Industria y Comercio

SUPERINTENDENCIA

Delegatura de propiedad Industrial

División de Nuevas Creaciones

SOLICITUD

PATENTE DE INVENCIÓN

21. **EXPEDIENTE No.** 04-94973

54. **TÍTULO** Uso de Isogenas para el Diseño de criptosistemas

51. **CLASIFICACIÓN INTERNACIONAL** H04K 1/00 H04L 9/30

71. **SOLICITANTE** Microsoft - corporation

DOMICILIO Redmond, Washington, Estados Unidos de America.

74. **APODERADO** Dario Cardenas Novas

22. **BOGOTÁ, D. C.,**

(FORMA P-10)

PETITORIO

Industria y Comercio
SUPERINTENDENCIA

SUPERINDUSTRIA Y COMERCIO
Radicacion : 04094973 00000000 Folios: 79
Fecha (DMA): 2004-09-23 17:01:36
Tramite : 002 PATENTES D 1 REGISTRO/ 411 PRESENTA
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

FORMULARIO UNICO DE SOLICITUD DE PATENTE
2000-3

SOLICITUD DE:

[X] Patente de Invención [ ] Patente de Modelo de Utilidad

			IDENTIFICACION
SOLICITANTE (71)	Nombre:	MICROSOFT CORPORATION	
	Dirección:	One Microsoft Way Redmond, Washington 98052, Estados Unidos de America	C.C. [ ] NIT [ ]
	Teléfono:	3123600 Fax: 3122410	C.E. [ ] Otro [X]
	E-Mail:	general@cardenasycardenas.com	
	Lugar de Constitución	Estado de Washington, Estados Unidos de América	Número
	Domicilio:	REDMOND, WASHINGTON, ESTADOS UNIDOS DE AMERICA.	
REPRESENTANTE O APODERADO (74)	Nombre:	DARIO CARDENAS NAVAS	IDENTIFICACION
	Dirección:	Carrera 7 No 71-52 Torre B Piso 9	C.C. [X] NIT [ ]
	Teléfono:	3123600 Fax: 3122410	C.E. [ ] Otro [ ]
	E-Mail:	general@cardenasycardenas.com	Número 17.086.629 BTA TP 1.250 C.S.J.
INVENTOR(ES) (72)	Nombre:	1. David Y Jao 2. Ramarathnam Venkatesan	IDENTIFICACION
	Dirección:	1. One Microsoft Way Redmond, Washington 98052, Estados Unidos de America 2. One Microsoft Way Redmond, Washington 98052, Estados Unidos de America	C.C. [ ] NIT [ ]
	Teléfono:	3123600 Fax: 3123600	C.E. [ ] Otro [X]
	E-Mail:	general@cardenasycardenas.com	Número
	Domicilio:	1. WASHINGTON, ESTADOS UNIDOS DE AMERICA 2. WASHINGTON, ESTADOS UNIDOS DE AMERICA	

Título(54):

USO DE ISOGENOS PARA EL DISEÑO DE CRIPTOSISTEMAS

Prioridad SI [X] NO [ ]

(33)País de Origen	(32)Fecha	(31)N° de Solicitud
Estados Unidos de América	Noviembre 3, 2003	60/517142
Estados Unidos de América	Marzo 31, 2004	10/816063

Para publicar a partir de la fecha de la presente solicitud a los:

[ ] 6 meses [ ] 12 meses [ ] 18 meses [ ] Otro

AMR/JAG/amg

2

Comprobante de Pago No.: 04-75,287 / 04-75,289 Fecha Sept. 22, 2004

ANEXOS

- [X] Comprobante de pago de la tasa de presentación de la solicitud. (No 04-75,287)
- [X] Comprobante de pago de la tasa por concepto de excedente de palabras en la publicación.
- [X] Comprobante de pago de la tasa por concepto de reivindicación de prioridad. (No 04-75,289)
- [X] Poderes, si fuere el caso. (Protocolo No 16.069)
- [X] Certificado de existencia y representación legal cuando el solicitante sea persona jurídica. Protocolo No 16.069)
- [ ] Copia certificada de la primera solicitud, si se reivindica prioridad.
- [ ] Traducción simple de la primera solicitud, si se reivindica prioridad.
- [ ] Documento de cesión del inventor al solicitante o a su causante.
- [X] Descripción de la invención.
- [X] Una o más reivindicaciones.
- [X] Dibujos y/o planos necesarios.
- [ ] De ser el caso, copia del contrato de acceso.
- [ ] De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de la comunidad de las comunidades indígenas.
- [ ] De ser el caso, certificado de depósito del material biológico.
- [X] Arte final 12x12 y 6x6 cm.
- [X] Resumen y extracto para publicación.

10

NOMBRE: DARIO CARDENAS NAVAS

FIRMA:

C.C. 17.066.629 BTA TP. 1.250 C.S.J.

3

SUPERINTENDENCIA Y COMERCIO Folios: 79
Radicacion : 04094973 00000000
Fecha (AMD): 2004-09-23 17:01:36
Tramite 1 000 PATENTES D 1 REGISTRO/ 411 PRESENTA
Dependencia: 2000 DIVISION DE NUEVAS CREACIONES

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 04 - 75,287
FECHA : SEPTIEMBRE 22 DE 2004

C O N S I G N A C I O N

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
CARDENAS Y CARDENAS P.I.	CONSIGNACION	BANCO POPULAR	050-00110-6	21338251	22/09/2004	2,571,000.00

C O N C E P T O

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	30005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE IN	422,000.00
		TOTAL : $	422,000.00

SON: CUATROCIENTOS VEINTIDOS MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No._____

USO DE ISOGENOS PARA EL DISEÑO DE CRIPTOSISTEMAS.

CARDENAS & CARDENAS
ABOGADOS

4

SUPERINDUSTRIA Y COMERCIO
Radicacion : 04094973 00000000 Folios: 79
Fecha (AMD): 2004-09-23 17:01:36
Tramite : 002 PATENTES D 1 REGISTRO/ 411 PRESENTAC
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 04 - 75,299
FECHA : SEPTIEMBRE 22 DE 2004

C O N S I G N A C I O N

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
CARDENAS Y CARDENAS P.I.	CONSIGNACION	BANCO POPULAR	050-00110-6	24338251	22/09/2004	2,571,000.00

C O N C E P T O

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01 SOLICITUDES	82 INVOCACION DE UNA PRIORIDAD EN NU	118,000.00
		TOTAL : $	118,000.00

SON: CIENTO DIEZ Y OCHO MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No._____

USO DE ISOGENOS PARA EL DISEÑO DE CRIPTOSISTEMAS

CARDENAS & CARDENAS ABOGADOS

4

US DE IS GEN S PARA EL DISEÑO DE CRIPTOSISTEMAS

APLICACIÓN RELACIONADA

[0001] La aplicación presente. demanda prioridad de la patente provisional del número de aplicación 60/517,142 de los Estados Unidos, archivado el 3 de noviembre de 2003, titulado "USO DE ISOGENOS PARA EL DISEÑO DE CRIPTOSISTEMAS," el descubrimiento que está incorporado aquí por referencia.

CAMPO TECNICO

[0002] La invención presente generalmente relaciona la criptografía, y más particularmente, la utilización de isógenos para el diseño de criptosistemas.

FUNDAMENTO

[0003] Como la comunicación digital se hace más común, la necesidad por afianzar los canales de comnicación asociado se vuelven incrementalmente más importantes. Por ejemplo, las tecnologías actuales le permiten a una usuaria acceder remótamente cuentas bancarias, datos médicos, y otra información privada y sensible.

[0004] La Criptografía se ha usado para proporcionar ampliamente seguridad en la comunicación digital. La Criptografía generalmente relaciona el cifrado (o encriptación) y descifrado (descencriptado) de mensajes. La encriptación y la descencriptaación utiliza alguna información confidencial (como una llave). En los métodos de encriptación diferentes, pueden usarse una sola o múltiples llaves para el encriptación y decryption.

[0005] Una llave múltiple de cryptosystem normalmente usada es una llave pública del sistema de encripción. En un sistema de llave pública, un remitente que desea enviar un mensaje encriptado a un destinatario obtiene una llave pública autenticada para el destinatario que se genera usando una llave privada. Como el nombre lo indica, la llave pública está disponible de fuentes públicas. Es más, para evitar un ataque no personal, la llave pública se autentica a menudo. La autenticación de llave pública puede hacerse por una técnica como intercambiar las llaves sobre un canal de confianza, usando un archivo público de confianza, usando un servidor de confiada en línea, o usando un servidor fuera de línea y certificades.

[0006] Después de obtener la llave pública autenticada, el remitente encripta un mensaje original con la llave pública y genera una clave cifrada. El destinatario intencional utiliza entonces la llave private codifican ara descifrar la clave cifrada para extraer el mensaje original. Se cree que descifrando la clave cifrada sin el

acceso a la llave privada no es factible. De acuerdo solo con una parte que tiene acceso a la llave privada puede sastifactoriamente descifrar la clave cifrada.

[0007] Una significante ventaja de los sistemas de clave pública por encima de los criptosistemas simétricos (como un flujo o bloque de cifras) es que en las comunicaciones de dos-partes, solo las necesidades importantes privadas son guardadas confidencialmente (mientras que en el criptosistema simétrico, la llave se mantiene confidencial en ambos extremos).

[0008] Un sistema de encriptación actual de clave pública utiliza ciertas curvas elípticas (ECs) sobre un campo finito. Un Patr de valores publicados derivados de una curva elíptica se utilizan como una llave pública (incluso los puntos en la curva y su llave pública correspondiente que se generan por un multiplicación simple (es decir, multiplicación del entero) en la curva). La verificación es hecha usando una doble línea que empareja sobre la curva.

[0009] Generalmente, se cree que las curvas elípticas proporcionan los relativamente más bajos requisitos de la comunicación a los sistemas de encriptación que los sistemas tradicionales como RSA (Rivest, Shamir, y Adieman la tecnología de encriptación importante pública), mientras se mantienen niveles de seguridad similares.

[0010] Una impresión con los sistemas de encriptación de llave pública actuales es que se ha demostrado que ninguno está seguro. Como resultado, la seguridad de sistemas de encriptación de llave pública actuales esta presuntamente basado en la dificultad de un conjunto de problemas teóricos.
[0011] Los sistemas de encriptación de llave pública son más deseados porque proporcionan seguridad adicional.

RESUMEN

[0012] Se descubren las técnicas para proporcionar los sistemas de encriptación de clave pública. Más particularmente, isógenos de variedades de Abelian (e.g -, curvas elípticas en los casos uni-dimensionales) se utilizan para proporcionar los sistemas de encriptación de llave pública. Por ejemplo, los isogenos permiten el uso de curvas múltiples en lugar de una sola curva, proporcionando la encriptación más segura. Las técnicas pueden aplicarse a las firmas digitales y/o identidad basados en las soluciones de encriptación (IBE). Además, pueden usarse los isogenos en otras aplicaciones como las firmas invisibles, los sistemas jerárquicos, y similares. Adicionalmente, se descubren las soluciones para generar el isógeno.

[0013] En una implementación descrita, un método incluye la publicación de una llave pública que corresponde a un isógeno. Además el método incluye el descifrando y cifrado de un mensaje que usa una llave de descencripción que corresponde al isogeno (por ejemplo, es su isogeny dual).

BREVE DESCRIPCIÓN DE LAS GRAFICAS

[0014] La descripción detallada se hace con referencia a las figuras incluidas. En las figuras, los dígitos más a la izquierda del número de referencia identifican la figura en la cual aparece primero el número de la referencia. El uso de los mismos números de referencia en las diferentes figuras indican ítems similares o idénticos.

[0015] La fig. 1 ilustra un método ejemplar para usar el isogeno en un cryptosystem (criptosistema).

[0016] La fig. 2 ilustra un mapa ejemplar de un isogeno entre dos curvas.

[0017] La fig. 3 ilustra un método ejemplar para firmar un mensaje utilizando isogenos.

[0018] La fig. 4 ilustra un mapa ejemplar de un isogeno entre múltiples curvas.

[0019] La fig. 5 ilustra un método ejemplar para la identidad basado en la encriptación (IBE) usando isogenos.

[0020] La fig. 6 ilustra una computadora general de ambiente 600 que puede usar para llevar a cabo las técnicas descritas aquí.

DESCRIPTION DETALLADA

[0021] La discusión siguiente asume que el lector está familiarizado con las técnicas de criptografía. Para una introducción básica de criptografía, el lector es dirigido al texto escrito por A. Menezes, P. Van Oorschot, y S. Vanstone titulado, "Manual de Criptografía Aplicada" quinta edición (agosto de 2001), publicó por la Prensa CRC.

[0022] El descubrimiento siguiente describe las técnicas para mejorar los sistemas de llave pública que son basados en el múltiples curvas elípticas (o variedades de Abelian en general). Se descubren varias técnicas para el generador de isogenos (o cartografías) entre las curvas. Los isogenos generados permiten uso de curvas múltiples en lugar de la sola curva para proporcionar la encriptación pública. Además, las técnicas pueden aplicarse a las firmas digitales relativamente cortas (por ejemplo, tecleó "en" por un usuario o envió sobre un canal de ancho de banda bajo) y/o identidad basada en las soluciones de encriptación (IBE) (por ejemplo, permitiendo las llaves públicas memorizables). Las firmas cortas pueden también proporcionar eficiencia adicional a través de la verificación agregada.

[0023] APRECIACIÓN GLOBAL DE CRYPT SISTEMS C N ISOGEN S

[0024] La fig. 1 ilustra un método ejemplar 100 para usar el isogenos en un criptosistema. Una fase 102 genera isogenies (de curvas elípticas, o más generalmente las variedades de Abelian). Los isogenies pueden generarse por una parte receptor u otra parte (tal como una paerte de confianza más discutida con referencia a la figura 5.

La fase 102 puede también generar el correspondiente isogeno dual para cada uno de los isógenos generados (como se discutirá más debajo). Varios métodos para el isogenos generador se detallan debajo bajo el mismo título. Adicionalmente, como será más detallado con referencia a los Higos. 3 y 5, los isogenos generados se utilizan para proporcionar llaves públicas y las llaves públicas se publican (104). Las llaves públicas pueden publicarse enviando una parte o una autoridad de confianza (vea, por ejemplo, la discusión de las Figs. 3 y 5).

[0025] Una parte enviada encripta entonces mensajes (o señales) que usan una llave de encriptación (106). Los mensajes encriptados en la fase 106 pueden ser verificados/desencriptados por la parte receptora usando una llave de decryption para determinar la autenticidad de la encriptación o de la firma (108). En una implementación, La paridad Weil se utiliza para verificar los mensajes encriptados (como se discutió bajo el mismo título). Sin embargo, el emparejamienmto Weil es solo un ejemplo de emparejar que puede ser utilizado para la comprobación o descripción. Por ejemplo, otra doble línea y/o no-degenerada técnicas de emparejamiento pueden utilizarse como el emparejamiento de Tate y el emparejamientio caudrado.

[0026] APRECIACIÓN GLOBAL DE ISOGENOS

[0027] La fig. 2 ilustra un mapa ejemplar de un isogeno 200 entre dos curvas (por ejemplo, las curvas elípticas). Como se ilustran, una curva E1 puede trazarse sobre una curva E2 por un isogeno Ø (donde Ø: E1–>E2). La Fig. 1 también ilustra el isogeno Ø dual (donde Ø: E1–>E2)

[0028] En varias implementaciones, usando isogenos en cryptosistemas se prevee para proporcionar las propiedades tales como: dada una curva E1, generando un par (Ø, E2) es relativamente eficiente dónde Ø: E1–>E2 es un isogeno, pero dado un par E1,E2) de curvas isógenas, se cree que es relativamente difícil construir cualquier isogeny no cero (nonzero) Ø: E1–>E2, mucho menos un isogeno específico. Por consiguiente, si una distinción es arrastrado entre una interrupción global (definido como un cómputo que permite romper cualquier mensaje subsecuente en el tiempo polinómico) y una

interrupción por instancia, entonces los mejores ataques conocidos en este momento contra el isogeno basado en los criptosistemas toman cualquiera substancialmente más tiempo que el registro discreto para una interrupción global o sino un cómputo de registro discreto por el mensaje para el ataque por instancia.

[0029] Por ejemplo, considerado un sistema de anillo dónde cada cliente se da a un mensaje firmado específico que concede el acceso a algún servicio (que pueden ser de bajo valor), el cliente puede tener que leer el anillo encima del teléfono a un representante, y además las firmas pueden ser relativamente cortas. Será razonable usar parámetros que son lo suficinetemente grande para hacer un el ataque por mensaje más costoso que el servicio proporcionado, mientras guarda un descanso global prohibitivamente caro.

[0030] **DETALLES DE LOS ISOGENOS**

[0031] Un campo *k* puede ser fijado con carácterísticas *p* con *q* elementos y teniendo un procedimiento algebráico k. Dejemos *E/k* ser una curva elíptica definida sobre el campo *k* y *E(k)* ser un grupo definido sobre *k*, dejemos k(E) denotada como el campo de función de la curva elíptica. También, dejemos *[n]*$_E$ ó *[n]* note el mapa *P* --> *n* * *P* sobre *E* y *E[n]* note el núcleo (kernel) de este mapa.

