On the Security of Biquadratic C^* Public-Key Cryptosystems

Patrick Felke

University of Applied Sciences
Emden-Leer

September 2017

HOCHSCHULE EMDEN·LEER

Preliminaries

From C^* to biquadratic C^*

The Attack

Further Research

Preliminaries

- Let $\mathbb{F}_q$ be a finite field of characteristic 2, i.e. $q = 2^m$ and $\mathbb{F}_{q^n}$ an extenstion of degree n.
- Let α be s.t. $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$. Thus $A = \{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathbb{F}_q$-Basis of $\mathbb{F}_{q^n}$.
- Let $\mathbb{F}_{q^n}[X]$ denote the univariate polynomialring over $\mathbb{F}_{q^n}$ and $\mathbb{F}_q[x_1, \ldots, x_n]$ the multivariate polynomialring over $\mathbb{F}_q$.
- The multivariate degree of a polynomial $p(x_1, \ldots, x_n)$ is defined as $\deg(p) :=$ $\max\{\sum_{j=1}^{n} i_j | \prod x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n} \text{ is a monomial of } p\}$.

Preliminaries

Representation Theorem (Univariate Case)

1. For every mapping M over $\mathbb{F}_{q^n}$ exists a polynomial $P(X) \in \mathbb{F}_{q^n}[X]$ such that $M(a) = P(a), \forall a \in \mathbb{F}_{q^n}$.
2. The polynomial is unique, if the deg$(P(X)) \leq q^n - 1$, i.e. if P is the remainder mod $X^{q^n} + X$.
3. This unique polynomial P is called the univariate representation of M.

Preliminaries

Representation Theorem (Multivariate Case)

1. For every Mapping M and basis $A = \{1, \alpha, \dots, \alpha^{n-1}\}$ of $\mathbb{F}_{q^n}$ exist multivariate polynomials
$p_1(x_1, \dots, x_n), \dots, p_n(x_1, \dots, x_n)$ such that
$M(a) = M(\sum_{i=1}^n a_i \alpha^{i-1}) = \sum_{i=1}^n p_i(a_1, \dots, a_n)\alpha^{i-1}$.
2. The representation is unique if $0 \leq j_1, \dots, j_n < q$ for every monomial $\prod x_1^{j_1} \cdot x_2^{j_2} \cdots x_n^{j_n}$ of p_i,
i.e. if p_i is the remainder mod $x_1^q + x_1, \dots, x_n^q + x_n$.
3. These unique polynomials $p_1, \dots, p_n$ are called the multivariate representation and mdeg(M):=max$\{$deg$(p_i), i = 1, \dots, n\}$ the multivariate degree of M (with respect to A).

Preliminaries

Transformation Theorem

Let $P(X)$ be the univariate and $p_1, \ldots, p_n$ the multivariate representation of a mapping M over $\mathbb{F}_{q^n}$ with respect to our basis A.
It is mdeg(M) equal to
max$\{q$-weight of $X^j|\ X^j$ a monomial of $P\}$.
Thereby the q-weight of X^j is defined as
$\sum z_i, j = \sum_i z_i q^i, 0 \leq z_i < q (q-$adic representation).

☞The multivariate degree does not depend on A.

Preliminaries

From C^* to biquadratic C^*

The Attack

Further Research

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.
- In 1993 Dobbertin analysed it to check if it can be employed in national crypto devices while he was working for the Federal Office for Information Security (FOIS) in Germany.

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.
- In 1993 Dobbertin analysed it to check if it can be employed in national crypto devices while he was working for the Federal Office for Information Security (FOIS) in Germany.
- Thereby he broke it (Patarin in '95) and introduced an alternative called biquadratic C^*.

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.
- In 1993 Dobbertin analysed it to check if it can be employed in national crypto devices while he was working for the Federal Office for Information Security (FOIS) in Germany.
- Thereby he broke it (Patarin in '95) and introduced an alternative called biquadratic C^*.This work was classified until 2001.

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.
- In 1993 Dobbertin analysed it to check if it can be employed in national crypto devices while he was working for the Federal Office for Information Security (FOIS) in Germany.
- Thereby he broke it (Patarin in '95) and introduced an alternative called biquadratic C^*.This work was classified until 2001.
- Biquadratic C^* shares almost all properties of C^*.

