A Polynomial-Time Attack on the BBCRS Scheme

Alain Couvreur [1] **Ayoub Otmani** [2] Jean-Pierre Tillich [3] Valérie Gauthier–Umaña [4]

[1]INRIA, Grace Team & LIX, CNRS UMR 7161
alain.couvreur@lix.polytechnique.fr

[2]University of Rouen, LITIS
ayoub.otmani@univ-rouen.fr

[3]INRIA, Secret Team
jean-pierre.tillich@inria.fr

[4]Universidad del Rosario
Faculty of Natural Sciences and Mathematics
gauthier.valerie@urosario.edu.co

PKC 2015
March 30 - April 1
Maryland, USA

Outline

Part I

Code-Based Cryptography

Coding Theory Terminology

- **Code.** Finite-dimensional vector subspace of $\mathbb{K}^n$ with finite field $\mathbb{K}$
- **Generating matrix.** $G \in \mathbb{K}^{k \times n}$ whose rows $\vec{g}_1, \ldots, \vec{g}_k$ form a basis

$$\mathscr{C} \stackrel{\text{def}}{=} \sum_{i=1}^{k} \mathbb{K}\, \vec{g}_i$$

- **Dual.**

$$\mathscr{C}^{\perp} \stackrel{\text{def}}{=} \left\{ \vec{v} \in \mathbb{K}^n \ : \ G\, \vec{v}^T = \vec{0} \right\}$$

McEliece Encryption Scheme

- **Private key**

  1. $G_{sec} \in \mathbb{K}^{k \times n}$ generates a code that corrects t errors
  2. Permutation $\Pi \in \mathfrak{S}n$
  3. $S \in GL_k(\mathbb{K})$

- **Public key**

$$G_{pub} \stackrel{\text{def}}{=} S\ G_{sec}\ \Pi^{-1}$$

- **Encryption** Plaintext $\vec{m} \in \mathbb{K}^k$ and ciphertext $\vec{z} \in \mathbb{K}^n$

$$\vec{z} = \vec{m}\, G_{pub} + \vec{e} \quad \text{with} \quad \left\|\, \vec{e} \,\right\| = t$$

- **Decryption** Decode $D\left(\vec{z}\,\Pi\right) \rightsquigarrow \vec{w}$ and output $\vec{w}\, S^{-1}$

Remark

1. *$\mathscr{C}_{pub}$ denotes code generated by G_{pub}*
2. *McEliece proposed **binary Goppa** codes*

Generalised Reed–Solomon (GRS) Code

Definition

- $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{K}^n$ with $x_i \neq x_j$ for all $i \neq j$
- $\vec{y} = (y_1, \ldots, y_n) \in \mathbb{K}^n$ with $y_i \neq 0$

$$\mathrm{GRS}_k(\vec{x}, \vec{y}) \stackrel{\text{def}}{=} \left\{ \big(y_1 f(x_1), \ldots, y_n f(x_n)\big) : f \in \mathbb{K}[X]_{<k} \right\}$$

Remark

1. $\mathrm{GRS}_k(\vec{x}, \vec{y}) \simeq \mathbb{K}[X]_{<k}$
2. *There exists* $\vec{z} \in \mathbb{K}^n$ *with* $z_i \neq 0$ *such that:*

$$\mathrm{GRS}_k(\vec{x}, \vec{y})^{\perp} = \mathrm{GRS}_{n-k}(\vec{x}, \vec{z})$$

GRS Codes in Cryptography

Niedereiter's variant ('88)

- McEliece scheme based on $\mathbf{GRS}_k(\vec{x}, \vec{y})$ where $(\vec{x}, \vec{y})$ is **secret**
- Sidelnikov–Shestakov attack ('92) finds in polynomial time $(\vec{x}_*, \vec{y}_*)$ such that

$$\mathbf{GRS}_k(\vec{x}_*, \vec{y}_*) = \mathbf{GRS}_k(\vec{x}, \vec{y})$$

Alternative hiding technique

- Taking subcode $\rightsquigarrow \mathrm{rank}(S) < k$ (Berger, Loidreau '05)
- Adjoining random columns A to $G_{sec} \rightsquigarrow (G_{sec} \mid A)$ (Wieschebrink '06)
- Replacing $\Pi \rightsquigarrow T + R$ (Baldi, Bianchi, Chiaraluce, Rosenthal, Schipani '11 & '14)

Homomorphic public-key encryption

- $G_{sec} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ (Bogdanov, Lee '12)

