Esquema de Matsumoto-Imai

Reporte de Estancia de Investigación

Pérez Ibarra Miguel Esteban **24th June 2020**

Indice

Esquemas de Matsumoto-Imai

- El cifrado original de Matsumoto-Imai fue derrotado por medio de un ataque algebraíco utilizando la linearización de ecuaciones de Patarin.

Esquemas de Matsumoto-Imai

- El cifrado original de Matsumoto-Imai fue derrotado por medio de un ataque algebraíco utilizando la linearización de ecuaciones de Patarin.
- El segundo esquema se llama el Cifrado Desequilibrado de Matsumoto-Imai y fue propuesto por el mismo Patarin.

Primera Esquema

Este esquema depende del teorema:

Theorem (Problema MQ)

Resuelva el sistema $p_1(x) = p_2(x) = \cdots = p_m(x) = 0$, donde cada p_i es cuadrático en $x = (x_1, \ldots, x_n)$.

Análogamente al esquema Rainbow también se utiliza un mapeo

$$\bar{F} = L_1 \circ \tilde{F} \circ L_2$$

Matsumoto e Imai proponen en específico a

$$F : X \mapsto X^{1+q^i}$$

Derrota

Al ser derrotado se proponen las modificaciones:

- Metodo Menos-Más

Derrota

Al ser derrotado se proponen las modificaciones:

- Metodo Menos-Más
- Metodo de ecuación de campo escondido.

Derrota

Al ser derrotado se proponen las modificaciones:

- Metodo Menos-Más
- Metodo de ecuación de campo escondido.
- Metodo de ecuación de campo escondido con el metodo Aceite-Vinagre

Derrota

Al ser derrotado se proponen las modificaciones:

- Metodo Menos-Más
- Metodo de ecuación de campo escondido.
- Metodo de ecuación de campo escondido con el metodo Aceite-Vinagre
- Metodo de Cifrado Desequilibrado propuesto por Patarin y trabajado por Jintai Ding.

Construcción de Esquema

Example (Requisitos)

- Un campo finito k de característica positiva con q elementos.

$$\bar{K} \equiv k[x]/g(x).$$

Example

Construcción de Esquema

Example (Requisitos)

- Un campo finito k de característica positiva con q elementos.
- $g(x)$ irreducible sobre k.

$$\bar{K} \equiv k[x]/g(x).$$

Example

Construcción de Esquema

Example (Requisitos)

- Un campo finito k de característica positiva con q elementos.
- $g(x)$ irreducible sobre k.
- $\bar{K}$ extensión de campo de k de grado n.

$$\bar{K} \equiv k[x]/g(x).$$

Example

Construcción de Esquema

Example (Requisitos)

- Un campo finito k de característica positiva con q elementos.
- $g(x)$ irreducible sobre k.
- $\bar{K}$ extensión de campo de k de grado n.

$$\bar{K} \equiv k[x]/g(x).$$

Example

- $\varphi(I + a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, \ldots, a_{n-1})$.

Construcción de Esquema

Example (Requisitos)

- Un campo finito k de característica positiva con q elementos.
- $g(x)$ irreducible sobre k.
- $\bar{K}$ extensión de campo de k de grado n.

$$\bar{K} \equiv k[x]/g(x).$$

Example

- $\varphi(I + a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, \ldots, a_{n-1})$.
- $t(1 + q^i) \equiv 1 \ (mod \ q^n - 1)$

Construcción de Esquema

Example (Requisitos)

- Un campo finito k de característica positiva con q elementos.
- $g(x)$ irreducible sobre k.
- $\bar{K}$ extensión de campo de k de grado n.

$$\bar{K} \equiv k[x]/g(x).$$

Example

- $\varphi(I + a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, \ldots, a_{n-1})$.
- $t(1 + q^i) \equiv 1 \ (mod\ q^n - 1)$
- $F(X) = X^{1+q^i}$, tal que $X \in \bar{K}$

Primer Encapsulamiento

El mapeo φ

$\tilde{F} = \varphi \circ F \circ \varphi^{-1} =$

$(\tilde{F}_1(x_1, \ldots, x_n), \tilde{F}_2(x_1, \ldots, x_n), \ldots, \tilde{F}_n(x_1, \ldots, x_n))$.

