Criptografía con curvas hiperelípticas de género 2*

L. Hernández Encinas y J. Muñoz Masqué

Departamento Tratamiento de la Información y Codificación
Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas
C/ Serrano 144, 28006-Madrid
{luis,jaime}@iec.csic.es

Resumen. En el presente trabajo se presentan las clases de isomorfismo de las curvas hiperelípticas de género 2, que admiten un punto de Weierstrass. Dicha clasificación se ha llevado a cabo según que la característica del cuerpo sea 2, 5 o diferente de 2 y de 5. Esta clasificación tiene gran importancia desde el punto de vista de la criptografía. Como ejemplo de aplicación, se incluye un protocolo de firma digital con curvas hiperelípticas.

Palabras clave: Criptografía de clave pública, Cuerpos finitos, Curvas hiperelípticas, Clases de isomorfismo.

1 Introducción

Uno de los problemas matemáticos sobre el que se basa la seguridad de algunos de los más importantes criptosistemas y protocolos de clave pública utilizados hoy en día es el problema del logaritmo discreto (DLP) (ver [18,19,38]).

El mejor algoritmo conocido para resolver el DLP en $\mathbb{Z}_p^*$ es el de la criba general del cuerpo de números, GNFS (General Number Field Sieve, ver [1,2,7,14,15,46]), cuyo tiempo de ejecución esperado es *subexponencial*:

$$\exp((1{,}923 + o(1)) (\log p)^{\frac{1}{3}} (\log\log p)^{\frac{2}{3}}).$$

Con el fin de prevenir el ataque mediante el GNFS, se recomienda que p tenga una longitud de 1024–2048 bits, para una seguridad a corto-medio plazo.

Este tamaño hace inviable la implementación de protocolos basados en el DLP sobre $\mathbb{Z}_p^*$ si los entornos computacionales son restringidos, tales como tarjetas inteligentes, dispositivos localizadores o teléfonos móviles ([5]). Por esta razón, se han propuesto grupos alternativos a $\mathbb{Z}_p^*$, que deberían tener propiedades tan deseables como por ejemplo; que los elementos del grupo tengan una

* Trabajo financiado por el CDTI, Ministerio de Industria, Turismo y Comercio, en colaboración con Telefónica I+D con el proyecto SEGUR@, de referencia CENIT-2007 2004.

representación compacta de modo que se puedan representar como una única cadena de, aproximadamente, el número de bits del orden del grupo; que dada una representación de los elementos, se debería conocer un algoritmo eficiente para llevar a cabo la operación del grupo; o que con el fin de preservar la seguridad y confidencialidad de los protocolos, debería ser computacionalmente difícil resolver el DLP en dicho grupo.

Los principales grupos propuestos pueden verse en [6,19,24,35,32,33,37,40] y en [42,44,45,47,49,50,52,53]. Para estos grupos, la operación interna no es muy difícil de implementar y, además, el problema computacional subyacente es un problema considerado difícil ([23]).

Una de las propuestas más interesantes consiste en utilizar la estructura de grupo de la variedad jacobiana de una curva algebraica. Sin embargo, en estos casos existen algunos inconvenientes, por ejemplo, ¿cómo seleccionar un representante canónico para cada clase de divisores del jacobiano?, o dada la representación canónica de dos clases de divisores, ¿cómo computar de forma eficiente la representación canónica de las suma de tales clases de divisores?

Estas dificultades se pueden resolver adecuadamente si se emplean curvas hiperelípticas definidas sobre cuerpos finitos.

Si C es una curva hiperelíptica de género g sobre $\mathbb{F}_q$, entonces el orden del jacobiano de C sobre $\mathbb{F}_q$, $\mathcal{J}(C)$, es aproximadamente q^g (recuérdese que si $g = 1$, la curva es una curva elíptica, para la que ya existen propuestas claras y concretas de implementación, tanto para los procesos de firma como para los de cifrado). Los elementos del jacobiano de las curvas hiperelípticas pueden ser representados de forma compacta mediante un par de polinomios sobre $\mathbb{F}_q$ de grado, a lo más, g. Además, es posible utilizar el algoritmo de Cantor ([8]) para llevar a cabo su suma.