[0032] Un isógeno $\varnothing$: E_1-->E_2 es un morphism no constante que envía el elemento identidad E_1 para el E_2. Cuando tal isógeno existe, uno puede decir que E_1 y E_2 son isogenos. El isogeny se define sobre k si $\varnothing$ tiene definidas ecuaciones con coeficientes en *k*. Cualquier isógeno también retorna a la salida un homomorphism de grupo, es decir, $\varnothing(P+Q)= \varnothing(P)+ \varnothing(Q)$ para todo $P,Q \in E_1$ donde la suma de la izquierda es la ley del grupo E_1 y la suma en el lado derecho es eso de E_2. Aquí el ernel de $\varnothing$ es un subgrupo de E_1.

[0033] Permita $Hom_k(E_1, E_2)$ denote el conjunto de isogenos desde E_1 hasta E_2 que son definidos sobre *k*. Hom $_{\bar{k}}$ (E_1, E_2) se denota por $Hom_k(E_1, E_2)$. Para cualquier isógeno
$\varnothing$: E_1--> E_2, hay un isógeno dual $\bar{\varnothing}$: E_2 --> E_1 tal que:
$\bar{\varnothing} \circ \varnothing = [n]_{E1}$ y $\varnothing \circ \bar{\varnothing} = [n]_{E2}$,
[0034] donde n = deg ($\varnothing$) es el grado del isogeny. El isogeny dual satisface las propiedades normales:

$$\bar{\bar{\varnothing}} = \varnothing,\ \varnothing + \Psi = \bar{\varnothing} + \bar{\Psi},\ \varnothing \circ \Psi = \bar{\Psi} \circ \bar{\varnothing},\ [\bar{n}] = [n]$$

[0035] En una implementación, el grado de $\varnothing$ como un mapa finito puede ser además definido como:: El grado de extensión $k(E_1)$ sobre el obstáculo (por $\varnothing$) del campo k (E_2) donde $\varnothing$ se define sobre k. Puede ser conveniente para pensar en términos del tamaño de su kernel (núcleo) (asumiendo la extensión del campo

de la función separable) o por la ecuación anterior. De aquí,se dice que el isógeno es B – smooth (plano) y su grado es B – plano (es decir los primeros divisores de deg ($\varnothing$) son menores o iguales a B). El conjunto Hom(E,E) de endomorphisms de una curva elíptica E se denota End(E); este conjunto tiene la estructura de un anillo dada por el defmidefinición:

$(\varnothing + \Psi)(P) = \varnothing(P) + \Psi(P)$, $(\varnothing \circ \Psi)(P) = \varnothing(\Psi(P))$

[0036] Generalmente, el grupo Hom(E_1, E_2) es una torsión libre del módulo End(E_2) izquierdo - el módulo derecho End(E_1). Cuando $E_1 = E_2 = E$, la estructura algebráica es más rica: Hom(E_1, E_2) = End(E) Is un anillo (no sólo un módulo) sin divisores cero y tiene el cero característico.

[0037] En una implementación, esto puede pensarse como una celosía: Permita a E ser una curva elíptica definida sobtre algún field k. Entonces, End(E) es el isomórfico a cada Z, una orden en un field imaginario cuadrático, o una orden máxima en el álgebra del cuaternio. Para cualquier dos curvas elípticas E_1, E_2, el grupo Hom(E_1, E_2) es un módulo libre Z del rango máximo de 4. Cuando End(E) es más grande que Z, uno dice que E tiene multiplicación compleja. El elemento en End(E) el corresponde al Frobenius.
el endomorfismo (x,y) –> (el x^p , y^p) se denota por π, y satisface la característica ecuación x^2 - tr(E)x+q = 0. El conductor de la curva elíptica c es [End(E): Z[π]].

[0038] **El APAREAMIENTO WEIL**

[0039] El apareamiento Weil que aparea e_n: E[n]x E[n] –> μ_n es un bilineal, no-genera trace con valores en el grupo de n^{th} raíces de la unidad en k. En una aplicación, el apareamento Weil se utiliza para realizar la verificación/descencripción estado 108 de la figura1. Sin embargo, el apareamento Weil aparear es pero un ejemplo que puede ser utilizado para la comprobación o descencripción. Por ejemplo, otro bilinear y/o apareamiento no-degenerado que puede ser utilizado tal como apareamiento Tate que aparea y apareamiento cuadrangular. El apareamiento Weil satisface la propiedad siguiente:
e_n (S, $\tilde{\varnothing}(T)$) = e_n ($\varnothing$(S),*T*), *donde* $S \varepsilon$ $E_1[n]$, $T \varepsilon E_2[n]$
E_1, E_2
el e^S^T) -) = el e^S),T^^S E E^T e E, [n]

[0040] Aquí, e_n (S, $\tilde{\varnothing}(T)$) es un cómputo de apareamiento sobre E_1 mientras e_n ($\varnothing$(S),*T*), e^(S'), T) está sobre E_2. Noteque ambas curvas tienen n puntos de torsión los cuales ponen una represión sobre sus órdenes de grupo. Esto no propone un problema, desde que por un teorema de Tate, E_1 (k) y E_2(k) son los isógenos sobre k si y solo si de los dos grupos de puntos tienen el mismo orden.

[0041] El apareamiento Weil evalua la identidad por todos los pares de entradas las cuales son linealmente independientes. Por consiguiente, un mecanismo debería ser beneficiado para asegurar que los puntos de la entrada no son escalas múltiples de cada uno. Un acercamiento es usar una curva E_2, definida encima de un fieid finito k que es bastante más grande que el grupo completo $E_2[n] \cong (Z/nZ)^2$
de n-torsión de puntos que está definido sobre k. En esta situación, la probabilidad que dos elementos aleatorios del grupo E_2 [n] son linealmente dependientes despreciables, en el orden de 1/n, para que el avlor del apareaiento Weil pueda ser no trivial con alta probabilidad. La ecuación arriba asegura que la distribución de los valores de apareamiento sobre E_1 harán pareja con los de E_2.

[0042] Alternativ una función de apareamiento modificado $\bar{e}(P,Q) = e_n(\lambda(P), Q)$ puede usarse donde λ es cualquier endomorphism no-escalar, entonces P y $(\lambda(P)$ son linealmente independiente y $\bar{e}(P,P) \neq 1$. Este mapa λ se llama una distorsión o variación de E.

[0043] **LA GENERACIÓN DE ISOGENOS**

[0044] En varias implementaciones, pueden usarse varios métodos para construir isogenos de grado alto (e.g -, de curvas elípticas, o más generalmente las variaciones de Abelian) y sus duales tal como discutida con referencia a la fase 102 de Fig. 1. La firma digital corta y los criptosistemas de IBE discutidos aquí dentro puede seguir la convención de pares de valores (P, *Ø (p))* que son publicados como la clave pública, mientras la evaluzión dual *Ø* constituye la clave privada.

[0045] En una aplicación, las construcciones pueden resumirse como: dado cualquier E, hay un algoritmo para construir el isógeno E –> E cuyo grado n es l r distribuldo aleatoriamente, y es una principal probabilidad ~l/log(n); dada cualquier curva E_1, hay un algoritmo por construir aleatorio B - isógeno plano de E_1 para los objetivos aleatorios a tiempo $O(B^3)$; y dado E_1, E_2 y dos isógenos linealmente independientes en $Hom_k(E_1, E_2)$ que tienen el relativamente grado principal, hay un algoritmo para construir isogenos de primer grado (vea, por ejemplo, la discusión debajo con respecto al isógeno independiente).

[0046] **ISOGENOS DE MULTIPLICACION COMPLEJA**

[0047].Permita $E_1=E_2$ como antes y asuma que E_1 tiene la multiplicación compleja (CM) por el orden 0_D cuadrático imaginario deL discriminantE $D < 0$. Un algoritmo de probabilidades puede ser descrito para producir tal curva E_1 junto con un endomorfismo Ø de E_1 de pricipal grado grande, en el tiempo polinómico esperado en $|D|$.

[0048] 1. Calcule la clase polinomial de H_D (X) polinómico} del discriminante D. Permita que K denote el campo de dividido de H_D (X) sobre Q.

[0049] 2. Escoge cualquier raíz x de H_D (X) y construya una curva elíptica E sobre C que tiene j - variante igual a x. Note que E es el definida sobre el número de campo K.

[0050] 3. Por construcción, la curva E tiene multiplicación compleja por $\sqrt{D}$ (raiz cuadrada de D). Usando álgebra lineal en q-expansiones, encuentra explícitamente la función racional I(X,Y) con los coeficientes en K. que corresponde al isogeny $\sqrt{D} \in$ EndE.

[0051] 4. Escoja los enteros aleatorios un *a y b* hasta $a^2 - b^2D$ es primero.

Entonces, el isógeno $a+b\sqrt{D}$ será un endorismo de *E* que tiene el primer grado.

[0052] 5. Escoja cualquier primero *P* ideal de *K* y reduzca los coeficientes de *E* y de *I* módulo P. Permita E_1, denote la reducción de *E* y permita $\varnothing$ sea la reducción de un $a+b\sqrt{D}$.

[0053] Los estados 1-3 del algoritmo son determinísticos y de tiempo polinomial en | D |. En cuanto a fase 4, el primer teorema numérico para los campos de número implica que el $a^2 - b^2D$ tiene probabilidad $1/\log(a^2 - b^2D)$ de ser pimero, para las interfases a y b de tamaño n uno puede esperar la fase 4 para terminar pruebas de $\log(Dn^2)$.

[0054] El endomorfismo resultante $\varnothing$ es un endomorfismo de E_1 de grado principal
el grado. Ambos $\varnothing$ y su dual $b\sqrt{D}$ pueden ser evaluados teniendo el conocimiento de a y b, usando solo la función racional I(X,Y) junto con la multiplicación escalar y suma. Así un isógeno $\varnothing$ puede llamarse un CM-isógeno.

[0055] **ISOGENOS MODULARES**

[0056] Para cualquier primero ε, la curva modular X_0 (ε) las clases de isomorfismos de isógenos E_1, E_2 de grado ε. Más especificamente, existe una ecuación polinómica $\varnothing$ (X,Y) para X_0 (ε) con la propiedad de que E_1 y E_2 son ε-isógenos si y solo si $\varnothing\varepsilon$ (j (E_1) , j (E_2)) = 0.

[0057] Usando el polinomio $\varnothing$(X,Y), uno puede calfícular para cualquiera E_1 una curva E_2 del isógeno ε junto con una ecuación polinómica explícita para el grado ε isogeny de E_1 --> E_2. Porque el polinomio modular es simétrico en el

cálculo de *X y Y* con las *j – constantes* reservadas que pueden ser usadas para encontrar el isógeno dual.

[0058] En la práctica, uno no puede usar los polinomios $\varnothing(X,Y)$ para los cálculos actuales porque los coeficientes de estos polinomios son bastante grandes. En cambio, diferentes pero equivalentes modelos polinómicos pueden usarse para X_0 (ε) teniendo los coeficientes más pequeños. Sin importar el modelo preciso utilizado para el cálculo, un isógeno derivado en su forma puede ser referido como un isógeno modular.

[0059] Los algoritmos actualmente conocidos para el cómputo de isógenos modulares son generalmente factibles para el valores pequeños de *l*. Solo, el uso de isógenos modulares de grado pequeño no agregan mucha seguridad, porque un atacante que conoce las curvas E_1 y E_2 podría verificar para cada *l* si las curvas son *l* -isogenous y recuperar el *l* - isogeny en el caso que ellas sean. Sin embargo, uno puede componer muchos isogenies modulares (por ejemplo, para seleccionar *l*) en un isógeno $\varnothing$ grande plano de Πl, y usa $\varnothing$ como un isógeno sin revelar las curvas intermedías. Un atacante que tiene la habilidad para evaluar $\varnothing$ en puntos arbitrarios todavía puede deducir los primeros *l* calculando todos las *l* - puntos de torsión de E_1 y ver si cualquiera de ellos es aniquilado por $\varnothing$. Sin embargo, bajo el supuesto de que el problema de cálculo del isógeno dual es difícil, el atacante no será capaz de evaluar $\varnothing$ *puntos* de su selección. Para la medida buena, uno puede también componer el isogeny resultante con el isógeno escalar o con el isógenos CM para introducir los factores no-planos grandes en el grado de una implementación.

[0060] **ISOGENOS LINEALMENTE INDEPENDIENTES**

[0061] En una implementación, los isógenos linealmente independientes $\varnothing$ y Ψ son dados desde E_1 hasta E_2 de primer grado relativamente. Como resultado de la combinación lineal $a\varnothing+b\Psi$ que tiene un grado dado por la ecuación cuadrática: $a^2\ \bar{\varnothing}\varnothing + ab(\bar{\varnothing}\Psi + \bar{\Psi}\varnothing) + b^2\ \bar{\Psi}\Psi$ en las dos variables a y b. la Note que los coeficientes de esta fórmula cuarática son enteros, desde que los coeficientes de fuera son de grados $\varnothing$ *y* Ψ y el término de la mitad es *igual* $deg(\varnothing+\Psi) - deg(\varnothing) - deg(\Psi)$. A pesar de que la forma cuadrática es primitiva, logra infinitamente a menudo los principales valores como a y b varían sobre de todos los pares $(a,b) \in Z^2$. De esta manera, muchos isogenies E_1 y E_2, de un grado no-plano (o incluso primero) el grado puede obtenerse. La probabilidad que el grado resultante será no-plano pueda también ser estimado.

[0062] **ESQUEMA DE FIRMA CORTA USANDO ISOGENOS**

[0063] En una implementación, pueden aplicarse las técnicas discutidas aquí dentro de los esquemas de la firma relativamente corta (por ejemplo, una entrada tecleada por un usuario o enviada sobre un canal de ancho de banda

bajo). Se discutirán dos esquemas de firma debajo de los que parcialmente absados en las propiedades matemáticas de isógenos y apareamientos en las curvas elípticas.

[0064] FIRMAS CONSTANTES DE GALOIS

[0065] Permita F_q^n / F_q sea una extensión de campos de grado finito n. Tome una curva elíptica E_1, definida sobre F_q^n junto con un isógeno $\varnothing: E_1 \rightarrow E_2$ definido sobre F_q^n, dónde E_2 es una curva elíptica definida sobre de F_q. En un implementación la curva E_2 es definida sobre L más que sobre un subcampo de L, pero es posible tomar E_2 definido sobre unicamente un subcampo. Sin embargo, por razones de seguridad, el isógeno $\varnothing$ no puede ser definido sobre ningún subcampo propio de F_q^n. Es más, el isógeno $\varnothing$ puede ser generado de acuerdo con varias técnicas como aquellas discutidas anteriormente.

[0066] Fig. 3 ilustra un método de ejmplo 300 para firmar un mensaje que usa isógenos. El método 300 incluye las siguientes fases:

[0067] **Clave Pública**. Escoja aleatoriamente $P \in E_1 (F_q)$ y publica (P,Q) (302), dónde $Q = \varnothing(P)$. Nota que P se define sobre F_q pero Q no se define sobre F_q, porque $\varnothing$ no está.

[0068] **Clave Secreta**. El isogeny dual $\bar{\varnothing}$ de $\varnothing$.

[0069] **La Firma**. Permita a H ser (público) del oráculo aleatorio del espacio del mensaje para el conjunto de k – *puntos de torsión* sobre E_2. Dado unmensaje m calcule $S = \Sigma_{i=0}^{n-1} \pi^i \bar{\varnothing} H(m)$ (fase 304, que proporciona una firma usando la clave secreta/privada generada como se discutió anteriormente), dónde π es la q^{th} del mapa de poder de Frobenius que los y la suma denota la suma de la curva elíptica sobre E_1. Para conveniencia, nosotros denotamos el operador $\Sigma_{i=0}^{n-1} \pi$ por Tr (posiciones para el rastro). El resultado Rendimiento $S \in E_1 (F_q)$ como la firma. La firma se envía entonces y es recibida por una parte receptora (306 y 308, respectivamente). Note que el grupom de Galois de F_q^n / F_q es $\{1, \pi, ..., \pi^{n-1}\}$, para que S essea la constante de Galois y además se defina sobre F_q.

[0070] **Verificación**. Permita e_1 y e_2 denote las paridades de Weil en $E_1[k]$ y $E_2[k]$, respectivamente. Dada una clave pública (P,Q) y un par de mensaje-firma (m,S), verifique si $e_1(P,S) = \prod_{i=1}^{n-1} \pi^i e_2(Q,H(m))$ (fase 310 que verifica lafirma recibida usando la clave pública generada como se discutió anteriormente). De acuerdo con, una firma válida satisface esta ecuación, como sigue:

$$e_1(P,S) = e_1(P, \Sigma_{i=0}^{n-1} \pi^i \bar{\varnothing} H(m)) = \prod_{i=0}^{n-1} e_1(P, \pi^i \bar{\varnothing} H(m))$$

$$= \prod_{i=0}^{n-1} e_1(\pi^i P, \pi^i \bar{\varnothing} H(m)) = \prod_{i=0}^{n-1} \pi^i e_1(P, \bar{\varnothing} H(m))$$

$= \Pi_{i=0}^{n-1} e_2(\varnothing(P), H(m)) = \Pi_{i=0}^{n-1} \pi^i e_2(Q, H(m))$

[0071] También, el mapa del rastro puede usarse abajo a un campo base para acortar los puntos en una curva elíptica (o más generalmente en cualquier variedad de Abelian). En otros términos, el rendimiento de un mapa del rastro en las curvas elípticas (o la dimensión más alta de las variaciones de Abelian) pueden ser utilizadas como un método para acortar la representación de un punto sobre una extensión de campo usando los datos en el más bajo campo.

