Desarrollo y análisis de criptosistemas de clave pública estilo HFE y Paillier

Por Javier y Gloria Areitio

Prof. Dr. Javier Areitio Bertolín – E. Mail: jareitio@eside.deusto.es
Catedrático de la Facultad de Ingeniería. ESIDE y Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.

Prof. Dra. Gloria Areitio Bertolín – E. Mail: ebparbeg@bs.ehu.es
Laboratorio de Informática Aplicada. Universidad del País Vasco (UPV / EHU

En el presente artículo se desarrollan cripto-sistemas de clave pública (ó asimétricos que utilizan dos claves una pública y otra secreta) estilo HFE y Paillier caracterizados uno por su rapidez en la realización de sus funciones y el otro por sus capacidades de seguridad semántica. Los criptosistemas asimétricos permiten realizar muchas funciones diferentes como por ejemplo el cifrado, la firma digital (convencional y a ciegas), funciones hash ó resumen unidireccionales, el intercambio de claves secretas de sesión para la gestión de claves en criptografía simétrica, etc. Por último se sintetiza un cripto-sistema estilo D-H basado en funciones de traza sobre campos finitos.

La seguridad de todo sistema criptográfico depende de ciertas hipótesis. Una hipótesis obvia que no se dice explícitamente es que existe aleatoriedad, es decir el mundo no es determinístico. La teoría cuántica fue la primera de las teorías físicas principales en la que la aleatoriedad es una característica inherente. Además, implícitamente se asume que los valores aleatorios pueden ser independientes. Esto implica, por ejemplo que la telepatía no existe, al menos que físicamente no se puede acceder a la información protegida (claves secretas) sin el consentimiento del propietario (la ingeniería social puede engañar a un sujeto y conseguir que fugue información sin su consentimiento).

Figura 1. Esquema jerárquico de relación entre los problemas matemáticos y los servicios criptográficos

Existen sistemas cripto-gráficos que no los puede romper ninguna cantidad de computación, dichos sistemas se denominan "teóricamente seguros" (por ejemplo el OTP, One Time Pad; un cripto-sistema próximo a este enfoque es el cifrador de Vernam). Sin embargo, la mayoría de los sistemas criptográficos pueden romperse teóricamente utilizando una cantidad suficiente de computación, por ejemplo con una búsqueda exhaustiva de claves (ataque por fuerza bruta). La seguridad de estos sistemas se basa en la no factibilidad computacional de romperlos y dicho sistema se denomina "computacionalmente seguro". Ya que no se conocen pruebas útiles y generales para evaluar la dificultad computacional de cualquier problema, la criptografía computacional descansa por entero en la hipótesis de la insolubilidad computacional.

Otra hipótesis crucial que no se hace explícitamente en criptografía es acerca de lo digno de confianza de ciertas entidades y/o componentes del sistema. El objetivo del diseño criptográfico cauteloso es formular estas hipótesis explícitas y tan débiles como se pueda (reduciendo los riesgos se aumenta la seguridad). Reducir la necesidad de hipótesis y requisitos de confianza para realizar un cierto objetivo de seguridad es el tema principal de las actuales y futuras investigaciones en criptografía.

La seguridad de los cripto-sistemas asimétricos se basa en la dificultad de diferentes problemas computacionales como por ejemplo:

(i) La factorización de números enteros grandes.

(ii) Los logaritmos discretos definidos en campos finitos.

(iii) Los logaritmos discretos en curvas elípticas.

Existe una diferencia clara entre las funciones criptográficas unidireccionales y las funciones criptográficas unidireccionales "trap-door". En las primeras es fácil pasar de "x" a f(x) pero es inviable volver de f(x) a "x" (ejemplo funciones hash SHA-1, MD5, etc.). En las funciones criptográficas "trap-door" (de puerta con trampa) es fácil pasar de "x" a f(x), sin embargo pasar de f(x) a "x" es inviable si no se conoce "k", en cambio es fácil si se conoce "k".

Síntesis de un sistema criptográfico estilo HFE

Los sistemas criptográficos de clave pública (ó asimétricos) estilo HFE (Hidden Fields Equations) utilizan operaciones con polinomios sobre campos finitos. Son una alternativa prometedora para aplicaciones prácticas de cifrado muy rápido de clave pública y firma digital muy corta.

