Quantum resistant code-based cryptosystems: the McEliece cryptosystem and its variants

Jon-Lark Kim

Sogang University, South Korea

March 1, 2019

At Crypto seminar, Univ. of California-Irvine

Abstract: The McEliece cryptosystem is the first code-based public key cryptosystem proposed by Robert McEliece in 1978 a few years after the appearance of RSA. The original McEliece cryptosystem uses binary Goppa codes which are a subclass of Algebraic Geometric Codes and it is still unbroken under quantum attack. In this talk, we introduce basic facts about coding theory and discuss various code-based public key cryptosystems including our new cryptosystem McNie, which is a combination of the McEliece cryptosystem and the Niederreiter cryptosystem.

1. Introduction to Coding Theory

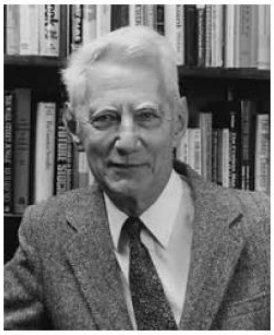
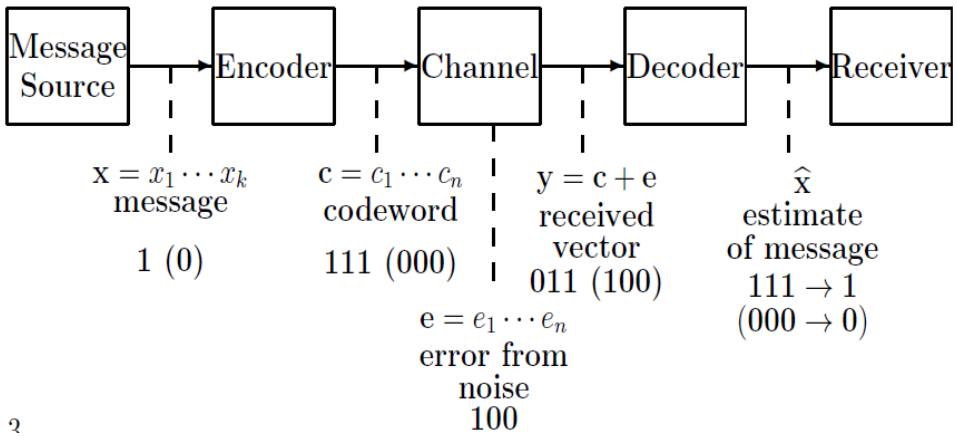


Figure: Claude Shannon (1916-2001)

Shannon's two foundational papers from Bell System Technical Journal:
"A Mathematical Theory of Communication" on Information Theory (1948)
"Communication Theory of Secrecy Systems" on Cryptography (1949)

Shannon(Ph.D. in Math) tried to understand both coding and cryptography from

information theory point of view. In particular, the concept of Information **Entropy** is due to him. Shannon's communication channel is given below. Main idea is to add redundant bits to message so that whenever there is an error in the coded message(i.e. codeword) we can find an error position in the codeword and correct it.



Shannon's work on information theory is motivated by Richard Hamming(Ph.D. in Math), a colleague at Bell Lab. Hamming found the first nontrivial one error correcting codes. Shannon showed that there exist codes which can correct any number of errors keeping the information rate below the channel capacity.

