_j = 0
\]

**Example**

If \( q = 2 \) and \( p(x_1, \ldots, x_6) = x_1 x_2 + x_3 x_4 + x_5 x_6 + 1 \) then

\[
x_1 x_3 x_5 (x_1 x_2 + x_3 x_4 + x_5 x_6 + 1) = x_1 x_2 x_3 x_5 + x_1 x_3 x_4 x_5 + x_1 x_3 x_5 x_6 + x_1 x_3 x_5
\]

is a non-trivial degree fall.
Let $p_i^h$ be the highest degree part of $p_i$ considered as an element of the truncated polynomial ring

$$p_i^h \in \frac{\mathbb{F}[x_1, \ldots, x_n]}{(x_1^q, \ldots, x_n^q)}$$

First fall degree of $p_1^h, \ldots, p_n^h$ is first degree at which non-trivial relations occur.

$$\deg \left( \sum_i f_i p_i^h \right) = 0$$

Trivial relations: $(p_i^h)^q - p_i^h = 0$, $p_j^h p_i^h - p_i^h p_j^h = 0$

Then

$$D_{ff}(p_1, \ldots, p_n) = D_{ff}(p_1^h, \ldots, p_n^h)$$
Let $p_i^h$ be the highest degree part of $p_i$ considered as an element of the truncated polynomial ring

$$p_i^h \in \frac{\mathbb{F}[x_1, \ldots, x_n]}{\langle x_1^q, \ldots, x_n^q \rangle}$$

First fall degree of $p_1^h, \ldots, p_n^h$ is first degree at which non-trivial relations occur.

$$\deg \left( \sum_i f_i p_i^h \right) = 0$$

Trivial relations: $(p_i^h)^{q-1} p_i^h = 0$, $p_j^h p_i^h - p_i^h p_j^h = 0$

Then

$$D_{ff}(p_1, \ldots, p_n) = D_{ff}(p_1^h, \ldots, p_n^h)$$
Let $p_i^h$ be the highest degree part of $p_i$ considered as an element of the truncated polynomial ring

$$p_i^h \in \frac{\mathbb{F}[x_1, \ldots, x_n]}{\langle x_1^q, \ldots, x_n^q \rangle}$$

First fall degree of $p_1^h, \ldots, p_n^h$ is first degree at which non-trivial relations occur.

$$\deg \left( \sum_i f_i p_i^h \right) = 0$$

Trivial relations: $(p_i^h)^{q-1} p_i^h = 0$, $p_j^h p_i^h - p_i^h p_j^h = 0$

Then

$$D_{ff}(p_1, \ldots, p_n) = D_{ff}(p_1^h, \ldots, p_n^h)$$
First-Fall Degree for HFE Systems

**Theorem (Dubois-Gama)**

\[ D_{ff}(p_1^h, \ldots, p_n^h) \leq D_{ff}(p_1^h, \ldots, p_j^h) \]

Recall that

\[ P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c \]

Define

\[ P_0(X_1, \ldots, X_n) = \sum a_{ij} X_i X_j \in K[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q) \]

Galois theory and filtered-graded arguments yield the key result:

**Theorem**

\[ D_{ff}(p_1^h, \ldots, p_n^h) \leq D_{ff}(P_0) \]
First-Fall Degree for HFE Systems

**Theorem (Dubois-Gama)**

\[ D_{\text{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\text{ff}}(p_1^h, \ldots, p_j^h) \]

Recall that

\[ P(X) = \sum_{q^i + q^j \leq D} a_{ij}X^{q^i+q^j} + \sum_{q^i \leq D} b_iX^{q^i} + c \]

Define

\[ P_0(X_1, \ldots, X_n) = \sum a_{ij}X_iX_j \in \mathbb{K}[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q) \]

Galois theory and filtered-graded arguments yield the key result:

**Theorem**

\[ D_{\text{ff}}(p_1^h, \ldots, p_n^h) \leq D_{\text{ff}}(P_0) \]
Theorem (Dubois-Gama)

\[ D_{ff}(p_1^h, \ldots, p_n^h) \leq D_{ff}(p_1^h, \ldots, p_j^h) \]

Recall that

\[ P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c \]

Define

\[ P_0(X_1, \ldots, X_n) = \sum a_{ij} X_i X_j \in \mathbb{K}[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q) \]

Galois theory and filtered-graded arguments yield the key result:

Theorem

\[ D_{ff}(p_1^h, \ldots, p_n^h) \leq D_{ff}(P_0) \]
Bounding the First-Fall Degree for HFE Systems

Lemma

\[ D_{ff} \left( P_0 = \sum_{i,j} a_{ij} X_i X_j \right) \leq \frac{\text{Rank}(P_0)(q - 1)}{2} + 2 \]

where \( \text{Rank}(P_0) \) is the rank of the quadratic form \( P_0 \).