El problema sobre el que se basan los cripto-sistemas estilo HFE denominado MQ ("Multivariable Quadratic") es NP-completo sobre campos finitos. MQ se refiere al hecho de que la clave pública se puede ver como un sistema de ecuaciones cuadráticas en muchas variables. Para cifrar un mensaje "m" se transfiere a un vector $(x_1, \ldots, x_n)$ sobre F^n. Se aplica la transformación S al vector produciendo el resultado parcial x', este a su vez se transforma de F^n a E al aplicar el polinomio privado P perteneciente a E[x] utilizando una correspondencia entre los coeficientes. El resultado y' = P(x) es un elemento de E. Luego se transforma y' al vector $(y'_1, \ldots, y'_n)$, se aplica la transformación T que da el resultado $y = (y_1, \ldots, y_n)$. Por último se puede calcular la redundancia "r" del mensaje original "m", de modo que el criptograma obtenido final es (y,r).

Para descifrar el mensaje cifrado (ó criptograma) "y" se realizan los pasos anteriores en orden inverso. Esto es posible ya que la clave privada es la terna (S, P, T) la conoce el receptor.

El paso más importante en el descifrado no es la inversión de S y T sino el cálculo de x' en la ecuación

$P(x') = y'$. Ya que el polinomio P tiene grado "d" existen "d" soluciones diferentes para esta ecuación; el añadir redundancia al mensaje hace posible seleccionar el "m" correcto del conjunto de soluciones posibles $\{S^{-1}(x_1), \ldots, S^{-1}(x_d)\}$ con d' menor o igual a d. Esta redundancia la añade el emisor en el primer paso del proceso de cifrado y el receptor debe aplicar la misma función para poder recuperar "m".

En los cripto-sistemas estilo HFE se utiliza un conjunto finito F con "q" elementos y un campo de extensión E definido sobre F. El campo de extensión se genera por medio del polinomio irreducible i(t) sobre F. Este polinomio i(t) es de grado "n". Cada elemento "e" que pertenece a E puede verse como un vector $(e_1, \ldots, e_n)$ donde cada elemento e_i pertenece a F y como un polinomio de grado (n-1) donde la multiplicación se hace en módulo el polinomio irreducible i(t).

Los tres parámetros secretos en los cripto-sistemas estilo HFE (es decir, su clave privada) son dos transformaciones afines S, T definidas de F^n en F^n y su polinomio privado P definido de E en E. Por tanto, la clave privada es la terna (S, P, T). La clave pública son los polinomios $(p_1, \ldots, p_n)$ definido sobre F donde cada uno depende de "n" variables $(x_1, \ldots, x_n)$ El polinomio privado P se define sobre el campo de extensión E y depende de una variable "x", tiene de grado "d". Las dos transformaciones afines S y T se pueden representar por una matriz (n x n) y un vector n-dimensional cada una.

Por ejemplo, la transformación afín S puede escribirse como:

$S(x) = (M_S . x^t + v_s)$

donde M_S pertenece a $F^{n.n}$, v_s pertenece a F^n y el vector "x" es:

$x = (x_1, \ldots, x_n)$

Se cumple que F^n y E tienen el mismo número de elementos, las transformaciones S y T se aplican a elementos de F, el polinomio P trata con elementos de E = F(t) / i(t).

Síntesis de un criptosistema HFE; caso práctico

1) Establecimiento de parámetros generales y claves pública y privada del receptor: Consideremos $F^n = F^2 = GF(2)$, donde n = 2, E = GF(4) generado por el polinomio de grado dos: $i(t) = t^2 + t + 1$.
Supongamos que:

$$M_S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; v_s = \begin{pmatrix} 1 \\ 1 \end{pmatrix}; M_T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}; v_t = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

De modo que $S = (M_S, v_s)$; $T = (M_T, v_t)$ y donde el polinomio secreto es de grado d = 2: $P(x) = x^2 + 1$.
La clave privada es la terna de transformaciones afines (S, P, T).
La clave pública es el producto de las tres transformaciones g = (S * P * T).

