(11) **MX 345371 B**

IMPI
INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

(12) **SOLICITUD de PATENTE**

(43) Fecha de publicación: **27/01/2017**

(22) Fecha de presentación: **16/06/2015**
(21) Número de solicitud: **2015007704**

(51) Int. Cl: ***H04L 9/08*** *(2006.01)*
H04L 29/06 (2006.01)

(86) Número de solicitud PCT: **EP 2013/077842**
(87) Número de publicación PCT: **WO 2014/096420 (26/06/2014)**

(30) Prioridad(es): **21/12/2012 US 61/740,488**
21/12/2012 EP 12198794.5

(71) Solicidante:
KONINKLIJKE PHILIPS N.V.
High Tech Campus 5 NL-5656 AE Eindhoven NL

(72) Inventor(es):
Oscar GARCIA MORCHON
High Tech Campus 5 AE Eindhoven NL-5656 NL
Ludovicus Marinus Gerardus Maria TOLHUIZEN
Jaime GUTIERREZ
Domingo GOMEZ

(74) Representante:
Francisco Javier UHTHOFF ORIVE
Hamburgo No. 260 CUAUHTEMOC Distrito Federal 06600 MX

(54) Título: **DISPOSITIVO DE RED DE CLAVES COMPARTIDAS Y SU CONFIGURACION.**

(54) Title: **KEY SHARING NETWORK DEVICE AND CONFIGURATION THEREOF.**

(57) Resumen

Un método de configuración de un dispositivo de red para compartir claves, el método comprende obtener (410) en forma electrónica por lo menos dos conjuntos de parámetros, un conjunto de parámetros comprende un módulo privado (p1), un módulo público (N), y un polinomio bivariable (f1) que tiene coeficientes enteros, la representación binaria del módulo público y la representación binaria del módulo, privado son las mismas en por lo menos bits consecutivos de longitud clave (b), generar material de clave local para el dispositivo de red que comprende obtener (420) en forma electrónica un número de identidad (A) para el dispositivo de red, y para cada conjunto de parámetros de los por lo menos dos conjuntos de parámetros obtener un polinomio monovariable correspondiente, determinando, mediante el uso de un dispositivo de manipulación polinomial, un polinomio monovariable a partir del polinomio bivariable del conjunto de parámetros sustituyendo (430) el número de identidad en el polinomio bivariable y reduciendo el resultado de la sustitución módulo el módulo privado del conjunto de parámetros, y almacenar electrónicamente (450) en el dispositivo de red el material de clave local generado, el material de clave local generado comprende el módulo público de cada conjunto de parámetros y el polinomio monovariable correspondiente de cada conjunto de parámetros.

(57) Abstract

A method of configuring a network device for key sharing, the method comprising obtaining (410) in electronic form at least two parameter sets, a parameter set comprising a private modulus (p 1) a public modulus (N), and a bivariate polynomial (f 1) having integer coefficients, the binary representation of the public modulus and the binary representation of the private modulus are the same in at least key length (b) consecutive bits, generating local key material for the network device comprising obtaining (420) in electronic form an identity number (A) for the network device, and for each parameter set of the at least two parameter sets obtaining a corresponding univariate polynomial, by determining, using a polynomial manipulation device, a univariate polynomial from the bivariate polynomial of the parameter set by substituting (430) the identity number into said bivariate polynomial, and reducing the result of the substitution modulo the private modulus of the parameter set, and electronically storing (450) at the network device the generated local key material, the generated

local key material comprising the public modulus of each parameter set and the corresponding univariate polynomial of each parameter set.

SE
SECRETARÍA DE ECONOMÍA

Instituto Mexicano de la Propiedad Industrial

TÍTULO DE PATENTE NO. 345371

Titular(es): KONINKLIJKE PHILIPS N.V.

Domicilio: High Tech Campus 5, NL-5656, AE Eindhoven, PAÍSES BAJOS

Denominación: DISPOSITIVO DE RED DE CLAVES COMPARTIDAS Y SU CONFIGURACIÓN.

Clasificación: Int.Cl.8: H04L29/06; H04L9/08

Inventor(es): DOMINGO GOMEZ; OSCAR GARCIA MORCHON; LUDOVICUS MARINUS GERARDUS MARIA TOLHUIZEN; JAIME GUTIERREZ

SOLICITUD

Número:	Fecha de presentación internacional:
MX/a/2015/007704	20 de Diciembre de 2013

PRIORIDAD

País:	Fecha:	Número:
EP	21 de diciembre de 2012	12198794.5
US	21 de diciembre de 2012	61/740,488

Vigencia: Veinte años

Fecha de Vencimiento: 20 de diciembre de 2033

La patente de referencia se otorga con fundamento en los artículos 1°, 2° fracción V, 6° fracción III, y 59 de la Ley de la Propiedad Industrial.

De conformidad con el artículo 23 de la Ley de la Propiedad Industrial, la presente patente tiene una vigencia de veinte años improrrogables, contada a partir de la fecha de presentación de la solicitud internacional y estará sujeta al pago de la tarifa para mantener vigentes los derechos.

Quien suscribe el presente título lo hace con fundamento en lo dispuesto por los artículos 6° fracciones III y 7° bis 2 de la Ley de la Propiedad Industrial (Diario Oficial de la Federación (D.O.F.) 27/06/1991, reformada el 02/08/1994, 25/10/1996, 26/12/1997, 17/05/1999, 26/01/2004, 16/06/2005, 25/01/2006, 06/05/2009,06/01/2010, 18/06/2010, 28/06/2010, 27/01/2012 y 09/04/2012); artículos 1°, 3° fracción V inciso a), 4° y 12° fracciones I y III del Reglamento del Instituto Mexicano de la Propiedad Industrial (D.O.F. 14/12/1999, reformado el 01/07/2002, 15/07/2004, 28/07/2004 y 7/09/2007); artículos 1°, 3°, 4°, 5° fracción V inciso a), 16 fracciones I y III y 30 del Estatuto Orgánico del Instituto Mexicano de la Propiedad Industrial (D.O.F. 27/12/1999, reformado el 10/10/2002, 29/07/2004, 04/08/2004 y 13/09/2007); 1°, 3° y 5° inciso a) del Acuerdo que delega facultades en los Directores Generales Adjuntos, Coordinador, Directores Divisionales, Titulares de las Oficinas Regionales, Subdirectores Divisionales, Coordinadores Departamentales y otros subalternos del Instituto Mexicano de la Propiedad Industrial. (D.O.F. 15/12/1999, reformado el 04/02/2000, 29/07/2004, 04/08/2004 y 13/09/2007).

Fecha de expedición: 27 de enero de 2017

LA DIRECTORA DIVISIONAL DE PATENTES

NAHANNY CANAL REYES

Arenal No. 550, Piso 1,
Col. Pueblo Santa María Tepepan,
Xochimilco, C.P. 16020,
Ciudad de México
Tel. (55) 53 34 67 00 www.impi.gob.mx

MX/2017/9740

DISPOSITIVO DE RED DE CLAVES COMPARTIDAS Y SU CONFIGURACIÓN

Campo de la Invención

La invención se relaciona con un método de configuración de un dispositivo de red par compartir claves, el método comprende generar material de claves locales para el dispositivo de red que comprende obtener en forma electrónica un número de identidad para el dispositivo de red, determinar mediante el uso de un dispositivo de manipulación polinomial un polinomio monovariable a partir de un polinomio bivariable por sustitución del número de identidad en el polinomio bivariable, y almacenar electrónicamente el material de clave generada en el dispositivo de red.

La invención se relaciona además con un método para un primer dispositivo de red para determinar una clave compartida, la clave es una clave cifrada, el método comprende, obtener el material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende un polinomio monovariable, obtener un número de identidad para un segundo dispositivo de red, el segundo dispositivo de red es diferente del primer dispositivo de red, sustituir el número de identidad del segundo dispositivo de red en el polinomio monovariable y derivar de ahí la clave compartida.

La invención se relaciona además con un sistema para

configurar un dispositivo de red para compartir claves, y con un dispositivo de red configurado para determinar una clave compartida.

Antecedentes de la Invención

El artículo de Song Guo, y colaboradores: "A Permutation-Based Multi-Polynomial Scheme for Pairwise Key Establishment in Sensor Networks", COMMUNICATIONS (ICC), 2010 IEEE INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, EE.UU., 23 de mayo de 2010 (2010-05-23), páginas 1-5, describe una solución de técnica anterior.

Dada una red de comunicaciones que comprende múltiples dispositivos de red, es problemático establecer conexiones seguras entre pares de tales dispositivos de red. Una manera de lograr esto se describe en C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro y M. Yung, "Perfectly-Secure Key distribution for Dynamic Conferences", Springer Lecture Notes in Mathematics, Vol. 740, páginas 471-486, 1993 (citado como 'Blundo').

Supone una autoridad central, también citada como autoridad de red o como tercera parte confiable (TTP, por sus siglas en inglés), que genera un polinomio bivariable simétrico f(x,y), con coeficientes en el campo finito F con p elementos, en donde p es un número primo o una potencia de un número primo. Cada dispositivo tiene un número de identidad en F y está provisto con material de clave local por medio de

TTP. Para un dispositivo con identificador η, el material de clave local son los coeficientes del polinomio $f(\eta,y)$.

Si un dispositivo η desea comunicarse con un dispositivo η', utiliza su material de clave para generar la clave $K(\eta,\eta) = f(\eta,\eta')$. Como f es simétrica, se genera la misma clave.

Un problema de este esquema de clave compartida ocurre si un atacante conoce el material de clave de r+1 o más dispositivos, en donde t es el grado del polinomio bivariable. El atacante puede reconstruir entonces el polinomio $f(x,y)$. En ese momento la seguridad del sistema está completamente quebrantada. Dados los números de identidad de cualesquiera dos dispositivos, el atacante puede reconstruir la clave compartida entre este par de dispositivos.

Breve Descripción de la Invención

Sería ventajoso tener un método mejorado para establecer una clave compartida entre dos dispositivos de red. La invención está definida por las reivindicaciones; las reivindicaciones dependientes definen modalidades ventajosas. Se proporciona un dispositivo de red para compartir claves, y un método para un dispositivo de red para determinar una clave compartida.

El método de configuración de un dispositivo de red para compartir claves comprende obtener en forma electrónica por lo menos dos conjuntos de parámetros, un conjunto de

parámetros comprende un módulo privado, un módulo público y un polinomio bivariable que tiene coeficientes enteros, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en por lo menos bits consecutivos de longitud clave, generar material de clave local para el dispositivo de red que comprende obtener en forma electrónica un número de identidad para el dispositivo de red, y para cada conjunto de parámetros de los por lo menos dos conjunto de parámetros obtener un polinomio monovariable correspondiente, por medio de: determinar utilizando un dispositivo de manipulación polinomial un polinomio monovariable a partir del polinomio bivariable del conjunto de parámetros sustituyendo el número de identidad en el polinomio bivariable y reduciendo el resultado de la sustitución módulo el módulo privado del conjunto de parámetros, y almacenar electrónicamente en el dispositivo de red el material de clave local generado, el material de clave local generado comprende el módulo público de cada conjunto de parámetros y el polinomio monovariable correspondiente de cada conjunto de parámetros.

El método para un primer dispositivo de red para determinar una clave compartida, siendo la clave una clave cifrada, comprende, obtener material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende por lo menos dos polinomios

monovariables opcionalmente ofuscados y los módulos públicos correspondientes, obtener un número de identidad para un segundo dispositivo de red, el segundo dispositivo de red es diferente del primer dispositivo de red, para cada uno de los dos polinomios monovariables opcionalmente ofuscados: sustituir el número de identidad del segundo dispositivo de red en el polinomio monovariable, y reducir el resultado de la sustitución módulo el módulo público que corresponde al polinomio monovariable, y sumar entre sí los resultados de las reducciones módulo un módulo público y reducir módulo un módulo de clave, y derivar la clave compartida del resultado de la reducción módulo el módulo de clave.

En una modalidad, el método comprende reducir el resultado de la sustitución módulo el módulo público dividiendo el resultado entre una potencia de dos, y reduciendo módulo un módulo de clave.

Cualquier par de dos dispositivos de red de los múltiples dispositivos de red cada uno teniendo un número de identidad y material de clave local generado para el número de identidad son capaces de negociar una clave compartida con pocos recursos. Los dos dispositivos de red solo necesitan intercambiar sus números de identidad, lo cual no necesita mantenerse en secreto, y realizar cálculos polinomiales. El tipo de cálculos necesarios no requieren grandes recursos de cálculo, lo cual significa que este método es adecuado para

un tipo de aplicaciones de alto volumen y bajo costo.

El material de clave local se ha obtenido de un polinomio común en el material de clave raíz; esto permite que ambos dispositivos de red en un par de dispositivos de red obtengan la misma clave compartida. Si todos los polinomios bivariables son simétricos en comparación con cualquiera de dos dispositivos de red pueden derivar un polinomio común. Si algunos o todos los polinomios bivariables son asimétricos algún par de dispositivos pueden y algunos no pueden derivar una clave compartida.

El material de clave local se deriva del conjunto de parámetros, en particular de múltiples módulos públicos diferentes y múltiples polinomios bivariables. El material de clave local resultante comprende múltiples, típicamente diferentes, polinomios monovariables cada uno con un módulo público correspondiente.

Si solo se utilizara un conjunto de parámetros, entonces el dispositivo de red está provisto con coeficientes de un polinomio de tal manera que al evaluarlo con el módulo N y tomando b bits es capaz de generar una clave de b bits con otro dispositivo. Esto se relaciona con el denominado problema de interpolación polinomial ruidosa, es decir, al tener muchos de esas claves de b bits, un atacante podría ser capaz de recuperar el polinomio de una entidad dada bajo ataque.

Por ejemplo, un ataque que se enfrenta a un sistema de un solo conjunto de parámetros podría obtener esos valores de b bits siguiendo 2 pasos: el atacante compromete N_c dispositivos asociados con N_c materiales clave, y el atacante utiliza esos N_c materiales clave para obtener N_c claves de b bits (al evaluar cada uno de los materiales clave en el identificador del dispositivo bajo ataque). Esto significa que el avance hecho en el problema de interpolación polinomial ruidoso puede extenderse a ataques en el sistema de un solo conjunto de parámetros. Esto se considera no deseable.

Al tener múltiples conjuntos de parámetros se evita este problema al mezclar operaciones modulares en el dispositivo así como también durante la generación de claves locales.

La clave común compartida KAB entre entre un par de dispositivos A y B se obtiene como la adición de por lo menos dos (en general m') subclaves K^{i}_{AB}, es decir $K_{AB} = K^{1}_{AB} + K^{2}_{AB}$. Cada subclave K^{1}_{AB}, se genera de un material generador de claves diferente en el cual las operaciones modulares realizan módulo el módulo público Ni. Dado que las operaciones modulares se mezclan durante la generación de claves locales así como durante la generación de claves compartidas no es posible extender el ataque de la interpolación polinomial ruidosa al sistema de cifrado. Incluso si un atacante obtiene el acceso a N_c claves de b

bits, cada una de ellas se deriva de dos subclaves, cada subclave proviene de la evaluación de un material generador de claves diferente. Pero el atacante no será capaz de diferenciar las subclaves de tal manera que el atacante no puede recuperar los dos materiales generadores de claves (m' en general) del dispositivo bajo ataque.

Existen dos niveles de seriedad de los ataques en los dispositivos. En la seriedad menor el atacante solo obtiene el acceso a muchas claves compartidas comunes. En la seriedad mayor el atacante obtiene el acceso a muchos materiales de claves locales. Se tiene que el mezclado de operaciones modulares en el dispositivo de red es una buena contramedida contra el ataque de la seriedad menor. Sin embargo, si el atacante tiene acceso al material de clave entonces también tiene acceso a las subclaves.