Con relación a la seguridad de los protocolos criptográficos basados en las curvas hiperelípticas de género $g > 1$, el DLP debe seguir siendo, al menos, tan seguro como para las curvas elípticas. De hecho, se sabe que cuando el género g de la curva es grande, existe un algoritmo subexponencial para el DLP en $\mathcal{J}(C)$ debido a Adleman, DeMarrais y Huang ([3], ver también [20,21,41]). Además, si $g \geq 4$ pero pequeño, existen algoritmos más rápidos que el algoritmo ρ de Pollard ([25,26,51]), pero aún de tiempo subexponencial.

Si $g = 2$ ó $g = 3$, el mejor algoritmo conocido para resolver el DLP sobre los jacobianos correspondientes requiere $O\left(\sqrt{p}\right)$ pasos, siendo p el mayor divisor primo del orden del jacobiano, $|\mathcal{J}(C)|$. Es decir, el algoritmo necesita tiempo exponencial. Por lo tanto, se puede utilizar una curva hiperelíptica de género 2 sobre el cuerpo finito $\mathbb{F}_q$, con $q \approx 2^{80}$, y lograr el mismo nivel de seguridad que cuando se usa el grupo de una curva elíptica $E(\mathbb{F}_q)$, con $q \approx 2^{160}$.

Una desventaja a la hora de emplear curvas de género 2 en lugar de curvas elípticas es que la operación del grupo en el primer caso es computacionalmente más cara que en el segundo ([31,43,48]).

2 Criptografía basada en curvas hiperelípticas de género 2

2.1 Curvas hiperelípticas

Sea $\bar{\mathbb{F}}$ la clausura algebraica del cuerpo finito $\mathbb{F} = \mathbb{F}_q$. Se define una *curva hiperelíptica* $C \in \mathcal{H}$ de género g sobre $\mathbb{F}$ como una curva proyectiva irreducible no singular de género g definida sobre $\mathbb{F}$ para la que existe una aplicación $C \to \mathbb{P}^1$ de grado 2. También se puede entender una curva hiperelíptica (sin puntos singulares) C de género g sobre $\mathbb{F}$ como una ecuación (de Wierstrass), $H \in \mathcal{W}$, de la forma ([34,36,39]):

$$H : y^2 + h(x)y = f(x), \tag{1}$$

donde $h(x) \in \mathbb{F}[x]$ es un polinomio de grado a lo sumo g, $f(x) \in \mathbb{F}[x]$ es un polinomio mónico de grado $2g+1$ y, además, no existen soluciones $(x, y) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$ que satisfagan simultáneamente las ecuaciones:

$$y^2 + h(x)y - f(x) = 0, \quad 2y + h(x) = 0, \quad h'(x)y - f(x) = 0.$$

La curva C tiene un único punto en el infinito $O = [0, 0, 1]$, llamado *punto de Weierstrass*, en las coordenadas homogéneas $x = x_1/x_0$, $y = x_2/x_0$. Además, O es un punto singular de multiplicidad $2g - 1$ y la recta del infinito $x_0 = 0$ es tangente a la curva en este punto.

En [9,10,17] se determinan las clases de isomorfismo de curvas hiperelípticas sin distinguir el punto del infinito.

2.2 Operaciones en el jacobiano

Una ventaja de las curvas hiperelípticas es que es relativamente sencillo sumar dos elementos de $\mathcal{J}(C)$. Este hecho viene determinado por la siguiente caracterización de los elementos del jacobiano de una curva hiperelíptica:

Teorema 1 (representación de Mumford, [13]). *Sea $C \in \mathcal{H}$ la curva hiperelíptica de género g sobre $\mathbb{F}_q$ dada por $H\colon y^2 + h(x)y = f(x)$ y sea $D \in \mathcal{J}(C)$, $D \neq 0$. Entonces D se puede representar mediante un único par de polinomios, $a(x), b(x) \in \mathbb{F}_q[x]$ de modo que*

1. *$a(x)$ es mónico.*
2. *$\mathrm{gr}(b) < \mathrm{gr}(a) \leq g$.*
3. *$a|(b^2 + hb - f)$.*

Esta representación de los elementos de $\mathcal{J}(C)$ mediante los llamados *divisores reducidos* se denota por $D = \mathrm{div}(a, b)$, por lo que los polinomios (a, b) se pueden considerar como las coordenadas de $D \in \mathcal{J}(C)$.