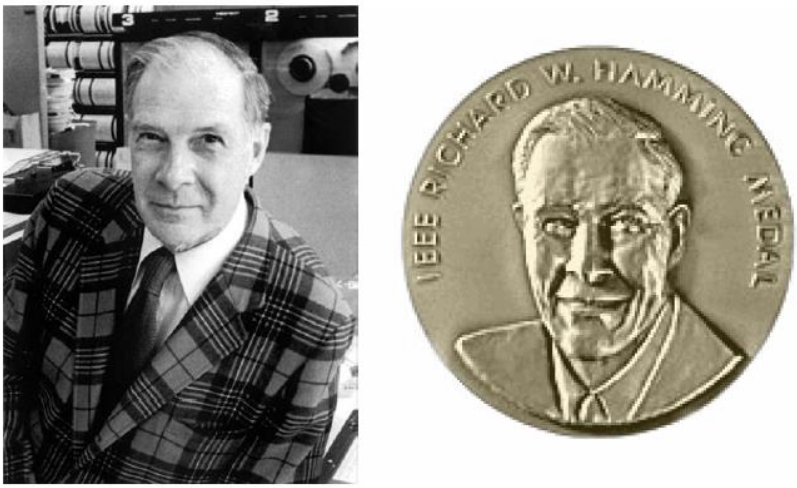


Figure: Richard Hamming (1915-1998, Bell Lab)

From now on we give some basic concepts from coding theory.

- A linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{Z}_p$:= a k-dimensional subspace of $\mathbb{Z}_p^n$.
- We denote $\mathcal{C}$ by an $[n, k]$ linear code over $\mathbb{Z}_p$.
- The minimum distance (weight) d of a linear code $\mathcal{C}$:=the minimum of wt($\mathbf{x}$), $\mathbf{x} \neq \mathbf{0} \in \mathcal{C}$.
- We denote it by an $[n, k, d]$ code. Given n and k, d can be at most $n - k + 1$ (Singleton' bound).
- A linear *[n,k,d]* code with *d=n-k+1* is **called an MDS code.**

Theorem

Any $[n, k, d]$ linear code can correct up to $t = \lfloor \frac{d-1}{2} \rfloor$ errors (by the nearest neighbor decoding).

- For $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$ in $\mathbb{Z}_p^n$, the dot product of $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n.$$

- The dual of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is $\mathcal{C}^\perp = \{\mathbf{y} \in \mathbb{Z}_p^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{x} \in \mathcal{C}\}$

- Let $\mathcal{C}$ be an $[n, k, d]$ code.
- Let G be a $k \times n$ generator matrix.
- Let $\mathbf{x}$ be a row vector of length k.
- Then the following mapping is an encoding processor:

$$\mathbf{x} \to \mathbf{x}G$$

- Note that length k vector $\mathbf{x}$ is mapped to a vector of larger length n. So encoding is a process to add redundancy bits (digits) to original message.
- For example, recall that $\mathcal{C}_1$ has $G = [111]$, $0 \to 0[111] = (000)$ and $1 \to 1[111] = (111)$

- To simplify, we describe how to decode $\mathcal{C}_1$.
- Recall that $\mathcal{C}_2$ is the dual of $\mathcal{C}_1$ and $\mathcal{C}_2$ has a generator matrix

$$G_2 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

- G_2 is also called a parity check matrix of $\mathcal{C}_1$.
- Let $H_1 = G_2$.

- Suppose $\mathbf{y} = (110)$ was received using $G_1 = [111]$.
- Compute the syndrome $H_1\mathbf{y}^T$ of $\mathbf{y}$ using H_1 as follows:

$$\begin{aligned} H_1\mathbf{y}^T &= \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \text{(error occurred. Why?)} \end{aligned}$$

- Note $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is the third column of H_1. Then there is an error in the third position of $\mathbf{y} = (110)$. Decode $\mathbf{y}$ as
- **y=(1 1 0)** $\rightarrow \mathbf{x} := \mathbf{y} - (001) = (111) \in \mathcal{C}_1$.

2. Quantum-Resistant Cryptography

Peter Shor(now at Applied Math Dept at MIT)

- Quantum algorithm solves factorization and discrete log problem in polynomial time.
- If a quantum computer is built, RSA and Elliptic curve cryptosystem will be broken.
- NIST calls for the 1st round competition of Post-Quantum Cryptography due Nov. 2018.

Post-Quantum Cryptography(PQC)

Lattice-based cryptography	•based on the NP-hardness of closest vector problem w.r.t. Euclidean metric on R^n •relevant to encryption and signature schemes
Code-based cryptography	•based on the NP-completeness of syndrome decoding w.r.t. Hamming metric(classical) and rank metric(new) on $\mathrm{GF}(q)^n$ •relevant for encryption schemes
Multivariate polynomial cryptography	•based on multivariate polynomials over finite fields •relevant for signature schemes
Hash-based signatures	•relevant for signature schemes

* Recently, supersingular elliptic curve isogeny cryptography was introduced for signature.

