Inverting HFE Systems is Quasi-Polynomial for All Fields

Jintai Ding[1,2] and Timothy Hodges[2]

Southern Chinese University of Technology[1]
University of Cincinnati[2]

August 18, 2011

Outline

1 Introduction

2 Our main results

3 The future work

Outline

1 Introduction

2 Our main results

3 The future work

Hidden Field Public Key Cryptosystems

$\mathbb{F} \subset \mathbb{K}$ finite fields, $|\mathbb{F}| = q$, $[\mathbb{F} \colon \mathbb{K}] = n$, $|\mathbb{K}| = q^n$

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

Private Key

Public Key

$P(X) \in \mathbb{K}[X]/\left\langle X^{q^n} - X \right\rangle$

$p_i(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]/\left\langle x_1^q - x_1, \ldots, x_n^q - x_n \right\rangle$

σ, τ invertible affine linear maps

Patarin's HFE System

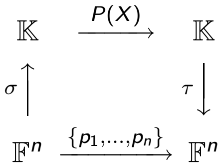
$P(X)$ is

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{P(X)} & \mathbb{K} \\ \sigma \big\uparrow & & \tau \big\downarrow \\ \mathbb{F}^n & \xrightarrow{\{p_1, \ldots, p_n\}} & \mathbb{F}^n \end{array}$$

Patarin's HFE System

$P(X)$ is

- of low total degree, D (efficient decryption).



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)

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{P(X)} & \mathbb{K} \\ \sigma \uparrow & & \downarrow \tau \\ \mathbb{F}^n & \xrightarrow{\{p_1, \ldots, p_n\}} & \mathbb{F}^n \end{array}$$

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)

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{P(X)} & \mathbb{K} \\ \sigma \uparrow & & \tau \downarrow \\ \mathbb{F}^n & \xrightarrow{\{p_1,\ldots,p_n\}} & \mathbb{F}^n \end{array}$$

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

where $a_{ij}, b_i, c \in \mathbb{K}$.

Direct Algebraic Attack

Use efficient Gröbner basis (algebraic) algorithms to solve the system of equations:

$$
\begin{aligned}
p_1(x_1, \ldots, x_n) &= y_1 \\
p_2(x_1, \ldots, x_n) &= y_2 \\
&\vdots \\
p_n(x_1, \ldots, x_n) &= y_n
\end{aligned}
$$

Direct Algebraic Attack

Use efficient Gröbner basis (algebraic) algorithms to solve the system of equations:

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= y_1 \\ p_2(x_1, \ldots, x_n) &= y_2 \\ &\vdots \\ p_n(x_1, \ldots, x_n) &= y_n \end{aligned}$$

Algorithm terminates significantly quicker on HFE systems than on random systems. How does the restriction on the degree D of P affect the complexity of algebraic solvers?

- Granboulan, Joux, Stern (Crypto 2006): If $q = 2$, complexity is quasi-polynomial.

Degree of Regularity

Degree of Regularity: 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:

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

Degree of Regularity

Degree of Regularity: 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:

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

Gröbner basis algorithms terminate shortly after this degree is reached.

Degree of Regularity of Leading Terms

Let p_i^h be the highest degree part of p_i considered as an element of the truncated polynomial ring

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

Degree of Regularity of Leading Terms

Let p_i^h be the highest degree part of p_i considered as an element of the truncated polynomial ring

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

Degree of Regularity 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: $(p_i^h)^{q-1} p_i^h = 0, \quad p_j^h p_i^h - p_i^h p_j^h = 0$

Degree of Regularity of Leading Terms

Let p_i^h be the highest degree part of p_i considered as an element of the truncated polynomial ring

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

Degree of Regularity 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: $(p_i^h)^{q-1} p_i^h = 0, \quad p_j^h p_i^h - p_i^h p_j^h = 0$
Then

$$D_{\mathrm{reg}}(p_1, \ldots, p_n) = D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h)$$

Dubois-Gama Reduction

Theorem. $D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{reg}}(p_1^h, \ldots, p_j^h)$

Dubois-Gama Reduction

Theorem. $D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{reg}}(p_1^h, \ldots, p_j^h)$

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

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

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

Dubois-Gama Reduction

Theorem. $D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{reg}}(p_1^h, \ldots, p_j^h)$

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

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

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

Theorem. $D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{reg}}(P_0)$

Outline

1 Introduction

2 Our main results

3 The future work

The main theorem

- We give a global upper bound on the degree of regularity (in the sense of DG) of an HFE system.