2) Operación de cifrado en la entidad emisora.
El cifrado de un mensaje "m" consiste en aplicar a dicho texto en claro "m" la clave pública g = (S * P * T) que es el producto de tres transformaciones. Sea el mensaje en claro a cifrar $m = (1, 0)^t$ sobre el campo finito $GF(2) = F^2$. El proceso es el siguiente:
(a) Aplicamos la transformación S a "m" obteniendo:

$$S(m) = (M_S . m + v_s) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

(b) Transferimos el resultado de GF(2) a E: $(0, 1)^t \rightarrow 1$.
(c) Aplicamos P: $1^2 + 1 = 1+1=0$.
(d) Transferimos el resultado de E a GF(2) : $0 \rightarrow (0, 0)^t$.
(e) Aplicamos la transformación T:

$$M_T (0, 0)^t + v_t = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} . \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

De modo que en este cifrador $(1, 0)^t \rightarrow (0, 1)^t$. No se necesita redundancia adicional ya que P puede invertirse de forma única.

3) Operación de descifrado en la entidad receptora. El proceso es el inverso de la operación de cifrado:
(a) Aplicamos T^{-1} :

$$M_T^{-1}[(0, 1)^t + v_t] = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} . \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} . \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

(b) Transferimos el resultado de F^2 a E: $(0. 0)^t \rightarrow 0$.
(c) Resolvemos P(x) = 0 inspeccionando todos los posibles valores $\{0, 1, t, t^2\}$, se observa que sólo x = 1 satisface la ecuación anterior, ya que $P(0) = 0^2 + 1 = 1$, $P(1) = 1^2 + 1 = 0$,
$P(t) = t^2 + 1 = t$, $P(t^2) = t^4 + 1 = t+1$.
(d) Transferimos el resultado de E a F^2: $1 \rightarrow (0. 1)^t$.
(e) Aplicamos S^{-1}:

$$M_S^{-1}[(0. 1)^t + v_s] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

De modo que se obtiene el mensaje sin cifrar original $m = (1, 0)^t$ después de realizar el proceso de descifrado con la clave privada del receptor que es la terna (S, P, T).

Ventajas e inconvenientes de los criptosistemas estilo HFE

Algunas de las ventajas aportadas por estos cripto-sistemas son:

(a) Teniendo en cuenta la teoría de la complejidad, la función de cifrado de HFE tiende a un sistema cuadrático aleatorio si "d" es suficientemente grande. El problema de resolver una forma cuadrática aleatoria es NP-completo.

(b) Actualmente se conocen varios ataques avanzados sobre este tipo de cripto-sistemas, pero todos ellos tienen la misma complejidad asintótica sub-exponencial y parece improbable que se conviertan en complejidad polinómica.

(c) Este tipo de cripto-sistemas permite generar firmas digitales muy cortas no rotas por criptoanálisis.

Entre los principales inconvenientes que se pueden identificar:

(a) La clave pública es bastante grande (pero, quién sabe si se puede volver esto en una ventaja).

(b) Las operaciones de la clave secreta son bastante lentas, pueden realizarse en un PC pero con más dificultad en una tarjeta inteligente poco sofisticada.

Figura 2. Esquema de Firma Digital estilo E-G (ElGamal) en su formulación original

1) *PARAMETROS DEL SISTEMA*: Se selecciona un campo finito GF(p) = Z_p donde "p" es primo por ejemplo p = 23. El firmante elige una clave privada "x" (0 < x < p) donde mcd (x, p-1)=1, por ejemplo x = 3. Para calcular la clave pública del firmante selecciona un elemento primitivo "a" de Z_{23} por ejemplo a = 5 (que no sea factor de (p-1); en este caso (p-1) = (2 . 11)) y lo eleva a la clave privada, en este caso x = 3, por tanto la clave pública es: $y = a^x \bmod p = 5^3 \bmod 23 = 10$.

2) *PROCESO DE FIRMADO*: Supongamos que el hash del mensaje a firmar es m = 7. Selecciona un número aleatorio "k" de un solo uso (0 < k < p) con mcd (k, p-1) =1, por ejemplo k = 9 y calcula $r = a^k \bmod p = 5^9 \bmod 23 = 11$. Calcula: $s = [k^{-1}(m - x \cdot r)] \bmod (p-1) = -5\,(7 - 3 \cdot 11) \bmod 22 = -2 \bmod 22 = -2+22 = 20$. Por tanto la firma digital es el par (r, s) = (11, 20).