Este último problema se evita agregando ruido a los dos materiales generadores de claves de un dispositivo. La adición de un número de ofuscación al material de clave local perturba la relación entre el material de clave local y al material de cave raíz. La relación que estaría presente entre el polinomio monovariable no ofuscado y los polinomios bivariables (simétricos) ya no está presente. Esto significa que el ataque directo en el esquema ya no funciona.

Es interesante que, al agregar ruido a los dos materiales generadores de claves de un dispositivo de tal

manera que la adición del ruido es igual a cero módulo 2b mejora más el sistema. En este caso: las claves generadas son aún ruidosas, y por lo tanto, un atacante no puede utilizarlas para recuperar el material generador de claves compartido de un dispositivo bajo ataque; sin embargo para remover el ruido, el atacante tiene que agregarlas, pero entonces tiene el valor agregado anterior y no puede diferenciar entre los componentes originados de cada uno de los materiales generadores de claves. Esta técnica puede generalizarse fácilmente a cualquier número de materiales generadores de claves. La condición solo puede extenderse para asegurar que el ruido es igual a cero en b bits localizados no en los bits significativos sino en cualquier otro lado.

En una modalidad, la representación binaria de todos los módulos públicos y la representación binaria del módulo privado en cada conjunto de parámetros son iguales en por lo menos (b) bits consecutivos de longitud de clave. Nótese que pueden usarse múltiples módulos privados: pueden elegirse de tal manera que la representación binaria de cualquiera de los múltiples módulos privados de los módulos públicos y la representación binaria del módulo privado son iguales en por lo menos (b) bits consecutivos de longitud de clave. Para cada módulo privado de los múltiples módulos privados se selecciona un polinomio bivariable opcionalmente simétrico

que tiene coeficientes enteros para obtener múltiples polinomios bivariable y opcionalmente simétricos.

Debido a que la derivación del material de clave local utiliza un módulo privado que es diferente del módulo público, la relación matemática que estaría presente cuando trabaja, por ejemplo, en un solo campo finito se perturba. Esto significa que las herramientas matemáticas usuales para analizar polinomios, por ejemplo, álgebra finita, ya no aplican. Cuando mucho un atacante puede emplear estructuras menos eficientes, tales como retículas. También cuando se deriva la clave compartida se combinan dos operaciones módulo que no son compatibles en el sentido matemático usual; por lo que la estructura matemática se evita en dos lugares. El método permite dirigir la generación de claves por pares y es flexible a la captura de un número muy alto, por ejemplo del orden de 10^5 o incluso mayor, de dispositivos de red. Por otro lado debido a que los módulos privado y público se traslapan en un número de bits consecutivos, dos dispositivos de red que tienen material de clave local son probablemente capaces de derivar la misma clave compartida.

Una percepción particular de los inventores fue que el módulo público no necesita ser un número primo. En una modalidad, el módulo público está combinado. También no hay ninguna razón por la que el módulo público deba ser un número de bits "todo en uno", por ejemplo, un número de biots que

solo consiste de T bits, en su representación binaria. En una modalidad, el módulo público no es una potencia de dos menos 1. En una modalidad, la representación binaria del módulo público comprende por lo menos un bit cero (sin contar el cero delantero, es decir, la representación binaria del módulo público comprende por lo menos un bit cero menos significativo que el bit más significativo del módulos público). En una modalidad, el módulo público es una potencia de dos menos 1 y combinado.

En una modalidad el módulo público de uno o más conjuntos de parámetros es mayor que uno o más módulos privados.

En una modalidad, por lo menos bits consecutivos de longitud de clave de la representación binaria del módulo público menos el módulo privado son todos bits cero. Esta diferencia debe evaluarse usando la representación de números firmada del módulo público menos el módulo privado, no la representación de dos complementos. Alternativamente, puede requerirse que por lo menos bits consecutivos de longitud de clave de la representación binaria del valor absoluto del módulo público menos el módulo privado sean todos bits cero. Existe un conjunto de (b) posiciones consecutivas de longitudes de clave en las cuales la representación binaria del módulo público concuerda con la representación binaria de todos los módulos privados.

Las posiciones de bits consecutivas en las cuales el módulo público concuerda con los módulos privados, pueden ser los bits menos significativos. En una modalidad, los bits de longitud de clave menos significativos de la representación binaria del módulo público menos el módulo privado son todos bits cero; esto tiene la ventaja de que no se necesita una división entre una potencia de dos cuando se deriva la clave compartida.

En una modalidad, en todos los conjunto de parámetros, los mismos por lo menos (b) bits consecutivos de longitud de clave de la representación binaria del módulo público de un conjunto de parámetros respectivo son iguales que los (b) bits de longitud de clave menos significativos. Es decir, existe un conjunto de posiciones de bits consecutivos que indican en cada conjunto de parámetros el lugar en el que los módulos público y privado concuerdan. Aunque este conjunto de posiciones de bits consecutivos es igual para todos los conjuntos de parámetros, los bits pueden ser diferentes a lo largo de los diferentes conjuntos de parámetros. En una modalidad, los por lo menos (b) bits consecutivos de longitud de clave son los (b) bits de longitud de clave menos significativos. Es decir, el conjunto de posiciones de bits son posiciones de bits menos significativas.

Se permite que un módulo privado de los múltiples módulos privados sea igual al módulo público. Sin embargo si

solo se usa un módulo privado entonces esto no es deseable.

Es deseable que los módulos privados introduzcan suficiente no linealidad. En una modalidad, existe un conjunto de posiciones de bits consecutivos en las cuales el módulo público difiere con cada uno de los módulos privados. Adicionalmente, también puede imponerse que los módulos privados difieran entre ellos mismos; una comparación de pares de la representación binaria del módulo privado también puede diferir en por lo menos un bit en un conjunto de, por ejemplo por menos bits consecutivos de longitud de clave, siendo el conjunto igual para todo módulo privado y posiblemente también lo mismo para el módulo público.

El dispositivo de red puede ser un dispositivo electrónico equipado con medios de comunicación y cómputo electrónico. El dispositivo de red puede estar unido, por ejemplo, en forma de una etiqueta de RFID, a cualquier objeto no electrónico. Por ejemplo, este método sería adecuado para la "Internet de cosas". Por ejemplo, objetos, en particular objetos de bajo costo, pueden estar equipados con etiquetas de radio a través de las cuales pueden comunicarse, por ejemplo, pueden ser identificados.

Tales objetos pueden inventariarse a través de medios electrónicos tales como una computadora. Los artículos robados o averiados pueden rastrearse y localizarse fácilmente. Una aplicación particularmente prometedora es una

lámpara que comprende un dispositivo de red configurado para determinar una clave compartida. La lámpara puede comunicar con seguridad su estado; la lámpara podría controlarse con seguridad, por ejemplo, encenderse y/o apagarse. Un dispositivo de red puede ser uno de múltiples dispositivos de red cada uno comprendiendo un comunicador electrónico para enviar y recibir un número de identidad y para enviar un mensaje de estado electrónico, y cada uno comprendiendo un circuito integrado configurado para derivar una clave compartida que sigue un método de conformidad con la invención.

En una modalidad, el método en la invención puede usarse como un método de cifrado para protocolos de seguridad, tales como IPSec, (D)TLS, HIP, o ZigBee. En particular, un dispositivo que utiliza uno de esos protocolos está asociado con un identificador. Un segundo dispositivo dispuesto a comunicarse con el primer dispositivo puede generar una clave por pares común con el primer dispositivo dado su identificador, y la clave por pares (o una clave derivada de éste por medio de, por ejemplo, una función de derivación común) puede usarse en un método de los protocolos anteriores con base en una clave previamente compartida. En particular, el identificador de un dispositivo como se define en la presente invención puede ser una dirección de red tal como una dirección corta de ZigBee, una dirección de IP o un

identificador anfitrión. Este identificador puede ser también la dirección de IEEE de un dispositivo o una cadena de bits propia asociada con el dispositivo de tal manera que el dispositivo recibe cierto material de clave local asociado con la dirección de IEEE durante la fabricación.

La derivación de una clave compartida puede usarse para muchas aplicaciones. Típicamente la clave compartida será una clave simétrica cifrada. La clave simétrica puede usarse para confidencialidad, por ejemplo, los mensajes salientes o entrantes pueden cifrarse con la clave simétrica. Solo un dispositivo con acceso tanto a los números de identidad como a uno de los dos materiales de clave local (o acceso al material de clave raíz) será capaz de descifrar las comunicaciones. La clave simétrica puede usarse para autenticación, por ejemplo, los mensajes salientes o entrantes pueden autenticarse con la clave simétrica. De esta manera puede validarse el origen del mensaje. Solo un dispositivo con acceso tanto a los números de identidad como a uno de los dos materiales de clave local (o acceso al material de clave raíz) será capaz de crear mensajes autenticados.

El método de configuración de un dispositivo de red para compartir claves típicamente será ejecutado por una autoridad de red, por ejemplo, una tercera parte confiable. La autoridad de red puede obtener el material necesario, por

ejemplo material de clave raíz de otra fuente, pero también puede generarlo por sí misma. Por ejemplo, puede generarse el módulo público. Por ejemplo, puede generarse el módulo privado, incluso si el módulo público es un parámetro de sistema y recibirse.

En una modalidad, uno o más de todos los módulos públicos N se eligen de tal manera que satisfacen $2^{(a+2)b-1} \leq N \leq 2^{(a+2)b} - 1$, en donde, a representa el grado del polinomio bivariable y b representa la longitud de la clave. Por ejemplo, en una modalidad $N = 2^{(a+2)b} - 1$. La operación módulo para ésta última selección puede implementarse de manera particularmente eficiente.

El haber fijado los módulos públicos tiene la ventaja de que no necesitan comunicarse a los dispositivos de red, sino integrarse, por ejemplo, con su software de sistema. En particular, el módulo público puede elegirse usando un generador de números aleatorios.

Los módulos públicos y privados puede representarse como una cadenas de bits. También pueden abreviarse usando cada estructura matemática particular. Por ejemplo, en lugar de guardar un módulo privado, también puede guardarse su diferencia con el módulo público, el cual es mucho más corto.

Al tener un módulo privado elegido de tal manera que un número de "longitud de clave" de por lo menos bits significativos de la representación binaria del módulo

público menos el módulo privado son todos cero bits aumenta la probabilidad de que la clave compartida en un primer dispositivo de red de un par de dispositivo de red está cerca de la clave privada derivada en un segundo dispositivo de red del par de dispositivo de red; es decir la representación binaria del módulo privado tiene los mismos bits en las posiciones menos significativas de "longitud de clave" como la representación binaria del módulo público. Por ejemplo, si la longitud de clave es 64, puede elegirse un módulo privado sustrayendo un múltiplo de 2^64 del módulo público. En una modalidad, el módulo público menos un módulo privado dividido entre dos a la potencia de la longitud de clave es menor que dos a la potencia de la longitud de clave.

En una modalidad se obtienen o generan múltiples módulos privados en forma electrónica, para cada módulo privado de los múltiples módulos privados se selecciona un polinomio bivariable opcionalmente simétrico que tiene coeficientes enteros para obtener múltiples polinomios bivariable simétricos, de tal manera que para cada módulo privado corresponde un polinomio bivariable simétrico. La determinación del polinomio monovariable comprende sustituir el número de identidad en cada uno de los múltiples polinomios bivariables simétricos, reducir módulo un módulo privado de los múltiples módulos privados que corresponden al polinomio bivariable simétrico, y sumar entre sí los

múltiples resultados de las múltiples reducciones. Al tener múltiples polinomios bivariables simétricos para diferentes módulos aumenta la seguridad porque las estructuras incompatibles se mezclas más. Típicamente los módulos privados son distintos. Teniendo múltiples módulos privados complica más el análisis aún más si las estructuras algebraicas correspondientes son muy diferentes; por ejemplo, eligiéndolos relativamente primos, en particular relativamente primos en pares, aún más en particular eligiéndolos como primos distintos.

Al tener un módulo privado diferente, y en particular múltiples módulos privados, complicará el análisis de un atacante. Para aumentar más la seguridad son posibles controles adicionales en los coeficientes. En una modalidad, la autoridad que suma entre sí los múltiples polinomios monovariables resultantes de las múltiples reducciones verifica si el valor de cada uno de los coeficientes resultantes es o muy pequeño o muy grande, por ejemplo menor que un umbral mínimo o mayor que un umbral máximo. Esto mejora la seguridad incluso más en cualquiera de los dos casos, un atacante podría hallar los componentes de las múltiples reducciones si son muy grandes o muy pequeños. Por ejemplo, si el valor de un coeficiente que resulta después de la adición es igual a 1 y solo hay dos polinomios monovariables, entonces un atacante sabe que, el coeficiente

correspondiente asociado con el primer polinomio es 1 y el asociado con el segundo polinomio es 0, o de manera contraria. En particular, la autoridad que genera el material de clave local para un dispositivo puede verificar si el valor de cada uno de los coeficientes resultantes del material generador de claves locales es por lo menos un "valor mínimo" y cuando mucho un "valor máximo". Esta comprobación puede omitirse, en particular, su el módulo público está relativamente cerca de todos los módulos privados y todos los elementos del material de clave están entre 0 y N-1. Si la TTP es capaz de asignar números de identidad también podría asignar otro número de identidad al dispositivo, si la TTP detecta coeficientes pequeños o grandes.

En una modalidad, cada módulo privado específico es tal que los (b) bits de longitud de clave menos significativos de la representación binaria del módulo público menos el módulo privado específico son todos bits cero.

El módulo público puede ser más grande o pequeño que el módulo privado. En una modalidad, la representación binaria del módulo público menos el módulo privado tiene por lo menos bits de longitud de clave todos de cero. Los bits cero por lo menos bits cero de longitud de clave son consecutivos y pueden presentarse en cualquier punto en la representación binaria. Al tener una cadena de bits cero en la diferencia

entre el módulo público y el módulo privado evita que la ofuscación sea llegue muy lejos. Nótese que la cadena puede pero no necesita estar presente en todos los conjuntos de parámetros.

En una modalidad, existe un parámetro entero 's', de tal manera que los bits menos significativos de longitud de clave del módulo público menos el módulo privado, divididos entre la potencia s son todos cero. El parámetro V es el mismo para todos los módulos privados, pero puede ser diferente para cada conjunto de parámetros.

Por ejemplo, puede definirse un divisor de cadena de bits cero que es una potencia de dos, de tal manera que cada módulo privado específico sea tal que los (b) bits de longitud de clave de la representación binaria del módulo público menos el módulo privado específico dividido entre el divisor de la cadena de bits cero sean todos bits cero. Si los bits menos significativos son cero, el divisor de cadena de bits cero puede considerarse que es 1. En una modalidad el divisor de cadena de bits cero es mayor que 1. La división entre una potencia de dos se interpretará como una división de enteros, dando el mismo resultado que un desplazamiento de los bits en dirección de los bits menos significativos. Cualquier residuo de la división se ignora.

Para generar la clave compartida del bit de longitud de clave, los dispositivos de red primero aplican un paso de

división adicional. El primer dispositivo de red evalúa el material generador de claves para determinar el número de identidad del segundo dispositivo módulo el módulo público para cada conjunto de parámetros y adiciona los resultados, después divide entre 2^s y reduce módulo dos a la potencia de la longitud de clave. Nótese que esto es equivalente a aplicar primero un módulo 2^(s+longitud de clave) después del módulo público, y después dividiendo entre 2^s. En este caso "dividir" incluye redondear hacia abajo.

En una modalidad, el módulo privado se genera usando un generador de números aleatorios. En una modalidad, se generan los múltiples módulos privados de tal manera que son primos relativamente en pares. Por ejemplo, los múltiples módulos privados pueden generarse iterativamente verificando para cada nuevo módulo privado que aún son primos relativamente en pares, y si no se descarta el último módulo privado generado. Una modalidad comprende generar iterativamente un módulo candidato, usando el generador de números aleatorios, de tal forma que los (b) bits consecutivos de longitud de clave de la representación binaria del módulo público menos el modulo candidato son todos bits cero, por ejemplo, los bits de longitud de clave menos significativos, hasta que el módulo candidato satisface un test de primalidad utilizando un dispositivo de test de primalidad, en donde el módulo candidato así obtenido que satisface el test de primalidad se

usa como el módulo privado. El test de primalidad puede ser, por ejemplo, el test de primalidad de Miller-Rabin o el test de primalidad de Solovay-Strassen.