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.
- In 1993 Dobbertin analysed it to check if it can be employed in national crypto devices while he was working for the Federal Office for Information Security (FOIS) in Germany.
- Thereby he broke it (Patarin in '95) and introduced an alternative called biquadratic C^*.This work was classified until 2001.
- Biquadratic C^* shares almost all properties of C^*.
  ☞No redundancy required as in HFE or decryption failures like in ABC-Schemes.

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.
- In 1993 Dobbertin analysed it to check if it can be employed in national crypto devices while he was working for the Federal Office for Information Security (FOIS) in Germany.
- Thereby he broke it (Patarin in '95) and introduced an alternative called biquadratic C^*.This work was classified until 2001.
- Biquadratic C^* shares almost all properties of C^*.
  ☞No redundancy required as in HFE or decryption failures like in ABC-Schemes.
- Its major drawback was its keysize (bigger than in HFE).

From C^* to biquadratic C^*

- In 1988 Imai and Matsumoto introduced C^*, a very elegant multivariate public-key cryptosystem resistent against quantum computer aided attacks.
- In 1993 Dobbertin analysed it to check if it can be employed in national crypto devices while he was working for the Federal Office for Information Security (FOIS) in Germany.
- Thereby he broke it (Patarin in '95) and introduced an alternative called biquadratic C^*.This work was classified until 2001.
- Biquadratic C^* shares almost all properties of C^*.
  ☞No redundancy required as in HFE or decryption failures like in ABC-Schemes.
- Its major drawback was its keysize (bigger than in HFE).
- The FOIS decided against usage of biquadratic C^*.

From C^* to biquadratic C^*

- Dobbertin, Felke published "Cryptochallenge 11" over 5000 € as a part of the mystery twister competition in cooperation with Faugère.

From C^* to biquadratic C^*

- Dobbertin, Felke published "Cryptochallenge 11" over 5000 € as a part of the mystery twister competition in cooperation with Faugère.
- This challenge remained unbroken until today and the security of biquadratic C^* an open problem.

From C^* to biquadratic C^*

- Dobbertin, Felke published "Cryptochallenge 11" over 5000 € as a part of the mystery twister competition in cooperation with Faugère.
- This challenge remained unbroken until today and the security of biquadratic C^* an open problem.
- Due to the initiative of NIST and ETSI to speed up the transition to post-quantum cryptography and loosen the constraints on the keysize multivariate cryptosystems have become of great interest again.

From C^* to biquadratic C^*

- Dobbertin, Felke published "Cryptochallenge 11" over 5000 € as a part of the mystery twister competition in cooperation with Faugère.
- This challenge remained unbroken until today and the security of biquadratic C^* an open problem.
- Due to the initiative of NIST and ETSI to speed up the transition to post-quantum cryptography and loosen the constraints on the keysize multivariate cryptosystems have become of great interest again.

☞It is about time to resume its security analysis.

Biquadratic C^*

Given $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha], q = 2^m$.

Biquadratic C^*

Given $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha], q = 2^m$.

- The central mapping is a bijective power mapping of the form $F(X) := X^{1+q^{i_1}+q^{i_2}+q^{i_3}} \in \mathbb{F}_{q^n}[X]$ mit $0 < i_1 < i_2 < i_3 < n$, $\gcd(1 + q^{i_1} + q^{i_2} + q^{i_3}, q^n - 1) = 1$.
  F^{-1} is of the form X^d with $0 \leq d < q^n - 1$.

HOCHSCHULE EMDEN·LEER

Biquadratic C^*

Given $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha], q = 2^m$.

- The central mapping is a bijective power mapping of the form $F(X) := X^{1+q^{i_1}+q^{i_2}+q^{i_3}} \in \mathbb{F}_{q^n}[X]$ mit $0 < i_1 < i_2 < i_3 < n$, $\gcd(1 + q^{i_1} + q^{i_2} + q^{i_3}, q^n - 1) = 1$.
  F^{-1} is of the form X^d with $0 \leq d < q^n - 1$.
- The secret key consists of two randomly chosen bijective, affine mappings S, T over $\mathbb{F}_{q^n}$.
- The public key is the multivariate representation $p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)$ of $P(X) := S \circ F \circ T$ with respect to $\{1, \alpha, \ldots, \alpha^{n-1}\}$, i.e. mdeg=4.

