Sidelnikov-Shestakov attack on Reed-Solomon code in McEliece

Elena Kirshanova

Seminar at RUB
November 30, 2021

Outline

Part I

Reed-Solomon Code

Reed-Solomon Code: definition

Fix the following parameters:

- $1 \leq k < n$, $\mathbb{F}_q$–finite field, $q > n$.
- $S = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$, α_i's are distinct

Reed-Solomon Code C of length n and dimension k is

$$\mathrm{RM}[n, k] = \Big\{(p(\alpha_1), \ldots, p(\alpha_n) \in \mathbb{F}_q^n \ : \ p \in \mathbb{F}_q[x], \deg p(x) \leq k - 1\Big\}$$

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

is a generator matrix of $\mathrm{RM}[n, k]$.

Reed-Solomon Code: parity-check matrix

When $S = \{1, \alpha, \ldots, \alpha^{n-1}\} = \mathbb{F}_q^\star$ for α primitive in $\mathbb{F}_q$, previous definition is equivalent to

$$\mathsf{RM}[n,k] = \Big\{(c_0, \ldots, c_{n-1} \in \mathbb{F}_q^n \;:\; c(x) = \sum c_i x^i, \\ c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{n-k}) = 0\Big\},$$

Hence, the parity check matrix of $\mathsf{RM}[n,k]$ is

$$H = \begin{pmatrix} 1 & \alpha & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \ldots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \ldots & \alpha^{(n-1)(n-k)} \end{pmatrix} \in \mathbb{F}_q^{n-k \times n}$$

Generalized Reed-Solomon Code

Add $(v_1, \dots, v_n) \in \mathbb{F}_q \setminus \{0\}$ to the parameters.

Generalized Reed-Solomon (GRS) is generated by

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} v_1 & 0 & \dots & 0 \\ 0 & v_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & v_n \end{pmatrix}$$

Its parity-check matrix is for some $(z_1, \dots, z_n) \in \mathbb{F}_q \setminus \{0\}$

$$H = \underbrace{\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha^{n-k-1} & \dots & \alpha_n^{(n-k-1)} \end{pmatrix}}_{V(\alpha_1, \dots, \alpha_n)} \begin{pmatrix} z_1 & 0 & \dots & 0 \\ 0 & z_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & z_n \end{pmatrix}$$

McEliece with Reed-Solomon

- sk $= (\alpha_1, \dots, \alpha_n, v_1, \dots v_n)$ – compact description of RM$[n, k]$
- pk $= B = M \cdot H$ for non-singular $M \in \mathbb{F}_q^{n-k \times n-k}$, i.e.,

$$B = MH = M \cdot \begin{pmatrix} z_1 & z_2 & \dots & z_n \\ z_1\alpha_1 & z_2\alpha_2 & \dots & z_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ z_1\alpha_1^{n-k-1} & z_2\alpha^{n-k-1} & \dots & z_n\alpha_n^{(n-k-1)} \end{pmatrix}$$

Knowledge of sk allows fast unique decoding algorithms for up to $\lfloor \frac{n-k}{2} \rfloor$ errors.

Part II.I

Sidelnikov-Shestakov (case $z_i = 1$)

Observation I

The attack is given B, the goal is to find $\alpha_1, \ldots, \alpha_n$.

Augment $\mathbb{F}_q$ with $\{\infty\}$, i.e., $\mathbb{F}_q^\infty := \mathbb{F}_q \cup \{\infty\}$.
Conventions: $1/\infty = 0, 1/0 = \infty, f(\infty) = f_{\deg f}$.

Observation I

The attack is given B, the goal is to find $\alpha_1, \dots, \alpha_n$.