Un polinomio bivariable simétrico en variables de x y y de grado a, tiene solo monomios de la forma x^iy^j, con $i \leq a, j \leq a$. Adicionalmente el coeficiente que corresponde a x^iy^j es el mismo que el coeficiente de x^jy^i. Esto puede usarse para reducir el número de coeficientes almacenados en aproximadamente la mitad. Nótese que se utiliza el grado de definición relajada del grado. Definimos el grado de un monomio como el grado máximo de las variables en el monomio. Por lo que el grado de x^jy^i es máx(i,j), es decir, que $i \leq a, j \leq a$. Por lo que por ejemplo llamamos polinomio de grado 1 al que tiene la forma general a + bx +cy + dxy, (nótese que dado que solo se consideran polinomios simétricos, tenemos que b=c). Nótese que si se desea podemos poner restricciones adicionales en el polinomio bivariable, incluyendo, por ejemplo, que solo se utilicen monomios con $i + j \leq a$, pero esto no es necesario.

En una modalidad el polinomio bivariable simétrico es generado por la autoridad de red. Por ejemplo, el polinomio bivariable simétrico puede ser un polinomio bivariable simétrico aleatorio. Por ejemplo, los coeficientes pueden seleccionarse como números aleatorios utilizando un generador de números aleatorios.

Aunque la ofuscación utilizada aumenta bastante la flexibilidad contra un ataque, en particular contra ataques de colusión en donde se combinan múltiples materiales de claves locales, tiene una desventaja potencial. Algunas veces la clave compartida derivada por el primer dispositivo de red no está en todos los bits idénticos a la clave compartida derivada por el segundo dispositivo de red. Esto se debe principalmente al desajuste en los bits de transporte después de la adición de los coeficientes de ofuscación. Otra razón es la falta de efecto de los efectos modulares de cada uno de los módulos privados durante la generación de la clave que afecta los bits de transporte generados. Aunque es una molestia, esta desventaja puede solucionarse de varias maneras. Al elegir la ofuscación con más cuidado puede reducirse significativamente la probabilidad de una diferencia y en particular la probabilidad de una gran diferencia. Adicionalmente, se encontró que las diferencias, si las hubiere, probablemente se localicen en los bits menos significativos de las claves generadas. Por lo que removiendo uno o más bits menos significativos puede aumentar la probabilidad de una clave compartida. Por ejemplo, en una modalidad del método de determinar una clave compartida comprende determinar si el primer dispositivo de red y el segundo dispositivo de red han derivado la misma clave compartida, y si no derivan una clave compartida adicional

del resultado de la reducción módulo el módulo de clave. Pueden derivarse claves compartidas adicionales hasta que se encuentra una que es igual en ambos lados. Si menos que un número de umbral de bits permanecen en la clave compartida, puede terminarse el método. Para algunas aplicaciones puede aceptarse simplemente que cierto porcentaje de los dispositivos de red no son capaces de comunicarse. Por ejemplo, en redes inalámbricas ad-hoc en donde un mensaje puede dirigirse a lo largo de varias rutas, no hay pérdida de conectividad si algunos de los dispositivos de red no son capaces de comunicarse.

En una modalidad, un número de los bits menos significativos de la clave compartida son removidos; por ejemplo, el número de bits removidos puede ser 1, 2 o más, 4 o más, 8 o más, 16 o más, 32 o más, 64 o más. Al remover más de los bits menos significativos, se reduce la probabilidad de tener claves que no son iguales; en particular puede reducirse a cualquier umbral deseado. La probabilidad de claves compartidas que son iguales puede calcularse, siguiendo las relaciones matemáticas, también puede determinarse experimentalmente.

También puede controlarse la probabilidad de números de ofuscación en una modalidad, el intervalo en el cual se elige un número de ofuscación se reduce para coeficientes que corresponden a monomios de grado mayor. En particular, se

requiere que $|\epsilon_{Ai}| < 2^{(a+1-1)b}$, en donde $\epsilon_{A,i}$ denota el número ofuscado para el iésimo monomio, i denota el grado del monomio que corresponde al coeficiente, a representa el grado del polinomio bivariable y b representa la longitud de la clave. A representa el dispositivo de red para el cual se genera el material de clave local. En una modalidad, un número ofuscado se genera para cada coeficiente, por ejemplo la fórmula anterior. Puede aplicarse una ofuscación diferente para diferentes dispositivos de red. Por ejemplo, incluso si hay 3 o más dispositivos de red, entonces para cada dispositivo de red pueden generarse diferentes números de ofuscación.

Nótese que el número de ofuscación puede estar restringido a número positivos pero no esto no es necesario, los números de ofuscación pueden ser negativos. En una modalidad, los números ofuscados se generan usando un generador de números aleatorios. Pueden generarse múltiples números de ofuscación y coeficientes agregados de polinomio monovariable para obtener el polinomio monovariable ofuscado. Uno o más, preferentemente todos los, coeficientes del polinomio monovariable pueden ofuscarse de esta manera.

El número de bits en el número de identidad para el dispositivo de red usualmente se elige como menor o igual que la longitud de la clave. El número de identidad puede ser una cadena de bits, por ejemplo una cadena de bits de 32 ó 64, o

más larga. La longitud de la clave puede ser de ~~32 o más, 48~~ o más, 64 o más, 96 o más, 128 o más, 256 o más. La longitud de la clave puede elegirse con ciertos números de bits más grandes con el objeto de reducir un número correspondiente de bits menos significativos de la clave compartida determinada. Por otro lado, en una modalidad, la longitud del número de identidad es más largo que la longitud de la clave. En este caso, el efecto de operaciones modulares puede dar lugar a un efecto mayor en los bits menos significativos de los bits de longitud de clave de la clave generada por lo que esos bits podrían no ser iguales para un par de dispositivos dispuestos a generar una clave común. Al tener una longitud más larga para el identificador puede tener, sin embargo, un efecto positivo en la seguridad dado que más bits se mezclan entre sí cuando se hacen los cálculos correspondientes.

Puede implementarse un dispositivo de manipulación polinomial en software que se ejecuta en una computadora, por ejemplo en un circuito integrado. Un dispositivo de manipulación polinomial puede implementarse muy eficientemente en hardware. También es posible una combinación. Por ejemplo, un dispositivo de manipulación polinomial puede implementarse manipulando matrices de coeficientes que representan los polinomios.

El almacenamiento electrónico del material de clave local generado en el dispositivo de red puede implementarse

enviando electrónicamente el material de clave local generado al dispositivo de red, por ejemplo, usando una conexión física, o usando una conexión inalámbrica y teniendo el material de clave local almacenado en el dispositivo de red. Esto puede hacerse durante la fabricación o instalación, por ejemplo, durante la prueba, de un circuito integrado en el dispositivo de red. El equipo de prueba puede comprender o conectarse a la autoridad de red. Esto también puede suceder después de una unión exitosa de un dispositivo con una red de operación (es decir, después del acceso a la red o cargado). En particular, el material de clave local puede distribuirse como parte de parámetros de red operacionales.

La obtención del material de clave local para el primer dispositivo de red en forma electrónica puede hacerse recibiendo electrónicamente el material de clave local desde un sistema para configurar un dispositivo de red para compartir claves, por ejemplo, un dispositivo de autoridad de red. La obtención de material de clave local también puede hacerse recuperando el material de clave local de un almacenamiento local, por ejemplo, una memoria tal como una memoria flash.

La obtención de un número de identidad para un segundo dispositivo de red, puede hacerse recibiendo el número de identidad del segundo dispositivo de red, por ejemplo, directamente del segundo dispositivo de red, por ejemplo

recibiendo de forma inalámbrica el segundo dispositivo de red.

El módulo público y módulo de clave pueden almacenarse en un dispositivo de red. También pueden recibirse de una autoridad de red. También pueden estar implícitos en el software del dispositivo de red. Por ejemplo, en una modalidad el módulo de clave es una potencia de dos. La reducción módulo de el módulo de clave puede hacerse descartando todos los bits excepto los bits menos significativos de la longitud de clave. Primero el resultado de la sustitución se reduce módulo el módulo público que entonces se reduce adicionalmente módulo el módulo clave.

Aunque no se requiere, el módulo público y el módulo de clave pueden ser relativamente primos. Esto puede lograrse teniendo el módulo público impar y el módulo de clave de una potencia de 2. En cualquier caso, se evita que el módulo de clave divida el módulo público, porque entonces podría omitirse reducción módulo del módulo público.

El método para la concordancia de claves entre dos dispositivos puede usar como material generador de clave raíz un número de polinomios bivariables. Puede usarse el método para la concordancia de claves para la concordancia de x entre x partes usando x polinomios bivariables como material generador de clave raíz. En esta extensión, la tercera parte confiable evalúa los polinomios de variable x en una variable

en el anillo correspondiente, los polinomios de variable x-1 resultantes se agregan entonces en los enteros que generan el material de clave local almacenado en un dispositivo. Cuando x dispositivos necesitan concordar en una clave, un dispositivo evalúa su material de clave local en identificadores de los otros x-1 dispositivos.

El uso de polinomios bivariables asimétricos como material generador de claves raíz, es decir, f(x,y) != f(y,x), permite acomodar la creación de dos grupos de dispositivos tales como dispositivos en el primer grupo que reciben KM(Id,y) y dispositivos en el segundo grupo que reciben KM(x,iD) siendo KM el material de clave local almacenado en un dispositivo. Dos dispositivos que pertenecen al mismo grupo no pueden generar una clave común, pero dos dispositivos en diferentes grupos pueden. Ver además Blundo.

El número de identidad de un dispositivo de red puede calcularse como la función unidireccional de una cadena de bits que contiene información asociada con el dispositivo. La función unidireccional puede ser una función de dispersión cifrada tal como SHA2 o SH3. La salida de la función unidireccional puede truncarse de tal manera que se ajuste al tamaño del identificador. Alternativamente el tamaño de la función unidireccional es más pequeño que el tamaño del identificador máximo.

En una modalidad, los polinomios simétricos involucran

un solo monomio de la forma $<ax^iy^i>p_j$ en donde $<>_p$ representa la operación modular. En este caso, los elementos están dentro de un grupo finito y la operación es la multiplicación. El módulo público puede ser más grande que el módulo privado o más pequeño; si hay múltiples módulos privados, algunos pueden ser más grandes que el módulo privado y algunos pueden ser más pequeños.

El material de clave raíz puede evaluarse en cualquier anillo. Es posible utilizar polinomios de un monomio simple tal como Ax^a, en cuyo caso puede usarse un grupos.

Un aspecto de la invención se relaciona con un sistema para configurar un dispositivo de red para compartir claves, por ejemplo una autoridad de red, el sistema comprende un obtenedor para obtener en forma electrónica por lo menos dos conjuntos de parámetros, un conjunto de parámetros comprende un módulo privado, un módulo público y un polinomio bivariable que tiene coeficientes enteros, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en por lo menos bits consecutivos de longitud de clave, un generador para generar material de clave local para el dispositivo de red que comprende un administrador de dispositivos de red para obtener en forma electrónica un número de identidad para el dispositivo de red, y para almacenar en forma electrónica el material de clave local generado, el generador está

configurado para, para cada conjunto de parámetros de los por lo menos dos conjunto de parámetros obtener un polinomio monovariable correspondiente, por medio de: determinar utilizando un dispositivo de manipulación polinomial un polinomio monovariable a partir del polinomio bivariable del conjunto de parámetros sustituyendo el número de identidad en el polinomio bivariable y reduciendo el resultado de la sustitución módulo el módulo privado del conjunto de parámetros, y almacenar electrónicamente en el dispositivo de red el material de clave local generado, el material de clave local generado comprende el módulo público de cada conjunto de parámetros y el polinomio monovariable correspondiente de cada conjunto de parámetros.

Una modalidad del sistema comprende un generador de números de ofuscación, por ejemplo, un generador de números aleatorios, para generar un número de ofuscación, el dispositivo de manipulación polinomial está configurado para agregar el número de ofuscación a un coeficiente del polinomio monovariable para obtener un polinomio monovariable, el material de clave local generado comprende el polinomio monovariable ofuscado. El número de ofuscación puede representarse como el coeficiente de un polinomio de ofuscación. En una modalidad, cada coeficiente de la suma de los polinomios de ofuscación es un múltiplo de 2 a la potencia de la longitud de clave. En una modalidad, cada

coeficiente de la suma de los polinomios de ofuscación dividido entre una potencia de dos es un múltiplo de 2 a la potencia de la longitud de clave. La división entre una potencia de dos puede calcularse por redondeo hacia abajo.

Un aspecto de la invención se relaciona con un primer dispositivo de red configurado para determinar una clave compartida, siendo la clave una clave cifrada, el primer dispositivo de red comprende: un obtenedor de material de clave local obtener material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende por lo menos dos polinomios monovariables opcionalmente ofuscados y los módulos públicos correspondientes, un receptor para obtener un número de identidad para un segundo dispositivo de red, el segundo dispositivo de red es diferente del primer dispositivo de red, un dispositivo de manipulación polinomial para, para cada uno de los por lo menos dos polinomios monovariables opcionalmente ofuscados: sustituir el número de identidad del segundo dispositivo de red en el polinomio monovariable, y reducir el resultado de la sustitución módulo el módulo público que corresponde al polinomio monovariable, y sumar entre sí los resultados de las reducciones módulo un módulo público y reducir módulo un módulo de clave, y un dispositivo de derivación de claves para derivar la clave compartida del resultado de la reducción módulo el módulo de clave.

Un dispositivo de derivación de claves puede implementarse como una computadora, por ejemplo un circuito integrado, software en ejecución, en una combinación de los dos. y similares, configurado para derivar la clave compartida del resultado de la reducción módulo el módulo de clave.

Derivar la clave compartida del resultado de la reducción módulo el módulo de clave, puede incluir la aplicación de una función de derivación de clave, por ejemplo la función KDF, definida en la especificación OMA_DRM de la Alianza Móvil Abierta (OMA-TS-DRM-DRM-V2_0_2-20080723-A, sección 7.1.2 KDF) y funciones similares. Derivar la clave compartida puede incluir descartar uno o más bits menos significativos (antes de aplicar la función de derivación de clave). Derivar la clave compartida puede incluir sumar, sustraer, o concatenar un entero (antes de aplicar la función de derivación de clave).

Cada uno de múltiples dispositivos de red que tiene un número de identidad y material de clave local correspondiente pueden formar conjuntamente una red de comunicación configurada para asegurar la comunicación, por ejemplo confidencial y/o autenticada entre pares de dispositivos de red.

La generación de claves se basa en ID y permite la generación de claves por pares entre pares de dispositivos.

Un dispositivo A puede depender de un algoritmo que deriva una clave del material de clave local y un número de identidad.

En una modalidad, un primer dispositivo envía un mensaje de confirmación de clave al segundo dispositivo de red. Por ejemplo, un mensaje de confirmación puede comprender el cifrado de un mensaje, y opcionalmente el mensaje. El segundo dispositivo de red puede verificar el cifrado del mensaje. El mensaje puede ser fijo y estar presente en el segundo dispositivo, para evitar la necesidad de enviarlo. El mensaje puede ser aleatorio, o momentáneo, etc., en cuyo caso puede enviarse junto con el cifrado. El segundo dispositivo puede replicar con un mensaje que contiene una indicación si las claves concuerdan. El segundo dispositivo puede replicar también con un mensaje de confirmación de clave por cuenta propia. Si el primer y/o segundo dispositivo encuentra que las claves no son iguales pueden iniciar un proceso de igualación, por ejemplo borrando bits menos significativos, etc.