[0072] **CURVAS ELIPTICAS MULTIPLES CON FIRMA**

[0073] Otra manera de ampliar la fuerza de esquemas de firma cortos es usar múltiple claves públicas y sumar las firmas resultantes. Esta modificación puede usarse solo o puede combinarse con la constante de Galois discutida previamente.

[0074] Con relación a la Fig. 4, nosotros asumimos que hay una familia de isogenos $\varnothing_i$: $E \rightarrow E_i$ y una familia de funciones de detalle del oráculo aleatorio H_i cada una mapenado un mensaje m en un punto en la curva elíptica E_i. Similar a las fases discutidas con referencia a la Fig. 3:

[0075] **Clave Pública**. Escoja aleatoriamente $P \in E$ y publique $P, Q_1, Q_2, \ldots, Q_n$, (vea, jemplo 302), donde $Q_i = \varnothing_i(P)$.

[0076] **Clave Secreta**. La familia de isogenies $\varnothing_i$.

[0077] **La firma**. Para cada mensaje m, la firma de m (S) es $\Sigma_{i=0}^{n} \bar{\varnothing}_i(H_i(m))$ (vea, e.g -, 304). El mensaje firmado se envía entonces a un parte receptora (ver por ejemplo, 306).

[0078] **La Verificación**. Dado un (mensaje, firma) el par (m,S), verifique si $e(P, S) = \Pi_{i=0}^{n} e(Q_i, H_i(m))$ (vea, por ejemplo, fase 310 discutida con referencia a la Fig. 3). Para una firma válida esta ecuación sostiene subsecuentemente:

$$e(P,S) = e(P, \Sigma_{i=1}^{n} \bar{\varnothing}_i(H_i(m))) = \Pi_{i=1}^{n} e(P, \bar{\varnothing}_i(H_i(m))) = \Pi_{i=1}^{n} e(Q_i, H_i(m))$$

[0079] Se cree que el sistema es por lo menos tan seguro como usar simplemente un solo isógeno, desde que alguien que puede romper la versión de isogenies múltiple puede convertir la versión del isógeno simple a la versión de isógenos múltiples agregando en el isógeno $\varnothing_2, \ldots, \varnothing_n$ determinado por ellos. Es más, para tal sistema, cualquier ataque del satisfactorio en la versión de isógenos múltiples requiere un rompimiento simultáneo de todos los isógenos simples $\varnothing_1, \ldots$ *hasta*..., $\varnothing_n$.

[0080] IDENTIDAD BASADA EN LA ENCRIPTACIÓN (IBE) ESQUEMA C N ISÓGENOS

[0081] La fig. 5 ilustra un método 500 ejemplar para la identidad basada en la encriptación (IBE) usando el isógeno. Se cree que la única manera de isógeno entre las curvas elípticas para hacer una identidad basada en la encriptación (IBE) es un esquema potencialmente seguro en contra de la computacional de Diffie-Hellman (CDH). El esquema IBE puede definirse como sigue.

[0082] **MAPEO HACIA EL PUNTO:** Defina la operación $ID \rightarrow P \in E$ para alguna curva E. Más específicamente, una forma de cómputo $H(id)$ y úsela para definir un punto. Puede asumirse que H se comporta como un oráculo aleatorio. Altemately, nosotros podemos guardar una mesa de puntos y detalle ID en un cordón aleatorio de pesos y entonces tomar una suma pesada. Nosotros podemos también asumir que hay una autoridad de confianza y un conjunto de usaurios finitos, cada uno con algún ID desde el cuál puede computar la clave pública correspondiente. Cada usuario consigue su clave privada después de la identificación conveniente por la autoridad de confianza.

[0083] **Clave pública para la Autoridad de Confianza:**

$\alpha \in E_1, \quad \beta = \emptyset(\alpha)$.

De acuerdo con, una autoridad de confianza (u otro entidad tal como una parte receptora) proporciona y publica las claves públicas (502). Si un cambio λ está usándose, nosotros podemos asumir que $\alpha = \lambda(a)$ es la imagen cambiada de algún punto *a*.

[0084] **Clave Privada para la Autoridad de confianza.** Un eficientemente calculado $\bar{\emptyset}$.

[0085] Por ejemplo, datos encriptados de Bob para Alice pueden así:

[0086] **Clave pública para Alice:** $T \in E_2$ se proporciona, por ejemplo, vía el mapeo al punto de la función $ID \rightarrow T$ (502) por una autoridad de confianza (u otra entidad tal como laparte receptora).

[0087] **Clave Privada para Alice:** $S = \bar{\emptyset}(T)$. Note que el atacante para conseguir rapidamente un clave para cada cliente tomaría tiempo similar para la interrupción global en el sistema de firmas (discutido anteriormente). como resultado, estos sistemas pueden también ser llamados sistemas de segundo grado.

[0088] **Encripción por Bob.** Calcule ALICE –> *T* (fase 504 que encripta un mensaje con la clave pública generada). Permita el mensaje ser m. Escoja r un entero aleatorio. Envíe a Alice el par (506):

$[m \oplus H(e(\beta, rT)), r\alpha]$

[0089] **Descencripción por Alice.** Permita el texto cifrado ser *[c,T]*. El mensaje encriptado enviado se descifra (508) usando una clave privada (510) proporcionada por una autoridad de confianza (u otra entidad como una parte receptora) después de la identification conveniente. Como resultado, el texto claro es:

$c \oplus H(e(r\alpha, S))$

[0090] Esto funciona porque la cantidad a ser detallada en la fase de encripción es:

$e(\beta, rT)) = e(\varnothing(\alpha), rT) = e(\alpha, \bar{\varnothing}(rT))) = e(\alpha, r\,\bar{\varnothing}(T)) = e(\alpha, rS) = e(r\alpha, S)$

[0091] El cual es iguala la cantidad siendo detalla en la fase de descencripción. Un isógeno puede representarse como se discute abajo (por ejemplo, para usar un acercamiento probabilístico involucrando una tabla de entadas).

[0092] **ESPECIFICANDO UN ISOGENO**

[0093] Si el isogeny es plano, puede representarse como una composición de isógenos de grado pequeño dada por un programa de línea recta que representa cálculos polinomiales. Para las curvas sobre las extensiones de interés, una mesa pequeña de pares de entrada-salida están en una implementación.

[0094] Tomando $End(E) = End_{\bar{k}}(E)$, pueden considerarse extensiones finitas de k y las extensiones pueden ser especificadas como apropiadas los specifled. En una implementación, un isógeno se especifica por su acción sobre el grupo de puntos sobre algunas extensiones finitas del terreno de campo. Note que dos isógenos pueden coincidi con algunas extensiones, pero pueden ser distintos en un campo más grande. De esta forma basta especificar $\varnothing$ en un conjunto de generadores S. Generalmente, el grupo es cíclico, o como anteriormente $/S/ = 2$. No es considerado fácil de encontrar los generadores, pero uno puede escoger aleatoriamente *S*.

[0095] Más particulariy, como un grupo de Abelian *E(k)* (la llamada: k es un campo finito de elementos *q*) es isomórfico a $Z/mZ \times Z/nZ$ dónde mn=#E(k),n | m y además $n \mid D$, $D = (el\ mn,\ q - 1)$. Uno puede calcular el mn = #HE(k) usando el

algoritmo de Schoofs y si la factorización de *D* es conocida, *n* puede ser obtenida usando un algoritmo polinomial aleatorio de tiempo. Si $\bar{P}$ y $\bar{Q}$ son de orden *n y m* respectivamente tal que cualquier punto puede escribirse como $a\ \bar{P} + b\ \bar{Q}$, ellos se llaman los generadores en el formulario del escalón y un $0(q^{1/2+\varepsilon})$ el algoritmo puede usarse para construirlos.

[0096] Retomando a selecciones aleatorias (Erdos-Renyi), permita a G ser un grupo finito de Abelian $g_1,,,,,,,g_k$ -, elementos aleatorios de G. Existe una constante pequeña *c*, tal que sus sumas del subconjunto están casi uniformemente distribuidas sobre G, si k>=c log | G .

En particular, el g puede generar G. para reducir el tamaño de la tabla, uno puede usar un su fortaleciendo del subconjunto pesado de sumas en lugar del subconjunto de sumas cuando el orden de grupo es primero. Esto se extiende a los órdenes arbitrarios con alguna pérdida pequeña de parámetros.

[0097] Es más, la estructura de *E(k)* puede usarse para obtener la información más detallada. Uno puede escoger puntos aleatorios $P_i, i <= 2$ y las escribe como $P_i=a_i\ \bar{P}+b_i\ \bar{Q}$. Más particularmente, uno puede expresar cada uno de los escalones generados por combinaciones lineales de P_i si la matriz

$$\begin{matrix} a_1 & a_2 \\ b_1 & b_2 \end{matrix}$$

es invertible en modo m. Note que n | m). Cuando esto pasa, $\{P_i\}$ genera el grupo. Note que la probabilidad (ambos P_1 y P_2) falla en el grupo ıor $\bar{P}$ es m^{-2}. Similarmente, la probabilidad para el grupo generado por le. Así, cualquiera de estos dos eventos no pasan con la probabilidad $- n^{-2}) = 1 + (\#E^{-2} - (m^{-2} + n^{-2})$.

[0098] **IMPLEMENTACION DE HARDWARE**

[0099] La fig. 6 ilustra una computadora general del ambiente 600 que puede usarse para llevar a cabo las técnicas descriats aquí dentro. Por ejemplo, la computadora del ambiente 600 puede utilizarse para ejecutar instrucciones asociadas con la realización de las tareas discutidas con referencia a las figuras anteriores. Además, cada entidad discutida aquí dentro (e.g -, con respecto a las figs. 1, 3, y 5 como la parte confiada, la aprte receptora, y/o la parte) puede cada uno tener el acceso a un ambiente de la computadora general.

[00100] La computadora del ambiente 600 es el único ejemplo de un ambiente de cómputo y no se piensa que sugerir cualquier limitación acerca del use del alcance o funcionalidad de la computadora y arquitectura de la red. Ninguno interpretraría la computadora del ambiente 600 como teniendo cualquier dependencia o requerimiento relacionando a cualquier combinación de componentes ilustrados en la computadora ejemplar del ambiente 600.

[00101] La computadora de ambiente 600 incluye un dispositivo de informática de uso general en el formulario de una computadora 602. Los componentes de la computadora 602 pueden incluir, pero no se limita a, uno o más procesadores o unidades de proceso 604 (opcionalmente incluyendo un procesador criptográfico o co-procesador), un sistema de memoria 606, y un sistema de bus 608 se acopla a varios componentes del sistema incluso el procesador 604 al sistema memoria 606.

[00102] El bus del sistema 608 representa uno o más de cualquiera de varios tipos de estructuras de bus, incluso un bus de memoria o controlador de memoria, un bus periférico, un puerto acelerador de gráficos, y un procesador o bus local que usa cualquiera de una variedad de arquitecturas del bus. A modo ejemplo, tales arquitecturas pueden incluir un bus de la Arquitectura Normal de Industria (ISA), un bus de Arquitectura de Micro Canal (MCA), un bus ISA extendido (EISA), una Asociación de Normas Electrónicas de Video (VESA) el bus, y un Componente Periférico de Interconexion (PCI) el también el bus conocido como bus del Entresuelo (Mezzanine Bus).

[00103] La computadora 602 incluye una variedad de medios de comunicación típicamente legibles por una computadora. Tales medios de comunicación pueden ser cualquier medio de comunicación disponible que es accesible por la computadora 602 e incluye los medios de comunicación volátiles y no-volátiles, los medios de comunicación removibles y no-removibles.

[00104] El sistema de memoria 606 incluye los medios de comunicación legibles por computadora en la forma de memoria de volátil, como la memoria de acceso aleatorio (RAM) 610, y/o la memoria no-volátil, como la memoria de solo lectura (ROM) 612. Un sistema del entrada/salida básico (BIOS) 614, conteniendo las rutinas básicas que ayudan a transferir la información entre los elementos dentro de la computadora 602, tal como durante el arranque, se guarda en ROM 612. La RAM 610 contiene los datos y/o módulos del programa que son inmediatamente accesible a y/o presentemente operados por la unidad de proceso 604 típicamente.

[00105] La computadora 602 puede incluir otros medios de comunicación de almacenamiento de computadora removible/no-removible, volátil/no-volátilA manera de ejemplo, la Fig. 6 ilustra una unidad de disco duro 616 para leer desde y escribir hacia un medio de comunicación magnéticos removible, no-volátil (no mostrado), una unidad de disco magnética 618 para leer desde y escribir hacia un disco magnético trasladable 620, no-volátil (por ejemplo, un "disco flexible"), y una unidad de disco 622 óptica para leer desde y/o escribir hacia un disco óptico 624 removible, no-volátil como un CD-ROM, DVD-ROM, u otros medios de comunicación ópticos. La unidad de disco duro 616, la unidad de disco magnética 618, y la unidad de disco óptica 622 están cada uno conectados al sistema de bus

608 por uno o más medios de comunicación de la interfase de datos 626. Alternativamente, al unidad de disco duro 616, la unidad de disco magnética 618, y la unidad de disco óptico 622 puede conectarse al sistema de bus 608 por una o más interfases (no mostradas).

[00106] Las unidades de disco y sus medios de comunicación legibles por computadora asociados proporcionan almacenamiento no-volátil de instrucciones de computadora-legible, los datos de estructura, módulos del programa, y otros datos para computadora 602, Aunque el ejemplo ilustra un disco duro 616, un disco magnético 620 removible, y un disco óptico 624 removible, es importante que otros tipos de medios de comunicación legibles por computadora que pueden guardar datos que son accesibles por una computadora, como cassettes magnéticos u otros dispositivos de almacenamiento magnéticos, las tarjetas de memoria flah, CD-ROM, los discos versátiles digitales (DVD) u otro almacenamiento óptico, la memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), la memoria eléctricamente borrable programable (EEPROM), y similares, pueden ser también implementadas para llevar a cabo el sistema del ambiente computmg ejemplar.

[00107] Cualquier número de módulos programables pueden guardarse en el disco duro 616, el disco magnético 620, el disco óptico 624, ROM 612, y/o RAM 610, mientras incluyendo a manera de ejemplo, un sistema operativo 626, una o más aplicaciones del programa 628, otro módulo de programa 630, y programa de datos 632. Cada uno de tales sistemas operativo 626, una o más aplicaciones del programa 628, otro programa de módulos 630, y programa de datos 632 (o alguna combinación de estos) pueden implementar todos o parte de componentes residentes que apoyan el sistema de archivos distribuidos.

[00108] Un usuario puede entrar comandos e información en la computadora 602 a través de los dispositivos de entrada como un teclado 634 y un dispositivo apuntador 636 (e.g -, un "ratón"). Otra entrada a los dispositivos 638 (no mostrada específicamente) puede incluir un micrófono, la palanca de mando, el cojjln de juego, el plato del satélite, el puerto de serie, el escáner, y/o similares. Se conectan éstos y otros dispositivos de entrada a la unidad de proceso 604 vía la entada/salida de las interfases 640 quie se acoplan al sistema de bus 608, pero puede conectarse por otra interfaz y estructuras del autobús, como un puerto paralelo, puerto listo, o un autobús de serie universal (USB).

[00109] Un monitor 642 u otro tipo de dispositivo de pantalla pueden ser conectados al sistema de bus 60S vía una interfase, como un adaptador de video 644. Además del monitor 642, otros dispositivos periféricos pueden incluir los componentes como los parlantes (no mostrado) y una impresora 646 qué puede conectarse a computadora 602 vía la entrada/salida une 640.

[00110] La computadora 602 puede operar en un ambiente conectado en red de computadoras que usan las conexiones lógicas a uno o más computadoras

remotas, como un dispositivo de cómputo remoto 648. A manera de ejemplo, el dispositivo de cómputo remoto 648 puede ser una computadora personal, un computador portátil, un servidor, un enrutador, una computadora de la red, un dispositivo par u otro nodo de la red común, una consola de juego, y similares. El dispositivo de cómputo remoto 648 está ilustrado como una computadora portátil que puede incluir muchos o todos los elementos de las características descritas aquí relacionadas con la computadora 602.

[00111] Las conexiones lógicas entre la computadora 602 y la computadora remota 648 son representadas como una red de área local (LAN) 650 y un red de área amplia general conectada (WAN) 652. Tales ambientes de gestión de redes son comúnes en las oficinas, redes de computadoras de empresa grande, intranets, y la Internet.