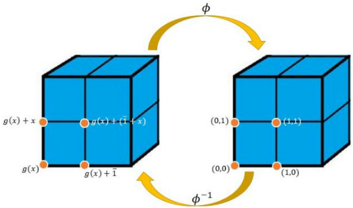

Figure: φ para $\bar{K} = \mathbb{Z}_2[x]/(\bar{1} + x + x^2)$

Segundo Encapsulamiento

El encapsulamiento de $\tilde{F}$

Se cumple que los $\tilde{F}_i(x_1, \ldots, x_n)$ son polinomios cuadraticos de n variables. Para terminar se eligen al azar L_1 y L_2 dos mapeos lineales afines sobre k^n

$$\bar{F}(x_1, \ldots, x_n) = L_1 \circ \tilde{F} \circ L_2(x_1, \ldots, x_n) =$$

$$(\bar{F}_1(x_1, \ldots, x_n), \bar{F}_2(x_1, \ldots, x_n), \ldots, \bar{F}_n(x_1, \ldots, x_n))$$

Construcción del Cifrado Desequilibrado

Example

- Condiciones de campo del esquema original.

Sea r un entero positivo pequeño, dado $(x_1, \ldots, x_n) \in k^n$ se debe de elegir al azar r funciones lineales

$$z_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} \alpha_{ji} x_j + \beta_i \in k,$$

Example

$$Z(x_1, \ldots, x_n) = (z_1(x_1, \ldots, x_n), \ldots, z_r(x_1, \ldots, x_n)) =$$

$$(\sum_{j=1}^{n} \alpha_{j1} x_j + \beta_1, \ldots, \sum_{j=1}^{n} \alpha_{jr} x_j + \beta_r).$$

Funciones Auxiliares

La función f

Consideré la función $f : k^r \mapsto k^n$ dada por

$$f(z_1, \ldots, z_r) = (f_1(z_1, \ldots, z_r), \ldots, f_n(z_1, \ldots, z_r))$$

$\hat{F}$ como el desequilibrio de $\tilde{F}$ causado por Z

Se define el mapeo $\hat{F} : k^n \mapsto k^r$ dada por la regla

$$\hat{F}(x_1, \ldots, x_n) = (\hat{F}_1(x_1, \ldots, x_n), \ldots, \hat{F}_n(x_1, \ldots, x_n))$$

$$= (\tilde{F}_1(x_1, \ldots, x_n) + f_1(z_1, \ldots, z_r), \ldots, \tilde{F}_n(x_1, \ldots, x_n) + f_n(z_1, \ldots, z_r))$$

$\bar{\bar{F}}$ como el Cifrado Desequilibrado de Matsumoto-Imai

Primera Forma

$$\bar{\bar{F}} = L_1 \circ \hat{F} \circ L_2(x_1, \ldots, x_n)$$
$$= (y_1(x_1, \ldots, x_n), \ldots, y_n(x_1, \ldots, x_n))$$

Segunda Forma

$$\bar{\bar{F}} = L_1 \circ \hat{F} \circ L_2(x_1, \ldots, x_n) + L_1 \circ \tilde{f} \circ L_2(x_1, \ldots, x_n)$$

Llave publica

1. Un campo k finito

Llave publica

1. Un campo k finito
2. Las estructuras $+$, $*$ de k

Requisitos

Esto incluye la generación de tablas de $+$, $*$ en k

Llave publica

1. Un campo k finito
2. Las estructuras $+, *$ de k
3. n polinomios cuadráticos
   $y_1(x_1, \ldots, x_n), \ldots, y_n(x_1, \ldots, x_n)$

Llave publica

1. Un campo k finito
2. Las estructuras $+$, $*$ de k
3. n polinomios cuadráticos $y_1(x_1, \ldots, x_n), \ldots, y_n(x_1, \ldots, x_n)$

