Physical layer security: combining error control coding and cryptography

Sounak Gupta – Goutam Paul

School of ECE, Georgia Institute of Technology, Atlanta, GA
Common approach:
Common approach:

- physical transmission;
Common approach:

- physical transmission;
- errors;
Common approach:

- physical transmission;
- errors;
- control coding;
Common approach:

- physical transmission;
- errors;
- control coding;
- cryptography.
Common approach:
- physical transmission;
- errors;
- control coding;
- cryptography.

Potential enhancement:
Common approach:

- physical transmission;
- errors;
- control coding;
- cryptography.

Potential enhancement: using these errors
Physical layer security: combining error control coding and cryptography

\[ S = M \oplus Z \]
Error Control enCoding
\[ P(s_n \text{ inverted}) = p_m \]
Physical layer security: combining error control coding and cryptography

\[ \mathbb{P}(s_n \text{ inverted }) = p_w \]
$N$ bits of $M$ are known
ECC favours the main channel
ECC favours the main channel

\[
\begin{align*}
\text{LFSR}_i & \rightarrow (a_n) \\
(1-p_1) & \rightarrow (z_n) \\
(1-p_2) & \rightarrow (v_n)
\end{align*}
\]
ECC favours the main channel

\[ p' = p_1(1 - p_2) + (1 - p_1)p_2 \]
Feedback polynomial

Checks

Attack A

Efficiency matters

Attack B

Efficiency matters

\[ g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_k x^k \]
\[ g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_k x^k \]

\((j_i)\): non zero coefficients of \(g\)
\[ g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_k x^k \]

\[(j_i): \text{non zero coefficients of } g\]

\[ a_{j+j_0} + a_{j+j_1} + \cdots + a_{j+j_t} = 0 \]
\[ a_j = a_{j+1} + a_{j+2} + \cdots + a_{j+t} \]
\[ a_j = a_{j+j_1} + a_{j+j_2} + \cdots + a_{j+j_t} \]

Checks.
\[ a_j = a_{j+j_1} + a_{j+j_2} + \cdots + a_{j+j_t} \]

Checks.

\[(x + y)^2 = x^2 + y^2\]
$a_j = a_{j+j_1} + a_{j+j_2} + \cdots + a_{j+j_t}$

Checks.

$(x + y)^2 = x^2 + y^2$

More checks.
\[ a_j = a_{j+j_1} + a_{j+j_2} + \cdots + a_{j+j_t} \]

Checks.

\[ (x + y)^2 = x^2 + y^2 \]

More checks.

\[ (p_n^*) = \mathbb{P}(y_n = a_n | \text{checks}) \]
Description:
Description:

- computing $(p_n^*)$;
Description:

- computing \( p_n^* \);
- choosing \( k \) bits;
Description:

- computing \((p_n^*)\);
- choosing \(k\) bits;
- constructing the associated set of equations;
Description:

- computing \((p_n^*)\);
- choosing \(k\) bits;
- constructing the associated set of equations;
- solving it (LU decomposition);
Description:

- computing \((p_n^*)\);
- choosing \(k\) bits;
- constructing the associated set of equations;
- solving it (LU decomposition);
- checking.
Feedback polynomial
Checks
Attack A
Efficiency matters
Attack B
Efficiency matters

Sounak Gupta – Goutam Paul

Physical layer security: combining error control coding and...
Description:

computing \((p \ast n)\); computing \(p\) thr; flipping some bits; iterate.
Description:
  - computing \( (p_n^*) \);
Description:

- computing \( (p_n^*) \);
- computing \( p_{\text{thr}} \);
Description:
- computing \( p_n^* \);
- computing \( p_{\text{thr}} \);
- flipping some bits;
Description:

- computing \( \left(p_n^*\right) \);
- computing \( p_{\text{thr}} \);
- flipping some bits;
- iterate.
Efficiency matters for Attack B. The correction capability of the feedback polynomial, $p_2$, is shown in the graph. As $p_2$ increases from 0 to 0.15, the correction capability decreases, indicating a trade-off between error correction and security.
• some enhancement by ECC matters;
• analysis only base on LFSR systems with plain-text attack;
• still useful for weak-encryption protocols (GSM, Bluetooth).