3) *PROCESO DE VERIFICACION*: Se trata de comprobar si se cumple la expresión $a^m \bmod p = (y^r \cdot r^s) \bmod p$; en este caso $a^m \bmod p = 5^7 \bmod 23 = 17$, además $(y^r \cdot r^s) \bmod p = 10^{11} \cdot 11^{20} \bmod 23 = 22 \cdot 6 \bmod 23 = 17$. Por tanto la verificación ha sido con éxito, lo que significa que la firma (11, 20) corresponde al hash del mensaje m = 7.

Seguridad semántica y desarrollo de cripto-sistemas asimétricos estilo Paillier

Un esquema de cifrado se dice que es semánticamente seguro si no es factible inferir-averiguar información alguna acerca del texto en claro sin cifrar, a partir del texto cifrado o criptograma (obsérvese que se ha utilizado el término de no factibilidad en vez de imposibilidad), es decir, se trata de la no factibilidad de distinguir entre los cifrados de dos mensajes dados. La seguridad semántica de un cripto-sistema se relaciona con la complejidad computacional análoga a la definición de Shannon de secreto-privacidad perfecta (que requiere que el texto cifrado no proporcione información alguna sobre el texto en claro). Veamos como ejemplo, la modelización de un criptosistema con seguridad semántica tal como el de clave pública estilo Paillier:

Proceso de generación de claves del receptor

Se elige de forma aleatoria dos número primos grandes "p" y "q" independientes entre sí. Se calcula su producto N = (p . q). Se determina el producto z = (p-1).(q-1). La clave pública es el valor N y la clave privada-secreta es "z".

Proceso de cifrado en el emisor con la clave pública del receptor

Sea "m" un mensaje a cifrar donde 0 < m < N. Sea "r" un número entero aleatorio comprendido entre 0 y N, entonces el texto cifrado se determina por la expresión:

$$c = (1+ m.N)\ r^N \bmod N^2 = (1 + N)^m \cdot r^N \bmod N^2$$

Proceso de descifrado en el receptor con su clave privada

Para recuperar el texto en claro "m" del mensaje enviado se utilizan:

$$r = c^{N^{-1} \bmod z} \bmod N;$$
$$m = [(c \cdot r^{-N} \bmod N^2) - 1] / N$$

Síntesis de un criptosistema asimétrico estilo Paillier

La modelización matemática de un cripto-sistema asimétrico estilo Paillier puede especificarse de la siguiente forma:

Generación de claves pública-privada del receptor

Sean dos números primos grandes "p" y "q", por ejemplo p = 47 y q = 53 y sea su producto:

n = (p . q) = 2491, y sea

z = (p-1) (q-1) = 2392

Se elige de forma aleatoria un valor de clave pública estilo RSA "e", por ejemplo e = 3 y se determina su inverso módulo "z", denominado "d", en este caso: (e . d) = 1 mod z, es decir d = 1595, de modo que (3 . 1595) = 1 mod 2392. Por tanto la clave pública del receptor es el par (e = 3, n = 2491) y su clave secreta es d = 1595.

Proceso de cifrado en la entidad emisora con la clave pública del receptor "e"

Sea "m" un mensaje a cifrar con la clave pública del receptor donde "m" pertenece al conjunto:

$Z_n = \{0, 1, 2, 3, \ldots, n-1\}$,

por ejemplo m = 777. La entidad emisora elige de forma aleatoria un número "r" perteneciente a Z_n, por ejemplo r = 1089. Calcula el texto cifrado o criptograma utilizando la expresión:

$$c = [(1+m.n).r^e] \bmod n^2 =$$
$$[(1+777n).r^e] \bmod n^2 =$$
$$(1+777n).811121 \bmod n^2 =$$
$$2255901$$

Proceso de descifrado en la entidad receptora con su clave privada-secreta

El receptor calcula primero:

$r = c^d \bmod n = 1089$ y seguidamente determina el texto en claro aplicando la expresión:

$m = [(c \cdot r^e \bmod n^2 - 1) / n] = 777$

Síntesis de un criptosistema estilo D-H basado en funciones de traza sobre un campo de Galois de característica tres GF(2³)

Primero se construye un campo finito $GF(p^n)$ donde "p" es un número primo por ejemplo p = 2 y "n" es un número entero positivo, por ejemplo n = 3, es decir $GF(2^3)$.