[00112] Cuando se implementa un ambiente de RED LAN, la computadora 602 se conecta a una red local 650 a través de una interfase de red o adaptador 654. Cuando se implementa un ambiente de red WAN, la computadora 602 incluye un módem 656 u otro medio típico para establecer las comunicaciones sobre la red amplia 652. El módem 656 puede ser interno o externo para la computadora 602, que puede conectarse al sistema de bus 608 vía las interfases de entrada/salida 640 u otros mecanismos apropiados. Se debe apreciar que las conexiones de red ilustradas son ejemplos y que otros medios de establecer enlaces de comunicación entre las computadoras 602 y 648 pueden emplearse.

[00113] En un ambiente conectado de red de computadoras, como está ilustrado con el ambiente cómputo 600, los módulos del programa representados relacionados a la computadora 602, o partes de eso, pueden guardarse en un dispositivo de almacenamiento de memoria remota. A manera de ejemplo, la aplicación remota del programa 658 reside en un dispositivo de memoria de computadora remota 648. Para los propósitos de ilustración, la aplicación del programa ilustra otros componentes del programa ejecutables como el sistema operativo aquí dentro como los bloques discretos, aunque se reconoce que tales programas y componentes residen en varios momentos en componentes de almacenamiento diferentes del dispositivo de cómputo 602, y son ejecutados por los procesadores (de datos) de la computadora.

[00114] Pueden describirse varios módulos y técnicas aquí dentro en el contexto general de instrucciones de computadora ejecutables, como los módulos de programa, ejecutado por uno o más computadoras u otros dispositivos. Generalmente, los módulos del programa incluyen las rutinas, programas, los objetos, los componentes, la estructura de datos, etc. que realizan tareas particulares o implementan tipos de datos abstractos particulares. Típicamente, la funcionalidad del programan puede combinarse o distribuirse como se desee en varias implementaciones.

[00115] Una implementación de estos módulos módulos y técnicas pueden guardarse o transmitirse por algún formulario de medios de comunicación legibles por computadora. Los medios de comunicación legibles por computadora pueden ser cualquier medios de comunicación que se puede accederse por una computadora. A manera de ejemplo, y sin limitación, los medios legibles por computadora comprenden: "medios de almacenamiento de cómputo" y "medios de comunicación."

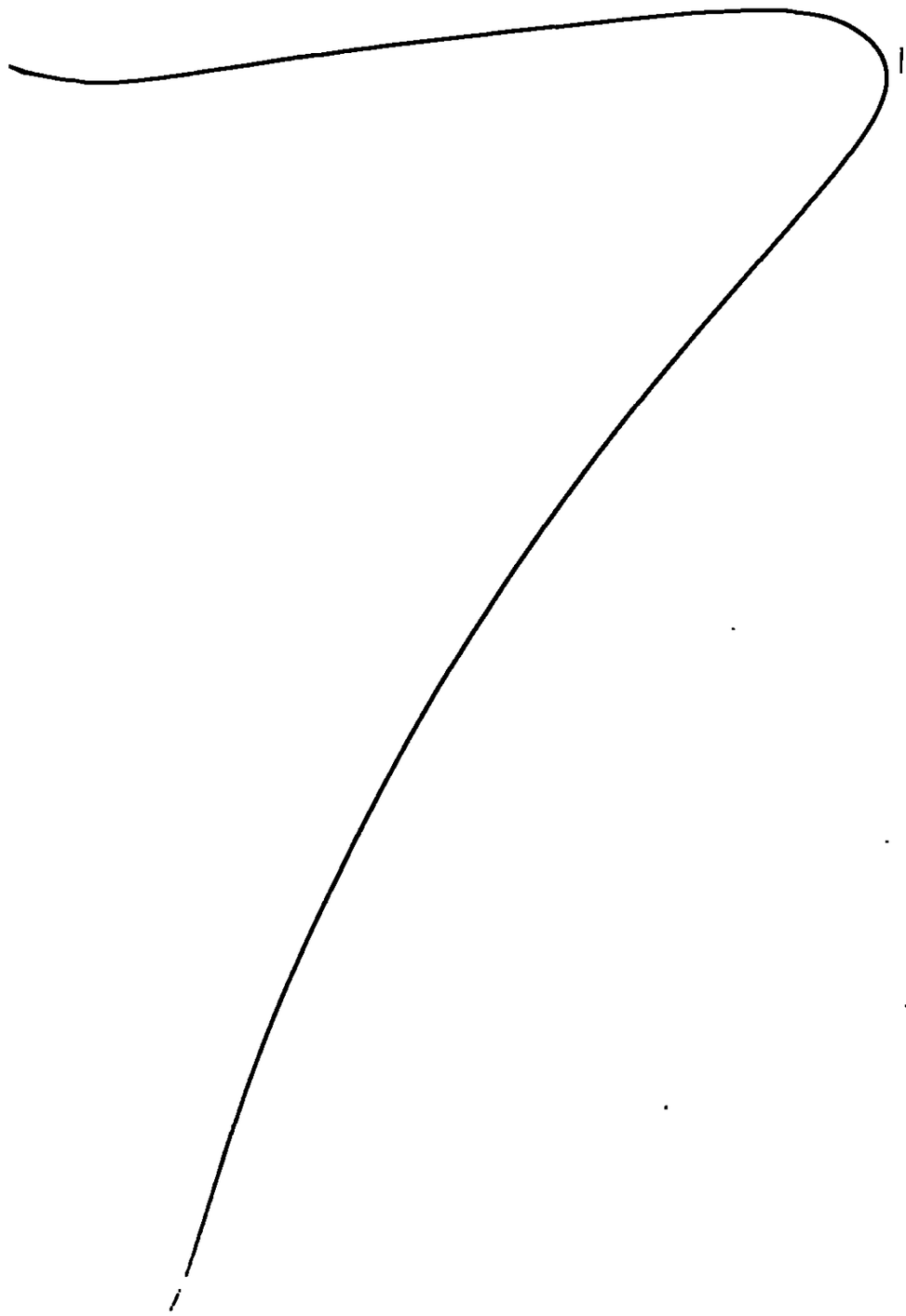
[00116] Los "medios de almacenamiento de computadora" incluyen medios volátiles y no-volátiles, removibles y no-removibles implementados en cualquier método o tecnología para el almacenamiento de información tales como las instrucciones legibles por computador, la estructura de datos, los módulos del programa, u otros datos. Los medios de almacenamiento de computadora incluyen, pero no se limitan a, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, los discos versátiles digitales (DVD) u otro almacenamiento óptico, los cassettes magnéticos, cinta magnetofónica, almacenamiento de disco magnético u otros dispositivos del almacenamiento magnéticos, o cualquier otro médio que puede usarse para guardar la información deseada y qué puede accederse por una computadora.

[00117] Los "medios de comunicación " incluyen instrucciones legibles por computador, estructuras de datos, módulos de programa, u otros datos en una señal modulada de datos, como una onda portadora u otro mecanismo de transporte. Los medios de comunicación incluyen cualquier medio de comunicación de entrega de información. El término "señal de datos modulada" significa una señal que tiene una o más de un conjunto de características cambiadas de tal manera que codifica la información en la señal. A manera de ejemplo, y sin limitación, los medios de comunicación incluyen los medios de comunicación cableados como una red alambrada o conexión directa cableada, y los medios de comunicación inalámbricos como la acústica, la frecuencia de radio (RF), infrarrojo (IR), fidelidad inalámbrica (e.g -, IEEE 802-11b - las redes inalámbricas) (Wi-Fi), el celular, Bluetooth habilitado, y otros medios de comunicación inalámbricos. Las combinaciones de cualquiera de los anteriores están también incluidos dentro del alcance de medios de comunicación legibles por computadora.

[00118] **CONCLUSIÓN**

[00119] Aunque la invención se ha descrito en el idioma específico a las características estructurales y/o los actos metodológicos, será entendido que la invención definida en las demandas adjuntas necesariamente no se limitan a los rasgos específicos o actos descritos. Más bien, las acracterísticas específicas y los actos descubren como las formas ejemplares de llevar a cabo la invención demandada. Por ejemplo, las curvas elípticas discutidas aquí dentro son un caso uni-dimensional de variedades de Abelian. También, pueden usarse los isogenos en otras aplicaciones como las firmas invisibles, sistemas jerárquicos, y similares.

Tales como, las técnicas descritas aquí dentro pueden ser aplicadas a la dimensión más alta de las variedades de Abelian.



DEMANDAS

Lo que se exige es:

1. Un método comprende:
   generando un isógeno que traza una pluralidad de puntos desde una primera curva elíptica hacia una segunda curva elíptica;
   publicando una clave pública que corresponde al isógeno;
   encriptando un mensaje que usa una clave de encriptación que corresponde al isogeny;and
   que descifra el mensaje encriptado que usa una clave de descencriptación correspondiendo al isogeny.

2. Un método como el citado por la demanda1, en qué por lo menos una clave de encriptación o de descencriptación es una clave privada, la clave privada siendo un isógeno dual del isógeno.

3. Un método como el citado por la demanda 1, en donde el isógeno se genera usando una técnica seleccionada de un grupo que comprende una generación múltiple compleja, una generación modular, una generación linealmente independiente, y combinaciones de ellas.

4. Un método como el citado por la demanda 1, en donde los mapas generanuna pluralidad de puntos de una primera curva elíptica hacia una pluralidad de curvas elípticas.

5. Un método como el citado por la demanda 1, en donde el descifrar se realiza por apareamiento bilineal.

6. Un método como el citado por la demanda 5, en donde el apareamiento bilineal es un apareamiento seleccionado de un grupo que comprende apareamiento Weil, apareamiento Tate, apareamiento cuadrado.

7. Un método como el citado por la demanda 1, en donde el método es aplicado utilizando las variaciones de Abelian.

8. Un método como el citado por la demanda 1, en donde el método señala el mensaje.

9. Un método como el citado por la demanda 1, en donde el método proporciona la identidad basada en la encriptación.
10. Un método como recitado por demanda 1, comprismg del fürther que compone una pluralidad de isogenies modular para proporcionar el isogeny sin revelar cualquier curva del intermedíate.

10. Un método como el citado por la demanda 1, además comprende el uso de un mapa de rastro con base en un campo para acortar los puntos en una curva elíptica trazados por el isógeno.

11. Un método como el citado por la demanda 1, además comprende el uso de un mapa de rastro para acortar los puntos en una variación de Abelian.

12. Un método comprende:

La publicación de una clave pública que corresponde a un isógeno que traza una

pluralidad de puntos una primera curva elíptica hacia una segunda curva elíptica; y

descifra un mensaje encriptado que usando una clave de descencripción que corresponde al isógeno.

13. Un método como el citado por la demanda 13, en donde la clave de descencripción es un isógeno dual del isogeny.

15. Un método como el citado por la demanda 13, en donde el isógeno se genera usando una técnica seleccionada de una generación de multiplicación compleja comprendiendo, la generación modular, la generación independiente lineal, y sus combinaciones.

16. Un método como el citado por la demanda 13, en donde del isógeno traza una pluralidad de puntos de una primera curva elíptica hacia una pluralidad de curvas elípticas.

17. Un método como el citado por la demanda 13, en donde la descencripción es realizado por apareamiento bilineal.

18. Un método como el citado por demanda 17, en donde el apareamiento bilineal es un grupo seleccionado que comprende apareamiento de Weil, apareamiento de Tate y apareamiento cuadrado.

19. Un método como el citado por la demanda 13, en donde el método es aplicado usando variaciones de Abehan.

20. Un método como el citado por la demanda 13, en donde el método señala el el mensaje.
21. Un método como el citado por la demanda 13, en donde el método proporciona la identidad basado en la encriptación.

22. Un método como el citado por la demanda 13, además comprende el uso de un mapa de rastro bajo hacia un campo base para acortar los puntos en una curva elíptica trazaronda por el isógeno.

23. Un sistema Comprende:
Un primer procesador;
Un primer sistema de memoria acoplado al primer procesador, el primer sistema de memoria almacenando una clave pública correspondiente a un isógeno que rastrea un pluralidad de puntos de una primera curva elíptica sobre una segunda curva elíptica;

Un segundo procesador;
Un segundo sistema de memoria acoplado al segundo porocesador, el segundo sistema de memoriaalmacenando un mensaje encriptado y una clave de descencipción correspondiente al isógeno para descencriptar el mensaje encriptado,
En donde el mensaje encripatdo es encriptado usando la clave de encripción.

24. Un sistema como el citado por la demanda 23, en donde al menos una de las claves de encripción o de descencripción es una clave privada, la clave privada siendo un isógeno dual del isógeno.

25. Un sistema como el citado por la demanda 23, en donde el isógeno rastrea un pluralidad de puntos de una primera curva elíptica sobre una pluralidad de curvas elípticas.

25. Un sistema como el citado por la demanda 23, en donde la descencripción es realizada por apareamiento bilineal.

27. Un sistema como el citado por demanda 26, en donde el apareamiento bilinear es un apareamiento seleccionado de un apareamiento Weil, apareamiento Tate apareando, y apareamiento cuadrado.

28. Uno o más medios de comunicación legibles por una computadora que tienen instrucciones almacenadas al punto que, cuando se ejecutan, directamente una máquina realiza actos que comprenden:

publicación de una clave pública que corresponde a un isógeno que traza una pluralidad de puntos de una primera curva elíptica hacia una segunda curva elíptica; y

descifrando un mensaje encriptado que usando una clave de descencripción que corresponde al isógenó.

29. Uno o más medios legibles por computador como el citado por la demanda 28, en donde la clave de encripción es una clave privada, la clave privada siendoun isígeno dual del isógeno.

30. Uno o más medios de comunicación legibles por computador como el citado por la demanda 28, en donde el isógeno se genera usando una técnica seleccionada de un grupo de que comprende una generación múltiple compleja, la generación modular, generación independiente lineal, y combinaciones de estas.

31. Uno o más medios de comunicación legibles por computador como el citado por la demanda 28, en donde el isógeno traza una pluralidad puntos de una primera curva elíptica sobre una pluralidad de curvas elípticas.

32. Uno o más medios de comunicación legibles por computador como el citado por la demanda 28, en donde la descencripción es realizada por el apareamiento bilineal.

33. Uno o más medios de comunicación legibles por computador como el citado por la demanda 32, en donde el apareamiento bilineal es un apareamiento seleccionado de un grupo que comprende apareamiento Weil, apareamiento Tate y apareamiento cuadrado.

34. Uno o más medios de comunicación legibles por computador como el citado por la demanda 28, en donde las acciones son aplicadas usando variacions de Abelian.

35. Uno o los medios de comunicación más computadora-leíbles como recitado por demanda 28, además comprende el uso de un mapa de rastro bajo hacia un campo base para acortar los puntos en una curva elíptica trazaronda por el isógeno.

36. Uno o los medios de comunicación más computadora-leíbles como recitado por demanda 28, en donde las acciones además conforman una composición de una pluralidad de isógenos modulares para proporcionar el isógeno sin revelar curvas intermedias.

37. Uno o los medios de comunicación más computadora-leíbles como recitado por demanda 28, en donde las acciones además conforman un mapa de rastreo para acortar puntos sobre una variación de Abelian.

38. Uno o los medios de comunicación más computadora-leíbles como recitado por demanda 28, en donde las acciones señalan el mensaje.

39. Uno o los medios de comunicación más computadora-leíbles como recitado por demanda 28, en donde los actos proporcionan la identidad basado en la encripción.

EL USO DE ISOGENOS PARA EL DISEÑO DE CRIPTOSISTEMAS

Se descubren las técnicas para proporcionar los sistemas de encriptación de clave pública. Más particularmente, isogenos de variaciones de Abelian (por ejemplo, las curvas elípticas en casos unidimensionales) son utilizados para proporcionar sistemas de encripción de clave pública. Por ejemplo, los isogenos permiten el uso de curvas múltiples en lugar de una sola curva para proporcionar la encriptación más segura. Las técnicas pueden aplicarse a las firmas digitales y/o identidad basada en las soluciones de encriptación (IBE). Además, los isogenies pueden usarse en otras applicaciones como las firmas invisibles, los sistemas jerárquicos, y similares. Adicionalmente, se descubren las soluciones para la generación de isogenos.