There is an analogue between lattice based cryptography and code-based cryptography as follows.

Lattice based crypto	Code based crypto
$\boldsymbol{R^n}$	$\boldsymbol{GF(q)^n}$
Lattice	Linear code(=a subspace of $\boldsymbol{GF(q)^n}$)
Euclidean distance	Hamming/rank distance
Theta series	Weight enumerator
Gosset/ Leech lattice	Hamming/Golay code
Mathieu groups	Conway Simple groups
SVP, CVP	minimum distance, SDP
Ideal lattice	Cyclic codes
LWE(or LNP) public key(A, b=As+e)	Enc(m)= mG' + e where G'=MGP
Sparse matrix	Low Density Parity Check Code

3. More on Code-Based Cryptography

- **McEliece (1978)**
  The first public key cryptosystem using error correcting codes (Goppa codes)
- **No efficient structural attacks that might distinguish between a permuted Goppa code used by McEliece and a random code**
- **Parameters of binary Goppa codes: $[n = 2^m, k, 2t + 1]$ where $t = \frac{n-k}{m}$**
- **Original parameters: $n = 1024,\ k = 524,\ t = 50$**
  resulting in over 100k bits of public keysizes
- **Goppa code-based McEliece crypto with parameters *n=4096, k=3844, t=21***
  giving 121086 bytes at the security level of 128 bits is still unbroken!
- **Due to large keysizes, no practical application of code-based cryptography so far**

Formal definition of Goppa codes

The Goppa code $\Gamma(L, g(z))$ is defined by the Goppa polynomial $g(z)$, which is a polynomial of degree t over the extension field $GF(q^m)$, for q a prime, and an accessory subset L of $GF(q^m)$.

$$\begin{aligned} g(z) &= g_0 + g_1 z + \ldots + g_t z^t = \sum_{i=0}^{t} g_i z^i, \\ L &= \{\alpha_1, \ldots, \alpha_n\} \subseteq GF(q^m), \end{aligned}$$

such that $g(\alpha_i) \neq 0$ for all $\alpha_i \in L$. With a vector $c = (c_1, \ldots, c_n)$ over $GF(q)$ we associate the function

$$R_c(z) = \sum_{i=1}^{n} \frac{c_i}{z - \alpha_i}, \tag{1}$$

in which $\frac{1}{z-\alpha_i}$ is the unique polynomial with $(z - \alpha_i) \cdot \frac{1}{z-\alpha_i} \equiv 1 \pmod{g(z)}$.

Definition 2.1 *The Goppa code $\Gamma(L, g(z))$ consists of all vectors c such that*

$$R_c(z) \equiv 0 \pmod{g(z)}. \tag{2}$$

Goppa codes are a special subclass of generalized Reed-Solomon codes.

For some polynomial $f(z) \in \mathbb{F}_{p^m}[z]_{<k}$, pairwise distinct elements $\mathcal{L} = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_{p^m}^n$, non-zero elements $V = (v_0, \ldots, v_{n-1}) \in \mathbb{F}_{p^m}^n$ and $0 \leq k \leq n$, GRS code can be defined as

$$GRS_{n,k}(\mathcal{L}, V) := \{\, c \in \mathbb{F}_{p^m}^n | c_i = v_i f(\alpha_i) \} \tag{3.2}$$

Alternant codes are subfield subcodes of a GRS codes, i.e. they can be obtained by restricting GRS-codes to the subfield $\mathbb{F}_p$:

$$Alt_{n,k,p}(\mathcal{L}, v) := GRS_{n,k}(\mathcal{L}, V) \cap \mathbb{F}_p^n \tag{3.3}$$

