**Introduction**

- Gong-Harn Public Key Cryptosystem (GH-PKC) is based on third-order linear feedback shift register (LFSR) sequence with a particular phase.
- Security is based on the difficult in solving discrete logarithm (DL) problem in GF(q^2), where q = p or q = q^2, depending on the implementation, and p is a prime.
- For an implementation of GH-PKC over GF(p), the security of the implementation is based on the difficult in solving DL problem in GF(p^2), i.e., in order to implement the GH-PKC over GF(p), with 1024-bit security, a 341-bit p is required!

**Dual State Fast Evaluation Algorithm (DSEA)**

- To compute the s_k sequence terms.
- Binary representation of k:

  \[ k = \sum_{i=0}^{k} k_i2^i = k_0 + k_12 + k_22^2 + \ldots + k_{k-1}2^{k-1} \]

- Let \( T_0 = k_0 \) and \( T_1 = k_0 + 2T_0 \) for \( 1 \leq k \leq n \) \( \Rightarrow T_k = k \).
- Let \( f(T) \) and \( f(T') \).

**Computation of a Previous Sequence Term**

- Given \( (s_k, s_{k+1}) \) and its dual. Determine \( s_{(k+1)} \) terms.
- Let \( \delta = s_{(k+1)} = s_{k+1} \cdot (s_{k+2} - s_k) \).
- Then \( s_{(k+1)} \) terms can be computed by:

  \[
  \begin{align*}
  D(s_k) &= s_0 \delta \\
  D(s_{k+1}) &= s_1 \delta \\
  D(s_{k+2}) &= s_2 \delta \\
  \end{align*}
  \]

**Computation of Mixed Terms \( S_{(k+1)}(s_k, s_{k+1}) \) and its dual**

1. Compute the sequence terms \( s_{(k+1)}(s_k, s_{k+1}) \)
   - Use a general result for LFSR sequence.
   - Define Transition Matrix A and State Matrix M:

   \[
   A = \begin{bmatrix}
   1 & 0 & \cdots & 0 \\
   0 & 1 & \cdots & 0 \\
   \vdots & \cdots & \ddots & \vdots \\
   0 & 0 & \cdots & 1
   \end{bmatrix}
   \]

   \[
   M_k = s_k \cdot (s_{k+1}, s_{k+2}, \ldots, s_{k+n})
   \]

2. Two properties:
   - \( \delta = s = s_k \cdot (s_{k+1}, s_{k+2}, \ldots, s_{k+n}) \cdot (s_{k+1}, s_{k+2}, \ldots, s_{k+n}) \cdot (s_{k+2}, s_{k+3}, \ldots, s_{k+n+1}) \cdot (s_{k+3}, s_{k+4}, \ldots, s_{k+n+2}) \cdot \ldots \cdot (s_{k+n}, s_{k+n+1}, \ldots, s_{k+n+n}) \)

**Third-order Characteristic Sequence**

- Irreducible polynomial \( f(x) \) of degree 3 over GF(p):

  \[ f(x) = x^3 - ax^2 + bx - 1 \]

- If initial state is:

  \[ s_i = 3s_i - a, s_{i+1} = a^2 - 2b \]

- Then the sequence generated by \( f(x) \) is called a third-order characteristic sequence.

**Profile of Third-order Characteristic Sequences**

- Period \( Q \) is a factor of \( p^2 + p + 1 \)
- Trace Representation:

  \[ s_i = Tr(a^i) = a^i + a^{2i} \]

where \( a \) is a root of \( f(x) \) in the extension field GF(p^2).

**Reciprocal Sequence**

- Given the \( f(x) \) above, the reciprocal polynomial is:

  \[ f(x) = x^3 - ax^2 + bx - 1 \]

- By choosing the corresponding initial states as shown above, the sequence generated by \( f(x) \) is also a third-order characteristic sequence.

**Commutative Law**

- Let \( f(x) = x^3 - ax^2 + bx - 1 \) be irreducible over GF(q) and \( s_k \) be the characteristic sequence generated by \( f(x) \). Then for any positive integers \( k \) and \( e \):

  \[ s_k(s_{a, b}, s_{b, -a, b}) = s_k(s_{a, b}) \]

**GH Diffie-Hellman Key Agreement Protocol**

**System Parameters:**

- \( f(x) = x^3 - ax^2 + bx - 1 \), an irreducible polynomial over GF(p), where p is a prime number. Period of the third-order characteristic sequence is denoted by Q.

**GH Digital Signature Algorithm (GH DSA)**

- ElGamal-like signature algorithm
  - Alice:
    - Private Key: Choose \( x \), with \( 0 < x < Q \) and \( \text{gcd}(x, Q) = 1 \)
    - Public Key: The \( s_k \) terms generate by \( f(x) \)
  - Signing Process:
    1. Randomly choose \( k \), with \( 0 < k < Q \) and \( \text{gcd}(k, Q) = 1 \).
    2. Use DSA algorithm to compute \( (u, v) \) and its dual such that \( \text{gcd}(u, Q) = 1 \)
  - Verifying Process:
    1. Compute \( s_k(u, v) \) and \( (u, v) \) using \( f(x) \) and their duals.
    2. If \( \text{gcd}(u, Q) = 1 \) else Cases 2 or 3

**References:**