Augment $\mathbb{F}_q$ with $\{\infty\}$, i.e., $\mathbb{F}_q^\infty := \mathbb{F}_q \cup \{\infty\}$.
Conventions: $1/\infty = 0, 1/0 = \infty, f(\infty) = f_{\deg f}$.

$$B = \begin{pmatrix} f_0^{(1)} & f_1^{(1)} & \dots & f_{n-k-1}^{(1)} \\ f_0^{(2)} & f_1^{(2)} & \dots & f_{n-k-1}^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ f_0^{(n-k)} & f_1^{(n-k)} & \dots & f_{n-k-1}^{(n-k)} \end{pmatrix} \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha^{n-k-1} & \dots & \alpha_n^{(n-k-1)} \end{pmatrix}$$

Observation I

The attack is given B, the goal is to find $\alpha_1, \ldots, \alpha_n$.

Augment $\mathbb{F}_q$ with $\{\infty\}$, i.e., $\mathbb{F}_q^\infty := \mathbb{F}_q \cup \{\infty\}$.
Conventions: $1/\infty = 0, 1/0 = \infty, f(\infty) = f_{\deg f}$.

$$B = \begin{pmatrix} f_0^{(1)} & f_1^{(1)} & \ldots & f_{n-k-1}^{(1)} \\ f_0^{(2)} & f_1^{(2)} & \ldots & f_{n-k-1}^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ f_0^{(n-k)} & f_1^{(n-k)} & \ldots & f_{n-k-1}^{(n-k)} \end{pmatrix} \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha^{n-k-1} & \ldots & \alpha_n^{(n-k-1)} \end{pmatrix}$$

$$= \begin{pmatrix} f^{(1)}(\alpha_1) & f^{(1)}(\alpha_2) & \ldots & f^{(1)}(\alpha_n) \\ f^{(2)}(\alpha_1) & f^{(2)}(\alpha_2) & \ldots & f^{(2)}(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ f^{(n-k)}(\alpha_1) & f^{(n-k)}(\alpha_2) & \ldots & f^{(n-k)}(\alpha_n) \end{pmatrix}$$

Entries of B are the evaluations of $n - k$ polynomials in α_i's.

Observation II

There are many solutions!

Let $(M, \alpha_1, \ldots, \alpha_n)$ be a solution, i.e., $B = M \cdot V(\alpha_1, \ldots, \alpha_n)$

Fix $a, b \in \mathbb{F}_q$. For $0 \leq i \leq n-k-1$:

$$(ax+b)^i = \sum_{j=0}^{n-k-1} m'_{i,j} x^j \quad \Rightarrow \quad M' = (m'_{i,j}) - \text{lower-triangular}$$

Observation II

There are many solutions!

Let $(M, \alpha_1, \ldots, \alpha_n)$ be a solution, i.e., $B = M \cdot V(\alpha_1, \ldots, \alpha_n)$

Fix $a, b \in \mathbb{F}_q$. For $0 \leq i \leq n-k-1$:

$$(ax+b)^i = \sum_{j=0}^{n-k-1} m'_{i,j} x^j \quad \Rightarrow \quad M' = (m'_{i,j}) \text{ -- lower-triangular}$$

$M' \cdot V(\alpha_1, \ldots, \alpha_n) = V(a\alpha_1 + b, \ldots, a\alpha_n + b)$ (easy to check).

$$\begin{aligned} B = M \cdot V(\alpha_1, \ldots, \alpha_n) &= MM'^{-1} \cdot M'V(\alpha_1, \ldots, \alpha_n) \\ &= (MM'^{-1}) \cdot V(a\alpha_1 + b, \ldots, a\alpha_n + b) \end{aligned}$$

Observation II

In general, any birational transformation

$$\phi(x) = \frac{ax+b}{cx+d}, \quad ab - cd \neq 0$$

generates a new solution $(M \cdot M_\phi^{-1}, \phi(\alpha_1), \ldots, \phi(\alpha_n)$.

