LCD codes from Cartesian codes

Hiram H. López, Felice Manganiello, Gretchen Matthews

Clemson University

The Sixth Code-Based Cryptography Workshop
April 5-6, 2018
Florida Atlantic University
Davie, Florida.
Linear codes

Let $K := \mathbb{F}_q$ be a finite field and $n \in \mathbb{Z}^+$. An $[n, k, d]$ code $C$ over $K$ is a $k$-dimensional subspace of $K^n$ with

$$d = \min\{|i : c_i \neq c_i'| : c, c' \in C, c \neq c'\}.$$ 

Elements of $C$ are called codewords; $d$ is the minimum distance of $C$. 

Hiram H. López

LCD codes from Cartesian codes
Linear codes

Let $K := \mathbb{F}_q$ be a finite field and $n \in \mathbb{Z}^+$. An $[n, k, d]$ code $C$ over $K$ is a $k$-dimensional subspace of $K^n$ with

$$d = \min \{ |\{ i : c_i \neq c'_i \}| : c, c' \in C, c \neq c' \}.$$ 

Elements of $C$ are called codewords; $d$ is the minimum distance of $C$.

The dual of $C$ is

$$C^\perp := \{ w \in K^n : w \cdot c = 0 \ \forall c \in C \}.$$ 

A generator matrix for $C$ is a matrix $G \in K^{k \times n}$ whose rows form a basis for $C$. 

Hiram H. López
LCD codes from Cartesian codes
Linear codes
Let $K := \mathbb{F}_q$ be a finite field and $n \in \mathbb{Z}^+$. An $[n, k, d]$ code $C$ over $K$ is a $k$-dimensional subspace of $K^n$ with

$$d = \min\{|\{i : c_i \neq c'_i\}| : c, c' \in C, c \neq c'\}.$$

Elements of $C$ are called codewords; $d$ is the minimum distance of $C$.

The dual of $C$ is

$$C^\perp := \{w \in K^n : w \cdot c = 0 \ \forall c \in C\}.$$

A generator matrix for $C$ is a matrix $G \in K^{k \times n}$ whose rows form a basis for $C$. A parity-check matrix for $C$ is a matrix $H \in K^{(n-k) \times n}$ such that for all $c \in C$,

$$Hc^T = 0.$$
Linear codes

Let $K := \mathbb{F}_q$ be a finite field and $n \in \mathbb{Z}^+$. An $[n, k, d]$ code $C$ over $K$ is a $k$-dimensional subspace of $K^n$ with

$$d = \min\{|\{i : c_i \neq c'_i\}| : c, c' \in C, c \neq c'\}.$$ 

Elements of $C$ are called codewords; $d$ is the minimum distance of $C$.

The dual of $C$ is

$$C^\perp := \{w \in K^n : w \cdot c = 0 \ \forall c \in C\}.$$ 

A generator matrix for $C$ is a matrix $G \in K^{k \times n}$ whose rows form a basis for $C$. A parity-check matrix for $C$ is a matrix $H \in K^{(n-k) \times n}$ such that for all $c \in C$,

$$Hc^T = 0.$$ 

Note that $GH^T = 0$. 

Linear complementary dual (LCD) codes

A linear code $C$ is a linear complementary dual code if and only if

$$C \cap C^\perp = \{0\}.$$
A linear code $C$ is a linear complementary dual code if and only if

$$C \cap C^\perp = \{0\}.$$ 

If $C \subseteq K^n$ is an LCD code, then

$$C \oplus C^\perp = K^n.$$
Linear complementary dual (LCD) codes

A linear code $C$ is a linear complementary dual code if and only if

$$C \cap C^\perp = \{0\}.$$ 

If $C \subseteq K^n$ is an LCD code, then

$$C \oplus C^\perp = K^n.$$ 

**Proposition (Massey, 1992)**

If $C$ is a code with generator matrix $G$ and parity-check matrix $H$, then the following are equivalent:

1. $C$ is LCD.
2. $GG^T$ is nonsingular.
3. $HH^T$ is nonsingular.
Good LCD codes can provide countermeasures to side-channel attacks (SCAs).