For instance

\[ X_1^{q-1} X_3^{q-1} \ldots X_{r-1}^{q-1} (X_1 X_2 + X_3 X_4 + \ldots + X_{r-1} X_r) = 0 \]

Theorem (Ding-Hodges)

The first fall degree of the system defined by \( P \) is bounded by

\[ D_{ff}(p_1, \ldots, p_n) \leq \frac{\text{Rank}(P_0)(q - 1)}{2} + 2 \leq \frac{(q - 1)(\lfloor \log_q(D - 1) \rfloor + 1)}{2} + 2 \]

if \( \text{Rank}(P_0) > 1 \).
Bounding the First-Fall Degree for HFE Systems

Lemma

\[ D_{\text{ff}} \left( P_0 = \sum_{i,j} a_{ij} X_i X_j \right) \leq \frac{\text{Rank}(P_0)(q - 1)}{2} + 2 \]

where \( \text{Rank}(P_0) \) is the rank of the quadratic form \( P_0 \).

For instance

\[ X_1^{q-1} X_3^{q-1} \ldots X_{r-1}^{q-1} (X_1 X_2 + X_3 X_4 + \ldots + X_{r-1} X_r) = 0 \]

Theorem (Ding-Hodges)

The first fall degree of the system defined by \( P \) is bounded by

\[ D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{\text{Rank}(P_0)(q - 1)}{2} + 2 \leq \frac{(q - 1)(\lceil \log_q(D - 1) \rceil + 1)}{2} + 2 \]

if \( \text{Rank}(P_0) > 1 \).
Bounding the First-Fall Degree for HFE Systems

**Lemma**

\[
D_{\text{ff}} \left( P_0 = \sum_{i,j} a_{ij} X_i X_j \right) \leq \frac{\text{Rank}(P_0)(q - 1)}{2} + 2
\]

where \( \text{Rank}(P_0) \) is the rank of the quadratic form \( P_0 \).

For instance

\[
X_1^{q-1} X_3^{q-1} \cdots X_{r-1}^{q-1} (X_1 X_2 + X_3 X_4 + \cdots + X_{r-1} X_r) = 0
\]

**Theorem (Ding-Hodges)**

The first fall degree of the system defined by \( P \) is bounded by

\[
D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{\text{Rank}(P_0)(q - 1)}{2} + 2 \leq \frac{(q - 1)(\lfloor \log_q(D - 1) \rfloor + 1)}{2} + 2
\]

if \( \text{Rank}(P_0) > 1 \).
Complexity of Grobner basis attack on HFE systems

For the sake of analysis of the complexity of attacks on HFE systems we usually assume that $D = O(n^\alpha)$.

**Conclusion**

*If we assume that the first fall degree of a system is a good indicator of the operational degree then we can conclude that the complexity of a Grobner basis attack on HFE system is quasi-polynomial.*

but...

**Problem**

*Prove that the first fall degree of a system is a good indicator of the operational degree in suitable situations.*
Higher Degree Analogs of HFE

Suppose that

\[ P(X) = \sum_{q^{i_1 + \cdots + i_d} \leq D} a_{ij} X^{q^{i_1} + \cdots + q^{i_d}} + \text{lower degree terms} \]

and let

\[ P_0(X_1, \ldots, X_n) = \sum_{q^{i_1 + \cdots + i_d} \leq D} a_{ij} X_{i_1} \cdots X_{i_d} \in \mathbb{K}[X_1, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q \rangle \]

Lemma

\[ D_{ff}(P_0) \leq (\text{Rank}(P_0)(q - 1) + d + 2)/2 \]

Theorem (Hodges-Petit-Schlather)