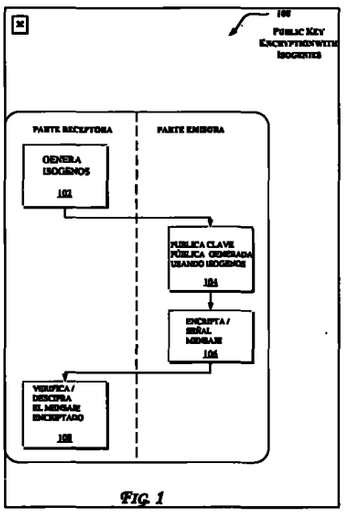

100
PUBLIC KEY
ENCRYPTION WITH
ISOGENIES
PARTE RECEPTORA
PARTE EMISORA
GENERA
ISOGENIOS
102
PUBLICA CLAVE
PÚBLICA GENERADA
USANDO ISOGENIOS
104
ENCRIPTA /
SEÑAL
MENSAJE
106
VERIFICA /
DESCIFRA
EL MENSAJE
ENCRIPTADO
108

FIG. 1

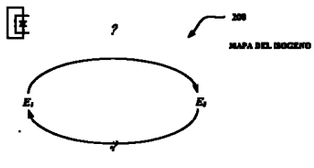

306
MAPA DEL EOCENO

FIG. 2

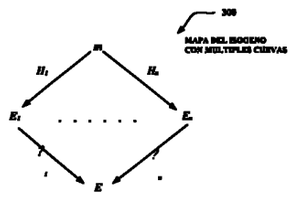

308
MAPA DEL EOCENO
CON MULTIPLES CURVAS

FIG. 4

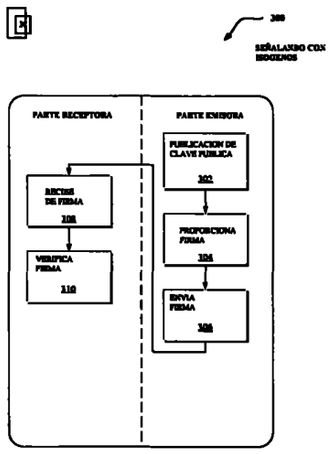

300
SEÑALANDO CON HOMINGS
PARTE RECEPTORA
PARTE EMISORA
PUBLICACION DE CLAVE PUBLICA
302
RECIBE DE FIRMA
308
PROPORCIONA FIRMA
304
VERIFICA FIRMA
310
ENVIA FIRMA
306

FIG. 3

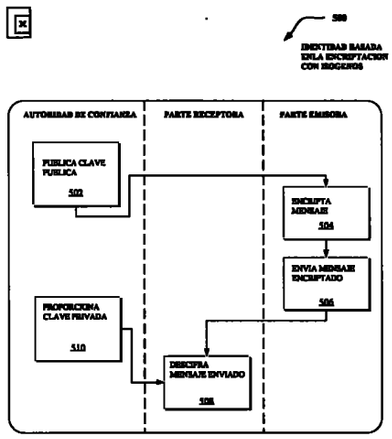

500
IDENTIDAD BASADA
EN LA ENCRIPTACION
CON HOGENOS
AUTORIDAD DE CONFIANZA
PARTE RECEPTORA
PARTE EMISORA
PUBLICA CLAVE
PUBLICA
502
ENCRIPTA
MENSAJE
504
ENVIA MENSAJE
ENCRIPTADO
506
PROPORCIONA
CLAVE PRIVADA
510
DESCIFRA
MENSAJE ENVIADO
508

FIG. 5

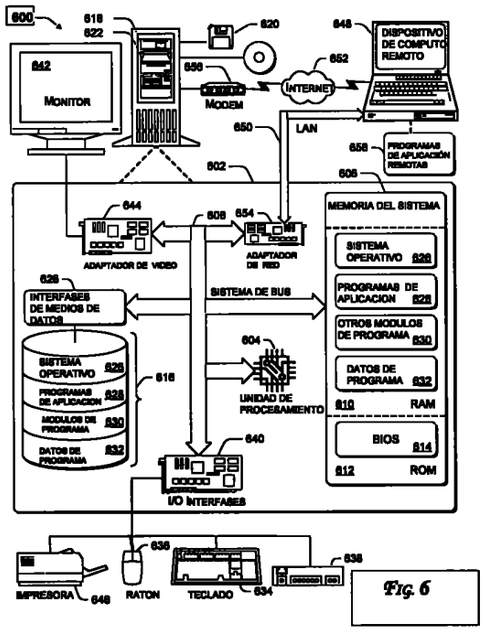

600
618
622
620
648
DISPOSITIVO DE COMPUTO REMOTO
642
MONITOR
656
MODEM
652
INTERNET
650
LAN
658
PROGRAMAS DE APLICACIÓN REMOTAS
602
606
MEMORIA DEL SISTEMA
644
ADAPTADOR DE VIDEO
608
654
ADAPTADOR DE RED
SISTEMA OPERATIVO 626
PROGRAMAS DE APLICACION 628
OTROS MODULOS DE PROGRAMA 630
DATOS DE PROGRAMA 632
626
INTERFASES DE MEDIOS DE DATOS
SISTEMA DE BUS
SISTEMA OPERATIVO 626
PROGRAMAS DE APLICACION 628
MODULOS DE PROGRAMA 630
DATOS DE PROGRAMA 632
616
604
UNIDAD DE PROCESAMIENTO
610 RAM
BIOS 614
612 ROM
640
I/O INTERFASES
636
638
IMPRESORA
646
RATON
TECLADO
634

Fig. 6

33

USE OF ISOGENIES FOR DESIGN OF CRYPTOSYSTEMS

RELATED APPLICATION

[0001] The present application claims priority from the United States provisional patent application number 60/517,142, filed November 3, 2003, entitled "Use of Isogenies for Design of Cryptosystems," the disclosure of which is incorporated herein by reference.

TECHNICAL FIELD

[0002] The present invention generally relates to cryptology, and more particularly, to utilization of isogenies for design of cryptosystems.

BACKGROUND

[0003] As digital communication becomes more commonplace, the need for securing the associated communication channels becomes increasingly more important. For example, current technologies allow a user to remotely access bank accounts, medical data, and other private and sensitive information.

[0004] Cryptology has been widely used to provide secure digital communication. Cryptology generally relates to the enciphering (or encrypting) and deciphering (decrypting) of messages. The encryption and decryption uses

some secret information (such as a key). In different encryption methods, a single key or multiple keys may be used for encryption and decryption.

[0005] One commonly used multiple key cryptosystem is a public-key encryption system. In a public-key system, a sender wishing to send an encrypted message to a recipient obtains an authenticated public key for the recipient that is generated using a private key. As the name implies, the public key can be available from public sources. Moreover, to avoid an impersonation attack, the public key is often authenticated. The public-key authentication may be made by a technique such as exchanging keys over a trusted channel, using a trusted public file, using an on-line trusted server, or using an off-line server and certificates.

[0006] After obtaining the authenticated public key, the sender encrypts an original message with the public key and generates a ciphertext. The intended recipient then utilizes the private key to decrypt the ciphertext to extract the original message. Decrypting the ciphertext without access to the private key is believed to be infeasible. Accordingly, only a party that has access to the private key may successfully decrypt the ciphertext.

[0007] One significant advantage of public-key systems over symmetric cryptosystems (such as stream or block ciphers) is that in two-party communications, only the private key needs to be kept secret (whereas in symmetric cryptosystems, the key is kept secret at both ends).

[0008] A current public-key encryption system utilizes certain elliptic curves (ECs) over a finite field. A pair of published values derived from an elliptic curve is utilized as a public key (including points on the curve and their corresponding public key which is generated by a simple multiplication (i.e., integer multiplication) on the curve). Verification is done using a bilinear pairing on the curve.

[0009] Generally, elliptic curves are believed to provide encryption systems with relatively lower communication requirements than traditional systems such as RSA (Rivest, Shamir, and Adleman public key encryption technology), while maintaining similar security levels.

[0010] An issue with the current public-key encryption systems is that none has been proven to be secure. As a result, the security of current public-key encryption systems is presumed based on the difficulty of a set of number-theoretic problems.

[0011] Accordingly, public-key encryption systems are desired which provide additional security.

SUMMARY

[0012] Techniques are disclosed to provide public-key encryption systems. More particularly, isogenies of Abelian varieties (e.g., elliptic curves in one-dimensional cases) are utilized to provide public-key encryption systems. For example, the isogenies permit the use of multiple curves instead of a single curve to provide more secure encryption. The techniques may be applied to digital signatures and/or identity based encryption (IBE) solutions. Furthermore, isogenies may be used in other applications such as blind signatures, hierarchical systems, and the like. Additionally, solutions are disclosed for generating the isogenies.

[0013] In one described implementation, a method includes publishing a public key corresponding to an isogeny. The method further includes decrypting an encrypted message using a decryption key which corresponds to the isogeny (e.g., is its dual isogeny).

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The detailed description is described with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The use of the same reference numbers in different figures indicates similar or identical items.

[0015] Fig. 1 illustrates an exemplary method for using isogenies in a cryptosystem.

[0016] Fig. 2 illustrates an exemplary map of an isogeny between two curves.

[0017] Fig. 3 illustrates an exemplary method for signing a message using isogenies.

[0018] Fig. 4 illustrates an exemplary map of an isogeny between multiple curves.

[0019] Fig. 5 illustrates an exemplary method for identity based encryption (IBE) using isogenies.

[0020] Fig. 6 illustrates a general computer environment 600, which can be used to implement the techniques described herein.

DETAILED DESCRIPTION

[0021] The following discussion assumes that the reader is familiar with cryptography techniques. For a basic introduction of cryptography, the reader is directed to a text written by A. Menezes, P. van Oorschot, and S. Vanstone entitled, "Handbook of Applied Cryptography," fifth printing (August 2001), published by CRC Press.

[0022] The following disclosure describes techniques for improving public-key systems that are based on multiple elliptic curves (or Abelian varieties in general). Various techniques are disclosed for generating isogenies (or mappings) between the curves. The generated isogenies permit use of multiple curves instead of single curve to provide public encryption. Furthermore, the techniques may be applied to relatively short digital signatures (e.g., typed in by a user or sent over a low-bandwidth channel) and/or identity based encryption (IBE) solutions (e.g., allowing memorizable public keys). The short signatures may also provide additional efficiency through aggregate verification.

[0023] OVERVIEW OF CRYPTOSYSTEMS WITH ISOGENIES

[0024] Fig. 1 illustrates an exemplary method 100 for using isogenies in a cryptosystem. A stage 102 generates isogenies (of elliptic curves, or more generally Abelian varieties). The isogenies may be generated by a receiving party or another party (such as a trusted party further discussed with reference to Fig. 5).

The stage 102 may also generate the corresponding dual isogeny for each of the generated isogenics (as will be further discussed below). Various methods for generating isogenics are detailed below under the same title. Additionally, as will be further detailed with reference to Figs. 3 and 5, the generated isogenies are utilized to provide public keys and the public keys are published (104). The public keys may be published by the sending party or a trusted authority (see, e.g., discussion of Figs. 3 and 5).

[0025] A sending party then encrypts (or signs) messages using an encryption key (106). The encrypted messages of the stage 106 may be verified/decrypted by the receiving party using a decryption key to determine the authenticity of the encryption or signing (108). In one implementation, Weil pairing is utilized to verify the encrypted messages (such as discussed below under the same title). However, Weil pairing is but one example of pairing that may be utilized for the verification or decryption. For example, other bilinear and/or non-degenerate pairing techniques may be utilized such as Tate pairing and square pairing.

[0026] OVERVIEW OF ISOGENIES

[0027] Fig. 2 illustrates an exemplary map of an isogeny 200 between two curves (e.g., elliptic curves). As illustrated, a curve E_1 may be mapped onto a

curve E_2 by an isogeny ϕ (where $\phi: E_1 \rightarrow E_2$). Fig. 1 also illustrates the dual isogeny $\hat{\phi}$ (where $\hat{\phi}: E_2 \rightarrow E_1$).

[0028] In various implementations, using isogenies in cryptosystems is envisioned to provide properties such as: given a curve E_1, generating a pair (ϕ, E_2) is relatively efficient, where $\phi: E_1 \rightarrow E_2$ is an isogeny, but given a pair (E_1, E_2) of isogenous curves, it is believed to be relatively hard to construct any nonzero isogeny $\phi: E_1 \rightarrow E_2$, much less a specific isogeny. Therefore, if a distinction is drawn between a global break (defined as a computation allowing any subsequent message to be broken in polynomial time) and a per-instance break, then the best known attacks at this time against isogeny based cryptosystems take either substantially more time than discrete log for a global break or else one discrete log computation per message for the "naive" per-instance attack.

[0029] For example, considering a token system where each client is given a specific signed message that grants access to some service (which may be of low value), the client may have to read the token over the phone to a representative, and thus the signatures can be relatively short. It will be reasonable to use parameters that are sufficiently large to make a per message attack more costly than the service provided, while keeping a global break prohibitively expensive.

[0030] DETAILS OF ISOGENIES

[0031] A field k can be fixed with characteristic p with q elements and having an algebraic closure $\bar{k}$. Let E/k be an elliptic curve defined over a field k and $E(k)$ be the group defined over k, and let $k(E)$ denote the function field of the elliptic curve. Also, let $[n]_E$ or $[n]$ denote the map $P \mapsto n \cdot P$ on E and $E[n]$ denote the kernel of this map.

[0032] An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism that sends the identity element of E_1 to that of E_2. When such an isogeny exists, one may say that E_1 and E_2 are isogenous. The isogeny is defined over k if ϕ has defining equations with coefficients in k. Any isogeny also turns out to be group homomorphism, i.e., $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$, where the addition on the left hand side is the group law on E_1 and the addition on the right hand side is that of E_2. Hence the kernel of ϕ is a subgroup of E_1.

[0033] Let $Hom_k(E_1, E_2)$ denote the set of isogenies from E_1 to E_2 that are defined over k. $Hom_{\bar{k}}(E_1, E_2)$ is denoted by $Hom(E_1, E_2)$. For any isogeny $\phi : E_1 \to E_2$, there is a *dual isogeny* $\hat{\phi} : E_2 \to E_1$ such that:

$$\hat{\phi} \circ \phi = [n]_{E_1} \text{ and } \phi \circ \hat{\phi} = [n]_{E_2},$$

[0034] where $n = \deg(\phi)$ is the degree of the isogeny. The dual isogeny satisfies the standard properties:

$$\hat{\hat{\phi}} = \phi, \widehat{\phi+\psi} = \hat{\phi}+\hat{\psi}, \widehat{\phi\circ\psi} = \hat{\psi}\circ\hat{\phi}, \widehat{[n]} = [n].$$

[0035] In an implementation, the degree of ϕ as a finite map can be further defined as: the degree of the extension of $k(E_1)$ over the pullback (by ϕ) of the field $k(E_2)$ where ϕ is defined over k. It may be convenient to think of it in terms of the size of its kernel (assuming the function field extension is separable) or by the equation above. Hence, it is said that the isogeny is *B-smooth* if its degree is B-smooth (i.e. the prime divisors of $\deg(\phi)$ are less than or equal to B). The set $Hom(E,E)$ of endomorphisms of an elliptic curve E is denoted $End(E)$; this set has the structure of a ring given by defining:

$$(\phi+\psi)(P) = \phi(P)+\psi(P), (\phi\circ\psi)(P) = \phi(\psi(P)).$$

[0036] Generally, the group $Hom(E_1,E_2)$ is a torsion free left $End(E_2)$-module and right $End(E_1)$-module. When $E_1 = E_2 = E$, the algebraic structure is richer: $Hom(E_1,E_2) = End(E)$ is a ring (not just a module) with no zero divisors and has characteristic zero.

[0037] In one implementation, this can be thought of as a lattice: Let E be an elliptic curve defined over some field k. Then, $End(E)$ is isomorphic to either Z, an order in a quadratic imaginary field, or a maximal order in quaternion algebra. For any two elliptic curves E_1, E_2, the group $Hom(E_1,E_2)$ is a free Z-module of rank at most 4. When $End(E)$ is larger than Z, one says that E has complex multiplication. The element in $End(E)$ corresponding to the Frobenius

endomorphism $(x,y)\mapsto(x^p,y^p)$ is denoted by π, and it satisfies the characteristic equation $x^2-tr(E)x+q=0$. The conductor of the elliptic curve c is $[End(E):Z[\pi]]$.

[0038] WEIL PAIRING

[0039] The Weil pairing $e_n: E[n]\times E[n]\rightarrow\mu_n$ is a bilinear, non-degenerate map with values in the group of n^{th} roots of unity in k. In one implementation, Weil pairing is utilized to perform the verification/decryption stage 108 of Fig. 1. However, Weil pairing is but one example of pairing that may be utilized for the verification or decryption. For example, other bilinear and/or non-degenerate pairing techniques may be utilized such as Tate pairing and square pairing. The Weil pairing satisfies the following property:

$$e_n(S,\hat{\phi}(T))=e_n(\phi(S),T), \text{where } S\in E_1[n], T\in E_2[n]$$

[0040] Here, $e_n(S,\hat{\phi}(T))$ is a pairing computation on E_1 while $e_n(\phi(S),T)$ is on E_2. Note that both curves have n-torsion points, which puts a constraint on their group orders. This does not pose a problem, since by a theorem of Tate, $E_1(k)$ and $E_2(k)$ are isogenous over k if and only if the two groups of points have the same order.

[0041] The Weil pairing evaluates the identity for all pairs of inputs which are linearly dependent. Consequently, a mechanism would be beneficial to ensure

that the input points are not scalar multiples of each other. One approach is to use a curve E_2 defined over a finite field k which is large enough that the full group $E_2[n] \cong (Z/nZ)^2$ of n-torsion points is defined over k. In this situation, the probability that two random elements of the group $E_2[n]$ are linearly dependent is negligible, on the order of $1/n$, so the value of the Weil pairing can be nontrivial with high probability. The equation above ensures that the distribution of pairing values on E_1 will match that of E_2.

[0042] Alternatively, a modified pairing function $\tilde{e}(P,Q) = e_n(\lambda(P),Q)$ may be used where λ is any non-scalar endomorphism, so that P and $\lambda(P)$ are linearly independent and $\tilde{e}(P,P) \neq 1$. Such a map λ is called a *distortion* or *twist* of E.