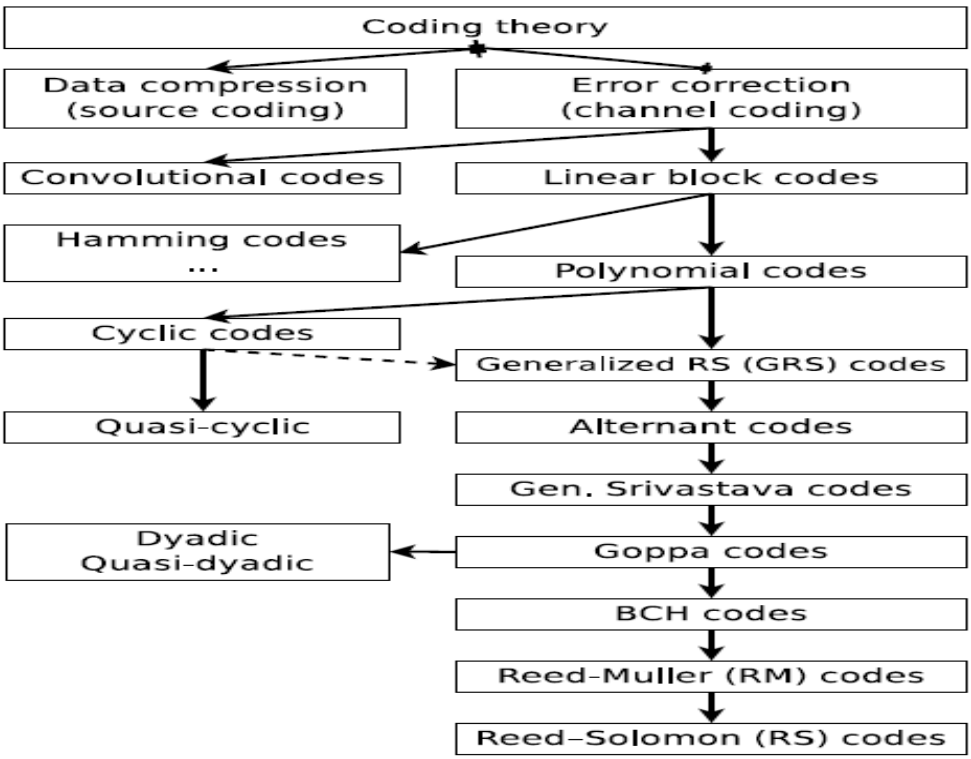


Figure 3.1: Hierarchy of code classes

- Definition: (Binary Syndrome Decoding (SD) problem; SDP)
  - **Input**: An $r \times n$ matrix H over F_2, a target binary vector $s \in F_2^r$, and an integer $t > 0$.
  - **Question**: Is there a binary word $x \in F_2^n$ of weight $\leq t$, such that $s = Hx^T$?
  - E. Berlekamp, R. McEliece, H. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inf. Theory*, 24(3), pp. 384–386, 1978

- Definition: (q-ary Syndrome Decoding (q-SD) problem)
  - **Input**: An $r \times n$ matrix H over F_q, a target vector $s \in F_q^r$, and an integer $t > 0$.
  - **Question**: Is there a word $x \in F_q^n$ of weight $\leq t$, such that $s = Hx^T$?

- McEliece's vs. Neiderreiter's Scheme
  - F_2: the field with two elements
  - $\boldsymbol{C}$: a binary code of length n and dimension k
  - G: $k \times n$ generating matrix
  - H: $(n–k) \times n$ parity check matrix, $GH^T = 0$
  - $s = Hc^T$: syndrome

McEliece and Niederreiter cryptosystems turn out to be equivalent.

	McEliece	Niederreiter
Public key	G	H
Plaintext	$x \in F_2^k$	$x \in F_2^n$, $w_H(x) = t$
Ciphertext	$y = xG + e$, $w_H(e) = t$	$y = Hx^T$
Ciphertext space	F_2^n	F_2^{n-k}
Used codes	*binary Goppa codes*	*generalized Reed-Solomon codes*

4. Results on McNie

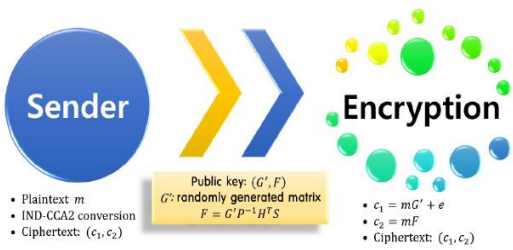
McNie is a new code-based cryptography introduced by Jon-Lark Kim's team consisting of Y.-S. Kim, L. Galvez, M. J. Kim, and N. Lee.

