EC500

Design of Secure and Reliable Hardware

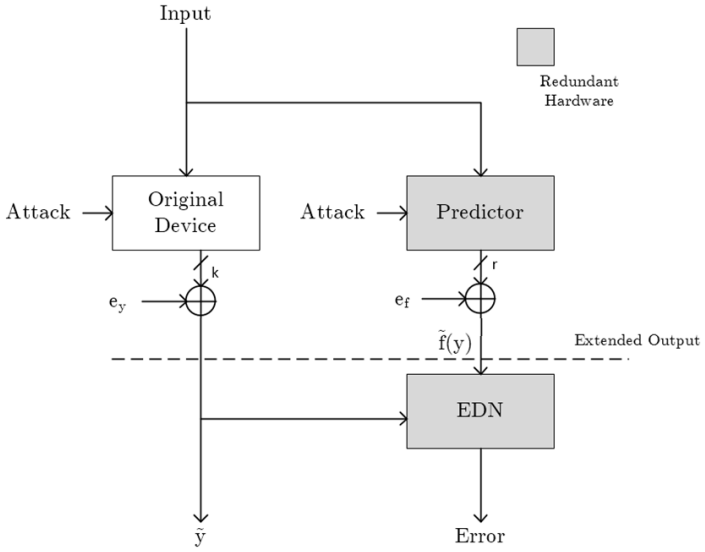
Lecture 17 – Algebraic Manipulation Detection Codes (Strong Attacks)

Mark Karpovsky

1 Motivations

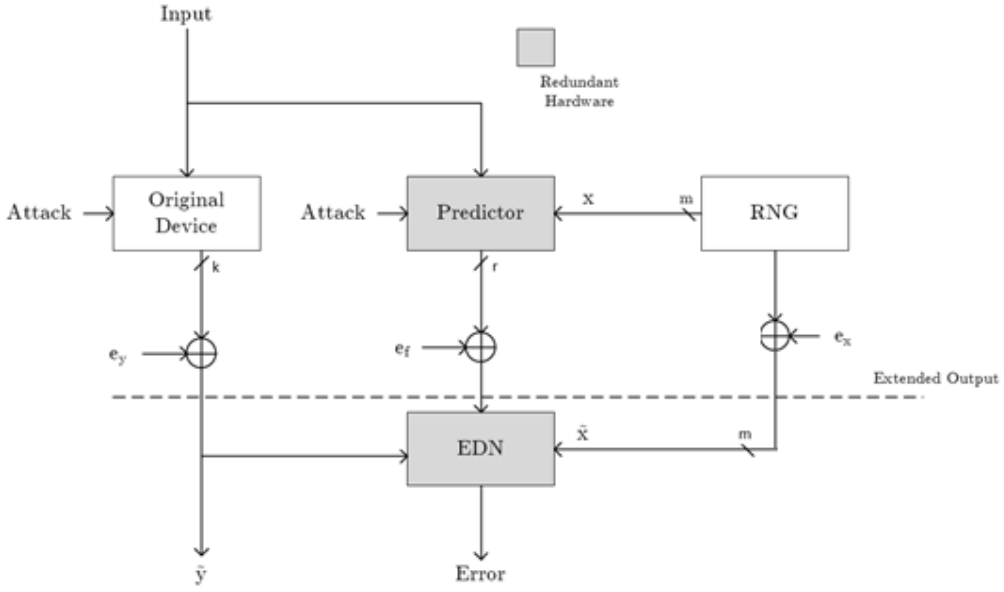
The steps to breaking any protection scheme based on a single error detecting codes are:

1. Select an input and observe y.
2. Investigate the code to select an error $e = (e_y, e_f)$ such that for a codeword $(y, f(y))$, $(y \oplus e_y, f(y) \oplus e_f)$ also belongs to the code.
3. Inject faults manifested as e.



This is the strongest attacker model. Any protection based on a single error detecting code will not work.

2 General Architecture (for strong attacks)



3 Definitions

- $C = \{(y, x, f(y,x))\}$
  - $y \in GF(2^k)$, $x \in GF(2^m)$, $f(y,x) \in GF(2^r)$

- $e = (e_y, e_x, e_f)$
  - $e_y \in GF(2^k)$, $e_x \in GF(2^m)$, $e_f \in GF(2^r)$

- **Security kernel**: $K_s = \{e | \exists y, f(y \oplus e_y, x \oplus e_x) = f(y,x) \oplus e_f \; for \; all \; x\}$
  - For AMD code, $K_s = \{0\}$ (This is the **definition of AMD codes**)

4 Worst Case Error Masking Probability

- $Q(y,e) = \frac{|\{x | f(y \oplus e_y, x \oplus e_x) = f(y,x) \oplus e_f\}|}{2^m}$
- Worst case error masking probability $\max_{y,e \neq 0} Q(y,e) = Q$
- The optimal codes should minimize $\max_{y,e \neq 0} Q(y,e) = Q$ among all codes with the same k, m, and r.
-
- $f(y,x) = x^{b+2} \oplus x^b \cdot y_b \oplus x^{b-1} \cdot y_{b-1} \oplus \cdots \oplus x \cdot y_1$
  - $y \in GF(2^r)$, $x \in GF(2^r)$, $f(y,x) \in GF(2^r)$
  - For this code, $k = br$, $m = r$, and $Q = \frac{b+1}{2^r}$.
  - Limitations:
    - b here is odd, otherwise $Q = \frac{b+2}{2^r}$.
    - The number of possible k is limited since $b \leq q-3$, $k = br \leq (q-3)r$. $Q > 2^{-r+1}$ when $b > 1$, thus to increase k further, we have to sacrifice Q.
    - r cannot be 1 for $q \neq 2$

5 Example

Suppose $f(y,x) = x^{b+2} \oplus x^b \cdot y_b \oplus x^{b-1} \cdot y_{b-1} \oplus \cdots \oplus x \cdot y_1$ and $y \in GF(2^r)$, $x \in GF(2^r)$, $f(y,x) \in GF(2^r)$. Let $r = 3$ and $b = 1$.

1. What is m and k?
2. What is $f(y,x)$?
3. What is the error masking equation?
4. How do we prove the maximum possible number of solutions for the error masking equation?

6 Horner's Method

We can reduce the number of multiplications by transforming $f(y,x)$ into a computationally efficient form. For example, for $b = 3$ and $r = 32$, $f(y,x) = y_1x + y_2x^2 + y_3x^3 + x^5 = x\left(y_1 + x\left(y_2 + x(y_3 + x^2)\right)\right)$. We have reduced the number of multipliers from 7 down to 4.