Los dispositivos de red y el sistema pueden ser dispositivos electrónicos. Los dispositivos de red pueden ser dispositivos de red móviles.

Un método de conformidad con la invención puede implementarse en una computadora como un método implementado en computadora, o en hardware dedicado, o en una combinación

de ambos. El código ejecutable para un método de conformidad con la invención puede almacenarse en un producto de programa de cómputo. Ejemplos de productos de programa de cómputo incluyen dispositivos de memoria, dispositivos de almacenamiento óptico, circuitos integrados, servidores, software en línea, etc. Preferentemente, el producto de programa de cómputo comprende medios de códigos de programa no transitorios almacenados en un medio de lectura por computadora para realizar un método de conformidad con la invención cuando el producto de programa de cómputo es ejecutado en una computadora.

En una modalidad preferida, el programa de cómputo comprende medios de códigos de programas de cómputo adaptados para realizar todos los pasos de un método de conformidad con la invención cuando el programa de cómputo es ejecutado en una computadora. Preferentemente, el programa de cómputo está incorporado en un medio de lectura por computadora.

Breve Descripción de las Figuras

Estos y otros aspectos de la invención serán evidentes y se entenderán al hacer referencia a las modalidades descritas de aquí en adelante. En las figuras,

las figuras 1a y 1b son un diagrama de bloques esquemático que ilustra un generador de material de clave raíz,

las figuras 2a y 2b son un diagrama de bloques

esquemático que ilustra un generador de material de clave local,

la figura 3 es un diagrama de bloques esquemático que ilustra una red de comunicación, la figura 4 es un diagrama de flujo esquemático que ilustra la generación de material de clave local, la figura 5 es un diagrama de flujo esquemático que ilustra la generación de una clave compartida,

la figura 6 es un diagrama de secuencia esquemático que ilustra la generación de una clave compartida. Debe apreciarse que los elementos que tienen los mismos números de referencia en diferentes figuras, tienen las mismas características estructurales y las mismas funciones, o son las mismas señales. Cuando la función y/o la estructura de el elemento ha sido explicada, no hay necesidad de una explicación repetida de la misma en la descripción detallada.

Descripción Detallada de la Invención

Aunque la presente invención es susceptible de modalidades de muchas formas diferentes, se muestran en las figuras y se describirán detalladamente en la presente una o más modalidades específicas, en el entendimiento de que la presente descripción se considerará como ejemplo de los principios de la invención y no pretende limitar la invención a las modalidades específicas mostradas y descritas.

Abajo se describe una modalidad del método para compartir claves. El método tiene una fase de configuración y

una fase de uso. La fase de configuración puede incluir pasos de iniciación y pasos de registro. Los pasos de iniciación no involucran los dispositivos de red.

Los pasos de iniciación seleccionan parámetros del sistema. Los pasos de iniciación pueden realizarlos la tercera parte confiable (TTP). Sin embargo, los parámetros del sistema pueden también considerarse que se proporcionan como entradas. En ese caso la tercera parte confiable no los genera, y pueden saltarse los pasos de iniciación. Por ejemplo, la tercera parte confiable puede recibir los parámetros del sistema de un fabricante de dispositivos. El fabricante de dispositivos puede haber realizado los pasos de iniciación para obtener los parámetros del sistema. Por conveniencia de exposición nos referiremos a la tercera parte confiable como realizando los pasos de iniciación, teniendo en mente que esto no es necesario.

En los pasos de iniciación se establece un número de conjuntos de parámetros. Dado el número de identificación de un dispositivo de red, los conjuntos de parámetros se usan para generar material de clave local; de cada conjunto de parámetros se obtienen polinomios monovariables y un módulo público correspondiente. Al dispositivo de red se le proporciona un material de clave local pero no obtiene el acceso a los conjuntos de parámetros. Dado que los conjuntos de parámetros permiten que se genere nuevo material de clave

local, solo son conocidos por la tercerea parte confiable, y son mantenidos en secreto de los dispositivos de red generales.

Un dispositivo de red A puede generar una clave compartida a partir de su material de clave local y el número de identificación de un dispositivo diferente B. Para hacer esto el dispositivo de red A realiza un cálculo usando su material de clave local.

Pasos de iniciación

En los pasos de iniciación se selecciona el material de clave raíz. Unos pocos parámetros son parámetros globales.

La longitud de clave deseada para la clave será compartida entre los dispositivos en la fase de uso seleccionada; esta longitud de clave se denomina 'b'. Un valor típico para una aplicación de seguridad baja puede ser 64 u 80. Un valor típico para una seguridad a nivel consumidor puede ser 128. Las aplicaciones altamente secretas pueden preferir 256 o incluso valores mayores. No necesita haber una relación directa entre la fuerza de seguridad del algoritmo y b; la seguridad proporcionada será cuando mucho b. Dependiendo de algoritmos futuros para atacar el sistema, la seguridad del algoritmo podría ser menor que b.

Se selecciona el número de conjuntos de parámetros que se generarán; el número de conjuntos de parámetros se denomina 't'. Un valor de t elevado implica que el ataque del

sistema resultante, por ejemplo usando técnicas basadas en retícula, es difícil. Por otro lado un valor elevado de t también implica más cálculos y requisitos de almacenamiento en los dispositivos de red. Para aplicaciones de muy baja seguridad es posible un valor de t = 1, sin embargo puede implicar que dado un número suficiente de claves comprometidas pueda recuperarse el material de clave subyacente. Se recomienda tomar por lo menos un valor de t = 2; este valor ya ocasiona un aumento significativo en la complejidad del criptoanálisis requerido, por ejemplo, ataques basados en retícula. Sin embargo, para aplicaciones de alta seguridad puede usarse un valor de 3, 4 o incluso mayor.

Enseguida se selecciona un número de t conjuntos de parámetros. Cada conjunto de parámetros j, con j = 1,...,t comprende un grado deseado a, un módulo público N, por lo menos un módulo privado p_1, y por lo menos un polinomio bivariable simétrico f_1. Cuando convenga, el módulo público se indicará con un subíndice para indicar el conjunto de parámetros al que pertenece: N_j.

Abajo se discuten maneras ventajosas de seleccionar estos parámetros.

Especialmente, los polinomios bivariables de cada conjunto de parámetros son sensibles a la seguridad y no serán revelados a los dispositivos de red normales; tampoco

hay razón de revelar los módulos privados, por lo que se recomienda mantenerlos en secreto, el conocimiento de los mismos puede incluso facilitar un ataque en el sistema. La longitud de clave b los módulos públicos Nj son necesarios en el dispositivo de red y no pueden mantenerse en secreto a la parte confiable.

Cada conjunto de parámetros contribuye a la dificultad del problema difícil subyacente. Como se explicará abajo algunas elecciones de parámetros ocasionarán un problema más fuerte que otras elecciones. En principio la selección de conjuntos de parámetros es independiente, por ejemplo, puede elegirse seleccionar un conjunto de parámetros con valores que corresponden a mayor seguridad y seleccionar un segundo conjunto con parámetros más pequeños. En este caso el segundo conjunto y/o conjuntos adicionales contribuyen principalmente a evitar ataques en el conjunto difícil. Para este escenario puede ser un tanto más fácil derivar límites en la seguridad. Por otro lado, también pueden seleccionarse todos los conjuntos de parámetros de dificultad comparable. En ésta última situación, la dificultad del problema proviene de todos los conjuntos. Esto optimiza recursos de cálculo en el dispositivo de red.

Pasos de selección de conjuntos de parámetros

Estos pasos se repetirán t veces; una vez por cada conjunto de parámetros deseado. Se selecciona el grado

deseado; el grado controla el grado de ciertos polinomios. El grado se denominará 'a', es por lo menos 1. Una elección práctica para a es 2. Una aplicación más segura puede utilizar un valor más alto de a, por ejemplo, 3 ó 4, o incluso mayor. Para una aplicación simple también es posible a = 1. El caso a = 1 se relaciona con el denominado "problema de números ocultos"; los valores de "a" más altos se relacionan con el problema de interpolación polinomial ruidosa que confirma que estos casos son difíciles de quebrantar.

Se selecciona el número de polinomios. El número de polinomios puede denominarse 'm'. Una elección práctica para m es 2. Una aplicación más segura puede utilizar un valor más alto de m, por ejemplo, 3 ó 4, o incluso mayor. Nótese que una aplicación de baja complejidad puede imponer un valor bajo de m, dado que un valor alto m implica mayor complejidad de implementación en la TTP.

Valores más altos de los parámetros de seguridad a y m aumentan la complejidad del sistema y consecuentemente aumentan su complejidad indescifrable. Los sistemas más complicados son más difíciles de analizar y por lo tanto más resistentes al criptoanálisis. Los grados a pueden ser convenientemente iguales para todos los conjuntos de parámetros, también m puede ser el mismo para todos los conjuntos de parámetros; nótese que esto no es necesario.

En una modalidad, un módulo público N se selecciona satisfaciendo $2^{(a+)b-1} \leq N$ y más preferentemente también $N \leq 2^{(a+2)b} - 1$. Los límites no son estrictamente necesarios; el sistema podría utilizar también un valor de N menor/mayor, aunque esto no se considera la mejor opción.

Con frecuencia la longitud de clave, el grado y número de polinomios estará predeterminado, por ejemplo por un diseñador de sistema, y se proporcionarán a la parte confiable como entradas Como una elección práctica puede considerarse $N = 2^{(a+2)b} - 1$. Por ejemplo si a = 1, b = 64 entonces N puede ser $N = 2^{192} - 1$. Por ejemplo si a = 1, b = 128 entonces N puede ser $N = 2^{512} - 1$. En la elección de N el límite superior o inferior del intervalo anterior tiene la ventaja de un cálculo fácil. Para aumentar la complejidad para un atacante, puede elegirse un número aleatorio en el intervalo de N.

Un número de m módulos privados $p_1, p_2, \ldots, p_m$, son seleccionados por la tercera parte confiable (TTP). Los módulos son enteros positivos. Durante los pasos de registro cada dispositivo se asociará con un número de identidad. Cada módulo privado seleccionado es mayor que el número de identidad más grande utilizado. Por ejemplo, pueden unirse números de identidad con el requisito de que sean menores o iguales a $2^b - 1$, y que los módulos privados seleccionados sean mayores que $2^b - 1$. Cada número seleccionado satisface

la siguiente relación $p_j = N + \gamma_j \cdot 2^b$. En donde γ_j son enteros tales que $|\gamma_j| < 2^b$. Una manera práctica de seleccionar números que satisfagan este requisito es seleccionar un conjunto de m números aleatorios γ_j tal que $-2^b + 1 \leq \gamma_j \leq 2^b - 1$ y calcular los módulos privados seleccionados a partir de la relación $p_j = N + \gamma_j \cdot 2^b$. Con $|\gamma_j|$ puede permitirse un bit mayor, sin embargo, puede ocurrir un problema porque la operación modular va muy lejos que las claves compartidas podrían no ser iguales.

Para $m > 1$, el sistema es más complicado, y por lo tanto más seguro, dado que la operación módulo para diferentes módulos se combinan a pesar de que tales operaciones no son compatibles en el sentido matemático usual. Por esta razón es ventajoso elegir los módulos privados seleccionados por pares distintos.

Se genera un número de m polinomios bivariables simétricos $f_1, f_2, \ldots, f_m$ de grados a_j. Todos los grados satisfacen $a_j \leq a$, más preferentemente $a = MAX\{a_1, \ldots, a_m\}$. Una elección práctica es considerar cada polinomio de grado a. Un polinomio bivariable es un polinomio de dos variables. Un polinomio simétrico f satisface $f\{x,y) = f(y,x)$. Cada polinomio f_j se evalúa en el anillo finito formado por los enteros módulo p_j, obtenidos por cálculo de módulo p_j. Los enteros módulo p_j forman un anillo finito con los elementos p_j. En una modalidad el polinomio f_j se representa con

coeficientes de 0 hasta p_j - 1. Los polinomios bivariable pueden seleccionarse aleatoriamente, por ejemplo, seleccionando coeficientes aleatorios en estos límites.

La seguridad de compartir claves depende de estos polinomios bivariables porque son el material generador de claves raíz del sistema; por lo que preferentemente se toman fuertes medidas para protegerlos, por ejemplo procedimientos de control, dispositivos resistentes a la alteración y similares. Preferentemente los enteros seleccionados $p_1, p_2, \ldots, p_m$ también se mantienen en secreto, incluyendo el valor Y_j que corresponde a p_j, aunque esto es menos crítico. También nos referiremos a los polinomios bivariable en la siguiente forma: para $j=1,2,\ldots,m$, escribimos $f_j(x,y) = \sum^{a}_{i=0} f_{i,j}(x)y^i$.

La modalidad anterior puede variarse de varias maneras. Las restricciones en los módulos público y privado pueden elegirse en una variedad de formas, de tal manera que es posible la ofuscación del polinomio monovariable, sin embargo las claves compartidas obtenidas en dispositivos de red permanecen suficientemente cercanas entre sí con suficiente frecuencia. Como se explicó, lo que es suficiente dependerá de la aplicación, el nivel de seguridad requerido y los recursos de cálculo disponibles en los dispositivos de red. La modalidad anterior combina enteros positivos de tal manera que las operaciones modulares que se llevan a cabo cuando se generan los polinomios compartidos se combinan de manera no

lineal cuando se agregan en los enteros creando una estructura no lineal para el material de clave local almacenado en un dispositivo de red. La elección anterior para N y p_j tiene la propiedad de que: (i) el tamaño de N es fijo para todos los dispositivos de red y está vinculado a a; (ii) el efecto no lineal aparece en los bits más significativos de los coeficientes que forman el material de clave almacenado en el dispositivo. Debido a esa forma específica la clave compartida puede generarse reduciendo módulo 2^b después de la reducción módulo N.

Estos conceptos de diseño pueden aplicarse de manera más general para mejorar en los aspectos (i) y (ii) como se mencionó en el último párrafo. Abajo se proporcionan diferentes construcciones generales para elegir los módulos público y privado. Para tratar el primer punto (i), esta estructura para N y p_j se ajusta a una expresión más general en donde escribimos $p_j = 2^X + \gamma_j 2^{Yj} - 1$ tal que para cada j, $Y_j + b\alpha_j = X$ y $|\gamma_j| < 2^b$. Esta expresión permite una forma p_j más variable a la vez que asegura un efecto máximo cuando se introducen efectos no lineales. Nótese que también puede hacerse que $Y_j + b\alpha_j \approx X$ en donde la diferencia entre el lado izquierdo y derecho es una fracción de la longitud de clave.

Para abordar el segundo punto, la forma anterior para N y p_j se ajusta a una expresión aún más general en la cual $p^j = \beta 2^X + \gamma_j 2^{Yj} + \zeta_j 2^{Zj}$. Estableciendo, por ejemplo $\zeta_j = -1, \beta = 1$, y

$Z_j = 0 \ \forall \ j$ obtenemos la expresión anterior en la cual los diferentes valores γ_j introducen un efecto no lineal en los bits más significativos de los coeficientes del material de clave almacenado en un dispositivo de red. En este caso, el módulo público constante (N) es $N = 2^X - 1$, mientras que la parte de variable privada utilizada en la generación de diferentes enteros positivos involucrados en operaciones modulares es $\gamma_j 2^{Yj}$. Alternativamente, podemos establecer $\gamma_j = 1, \beta = 1, Z_j = 0$, $Y_j = (\alpha_j + 1)b$, $X = (\alpha_j + 2)b \ \forall \ j$ mientras que ζ_j son diferentes para diferentes j tal que $|\zeta_j| < 2^b$. En este caso, las diferencias ζj permiten introducir un efecto no lineal en los bits menos significativos de los coeficientes del material local almacenado en un nodo. La construcción de la parte pública en este caso es también diferente e igual a $N = \beta_j 2^{Xj} + \gamma_j 2^{Yj} = 2^X + 2^{b(\alpha j+1)}$ es decir, las partes que permanecen constante. Nótese que en este caso el efecto no lineal está en la parte más baja, y debido a la condición para un máximo efecto de mezclado mencionado anteriormente, entonces la diferente entre $Y_j - Z_j - \log_2 (\zeta_j)$ debe ser $\alpha_j b$. De manera similar, pueden definirse otras construcciones siguiendo el mismo concepto.