The first fall degree of the system defined by \( P \) is bounded by

\[ D_{ff}(p_1, \ldots, p_n) \leq \frac{(q - 1) \log_q (D - d + 1) + q + d + 1}{2} \]
Higher Degree Analogs of HFE

Suppose that

\[ P(X) = \sum_{q_1 + \ldots + q_d \leq D} a_{ij} X^{q_1 + \ldots + q_d} + \text{lower degree terms} \]

and let

\[ P_0(X_1, \ldots, X_n) = \sum_{q_1 + \ldots + q_d \leq D} a_{ij} X_1^{q_1} \ldots X_d \in \mathbb{K}[X_1, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q \rangle \]

**Lemma**

\[ D_{\text{ff}}(P_0) \leq (\text{Rank}(P_0)(q - 1) + d + 2)/2 \]

**Theorem (Hodges-Petit-Schlather)**

The first fall degree of the system defined by \( P \) is bounded by

\[ D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{(q - 1) \log_q (D - d + 1) + q + d + 1}{2} \]
Higher Degree Analogs of HFE

Suppose that

\[ P(X) = \sum_{q^{i_1+\ldots+q^{i_d} \leq D}} a_{i_1} X^{q^{i_1} + \ldots + q^{i_d}} + \text{lower degree terms} \]

and let

\[ P_0(X_1, \ldots, X_n) = \sum_{q^{i_1+\ldots+q^{i_d} \leq D}} a_{i_1} X_1^{i_1} \ldots X_d^{i_d} \in K[X_1, \ldots, X_n]/\langle X_1^{q}, \ldots, X_n^{q} \rangle \]

Lemma

\[ D_{ff}(P_0) \leq (\text{Rank}(P_0)(q - 1) + d + 2)/2 \]

Theorem (Hodges-Petit-Schlather)

The first fall degree of the system defined by \( P \) is bounded by

\[ D_{ff}(p_1, \ldots, p_n) \leq \frac{(q - 1) \log_q(D - d + 1) + q + d + 1}{2} \]
<table>
<thead>
<tr>
<th>$k$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>35</td>
<td>35</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>55</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>121</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>209</td>
<td>210</td>
<td>209</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>199</td>
<td>325</td>
<td>325</td>
<td>320</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>400</td>
<td>470</td>
<td>470</td>
<td>455</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>605</td>
<td>640</td>
<td>640</td>
<td>605</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>356</td>
<td>811</td>
<td>826</td>
<td>826</td>
<td>756</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>690</td>
<td>1010</td>
<td>1015</td>
<td>1015</td>
<td>889</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>980</td>
<td>1189</td>
<td>1190</td>
<td>1189</td>
<td>980</td>
</tr>
<tr>
<td>13</td>
<td>315</td>
<td>1204</td>
<td>1330</td>
<td>1330</td>
<td>1325</td>
<td>1005</td>
</tr>
<tr>
<td>14</td>
<td>594</td>
<td>1350</td>
<td>1420</td>
<td>1420</td>
<td>1405</td>
<td>950</td>
</tr>
<tr>
<td>15</td>
<td>811</td>
<td>1416</td>
<td>1451</td>
<td>1451</td>
<td>1416</td>
<td>811</td>
</tr>
<tr>
<td>16</td>
<td>950</td>
<td>1405</td>
<td>1420</td>
<td>1420</td>
<td>1350</td>
<td>594</td>
</tr>
<tr>
<td>17</td>
<td>1005</td>
<td>1325</td>
<td>1330</td>
<td>1330</td>
<td>1204</td>
<td>315</td>
</tr>
<tr>
<td>18</td>
<td>980</td>
<td>1189</td>
<td>1190</td>
<td>1189</td>
<td>980</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>889</td>
<td>1015</td>
<td>1015</td>
<td>1010</td>
<td>690</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>756</td>
<td>826</td>
<td>826</td>
<td>811</td>
<td>356</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>605</td>
<td>640</td>
<td>640</td>
<td>605</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>455</td>
<td>470</td>
<td>470</td>
<td>400</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>320</td>
<td>325</td>
<td>325</td>
<td>199</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>209</td>
<td>210</td>
<td>209</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>126</td>
<td>126</td>
<td>121</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>26</td>
<td>70</td>
<td>70</td>
<td>55</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>27</td>
<td>35</td>
<td>35</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>28</td>
<td>15</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Shifted difference of periodic sums of generalized binomial coefficients

