*International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137*

*Volume –04, Issue – 11, November 2019, PP – 09-12*

# A symmetric cryptosystem based on Reed-Solomon codes

Carolin Hannusch

*Faculty of Informatics, University of Debrecen (Hungary)*

**Abstract:** We give a method how to construct a binary code from a non-binary Reed-Solomon code and we introduce a cryptosystem based on this code. The invented cryptosystem is symmetric, i.e. its key has to be secret. Only elementary mathematical operations are used, thus computations will be fast.

**Keywords:** symmetric cryptosystem error-correcting codes.

MSC 2010: 94A60 94B50.

## 1 Introduction and Notation

Reed-Solomon codes were introduced in [3]. They are an important class of error-correcting codes and they can be used in different areas of Coding Theory and Cryptography, see for example [4]. Recently, an effective decoding scheme for these codes were developed in [1].

In the current paper, we will construct a binary code from a classical Reed-Solomon code by using binary representation. Further, a cryptographic system based on these binary codes is developed. If the finite field is large enough, then the cryptosystem can be secure. The key has to be kept secret, as well as plaintext - ciphertext pairs, which will be explained in the last section.

First we repeat the definition of a Reed-Solomon code.

**Definition 1** *Let* $GF(q)$ *denote the finite field of* $q$ *elements and let* $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ *be distinct elements of* $GF(q)$. *Then for* $k \leq n$ *the matrix*

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \vdots & & & \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \ldots & \alpha_{n-1}^{k-1} \end{pmatrix}$$

generates a Reed-Solomon code of length $n$, dimension $k$ and minimum distance $n-k+1$.

In the following, we will consider $q$ as a power of $2$. Thus

$$GF(2^\nu) \cong \mathbb{Z}_2/(f(x)),$$

where $f(x)$ is an irreducible monic polynomial of degree $\nu$.

Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be distinct elements of $GF(2^\nu)$. Then there exists a binary representation for $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ as a $\nu$-tuple. Further, let $X = \{\varepsilon^0, \varepsilon^1, \ldots, \varepsilon^{\nu-1}\}$ and let $\sigma$ be an arbitrary permutation in the symmetric group $S_X$. We define a binary representation of the elements of $GF(2^\nu)$ in the following:

$$b : GF(2^\nu) \to \sigma(X)$$

$$b : \alpha_i \mapsto b(\alpha_i) \ \forall i \in \{0, \ldots, n-1\},$$

where $b(\alpha_i)$ is the binary representation of $\alpha_i$ with respect to the permutation $\sigma$.

**Definition 2** *Let* $GF(2^\nu)$ *be a finite field and* $G$ *a generator matrix of an RS-code as in Definition 1. Further let* $b(\alpha_i)$ *be the binary representation of* $\alpha_i$ *. Then the matrix*

  

$$G^{å} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ b(\alpha_0) & b(\alpha_1) & \dots & b(\alpha_{n-1}) \\ \vdots & & & \\ b(\alpha_0^{k-1}) & b(\alpha_1^{k-1}) & \dots & b(\alpha_{n-1}^{k-1}) \end{pmatrix}$$

generates a binary code of length $n \cdot \nu$ and dimension $k$.

**Example 3** *Let* $GF(8) \cong \mathsf{Z}_2/(x^3+x+1) = \{s+t\varepsilon+u\varepsilon^2 \mid s,t,u \in \{0,1\}, \varepsilon^3 = \varepsilon+1\}$ *and* $0,\ 1,\ \varepsilon+1$ *and* $\varepsilon^2$ *be four different elements. Further let* $\sigma_1 = 1_{id}$ *and* $\sigma_2 = (23)$ *be two permutations of* $S_3$. *Then the binary representations of* $0,\ 1,\ \varepsilon+1$ *and* $\varepsilon^2$ *are shown in Table 3.*

Table 1: Binary representation of $0,\ 1,\ \varepsilon+1$ and $\varepsilon^2$

| [10mm] $\alpha_i$ ) | 3em] $b_1(\alpha_i)$ | 3em] $b_2(\alpha_i)$ |
|---|---|---|
| | $\sigma_1 = 1_{id}$ | $\sigma_2 = (23)$ |
| | $\varepsilon^2\,\varepsilon 1$ | $\varepsilon^2 1 \varepsilon$ |
| 0 | 000 | 000 |
| 1 | 001 | 010 |
| $1+\varepsilon$ | 011 | 011 |
| $\varepsilon^2$ | 100 | 100 |
| | | |

We fix $k = 3$. Then we have

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1+\varepsilon & \varepsilon^2 \\ 0 & 1 & 1+\varepsilon^2 & \varepsilon+\varepsilon^2 \end{pmatrix}$$

and by $G$ we get

$$G_1^{å} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

and

$$G_2^{å} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

respectively applying $b_1$ and $b_2$.