Assume $C$ is an LCD with generator matrix $G$ and parity-check matrix $H$. Suppose $z$ is a masked element. Since $C \oplus C^\perp = K^n$, $\exists (x, y) \in K^k \times K^{n-k}$ with

$$z = xG + yH.$$ 

Then

$$zG^T(GG^T)^{-1} = xGG^T(GG^T)^{-1} + yHG^T(GG^T)^{-1} = x.$$ 

and

$$zH^T(HH^T)^{-1} = xGH^T(HH^T)^{-1} + yHH^T(HH^T)^{-1} = y.$$ 

According to Carlet and Guilley (2015), the countermeasure is $(d - 1)^{th}$ degree secure where $d$ is the minimum distance of $C$, and the greater the degree of the countermeasure, the harder it is to pass a successful SCA.
Good LCD codes can provide countermeasures to fault-injection attacks.

Suppose $z$ is modified into $z + \epsilon$ where $\epsilon \in K^n$. Then $\epsilon = eG + fH$ for some $(e, f) \in K^k \times K^{n-k}$. Detection amounts to distinguishing $z$ from $z + \epsilon$. We have that

$$z + \epsilon = (x + e)G + (y + f)H.$$ 

Then

$$(z + \epsilon)H^T(HH^T)^{-1} = (x + e)GH^T(HH^T)^{-1} + (y + f)HH^T(HH^T)^{-1} = y + f.$$ 

Notice that $z + \epsilon = y$ if and only if $f = 0$ if and only if $\epsilon \in C$. Thus, fault not detected if $\epsilon \in C$. If $wt(\epsilon) < d(C)$, then fault is detected. This demonstrates why we want $d(C)$ large.
Affine Cartesian codes.

Let $A_1, \ldots, A_m$ be a collection of non-empty subsets of $K$. Define the Cartesian product set

$$\mathcal{A} := A_1 \times \cdots \times A_m \subset K^m.$$
Affine Cartesian codes.

Let $A_1, \ldots, A_m$ be a collection of non-empty subsets of $K$. Define the Cartesian product set

$$A := A_1 \times \cdots \times A_m \subset K^m.$$ 

Assume $A = \{a_1, \ldots, a_n\}$. Take and fix $n$ non-zero elements $v_{a_1}, \ldots, v_{a_n}$ of the field $K$ and define $v := (v_{a_1}, \ldots, v_{a_n})$.

The evaluation map

$$\text{ev}_k : K[X_1, \ldots, X_m]_{<k} \rightarrow K^{|A|},$$

$$f \mapsto (v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)),$$

defines a linear map of $K$-vector spaces. The image of $\text{ev}_k$, denoted by $C_k(A, v)$, defines a linear code.
Affine Cartesian codes.

Let $A_1, \ldots, A_m$ be a collection of non-empty subsets of $K$. Define the 
Cartesian product set

$$\mathcal{A} := A_1 \times \cdots \times A_m \subset K^m.$$ 

Assume $\mathcal{A} = \{a_1, \ldots, a_n\}$. Take and fix $n$ non-zero elements $v_{a_1}, \ldots, v_{a_n}$ of the field $K$ and define $v := (v_{a_1}, \ldots, v_{a_n})$.

The evaluation map

$$\text{ev}_k : K[X_1, \ldots, X_m]_k \longrightarrow K^{\mathcal{A}},$$

$$f \mapsto (v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)),$$

defines a linear map of $K$-vector spaces. The image of $\text{ev}_k$, denoted by $C_k(\mathcal{A}, v)$, defines a linear code.

Definition

We call $C_k(\mathcal{A}, v)$ the generalized affine Cartesian evaluation code 
(Cartesian code for short) of degree $k$ associated to $\mathcal{A}$ and $v$. 
We will focus on the case when $A = A_1 := \{a_1, \ldots, a_n\}$.

Observe that in this case the Cartesian code $C_k(A_1, \mathbf{v})$ is the generalized Reed-Solomon code of length $n$ and dimension $k$. 

Define the following polynomials:

$L_1(X_1) := \prod_{a \in A_1} (X_1 - a)$.

$L'_1(X_1)$ denotes the formal derivative of $L_1(X_1)$.

For each element $a \in A_1$, $L_a(X_1) := L_1(X_1)(X_1 - a)$.

Then $L_a(a) = L'_1(a)$. 