Part II

Distinguishing Properties of GRS Codes

Toolbox

- **Componentwise product**
  1. $\vec{a}, \vec{b} \in \mathbb{K}^n$
  $$\vec{a} \star \vec{b} \stackrel{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n)$$
  2. $A \in \mathbb{K}^{k_A \times n}$ and $B \in \mathbb{K}^{k_B \times n}$
  $$A \star B \stackrel{\text{def}}{=} \left(\vec{a_i} \star \vec{b_j}\right)_{\substack{1 \leqslant i \leqslant k_A \\ 1 \leqslant j \leqslant k_B}}$$
- **Componentwise product of codes** generated by $A \star B$
  $$\mathscr{A} \star \mathscr{B} \stackrel{\text{def}}{=} \sum_{\substack{1 \leqslant i \leqslant k_A \\ 1 \leqslant j \leqslant k_B}} \mathbb{K}\, \vec{a_i} \star \vec{b_j}$$
- **Square code** $\mathscr{A}^2 \stackrel{\text{def}}{=} \mathscr{A} \star \mathscr{A}$

Proposition

$\mathscr{A}^2$ can be computed in $O(n^2 k^2)$ operations for $\mathscr{A} \subset \mathbb{K}^n$ of dimension k

Distinguisher of GRS Codes

1. $\mathscr{C}$ is random code of dimension k

$$\dim \mathscr{C}^2 = \binom{k+1}{2} \text{ as long as } \binom{k+1}{2} < n$$

2. $\mathscr{C}$ is $\mathbf{GRS}_k(\vec{x}, \vec{y})$

$$\dim \mathscr{C}^2 = 2k-1 \text{ as long as } 2k-1 < n$$

Definition

A code $\mathscr{C} \subset \mathbb{K}^n$ of dimension k is said to be **distinguishable** if

$$\dim \mathscr{C}^2 < \min \left\{ \binom{k+1}{2}, n \right\}$$

Remark

If $2k-1 \geqslant n$ don't forget the dual ode!

Extending the Range of the Distinguisher

Definition

- **Shortening** of $\mathscr{C}$ over $U \subset \{1, \ldots, n\}$ is the restriction to $\vec{c} \in \mathscr{C}$ such that:

$$\forall i \in U, \quad c_i = 0$$

- $\mathcal{S}_U(\mathscr{C})$ denotes the shortening of $\mathscr{C}$ over U

Facts

1. $\dim \mathcal{S}_U(\mathscr{C}) = \dim \mathscr{C} - |U|$
2. If $\mathscr{C} = \mathbf{GRS}_k(\vec{x}, \vec{y})$ then:

$$\begin{aligned} \mathcal{S}_U(\mathscr{C}) &\simeq \left\{ f \in \mathbb{K}[X]_{<k} \ : \ \forall u \in U, \ f(x_u) = 0 \right\} \\ &\simeq \prod_{u \in U} (X - x_u) \mathbb{K}[X]_{<k-|U|} \end{aligned}$$

Part III

BBCRS Scheme

BBCRS Scheme (Baldi, Bianchi, Chiaraluce, Rosenthal, Schipani '11 & '14)

- Secret key
  1. $G_{sec} \in \mathbb{K}^{k \times n}$ is a generating matrix of $\mathbf{GRS}_k(\vec{x}, \vec{y})$
  2. **Sparse** $T \in GL_n(\mathbb{K})$
  3. **Low rank** R such that $T + R \in GL_n(\mathbb{K})$
  4. $S \in GL_k(\mathbb{K})$

- Public key $G_{pub} \stackrel{\text{def}}{=} S\, G_{sec}\, (T + R)^{-1}$

1. **Version 1** (BBCRS '11). T is a permutation broken by Couvreur *et al.* ('13)
2. **Version 2** (BBCRS '14). $T \in GL_n(\mathbb{K})$ is a sparse

Remark

Error has the form $\vec{e}\,T + \vec{e}R \rightsquigarrow$ *Decryption remove* $\vec{e}R$ *by enumerating all elements of* $\mathbb{K}$

Preliminaries

Proposition

There exists $\vec{z}$ such that ${\mathscr{C}_{pub}}^{\perp} = \mathsf{GRS}_{n-k}(\vec{x}, \vec{z})(T + R)^{T}$

Proof.