Como se muestra arriba son posibles muchas elecciones para los parámetros. Sin embargo, algunas elecciones darán mejores implementaciones. Especialmente la elección del módulo público es importante. Por ejemplo, algunas elecciones

para el módulo público permiten operaciones módulo eficientes. También el efecto del módulo público en los bits de los cuales tomamos la clave, por ejemplo LSB, es preferentemente diferente. Puede probarse un efecto diferente realizando las operaciones para generar la clave compartida y probar si las diferencias en p_i dan lugar a una manera diferente de generar la clave. Esto puede observarse, en el siguiente ejemplo.

Por ejemplo, es ventajoso seleccionar módulos públicos que tienen diferencias pequeñas en el número de bits menos significativos, por ejemplo menores que una diferencia predeterminada. Por ejemplo, una modalidad puede utilizar números tales que $t = 2$, y $N_1 = 2^{(\alpha+2)b} - 1$ y $N_2 = 2^{(\alpha+2)b} - 2 - 1$. En este caso específico, el término -2 juega un papel importante durante la fase de generación de claves dado que las reducciones módulo N_1 no incluirán ese efecto, pero las reducciones módulo N_2 lo incluirán. Nótese que la reducción en este caso se relaciona con mover bits de exceso que son mayores que $(\alpha + 2)b$ bits a la parte más baja.

Sin embargo, un problema con la elección de los módulos públicos en esa forma es que solo están disponibles un número limitado de opciones mucho más pequeño que 2^b. En general, deseamos introducir un término 2^h en N de tal manera que $h < v$ y $h > 1$. También el problema es que el número de bits que son realmente afectados por la forma diferente de N será

aproximadamente b - h y habrá solo aproximadamente 2^h números diferentes. Para superar estos problemas, por ejemplo teniendo más opciones para N y maximizando el número de bits que pueden usarse para la clave afectada mediante diferentes operaciones, podría usarse una definición más general del pi en la forma mencionada dos párrafos arriba. En ese caso se introduce un efecto no lineal tanto en MSB como LSB de los coeficientes polinomiales, por ejemplo, usando $p_i = N - Y_j 2^{b(a+1)} - \zeta_i$ con el módulo público correspondiente $N = 2^{(a+2)b} - 2^{ba}$. Como se definió aquí Y_i y ζ_i se eligen diferentes para todo p_i, preferentemente también diferentes a través de todos los conjuntos de parámetros. La clave en este caso se genera desde los bits intermedios, y no de LSB.

Una elección similar es la siguiente. En estas ecuaciones el primer índice i indexa los conjuntos de parámetros y va hasta t; el segundo índice j indexa el número de números p utilizados por cada conjunto de parámetros y va hasta m.

$$N_i = 2^{(a+2)b} - 2^{ba} - \zeta_i$$

$$p_{i,j} = N_i - \gamma_{i,j} 2^{b(a+1)}$$

Una elección práctica es considerar t = 2. Entonces puede elegirse cada conjunto de parámetros. Una elección práctica es considerar m = 2 para cada conjunto de parámetros. Especialmente en las ecuaciones inmediatamente anteriores, estas son buenas elecciones. Con esta

construcción podemos hallar muchos N_i variando los valores de ζ de b bits, por ejemplo al azar. En esta construcción los parámetros realizan el mezclado en la generación del material generador de claves compartido almacenado en los dispositivos. Esto puede hacerlo la parte confiable. Los parámetros ζ realizan el mezclado de las claves en el dispositivo. Más preferentemente, también se agrega ruido en este caso, siguiendo la misma motivación como en la modalidad. En este caso, la condición para el ruido necesita actualizarse de tal manera que la suma del ruido, es decir, polinomios de ofuscación, es igual a cero en la posición de la cual se extrae la clave (es decir, de los bits intermedios).

Se prefiere que los módulos públicos, por ejemplo N_1 y N_2, no sean todos múltiplos de 2^b. Esto es así porque para enteros positivos a, m, n y para un entero q adecuado, tenemos que $a = qmn + \langle a \rangle_{mn}$, y así $a \equiv \langle a \rangle_{mn} \bmod n$ de lo que inferimos que $\langle a \rangle_n = \langle \langle a \rangle_{mn} \rangle_n$. Consecuentemente, si N_1 y N_2 son ambos múltiplos de 2^b, entonces

$$\left\langle \left\langle F_\eta^1(\eta') \right\rangle_{N_1} + \left\langle F_\eta^2(\eta') \right\rangle_{N_2} \right\rangle_{2^b} = \left\langle F_\eta^1(\eta') + F_\eta^2(\eta') \right\rangle_{2^b}.$$

Es decir, el problema se reduce al caso t = 1.

Pasos de registro

En el paso de registro a cada dispositivo de red se le asigna material generador de claves (KM). Un dispositivo de red está asociado con un número de identidad. El número de

identidad puede asignarse a demanda, por ejemplo, la TTP, o puede ya estar almacenado en el dispositivo, por ejemplo, almacenado en el dispositivo durante la fabricación, etc.

La TTP genera un conjunto de material generador de claves KMA para un dispositivo con número de identidad A calculando t polinomios de la siguiente manera:

$$F_i^A(X) = \sum_j^m <f_j(x, A)>_{pj} + \sum_k^a \in_{i,k}^A X^k = C_{i,k}^A X^k$$

En la ecuación inmediatamente anterior, el índice i indexa los conjuntos de parámetros, es decir, va de 1 a t. El índice j indexa el número de polinomios y módulos privados por cada conjunto de parámetros. El índice k indexa los coeficientes en el polinomio de ofuscación. Nótese que se selecciona un polinomio de ofuscación por cada conjunto de parámetros. Algunos o todos los conjuntos de parámetros pueden no tener un polinomio de ofuscación. También los módulos públicos del conjunto de parámetros que corresponden a los polinomios monovariables están incluidos en el material de clave local.

X es una variable formal. Nótese que el material generador de claves en no lineal. La notación $< \cdots >_{pj}$ denota reducción módulo pj de cada coeficiente del polinomio entre los corchetes. La notación '$\in_{A,i}$' denota un entero aleatorio, el cual es un ejemplo de un número de ofuscación, tal que $|\in_{A_{i,k}}| < 2^{(a+2-k)b-2}$. Nótese que cualquiera de los enteros aleatorios puede ser positivo o negativo. Los números

aleatorios ϵ se generan de nuevo para cada dispositivo. El término $\sum^{a}_{k=0} \epsilon^{A}_{i,k}X^{k}$ representa por lo tanto para cada i un polinomio en X de grado a, cuya longitud de coeficiente es más corta al aumentar el grado. Alternativamente, una condición más general, pero más complicada es que $\sum^{a}_{k=0} |\epsilon^{A}_{i,k}| \cdot 2^{b+k}$ es pequeña, por ejemplo < 2a.

Todas las demás adiciones puede emplear una aritmética de enteros comunes, o (preferentemente) utilizan una adición módulo Ni. Por lo que la evaluación de cada uno de los polinomios monovariables $\sum^{m}_{j=1} <f_j(x,A)>_{pj}$ realizaron individualmente una operación módulo de módulo pj más pequeño pero la sumatoria de éstos polinomios monovariables realizó preferentemente módulo N. También agregar el polinomio de ofuscación $\sum^{a}_{k=0} \epsilon^{A}_{i,k}X^{k}$ puede hacerse usando aritmética de enteros convencional o, preferentemente módulo N. El material generador de claves comprende los coeficientes $C^{A}_{i,k}$ con k = 0, ..., a, y i = 1, ..., t. El material generador de claves puede presentarse como un conjunto de polinomios como se mencionó anteriormente. En la práctica, el material generador de claves puede almacenarse como una lista, por ejemplo, una matriz bidimensional, de los enteros $C^{A}_{i,k}$ El dispositivo A también recibe los números Ni y b. La manipulación de polinomios puede implementarse, por ejemplo como manipulación de matrices que contienen los coeficientes, por ejemplo enumerando todo coeficiente en un orden predeterminado.

Nótese que los polinomios pueden implementarse, en otras estructuras de datos, por ejemplo como una matriz asociativa (conocida como "mapa") que comprende un conjunto de pares (de grados, coeficientes), preferentemente de tal manera que cada coeficiente aparece cuando mucho una vez en el conjunto. Los coeficientes C^{A}_{i} que se proveen al dispositivo están preferentemente en el intervalo 0, 1, .. N-1. Debido a un tamaño de identificador pequeño puede ocurrir que no todos los bits de los coeficientes serán utilizados para la generación de claves. En ese caso, solo necesitan almacenarse partes de coeficientes relevantes.

Como se indicó al principio de este documento, para reducir la probabilidad de que el dispositivo A derive una clave compartida diferente en comparación con su contraparte el dispositivo B, los polinomios de ofuscación pueden seleccionarse de tal forma que para cada k = 0, ..., a

$$\sum^{t}_{i=1} \varepsilon_{i,k} \equiv 0 \bmod 2^{b}$$

Es decir la suma de todos los polinomios de ofuscación es un múltiplo de 2^{b}. Como ya se mencionó, esto tiene la buena propiedad de que si el atacante quiere remover el ruido agregando materiales generadores de claves, entonces estará mezclando materiales generadores de claves obtenidos por la realización de operaciones modulares con diferentes módulos. Si no los agrega, entonces los materiales generadores de claves están ocultos por el ruido

En caso de que se utilice la construcción más general para N y los números enteros p_j, el polinomio de ofuscación necesita adaptarse de tal manera que los números aleatorios ϵ afecten diferentes partes de los coeficientes. Por ejemplo, si el efecto no lineal se introduce en los bits menos significativos de los coeficientes del material de clave almacenado en los dispositivos de red, entonces los números aleatorios solo deben afectar la parte más alta de los coeficientes y un número variable de bits en la parte más baja de los coeficientes. Esto es una extensión directa del método descrito arriba y son factibles otras extensiones.

Fase de uso

Una vez que los dispositivos A y B tienen un número de identidad y han recibido su material generador de claves de la TTP, pueden usar su material generador de claves para obtener una clave compartida. El dispositivo A puede realizar los siguientes pasos para obtener su clave compartida. Primero, el dispositivo A obtiene el número de identidad B del dispositivo B, después A genera la clave compartida calculando lo siguiente:

$$K_{AB} = <\sum_i < F^{A_i}(X) \,/\, _{X=B} >{Ni} >{2b} = < \sum_i < \sum_k C^{A_{i,k}} B^k >{Ni} >{2b}$$

Es decir, A evalúa cada uno de sus polinomios monovariable F^{A_i} de su material generador de claves, para el valor B; el resultado de evaluar el material generador de claves es un entero. Enseguida el dispositivo A reduce el

resultado de la evaluación del primer módulo el módulo público Ni correspondiente. Enseguida el resultado de la evaluación de todos los polinomios F^{A}_{i} después de la evaluación modularse agrega como enteros, y entonces el resultado de esta suma se considera como módulo el módulo de clave 2^{b}. El resultado se citará como clave compartida de A, se trata de un entero en el intervalo de 0 hasta $2^{b} - 1$. Para esta parte, el dispositivo B puede generar la clave compartida de B evaluando su material de clave para la identidad A y reducir el resultado módulo N y después módulo 2^{b}, de la misma manera que lo hizo A.

En línea con la descripción anterior, si se utilizan una expresión más general de N y los enteros positivos p_{j}, entonces el método para obtener la clave de b bits necesita una pequeña adaptación. En particular, podemos considera que $p_{i*m+j} = \beta 2^{X} + \gamma_{i*m+j} 2^{Yi,j} + \delta 2^{W} + \zeta_{i} 2^{Zi}$ para los módulos privados y $N_{i} = \beta 2^{X} + \delta 2^{W} + \zeta_{i} 2^{Zi}$ para el módulo público, después esto permite introducir una no linealidad en el material generador de claves compartido medio del término Y_{i*m+j} de b bits. Nótese que en esta construcción específica, tenemos m polinomios en cada conjunto de material generador de claves y cada uno de esos polinomios está indexado por un identificador j. Adicionalmente podemos tener hasta t conjuntos de materiales generadores de claves diferentes indexados por medio de i. Nótese también que típicamente Yij es constante $\forall$ i,j.

Adicionalmente los términos ζ_i de b bits ~~difieren para~~ diferentes N_i con i = 1, ..., t y son los que introducen el efecto no lineal cuando se mezclan claves generadas de diferentes materiales generadores de claves en el nodo. En este caso, la clave se genera de la siguiente manera:

$$K_{AB} = < \frac{\Sigma_i < F_i^A(X)\big|_{X=B} >_{N_i}}{2^W} >_{2^b}$$

Como podemos ver, cada uno del t material generador de claves compartido se evalúan en x = B y se reducen módulo Ni. En esta reducción se introduce el efecto de ζ_i. Dado que la potencia más pequeña de dos comunes a todo P_{i*m+j} es w, entonces el resultado se divide (división de enteros) entre 2^W de tal manera que puede generarse una clave común.

Debido a que los polinomios bivariables en el material de clave raíz son simétricos la clave compartida de A y la clave compartidas de B son con frecuencia, aunque no necesariamente siempre, iguales. Los requisitos particulares en los módulos privados, los enteros $p_1, p_2, \ldots, p_m$, en los conjuntos de parámetros y en los números aleatorios ϵ son tales que las claves son frecuentemente iguales y casi siempre cercanas entre sí módulo dos a la potencia de la longitud de clave. Si A y B han obtenido la misma clave compartida, entonces pueden usarla como una clave simétrica que es compartida entre A y B; por ejemplo, puede usarse para una variedad de aplicaciones criptográficas, por ejemplo,

pueden intercambiar uno o más mensajes cifrados y/o autenticarse empleando una clave compartida. Preferentemente, se aplica un algoritmo de derivación de clave a la clave compartida para protección adicional de la clave maestra, por ejemplo, puede aplicarse una función de dispersión.

Si A y B no han obtenido la misma clave compartida, entonces es casi cierto que estas claves están cerca una de la otra, al remover un número de bits menos significativos de las claves, las claves generadas casi siempre pueden hacerse iguales. A y B pueden comprobar si sus claves compartidas son iguales realizando una confirmación de claves, por ejemplo A puede enviar a B un mensaje que contiene el par (m, E(m)), en donde m es un mensaje, por ejemplo una cadena fija o un número aleatorio y E(m) es el cifrado que utiliza una clave compartida de A.

Al descifrar E(m) utilizando la clave compartida de B, B puede comprobar su las claves son iguales. Si es así, B puede responder a A informándole de la situación.

Si las claves no son iguales, A y B pueden involucrarse en un protocolo de igualación. Por ejemplo, pueden utilizar el hecho de que dos claves son aritméticamente cercanas entre sí. Por ejemplo, el dispositivo de red A y B puede remover iterativamente un bit menos significativo y enviar un mensaje de confirmación de clave hasta que las claves sean iguales. Después de obtener claves iguales, A y B pueden ejecutar un

algoritmo de derivación de clave para volver a obtener claves de una longitud de clave usual.

Los m módulos privados seleccionados $p_1, p_2, \ldots, p_m$, son preferentemente relativamente primos por pares. Si estos números son relativamente primos por pares aumenta la falta de compatibilidad entre las operaciones módulo. La obtención de números relativamente primos por pares puede obtenerse seleccionando los enteros en orden, probando para cada nuevo entero su todos los pares de diferentes números son aún relativamente primos, si no el número que se acaba de seleccionar es eliminado del conjunto. Este procedimiento continúa hasta que se seleccionan todos los m números.

