

Code-Based Cryptography

Error-Correcting Codes and Cryptography

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. Encoding (Linear Transformation)
4. Parity Checking
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. **Reed-Solomon Codes**
8. Goppa Codes
9. McEliece Cryptosystem

Generalized Reed-Solomon codes

→ n, k nonnegative integers such that $1 \leq k \leq n \leq q$.

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i .

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i .

Polynomial Vector
Space:

$$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$$

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i .

Polynomial Vector

Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$
 L_k is a vector space of dimension k over \mathbb{F}_q

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i .

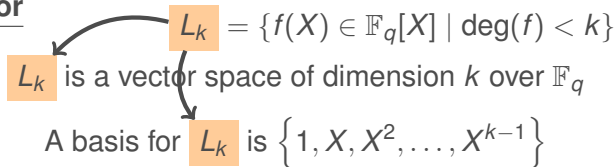
Polynomial Vector

Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$

L_k is a vector space of dimension k over \mathbb{F}_q

A basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$



Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i .

Polynomial Vector

Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$
 L_k is a vector space of dimension k over \mathbb{F}_q
A basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Evaluation
Map:

$$\begin{array}{lll} \text{ev}_{\mathbf{a}, \mathbf{b}} & L_k & \longrightarrow \mathbb{F}_q^n \\ & f(X) & \longmapsto \mathbf{b} * f(\mathbf{a}) \\ & & = (b_1 f(a_1), \dots, b_n f(a_n)) \end{array}$$

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i .

Polynomial Vector

Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$
 L_k is a vector space of dimension k over \mathbb{F}_q
A basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Evaluation
Map:

$$\begin{array}{lll} \text{ev}_{\mathbf{a}, \mathbf{b}} & L_k & \longrightarrow \mathbb{F}_q^n \\ & f(X) & \longmapsto \mathbf{b} * f(\mathbf{a}) \\ & & = (b_1 f(a_1), \dots, b_n f(a_n)) \end{array}$$

The Generalized Reed-Solomon code (GRS)

$$\text{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \text{ev}_{\mathbf{a}, \mathbf{b}}(f) \mid f \in L_k \right\}$$

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. \implies **code locators**
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i .

Polynomial Vector

Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$
 L_k is a vector space of dimension k over \mathbb{F}_q
A basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Evaluation

Map:

$$\begin{array}{lll} \text{ev}_{\mathbf{a}, \mathbf{b}} & L_k & \longrightarrow \mathbb{F}_q^n \\ & f(X) & \longmapsto \mathbf{b} * f(\mathbf{a}) \\ & & = (b_1 f(a_1), \dots, b_n f(a_n)) \end{array}$$

The Generalized Reed-Solomon code (GRS)

$$\text{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \text{ev}_{\mathbf{a}, \mathbf{b}}(f) \mid f \in L_k \right\}$$

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. \implies **code locators**
- $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i . \implies **column multipliers**

Polynomial Vector

Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$
 L_k is a vector space of dimension k over \mathbb{F}_q
A basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Evaluation
Map:

$$\begin{array}{lcl} \text{ev}_{\mathbf{a}, \mathbf{b}} & L_k & \longrightarrow \mathbb{F}_q^n \\ & f(X) & \longmapsto \mathbf{b} * f(\mathbf{a}) \\ & & = (b_1 f(a_1), \dots, b_n f(a_n)) \end{array}$$

The Generalized Reed-Solomon code (GRS)

$$\text{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \text{ev}_{\mathbf{a}, \mathbf{b}}(f) \mid f \in L_k \right\}$$

Parameters of GRS codes

Proposition

The $\text{GRS}_k(\mathbf{a}, \mathbf{b})$ is an $[n, k]_q$ code with minimum distance $d = n - k + 1$

Canonical Generator matrix for GRS

Canonical Generator matrix for GRS

One basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Canonical Generator matrix for GRS

One basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Thus, $\left\{ \text{ev}_{\mathbf{a}, \mathbf{b}}(1), \text{ev}_{\mathbf{a}, \mathbf{b}}(X), \text{ev}_{\mathbf{a}, \mathbf{b}}(X^2), \dots, \text{ev}_{\mathbf{a}, \mathbf{b}}(X^{k-1}) \right\}$ gives a generator matrix for $\text{GRS}_k(\mathbf{a}, \mathbf{b})$

Canonical Generator matrix for GRS

One basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Thus, $\{\text{ev}_{\mathbf{a}, \mathbf{b}}(1), \text{ev}_{\mathbf{a}, \mathbf{b}}(X), \text{ev}_{\mathbf{a}, \mathbf{b}}(X^2), \dots, \text{ev}_{\mathbf{a}, \mathbf{b}}(X^{k-1})\}$ gives a generator matrix for $\text{GRS}_k(\mathbf{a}, \mathbf{b})$