[0043] GENERATION OF ISOGENIES

[0044] In various implementations, a number of methods can be used to construct isogenies of high degree (e.g., of elliptic curves, or more generally Abelian varieties) and their duals such as discussed with reference to the stage 102 of Fig. 1. The short digital signature and IBE cryptosystems discussed herein may follow the convention that pairs of values $(P,\phi(P))$ are published as the public key, while evaluation of the dual $\hat{\phi}$ constitutes the private key.

[0045] In one implementation, the constructions can be summarized as: given any E, there is an algorithm for constructing isogenies $E \to E$ whose degree n is randomly distributed, and is a prime with probability $\sim 1/\log(n)$; given any curve E_1, there is an algorithm for constructing random B-smooth isogenies from E_1 to random targets in time $O(B^3)$; and given E_1, E_2 and two linearly independent isogenies in $Hom_k(E_1, E_2)$ that have relatively prime degree, there is an algorithm to construct isogenies of prime degree (see, e.g., the discussion below with respect to independent isogenies).

[0046] COMPLEX MULTIPLICATION ISOGENIES

[0047] Let $E_1 = E_2$ as before and assume that E_1 has complex multiplication (CM) by the imaginary quadratic order O_D of discriminant $D < 0$. A probabilistic algorithm may be described for producing such a curve E_1 together with an endomorphism ϕ of E_1 of large prime degree, in expected time polynomial in $|D|$.

[0048] 1. Compute the Hilbert class polynomial $H_D(X)$ of discriminant D. Let K denote the splitting field of $H_D(X)$ over Q.

[0049] 2. Choose any root x of $H_D(X)$ and construct an elliptic curve E over C having j-invariant equal to x. Note that E is defined over the number field K.

[0050] 3. By construction, the curve E has complex multiplication by $\sqrt{D}$. Using linear algebra on q–expansions, find explicitly the rational function $I(X,Y)$ with coefficients in K corresponding to the isogeny $\sqrt{D} \in EndE$.

[0051] 4. Choose random integers a and b until $a^2 - b^2 D$ is prime. Then, the isogeny $a + b\sqrt{D}$ will be an endomorphism of E having prime degree.

[0052] 5. Choose any prime ideal P of K and reduce the coefficients of E and of I modulo P. Let E_1 denote the reduction of E and let ϕ be the reduction of $a + b\sqrt{D}$.

[0053] Stages 1–3 of the algorithm are deterministic and polynomial time in $|D|$. As for stage 4, the prime number theorem for number fields implies that $a^2 - b^2 D$ has probability $1/\log(a^2 - b^2 D)$ of being prime, so for integers a and b of size n one can expect stage 4 to terminate after $\log(Dn^2)$ trials.

[0054] The resulting endomorphism ϕ is an endomorphism of E_1 of prime degree. Both ϕ and its dual $\hat{\phi} = a - b\sqrt{D}$ can be evaluated by having knowledge of a and b, using only the rational function $I(X,Y)$ along with scalar multiplication and addition. Such an isogeny ϕ may be called a *CM-isogeny*.

[0055] MODULAR ISOGENIES

[0056] For any prime ℓ, the modular curve $X_0(\ell)$ parameterizes isomorphism classes of isogenies $E_1 \to E_2$ of degree ℓ. More specifically, there

exists a polynomial equation $\Phi_\ell(X,Y)$ for $X_0(\ell)$ with the property that E_1 and E_2 are ℓ–isogenous if and only if $\Phi_\ell(j(E_1), j(E_2)) = 0$.

[0057] Using the polynomial $\Phi_\ell(X,Y)$, one can compute for any E_1 an ℓ–isogenous curve E_2 together with an explicit polynomial equation for the degree ℓ isogeny $E_1 \to E_2$. Because the modular polynomial is symmetric in X and Y computation with the j–invariants reversed can be used to find the dual isogeny.

[0058] In practice, one may not use the polynomials $\Phi_\ell(X,Y)$ for actual computations because the coefficients of these polynomials are rather large. Instead, different but equivalent polynomial models may be used for $X_0(\ell)$ having smaller coefficients. Regardless of the precise model used for the computation, an isogeny derived in this way may be referred to as a *modular isogeny*.

[0059] The currently known algorithms for computing modular isogenies are generally feasible for small values of l. By itself, the use of modular isogenies of small degree does not add much security, because an attacker who knows the curves E_1 and E_2 could check for each l whether the curves are l–isogenous and recover the l–isogeny in the case that they are. However, one can compose many modular isogenies (e.g., for different choices of l) into one isogeny ϕ of large smooth degree $\prod l$, and use ϕ as an isogeny without revealing the intermediate curves. An attacker who has the ability to evaluate ϕ on arbitrary points may still deduce the primes l by computing all the l–torsion points of E_1 and seeing

whether any of them are annihilated by ϕ. However, under the assumption that the dual isogeny computation problem is hard, the attacker will not be able to evaluate ϕ on points of his choosing. For good measure, one can also compose the resulting isogeny either with scalar isogenies or with CM isogenies in order to introduce large non–smooth factors into the degree in an implementation.

[0060] . LINEARLY INDEPENDENT ISOGENIES

[0061] In an implementation, the linearly independent isogenies ϕ and ψ are given from E_1 to E_2 of relatively prime degree. As a result, the linear combination $a\phi+b\psi$ has a degree given by the quadratic form $a^2\hat{\phi}\phi+ab(\hat{\phi}\psi+\hat{\psi}\phi)+b^2\hat{\psi}\psi$ in the two variables a and b. Note that the coefficients of this quadratic form are integers, since the outer coefficients are the degrees of ϕ and ψ and the middle term is equal to $\deg(\phi+\psi)-\deg(\phi)-\deg(\psi)$. Since the quadratic form is primitive, it attains prime values infinitely often as a and b vary over all pairs $(a,b)\in Z^2$. In this way, many isogenies $E_1\rightarrow E_2$ of large non–smooth (or even prime) degree may be obtained. The probability that the resulting degree will be non-smooth may also be estimated.

[0062] SHORT SIGNATURE SCHEMES USING ISOGENIES

[0063] In an implementation, the techniques discussed herein may be applied to relatively short signature schemes (e.g., typed in by a user or sent over a

low-bandwidth channel). Two signature schemes will be discussed below which are partly based on mathematical properties of isogenies and pairings on elliptic curves.

[0064] GALOIS INVARIANT SIGNATURES

[0065] Let F_{q^n}/F_q be an extension of finite fields of degree n. Take an elliptic curve E_1 defined over F_q together with an isogeny $\phi: E_1 \to E_2$ defined over F_{q^n}, where E_2 is an elliptic curve defined over F_{q^n}. In one implementation, the curve E_2 is defined over L rather than over a subfield of L, but it is possible to take E_2 defined over only a subfield. However, for security reasons, the isogeny ϕ may not be defined over any proper subfield of F_{q^n}. Moreover, the isogeny ϕ may be generated in accordance with various techniques such as those discussed above.

[0066] Fig. 3 illustrates an exemplary method 300 for signing a message using isogenies. The method 300 includes the following stages:

[0067] Public Key. Pick random $P \in E_1(F_q)$ and publish (P,Q) (302), where $Q=\phi(P)$. Note that P is defined over F_q but Q is not defined over F_q, because ϕ is not.

[0068] Secret Key. The dual isogeny $\hat{\phi}$ of ϕ.

[0069] Signature. Let H be a (public) random oracle from the message space to the set of k-torsion points on E_2. Given a message m, compute

$S = \sum_{i=0}^{n-1} \pi^i \hat{\phi} H(m)$ (stage 304, which provides a signature using the secret/private key generated as discussed above), where π is the q^{th} power Frobenius map and the sum denotes the elliptic curve sum on E_1. For convenience, we denote the operator $\sum_{i=0}^{n-1} \pi^i$ by Tr (which stands for "trace"). Output $S \in E_1(F_q)$ as the signature. The signature is then sent to and received by a receiving party (306 and 308, respectively). Note that the Galois group of F_{q^n}/F_q is $\{1, \pi, ..., \pi^{n-1}\}$, so S is Galois invariant and thus is defined over F_q.

[0070] **Verification.** Let e_1 and e_2 denote the Weil pairings on $E_1[k]$ and $E_2[k]$, respectively. Given a public key (P,Q) and a message-signature pair (m,S), check whether $e_1(P,S) = \prod_{i=0}^{n-1} \pi^i e_2(Q, H(m))$ (stage 310, which verifies the received signature using the public key generated as discussed above). Accordingly, a valid signature satisfies this equation, as follows:

$$\begin{aligned} e_1(P,S) &= e_1\left(P, \sum_{i=0}^{n-1} \pi^i \hat{\phi} H(m)\right) = \prod_{i=0}^{n-1} e_1(P, \pi^i \hat{\phi} H(m)) \\ &= \prod_{i=0}^{n-1} e_1(\pi^i P, \pi^i \hat{\phi} H(m)) = \prod_{i=0}^{n-1} \pi^i e_1(P, \hat{\phi} H(m)) \\ &= \prod_{i=0}^{n-1} \pi^i e_2(\phi(P), H(m)) = \prod_{i=0}^{n-1} \pi^i e_2(Q, H(m)). \end{aligned}$$

[0071] Also, the trace map may be used down to a base field to shorten points on an elliptic curve (or more generally on any Abelian variety). In other words, the output of a trace map on elliptic curves (or higher dimensional Abelian

varieties) may be utilized as a method for shortening the representation of a point over an extension field by using data on the lower field.

[0072] SIGNING WITH MULTIPLE ELLIPTIC CURVES

[0073] Another way to enhance the strength of short signature schemes is to use multiple public keys and add up the resulting signatures. This modification can be used by itself or combined with the Galois invariant enhancement discussed above.

[0074] With reference to Fig. 4, we assume there is a family of isogenies $\phi_i : E \to E_i$ and a family of random oracle hash functions H_i each mapping a message m into a point on the elliptic curve E_i. Similar to the stages discussed with reference to Fig. 3:

[0075] **Public key.** Pick random $P \in E$ and publish $P, Q_1, Q_2, \ldots, Q_n$ (see, e.g., 302), where $Q_i = \phi_i(P)$.

[0076] **Secret key.** The family of isogenies ϕ_i.

[0077] **Signature.** For each message m, the signature of m (S) is $\sum_{i=1}^{n} \phi_i(H_i(m))$ (see, e.g., 304). The signed message is then sent to a receiving party (see, e.g., 306).

[0078] Verification. Given a (message, signature) pair (m,S), check whether $e(P,S)=\prod_{i=1}^{n} e(Q_i,H_i(m))$ (see, e.g., stage 310 discussed with reference to Fig. 3). For a valid signature this equation holds since:

$$e(P,S)=e\left(P,\sum_{i=1}^{n}\hat{\phi}_i(H_i(m))\right)=\prod_{i=1}^{n}e(P,\hat{\phi}_i(H_i(m)))=\prod_{i=1}^{n}e(Q_i,H_i(m)).$$

[0079] The system is believed to be at least as secure as using just a single isogeny, since anybody who can break the multiple isogenies version can convert the single isogeny version to the multiple isogenies version by adding in isogenies $\phi_2,\ldots,\phi_n$ as determined by them. Moreover, for such a system, any successful attack on the multiple isogenies version requires a simultaneous break of all of the single isogenies ϕ_1 through ϕ_n.

[0080] IDENTITY BASED ENCRYPTION (IBE) SCHEME WITH ISOGENIES

[0081] Fig. 5 illustrates an exemplary method 500 for identity based encryption (IBE) using isogenies. The one-way isogeny between the elliptic curves is believed to make an identity based encryption (IBE) scheme potentially secure against computational Diffie-Hellman (CDH). The IBE scheme may be defined as follows.

[0082] MAP TO POINT: Define the operation $\mathrm{ID} \mapsto P \in E$ for some curve E. More specifically, one may compute $H(id)$ and use it to define a point. It may be assumed that H behaves like a random oracle. Alternately, we may keep a table of

points and hash ID into a random string of weights and then take a weighted sum. We may also assume that there is a trusted authority and a finite set of users, each with some ID from which one can compute the corresponding public key. Each user gets his private key after suitable identification by the trusted authority.

[0083] **Public Key for the Trusted Authority:** $\alpha \in E_1$, $\beta = \phi(\alpha)$. Accordingly, a trusted authority (or another entity such as a receiving party) provides and publishes public keys (502). If a twist λ is being used, we may assume that $\alpha = \lambda(a)$ is the twisted image of some point a.

[0084] **Private Key for the Trusted Authority.** An efficiently computable $\hat{\phi}$.

[0085] For example, encrypted data from Bob to Alice can be implemented as follows:

[0086] **Public Key for Alice:** $T \in E_2$ is provided, e.g., via the `map-to-point` function $\mathrm{ID} \mapsto T$ (502) by a trusted authority (or another entity such as a receiving party).

[0087] **Private Key for Alice:** $S = \hat{\phi}(T)$. Note that attacking to get a private key quickly for each client would take time similar to the one for global break in the signature system (discussed above). As a result, these systems may also be referred to as two-tier systems.

[0088] **Encryption by Bob.** Compute ALICE $\mapsto T$ (stage 504, which encrypts a message with the generated public key). Let the message be $\mathbf{m}$. Pick a random integer r. Send to Alice the pair (506):

$$[m \oplus H(e(\beta, rT)), r\alpha]$$

[0089] **Decryption by Alice.** Let the cipher text be $[c,T]$. The encrypted message sent is decrypted (508) using a private key (510) provided by a trusted authority (or another entity such as a receiving party) after suitable identification. As a result, the clear text is:

$$c \oplus H(e(r\alpha, S))$$

[0090] This works because the quantity being hashed in the encryption stage is:

$$e(\beta, rT) = e(\phi(\alpha), rT) = e(\alpha, \hat{\phi}(rT)) = e(\alpha, r\hat{\phi}(T)) = e(\alpha, rS) = e(r\alpha, S),$$

[0091] which is equal to the quantity being hashed in the decryption stage. An isogeny may be represented as discussed below (e.g., to use a probabilistic approach involving a table of entries).

[0092] SPECIFYING AN ISOGENY

[0093] If the isogeny is smooth, it may be represented as a composition of small degree isogenies given by a straight-line program representing polynomial

computations. For curves over extensions of interest, a small table of input-output pairs suffices in an implementation.

[0094] Taking $End(E) = End_{\bar{k}}(E)$, finite extensions of k may be considered and the extension may be specified as appropriate. In one implementation, an isogeny is specified by its action on the group of points over some finite extension of the ground field. Note that two isogenies may coincide up to some extensions, but may be distinct in a larger field. Accordingly, it suffices to specify ϕ on a set of generators S. Generally, the group is cyclic, or as above $|S| = 2$. It is considered not easy to find the generators, but one can choose S randomly.

[0095] More particularly, as an Abelian group $E(k)$ (recall: k is a finite field of q elements) is isomorphic to $Z/mZ \times Z/nZ$, where $mn = \#E(k), n \mid m$ and in addition $n \mid D, D = (mn, q-1)$. One can compute $mn = \#E(k)$ using Schoof's algorithm and if the factorization of D is known, n can be obtained using a randomized polynomial time algorithm. If $\tilde{P}$ and $\tilde{Q}$ are of order n and m respectively such that any point can be written as $a\tilde{P} + b\tilde{Q}$, they are called generators in echelon form and an $O(q^{1+\varepsilon})$ algorithm may be used for constructing them.

[0096] Turning to random choices (Erdos-Renyi), let G be a finite Abelian group and $g_1, \ldots, g_t$ be random elements of G. There exists a small constant c, such that its subset sums are almost uniformly distributed over G, if $k \geq c \cdot \log |G|$.

In particular, the g_i may generate G. To reduce the table size, one can use its strengthening weighted subset sums rather than subset sums when the group order is a prime. This extends to arbitrary orders with some small loss of parameters.

[0097] Moreover, the structure of $E(k)$ may be used to obtain more detailed information. One can pick random points $P_i, i \leq 2$ and write them as $P_i = a_i \tilde{P} + b_i \tilde{Q}$. More particularly, one can express each of the echelon generators by linear combinations of P_i if the matrix $\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}$ is invertible mod m (note that $n|m$). When this happens, $\{P_i\}$ will generate the group. Note that the probability (both P_1 and P_2) falls in the group generated by $\tilde{P}$ is m^{-2}. Similarly, the probability for the group generated by $\tilde{Q}$ is n^{-2}. Thus, either of these two events do not happen with probability $(1-m^{-2})(1-n^{-2}) = 1+(\#E)^{-2}-(m^{-2}+n^{-2})$.

[0098] HARDWARE IMPLEMENTATION

[0099] Fig. 6 illustrates a general computer environment 600, which can be used to implement the techniques described herein. For example, the computer environment 600 may be utilized to execute instructions associated with performing the tasks discussed with reference to the previous figures. Furthermore, each entity discussed herein (e.g., with respect to Figs. 1, 3, and 5 such as the trusted party, receiving party, and/or sending party) may each have access to a general computer environment.

[00100] The computer environment 600 is only one example of a computing environment and is not intended to suggest any limitation as to the scope of use or functionality of the computer and network architectures. Neither should the computer environment 600 be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in the exemplary computer environment 600.