El algoritmo de Cantor ([8]) permite sumar dos divisores reducidos dados, $D_1 = \mathrm{div}(a_1, b_1)$, $D_2 = \mathrm{div}(a_2, b_2)$, dando como salida otro divisor reducido, $D_1 + D_2 = D = \mathrm{div}(a, b)$. El algoritmo escrito en pseudocódigo es el siguiente:

Entrada. Dos divisores $D_1 = (a_1, b_1)$ y $D_2 = (a_2, b_2)$ sobre C.
Salida. El único divisor reducido $D = (a, b)$ tal que $D = D_1 + D_2$.
$d_1 \leftarrow \mathrm{mcd}\,(a_1, a_2)\,,$ $[d_1 = e_1 a_1 + e_2 a_2]$
$d \leftarrow \mathrm{mcd}\,(d_1, b_1 + b_2 + h)\,,$ $[d = c_1 d_1 + c_2(b_1 + b_2 + h)]$
$s_1 \leftarrow c_1 e_1, \quad s_2 \leftarrow c_1 e_2, \quad s_3 \leftarrow c_2,$
$a \leftarrow (a_1 a_2)/d^2, \quad b \leftarrow (s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f))/d \pmod{a},$
`Repetir`
  $a' \leftarrow (f - bh - b^2)/a, \quad b' \leftarrow (-h - b) \pmod{a'},$
  $a \leftarrow a', \quad b \leftarrow b'$
`hasta` $(\mathrm{gr}(a) \leq g)$
`Hacer` a `mónico`
`return` $[a, b]$

En resumen, el algoritmo de Cantor proporciona un divisor semirreducido $D' = \mathrm{div}(a', b')$, de modo que si $\mathrm{gr}(a') \leq g$, el divisor D' es reducido y el algoritmo se para. En caso contrario, se ejecuta el segundo paso del algoritmo, obteniéndose el divisor reducido $D = \mathrm{div}(a, b) = D_1 + D_2$.

En el caso de curvas de género 2 sobre cuerpos de característica 2, el número máximo de operaciones en el cuerpo base necesarias para obtener el divisor reducido, suma de otros dos dados, ha sido calculado en [27].

2.3 Protocolo de firma digital (HECDSA)

Como es bien sabido, de entre los diferentes tipos de curvas algebraicas propuestos para su uso criptográfico, sólo el esquema de firma digital para curvas elípticas se ha convertido en un estándar (ECDSA, ver [4]). El protocolo de firma digital para curvas hiperelípticas es, por tanto, una generalización del esquema ECDSA, que llamaremos HECDSA.

Los parámetros del protocolo HECDSA son los siguientes: $(\mathbb{F}_q, C, D, n, p)$, donde $\mathbb{F}_q$ es el cuerpo base, C es la curva hiperelíptica, $n = |\mathcal{J}(C)|$ es el orden del grupo y $D \in \mathcal{J}(C)$ es el punto base del sistema, cuyo orden es un primo grande, p, con $p|n$.

Supondremos que los elementos de $\mathcal{J}(C)$ admiten una representación de Mumford y que los elementos del cuerpo finito $u \in \mathbb{F}_q$ están ordenados de modo que $0 \leq L(u) < q$ es un entero asociado de modo único a u, de forma invertible. Sea $\mathfrak{h}$ una función resumen, y sean a la clave privada del usuario A y D_A su clave pública, es decir, el producto de a por D: $D_A = [a]D \in \mathcal{J}(C)$.

El algoritmo, HECDSAg, de generación de firma para un mensaje M es:

Entrada. Parámetros del sistema: $(\mathbb{F}_q, C, D, n, p)$, clave privada: a, función resumen: $\mathfrak{h}$, y mensaje: M.
Salida. Firma digital (F, s) de M.
`Repetir`
  `Repetir`
    `generar aleatoriamente` $r \in [0, p-1]$

$E \leftarrow [r]D$, $[E = (u, v), u = x^t + \sum_{i=0}^{t-1} u_i,$ `para algún` $t \leq g]$
$F \leftarrow \sum_{i=0}^{t-1} L(u_i)q^i \pmod p$,
`hasta` $(F \neq 0, 1)$
$s \leftarrow r^{-1}(\mathfrak{h}(M) - [a]F) \pmod p$,
`hasta` $(s \neq 0)$
`return` (F, s)