LCD codes on Cartesian codes

We will focus on the case when $\mathcal{A} = A_1 := \{a_1, \ldots, a_n\}$. Observe that in this case the Cartesian code $C_k(A_1, \mathbf{v})$ is the generalized Reed-Solomon code of length $n$ and dimension $k$. Define the following polynomials:

$$L_1(X_1) := \prod_{a \in A_1} (X_1 - a).$$
LCD codes on Cartesian codes

We will focus on the case when $\mathcal{A} = A_1 := \{a_1, \ldots, a_n\}$.
Observe that in this case the Cartesian code $C_k(A_1, \mathbf{v})$ is the *generalized Reed-Solomon code* of length $n$ and dimension $k$. Define the following polynomials:

$$L_1(X_1) := \prod_{a \in A_1} (X_1 - a).$$

$L_1'(X_1)$ denotes the formal derivative of $L_1(X_1)$. 
LCD codes on Cartesian codes

We will focus on the case when \( \mathcal{A} = A_1 := \{a_1, \ldots, a_n\} \).

Observe that in this case the Cartesian code \( C_k(A_1, \mathbf{v}) \) is the \textit{generalized Reed-Solomon code} of length \( n \) and dimension \( k \). Define the following polynomials:

\[
L_1(X_1) := \prod_{a \in A_1} (X_1 - a).
\]

\( L'_1(X_1) \) denotes the formal derivative of \( L_1(X_1) \). For each element \( a \in A_1 \),

\[
L_a(X_1) := \frac{L_1(X_1)}{X_1 - a}.
\]

Then

\[
L_a(a) = L'_1(a).
\]
An element of the code $C_k(A_1, v)$ is of the form

$$(v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)),$$

where $f(X_1) \in K[X_1], \deg f(X_1) < k$. 
An element of the code $C_k(A_1, \mathbf{v})$ is of the form

$$(v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)),$$

where $f(X_1) \in K[X_1]$, $\deg f(X_1) < k$.

An element of the dual is of the form

$$\left(\frac{g(a_1)}{v_{a_1} L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_{a_n} L_{a_n}(a_n)}\right),$$

where $g(X_1) \in K[X_1]$, $\deg g(X_1) < n - k$. 
An element of the code $C_k(A_1, \mathbf{v})$ is of the form

$$(v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)),$$

where $f(X_1) \in K[X_1], \deg f(X_1) < k$.

An element of the dual is of the form

$$\left( \frac{g(a_1)}{v_{a_1} L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_{a_n} L_{a_n}(a_n)} \right),$$

where $g(X_1) \in K[X_1], \deg g(X_1) < n - k$.

We are interested in finding conditions over $A_1$ and $\mathbf{v}$ such that $C_k(A_1, \mathbf{v})$ is LCD.
Observe that the Cartesian code $C_k(A_1, \mathbf{v})$ is not LCD if and only if there are polynomials $f(X_1)$ and $g(X_1)$ such that $\deg(f) < k$, $\deg(g) < n - k$ and

$$(v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)) = \left( \frac{g(a_1)}{v_{a_1} L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_{a_n} L_{a_n}(a_n)} \right). \quad (1)$$
Observe that the Cartesian code $C_k(A_1, \mathbf{v})$ is not LCD if and only if there are polynomials $f(X_1)$ and $g(X_1)$ such that $\deg(f) < k$, $\deg(g) < n - k$ and

$$(v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)) = \left(\frac{g(a_1)}{v_{a_1} L_{a_1}(a_1)}, \ldots, \frac{g(a_n)}{v_{a_n} L_{a_n}(a_n)}\right). \quad (1)$$

Equation (1) holds if and only if

$$v_{a_i}^2 L_1'(a_i) f(a_i) = g(a_i), \quad \text{for all } i \in [n]. \quad (2)$$
Observe that the Cartesian code $C_k(A_1, \mathbf{v})$ is not LCD if and only if there are polynomials $f(X_1)$ and $g(X_1)$ such that $\deg(f) < k$, $\deg(g) < n - k$ and

$$
(v_{a_1} f(a_1), \ldots, v_{a_n} f(a_n)) = \left( \frac{g(a_1)}{v_{a_1} \La_1(a_1)}, \ldots, \frac{g(a_n)}{v_{a_n} \La_n(a_n)} \right). \quad (1)
$$

Equation (1) holds if and only if

$$
v_{a_i}^2 \La'_1(a_i) f(a_i) = g(a_i), \quad \text{for all } i \in [n]. \quad (2)
$$

**Lemma**

$$
H_1(X_1) := \sum_{a \in A_1} \frac{\La(X_1)}{\La(a)} v_{a_i}^2 \La'_1(a) \text{ has the following properties:}
$$

(i) $H_1(a_i) = v_{a_i}^2 \La'_1(a_i)$, for all $i \in [n]$.