1. By assumption $\mathscr{C}_{\text{pub}} = \mathsf{GRS}_k(\vec{x}, \vec{y})(T + R)^{-1}$

$$\rightsquigarrow {\mathscr{C}_{\text{pub}}}^{\perp} = \mathsf{GRS}_k(\vec{x}, \vec{y})^{\perp}(T + R)^{T}$$

2. There exists $\vec{z}$ such that:

$$\mathsf{GRS}_k(\vec{x}, \vec{y})^{\perp} = \mathsf{GRS}_{n-k}(\vec{x}, \vec{z})$$

□

Notation

$$\mathscr{D}_{\text{pub}} \stackrel{\text{def}}{=} {\mathscr{C}_{\text{pub}}}^{\perp}$$

BBCRS – v1

$\mathscr{D}_{\text{pub}} = \mathbf{GRS}_{n-k}(\vec{x}, \vec{z})\left(T^T + R^T\right)$ with

- T^T is a **permutation** denoted by Π
- $\text{rank}(R^T) = \text{rank}(R) = z$ where z is small ($z \leqslant 4$)

Fundamental Properties

1. $\mathscr{D}_{\text{pub}} = \mathbf{GRS}_{n-k}(\vec{x}\,\Pi, \vec{z}\,\Pi)\left(I_n + (R\Pi)^T\right)$
2. $\mathbf{GRS}_{n-k}(\vec{x}\,\Pi, \vec{z}\,\Pi)$ is a GRS code $\rightsquigarrow \vec{x}_* \stackrel{\text{def}}{=} \vec{x}\,\Pi$ and $\vec{z}_* \stackrel{\text{def}}{=} \vec{z}\,\Pi$
3. $\text{rank}\,(R\Pi) = \text{rank}(R)$ $\rightsquigarrow R_* \stackrel{\text{def}}{=} (R\Pi)^T$
4. $\mathscr{D}_{\text{pub}} \cap \mathbf{GRS}_{n-k}(\vec{x}_*, \vec{z}_*)$ is of co-dimension z

Cryptanalysis of BBCRS – v1 (Couvreur et al. '14)

Assumptions

1. $\mathscr{D}_{\text{pub}} = \mathbf{GRS}_{n-k}(\vec{x}_*, \vec{z}_*)(I_n + R_*)$
2. $\text{rank}(R_*) = 1$

Fundamental facts

- Attack builds a polynomial-time **distinguisher** that recognises samples from
$$\mathscr{S} \stackrel{\text{def}}{=} \mathscr{D}_{\text{pub}} \cap \mathbf{GRS}_{n-k}(\vec{x}_*, \vec{z}_*)$$
- Distinguisher relies on the star product operation $\star$

Time complexity $O(n^6)$ field operations

BBCRS – v2

Assumption $\mathscr{D}_{\text{pub}} = \mathbf{GRS}_{n-k}(\vec{x}, \vec{z})\left(T^T + R^T\right)$ with

- Columns of T^T are either of weight 1 or 2
  1. $\mathcal{J}_1 = \{i : i\text{-th column of weight } 1\}$
  2. $\mathcal{J}_2 = \{i : i\text{-th column of weight } 2\}$
- Average row weight $1 < m \leqslant 2$

Terminology

1. $\mathcal{J}_1 \stackrel{\text{def}}{=} \{\text{ degree-1 position }\}$
2. $\mathcal{J}_2 \stackrel{\text{def}}{=} \{\text{ degree-2 position }\}$

Public Key of BBCRS – v2

- Generating matrix of $\mathscr{D}_{\text{pub}}$ has the following form:

$$\underbrace{\underbrace{\begin{pmatrix} \dots & \overbrace{\alpha_u f_1(x_u)}^{i\text{–th column}} & \dots & \dots & \overbrace{\beta_v f_1(x_v) + \eta_\ell f_1(x_\ell)}^{j\text{–th column}} & \dots \\ & \vdots & & & \vdots & \\ \dots & \alpha_u f_{n-k}(x_u) & \dots & \dots & \beta_v f_{n-k}(x_v) + \eta_\ell f_{n-k}(x_\ell) & \dots \end{pmatrix}}_{\mathcal{J}_1}}_{\mathcal{J}_2} + S G_{sec} R^T$$

- $f_1, \dots, f_{n-k}$ belong to $\mathbb{K}[X]_{<n-k}$

- α_u, β_v and η_ℓ are non-zero elements from $\mathbb{K}$ (= non-zero entries of T^T)

Part IV

Cryptanalysis of BBCRS – v2

A Foretaste of the New Attack

Assumption $\mathscr{D}_{\text{pub}} = \mathsf{GRS}_{n-k}(\vec{x}, \vec{z})\left(T^T + R^T\right)$ with $\mathsf{rank}(R^T) = 1$

- **Step 1.** Finding all degree-2 positions
- **Step 2.** Transforming degree-2 positions into degree-1
- **Step 3.** Applying attack against BBCRS – v1