La complejidad aumenta aún más requiriendo que los m módulos privados seleccionados $p_1, p_2, \ldots, p_m$, sean números primos distintos. En ese caso puede requerirse que cada número primo tenga la forma $p_j = N + \gamma_j \cdot 2^b$. En donde γ_j son enteros tales que $|\gamma_j| < 2^b$. Experimentos han confirmado que estos primos están fácilmente disponibles. Por ejemplo, puede seleccionarse repetidamente un γ_j aleatorio y probar el p_j resultante hasta que se encuentre un número primo. Lo mismo aplica si se aplica una expresión más general como se describió arriba. De hecho se tiene que del teorema de números primos para progresiones aritméticas que siempre y cuando a sea de aproximadamente el mismo orden de magnitud que b, en particular $a < b$, los números primos son

abundantes. En particular, para cualquier combinación de longitud de clave en el grupo 64, 128, 196, 256 y grado en el grupo 2, 3, confirmamos experimentalmente que podrían generarse muchos números primos usando el algoritmo anterior en los límites de tiempo prácticos. Cuando se usan números primos cada polinomio f_j se considera entonces en el campo finito con p_j elementos.

Son posibles muchas variantes para elegir varios parámetros utilizados durante la fase de registro y uso. Por ejemplo, en una modalidad simplificada, los módulos privados son más pequeños que el módulo público y satisfacen la relación $p_j = N - \beta_j \cdot 2^b$. En donde β_j son enteros positivos tales que $\beta_j < 2^b$. Una manera práctica de seleccionar números que satisfagan este requisito es seleccionar un conjunto de m enteros positivos aleatorios β_j tales que $\beta_j < 2^b$ y calcular los módulos privados seleccionados a partir de la relación $p_j = N - \beta_j \cdot 2^b$.

Como se indica, la diferencia entre $Y_j - Z_j - \log_2(\zeta_j)$ puede ser $\alpha_j b$. De manera similar, pueden definirse otras construcciones siguiendo el mismo concepto. En particular, podemos escribir $p_j = \beta 2^X + \gamma_j 2^{Y_j} + \delta 2^W + \zeta_j 2^{Z_j}$ para los módulos privados y $N = \beta 2^X + \delta 2^W$ para el módulo público. Una ejemplificación particular de esta construcción es $p_j = 2^{2(a+1)b} + \gamma_j 2^{(a+1)b} + 2^{ab} + \zeta_j$ y $N = 2^{2(a+1)b} + 2^{ab}$. En este caso, el valor absoluto de los términos γ_j y β_j es menor que 2b y son

responsables de crear un efecto no lineal en los MSB y LSB de los coeficientes del material de clave local almacenado en un dispositivo. Nótese que dado que los identificadores de dispositivos son de aproximadamente b bits de largo, $\gamma_j(\beta_j)$ afecta al MSB (LSB) de los coeficientes del polinomio compartido evaluado en el anillo de eneros módulo p_j. Posteriormente durante la generación del material de clave local para un dispositivo los coeficientes del polinomio compartido en diferentes anillos se suman a los enteros de tal manera que se oculta el origen de las contribuciones.

La clave puede generarse de la siguiente manera:

$$K_{AB} = < \frac{\Sigma_i < F_i^A(X)\big|_{X=B} >_{N_i}}{2^W} >_{2^b},$$

pero si incluso se utiliza la expresión más general de p_j y N que permite introducir un efecto non lineal tanto en MSB como en LSB, entonces la división después de la reducción módulo N es por 2 a la potencia de W, en donde 2^W es la potencia entero más alta de 2 cuyo N es un entero múltiple. Otras construcciones de N y p_j pueden requerir una división entre otra potencia de dos. Debido a que los polinomios bivariables en el material de clave raíz son simétricos la clave compartida de A y la clave compartidas de B son con frecuencia, aunque no necesariamente siempre, iguales.

La figura 1 es un diagrama de bloques esquemático que ilustra un generador de material de clave raíz 100. Un

obtenedor de material de clave está configurado para proporcionar datos de entrada, excepto un número de identidad, requerido por un generador de material de clave para generar material de clave local. Un generador de claves es un ejemplo de un obtenedor de material de clave. En lugar de generar todo o parte de los datos de entrada, algunos parámetros pueden obtenerse también por el generador de materiales de claves raíz al recibirlos, por ejemplo el obtenedor de claves puede comprender un receptor electrónico para recibir datos de entrada, por ejemplo, un módulo público y privado. Un obtenedor de material de clave obtiene todos los parámetros necesarios excepto los números de identidad de una fuente externa. En una modalidad, a, b, m están predeterminados, por ejemplo son recibidos y se generan el módulo público y los módulos privados en los conjuntos de parámetros y los polinomios bivariables (simétricos) correspondientes. En una modalidad también se predeterminan los módulos públicos, por ejemplo son recibidos.

El generador de clave raíz 100 genera múltiples conjuntos de parámetros y comprende un número t del elemento de conjuntos de parámetros 130 que contiene el número de conjuntos de parámetros que necesitan generarse. Por ejemplo, t = 2 o t = 3, etc.

El generador de clave raíz 100 comprende un elemento de grado polinomial 112, un elemento de longitud de clave 114 y

un número de elemento de polinomios 116 configurado para proporcionar el grado del polinomio, la longitud de la clave y el número de polinomios, es decir, a, b y m respectivamente, para un conjunto de parámetros dado. Típicamente, un elemento de longitud de clave 114 será igual en todos los conjuntos de parámetros. Típicamente, un elemento de grado de polinomio 112 también será el mismo en todos los conjuntos de parámetros, aunque esto no es necesario. En algunas modalidades el número del elemento de polinomios 116 varía a lo largo de los conjuntos de parámetros; por ejemplo algunos pueden usar m = 1, mientras que algunos pueden usar m = 2. También es posible tener m constante, por ejemplo m = 1 o m = 2, a lo largo de los conjuntos.

Aunque estos elementos pueden generarse, por ejemplo dependiendo de las circunstancias, típicamente estos parámetros los elije un diseñador de sistemas. Por ejemplo, los elementos puede diseñarse como memorias no volátiles, o como receptores para recibir los valores de elementos, o como memorias volátiles conectadas a un receptor, etc. Una elección adecuada incluye t = 2, a = 2, b = 128, m = 2. Cualquiera de los números puede aumentarse o disminuirse para obtener un sistema más o menos seguro.

El generador de clave raíz 100 comprende un elemento de módulo público 110 configurado para proporcionar el módulo

público N de un conjunto de parámetros. El módulo público puede o no ser elegido por un diseñador de sistemas. Por ejemplo, el módulo público puede ser establecer un número convencional que permite una rápida reducción (cerca o igual a una potencia de dos). El módulo público se elige en un intervalo determinado por los elementos 112 y 114.

El generador de clave raíz 100 comprende un administrados de módulos privados 122 configurado para proporcionar el módulo privado p, o múltiples módulos privados p_1; ... ,p_m. Por ejemplo, se eligen al azar en los límites apropiados.

El generador de clave raíz 100 comprende un administrador de polinomios bivariables simétricos 124 configurado para proporcionar el polinomio bivariable simétrico f, o múltiples polinomios bivariables simétricos f_1, ..., f_m. Cada polinomio bivariable simétrico se elige con coeficientes aleatorios módulo el módulo privado correspondiente, es decir, el módulo privado que tiene el mismo índice. Los coeficientes pueden elegirse en el intervalo de 0 a p - 1, y pueden elegirse al azar.

Los módulos privados pueden elegirse sumando al módulo público o sustrayendo de éste un múltiplo de dos a la potencia de la longitud de clave. Esto resultará en módulos privados tales que la diferencia con el módulo público termina en una serie de ceros consecutivos. Puede elegirse un

módulo público y uno o más módulos privados tales que se presenta una serie de ceros consecutivos de longitud de clave no al final sino en otra posición, por ejemplo la posición 's', contando desde el bit menos significativo.

La figura 1' muestra un ejemplo de material de clave raíz 180 generado por el generador de claves raíz 100. El material de clave raíz 180 comprende un número de conjuntos de parámetros 140, en este caso tiene el valor de 3. El material de clave raíz 180 comprende tres conjuntos de parámetros. El primer conjunto comprende el módulo público 141, los módulos privados 151, 153 y 155 y los polinomios bivariables correspondientes 152, 154 y 156. El segundo conjunto comprende el módulo público 142, los módulos privados 161 y 163 y los polinomios bivariables correspondientes 162 y 164. El tercer conjunto comprende el módulo público 143, los módulos privados 171, 173 y 175 y los polinomios bivariables correspondientes 172, 174 y 176. En este caso el grado de los polinomios es implícito en la representación de los polinomios, podría hacerse también explícito. En este ejemplo de material de clave raíz 180 también se registra la longitud de la clave 144.

Durante la operación, el obtenedor de material de clave raíz 100 genera repetidamente conjuntos de parámetros hasta que se ha producido un número igual al número en el elemento 130. El número de los conjuntos de parámetros puede

registrarse en el material de clave raíz 180 en 140.

La figura 2 es un diagrama de bloques esquemático que ilustra un generador de material de clave local 200. El generador de material de clave 100 y el generador de material de clave local 200 forman conjuntamente un sistema para configurar un dispositivo de red para compartir claves.

El generador de material de clave local 200 comprende un dispositivo de manipulación polinomial 240. El generador de material de clave local 200 comprende un elemento de material de clave raíz 210 para proporcionar el material de clave raíz al dispositivo de manipulación polinomial 240, es decir, proporcionar múltiples conjuntos de parámetros al dispositivo de manipulación polinomial 240, a su vez para producir múltiples polinomios monovariables. El elemento 210 puede implementarse por medio de los elementos correspondientes del generador de material de clave 100; estos elementos puede ser también memorias o buses para conectar al generador de material de clave 100.

El generador de material de clave local 200 comprende un generador de números de ofuscación 260 para proporcionar un números de ofuscación $'\in_{Ai}$ al dispositivo de manipulación polinomial 240. El número de ofuscación puede ser un número aleatorio, por ejemplo generado con el generador de números aleatorios. El generador de números de ofuscación 260 puede generar múltiples números de ofuscación para múltiples

coeficientes del polinomio monovariable. El generador 260 puede estar restringido para generar números simples, por ejemplo un número de ofuscación por cada conjunto de parámetros, o un número de ofuscación para por lo menos dos de los conjuntos de parámetros, pero el generador 260 también puede configurarse para generar polinomios de ofuscación diferentes de cero, los cuales se agregarán al polinomio monovariable que corresponde al conjunto de parámetros para obtener un polinomio monovariable ofuscado. En una modalidad, se determina un número de ofuscación para cada coeficiente del polinomio monovariable. Un polinomio de ofuscación puede tener 1 ó 2 o más coeficientes diferentes de cero.

El generador de material de clave local 200 comprende un administrador de dispositivos de red 250 configurado para recibir un número de identidad para el cual debe generarse material de clave local, por ejemplo de un dispositivo de red, y está configurado para enviar el material de clave local al dispositivo de red correspondiente al número de identidad. En lugar de recibir un número de identidad, también puede generarse, por ejemplo como un número aleatorio, en serie o momentáneo. En este último caso el número de identidad es enviado junto con el material de clave local al dispositivo de red.

El dispositivo de manipulación polinomial 240 genera un polinomio monovariable para cada conjunto de parámetros en el

elemento del material de clave raíz 210.

Para cada conjunto de parámetros, el dispositivo de manipulación polinomial 240 obtiene, posiblemente múltiples, polinomios monovariables sustituyendo el número de identidad del administrador 250 en cada uno de los polinomios bivariables y reduciendo cada módulo el módulo privado correspondiente. Los múltiples polinomios monovariables reducidos resultantes se agregan, como coeficientes, con adición aritmética natural. También se adicionan el número o los números de ofuscación. Preferentemente, el resultado se reduce, de nuevo en cuanto a coeficiente, módulo el módulo público; los coeficientes de éste pueden representarse en el intervalo de 0 a N - 1.

Los polinomios monovariables ofuscados son parte del material de clave local que pertenece al número de identidad. Si es necesario, los módulos públicos, el grado y la longitud de clave también se envían al dispositivo de red.

La figura 2' muestra material de clave raíz 280 generado para un dispositivo de red de un material de clave raíz 180. El material de clave raíz local 280 comprende el número de conjuntos de parámetros 140 (en este caso 3), la longitud de clave 144, los módulos públicos 141, 142 y 143 y los polinomios monovariables generados correspondientes (posiblemente ofuscados) 252, 262 y 274, respectivamente. Opcionalmente, el material de clave raíz local 280 puede

comprender una potencia de 2 para división y módulo de clave para generar la clave compartida.

La figura 3 es un diagrama de bloques esquemático que ilustra una red de comunicación 300 que comprende múltiples dispositivos de red; se muestran un primer dispositivo de red 310 y un segundo dispositivo de red 320. Ilustraremos primero el primer dispositivo de red 310. El segundo dispositivo de red 320 puede ser el mismo, o trabajar con los mismos principios.

El dispositivo de red 310 comprende un transceptor 330 que combina un emisor y un receptor para enviar y recibir mensajes en formato electrónico, por ejemplo digital, en forma física o inalámbrica desde y hacia un segundo dispositivo de red 320. Posiblemente, el transceptor 330 también se usa para recibir el material de clave local de la autoridad de red 200. A través del transceptor 330 es recibido el número de identidad de otro dispositivo de red; en la figura del segundo dispositivo de red 320.

El dispositivo de red 310 comprende un obtenedor de material de clave local 344. El obtenedor de material de clave local 344 puede implementarse como una memoria local, por ejemplo una memoria no volátil tal como una memoria flash para almacenar el material de clave local. El obtenedor de material de clave local 344 también puede configurarse para obtener el material de clave local del

generador 200, por ejemplo vía el transceptor 330. El obtenedor de material de clave local 344 está configurado para proporcionar el dispositivo de manipulación polinomial con los parámetros necesarios.

El dispositivo de red 310 comprende un dispositivo de manipulación polinomial 342. El dispositivo de manipulación polinomial 342 funciona en dos fases.

En la fase de sustitución, el número de identidad del segundo dispositivo de red se sustituye (530) en cada uno de los polinomios monovariables en el material de clave local. El resultado de la sustitución se reduce módulo el módulo público que corresponde a el polinomio monovariable. En la fase de adición subsiguiente, los resultados de las reducciones módulo un módulo público se adicionan juntos y se reducen (540) módulo un módulo de clave. Nótese que para algunas combinaciones de N y el módulo privado, se requiere un a división entre 2 antes de que el resultado se reduzca módulo un módulo de clave.

El dispositivo de red 310 comprende un dispositivo de derivación de claves 346 para derivar la clave compartida del resultado de la reducción módulo el módulo de clave. Por ejemplo, el dispositivo de derivación de claves 346 puede remover uno o más bits menos significativos. El dispositivo de derivación de claves 346 también puede aplicar una función de derivación. También es posible usar

el resultado de la segunda reducción sin procesamiento adicional.

El dispositivo de red 310 comprende un igualador de claves opcional 348. Nótese que puede suceder que la clave compartida derivada en el primer dispositivo de red no sea igual que la clave derivada en el segundo dispositivo de red (con base en el número de identidad del primer dispositivo de red). Si esto es considerablemente no deseable, puede seguirse un protocolo de igualación.

El dispositivo de red 310 comprende un elemento criptográfico 350 configurado para utilizar la clave compartida para una aplicación criptográfica. Por ejemplo, el elemento criptográfico 350 puede cifrar o autenticar un mensaje del primer dispositivo de red con la clave compartida antes de enviarlo al segundo dispositivo de red, por ejemplo un mensaje de estado. Por ejemplo, el elemento criptográfico 350 puede descifrar o comprobar la autenticidad de un mensaje recibido del segundo dispositivo de red.

Típicamente, un sistema para configurar un dispositivo de red para compartir claves 200, y un primer dispositivo de red configurado para determinar una clave compartida 310, comprenden cada uno un microprocesador (no se muestra) que ejecuta software apropiado almacenado en los respectivos dispositivos, por ejemplo, cuyo software puede

haberse descargado y almacenado en una memoria correspondiente, por ejemplo RAM (no se muestra).