[00101] Computer environment 600 includes a general-purpose computing device in the form of a computer 602. The components of computer 602 can include, but are not limited to, one or more processors or processing units 604 (optionally including a cryptographic processor or co-processor), a system memory 606, and a system bus 608 that couples various system components including the processor 604 to the system memory 606.

[00102] The system bus 608 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. By way of example, such architectures can include an Industry Standard Architecture (ISA) bus, a Micro Channel Architecture (MCA) bus, an Enhanced ISA (EISA) bus, a Video Electronics Standards Association (VESA) local bus, and a Peripheral Component Interconnects (PCI) bus also known as a Mezzanine bus.

[00103] Computer 602 typically includes a variety of computer-readable media. Such media can be any available media that is accessible by computer 602 and includes both volatile and non-volatile media, removable and non-removable media.

[00104] The system memory 606 includes computer-readable media in the form of volatile memory, such as random access memory (RAM) 610, and/or non-volatile memory, such as read only memory (ROM) 612. A basic input/output system (BIOS) 614, containing the basic routines that help to transfer information between elements within computer 602, such as during start-up, is stored in ROM 612. RAM 610 typically contains data and/or program modules that are immediately accessible to and/or presently operated on by the processing unit 604.

[00105] Computer 602 may also include other removable/non-removable, volatile/non-volatile computer storage media. By way of example, Fig. 6 illustrates a hard disk drive 616 for reading from and writing to a non-removable, non-volatile magnetic media (not shown), a magnetic disk drive 618 for reading from and writing to a removable, non-volatile magnetic disk 620 (e.g., a "floppy disk"), and an optical disk drive 622 for reading from and/or writing to a removable, non-volatile optical disk 624 such as a CD-ROM, DVD-ROM, or other optical media. The hard disk drive 616, magnetic disk drive 618, and optical disk drive 622 are each connected to the system bus 608 by one or more data media interfaces 626. Alternatively, the hard disk drive 616, magnetic disk drive 618, and

optical disk drive 622 can be connected to the system bus 608 by one or more interfaces (not shown).

[00106] The disk drives and their associated computer-readable media provide non-volatile storage of computer-readable instructions, data structures, program modules, and other data for computer 602. Although the example illustrates a hard disk 616, a removable magnetic disk 620, and a removable optical disk 624, it is to be appreciated that other types of computer-readable media which can store data that is accessible by a computer, such as magnetic cassettes or other magnetic storage devices, flash memory cards, CD-ROM, digital versatile disks (DVD) or other optical storage, random access memories (RAM), read only memories (ROM), electrically erasable programmable read-only memory (EEPROM), and the like, can also be utilized to implement the exemplary computing system and environment.

[00107] Any number of program modules can be stored on the hard disk 616, magnetic disk 620, optical disk 624, ROM 612, and/or RAM 610, including by way of example, an operating system 626, one or more application programs 628, other program modules 630, and program data 632. Each of such operating system 626, one or more application programs 628, other program modules 630, and program data 632 (or some combination thereof) may implement all or part of the resident components that support the distributed file system.

[00108] A user can enter commands and information into computer 602 via input devices such as a keyboard 634 and a pointing device 636 (e.g., a "mouse"). Other input devices 638 (not shown specifically) may include a microphone, joystick, game pad, satellite dish, serial port, scanner, and/or the like. These and other input devices are connected to the processing unit 604 via input/output interfaces 640 that are coupled to the system bus 608, but may be connected by other interface and bus structures, such as a parallel port, game port, or a universal serial bus (USB).

[00109] A monitor 642 or other type of display device can also be connected to the system bus 608 via an interface, such as a video adapter 644. In addition to the monitor 642, other output peripheral devices can include components such as speakers (not shown) and a printer 646 which can be connected to computer 602 via the input/output interfaces 640.

[00110] Computer 602 can operate in a networked environment using logical connections to one or more remote computers, such as a remote computing device 648. By way of example, the remote computing device 648 can be a personal computer, portable computer, a server, a router, a network computer, a peer device or other common network node, game console, and the like. The remote computing device 648 is illustrated as a portable computer that can include many or all of the elements and features described herein relative to computer 602.

[00111] Logical connections between computer 602 and the remote computer 648 are depicted as a local area network (LAN) 650 and a general wide area network (WAN) 652. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

[00112] When implemented in a LAN networking environment, the computer 602 is connected to a local network 650 via a network interface or adapter 654. When implemented in a WAN networking environment, the computer 602 typically includes a modem 656 or other means for establishing communications over the wide network 652. The modem 656, which can be internal or external to computer 602, can be connected to the system bus 608 via the input/output interfaces 640 or other appropriate mechanisms. It is to be appreciated that the illustrated network connections are exemplary and that other means of establishing communication link(s) between the computers 602 and 648 can be employed.

[00113] In a networked environment, such as that illustrated with computing environment 600, program modules depicted relative to the computer 602, or portions thereof, may be stored in a remote memory storage device. By way of example, remote application programs 658 reside on a memory device of remote computer 648. For purposes of illustration, application programs and other executable program components such as the operating system are illustrated herein as discrete blocks, although it is recognized that such programs and components

reside at various times in different storage components of the computing device 602, and are executed by the data processor(s) of the computer.

[00114] Various modules and techniques may be described herein in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Typically, the functionality of the program modules may be combined or distributed as desired in various implementations.

[00115] An implementation of these modules and techniques may be stored on or transmitted across some form of computer-readable media. Computer-readable media can be any available media that can be accessed by a computer. By way of example, and not limitation, computer-readable media may comprise "computer storage media" and "communications media."

[00116] "Computer storage media" includes volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules, or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices,

or any other medium which can be used to store the desired information and which can be accessed by a computer.

[00117] "Communication media" typically includes computer-readable instructions, data structures, program modules, or other data in a modulated data signal, such as carrier wave or other transport mechanism. Communication media also includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), infrared (IR), wireless fidelity (e.g., IEEE 802.11b wireless networking) (Wi-Fi), cellular, Bluetooth enabled, and other wireless media. Combinations of any of the above are also included within the scope of computer-readable media.

[00118] CONCLUSION

[00119] Although the invention has been described in language specific to structural features and/or methodological acts, it is to be understood that the invention defined in the appended claims is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as exemplary forms of implementing the claimed invention. For example, the elliptic curves discussed herein are a one-dimensional case of Abelian varieties. Also, isogenies may be used in other applications such as blind signatures, hierarchical

systems, and the like. As such, the techniques described herein may be applied to higher dimension Abelian varieties.

CLAIMS

What is claimed is:

1. A method comprising:

generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve;

publishing a public key corresponding to the isogeny;

encrypting a message using a encryption key corresponding to the isogeny; and

decrypting the encrypted message using a decryption key corresponding to the isogeny.

2. A method as recited by claim 1, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny.

3. A method as recited by claim 1, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof.

4. A method as recited by claim 1, wherein the generating maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

5. A method as recited by claim 1, wherein the decrypting is performed by bilinear pairing.

6. A method as recited by claim 5, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

7. A method as recited by claim 1, wherein the method is applied using Abelian varieties.

8. A method as recited by claim 1, wherein the method signs the message.

9. A method as recited by claim 1, wherein the method provides identity based encryption.

10. A method as recited by claim 1, further comprising composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves.

11. A method as recited by claim 1, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

12. A method as recited by claim 1, further comprising using a trace map to shorten points on an Abelian variety.

13. A method comprising:

publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; and

decrypting an encrypted message using a decryption key corresponding to the isogeny.

14. A method as recited by claim 13, wherein the decryption key is a dual isogeny of the isogeny.

15. A method as recited by claim 13, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof.

16. A method as recited by claim 13, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

17. A method as recited by claim 13, wherein the decryption is performed by bilinear pairing.

18. A method as recited by claim 17, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

19. A method as recited by claim 13, wherein the method is applied using Abelian varieties.

20. A method as recited by claim 13, wherein the method signs the message.

21. A method as recited by claim 13, wherein the method provides identity based encryption.

22. A method as recited by claim 13, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

23. A system comprising:

a first processor;

a first system memory coupled to the first processor, the first system memory storing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve;

a second processor;

a second system memory coupled to the second processor, the second system memory storing an encrypted message and a decryption key corresponding to the isogeny to decrypt the encrypted message,

wherein the encrypted message is encrypted using an encryption key.

24. A system as recited by claim 23, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny.

25. A system as recited by claim 23, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

26. A system as recited by claim 23, wherein the decryption is performed by bilinear pairing.

27. A system as recited by claim 26, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

28. One or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; and

decrypting an encrypted message using a decryption key corresponding to the isogeny.

29. One or more computer-readable media as recited by claim 28, wherein the decryption key is a private key, the private key being a dual isogeny of the isogeny.

30. One or more computer-readable media as recited by claim 28, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof.

31. One or more computer-readable media as recited by claim 28, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

32. One or more computer-readable media as recited by claim 28, wherein the decrypting is performed by bilinear pairing.

33. One or more computer-readable media as recited by claim 32, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

34. One or more computer-readable media as recited by claim 28, wherein the acts are applied using Abelian varieties.

35. One or more computer-readable media as recited by claim 28, wherein the acts further comprise using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

36. One or more computer-readable media as recited by claim 28, wherein the acts further comprise composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves.

37. One or more computer-readable media as recited by claim 28, wherein the acts further comprise using a trace map to shorten points on an Abelian variety.

38. One or more computer-readable media as recited by claim 28, wherein the acts sign the message.

39. One or more computer-readable media as recited by claim 28, wherein the acts provide identity based encryption.

USE OF ISOGENIES FOR DESIGN OF CRYPTOSYSTEMS

Techniques are disclosed to provide public-key encryption systems. More particularly, isogenies of Abelian varieties (e.g., elliptic curves in one-dimensional cases) are utilized to provide public-key encryption systems. For example, the isogenies permit the use of multiple curves instead of a single curve to provide more secure encryption. The techniques may be applied to digital signatures and/or identity based encryption (IBE) solutions. Furthermore, the isogenies may be used in other applications such as blind signatures, hierarchical systems, and the like. Additionally, solutions are disclosed for generating the isogenies.

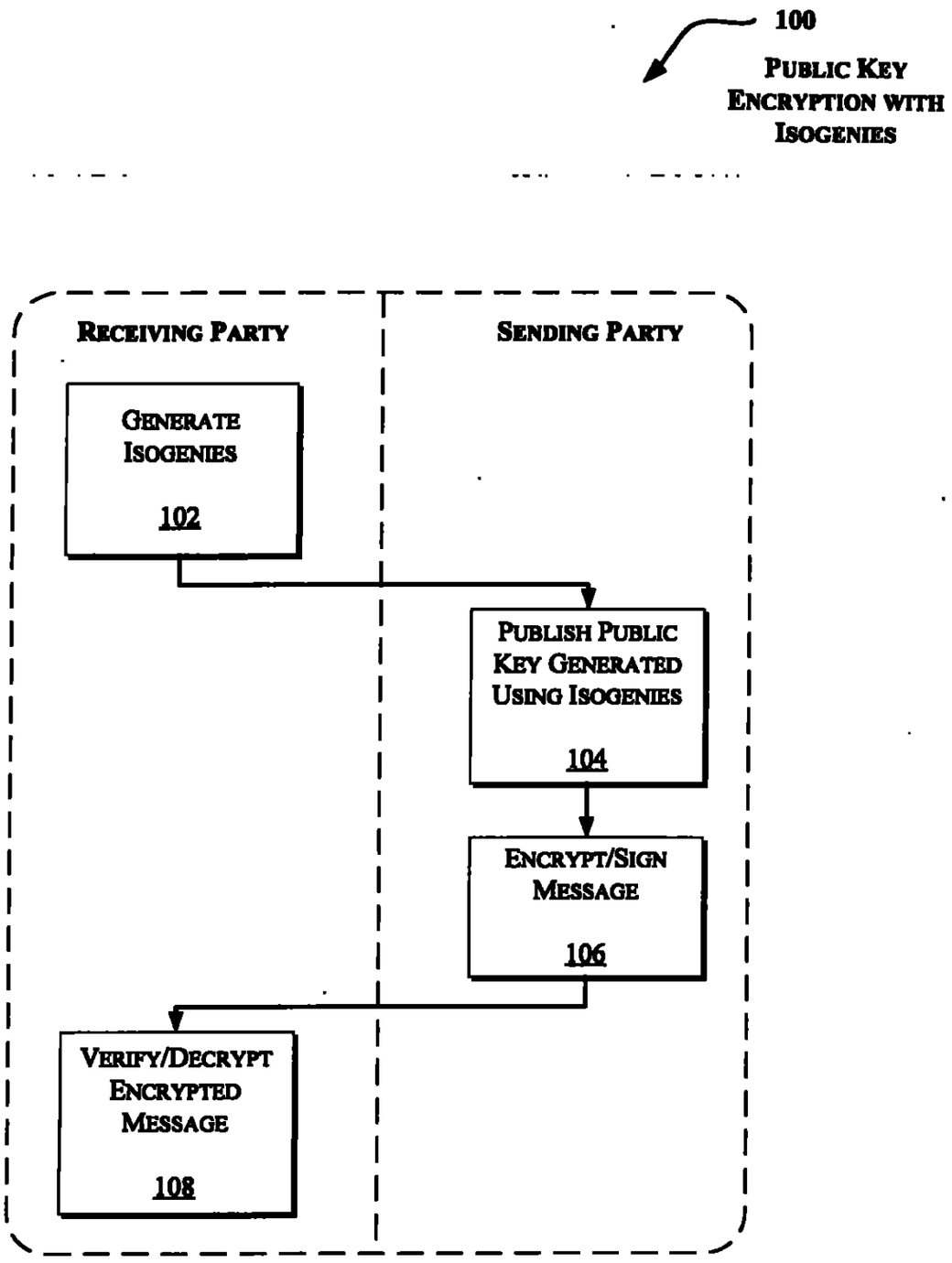

100
PUBLIC KEY ENCRYPTION WITH ISOGENIES
RECEIVING PARTY
SENDING PARTY
GENERATE ISOGENIES
102
PUBLISH PUBLIC KEY GENERATED USING ISOGENIES
104
ENCRYPT/SIGN MESSAGE
106
VERIFY/DECRYPT ENCRYPTED MESSAGE
108

FIG. 1

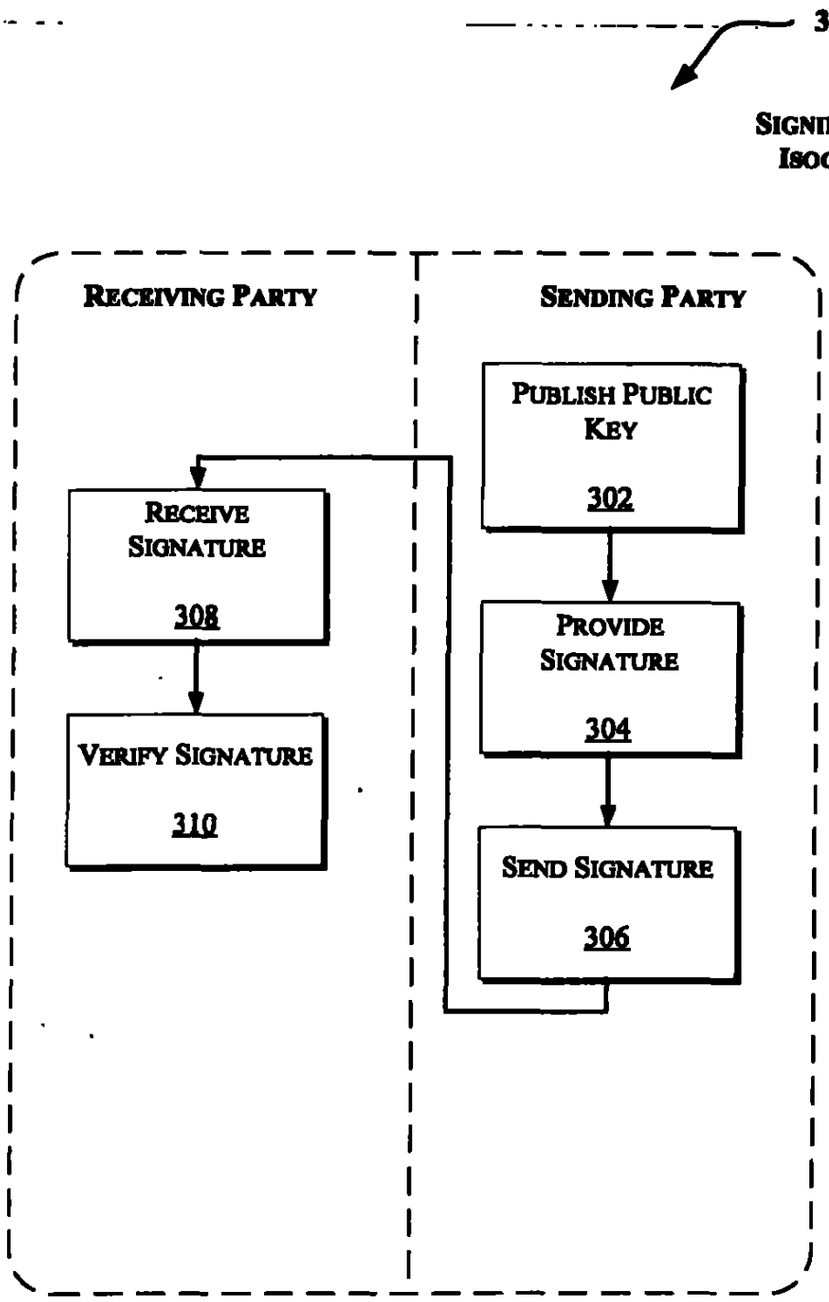

300
SIGNING WITH ISOGENIES
RECEIVING PARTY
SENDING PARTY
PUBLISH PUBLIC KEY
302
RECEIVE SIGNATURE
308
PROVIDE SIGNATURE
304
VERIFY SIGNATURE
310
SEND SIGNATURE
306