**Remark 4** *If the matrix* $G$ *generates an* $(n,k,d)$*- RS-code, then* $G^{å}$ *generates a binary* $(n \cdot \nu, k, d^{å})$ *-code, where* $d^{å} \geq d$.

**Theorem 5** *Let* $C$ *be a binary code generated by a matrix* $G^{å}$ *defined in Definition 2. Then* $C$ *is equivalent to all binary codes generated by matrices of type* $G^{å}$ *over the same field independent from the choice of the permutation* $\sigma$.

  

*Proof.* Let $G_1$ be constructed using $\sigma_1$ and $G_2$ be constructed using $\sigma_2$. The generated codes $C_1$ and $C_2$ are equivalent iff there exists a permutation $\tau$ on the coordinates of $C_1$, such that $\tau(C_1) = C_2$. Since $\sigma_1, \sigma_2 \in S_X$ and $S_X$ is a group, there exists an element $\sigma^{å} \in S_X$, such that $\sigma_1 \cdot \sigma^{å} = \sigma_2$. With the choice $\tau = \sigma^{å}$ we get that $C_1$ and $C_2$ are equivalent.

## 2 Encryption

The key of the cryptosystem is

**Key:** $(f(x), \sigma, k, \alpha = [\alpha_0, \alpha_1, \ldots, \alpha_{n-1}])$

Knowing the key, we can generate the matrix $G$ by Definition 2. Let $m = (m_0, \ldots, m_{k-1})$ be a message. Then we encrypt the message $m$ in the following way:

$$c = m \cdot G^{å}.$$

## 3 Decryption

Suppose we received the encrypted message with an error:

$$v = c + e.$$

We know the key, thus we obtain $v$ from $f(x)$. Therefore we can detect wrong $v$-tuples. We know the binary representation of elements of the finite field by the permutation $\sigma$. Thus we can write back $v$ into an $n$-tuple with elements of $GF(2^v)$:

$$v' = (a_0, a_1, \ldots, a_{n-1}).$$

Then we solve the linear equation system $v' = m \cdot G$, which means

$$(a_0, \ldots, a_{n-1}) = (m_0, \ldots, m_{k-1}) \cdot G \tag{1}$$

If an equation cannot be solved, then the block corresponding to $a_i$ is not correct,i.e. the encoded message contains at least one error.

**Error detection and correction**

If

$$a_i = m_0 \cdot g_{i,1} + m_1 g_{i,2} + \ldots + m_{k-1} \cdot g_{i,k-1}$$

is not solvable, then $b(a_i)$ is not correct in $v$.

Thus

$$w(e) \geq |\#| \{ i \mid a_i = m_0 \cdot g_{i,1} + m_1 g_{i,2} + \ldots + m_{k-1} \cdot g_{i,k-1} \text{ has no solution } \}.$$

By (1) we have $n$ equations and $k$ unknown variables (which are the coordinates of the message). The system can be solved if $k$ equals the number of solvable equations. Thus we are able to correct $n-k$ wrong blocks, which implies that $(n-k)v$ errors can be corrected.

The message can be recovered by the solution we find for the system of equations consisting of all solvable equations of (1).

## 4 Security of the key

The security of this cryptosystem relies on the secret key. The key actually itself can be chosen from $M_v(2)$ polynomials (where $M_v(2)$ denotes the number of monic irreducible polynomials of degree $v$ over $GF(2)$), $S_v$ permutations, and the elements $\alpha_0, \ldots, \alpha_{n-1}$ can be freely chosen from the field $GF(2^v)$. If we choose $v = 64$ and $1 \leq n < 2^{64}$, then the number of possible keys will be

  

$$\frac{1}{64}(2^{64}-2^{32})\cdot\nu!\left(\begin{matrix}2^{\nu}\\ n\end{matrix}\right)?10^{125}.$$

## References

[1]. Gao, Xin. "An iterative decoding scheme on random burst error correction with Reed-Solomon codes." International Journal of Information and Coding Theory 5.2: 117-129. (2018)

[2]. McEliece, R. J., Sarwate, D. V. "On sharing secrets and Reed-Solomon codes." Communications of the ACM, 24(9), 583-584. (1981)

[3]. Reed, I. S.; Solomon, G. "Polynomial codes over certain finite fields." Journal of the society for industrial and applied mathematics, 8(2), 300-304. (1960)

[4]. Wicker, S. B., Bhargava, V. K. (Eds.). "Reed-Solomon codes and their applications." John Wiley and Sons. (1999)

  