EC500

Design of Secure and Reliable Hardware

Lecture 8

Mark Karpovsky

1 Extensions of Finite Fields

Let Z be a field and consider $Z^n = \{(Z_1, \cdots, Z_n): Z_i \in Z\}$. Z^n is a linear space over Z and we can take a polynomial over Z, $p(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} + x^n$ where $c_i \in Z$; $\deg p(x) = n$. $p(x)$ is irreducible if $p(x)$ cannot be represented as $S(x)R(x)$ ($\deg S(x) > 1$, $\deg R(x) > 1$). $p(x)$ is primitive if $x^i \neq x^j$ for all $i, j = 0,1, \cdots, |Z|^n - 2$.

T1. If $p(x)$ is primitive → it is irreducible (the opposite is not true)

T2. For any Z and any n, there exists at least one primitive polynomial $p(x)$

T3. If $p(x)$ is primitive, then Z^n is a field (called n-th extension of Z) if all vectors in Z^n are interpreted as polynomials and all operations in Z^n are modulo $p(x)$

i.e. $p(x) = 0$; x is the primitive element of Z^n (Z itself may be an extension of another field; e.g. $z = Z_2^3 \to z^4 = (Z_2^3)^4$)

T4. For any finite field or its extension, the number of elements is q^n (where q is a prime)

T5. Any two fields with the same number of elements are isomorphic

There are no simple procedures to decide whether $p(x)$ is primitive over Z (irreducibility is a necessary condition for primitivity). For Z_2^n, there are good tables of primitive polynomials.

Example: $Z = Z_2 = \{0,1\}$, $n = 3$

Binary	Polynomial	Exponential
0 0 0	0	−
0 0 1	x^2	x^2
0 1 0	x	x^1
0 1 1	$x^2 + x$	x^4
1 0 0	1	x^0
1 0 1	$x^2 + 1$	x^6
1 1 0	$1 + x$	x^3
1 1 1	$1 + x + x^2$	x^5
1 x x^2		

$p(x) = x^3 + x + 1 \to$ $x^3 = x + 1$

$x^4 = x^2 + x$

$x^5 = x^3 + x^2 = x^2 + x + 1$

$x^6 = x^3 + x^2 + x = x + 1 + x^2 + x = x^2 + 1$

$x^7 = x^3 + x = 1$

$x^{2^n - 1} = x^7 = 1$, $|Z_2^n| = 8$

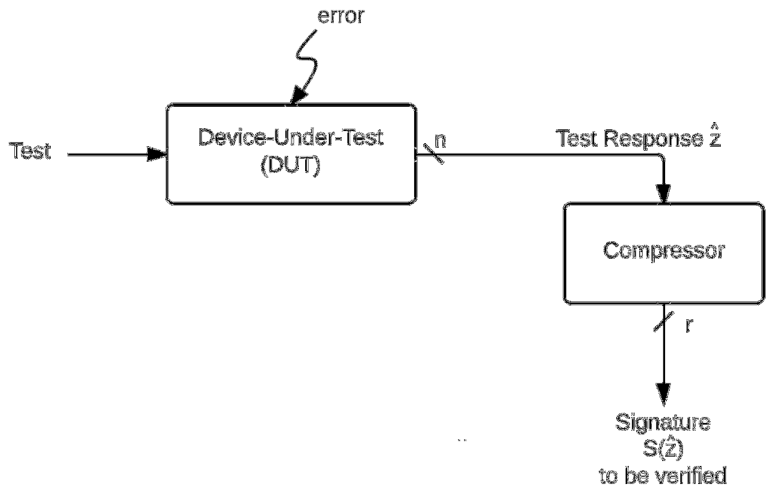
$(101)(110) = x^6 \cdot x^3 = x^9 = x^2 = 001$

$111/110 = x^2 = 001$, $110/101 = x^{-3} = x^4 = 011$

2 Authentication

Data Compression of Test Responses in Computation Channels by Error Detecting Codes

Signature analysis



z – fault free response

$\hat{z}$ – faulty reponse

$\hat{z} = z \oplus e$, e is the error

Problem:

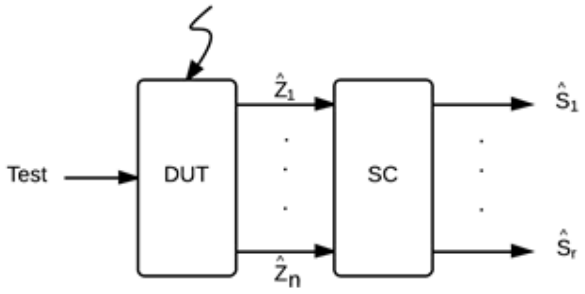
Minimize r (number of observation points, length of the signature to be stored) for a given class E of errors which may appear at the output of the DUT such that for any z: $\boxed{S(z+e) \neq S(z)}$.