Una vez elaborada la firma, la verificación de la misma se lleva a cabo mediante el algoritmo correspondiente, HECDSAv:

Entrada. Parámetros del sistema: $(\mathbb{F}_q, C, D, n, p)$, clave pública: D_A, función resumen: $\mathfrak{h}$, mensaje: M y posible firma digital de M: (F, s).
Salida. Aceptación o Rechazo de la firma.
`if` $(F \notin [0, p-1]$ `or` $s \notin [0, p-1])$ `then return ‘‘Rechazo’’`
`else` $w \leftarrow s^{-1} \pmod p$
$u_1 = \mathfrak{h}(M)w \pmod p$, $u_2 = Fw \pmod p$,
$G = [u_1]D \oplus [u_2]D_A$, $[G = (u, v)]$
`if` $(G = 0)$ `then return ‘‘Rechazo’’`
`else` $F_1 = \sum_{i=0}^{t-1} L(u_i)\, q^i \pmod p$, $[u = x^t + \sum_{i=0}^{t-1} u_i,$ `para algún` $t \leq g]$
`if` $(F = F_1)$ `then return ‘‘Aceptación’’`
`else return ‘‘Rechazo’’`

3 Clasificación de curvas hiperelípticas de género 2

3.1 Formas normales de curvas hiperelípticas en $\mathcal{H}$

Como es sabido, para cada curva hiperelíptica $C \in \mathcal{H}$ de género g, existe una ecuación de Weierstrass $H \in \mathcal{W}$ y un morfismo birracional $C \to H$. Por tanto, para contar el número de clases de isomorfismo en $\mathcal{H}$ basta con contar el número de clases de equivalencia en $\mathcal{W}$. En efecto, se tiene:

Proposición 1 ([36]). *Existe una correspondencia 1-1 entre clases de isomorfismo de curvas hiperelípticas en $\mathcal{H}$ y clases de equivalencia de ecuaciones de Weierstrass en $\mathcal{W}$, donde $H, \bar{H} \in \mathcal{W}$ se dice que son equivalentes sobre $\mathbb{F}_q$ si existen $\alpha, \beta \in \mathbb{F}_q$, $\alpha \neq 0$, y $t \in \mathbb{F}_q[x]$, $\mathrm{gr}(t) \leq 2$, tal que el cambio de coordenadas*

$$(x, y) \mapsto (\alpha^2 x + \beta, \alpha^5 y + t)$$

transforma la ecuación H en la ecuación $\bar{H}$.

La ecuación (1) que define una curva hiperelíptica H de género 2 es única salvo un cambio de coordenadas de la siguiente forma ([36]):

$$(x, y) \mapsto \left(\alpha^2 x + \beta, \alpha^5 y + \alpha^4 \gamma x^2 + \alpha^2 \delta x + \epsilon\right),$$

donde $\alpha \in \mathbb{F}_q^*$ y $\beta, \gamma, \delta, \epsilon \in \mathbb{F}_q$.

3.2 Clases de isomorfismo en $\mathcal{H}$ si $\mathbf{char}(\mathbb{F}_q) \neq 2, 5$

En esta sección se determinan las clases de isomorfismo de las curvas hiperelípticas de género 2 para el caso particular en que la característica del cuerpo base, $\mathbb{F}_q$, no sea ni 2 ni 5.

Teorema 2 ([28, Proposition 2, Theorem 5]). *Se verifica lo siguiente:*
(i) *En característica diferente de* 2 *y* 5*, toda curva hiperelíptica de género* 2 *puede ser representada por una ecuación de la forma siguiente:*

$$y^2 = x^5 + a_4x^3 + a_6x^2 + a_8x + a_{10}.$$

(ii) *El número de clases de isomorfismo de curvas hiperelípticas de género* 2 *sobre* $\mathbb{F}_q$ *con* $\mathrm{char}(\mathbb{F}_q) \neq 2, 5$*, es*

$$2q^3 + r(q)$$

donde $r(q)$ *viene dado por el siguiente cuadro:*

$r(q)$	$q \equiv 1 \pmod 8$	$q \not\equiv 1 \pmod 8, q \equiv 1 \pmod 4$	$q \not\equiv 1 \pmod 4$
$q \equiv 1 \pmod 5$	$2q + 10$	$2q + 6$	8
$q \not\equiv 1 \pmod 5$	$2q + 2$	$2q - 2$	0

3.3 Clases de isomorfismo en $\mathcal{H}$ si $\mathbf{char}(\mathbb{F}_q) = 2$

A continuación se calcula el número de clases de isomorfismo de curvas hiperelípticas de género 2 sobre un cuerpo finito de característica 2, $\mathbb{F}_{2^m}$.