Prerequisite Choose $U \subset \{1, \ldots, n\}$ such that $\mathcal{S}_U\left(\mathscr{D}_{\text{pub}}\right)$ is **distinguishable**

Distinguishing $\mathcal{S}_U(\mathscr{D}_{\text{pub}})$

$\mathscr{D} \overset{\text{def}}{=} \mathcal{S}_U(\mathscr{D}_{\text{pub}})$ is **distinguishable** and since $\dim \mathscr{D} = n - k - |U|$ then

$$\dim \mathscr{D}^2 < \min \left\{ n - |U|, \binom{n-k-|U|+1}{2} \right\} \tag{1}$$

Proposition

$$U \subseteq \mathcal{J}_1, \qquad \dim \mathscr{D}^2 \leqslant 3\Big(n-k-|U|\Big) - 1 + |\mathcal{J}_2| \tag{2}$$

Corollary

$$(1) + (2) \rightsquigarrow \begin{cases} n - k - |U| = O\left(\sqrt{n}\right) \\ m < 1 + \frac{k}{n} + O\left(\frac{1}{\sqrt{n}}\right) \end{cases}$$

Fundamental Property

Definition

- **Puncturing** at position i consists in removing the i-th coordinate
- $\mathcal{P}_i(\mathscr{A})$ denotes the punctured code at position i of the code $\mathscr{A}$

Facts If $\mathscr{D} \stackrel{\text{def}}{=} \mathcal{S}_U(\mathscr{D}_{\text{pub}})$ is **distinguishable** then

1. When $i \in \mathcal{J}_1$ then it **always** holds:

$$\dim \mathscr{D}_U^2 = \dim \mathcal{P}_i\left(\mathscr{D}_U^2\right) \tag{3}$$

2. Whereas for "good choices" of U when $i \in \mathcal{J}_2$

$$\dim \mathscr{D}_U^2 = \dim \mathcal{P}_i\left(\mathscr{D}_U^2\right) + 1 \tag{4}$$

First Step – Finding All Degree-2 Positions

$\mathcal{J}_2 \leftarrow \{\ \}$

Repeat $O(1)\{$

Pick at random $U \subset \{1, \ldots, n\}$ with $i \notin U$

$\mathscr{D} \stackrel{\text{def}}{=} \mathcal{S}_U\left(\mathscr{D}_{\text{pub}}\right)$

For $i \in \{1, \ldots, n\} \setminus \mathcal{J}_2$ do $\{$

If $\dim \mathscr{D}^2 \neq \dim \mathcal{P}_i\left(\mathscr{D}^2\right)$ then

$\mathcal{J}_2 \leftarrow \mathcal{J}_2 \cup \{i\}$

$\}$

$\}$

return $\mathcal{J}_2$

Complexity $O\left((n-k-|U|)^2 n^2\right) = O\left(n^3\right)$ field operations

Detection of a Degree–1 Position Involved in Degree–2 Position

- Assume that a degree–2 position (j–th column) involves a degree–1 position (i–th column)

$$D = \underbrace{\begin{pmatrix} \cdots & \overbrace{\alpha_u f_1(x_u)}^{i\text{–th column}} & \cdots \\ & \vdots & \\ \cdots & \alpha_u f_{n-k}(x_u) & \cdots \end{pmatrix}}_{\mathcal{J}_1} \underbrace{\begin{pmatrix} \cdots & \overbrace{\beta_u f_1(x_u) + \eta_\ell f_1(x_\ell)}^{j\text{–th column}} & \cdots \\ & \vdots & \\ \cdots & \beta_u f_{n-k}(x_u) + \eta_\ell f_{n-k}(x_\ell) & \cdots \end{pmatrix}}_{\mathcal{J}_2}$$

- Shortening at position $i \rightsquigarrow f_1(x_u) = \cdots = f_{n-k}(x_u) = 0$

$$D \text{ becomes } \rightsquigarrow \underbrace{\begin{pmatrix} \cdots & 0 & \cdots \\ & \vdots & \\ \cdots & 0 & \cdots \end{pmatrix}}_{\mathcal{J}_1} \underbrace{\begin{pmatrix} \cdots & 0 + \eta_\ell f_1(x_\ell) & \cdots \\ \cdots & \vdots & \cdots \\ \cdots & 0 + \eta_\ell f_{n-k}(x_\ell) & \cdots \end{pmatrix}}_{\mathcal{J}_2}$$

IsDegree2($\mathscr{C}, i$)