Se elige un polinomio irreducible f(x) sobre GF(p) de grado "n" por ejemplo $f(x) = x^3+x + 1$. Sea α un elemento que satisface $f(\alpha) = 0$, en este caso $\alpha^3+ \alpha+1=0$; entonces $GF(2^3) = \{a_0+ a_1\alpha+ a_2\alpha^2\}$ donde a_i pertenece a GF(2). Se define la función traza Tr(x) de un elemento "x" de $GF(p^n)$ sobre GF(p) como una función de $GF(p^n)$ en GF(p) definida como:

$$Tr(x) = (x + x^p + \ldots + x^{p^{n-1}})$$

La función traza presenta entre otras la propiedad de función lineal y además $(x + y)^p = (x^p + y^p)$ para todo "x" e "y" perteneciente a $GF(p^n)$. La figura 3 muestra las tres representaciones de los elementos de $GF(2^3)$ como cadena de tres bits, como polinomio y como potencia de α.

En $GF(2^3)$ el producto de $(p^2+ 1)$ por $(p^2+ p + 1)$ módulo $(p^3+ p + 1)$ da como resultado $(p^2+ p)$.

A continuación se describe un cripto-sistema estilo D-H (Diffie-Hellman) basado en funciones de traza con subgrupos de campos finitos de extensión donde se pretende intercambiando entre los extremos de la comunicación A y B (a través de un canal no confidencial pero autenticado) un valor público, poder determinar un secreto ó clave común K:

1) La entidad emisora A guarda en secreto "a", por ejemplo a = 3 y envía a la entidad receptora B utilizando un canal autenticado pero no confidencial el valor:

$$Tr(\alpha^3) = \alpha^3+ \alpha^6+ \alpha^{12} =$$
$$(1+\alpha) + (1+\alpha^2) + \alpha^5 = 1$$

2) La entidad receptora B guarda en secreto "b", por ejemplo b=2 y envía a la entidad A utilizando un canal autenticado pero no confidencial el valor: $Tr(\alpha^2) = \alpha^2+ \alpha^4+ \alpha^8 = 0$.

3) La entidad A calcula en secreto la clave común o secreto compartido:

$$K = [Tr(\alpha^2)]^a = [\alpha+ \alpha^2+ \alpha^4]^3 =$$
$$\alpha^3+ \alpha^6+ \alpha^{12} = 1$$

4) La entidad B calcula en secreto la clave común o secreto compartido:

$$K = [Tr(\alpha^3)]^b = [\alpha+ \alpha^3]^2 = [\alpha^2+ \alpha^6] = 1$$

Dado $GF(2^3)$ definido por el polinomio $f(x) = x^3 + x + 1$ donde $f(\alpha) = 0$ se definen los siguientes elementos del campo $GF(2^3)$

COMO TUPLA DE TRES BITS	COMO POLINOMIO	COMO POTENCIA DE α
000	0	0
001	1	1
010	α	α
100	α^2	α^2
011	$1 + \alpha$	α^3
110	$\alpha + \alpha^2$	α^4
111	$1 + \alpha + \alpha^2$	α^5
101	$1 + \alpha^2$	α^6
	Si k >=7 ==> $\alpha^k = \alpha^g$ donde g es el resto de dividir k entre 7	$\alpha^7 = \alpha^0 = 1$
		$\alpha^8 = \alpha$
		$\alpha^9 = \alpha^2$

Figura 3. Tres representaciones de los elementos del campo finito $GF(2^3)$

Bibliografía

- Areitio, J. y Areitio, G. "Integración entre Políticas de Seguridad y Procedimientos de Seguridad". Revista Seguridad Informática. nº 8. Diciembre 1993.
- Areitio, J. "Diseño y Monitorización de Cripto-sistemas Simétricos". Revista Española de Electrónica. nº 595. Junio 2004.
- Areitio, J. Seguridad en la Transmisión Electrónica de Datos".Revista Española de Electrónica. nº 437. Abril 1991.