Biquadratic C^*

Given $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha], q = 2^m$.

- The central mapping is a bijective power mapping of the form $F(X) := X^{1+q^{i_1}+q^{i_2}+q^{i_3}} \in \mathbb{F}_{q^n}[X]$ mit $0 < i_1 < i_2 < i_3 < n$, $\gcd(1 + q^{i_1} + q^{i_2} + q^{i_3}, q^n - 1) = 1$.
  F^{-1} is of the form X^d with $0 \leq d < q^n - 1$.
- The secret key consists of two randomly chosen bijective, affine mappings S, T over $\mathbb{F}_{q^n}$.
- The public key is the multivariate representation $p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)$ of $P(X) := S \circ F \circ T$ with respect to $\{1, \alpha, \ldots, \alpha^{n-1}\}$, i.e. mdeg=4.

☞In case of C^* the central mapping is of the form $X^{1+q^{i_1}}$ which explains Dobbertin's choice of the name.

Encryption/Decryption with biquadratic C^*

$$
\begin{tikzcd}
\text{Encryption (public):} & \mathcal{M} \arrow[rr, "P=T\circ F\circ S"] & & \mathcal{C} \arrow[d, "T^{-1}"] \\
\text{Decryption (secret):} & \mathbb{F}_{q^n} \arrow[u, "S^{-1}"'] & & \mathbb{F}_{q^n} \arrow[ll, "P=F^{-1}"']
\end{tikzcd}
$$

Encryption/Decryption with biquadratic C^*

Encryption (public):

Decryption (secret):

$$
\begin{tikzcd}
\mathcal{M} \arrow[rr, "P=T\circ F\circ S"] & & \mathcal{C} \arrow[d, "T^{-1}"] \\
\mathbb{F}_{q^n} \arrow[u, "S^{-1}"] & & \mathbb{F}_{q^n} \arrow[ll, "P=F^{-1}"']
\end{tikzcd}
$$

☠

The system is broken if given a ciphertext $b_1, \ldots, b_n$ the system of equations

$$
\begin{aligned}
p_1(x_1, \ldots, x_n) &= b_1 \\
&\vdots \\
p_n(x_1, \ldots, x_n) &= b_n
\end{aligned}
$$

can be solved efficiently over $\mathbb{F}_q$.

For biquadratic C^* this system is of mdeg 4 (C^*, mdeg 2)!

CryptoChallenge 11

CryptoChallenge 11 (2005)

- A base field $\mathbb{F}_{2^4}$.
- A large field $\mathbb{F}_{2^{100}}$, i.e. an extension of degree 25.
- $d = 1 + q + q^3 + q^{12}$.
- Randomly chosen secret affin mappings S, T over $\mathbb{F}_{2^{100}}$.
- A 100 bit ciphertext $(b_1, \ldots, b_{25})$ together with the corresponding public key.

The person who would have submitted the correct solution before the end of the year 2005 would have won 5000€.

CryptoChallenge 11

CryptoChallenge 11 (2005)

- A base field $\mathbb{F}_{2^4}$.
- A large field $\mathbb{F}_{2^{100}}$, i.e. an extension of degree 25.
- $d = 1 + q + q^3 + q^{12}$.
- Randomly chosen secret affin mappings S, T over $\mathbb{F}_{2^{100}}$.
- A 100 bit ciphertext $(b_1, \ldots, b_{25})$ together with the corresponding public key.

The person who would have submitted the correct solution before the end of the year 2005 would have won 5000€.

Remark. For the system in CryptoChallenge 11 we had

block size:	100 bit
public key length:	290 kb,
private key length:	5,200 bit.

Preliminaries

From C^* to biquadratic C^*

The Attack

Further Research

The Attack

Given a ciphertext $b_1, \ldots, b_n$ the system of equations

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= b_1 \\ &\vdots \\ p_n(x_1, \ldots, x_n) &= b_n \end{aligned}$$

has to be solved over $\mathbb{F}_q$.

- F_5 by Faugère is the state of the art algorithm to solve such equations.