Solution:

Let V be a (n, k, d) code and E is a class of errors with multiplicities of at most $d-1$. ($E = \{e | \|e\| \leq d-1\}$). Let H be a check matrix for V. Then, $H\tilde{z} = Hz + He$, $\|e\| \leq d-1$. Since V has distance d, $He \neq 0$. Thus $H\tilde{z} = Hz$ and we can take $S(\tilde{z}) = H\tilde{z}$.

- Optimal compressors are network computing syndromes for the corresponding optimal codes
- Optimal compressors are linear (can be built by using XOR gates only)
- Minimal numbers of observation points are equal to the minimal numbers of redundant bits $r = n - k$ in the corresponding codes
- Compressors compute syndromes of errors
- Good codes generate good compressors with min r

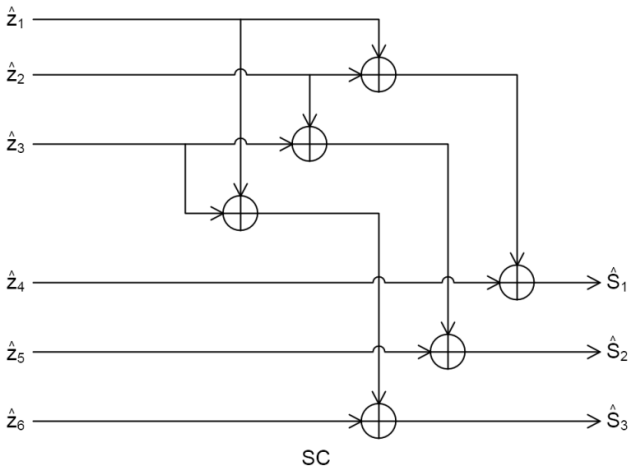
Space Compressors (SC)



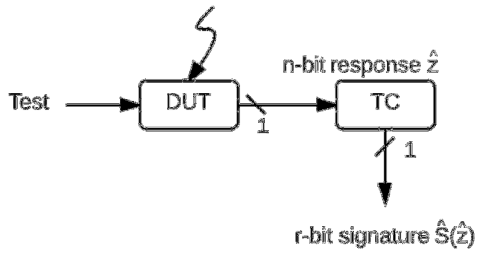
SC is a combinational network of XOR gates computing $\hat{S} = H\hat{z}$

Example:
SC for single errors and double errors based on Hamming codes
$l = 2$, $r = \lceil \log_2(n+1) \rceil$

Let $n = 6 \rightarrow G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \rightarrow H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$, $r = 3$

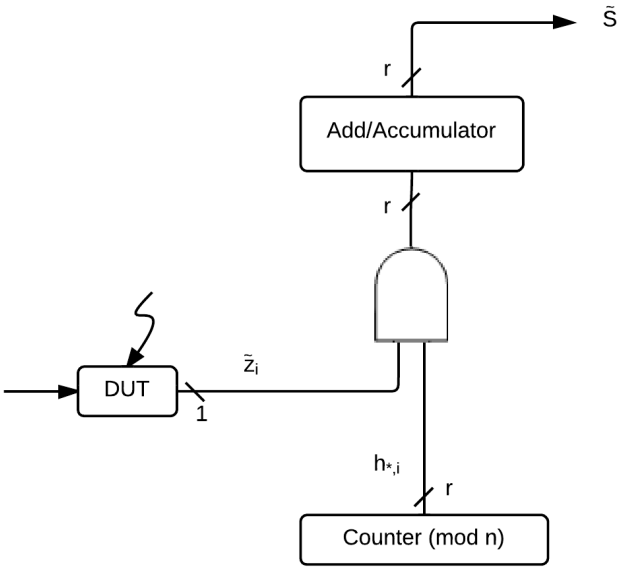


Time Compressors (TC)
TC may be used after SC



- TC is a sequential network computing $\hat{S}(\hat{z})$ in n-clocks, $\hat{S}(\hat{z}) = H\hat{z}$.
- At most l bits in any n-bit response can be distorted
- $\hat{S}(\hat{z}) \neq S(z)$

Let $H = [h_{*,1} \quad \cdots \quad h_{*,n}]$ be a $r \times n$ check matrix for a (n, k, d) code $(d = l - 1)$.



The counting sequence is $h_{*,1}, \cdots, h_{*,n}$

$\tilde{S} = \bigoplus_{i=1}^{n} h_{*,1} \cdot \tilde{z}_i$