Una modalidad interesante se obtiene para a = 1, especialmente en combinación con valores más altos de m, por ejemplo más altos que 1, 2 o mayores, 4 o mayores. La manipulación polinomial requerida se reduce a una multiplicación y reducción simples, obteniendo una implementación especialmente simple. Sin embargo, incluso para este caso simple la recuperación de los polinomios bivariables originales no es directa, y se complica cada vez más con valores de m más altos. Aunque no se conoce un ataque viable incluso para a = 1, la estructura lineal puede ser un punto de inicio para análisis futuro, por lo que puede desearse restringir a a > 1, por esta razón.

La figura 4 es un diagrama de flujo esquemático que ilustra un método 400 de generación de material de clave local. El método 400 puede usarlo una tercera parte confiable. En el paso 410, se obtienen los parámetros requeridos. En particular, se obtienen múltiples conjuntos de parámetro, por lo menos dos. Cada conjunto de parámetros contiene módulos públicos y por lo menos un módulo privado y por lo menos un polinomio bivariable. En el paso 420, se obtiene un número de identidad, por ejemplo, en una red de telecomunicación. El número de identidad puede recibirse en un mensaje electrónico.

El paso 430 se repite una vez para cada conjunto de parámetros. El número de identidad obtenido es sustituido en el polinomio bivariable, t reducido módulo el módulo privado. Pueden haber más polinomios bivariables, por ejemplo 2. En ese caso la sustitución se hace en cada uno, y los resultados se adicionan en aritmética de enteros. En el paso 440, el resultado se ofusca, por ejemplo adicionando un polinomio de ofuscación. En una implementación simple la ofuscación puede ser solo un coeficiente simple. El paso 440 es opcional. De esta manera, o como se describió en la presente, se obtiene una combinación de polinomio monovariable y módulo público que formará parte del material de clave local. En el paso 450, se decide si quedan conjuntos de parámetros y si es así se repiten los pasos 430 y 440 para un siguiente conjunto de parámetros. En el paso 450, el material de clave local que incluye los polinomios monovariables se almacenan en el dispositivo de red.

La figura 5 es un diagrama de flujo esquemático que ilustra un método 500 de generación de una clave compartida. El método 500 puede ejecutarse en un dispositivo de red.

En el paso 510, se obtiene el número de identidad externo de otro dispositivo de red, por ejemplo recibiendo un mensaje electrónico. En el paso 520, el número de

identidad local se envía al otro dispositivo de red. Después de los pasos 510 y 520, el dispositivo de red local y el dispositivo de red externo tienen cada uno el número de identidad del otro. Utilizando su material de clave local proceden a derivar la clave compartida común.

El dispositivo de red local repite un paso de sustitución 530 para un polinomio monovariable en su material de clave local. En el paso 530, el número de identidad local se sustituye en un polinomio monovariable ofuscado módulo el módulo público correspondiente. En el paso 535, se decide si quedan polinomios monovariables y si es así se repite el paso 530 para un siguiente polinomio monovariable del material de clave local. En el paso 540, los resultados de las reducciones módulo un módulo público se adicionan juntos y se reducen módulo un módulo de clave.

El resultado del paso 550 es el inicio de la obtención de la clave compartida. En el paso 550, se deriva una clave compartida, por ejemplo aplicando un algoritmo de derivación de clave. En el paso 560, se envía un mensaje de confirmación al otro dispositivo de red, y en paso 570, se determina si se confirma la clave. Si la clave no se confirma en el paso 570, entonces el método continúa en el paso 550 con la derivación de una nueva clave. Por ejemplo, el paso 550 puede remover un bit menos

significativo adicional cada vez que no se confirme la clave. Si la clave es confirmada puede usarse una aplicación criptográfica opcional, o almacenarse localmente para uso posterior.

Los pasos 550, 560 y 570 forman conjuntamente un protocolo de igualación de claves. Por ejemplo, en el paso 560, puede enviarse un valor momentáneo y el cifrado del valor momentáneo bajo la clave compartida derivada en el paso 550 al segundo dispositivo. En el paso 560 se recibe un mensaje del segundo dispositivo. El mensaje recibido puede simplemente decir que el mensaje de confirmación de claves recibido mostró que las claves no son iguales. El mensaje recibido también puede contener un mensajes de confirmación de claves. En este último caso, el primer dispositivo de red verifica el mensaje del confirmación de claves y establece si las claves son iguales. Si no es así se deriva una nueva clave, por ejemplo, eliminando un bit menos significativo.

La figura 6 muestra en forma esquemática una secuencia posible de mensaje entre dos dispositivos de red, el dispositivo A y B, mientras están generando una clave compartida. El tiempo transcurre hacia abajo. En el paso 610, un dispositivo de red A envía su número de identidad al dispositivo B. En el paso 620, el dispositivo B envía su número de identidad y un mensaje de confirmación de

claves para la clave compartida (K1) derivada con base en el número de identidad A y su material de clave local. En el paso 630, el dispositivo A encuentra que no generaron la misma clave. El dispositivo A ha eliminado un bit menos significativo (por ejemplo un entero dividido entre 2) para obtener la clave K2. En el paso 630, el dispositivo A envía un nuevo mensaje de confirmación de claves. De esta manera A y B intercambian mensajes de confirmación de claves 640 hasta que arriban a la misma clave en el paso 650. En el paso 650, el dispositivo A envía un mensaje de confirmación de claves al dispositivo B. El dispositivo B fue capaz de verificar que hubo arribado a la misma clave. En el paso 660, envía su confirmación, esto puede ser un mensaje autenticado o un mensaje de confirmación de claves, etc. En el paso 670, el dispositivo A envía un mensaje M1 que está cifrado (por ejemplo empleando AES) y /o autenticado (por ejemplo empleando HMAC) utilizando la ahora igual clave compartida.

Se apreciará que la invención también se extiende a programas de cómputo, particularmente programas de cómputo sobre o en un portador, adaptado para poner en práctica la invención. El programa puede estar en forma de código fuente, código de objetos, una fuente intermedia de código y código de objetos tal como una forma parcialmente compilada, o en cualquier otra forma adecuada para usarse

en la implementación del método de conformidad con la invención. Una modalidad que se relaciona con un producto de programa de computadora comprende instrucciones ejecutables en computadora que corresponden a cada uno de los pasos de procesamiento de por lo menos uno de los métodos presentados. Estas instrucciones pueden subdividirse en subrutinas y/o almacenarse en uno o más archivos que pueden vincularse estáticamente o dinámicamente. Otra modalidad que se relaciona con un producto de programa de computadora comprende instrucciones ejecutables en computadora que corresponden a cada uno de los medios de por lo menos uno de los sistemas y/o productos presentados.

Debe apreciarse que las modalidades antes mencionadas ilustran en lugar de limitar la invención, y que aquellos con experiencia en la técnica serán capaces de diseñar muchas modalidades alternativas.

En las reivindicaciones, cualquier signo de referencia colocado entre paréntesis no debe considerarse como limitante de la invención. El uso del verbo "comprende" y sus conjugaciones no excluyen la presencia de elementos o pasos distintos de los establecidos en una reivindicación. El artículo "un" o "una" que antecede a un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede implementarse por medio de hardware que

comprende varios elementos distintos, y por medio de un computadora adecuadamente programada. En la reivindicación de dispositivo que enumera varios medios, varios de estos medios pueden estar conformados por un mismo elemento de hardware. El simple hecho de que se citen ciertas medidas en reivindicaciones mutuamente diferentes no indica que una combinación de esas medidas no pueda usarse ventajosamente.

Lista de Números de Referencia para las figuras 1-3:

100 obtenedor de material de clave raíz

110 administrador de módulos públicos

112 elemento de grado polinomial

114 elemento de longitud de clave

116 número de elemento de polinomios

122 administrador de módulos privados

124 administrador de polinomios bivariables simétricos

130, 140 polinomio bivariable

180 material de clave raíz

200 generador de material de clave local

210 elemento de material de clave raíz

240 dispositivo de manipulación polinomial

250 administrador de dispositivos de red

252, 262, 272 polinomio monovariable

260 generador de números de ofuscación

300 red de comunicación

310 primer dispositivo de red

320 segundo dispositivo de red

330 transceptor

342 dispositivo de manipulación polinomial

344 obtenedor de material de clave local

346 elemento de derivación de claves

348 igualador de claves

350 elemento criptográfico

Se hace constar que con relación a esta fecha, el mejor método conocido por la solicitante para llevar a la práctica la citada invención, es el que resulta claro de la presente descripción de la invención.

REIVINDICACIONES

Habiéndose descrito la invención como antecede, se reclama como propiedad lo contenido en las siguientes reivindicaciones:

1. Un método de configuración de un dispositivo de red para compartir claves, caracterizado porque comprende:

obtener en forma electrónica por lo menos dos conjuntos de parámetros, un conjunto de parámetros comprende un módulo privado, un módulo público y un polinomio bivariable que tiene coeficientes enteros, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en por lo menos bits consecutivos de longitud de clave,

generar material de clave local para el dispositivo de red, el paso generar comprende

obtener en forma electrónica un número de identidad para el dispositivo de red, y

para cada conjunto de parámetros obtener un polinomio monovariable correspondiente, determinando, mediante el empleo de un dispositivo de manipulación polinomial, un polinomio monovariable a partir del polinomio bivariable del conjunto de parámetros por sustitución del número de identidad en el polinomio bivariable y reduciendo el resultado de la sustitución módulo el módulo privado del

conjunto de parámetros, y

almacenar electrónicamente en el dispositivo de red el material de clave local generado, el material de clave local generado comprende el módulo público de cada conjunto de parámetros y el polinomio monovariable correspondiente de cada conjunto de parámetros.

2. Un método de conformidad con la reivindicación 1, caracterizado porque generar material de clave local para el dispositivo de red comprende:

para por lo menos dos de los por lo menos dos conjuntos de parámetros

generar un polinomio de ofuscación diferente de cero que corresponde al conjunto de parámetros,

adicionar, usando un dispositivo de manipulación polinomial, el polinomio de ofuscación diferente de cero al polinomio monovariable que es correspondiente con el conjunto de parámetros para obtener un polinomio monovariable ofuscado,

el material de clave local generado comprende el polinomio monovariable ofuscado.

3. Un método de conformidad con la reivindicación 2, caracterizado porque cada coeficiente de la suma de los polinomios de ofuscación es un múltiplo de 2 a la potencia de la longitud de clave.

4. Un método de conformidad con la reivindicación 2,

caracterizado porque cada coeficiente de la suma de los polinomios de ofuscación dividido entre una potencia de dos, redondeado hacia abajo a un número entero, es un múltiplo de 2 a la potencia de la longitud de clave.

5. Un método de conformidad con la reivindicación 1 ó 2, caracterizado porque todos los polinomios bivariables en todos los conjuntos de parámetros son polinomios simétricos.

6. Un método de conformidad con cualquiera de las reivindicaciones anteriores, caracterizado porque en todos los conjunto de parámetros, los mismos por lo menos bits consecutivos de longitud de clave de la representación binaria del módulo público de un conjunto de parámetros respectivo son iguales que los bits de longitud de clave menos significativos del módulo privado del respectivo conjunto de parámetros.

7. Un método de conformidad con la reivindicación 6, caracterizado porque los por lo menos bits consecutivos de longitud de clave son los bits de longitud de clave menos significativos.

8. Un método de configuración de un dispositivo de red para compartir claves de conformidad con cualquiera de las reivindicaciones anteriores, caracterizado porque comprende:

generar el módulo privado usando un generador de números aleatorios electrónico, y/o

generar el polinomio bivariable usando un generador de

números aleatorios electrónico mediante la generación de uno o más coeficientes aleatorios para el polinomio bivariable.

9. Un método de configuración de un dispositivo de red para compartir claves de conformidad con cualquiera de las reivindicaciones anteriores, caracterizado porque uno o todos los módulos públicos satisfacen $2^{(a+2)b-1} \leq N$, en donde N representa el módulo público, a representa el grado del polinomio bivariable y b representa la longitud de la clave.

10. Un método de configuración de un dispositivo de red para compartir claves de conformidad con cualquiera de las reivindicaciones anteriores, caracterizado porque por lo menos dos conjuntos de parámetros comprenden múltiples módulos privados, y múltiples polinomios bivariables que tienen coeficientes módulo p_i, tales que existe un conjunto de posiciones consecutivas de longitudes de clave en las cuales la representación binaria del módulo público concuerda con la representación binaria de todos los módulos privados, el método adicionalmente comprende:

determinar el polinomio monovariable que comprende sustituir el número de identidad en cada uno de los múltiples polinomios bivariables, reducir módulo un módulo privado de los múltiples módulos privados que corresponden al polinomio bivariable simétrico, y sumar los múltiples resultados de las múltiples reducciones.

11. Un método de configuración de un dispositivo de red

para compartir claves de conformidad con cualquiera de las reivindicaciones anteriores, caracterizado porque el número de ofuscación se genera de tal manera que $|\epsilon^{A}_{i,k}| < 2^{(a+2-k)b-2}$, en donde $\epsilon_{A,i}$ denota el número de ofuscación, i denota el grado del monomio que corresponde al coeficiente, a representa el grado del polinomio bivariable y b representa la longitud de la clave.

12. Un método para que un primer dispositivo de red determine una clave compartida, siendo la clave una clave criptográfica, caracterizado porque comprende:

obtener el material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende por lo menos dos polinomios monovariables y módulos públicos correspondientes,

obtener un número de identidad para un segundo dispositivo de red, el segundo dispositivo de red es diferente del primer dispositivo de red,

para cada conjunto de los por lo menos dos polinomios monovariables: sustituir el número de identidad del segundo dispositivo de red en el polinomio monovariable y reducir el resultado de la sustitución módulo el módulo público que corresponde al polinomio monovariable, y

sumar entre sí los resultados de las reducciones módulo un módulo público y reducir módulo un módulo de clave, y

derivar la clave compartida del resultado de la

reducción módulo el módulo de clave.

13. Un método para que un primer dispositivo de red determine una clave compartida de conformidad con la reivindicación 11, caracterizado porque comprende:

determinar si el primer dispositivo de red y el segundo dispositivo de red han derivado la misma clave compartida, y si no, derivar una clave compartida adicional del resultado de la reducción módulo el módulo de clave.

14. Un método de conformidad con las reivindicaciones 12 ó 13, caracterizado porque comprende dividir el resultado de la sustitución módulo el módulo público entre un divisor de cadena de cero bits el cual es una potencia de dos, el divisor de cadena de cero bits es mayor que 1, y redondear hacia abajo a un número entero el resultado de la división.

15. Un dispositivo de red configurado para determinar una clave compartida, siendo la clave una clave criptográfica, caracterizado porque comprende:

un obtenedor de material de clave local configurado para obtener el material de clave local para el dispositivo de red en forma electrónica, el material de clave local comprende por lo menos dos polinomios monovariables y módulos públicos correspondientes,

un receptor configurado para obtener un número de identidad para un dispositivo de red adicional diferente.

un dispositivo de manipulación polinomial configurado

para, para cada uno de los por lo menos dos polinomios monovariables: sustituir el número de identidad del segundo dispositivo de red en el polinomio monovariable, y reducir el resultado de la sustitución módulo el módulo público que corresponde al polinomio monovariable, y sumar entre sí los resultados de las reducciones módulo un módulo público y reducir módulo un módulo de clave, y

un dispositivo de derivación de claves configurado para derivar la clave compartida del resultado de la reducción módulo el módulo de clave.