HOCHSCHULE EMDEN-LEER

The Attack

Given a ciphertext $b_1, \ldots, b_n$ the system of equations

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= b_1 \\ &\vdots \\ p_n(x_1, \ldots, x_n) &= b_n \end{aligned}$$

has to be solved over $\mathbb{F}_q$.

- F_5 by Faugère is the state of the art algorithm to solve such equations.
- Its complexity is $\mathcal{O}\left(\binom{n+D}{n}^{\omega}\right)$, where $\omega := 2,373$ is the gaussian elimination constant.
- Its required memory is $\mathcal{O}\left(\binom{n+D}{n}^{2}\right)$.
- D is the maximal multivariate degree generated during the execution of F_5.

The Attack

Given a ciphertext $b_1, \dots, b_n$ the system of equations

$$\begin{aligned} p_1(x_1, \dots, x_n) &= b_1 \\ &\vdots \\ p_n(x_1, \dots, x_n) &= b_n \end{aligned}$$

has to be solved over $\mathbb{F}_q$.

- F_5 by Faugère is the state of the art algorithm to solve such equations.
- Its complexity is $\mathcal{O}\left(\binom{n+D}{n}^{\omega}\right)$, where $\omega := 2,373$ is the gaussian elimination constant.
- Its required memory is $\mathcal{O}\left(\binom{n+D}{n}^{2}\right)$.
- D is the maximal multivariate degree generated during the execution of F_5.
- The term order has to be degree-based.

Degree lexicographical ordering

With $<_{\mathsf{dlex}}$ we denote the degree lexicographical ordering which is defined as follows:
$x_1^{\alpha_1}\cdots x_n^{\alpha_n} <_{\mathsf{dlex}} x_1^{\beta_1}\cdots x_n^{\beta_n}$ iff $\deg(x_1^{\alpha_1}\cdots x_n^{\alpha_n}) < \deg(x_1^{\beta_1}\cdots x_n^{\beta_n})$ or in case of equality the leftmost nonzero entry of $(\beta_1-\alpha_1,\dots,\beta_n-\alpha_n)$ is positive.
With $\mathsf{lt}(f)$ we denote the leading term of f, which is the first term that appears when the polynomial is listed according to $<_{\mathsf{dlex}}$.

☞ $x_1 > x_2 > \cdots > x_n$

Determining D (Dubois, Gama, Hodges and Ding)

- It is hard to determine D in advance for multivariate (crypto)systems.

Determining D (Dubois, Gama, Hodges and Ding)

- It is hard to determine D in advance for multivariate (crypto)systems.
- It is commonly accepted that the degree of regularity R yields a very good approximation for D, i.e. the complexity of F_5 can be estimated by $\mathcal{O}\left(\binom{n+R}{n}^{\omega}\right)$ and $\mathcal{O}\left(\binom{n+R}{n}^{2}\right)$.

Determining D (Dubois, Gama, Hodges and Ding)

- It is hard to determine D in advance for multivariate (crypto)systems.
- It is commonly accepted that the degree of regularity R yields a very good approximation for D, i.e. the complexity of F_5 can be estimated by $\mathcal{O}\left(\binom{n+R}{n}^{\omega}\right)$ and $\mathcal{O}\left(\binom{n+R}{n}^{2}\right)$.
- Let $g_1, \ldots, g_n$ be the multivariate representation of the central mapping. The degree of regularity for equations from the public key equals the degree of regularity of
$$\begin{array}{rcl} g_1(x_1,\ldots,x_n) & = & \beta_1 \\ & \vdots & \\ g_n(x_1,\ldots,x_n) & = & \beta_n \end{array}$$
for a proper choice of $(\beta_1, \ldots, \beta_n)$.

Degree of Regularity by Hodges (simplified version)

Let g_i^h denote the homogeneous part of highest degree of g_i (multi. rep. of $F(X)$, $\mathrm{mdeg}(F(X)) = 4$).

Degree of Regularity by Hodges (simplified version)

Let g_i^h denote the homogeneous part of highest degree of g_i (multi. rep. of $F(X)$, mdeg$(F(X)) = 4$).

- Set $B := \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$ and $B_k \subset B$ the set of polynomials which have a homogeneous representation of degree k mod $x_1^q, \ldots, x_n^q$.