Generalized binomial coefficients

\[(1 + z + \cdots + z^{q-1})^n = \frac{1 - z^q}{1 - z} = \sum C_q(n, k) z^k\]

Periodic or lacunary sums of generalized binomial coefficients

\[PC_q(n, k, s) = \sum_{j=-\infty}^{\infty} C_q(n, k + sj)\]

Shifted difference of periodic sums of generalized binomial coefficients

\[\Gamma_q(n, d, r, k) = PC_q(n, k, dq) - PC_q(n, k - rd, dq)\]
Shifted difference of periodic sums of generalized binomial coefficients

Generalized binomial coefficients

\[(1 + z + \cdots + z^{q-1})^n = \frac{1 - z^q}{1 - z} = \sum C_q(n, k) z^k\]

Periodic or lacunary sums of generalized binomial coefficients

\[PC_q(n, k, s) = \sum_{j=-\infty}^{\infty} C_q(n, k + sj)\]

Shifted difference of periodic sums of generalized binomial coefficients

\[\Gamma_q(n, d, r, k) = PC_q(n, k, dq) - PC_q(n, k - rd, dq)\]
Generalized binomial coefficients

\[(1 + z + \cdots + z^{q-1})^n = \frac{1 - z^q}{1 - z} = \sum C_q(n, k)z^k\]

Periodic or lacunary sums of generalized binomial coefficients

\[PC_q(n, k, s) = \sum_{j=-\infty}^{\infty} C_q(n, k + sj)\]

Shifted difference of periodic sums of generalized binomial coefficients

\[\Gamma_q(n, d, r, k) = PC_q(n, k, dq) - PC_q(n, k - rd, dq)\]
An example of a Gamma function

Figure: $\Gamma_{17}(6, 4, k)$

Note: $((q - 1)n + d)/2 = (16.6 + 4)/2 = 50$
When \( q = 2 \), we have, for instance,

\[
PC_2(n, k, 4) = \frac{2^{n-1} + 2^{n/2} \cos\left(\frac{\pi}{4}(n - 2k)\right)}{2}
\]

(Ramus, 1834)

If \( q \) is odd, \( PC_q(n, k, r) \) is equal to

\[
\frac{1}{r} \sum_{m=0}^{r-1} \left( 2 \sum_{j=1}^{\frac{q-1}{2}} \cos \left( \frac{m(q - 2j + 1)\pi}{r} \right) + 1 \right)^n \cos \left( \frac{m\pi((q - 1)n - 2k)}{r} \right)
\]

(Hoggat and Alexanderson, 1976)
When $q = 2$, we have, for instance,

$$PC_2(n, k, 4) = \frac{2^{n-1} + 2^{n/2} \cos\left(\frac{\pi}{4}(n - 2k)\right)}{2}$$

(Ramus, 1834)

If $q$ is odd, $PC_q(n, k, r)$ is equal to

$$\frac{1}{r} \sum_{m=0}^{r-1} \left( 2 \sum_{j=1}^{\frac{q-1}{2}} \cos\left(\frac{m(q - 2j + 1)\pi}{r}\right) + 1 \right)^n \cos\left(\frac{m\pi((q - 1)n - 2k)}{r}\right)$$

(Hoggat and Alexanderson, 1976)
Determinants with binomial coefficient entries

Problem: show that

\[
\begin{vmatrix}
\binom{r}{k} & \cdots & \binom{r}{k+s} \\
\vdots & \ddots & \vdots \\
\binom{r+s}{k} & \cdots & \binom{r+s}{k+s}
\end{vmatrix}
\]

is non-zero mod \( p \) if \( r + s < p \).

Theorem (Zeipel, 1870's)

\[
\begin{vmatrix}
\binom{r}{k} & \cdots & \binom{r}{k+s} \\
\vdots & \ddots & \vdots \\
\binom{r+s}{k} & \cdots & \binom{r+s}{k+s}
\end{vmatrix} = \frac{\binom{r}{k} \cdots \binom{r+s}{k}}{\binom{k}{k} \cdots \binom{k+s}{k}}
\]

Determinants with binomial coefficient entries

Problem: show that

\[
\begin{vmatrix}
{r \choose k} & \cdots & {r \choose k+s} \\
\vdots & \ddots & \vdots \\
{r+s \choose k} & \cdots & {r+s \choose k+s}
\end{vmatrix}
\]

is non-zero mod \( p \) if \( r + s < p \).

