# EC500

## Design of Secure and Reliable Hardware

Lecture 16 – Robust Codes (Weak Attacks)

Mark Karpovsky

# 1 Motivation & Characteristics of Linear Codes

Linear codes are designed for specific error models. For example, let us denote $\|e\|$ as the total number of 1's in the error vector. A **1-d parity code** is capable of detecting all errors $e$, where $\|e\|$ is odd. An **extended Hamming code** can correct all single errors and detect all triple errors. But, what if we are using a **1-d parity code** and $\|e\|$ is even? Or if for an **extended Hamming code**, how do we detect an error with $\|e\| > 3$?

## 1.1 Inherent Weakness of Linear Codes

For a linear code, there is always a large number of undetectable errors and a large number of miscorrected errors. This is the case if the error model or the bit error rate is hard to predict or nonstationary. For example, consider fault injection attacks, what happens if the error repeats? Here, we say an error $e$ is not detected iff $He = 0$ where $H$ is the check matrix of the code. It is actually very easy to generate undetectable errors for linear codes (e.g. choose any valid codeword as the error).

# 2 Robust Codes and Their Variations

## 2.1 Definitions

We define the **detection kernel** of a code $C$ as $K_d = \{e|e \oplus c \in C, \forall c \in C\}$. For linear codes, the detection kernel $|K_d| = 2^k = |C|$ because the sum of any two valid codewords is another valid codeword. For a **robust code**, $|K_d| = 1 = |\{0\}|$, meaning that no errors will be undetected for all codewords of a robust code $C$. We also define a **partially robust code** when $1 < |K_d| < 2^k$.

## 2.2 Characteristics of Robust Codes

First, we will define the **error masking probability** as $Q(e) = \frac{|\{c|c \oplus e \in C\}|}{|C|}$ and the worst case error masking probability is $\max_{e \neq 0} Q(e)$. An optimal robust code minimizes $Q(e)$ given all other parameters. For a linear code, $\max_{e \neq 0} Q(e) = 1$, for a robust code, $\max_{e \neq 0} Q(e) \ll 1$, and for a minimum distance robust code $\max_{e \neq 0} Q(e) \ll 1$ and $\max_{e \neq 0} Q(e) = 0$ for $\|e\| < d$.

## 2.3 Examples

1) Consider a (3,2) linear 1-d parity code: $\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}$

2) Consider a (3,2) robust parity code: $\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}$

For the above two codes? What is $Q(e)$ and $K_d$ if $e = (0 \quad 1 \quad 1)$? Also, what is the error masking probability for this error?

## 2.4 Error Masking Equations (EME) for Robust Codes

Consider a robust code of the form $C = \{(x, f(x))\}$ where $x \in GF(q^k)$ and $f(x) \in GF(q^r)$. If an error is injected of the form $e = (e_x, e_f)$ where $e_x \in GF(q^k)$ and $e_f \in GF(q^r)$. ($q$ is a power of a prime number). We drive the **error masking equation** (EME) to be $f(x \oplus e_x) \oplus e_f = f(x)$ and the number of solutions for $x$ in the EME divided by $q^k$ is the error masking probability $Q(e)$ for this code $C$. We assume that all messages $x \in q^k$ are equiprobable.

## 2.5 Quadratic Codes (binary and q-ary)

Suppose a **quadratic code** has the form $C = \{(x, f(x))\}$ where $x \in GF(q^{64})$ and $f(x) \in GF(q^8)$. We can consider $x$ as $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ where $x_i \in GF(2^8)$ and now we can construct our $f(x) = x_1 \cdot x_2 \oplus x_3 \cdot x_4 \oplus x_5 \cdot x_6 \oplus x_7 \cdot x_8$. There is a special case when $x_i \in GF(2)$ which we call **robust parity**.