For any $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q^\infty$, there exists ϕ s.t.

$$\phi(\alpha_1) = 1$$
$$\phi(\alpha_2) = 0$$
$$\phi(\alpha_3) = \infty$$

So we search for a specific solution

$$(M, (1, 0, \infty, \alpha_4, \ldots, \alpha_n)), \quad \alpha_i \notin \{0, 1, \infty\} \quad i \geq 4.$$

Step I

Take columns of B indexed by $\{1, n-k+1, \ldots, 2(n-k-1)\}$

$$B = \begin{pmatrix} f^{(1)}(\alpha_1) & \ldots & f^{(1)}(\alpha_{n-k+1}) & \ldots & f^{(1)}(\alpha_{2(n-k-1)}) & \ldots \\ f^{(2)}(\alpha_1) & \ldots & f^{(2)}(\alpha_{n-k+1}) & \ldots & f^{(2)}(\alpha_{2(n-k-1)}) & \ldots \\ \vdots & \ddots & \vdots & \ddots & \ldots & \vdots \\ f^{(n-k)}(\alpha_1) & \ldots & f^{(n-k)}(\alpha_{n-k+1}) & \ldots & f^{(s)}(\alpha_{2(n-k-1)}) & \ldots \end{pmatrix}$$

Find $\mathbf{c}_1 \in \mathbb{F}_q^{n-k}$ from the (left) kernel of these columns:

$$\begin{aligned} \langle \mathbf{c}_1, f^{(i)}(\alpha_1) \rangle &= 0, \\ &\vdots \\ \langle \mathbf{c}_1, f^{(i)}(\alpha_{2(n-k-1)}) \rangle &= 0. \end{aligned}$$

Step I (cont.)

$$\begin{aligned} \langle \mathbf{c}_1, f^{(i)}(\alpha_1) \rangle &= 0, \\ &\vdots \\ \langle \mathbf{c}_1, f^{(i)}(\alpha_{2(n-k-1)}) \rangle &= 0 \end{aligned} \qquad \longrightarrow \qquad F_1(x) := \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(x)$$

Step I (cont.)

$$\begin{matrix} \langle \mathbf{c}_1, f^{(i)}(\alpha_1)\rangle = 0, \\ \vdots \\ \langle \mathbf{c}_1, f^{(i)}(\alpha_{2(n-k-1)})\rangle = 0 \end{matrix} \quad \longrightarrow \quad F_1(x) := \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(x)$$

$F_1(x)$ is 0 in $\{\alpha_1, \alpha_{n-k+1}, \ldots, \alpha_{2(n-k-1)}\}$, so

$$F_1(x) = a_1(x-\alpha_1)(x-\alpha_{n-k+1})\cdots(x-\alpha_{2(n-k-1)})$$

We know a_1, since we know $b_{i,3}$:

$$F_1(\infty) = F_1(\alpha_3) = \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(\alpha_3) = \sum_{i=1}^{n-k} c_{1,i} b_{i,3}.$$

Step I (cont.)

$$\begin{aligned} \langle \mathbf{c}_1, f^{(i)}(\alpha_1)\rangle &= 0, \\ &\vdots \\ \langle \mathbf{c}_1, f^{(i)}(\alpha_{2(n-k-1)})\rangle &= 0 \end{aligned} \qquad \longrightarrow \qquad F_1(x) := \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(x)$$

$F_1(x)$ is 0 in $\{\alpha_1, \alpha_{n-k+1}, \ldots, \alpha_{2(n-k-1)}\}$, so

$$F_1(x) = a_1(x-\alpha_1)(x-\alpha_{n-k+1})\cdots(x-\alpha_{2(n-k-1)})$$

We know a_1, since we know $b_{i,3}$:

$$F_1(\infty) = F_1(\alpha_3) = \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(\alpha_3) = \sum_{i=1}^{n-k} c_{1,i} b_{i,3}.$$

We also know another evaluations of F_1:

$$F_1(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} b_{i,j}.$$

Step I (cont.)

Considered columns of B indexed by $\{1, n-k+1, \ldots, 2(n-k-1)\}$

Step I (cont.)

Consider columns of B indexed by $\{2, n-k+1, \ldots, 2(n-k-1)\}$.

Step I (cont.)