Degree of Regularity by Hodges (simplified version)

Let g_i^h denote the homogeneous part of highest degree of g_i (multi. rep. of $F(X)$, mdeg$(F(X)) = 4$).

- Set $B := \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$ and $B_k \subset B$ the set of polynomials which have a homogeneous representation of degree k mod $x_1^q, \ldots, x_n^q$.
- For $g_1^h, \ldots, g_n^h$ the mapping
  $\psi_k(g_1^h, \ldots, g_n^h) : B_k^n \to B_{k+4}$
  $(b_1, \ldots, b_n) \mapsto \sum_i b_i g_i^h$
  is linear.

HOCHSCHULE EMDEN·LEER

Degree of Regularity by Hodges (simplified version)

Let g_i^h denote the homogeneous part of highest degree of g_i (multi. rep. of $F(X)$, mdeg$(F(X)) = 4$).

- Set $B := \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$ and $B_k \subset B$ the set of polynomials which have a homogeneous representation of degree k mod $x_1^q, \ldots, x_n^q$.
- For $g_1^h, \ldots, g_n^h$ the mapping
  $\psi_k(g_1^h, \ldots, g_n^h) : B_k^n \to B_{k+4}$
  $(b_1, \ldots, b_n) \mapsto \sum_i b_i g_i^h$
  is linear.
- Let $T_k(g_1^h, \ldots, g_n^h)$ be the subspace of kernel$(\psi_k(g_1^h, \ldots, g_n^h))$ generated by
  1. $b \cdot (0, \ldots, 0, g_j^h, 0, \ldots, 0, g_i^h, 0, \ldots, 0), 1 \leq i < j \leq n, b \in B_k$, g_j^h the i-th entry and g_i^h the j-th.
  2. $b \cdot (0, \ldots, 0, g_i^{h^{q-1}}, 0, \ldots, 0), 1 \leq i \leq n, b \in B_{k-q-1}$, $g_i^{h^{q-1}}$ the i-th entry.

Degree of Regularity by Hodges (simplified version)

Let g_i^h denote the homogeneous part of highest degree of g_i (multi. rep. of $F(X)$, mdeg$(F(X)) = 4$).

- Set $B := \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$ and $B_k \subset B$ the set of polynomials which have a homogeneous representation of degree k mod $x_1^q, \ldots, x_n^q$.
- For $g_1^h, \ldots, g_n^h$ the mapping
  $\psi_k(g_1^h, \ldots, g_n^h) : B_k^n \to B_{k+4}$
  $(b_1, \ldots, b_n) \mapsto \sum_i b_i g_i^h$
  is linear.
- Let $T_k(g_1^h, \ldots, g_n^h)$ be the subspace of kernel$(\psi_k(g_1^h, \ldots, g_n^h))$ generated by
  1. $b \cdot (0, \ldots, 0, g_j^h, 0, \ldots, 0, g_i^h, 0, \ldots, 0), 1 \leq i < j \leq n, b \in B_k$, g_j^h the i-th entry and g_i^h the j-th.
  2. $b \cdot (0, \ldots, 0, {g_i^h}^{q-1}, 0, \ldots, 0), 1 \leq i \leq n, b \in B_{k-q-1}$, ${g_i^h}^{q-1}$ the i-th entry.
- The degree of regularity is $R(g_1^h, \ldots, g_n^h) :=$ $\min\{k + 4 | \text{kernel}(\psi_k(g_1^h, \ldots, g_n^h))/T_k(g_1^h, \ldots, g_n^h) \neq 0\}$.

Basic Idea

Cut out trivial relations:
If the leading terms conforming a degree-based term ordering of e.g. $g_1 + \beta_1, g_2 + \beta_2$ have no common divisor then:

- The reduction in F_5 will be based on $(g_1 + \beta_1)(g_2 + \beta_2) + (g_2 + \beta_2)(g_1 + \beta_1) = 0.$
- From this nothing is gained to find a solution.

Main Result

Biquadratic C^* is weak

Let $p_1, \ldots, p_n$ be the public key of a biquadratic C^* public-key cryptosystem and $b_1, \ldots, b_n$ a ciphertext.
The complexity to find the plaintext $a_1, \ldots, a_n$ is at most $\mathcal{O}\left(\binom{n+7}{n}^{\omega}\right), \omega = 2,373$ and the required memory $\mathcal{O}\left(\binom{n+7}{n}^{2}\right)$.