The main theorem

- We give a global upper bound on the degree of regularity (in the sense of DG) of an HFE system.
- **Main Theorem.**
  The degree of regularity of the system defined by P is bounded by

$$\frac{\mathrm{Rank}(P_0)(q-1)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2$$

  if $\mathrm{Rank}(P_0) > 1$. Here $\mathrm{Rank}(P_0)$ is the rank of the quadratic form P_0.

The main theorem

- We give a global upper bound on the degree of regularity (in the sense of DG) of an HFE system.
- **Main Theorem.**
  The degree of regularity of the system defined by P is bounded by

$$\frac{\mathrm{Rank}(P_0)(q-1)}{2} + 2 \leq \frac{(q-1)(\lfloor \log_q(D-1) \rfloor + 1)}{2} + 2$$

  if $\mathrm{Rank}(P_0) > 1$. Here $\mathrm{Rank}(P_0)$ is the rank of the quadratic form P_0.
- These are universal bounds that require no additional assumption.

The contribution of GJS

- Granboulan, Joux and Stern **outlined** a new way to bound the degree of regularity in the case $q = 2$.

The contribution of GJS

- Granboulan, Joux and Stern **outlined** a new way to bound the degree of regularity in the case $q = 2$.
- Their approach – lift the problem back up to the extension field $\mathbb{K}$.

The contribution of GJS

- Granboulan, Joux and Stern **outlined** a new way to bound the degree of regularity in the case $q = 2$.
- Their approach – lift the problem back up to the extension field $\mathbb{K}$.
- They sketched a way to connect the degree of regularity of an HFE system to the degree of regularity of a lifted system over the big field.

The key assumptions of GJS

- **Assuming**
  1. the degree of regularity of an HFE system $=$ the degree of regularity of a lifted system over the big field.
  2. the degree of regularity of a subsystem $\geq$ than that of the original system;
  3. asymptotic analysis results of the degree of regularity of random systems;
  4. the subsystem is generic or random,

The key assumptions of GJS

- **Assuming**
  1. the degree of regularity of an HFE system = the degree of regularity of a lifted system over the big field.
  2. the degree of regularity of a subsystem $\geq$ than that of the original system;
  3. asymptotic analysis results of the degree of regularity of random systems;
  4. the subsystem is generic or random,
- they derived **heuristic asymptotic bounds** for the case $q = 2$.

The key assumptions of GJS

- **Assuming**
  1. the degree of regularity of an HFE system $=$ the degree of regularity of a lifted system over the big field.
  2. the degree of regularity of a subsystem $\geq$ than that of the original system;
  3. asymptotic analysis results of the degree of regularity of random systems;
  4. the subsystem is generic or random,
- they derived **heuristic asymptotic bounds** for the case $q = 2$.

The key assumptions of GJS

- **Assuming**
  1. the degree of regularity of an HFE system $=$ the degree of regularity of a lifted system over the big field.
  2. the degree of regularity of a subsystem $\geq$ than that of the original system;
  3. asymptotic analysis results of the degree of regularity of random systems;
  4. the subsystem is generic or random,
- they derived **heuristic asymptotic bounds** for the case $q = 2$.
- To derive any definitive general bounds on the degree of regularity for general q and n – **an open problem**.

Interest in the odd q case

- The work by Ding, Schmidt, Werner.
  The role of the field equations $X_1^q - X_2, \ldots, X_n^q - X_1$.

Interest in the odd q case

- The work by Ding, Schmidt, Werner.
  The role of the field equations $X_1^q - X_2, \ldots, X_n^q - X_1$**.**
- No asymptotic analysis for systems over odd q.

The work of Dubois and Gama

- A breakthrough in the case of general q came in the recent work of Dubois and Gama DG – a **rigorous** mathematical foundation for the arguments in GJS.

The work of Dubois and Gama

- A breakthrough in the case of general q came in the recent work of Dubois and Gama DG – a **rigorous** mathematical foundation for the arguments in GJS.
- A new method to compute the degree of regularity over any field and an inductive algorithm that can be used to calculate a bound for the degree of regularity for any choice of q, n and D.

The work of Dubois and Gama

- A breakthrough in the case of general q came in the recent work of Dubois and Gama DG – a **rigorous** mathematical foundation for the arguments in GJS.
- A new method to compute the degree of regularity over any field and an inductive algorithm that can be used to calculate a bound for the degree of regularity for any choice of q, n and D.
- No closed formula.

Our approach

- Recall: **Theorem.** $D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{reg}}(P_0)$

Our approach

- Recall: Theorem. $D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{reg}}(P_0)$
- We find a bound for $D_{\mathrm{reg}}(P_0)$.