Consider columns of B indexed by $\{2, n-k+1, \ldots, 2(n-k-1)\}$

Do the same, obtain

$$F_2(x) = a_2(x-\alpha_2)(x-\alpha_{n-k+1})\cdots(x-\alpha_{2(n-k-1)}),$$

where the leading coeff. a_2 is again known:

$$F_2(\infty) = F_1(\alpha_2) = \sum_{i=1}^{n-k} c_{2,i} f^{(i)}(\alpha_3) = \sum_{i=1}^{n-k} c_{2,i} b_{i,3}.$$

We also know

$$F_2(\alpha_j) = \sum_{i=1}^{n-k} c_{2,i} f^{(i)}(\alpha_j) = \sum_{i=1}^{n-k} c_{2,i} b_{i,j}.$$

Step I (cont.)

We have

$$F_1(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} b_{i,j}.$$

$$F_2(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(\alpha_j) = \sum_{i=1}^{n-k} c_{2,i} b_{i,j}.$$

For $3 \leq j \leq n-k$, α_j are not the roots of F_1, F_2, hence compute

$$\frac{F_1(\alpha_j)}{F_2(\alpha_j)} = \frac{a_1(\alpha_j - \alpha_1)(\alpha_j - \alpha_{n-k+1}) \cdots (\alpha_j - \alpha_{2(n-k-1)})}{a_2(\alpha_j - \alpha_2)(\alpha_j - \alpha_{n-k+1}) \cdots (\alpha_j - \alpha_{2(n-k-1)})}$$

$$= \frac{a_1(\alpha_j - \alpha_1)}{a_2(\alpha_j - \alpha_2)}$$

Step I (cont.)

We have

$$F_1(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} b_{i,j}.$$

$$F_2(\alpha_j) = \sum_{i=1}^{n-k} c_{1,i} f^{(i)}(\alpha_j) = \sum_{i=1}^{n-k} c_{2,i} b_{i,j}.$$

For $3 \le j \le n-k$, α_j are not the roots of F_1, F_2, hence compute

$$\frac{F_1(\alpha_j)}{F_2(\alpha_j)} = \frac{a_1(\alpha_j - \alpha_1)(\alpha_j - \alpha_{n-k+1}) \cdots (\alpha_j - \alpha_{2(n-k-1)})}{a_2(\alpha_j - \alpha_2)(\alpha_j - \alpha_{n-k+1}) \cdots (\alpha_j - \alpha_{2(n-k-1)})}$$
$$= \frac{a_1(\alpha_j - \alpha_1)}{a_2(\alpha_j - \alpha_2)}$$

From $\alpha_1 = 1, \alpha_2 = 0$:

$$\alpha_j = \frac{a_1/a_2}{a_1/a_2 - F_1(\alpha_j)/F_2(\alpha_j)} \quad 3 \le j \le n-k$$

Step II

We have found $\alpha_4, \ldots, \alpha_{n-k}$.

To find the remaining $\alpha_j, j \geq n-k+1$:

- Consider the columns of B indexed by $\{1, 3, \ldots n-k\}$. Obtain $\mathbf{c}_3$ and F_3 with roots in $\{\alpha_1, \alpha_4, \ldots \alpha_{n-k}\}$.
  ⋆ Root in α_3 means that the coefficient for x^{n-k} is 0, i.e., $\deg F_3 = n-k-1$.
- Consider the columns of B indexed by $\{2, 3 \ldots n-k\}$. Obtain $\mathbf{c}_4$ and F_4 with roots in $\{\alpha_2, \alpha_4, \ldots \alpha_{n-k}\}$, $\deg F_4 = n-k-1$.
- Similar computations lead to

$$\frac{F_3(\alpha_j)}{F_4(\alpha_j)} = \frac{a_3(\alpha_j - \alpha_1)}{a_4(\alpha_j - \alpha_2)} \quad \Longrightarrow \quad \alpha_j = \frac{a_1/a_2}{a_1/a_2 - F_3(\alpha_j)/F_4(\alpha_j)}$$

Step II

We have found $\alpha_4, \dots, \alpha_{n-k}$.