FIG. 3

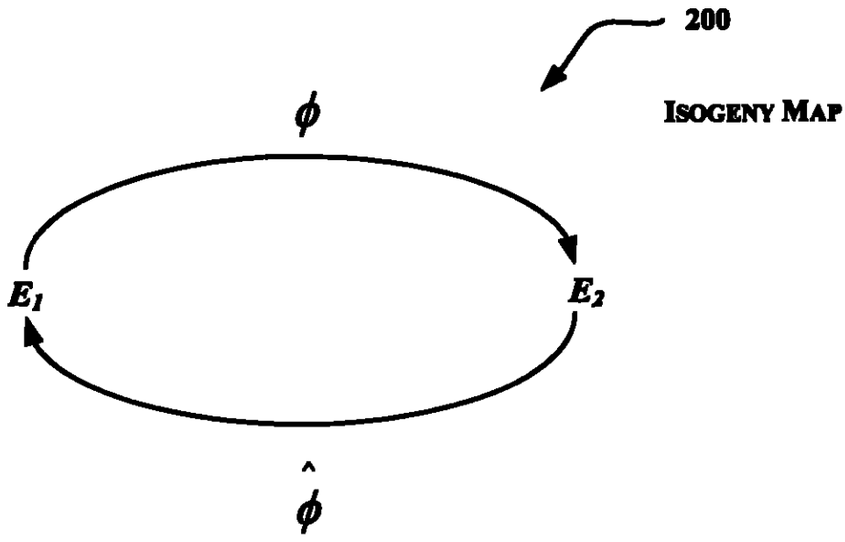

200
ISOGENY MAP
ϕ
E_1
E_2
$\hat{\phi}$

FIG. 2

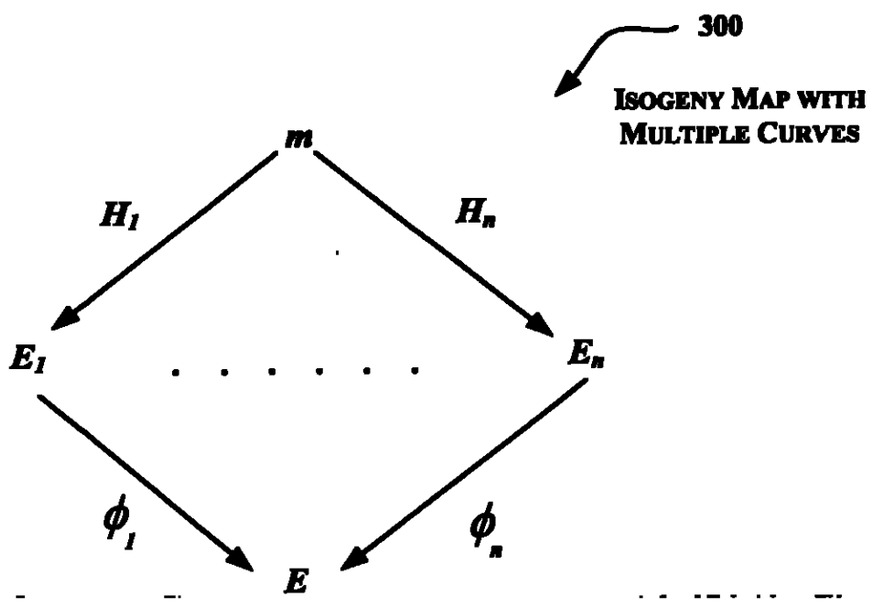

300
ISOGENY MAP WITH MULTIPLE CURVES
m
H_1
H_n
E_1
E_n
ϕ_1
ϕ_n
E

FIG. 4

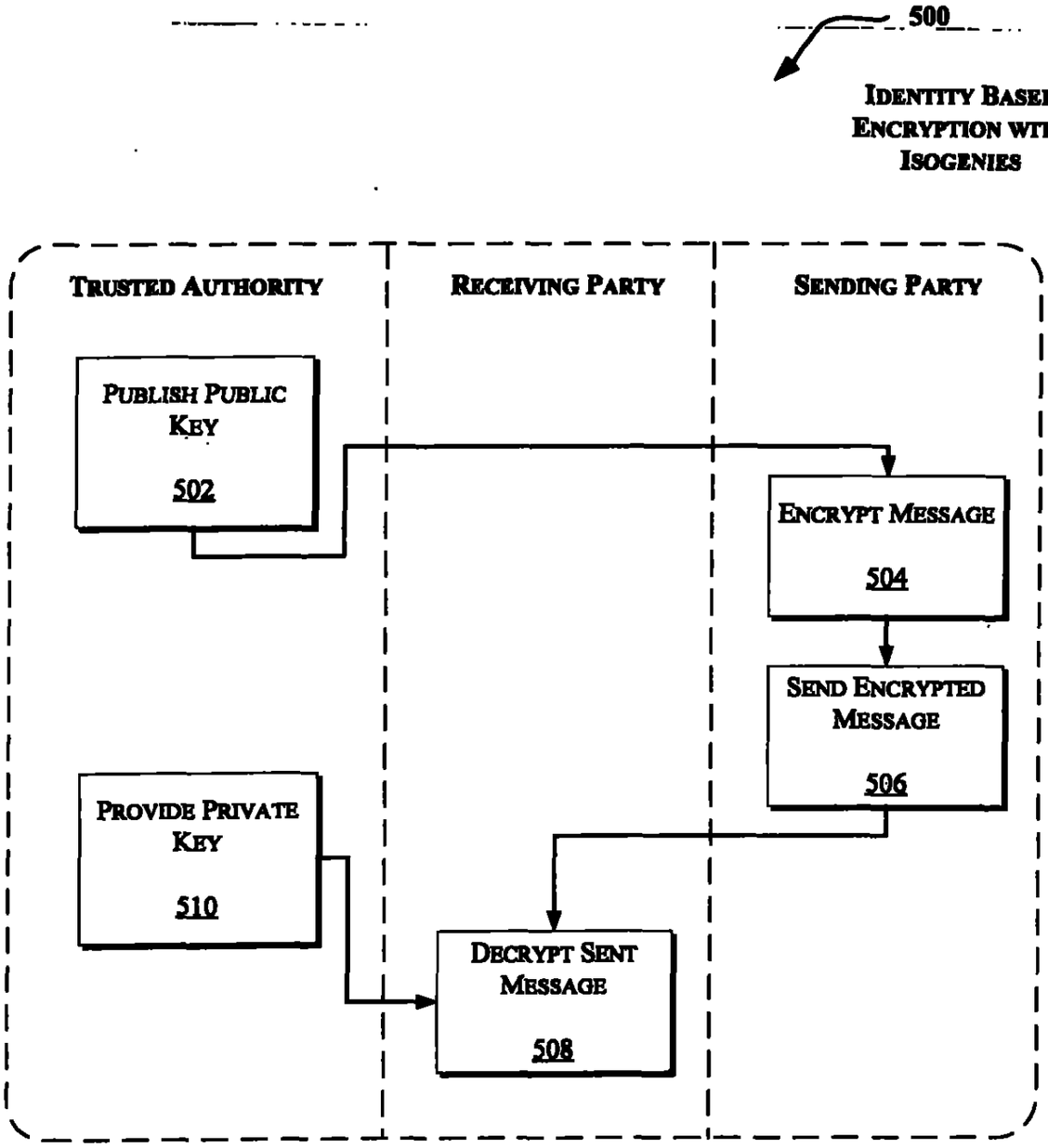

500
IDENTITY BASED ENCRYPTION WITH ISOGENIES
TRUSTED AUTHORITY
RECEIVING PARTY
SENDING PARTY
PUBLISH PUBLIC KEY
502
ENCRYPT MESSAGE
504
SEND ENCRYPTED MESSAGE
506
PROVIDE PRIVATE KEY
510
DECRYPT SENT MESSAGE
508

FIG. 5

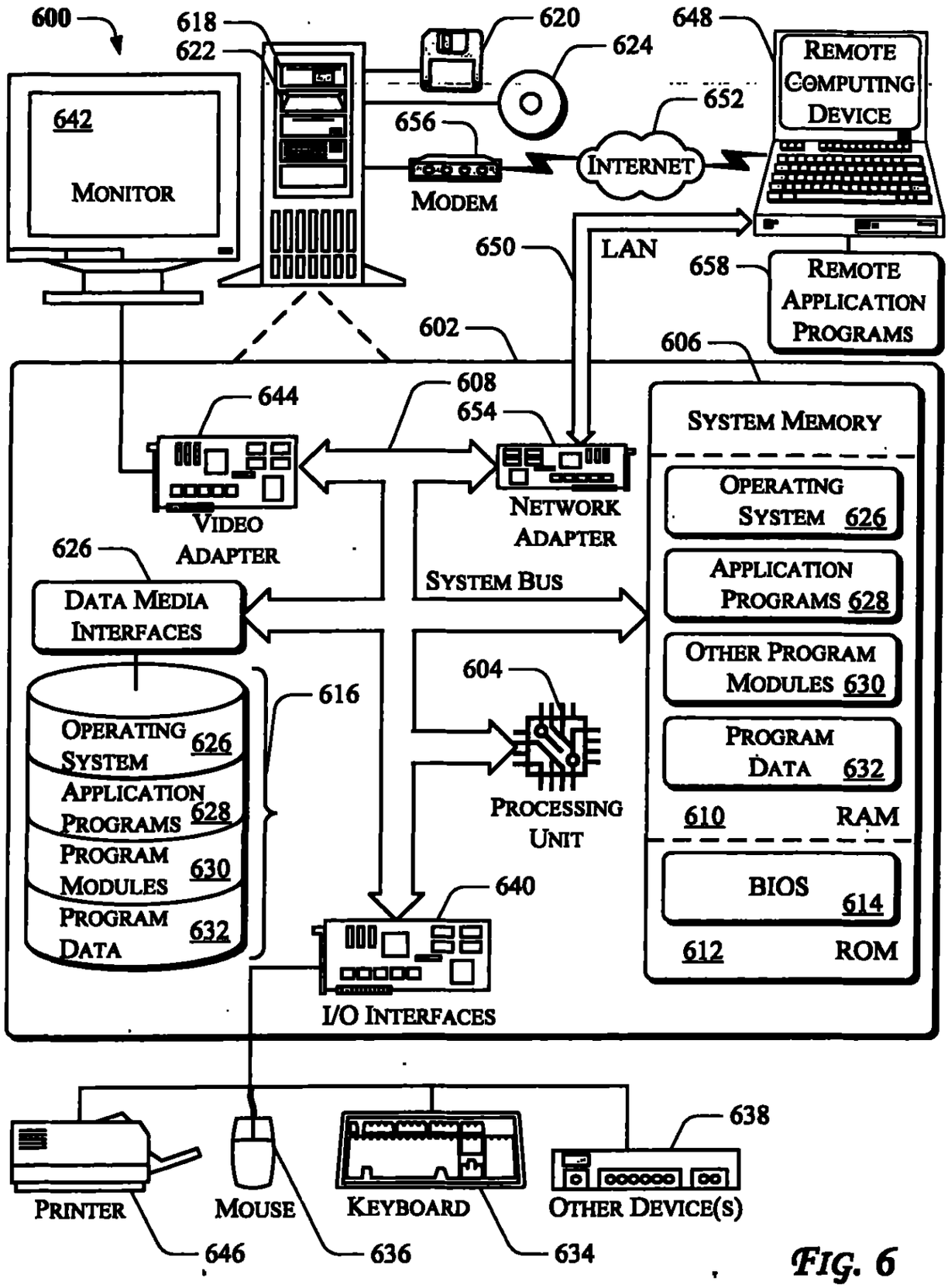

600
618
622
620
624
648
REMOTE COMPUTING DEVICE
642
MONITOR
656
MODEM
652
INTERNET
650
LAN
658
REMOTE APPLICATION PROGRAMS
602
606
644
608
654
SYSTEM MEMORY
VIDEO ADAPTER
NETWORK ADAPTER
OPERATING SYSTEM 626
626
SYSTEM BUS
APPLICATION PROGRAMS 628
DATA MEDIA INTERFACES
OTHER PROGRAM MODULES 630
604
616
PROGRAM DATA 632
OPERATING SYSTEM 626
APPLICATION PROGRAMS 628
PROGRAM MODULES 630
PROGRAM DATA 632
PROCESSING UNIT
610
RAM
BIOS 614
640
612
ROM
I/O INTERFACES
638
PRINTER
MOUSE
KEYBOARD
OTHER DEVICE(S)
646
636
634

FIG. 6

80

REQUISITOS NECESARIOS PARA PRESENTACION Y AGILIZACION DEL TRAMITE

USUARIO · RADICADOR

PATENTE DE INVENCIÓN · MODELO DE UTILIDAD ( ) ( )

- Indicación de que se solicita la concesión de una patente ( ) ( )
- Datos de identificación del solicitante o de la persona que se presenta la solicitud. ( ) ( )
- Descripción de la invención ( ) ( )
- Dibujos de ser estos pertinentes ( ) ( )
- Comprobante de Pago de las tasas establecidas

COMPLETA ( ) INCOMPLETA ( ) ( )

DISEÑO INDUSTRIAL ( )

- Indicación de que se solicita el registro de Diseño Industrial ( ) ( )
- Datos de identificación del solicitante o de la persona que presenta la solicitud. ( ) ( )
- Representación gráfica o fotográfica del Diseño Industrial o muestra del Material que incorpora el diseño ( ) ( )
- Comprobante de pago de las tasas establecidas ( ) ( )

COMPLETA ( ) INCOMPLETA ( ) ( )

ESQUEMA DE TRAZADO ( )

- Indicación de que solicita el registro de un Esquema de trazado. ( ) ( )
- Datos de identificación del solicitante o de la persona que presenta La solicitud. ( ) ( )
- Representación gráfica del esquema de trazado ( ) ( )
- Comprobante de pago de las tasas establecidas. ( ) ( )

COMPLETA ( ) INCOMPLETA ( ) ( )

Firma Responsable:

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Radicacion : 04094973 00000000 Folios: 79
Fecha (AMD): 2004-09-23 17:01:36
Tramite : 002 PATENTES D 1 REGISTRO/ 411 PRESENTA
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Fecha:

Industria y Comercio
SUPERINTENDENCIA

PROTOCOLO

Expediente 04-94973

SUPERINDUSTRIA Y COMERCIO
SISTEMA DE REGISTRO

MANTENIMIENTO DE PROTOCOLOS

Numero : 16069
Fecha : 04/08/1995
Conferido: MICROSOFT CORPORATION

Pais : US ESTADOS UNIDOS DE AMERICA

Ciudad : 234 REDMOND, WASHINGTON

Represent: S Sustituir : S Desistir : S
No. Radicacion : 95 34920 Clase: 0 Seev: 0 Seac: 0

scncia	Codigo	Ctr	Nombre
1	77	A	CARDENAS NAVAS DARIO
2	3653		CARDENAS CABALLERO EDUARDO
3	5048		CARDENAS MARTINEZ BERNARDO

Encontrados (1/1) registro(s)

Carrera 13 No. 27-00 Pisos 5, 7 y 10
Conmutador: 382 0840
Fax: 350 5220
E-mail: info@sic.gov.co
www.sic.gov.co
Bogotá, D.C., Colombia

2020
Bogotá, D. C.

Doctor(a)
DARIO CARDENAS NAVAS
Apoderado(a)

Oficio No.
10016

REFERENCIA:		
	Radicación	04-94973
	Trámite	002
	Evento	001
	Actuación	430
	Folios	001

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, se le comunica que:

- Allegar copia del documento en que conste la cesión del derecho a la patente otorgado por los inventores al solicitante o a su causante. (art. 26-k,Dec 486/2000).

- Para efectos de entendimiento, y posterior digitalización de la solicitud es importante que los documentos aportados se encuentren completos, por lo tanto se sugiere enviar un nuevo capítulo reivindicatorio, ya que el presentado con la solicitud contiene defectos en la numeración.

En cumplimiento del artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos (2) meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Unica No.10 de 2001.

ALIX CESPEDES DE VERGEL
Jefe de la División de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista de fecha 28 ... ...

Se recuerda al interesado que debe presentar, dentro de los diecidós meses siguientes contados a partir de la fecha de presentación de la solicitud cuya prioridad se invoca, copia de la misma certificada por la autoridad que la expidió y, en los casos en que haya lugar, la traducción simple del capítulo reivindicatorio. El incumplimiento de éste plazo, acarreará la pérdida de la prioridad invocada.

202027