Our approach

- Recall: **Theorem.** $D_{\mathrm{reg}}(p_1^h, \ldots, p_n^h) \leq D_{\mathrm{reg}}(P_0)$
- We find a bound for $D_{\mathrm{reg}}(P_0)$.
- The proof is a constructive proof – explicitly constructing non-trivial syzygies.

The Constructive Proof

- finding $D_{\mathrm{reg}}(P_0)$ = finding low-degree non-trivial annihilators in an associated graded algebra.

The Constructive Proof

- finding $D_{\mathrm{reg}}(P_0) =$ finding low-degree non-trivial annihilators in an associated graded algebra.
- explicit construction of non-trivial annihilators.

The Constructive Proof

- finding $D_{\mathrm{reg}}(P_0) =$ finding low-degree non-trivial annihilators in an associated graded algebra.
- explicit construction of non-trivial annihilators.
- basis of the constructions – the classification of quadratic forms.

The case when q is even

- A quadratic polynomial in the polynomial algebra $\mathbb{K}[X_1, \ldots, X_n]$ is equivalent to an polynomial of one of the following forms for some $r \leq n$:
  1. $X_1X_2 + ... + X_{r-1}X_r$
  2. $X_1X_2 + ... + X_{r-2}X_{r-1} + X_r^2$
  3. $X_1X_2 + ... + X_{r-1}X_r + X_{r-1}^2 + cX_r^2$ where $c \in \mathbb{K}\backslash\{0\}$ satisfies $\mathrm{TR}_{\mathbb{K}}(c) = 1$.

An example of annihilator

- when rank is 4:

$$x_1x_2 + x_3x_4.$$

An example of annihilator

- when rank is 4:

$$x_1x_2 + x_3x_4.$$

- The annihilators:

$$x_1^{q-1}x_3^{q-1}, x_1^{q-1}x_4^{q-1}, x_2^{q-1}x_3^{q-1}, x_2^{q-1}x_4^{q-1}$$

An example of annihilator

- when rank is 4:
$$x_1x_2 + x_3x_4.$$
- The annihilators:
$$x_1^{q-1}x_3^{q-1}, x_1^{q-1}x_4^{q-1}, x_2^{q-1}x_3^{q-1}, x_2^{q-1}x_4^{q-1}$$
- $$(x_1x_2 + x_3x_4)x_1^{q-1}x_3^{q-1} = x_1^qx_2x_3 + x_1x_3^qx_4 = 0.$$

An example of annihilator

- when rank is 4:
$$x_1x_2 + x_3x_4.$$
- The annihilators:
$$x_1^{q-1}x_3^{q-1}, x_1^{q-1}x_4^{q-1}, x_2^{q-1}x_3^{q-1}, x_2^{q-1}x_4^{q-1}$$
- $$(x_1x_2 + x_3x_4)x_1^{q-1}x_3^{q-1} = x_1^qx_2x_3 + x_1x_3^qx_4 = 0.$$
- Proof that the annihiltor is non-trivial.

Conclusion

- For fixed q the degree of regularity is $O(\log_q D)$. Assuming that the proper parameter: $D = O(n^{\alpha})$, the complexity will be quasi-polynomial.

Conclusion

- For fixed q the degree of regularity is $O(\log_q D)$.
  Assuming that the proper parameter: $D = O(n^\alpha)$, the complexity will be quasi-polynomial.
- Conjecture: assume
  1) q itself is of scale $O(n)$,
  2) the bound above is asymptotically sharp,
  then the degree of regularity will be at least of the scale $O(n)$, so inverting HFE systems will be exponential.

- Our bound not optimal.

- Our bound not optimal.
- A detailed comparison of our bound with the bound calculated in DG.

- Our bound not optimal.
- A detailed comparison of our bound with the bound calculated in DG.

- Our bound not optimal.
- A detailed comparison of our bound with the bound calculated in DG.
- As n becomes large relative to q, the two bounds appear to be getting very close.

Outline

1 Introduction

2 Our main results

3 The future work

Future (or current) work

- The Square case: $P(X) = X^2$. (JD, IACR eprint)
- The HFE Minus case. (JD and T. Kleinjung)
- The higher degree (non-quadratic) case (TH and J. Schlather)
- Exact calculation of $D_{\mathrm{reg}}(P_0)$ (TH and J. Schlather)
- Better comparison with DG's results.
- Better bounds
- Apply our technique to other systems and provable security.

Acknowledgment

- The support of **NSF China** and **the Taft Research Center**.

Acknowledgment

- The support of **NSF China** and **the Taft Research Center**.
- The help from **V. Dubois** and **N. Gama**.

Acknowledgment

Thank you and questions?