16. Un sistema para configurar un dispositivo de red para compartir claves, caracterizado porque comprende:

un obtenedor de material de clave para obtener en forma electrónica por lo menos dos conjuntos de parámetros, un conjunto de parámetros comprende un módulo privado, un módulo público y un polinomio bivariable que tiene coeficientes enteros, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en por lo menos bits consecutivos de longitud de clave,

un generador para generar material de clave local para el dispositivo de red, el generador comprende

un administrador de dispositivos de red para obtener en forma electrónica un número de identidad para el dispositivo de red y para almacenar electrónicamente el material de clave local generado en el dispositivo de red,

un dispositivo de manipulación polinomial configurado para obtener, para cada conjunto de parámetros, un polinomio monovariable correspondiente, determinando un polinomio monovariable a partir del polinomio bivariable del conjunto de parámetros por sustitución del número de identidad en el polinomio bivariable y reduciendo el resultado de la sustitución módulo el módulo privado del conjunto de parámetros.

RESUMEN DE LA INVENCIÓN

Un método de configuración de un dispositivo de red para compartir claves, el método comprende obtener (410) en forma electrónica por lo menos dos conjuntos de parámetros, un conjunto de parámetros comprende un módulo privado (p_1), un módulo público (N), y un polinomio bivariable (f_1) que tiene coeficientes enteros, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en por lo menos bits consecutivos de longitud clave (b), generar material de clave local para el dispositivo de red que comprende obtener (420) en forma electrónica un número de identidad (A) para el dispositivo de red, y para cada conjunto de parámetros de los por lo menos dos conjuntos de parámetros obtener un polinomio monovariable correspondiente, determinando, mediante el uso de un dispositivo de manipulación polinomial, un polinomio monovariable a partir del polinomio bivariable del conjunto de parámetros sustituyendo (430) el número de identidad en el polinomio bivariable y reduciendo el resultado de la sustitución módulo el módulo privado del conjunto de parámetros, y almacenar electrónicamente (450) en el dispositivo de red el material de clave local generado, el material de clave local generado comprende el módulo público de cada conjunto de parámetros y el polinomio monovariable correspondiente de cada conjunto de parámetros.

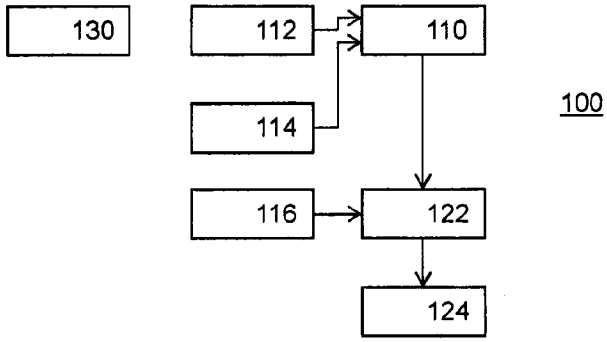

Figura 1a

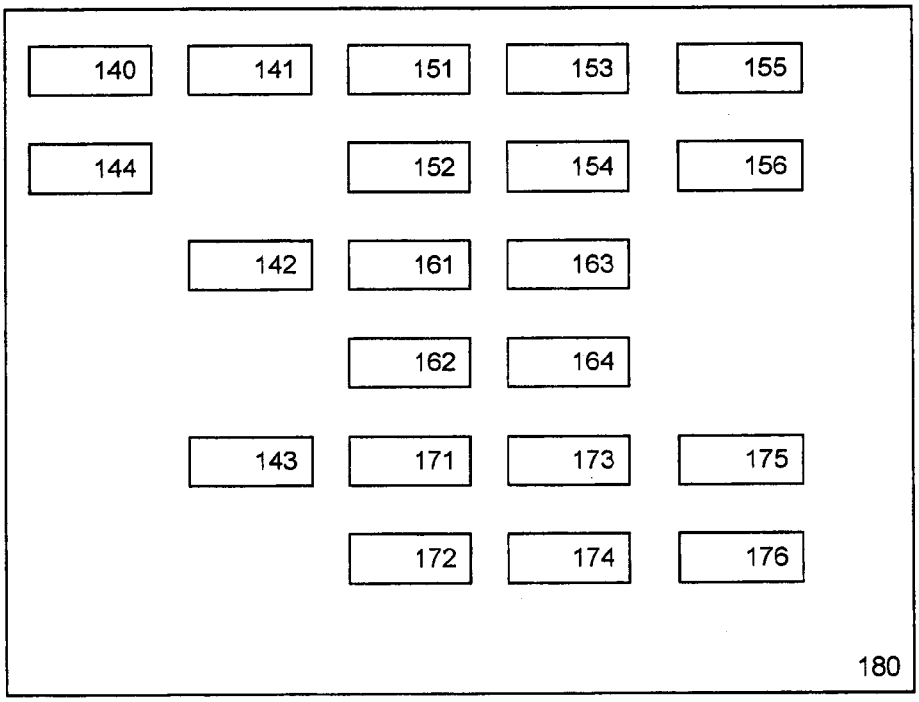

Figura 1b

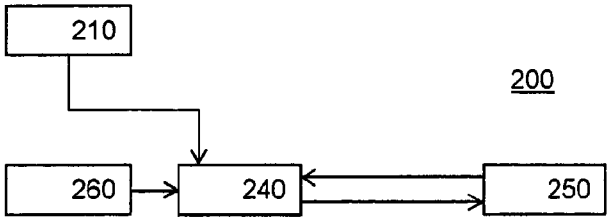

Figura 2a

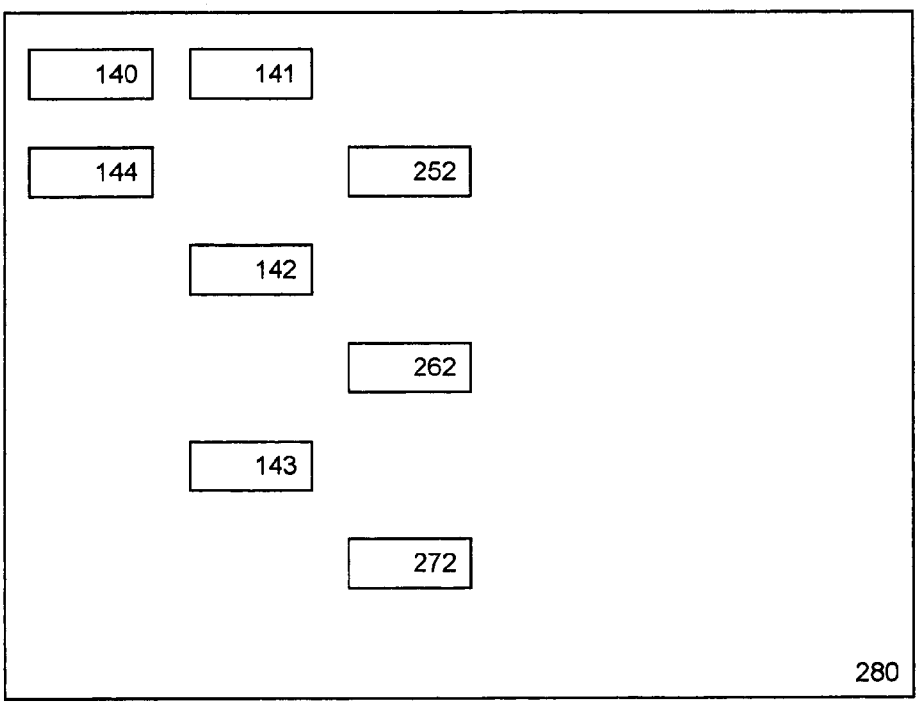

Figura 2b

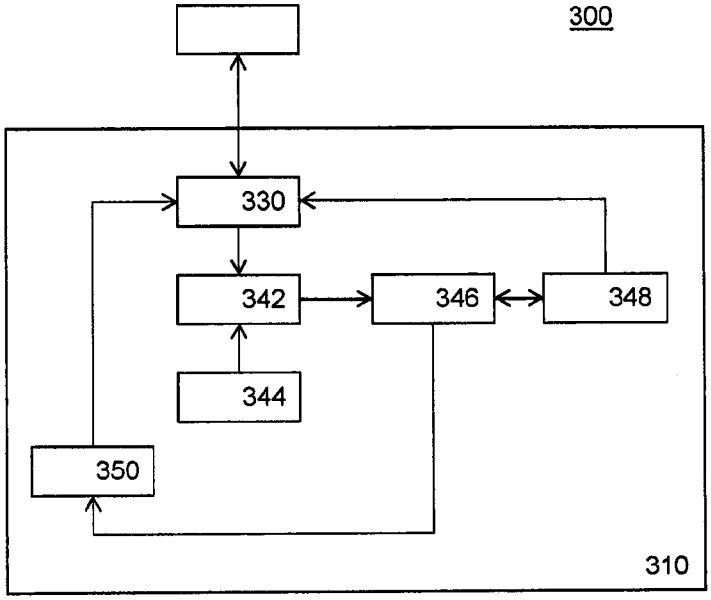

Figura 3

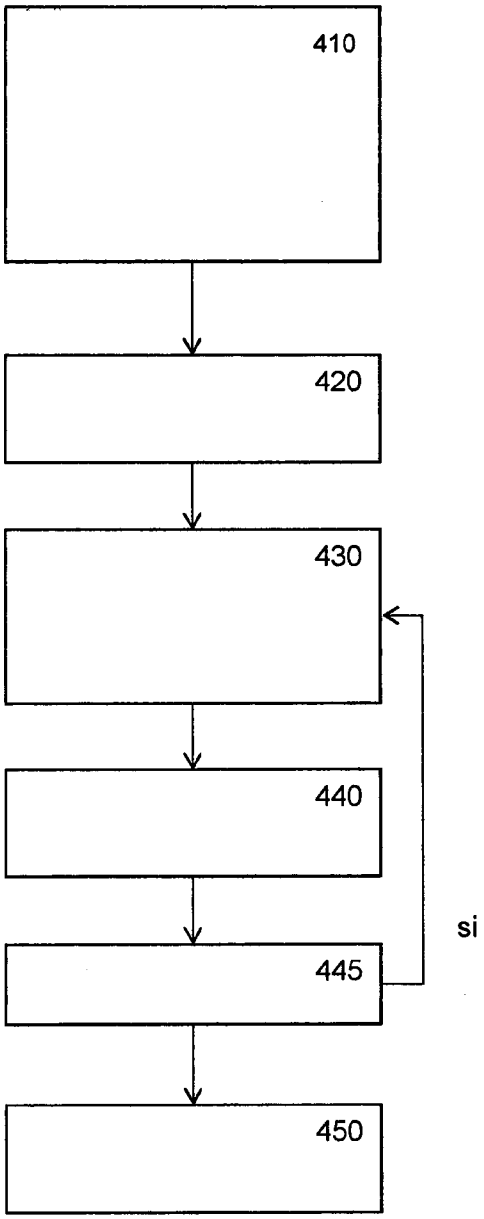

Figura 4

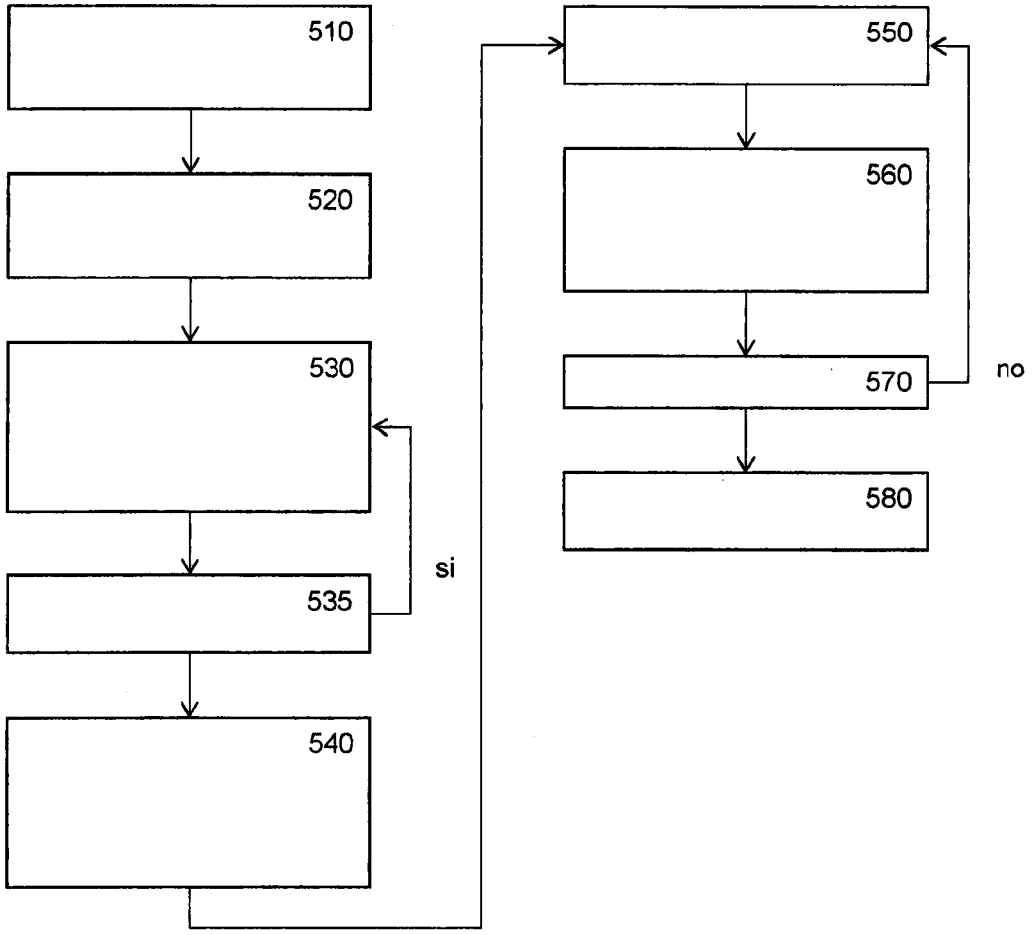

Figura 5

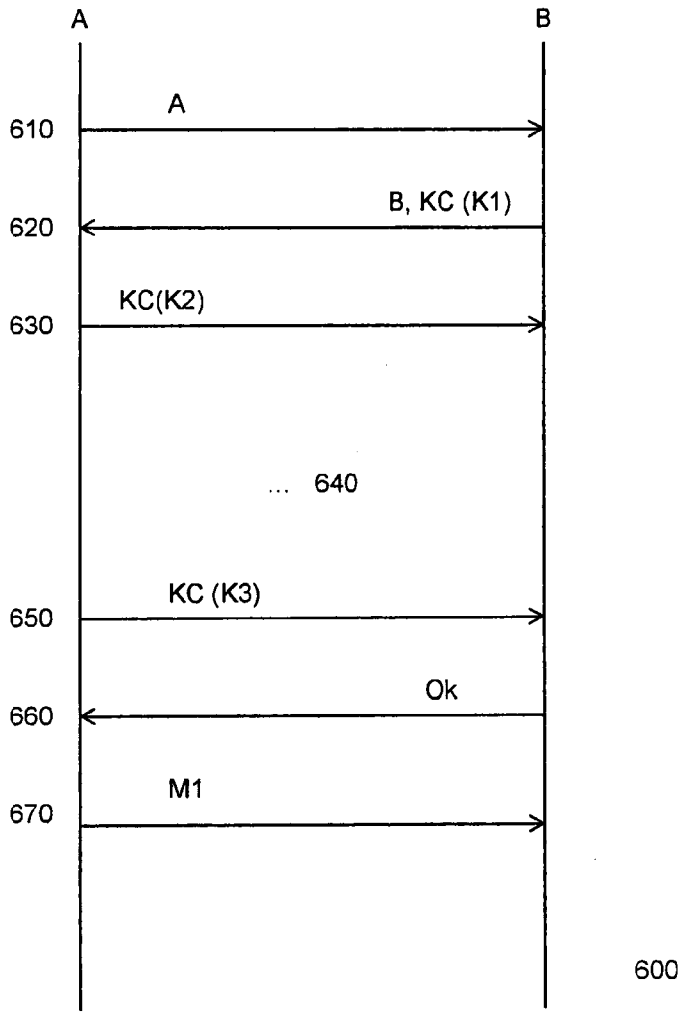

Figura 6