### 2.5.1 Examples

We take a code of the form $C = \{(x, f(x))\}$ where $x = (x_1, x_2, x_3, x_4)$ and $x_i \in GF(2^3)$. Let $f(x) = x_1 \cdot x_2 \oplus x_3 \cdot x_4$, what is $f(x)$ when $x = (010,100,001,111)$? What is the error masking equation? For this $x$, if the error is $e_x = (100,100,000,000)$, and $e_f = 000$, will this error be detected?

| | | | |
|---|---|---|---|
| 0 | 0 | 0 | $0$ |
| 1 | 0 | 0 | $1$ |
| 0 | 1 | 0 | $\alpha$ |
| 0 | 0 | 1 | $\alpha^2$ |
| 1 | 1 | 0 | $\alpha^3$ |
| 0 | 1 | 1 | $\alpha^4$ |
| 1 | 1 | 1 | $\alpha^5$ |
| 1 | 0 | 1 | $\alpha^6$ |
| $1$ | $\alpha$ | $\alpha^2$ | |

## 2.6 EME and Q(e) for Quadratic Codes

Let $x = (x_1, x_2, \cdots, x_{2s-1}, x_{2s})$, $x_i \in GF(q^r)$ and $f(x) = x_1 \cdot x_2 \oplus x_3 \cdot x_4 \oplus \cdots \oplus x_{2s-1} \cdot x_{2s}$ (Non-repetitive Quadratic form). Suppose there is an error $e = (e_1, e_2, \cdots, e_{2s-1}, e_{2s}, e_f)$ and $e_i, e_f \in GF(q^r)$. The error masking equation here is $(x_1 \oplus e_1)(x_2 \oplus e_2) \oplus (x_3 \oplus e_3)(x_4 \oplus e_4) \oplus \cdots \oplus (x_{2s-1} \oplus e_{2s-1})(x_{2s} \oplus e_{2s}) \oplus e_f = x_1 \cdot x_2 \oplus x_3 \cdot x_4 \oplus \cdots \oplus x_{2s-1} \cdot x_{2s}$. Let $e_1 \neq 0$, if we select $x_1, x_3, \cdots, x_{2s-1}, x_{2s}$, there are a total of $q^{r(2s-1)}$ ways to make this selection. Then, we have the following <u>linear</u> equation for $x_2 \to e_1 x_2 = A$, where $A \in GF(q^r)$ is the sum of all the other terms. Thus, for any $e$, $Q(e) \le \frac{q^{r(2s-1)}}{|C|} = \frac{q^{r(2s-1)}}{|q^{r2s}|} = q^{-r}$.

## 2.7 Robust Duplication Codes and Partially Robust Codes (r=k)

For **binary case**:

$C = \{(x, f(x) = x^3)\}$, $x \in GF(2^{32})$, and $f(x) \in GF(2^{32})$

→ $\dim K_{d_{e \neq 0}} = 0$, $\max Q(e) = 2^{-r+1} = 2^{-31}$

This is an alternative to linear duplication codes.

$C = \{(x, f(x) = (Px)^3)\}$, $x \in GF(2^{32})$, and $f(x) \in GF(2^6)$

→ $\dim K_d = k - r = 26$, $\max_{e \notin K_d} Q(e) = 2^{-r+1} = 2^{-5}$

This is a **partially robust code**.

For **non-binary case** $q > 2$:

$C = \{(x, f(x) = x^2)\} \rightarrow \max_{e \neq 0} Q(e) = q^{-r}$

### 2.7.1 EME for Robust Duplication Codes (r=k)

For binary, let $f(x) = x^3$, $e = (e_x, e_f)$ where $e_x, e_f \in GF(2^k)$. The error masking equation is $(x \oplus e_x)^3 \oplus e_f = x^3$ which can be simplified to $e_x x^3 \oplus {e_x}^2 x \oplus {e_x}^3 \oplus e_f = 0$. If $e_x \neq 0$, there are at most 2 solutions for $x$. Thus, $Q(e) \leq \frac{2}{2^k} = 2^{-r+1}$ $(r = k)$ for any $e$.

For $q$-ary, let $f(x) = x^2$, $e = (e_x, e_f)$ where $e_x, e_f \in GF(q^k)$. The error masking equation is $(x \oplus e_x)^2 \oplus e_f = x^2$ which simplifies to $2e_x x + {e_x}^2 + e_f = 0$. Thus there is at most one solution for the error masking equation for $x$ and so $Q(e) \leq \frac{1}{q^k} = q^{-r}$.