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \dots & a_n^{d-2} \end{pmatrix} \begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix}$$

Canonical Generator matrix for GRS

One basis for L_k is $\{1, X, X^2, \dots, X^{k-1}\}$

Thus, $\{\text{ev}_{\mathbf{a},\mathbf{b}}(1), \text{ev}_{\mathbf{a},\mathbf{b}}(X), \text{ev}_{\mathbf{a},\mathbf{b}}(X^2), \dots, \text{ev}_{\mathbf{a},\mathbf{b}}(X^{k-1})\}$ gives a generator matrix for $\text{GRS}_k(\mathbf{a}, \mathbf{b})$

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \dots & a_n^{d-2} \end{pmatrix} \begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix}$$

$$= \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1 a_1 & b_2 a_2 & \dots & a_n \\ b_1 a_1^2 & b_2 a_2^2 & \dots & b_n a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{d-2} & b_2 a_2^{d-2} & \dots & b_n a_n^{d-2} \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

The dual code of a GRS code

$$\mathcal{C} \text{ is MDS} \iff \mathcal{C}^\perp \text{ is MDS}$$

The dual code of a GRS code

$$\mathcal{C} \text{ is MDS} \iff \mathcal{C}^\perp \text{ is MDS}$$

Proposition

$$\text{GRS}_k(\mathbf{a}, \mathbf{b})^\perp = \text{GRS}_{n-k}(\mathbf{a}, \mathbf{b}')$$

Decoding GRS codes

Let $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{b})$ be an $[n, k, d]_q$ code with parity check matrix:

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \cdots & a_n^{d-2} \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & \cdots & 0 \\ 0 & & \ddots & b_n \end{pmatrix} \in \mathbb{F}_q^{(n-k) \times n}$$

Decoding GRS codes

Let $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{b})$ be an $[n, k, d]_q$ code with parity check matrix:

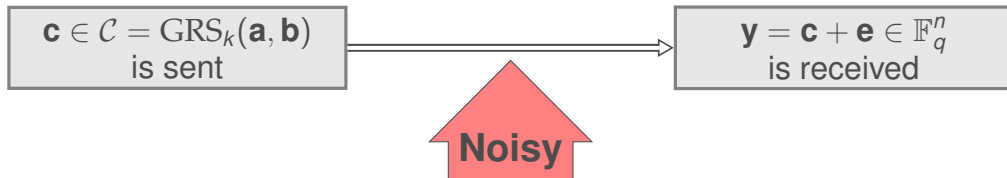
$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \cdots & a_n^{d-2} \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & \cdots & 0 \\ 0 & & \ddots & b_n \end{pmatrix} \in \mathbb{F}_q^{(n-k) \times n}$$

$\mathbf{c} \in \mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{b})$
is sent

Decoding GRS codes

Let $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{b})$ be an $[n, k, d]_q$ code with parity check matrix:

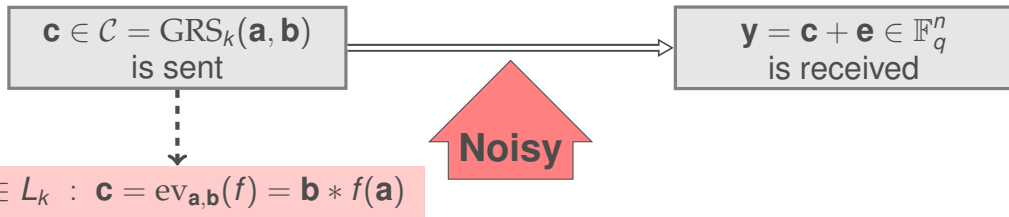
$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \cdots & a_n^{d-2} \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & \cdots & 0 \\ 0 & & \ddots & \\ 0 & & & b_n \end{pmatrix} \in \mathbb{F}_q^{(n-k) \times n}$$



Decoding GRS codes

Let $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{b})$ be an $[n, k, d]_q$ code with parity check matrix:

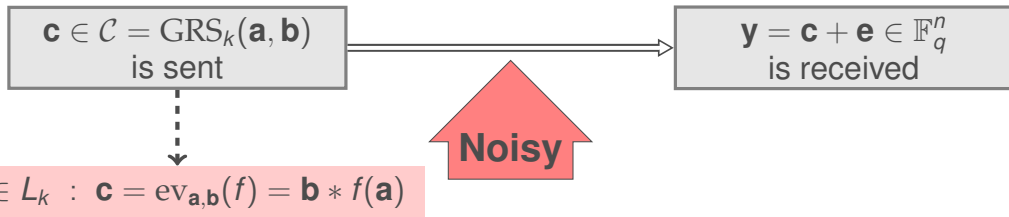
$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \cdots & a_n^{d-2} \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & \cdots & 0 \\ 0 & & \ddots & \\ 0 & & & b_n \end{pmatrix} \in \mathbb{F}_q^{(n-k) \times n}$$