Output

- `true` : i is a degree-2 for $\mathscr{C}$
- `false` : i is a degree-1 for $\mathscr{C}$

repeat $O(1)\{$

Pick at random $U \subset \{1, \ldots, n\}$ with $i \notin U$

$\mathscr{C}_U \stackrel{\text{def}}{=} \mathcal{S}_U(\mathscr{C})$

if $\dim \mathscr{C}_U^2 \neq \dim \mathcal{P}_i\left(\mathscr{C}_U^2\right)$ then

return `true`

$\}$

return `false`

Complexity $O\left(n^3\right)$ field operations

Computing $\mathcal{J}_2(i)$

Input

- $i \in \mathcal{J}_1$
- $\mathscr{D} \stackrel{\text{def}}{=} \mathcal{S}_i\left(\mathscr{D}_{\text{pub}}\right)$

Output

- $\mathcal{J}_2(i)$ = Set of degree-2 positions in which i is involved

$\mathcal{J}_2(i) \leftarrow \{\ \}$
for $j \in \mathcal{J}_2$ do {
    if IsDegree2($\mathscr{D}, j$) = `false` then
        $\mathcal{J}_2(i) \leftarrow \mathcal{J}_2(i) \cup \{j\}$
}
return $\mathcal{J}_2(i)$

Complexity $O\left(|\mathcal{J}_2| n^3\right) = O\left(n^4\right)$ since $|\mathcal{J}_2| = O(n)$ field operations

Second Step – Transforming Degree-2 Positions into Degree-1

Notation

- $\Delta_{j,\alpha,i}$ transforms j-th column by j-th column $+\ \alpha\times$ i-th column

Input

- $i \in \mathcal{J}_1$
- $j \in \mathcal{J}_2(i)$

for $\alpha \in \mathbb{K}$ do {
  $\mathscr{D}^{\mathrm{tmp}} \leftarrow \Delta_{j,\alpha,i}\left(\mathscr{D}_{\mathrm{pub}}\right)$
  if IsDegree2$(\mathscr{D}^{\mathrm{tmp}}, j) =$ `false`
    $\mathscr{D}_{\mathrm{pub}} \leftarrow \mathscr{D}^{\mathrm{tmp}}$
}

Complexity $O\left(|\mathbb{K}|n^3\right)$ field operations for given i and j

Time Complexity of the Attack

Facts

1. $|\mathbb{K}| = O(n)$
2. $|\mathcal{J}_1| = O(n)$ and $|\mathcal{J}_2| = O(n)$
3. For all $i \in \mathcal{J}_1$, $|\mathcal{J}_2(i)| = O(1)$

- Step 1. Finding all degree-2 positions. $O(n^3)$
- Step 2. Transforming degree-2 positions into degree 1. $O(n^5)$
- Step 3. Attack of BBCRS – v1. $O(n^6)$

Experimental Results

(q, n, k)	m	Step 1	Step 2
(347, 346, 180)	1.471	15s	$\approx$ 5 hours
(347, 346, 188)	1.448	8s	$\approx$ 3 hours
(347, 346, 204)	1.402	10s	$\approx$ 2.25 hours
(347, 346, 228)	1.332	15s	$\approx$ 2.5 hours
(347, 346, 252)	1.263	36s	$\approx$ 2.75 hours
(347, 346, 268)	1.217	3s	$\approx$ 4 hours
(347, 346, 284)	1.171	3s	$\approx$ 2 hours
(547, 546, 324)	1.401	60s	$\approx$ 16 hours
(547, 546, 340)	1.372	83s	$\approx$ 20 hours
(547, 546, 364)	1.328	100s	$\approx$ 20 hours
(547, 546, 388)	1.284	170s	$\approx$ 24 hours
(547, 546, 412)	1.240	15s	$\approx$ 43 hours
(547, 546, 428)	1.211	15s	$\approx$ 30.5 hours

Magma V2.20-3 with Xeon 2.27GHz and 72 Gb of RAM

Conclusion

- BBCRS scheme proposes an alternative way of "hiding" codes

$$\Pi \rightsquigarrow T + R \text{ where } T \text{ is sparse and } \mathbf{rank}(R) = z \text{ is low}$$

- Polynomial-time attack when:
  1. GRS codes are used
  2. Average row density $1 \leqslant m < 1 + \frac{k}{n} + O\left(\frac{1}{\sqrt{n}}\right)$
  3. $z = 1$

- Increasing z avoids the attack but the scheme becomes less efficient (decryption is exponentiel in z)

- Taking $m = 2$ deserves a better understanding