229

SUPERINDUSTRIA Y COMERCIO
Radicacion : 04094973 00000003 Folios: 9
Fecha (AMD): 2004-12-21 16:04:58
Tramite : 002 PATENTES D 1 REGISTRO/ 444 PROPUESTA
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Señores
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISIÓN DE NUEVAS CREACIONES
E. S. D.

Ref.: Expediente No. 04-094.973
Solicitud de Patente para "USO DE ISOGENOS PARA EL DISEÑO DE CRIPTOSISTEMAS".

Solicitante: Microsoft Corporation.

Darío Cárdenas Navas, identificado como aparece al pie de mi firma, atentamente me dirijo a ese Despacho dando respuesta en término al Oficio No. 10016 de fecha 28 de Octubre de 2004.

Informo a ese Despacho que revisados los documentos adjuntos al memorial de fecha 17 de Diciembre de 2004 y debido a razones de numerado automático del software encontramos que en el capítulo reivindicatorio adjunto persistieron ciertos errores involuntarios de numeración.

Por lo anterior, me permito adjuntar nuevamente el capítulo reivindicatorio debidamente numerado. Solicito a ese Despacho que tome en cuenta este último documento para efectos de entendimiento y posterior digitalización de la solicitud.

Atentamente,

Darío Cárdenas Navas
c.c. 17.066.629 de Bogotá
t.p. 1.250 Minjusticia

jag/correspo/Microsoft.patentes.usodelsogenos.doc
f. p-283

REIVINDICACIONES

Lo que se reivindica 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 isógeno; y

que descifra el mensaje encriptado que usa una clave de descencriptación correspondiendo al isógeno.

2. Un método como el citado por la reivindicación1, 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 reivindicación 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 reivindicación 1, en donde los mapas generan una pluralidad de puntos de una primera curva elíptica hacia una pluralidad de curvas elípticas.

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

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

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

9. Un método como el citado por la reivindicación 1, en donde el método proporciona la identidad basada en la encriptación.

10. Un método como recitado por reivindicación 1, que se compone además de una pluralidad de isógenos modular para proporcionar el isógeno sin revelar cualquier curva intermedias.

11. Un método como el citado por la reivindicación 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.

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

13. 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.

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

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

18. Un método como el citado por reivindicación 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 reivindicación 13, en donde el método es aplicado usando variaciones de Abehan.

20. Un método como el citado por la reivindicación 13, en donde el método señala el mensaje.

21. Un método como el citado por la reivindicación 13, en donde el método proporciona la identidad basado en la encriptación.

22. Un método como el citado por la reivindicación 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 una 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 memoria almacenando un mensaje encriptado y una clave de descencripción 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 reivindicación 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 reivindicación 23, en donde el isógeno rastrea un pluralidad de puntos de una primera curva elíptica sobre una pluralidad de curvas elípticas.

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

27. Un sistema como el citado por reivindicación 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 reivindicación 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 reivindicación 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 reivindicación 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 reivindicación 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 reivindicación 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 reivindicación 28, en donde las acciones son aplicadas usando variacions de Abelian.

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

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