Decoding GRS codes

Let $\mathcal{C} = \text{GRS}_k(\mathbf{a}, \mathbf{b})$ be an $[n, k, d]_q$ code with parity check matrix:

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \cdots & a_n^{d-2} \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & \cdots & 0 \\ 0 & & \ddots & \\ 0 & & & b_n \end{pmatrix} \in \mathbb{F}_q^{(n-k) \times n}$$



Error positions:

$$I = \{i \in \{1, \dots, n\} \mid b_i f(a_i) \neq y_i\} = \{i_1, \dots, i_t\}$$

Decoding GRS codes

We define the polynomial: $E(X) = \prod_{i \in I} (X - a_i)$

Decoding GRS codes

We define the polynomial: $E(X) = \prod_{i \in I} (X - a_i)$

$$E(X)b_i f(a_i) = E(X)y_i \text{ for every } i \in \{1, \dots, n\}$$

Decoding GRS codes

We define the polynomial: $E(X) = \prod_{i \in I} (X - a_i)$

$$E(X)b_i f(a_i) = E(X)y_i \text{ for every } i \in \{1, \dots, n\}$$

→ If $i \in I$, $E(a_i) = 0$

→ Otherwise, $b_i f(a_i) = y_i$

Decoding GRS codes

We define the polynomial: $E(X) = \prod_{i \in I} (X - a_i)$

$E(X)$ is a polynomial of degree t

$$E(X) = X^t + \sum_{i=0}^{t-1} A_i X^i \text{ with } A_i \in \mathbb{F}_q \text{ (unknown)}$$

$$E(X)b_i f(a_i) = E(X)y_i \text{ for every } i \in \{1, \dots, n\}$$

Decoding GRS codes

We define the polynomial: $E(X) = \prod_{i \in I} (X - a_i)$

$E(X)$ is a polynomial of degree t

$$E(X) = X^t + \sum_{i=0}^{t-1} A_i X^i \text{ with } A_i \in \mathbb{F}_q \text{ (unknown)}$$

$$E(X)b_i f(a_i) = E(X)y_i \text{ for every } i \in \{1, \dots, n\}$$

$E(X)f(X)$ is a polynomial of degree $\leq t + (k - 1)$

$$E(X)f(X) = \sum_{i=0}^{t+k-1} B_i X^i \text{ with } B_i \in \mathbb{F}_q \text{ (unknown)}$$

Decoding GRS codes

We define the polynomial: $E(X) = \prod_{i \in I} (X - a_i)$

$E(X)$ is a polynomial of degree t

$$E(X) = X^t + \sum_{i=0}^{t-1} A_i X^i \text{ with } A_i \in \mathbb{F}_q \text{ (unknown)}$$

$$E(X)b_i f(a_i) = E(X)y_i \text{ for every } i \in \{1, \dots, n\}$$

$E(X)f(X)$ is a polynomial of degree $\leq t + (k - 1)$

$$E(X)f(X) = \sum_{i=0}^{t+k-1} B_i X^i \text{ with } B_i \in \mathbb{F}_q \text{ (unknown)}$$

We have a system with:

→ n equations

→ $2t + k$ unknowns

Decoding GRS codes

We define the polynomial: $E(X) = \prod_{i \in I} (X - a_i)$

$E(X)$ is a polynomial of degree t

$$E(X) = X^t + \sum_{i=0}^{t-1} A_i X^i \text{ with } A_i \in \mathbb{F}_q \text{ (unknown)}$$

$$E(X)b_i f(a_i) = E(X)y_i \text{ for every } i \in \{1, \dots, n\}$$

$E(X)f(X)$ is a polynomial of degree $\leq t + (k - 1)$

$$E(X)f(X) = \sum_{i=0}^{t+k-1} B_i X^i \text{ with } B_i \in \mathbb{F}_q \text{ (unknown)}$$

This system has solution if $2t + k < n$

Thus, we can correct up to $t < \frac{n-k}{2} = \frac{d-1}{2}$

We have a system with:

→ n equations

→ $2t + k$ unknowns

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. Encoding (Linear Transformation)
4. Parity Checking
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. **Goppa Codes**
9. McEliece Cryptosystem