1. Se da un mensaje de texto plano $M = (x'_1, \ldots, x'_n)$

Llave publica

1. Un campo k finito
2. Las estructuras $+$, $*$ de k
3. n polinomios cuadráticos $y_1(x_1, \ldots, x_n), \ldots, y_n(x_1, \ldots, x_n)$

1. Se da un mensaje de texto plano $M = (x'_1, \ldots, x'_n)$
2. Se obtiene el texto cifrado $(y_1(x'_1, \ldots, x'_n), \ldots, y_n(x'_1, \ldots,$

Propiedades de la Llave Publica

- El mapeo F

Propiedades de la Llave Publica

- El mapeo F
- El conjunto de funciones lineales $z_1, \ldots, z_r$

Propiedades de la Llave Publica

- El mapeo F
- El conjunto de funciones lineales $z_1, \ldots, z_r$
- Los polinomios $f_i(z_1, \ldots, z_r)$

Propiedades de la Llave Publica

- El mapeo F
- El conjunto de funciones lineales $z_1, \ldots, z_r$
- Los polinomios $f_i(z_1, \ldots, z_r)$
- Dos mapeos lineales afines L_1 y L_2

Para Decifrar

Texto Cifrado

Primero se requiere del texto cifrado $(y_1', \ldots, y_n')$

- Se cálcula $(\bar{y}_1, \ldots, \bar{y}_n) = L_1^{-1}(y_1', \ldots, y_n')$

Para Decifrar

Texto Cifrado

Primero se requiere del texto cifrado $(y'_1, \ldots, y'_n)$

- Se cálcula $(\bar{y}_1, \ldots, \bar{y}_n) = L_1^{-1}(y'_1, \ldots, y'_n)$
- Revisamos todas la imagenes de la función f denotados por λ y su preimágen μ, se cálcula

$$(y_{\lambda 1}, \ldots, y_{\lambda n}) = \varphi^{-1} \circ F^{-1}((\bar{y}_1, \ldots, \bar{y}_n) + \lambda)$$

Para Decifrar

Texto Cifrado

Primero se requiere del texto cifrado $(y'_1, \ldots, y'_n)$

- Se cálcula $(\bar{y}_1, \ldots, \bar{y}_n) = L_1^{-1}(y'_1, \ldots, y'_n)$
- Revisamos todas la imagenes de la función f denotados por λ y su preimágen μ, se cálcula
$$(y_{\lambda 1}, \ldots, y_{\lambda n}) = \varphi^{-1} \circ F^{-1}((\bar{y}_1, \ldots, \bar{y}_n) + \lambda)$$
- Se revisa si μ corresponde con $Z(y_{\lambda 1}, \ldots, y_{\lambda n})$

Para Decifrar

Texto Cifrado

Primero se requiere del texto cifrado $(y'_1, \ldots, y'_n)$

- Se cálcula $(\bar{y}_1, \ldots, \bar{y}_n) = L_1^{-1}(y'_1, \ldots, y'_n)$
- Revisamos todas la imagenes de la función f denotados por λ y su preimágen μ, se cálcula

$$(y_{\lambda 1}, \ldots, y_{\lambda n}) = \varphi^{-1} \circ F^{-1}((\bar{y}_1, \ldots, \bar{y}_n) + \lambda)$$

- Se revisa si μ corresponde con $Z(y_{\lambda 1}, \ldots, y_{\lambda n})$
- Finalmente se cálcula

$$(x_{\lambda 1}, \ldots, x_{\lambda n}) = L_2^{-1} \circ \varphi(y_{\lambda 1}, \ldots, y_{\lambda n})$$

Referencias I

W. Gilbert.
Modern Algebra With Applications.
Wiley-Interscience, 2004.

D. Bernstein.
Post-Quantum Cryptography.
Springer, 2009.

J. Ding.
A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation.
PKC 2004, LNC 2947, pp.305-318 2004

Pérez Ibarra Miguel Esteban

Matsumoto-Imai Cryptosystems

Reporte de Estancia de Investigación