- Our McNie is a new code-based public key cryptosystem which is less vulnerable against currently known structural attacks.
- McNie is one of the 64 algorithms which passed round 1 of 2017 NIST Competition for Post-Quantum Cryptography.
- McNie can use Hamming weight or rank weight in general.
- Consider Hamming weight or rank weight.
- **Secret key:** (H, P, S, Φ_H)
  H: a parity check matrix for an $[n, k]$ code C over $\mathbb{F}_{q^m}$
  P: an $n \times n$ permutation matrix
  S: an $(n-k) \times (n-k)$ invertible matrix over $\mathbb{F}_{q^m}$
  Φ_H: an efficient decoding algorithm for C which corrects errors of weight up to r
- **Public key:** (G', F)
  G': Generator matrix for a random $[n, l]$ code over $\mathbb{F}_{q^m}$
  $F = G'P^{-1}H^TS$

<u>Encryption</u>

Message: $\mathbf{m} \in \mathbb{F}_{q^m}^l$

- Randomly generate $\mathbf{e} \in \mathbb{F}_{q^m}^n$ of weight r
- $Enc(\mathbf{m}) = (\mathbf{c_1}, \mathbf{c_2})$
  $\mathbf{c_1} = \mathbf{m}G' + \mathbf{e}$
  $\mathbf{c_2} = \mathbf{m}F = \mathbf{m}G'P^{-1}H^TS$

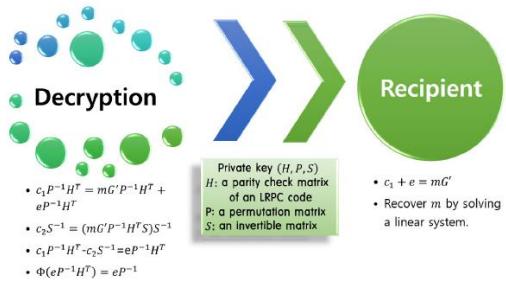


Decryption

Received vector: $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2})$

- Compute

$$
\begin{aligned}
\mathbf{s}' &= \mathbf{c_1} P^{-1} H^T - \mathbf{c_2} S^{-1} \\
&= (\mathbf{m} G' + \mathbf{e}) P^{-1} H^T \\
&\quad -(\mathbf{m} G' P^{-1} H^T S) S^{-1} \\
&= \mathbf{e} P^{-1} H^T \\
\mathbf{e}' &= \Phi_H(\mathbf{s}') = \mathbf{e} P^{-1} \\
\mathbf{e} &= \mathbf{e}' P
\end{aligned}
$$



- Solve the system

$$\mathbf{m} G' = \mathbf{c_1} - \mathbf{e}$$

to recover $\mathbf{m}$.

We applied this algorithm to 3-quasi and 4-quasi cyclic LRPC codes to get the following result.

n	l	k	d	r	m	q	failure	Key Size (bytes)	security
120	80	80	3	8	53	2	-23	795	128
138	92	92	3	10	67	2	-25	1156	192
156	104	104	3	12	71	2	-27	1385	256

Table: New suggested parameters for McNie using 3-quasi-cyclic LRPC code

n	l	k	d	r	m	q	failure	Key Size (bytes)	security
92	46	69	3	10	59	2	-36	849	128
112	56	84	3	13	67	2	-38	1173	192
128	64	96	3	16	73	2	-36	1460	256

Table: New suggested parameters for McNie using 4-quasi-cyclic LRPC code

We have applied a modified McNie to Gabidulin codes and polar codes to get meaningful results (omitted).