Theorem (Zeipel, 1870’s)

\[
\begin{vmatrix}
{r \choose k} & \cdots & {r \choose k+s} \\
\vdots & \ddots & \vdots \\
{r+s \choose k} & \cdots & {r+s \choose k+s}
\end{vmatrix} = \frac{{r \choose k} \cdots {r+s \choose k}}{\frac{k}{k} \cdots \frac{k+s}{k}}
\]

1 Multivariate Public Key Cryptosystems

2 Solving Systems of Polynomial Equations

3 First Fall Degree and HFE-systems

4 Semi-regular systems
Semi-regular Sequences

Henceforth the base field will be $\mathbb{F}_2$.

**Definition**

A set $\lambda_1, \ldots, \lambda_m \in B = \mathbb{F}_2[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q)$ is semi-regular if $D_{\text{ff}}(\lambda_1, \ldots, \lambda_m)$ is as large as possible.

**Theorem (Bardet-Faugere-Salvy)**

*The set $\lambda_1, \ldots, \lambda_m$ is semi-regular if and only if*

$$HS_{B/(\lambda_1, \ldots, \lambda_m)}(z) = \left[ \frac{(1 + z)^n}{\prod_{i=1}^{m} (1 + z^{d_i})} \right]$$

*In this case the operational degree of Grobner basis algorithms is the index of this series.*

Here

$$[1 + 2t + 7t^2 + 3t^3 - 6t^4 + t^5 + \ldots] = 1 + 2t + 7t^2 + 3t^3$$
Existence of semi-regular sequences

It is widely believed that in some sense “most” sequences are semi-regular.

<table>
<thead>
<tr>
<th>n \ m</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>.8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>.35</td>
<td>1</td>
<td>.75</td>
<td>.75</td>
<td>.3</td>
<td>.65</td>
<td>.85</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>.85</td>
<td>.95</td>
<td>1</td>
<td>.9</td>
<td>.85</td>
<td>.75</td>
<td>.6</td>
<td>.2</td>
<td>.65</td>
<td>.7</td>
<td>.9</td>
<td>.9</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>.85</td>
<td>.7</td>
<td>.65</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.95</td>
<td>.95</td>
<td>.95</td>
<td>.75</td>
<td>.8</td>
<td>.5</td>
<td>.25</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>.85</td>
<td>1</td>
<td>.1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.95</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>.7</td>
<td>.45</td>
<td>1</td>
<td>1</td>
<td>.95</td>
<td>.1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>.95</td>
<td>.7</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.8</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>.85</td>
<td>1</td>
<td>.35</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.25</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>.95</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.4</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.45</td>
</tr>
</tbody>
</table>

Table: Proportion of Samples of 20 Sets of $m$ Homogeneous Quadratic Elements in $n$ variables that are Semi-Regular
Existence of semi-regular sequences

It is widely believed that in some sense “most” sequences are semi-regular.

<table>
<thead>
<tr>
<th>$n \setminus m$</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>.8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>.35</td>
<td>1</td>
<td>.75</td>
<td>.75</td>
<td>.3</td>
<td>.65</td>
<td>.85</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>.85</td>
<td>.95</td>
<td>1</td>
<td>.9</td>
<td>.85</td>
<td>.75</td>
<td>.6</td>
<td>.2</td>
<td>.65</td>
<td>.7</td>
<td>.9</td>
<td>.9</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>.85</td>
<td>.7</td>
<td>.65</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.95</td>
<td>.95</td>
<td>.95</td>
<td>.75</td>
<td>.8</td>
<td>.5</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>.85</td>
<td>1</td>
<td>.1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.95</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>.7</td>
<td>.45</td>
<td>1</td>
<td>1</td>
<td>.95</td>
<td>.1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>.95</td>
<td>.7</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.8</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>.85</td>
<td>1</td>
<td>.35</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.25</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>.95</td>
<td>1</td>
<td>.35</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.4</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.45</td>
</tr>
</tbody>
</table>

**Table:** Proportion of Samples of 20 Sets of $m$ Homogeneous Quadratic Elements in $n$ variables that are Semi-Regular