Como $\mathrm{char}(\mathbb{F}_{2^m}) = 2$, se tiene que $h(x) = a_1x^2 + a_3x + a_5 \neq 0$ (ver [39]). Por tanto, se deben considerar los siguientes tipos de curvas:

Tipo I: $a_1 \neq 0$; Tipo II: $a_1 = 0$, $a_3 \neq 0$; y Tipo III: $a_1 = a_3 = 0$, $a_5 \neq 0$.

Teorema 3 ([11]). *Se verifica lo siguiente:*
(i) *Cada curva hiperelíptica de género* 2 *de Tipo I sobre* $\mathbb{F}_{2^m}$ *puede representarse por una ecuación de la forma*

$$y^2 + (x^2 + a_3x + a_5)y = x^5 + a_8x + a_{10}.$$

(ii) *El número de clases de isomorfismo de curvas hiperelípticas de género* 2 *de Tipo I sobre* $\mathbb{F}_{2^m}$ *es*

$$(q-1)\left(2q^2 + q - 2\right), \quad q = 2^m.$$

Teorema 4 ([12]). *Se verifica lo siguiente:*
(i) *Cada curva hiperelíptica de género* 2 *de Tipo II sobre* $\mathbb{F}_{2^m}$ *puede ser representada por una ecuación de la forma*

$$y^2 + a_3xy = x^5 + a_4x^3 + a_6x^2 + a_{10}, \quad a_3 \neq 0.$$

(ii) *El número de clases de isomorfismo de curvas hiperelípticas de género* 2 *de Tipo II sobre* $\mathbb{F}_{2^m}$ *es*

$$2q(q-1), \quad q = 2^m.$$

Teorema 5 ([16]). *Se verifica lo siguiente:*
(i) *Cada curva hiperelíptica de género* 2 *de Tipo III sobre* $\mathbb{F}_{2^m}$ *puede ser representada por una ecuación de la forma*

$$y^2 + a_5 y = x^5 + a_4 x^3 + a_8 x + a_{10}, \quad a_5 \neq 0.$$

(ii) *El número de clases de isomorfismo de curvas hiperelípticas de género* 2 *de Tipo III sobre* $\mathbb{F}_q$, *con* $q = 2^m$ *es:*

$$4q - 2, \ \textit{si } 4 \nmid m, \qquad 4q + 6, \ \textit{si } 4 | m.$$

Corolario 1. *El número de clases de isomorfismo de curvas hiperelípticas de género* 2 *sobre* $\mathbb{F}_q$, *con* $q = 2^m$, *es el siguiente:*

$$q(q+1)(2q-1), \ \textit{si } 4 \nmid m, \qquad 2q^3 + q^2 - q + 8, \ \textit{si } 4 | m.$$

3.4 Clases de isomorfismo en $\mathcal{H}$ si $\mathbf{char}(\mathbb{F}_q) = 5$

Teorema 6 ([29,30]). *Se verifica lo siguiente:*
(i) *Toda curva hiperelíptica de género* 2 *sobre* $\mathbb{F}_{5^m}$ *puede ser representada por una y sólo una de las siguientes ecuaciones:*

$$\begin{aligned}
y^2 &= x^5 + a_2 x^4 + a_6 x^2 + a_8 x + a_{10}, \quad a_2 \in \mathbb{F}_{5^m}^*, \\
y^2 &= x^5 + a_4 x^3 + a_8 x + a_{10}, \quad a_4 \in \mathbb{F}_{5^m}^*, \\
y^2 &= x^5 + a_6 x^2 + a_{10}, \quad a_6 \in \mathbb{F}_{5^m}^*, \\
y^2 &= x^5 + a_8 x + a_{10}, \quad a_8 \in \mathbb{F}_{5^m}^*.
\end{aligned}$$

(ii) *El número de clases de isomorfismo de curvas hiperelípticas de género* 2 *sobre un cuerpo* $\mathbb{F}_q$, *con* $q = 5^m$, *es*

$$2q^3 + 2q + 4, \ \textit{si } m \textit{ es par}, \qquad 2q^3 + 2q, \ \textit{si } m \textit{ es impar}.$$

4 Conclusiones

En este trabajo se han presentado las clases de equivalencia de las curvas hiperelípticas de género 2, que admiten un punto de Weierstrass. Dicha clasificación se ha llevado a cabo teniendo en cuenta si la característica del cuerpo es 2, 5 o diferente de 2 y de 5.