To find the remaining $\alpha_j, j \geq n-k+1$:

- Consider the columns of B indexed by $\{1, 3, \dots n-k\}$. Obtain $\mathbf{c}_3$ and F_3 with roots in $\{\alpha_1, \alpha_4, \dots \alpha_{n-k}\}$.
  ⋆ Root in α_3 means that the coefficient for x^{n-k} is 0, i.e., $\deg F_3 = n-k-1$.
- Consider the columns of B indexed by $\{2, 3 \dots n-k\}$. Obtain $\mathbf{c}_4$ and F_4 with roots in $\{\alpha_2, \alpha_4, \dots \alpha_{n-k}\}$, $\deg F_4 = n-k-1$.
- Similar computations lead to

$$\frac{F_3(\alpha_j)}{F_4(\alpha_j)} = \frac{a_3(\alpha_j - \alpha_1)}{a_4(\alpha_j - \alpha_2)} \implies \alpha_j = \frac{a_1/a_2}{a_1/a_2 - F_3(\alpha_j)/F_4(\alpha_j)}$$

Runtime: $\mathcal{O}(n^3)$.

Part II.II

Sidelnikov-Shestakov: handling $z_i \neq 1$.

Again, many solutions

$$B = M \cdot \begin{pmatrix} z_1 & z_2 & \dots & z_n \\ z_1\alpha_1 & z_2\alpha_2 & \dots & z_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ z_1\alpha_1^{n-k-1} & z_2\alpha^{n-k-1} & \dots & z_n\alpha_n^{n-k-1} \end{pmatrix} = M \cdot V(\alpha_1, \dots, \alpha_n) \cdot Z$$

Observe: multiplying elements of Z by $a \in F_q \setminus \{0\}$ and elements of $V(\alpha_1, \dots, \alpha_n)$ by a^{-1} gives the same B.

Hence, assume $z_1 = 1$.

Again, search for kernel vector

Choose first $n-k+1$ columns of B:

$$B = \begin{pmatrix} z_1 f^{(1)}(\alpha_1) & z_2 f^{(1)}(\alpha_2) & \dots & z_{n-k+1} f^{(1)}(\alpha_{n-k+1}) \\ \vdots & \vdots & \ddots & \vdots \\ z_1 f^{(n-k)}(\alpha_1) & z_{n-k+1} f^{1}(\alpha_2) & \dots & z_{n-k+1} f^{(n-k)}(\alpha_{n-k+1}) \end{pmatrix}$$

Again, search for kernel vector

Choose first $n-k+1$ columns of B:

$$B = \begin{pmatrix} z_1 f^{(1)}(\alpha_1) & z_2 f^{(1)}(\alpha_2) & \ldots & z_{n-k+1} f^{(1)}(\alpha_{n-k+1}) \\ \vdots & \vdots & \ddots & \vdots \\ z_1 f^{(n-k)}(\alpha_1) & z_{n-k+1} f^{1}(\alpha_2) & \ldots & z_{n-k+1} f^{(n-k)}(\alpha_{n-k+1}) \end{pmatrix}$$

Now find $\mathbf{c} \in \mathbb{F}_{n-k+1}$ from the right kernel of these columns:

$$\sum_{j=1}^{n-k+1} c_j z_j f^{(i)}(\alpha_j) = 0 \quad 1 \leq i \leq n-k$$

$$\Longleftrightarrow$$

$$M \cdot V(\alpha_1, \ldots, \alpha_n) \cdot \text{Diag}(\mathbf{c}) \cdot Z = 0$$

$$\Longleftrightarrow \qquad (M \text{ is invertible})$$

$$V(\alpha_1, \ldots, \alpha_n) \cdot \text{Diag}(\mathbf{c}) \cdot Z = 0$$

$\Rightarrow$ system of $n-k$ eqs. with $n-k$ unknowns $\{z_2, \ldots, z_{n-k+1}\}$.

Repeat the process with different columns of B.

Part III

Discussion

Goppa vs. Reed-Solomon

GRS