Main Result

Biquadratic C^* is weak

Let $p_1, \ldots, p_n$ be the public key of a biquadratic C^* public-key cryptosystem and $b_1, \ldots, b_n$ a ciphertext.
The complexity to find the plaintext $a_1, \ldots, a_n$ is at most $\mathcal{O}\left(\binom{n+7}{n}^{\omega}\right), \omega = 2,373$ and the required memory $\mathcal{O}\left(\binom{n+7}{n}^{2}\right)$.

Good news: We skip the proof

Main Result

Biquadratic C^* is weak

Let $p_1, \ldots, p_n$ be the public key of a biquadratic C^* public-key cryptosystem and $b_1, \ldots, b_n$ a ciphertext.
The complexity to find the plaintext $a_1, \ldots, a_n$ is at most $\mathcal{O}\left(\binom{n+7}{n}^{\omega}\right), \omega = 2,373$ and the required memory $\mathcal{O}\left(\binom{n+7}{n}^{2}\right)$.

Good news: We skip the proof
and explain it with the help of Cryptochallenge 11 instead.

Example CryptoChallenge 11

- Base field $\mathbb{F}_{2^4}$
- Large field $\mathbb{F}_{2^{100}}$, i.e. an extension of degree 25.
- $d = 1 + q + q^3 + q^{12}$.

Example CryptoChallenge 11

- Base field $\mathbb{F}_{2^4}$
- Large field $\mathbb{F}_{2^{100}}$, i.e. an extension of degree 25.
- $d = 1 + q + q^3 + q^{12}$.

It is $F(X) = XX^qX^{q^3}X^{q^{12}}$ and thus

$$X^qX^{q^3}X^{q^{12}}F(X)^{q^{13}} + X^{q^{13}}X^{q^{14}}X^{q^{16}}F(X)$$

$$X^qX^{q^3}X^{q^{12}}\left(XX^{q^{13}}X^{q^{14}}X^{q^{16}}\right) + X^{q^{13}}X^{q^{14}}X^{q^{16}}\left(XX^qX^{q^3}X^{q^{12}}\right) = 0.$$

Example CryptoChallenge 11

- Base field $\mathbb{F}_{2^4}$
- Large field $\mathbb{F}_{2^{100}}$, i.e. an extension of degree 25.
- $d = 1 + q + q^3 + q^{12}$.

It is $F(X) = X X^q X^{q^3} X^{q^{12}}$ and thus

$$X^q X^{q^3} X^{q^{12}} F(X)^{q^{13}} + X^{q^{13}} X^{q^{14}} X^{q^{16}} F(X)$$

$$X^q X^{q^3} X^{q^{12}} \left(X X^{q^{13}} X^{q^{14}} X^{q^{16}} \right) + X^{q^{13}} X^{q^{14}} X^{q^{16}} \left(X X^q X^{q^3} X^{q^{12}} \right) = 0.$$

☞The degree of regularity is 7 and we have the following

Corollary

Cryptochallenge 11 can be broken in running time $\mathcal{O}\left(\binom{25+7}{25}^{2{,}373}\right) \approx 2^{52}$ and with a required memory of $\mathcal{O}\left(\binom{25+7}{25}^{2}\right) \approx 1,3$ Tb.

Corollary

Cryptochallenge 11 can be broken in running time $\mathcal{O}\left(\binom{25+7}{25}^{2,373}\right) \approx 2^{52}$ and with a required memory of $\mathcal{O}\left(\binom{25+7}{25}^{2}\right) \approx 1,3$ Tb.

☠ When Dobbertin and I developed this challenge in 2005 we were convinced that biquadratic C^* is strong in general.

Preliminaries

From C^* to biquadratic C^*

The Attack

Further Research

Further Research/Work in Progress

- Proof a strong bound on D with the help of the above used syszygies directly for these simple bijective power mappings to better understand the degree of regularity.

HOCHSCHULE EMDEN·LEER

Further Research/Work in Progress

- Proof a strong bound on D with the help of the above used syszygies directly for these simple bijective power mappings to better understand the degree of regularity.

Any questions?