Se ha determinado el número de curvas hiperelípticas que existen en cada uno de los casos mencionados, lo que tiene gran importancia desde el punto de vista de la criptografía, dado que para la implementación de posibles criptosistemas o protocolos de firma digital basados en tales curvas, esta clasificación permite conocer "a priori" el número de curvas "diferentes" de que se dispone.

Sería de gran interés poder llevar a cabo, en el futuro, implementaciones prácticas de protocolos criptográficos basados en curvas hiperelípticas con el fin de evaluar de forma clara su aplicabilidad criptográfica.

Referencias

[1] L. Adleman. A subexponential algorithm for discrete logarithm problem with applications to cryptography. *Proc. 20th IEEE Found. Comp. Sci. Symp.*, 55–60, 1979.

[2] L. Adleman and J. DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. *Math. of Comp.*, 61: 1–15, 1993.

[3] L. Adleman, J. DeMarrais and M. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. *LNCS*, 877: 28–40, 1994.

[4] American National Standards Institute. *Public key cryptography for the financial services industry: The elliptic curve digital signature algoritm* (ECDSA), ANSI X9.62-1998.

[5] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes. PGP in constrained wireless devices. *Proceedings of the Ninth USENIX Security Symposium*, 247–261, 2000.

[6] J. Buchmann and H. Williams. A key-exchange system based on imaginary quadratic fields. *J. Cryptology*, 1: 107–118, 1988.

[7] J.P. Buhler, H.W. Lenstra Jr. and C. Pomerance. Factoring integers with the number field sieve. *The development of the number field sieve*, LNM 1554, 50–94, Springer-Verlag, 1993.

[8] D. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comput.*, 48: 95–101, 1987.

[9] G. Cardona. On the number of curves of genus 2 over a finite field. *Finite Fields Appl.*, 9: 505–526, 2003.

[10] G. Cardona, E. Nart, and J. Pujolàs. Curves of genus two over fields of even characteristic. Available from `http://arxiv.org/abs/math.NT/0210105`.

[11] Y. Choie and E. Jeong. Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_{2^n}$. *Cryptology ePrint Archive* 2003/213.

[12] Y. Choie and D. Yun. Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_q$. *LNCS*, 2384: 190–202, 2002.

[13] H. Cohen and G. Frey. *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman & Hall/CRC, Boca Raton, FL, 2006.

[14] D. Coppersmith. Fast evaluation of logarithms in finite fields of characteristic two. *IEEE Trans. Inform. Theory*, 30(4): 587–594, 1984.

[15] D. Coppersmith, A. Odlyzko, and R. Schroeppel Discrete logarithms in $GF(p)$. *Algorithmica*, 1: 1–15, 1986.

[16] Y. Deng and M. Liu. Isomorphism classes of hyperelliptic curves of genus 2 over finite fields with characteristic 2 *Science in China, Ser. A*, 49(2): 173–184, 2005.

[17] C. Dermirkiran and E. Nart. Counting hyperelliptic curves that admit a Koblitz model. *J. Math. Crypt.*, 1: 1–17, 2007.

[18] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, 22: 644–654, 1976.

[19] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithm. *IEEE Trans. Inform. Theory*, 31, 469–472, 1985.

[20] A. Enge. Computing discrete logarithms in high-genus hyperelliptic jacobians in probably subexponential time. *Math. Compt.*, 71: 729–742, 2002.

[21] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arithmetica*, 1: 83–103, 2202.

[22] J. Espinosa García, L. Hernández Encinas, and J. Muñoz Masqué. A review on the isomorphism classes of hyperelliptic curves of genus 2 over finite fields admitting a Weierstrass point. *Acta Appl. Math.*, 93: 299–318, 2006.