(ii) $\deg(H_1) < n$.

(iii) $H_1(X_1)$ and $\La_1(X_1)$ are coprime in $K[X_1]$. 
Theorem

$C_k(A_1, \mathbf{v})$ is not LCD if and only if there are polynomials $f(X_1), g(X_1)$ and $h(X_1)$ in $K[X_1]$ such that $\deg(f) < k$, $\deg(g) < n - k$ and

$$L_1(X_1)h(X_1) + H_1(X_1)f(X_1) = g(X_1),$$

where $H_1(X_1)$ is the polynomial associated to $C_k(A_1, \mathbf{v})$ defined on previous lemma.
Theorem

\( C_k(A_1, \nu) \) is not LCD if and only if there are polynomials \( f(X_1), g(X_1) \) and \( h(X_1) \) in \( K[X_1] \) such that \( \deg(f) < k, \deg(g) < n - k \) and

\[
L_1(X_1)h(X_1) + H_1(X_1)f(X_1) = g(X_1),
\]

where \( H_1(X_1) \) is the polynomial associated to \( C_k(A_1, \nu) \) defined on previous lemma.

Theorem

Let \( g_1(X_1), \ldots, g_{m+2}(X_1) \) be the remainders of the polynomials \( L_1(X_1) \) and \( H_1(X_1) \). The Cartesian code \( C_k(A_1, \nu) \) is not LCD if and only if there is \( i \in [m+2] \) such that

\[
\deg(g_i) < n - k < \deg(g_{i-1}).
\]
Theorem

Let \( g_1(X_1), \ldots, g_{m+2}(X_1) \) be the remainders of the polynomials \( L_1(X_1) = \prod_{a_1 \in A_1} (X_1 - a_1) \) and \( H_1(X_1) := \sum_{a \in A_1} \frac{L_a(X_1)}{L_a(a)} v_a L'_1(a) \). The Cartesian code \( C_k(A_1, v) \) is LCD if and only if

\[
    n - k \in \{ n, n - 1, \ldots, \deg(g_1), \deg(g_2), \ldots, \deg(g_{m+2}) \}.
\]
Theorem

Let \( g_1(X_1), \ldots, g_{m+2}(X_1) \) be the remainders of the polynomials
\[ L_1(X_1) = \prod_{a_1 \in A_1} (X_1 - a_1) \]
and \( H_1(X_1) := \sum_{a \in A_1} \frac{L_a(X_1)}{L_a(a)} v_a^2 L'_1(a) \). The Cartesian code \( C_k(A_1, v) \) is LCD if and only if
\[ n - k \in \{ n, n - 1, \ldots, \deg(g_1), \deg(g_2), \ldots, \deg(g_{m+2}) \} \].

Corollary

Let \( g_1(X_1), \ldots, g_{m+2}(X_1) \) be the remainders of the polynomials
\[ L_1(X_1) = \prod_{a_1 \in A_1} (X_1 - a_1) \]
and \( L'_1(X_1) \), the formal derivative of \( L_1(X_1) \). The Reed-Solomon code \( RS_k(A_1) \) is LCD if and only if
\[ n - k \in \{ n, n - 1, \ldots, \deg(g_1), \deg(g_2), \ldots, \deg(g_{m+2}) \} \].
Example

Let \( K := \mathbb{F}_{13} \) and \( A_1 := \{0, 2, 3, 5, 6, 8, 10, 11\} \). Then the degrees of the remainders are 0, 3, 4, 5, 6 and 7. Thus, the Reed-Solomon code \( GRS_k(A_1, 1) \) is LCD if and only if \( k \in \{0, 1, 2, 3, 4, 5, 8\} \).
Example

Let $K := \mathbb{F}_{13}$ and $A_1 := \{0, 2, 3, 5, 6, 8, 10, 11\}$. Then the degrees of the remainders are 0, 3, 4, 5, 6 and 7. Thus, the Reed-Solomon code $GRS_k(A_1, 1)$ is LCD if and only if $k \in \{0, 1, 2, 3, 4, 5, 8\}$.

Example

Using the same $A_1$ than previous example but now $K := \mathbb{F}_{17}$, we obtain that the degrees of the remainders are 0, .., 7. Thus, the Reed-Solomon code $GRS_k(A_1, 1)$ is always LCD. Of course $0 \leq k \leq 8$. 


Thanks for your time.