[23] S. Galbraith and A. Menezes. Algebraic curves and cryptography. *Finite Fields Appl.* 11: 544–577, 2005.

[24] S. Galbraith, S. Paulus, and N. Smart. Arithmetic of superelliptic curves. *Math. Comp.*, 71: 393–405, 2002.

[25] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. *LNCS*, 1807: 19–34, 2000.

[26] P. Gaudry, N. Thériault, and E. Thomé. A double large prime variation for small genus hyperelliptic index calculus. *Cryptology ePrint Archive*, 2004/153.

[27] L. Hernández Encinas, A.J. Menezes y J. Muñoz Masqué. Algunas propiedades de las curvas hiperelípticas de género 2 sobre un cuerpo finito de característica 2 y su uso criptográfico. *Actas de la V Reunión Española de Criptología y Seguridad de la Información (V RECSI)*, 155–166, 1998.

[28] L. Hernández Encinas, A.J. Menezes, and J. Muñoz Masqué. Isomorphism classes of genus-2 hyperelliptic curves over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 13: 57–65, 2002.

[29] L. Hernández Encinas and J. Muñoz Masqué. Isomorphism classes of hyperelliptic curves of genus 2 in characteristic 5. *Technical Report CORR2002-07*, Centre For Applied Cryptographic Research (CACR), University of Waterloo, 2002.

[30] ——. Isomorphism classes of genus-2 hyperelliptic curves over finite fields $\mathbb{F}_{5^m}$. *Information*, 8(6): 8 pp., 2005.

[31] M. Jacobson Jr., A. Menezes, and A. Stein. Hyperelliptic curves and cryptography. *Technical Report CORR 2003-13*, Centre for Applied Cryptography Research (CACR), University of Waterloo, 2003.

[32] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48: 203–209, 1987.

[33] ——. Hyperelliptic cryptosystems. *J. Cryptology*, 1: 139–150, 1989.

[34] ——. *Algebraic aspects of cryptography.* Springer, Berlin, 1998.

[35] K. Kurosawa, T. Ito, and M. Takeuchi. Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number. *Cryptologia*, 12: 225–233, 1988.

[36] P. Lockhart. On the discriminant of a hyperelliptic curve. *Trans. Amer. Math. Soc.* 342(2): 729–752, 1994.

[37] K. McCurley. A key distribution system equivalent to factoring. *J. Cryptology*, 1: 95–105, 1998.

[38] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of applied cryptography*. CRC Press, Boca Raton, FL, 1997.

[39] A. Menezes, Y. Wu, and R. Zuccherato. An elementary introduction to hyperelliptic curves. In N. Koblitz, *Algebraic aspects of cryptography*, Springer, Berlin, 155–178, 1998.

[40] V. Miller. Uses of elliptic curves in cryptography. *LNCS*, 218: 417–426, 1986.

[41] V. Müller, A. Stein, and C. Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Math. Comp.*, 68: 807–822, 1999.

[42] National Institute for Standards and Technology. Digital Signature Standard (DSS). *FIPS PUB*, 186: 1993; 186-2: 2000.

[43] M. Petersen. Hyperelliptic cryptosystems. *Technical Report*, University of Aarhus, Denmark, 1994.

[44] M.O. Rabin. Digitalized signatures and public key functions as intractable as factorization. *Technical Report TM-212*, Lab. for Computer Science, M.I.T., 1979.

[45] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21: 120–126, 1978.

[46] O. Schirokauer, D. Weber, and T. Denny. Discrete logarithms: the effectiveness of the index calculus method. *LNCS*, 1122: 337–361, 1996.

[47] C. Schnorr. Efficient signature generation by smart cards. *J. Cryptology*, 4: 161–174, 1991.

[48] N. Smart. On the performance of hyperelliptic cryptosystems. *LNCS*, 1592: 165–175, 1999.

[49] T. Takagi. Fast RSA-type cryptosystems using N-adic expansion. *LNCS*, 1294: 372–384, 1997.

[50] ——. Fast RSA-type cryptosystem modulo $p^k q$. *LNCS*, 1462: 318–326, 1998.

[51] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. *LNCS*, 2894: 75–92, 2003.

[52] H.C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Trans. Inform. Theory*, 26: 726–729, 1980.

[53] ——. An M^3 public-key encryption scheme. *LNCS*, 218: 358–368, 1986.