(11) **MX 2014012053 A**

(12) **SOLICITUD de PATENTE**

(43) Fecha de publicación: **12/01/2015**

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

(22) Fecha de presentación: **06/10/2014**
(21) Número de solicitud: **2014012053**

(86) Número de solicitud PCT: **EP 13/56730**
(87) Número de publicación PCT: **WO 2013/174554 (28/11/2013)**

(30) Prioridad(es): **21/05/2012 EP 12168710.7**
21/05/2012 US 61/649,464
12/06/2012 US 61/658,475

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

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

(74) Representante:
Eugenio PÉREZ PÉREZ
Hamburgo No. 260 CUAUHTEMOC Distrito Federal 06600 MX

(54) Título: **DISPOSITIVO PARA COMPARTIR CLAVE Y SISTEMAS PARA CONFIGURACION DEL MISMO.**

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

(57) Resumen

Se proporcionan un método para configurar un dispositivo de red para compartir clave y un método para un primer dispositivo de red para determinar una clave compartida. El método para configurar usos de módulo privado (pj), un módulo público (N), y un polinomio bivariado (fj) que tienen coeficientes de número entero, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas al menos en bits consecutivos de longitud de clave (b). Se genera material de clave local para un dispositivo de red al sustituir un número de identidad en el polinomio bivariado y al reducir por módulo el resultado del módulo privado de la sustitución para obtener un polinomio univariado. Puede aumentar seguridad al agregar (440) uno o más números de ofuscación a coeficientes del polinomio univariado para obtener un polinomio univariado ofuscado. En una fase de uso, el dispositivo de red determina una clave criptográfica compartida, al sustituir (530) el número de identidad de otro dispositivo de red dentro del polinomio univariado y al reducir por módulo el módulo público y al reducir por módulo un módulo de clave.

(57) Abstract

A method of configuring a network device for key sharing and a method for a first network device to determine a shared key are provided. The method of configuring uses a private modulus (p 1) a public modulus (N), and a bivariate polynomial (Æ# 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. Local key material for a network device is generated by substituting an identity number into the bivariate polynomial and reducing modulo the private modulus the result of the substitution to obtain a univariate polynomial. Security may be increased by adding (440) one or more obfuscating numbers to coefficients of the univariate polynomial to obtain an obfuscated univariate polynomial. In a use phase, the network device determines a shared cryptographic key, by substituting (530) the identity number of another network device into the univariate polynomial and reducing modulo the public modulus and reducing modulo a key modulus.

DISPOSITIVO PARA COMPARTIR CLAVE Y SISTEMAS PARA CONFIGURACION DEL MISMO

CAMPO DE LA INVENCION

La invención se refiere a un método para configurar un dispositivo de red para compartir clave, el método comprende 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, determinar utilizando un dispositivo de manipulación de polinomio de una forma de polinomio univariado de un polinomio bivariado, y almacenar electrónicamente el material de clave local generado en el dispositivo de red.

La invención además se refiere a un método para que un primer dispositivo de red determine una clave compartida, la clave es la clave criptográfica, el método comprende, obtener material de clave local de primer dispositivo de red en forma electrónica, el material de clave local comprende un polinomio univariado, 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 dentro del polinomio univariado y derivar la clave compartida del mismo.

La invención además se refiere a un sistema para configurar un dispositivo de red para compartir clave, y a un

dispositivo de red configurado para determinar una clave compartida.

ANTECEDENTES DE LA INVENCION

Dada una red de comunicaciones que comprende múltiples dispositivos de red, es un problema establecer conexiones seguras entre pares de tales dispositivos de red. Una forma de lograr esto se describe en C. Blundo, A. De Santis, A. Herzeberg, 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 (denominado como 'Blundo').

Asume una autoridad central, también indicada como la autoridad de red o como la Tercera Parte Confiada (TTP, por sus siglas en inglés) que genera un polinomio bivariado simétrico $f(x,y)$, con coeficientes en el campo finito F con p elementos, en donde p es un número primo o una energía de un número primo. Cada dispositivo tiene un número de identidad en F y se proporciona con material de clave local mediante la 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 el dispositivo η', utiliza su material clave para generar la clave $K(\eta,\eta) = f(\eta,\eta')$. Ya que f es simétrico, se genera la misma clave.

Un problema de este esquema para compartir clave ocurre si un atacante conoce el material de clave de t+1 o

más dispositivos, en donde t es el grado del polinomio bivariado. El atacante entonces puede reconstruir el polinomio f(x,y). En ese momento se rompe completamente la seguridad del sistema. Dados los números de identidad de cualquiera de los dispositivos, el atacante puede reconstruir la clave compartida entre éste par de dispositivos.

Se hace referencia al documento "A Permutation-Based Multi-Polynomial Schem for Pairwise Key Establishment in Sensor Networks" por autores Song Guo, Victor Leung, y Zhuzhong Qian, Conferencia Internacional de IEEE sobre comunicaciones, 2010. Presenta un esquema de polinomio múltiple con base en permutación para establecimiento o de clave en pares en redes de sensor inalámbricas. Diferente de Blundo, el esquema presentado en Song no da a cada nodo sólo una porción de un polinomio simétrico, sino un grupo de porciones permutadas.

SUMARIO DE LA INVENCION

Sería ventajoso tener un método mejorado para establecer una clave compartida entre dos dispositivos de red. Se proporcionan un método para configurar un dispositivo de red para compartir clave y un método para que un positivo de red determine una clave compartida.

El método para configurar un dispositivo de red para compartir clave comprende obtener en forma electrónica un módulo privado, un módulo público, y un polinomio

bivariado que tiene coeficientes de número entero, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en al menos bits consecutivos de longitud de 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, determinar utilizando un dispositivo de manipulación de polinomio de un polinomio univariado del polinomio bivariado al sustituir el número de identidad en el polinomio bivariado, reducir módulo del resultado del módulo privado de la sustitución, y almacenar electrónicamente el material de clave local generado en el dispositivo de red. En una modalidad, el material de clave local de generación para el dispositivo de red comprende generar un número de ofuscación, por ejemplo, al utilizar un generador de número al azar electrónico, y agregar utilizando un dispositivo de manipulación de polinomio, el número de ofuscación a un coeficiente del polinomio univariado para obtener un polinomio univariado ofuscado, el material de clave local generado comprende el polinomio univariado ofuscado. Puede ofuscarse más de un coeficiente, preferiblemente con diferentes coeficientes que son ofuscados de manera diferente. En una modalidad, el material de clave local de generación para el dispositivo de red comprende generar múltiples números de ofuscación, por ejemplo, al utilizar el

generador de número al azar electrónico, y agregar utilizando el dispositivo de manipulación de polinomio, cada número de ofuscación de los múltiples números de ofuscación a uno respectivo de los coeficientes del polinomio univariado para obtener un polinomio univariado ofuscado. En una modalidad se agrega a cada coeficiente del polinomio univariado un número ofuscado.

El polinomio bivariado puede o no ser simétrico. Si el polinomio o polinomios bivariados son simétricos cualquiera de dos dispositivos de red puede derivar una clave compartida. De manera interesante, utilizar un polinomio bivariado asimétrico o uno o más polinomios bivariados asimétricos entre múltiples polímeros bivariados, como material de clave de raíz, permite adaptar la creación de dos grupos de dispositivos tal como dispositivos; dos dispositivos que pertenecen al mismo grupo no pueden generar una clave común, pero dos dispositivos en diferentes grupos pueden hacerlo.

Agregar ofuscación es un paso adicional. Sin ofuscación aún se obtiene protección contra ataques, debido a que la derivación del material de clave local utiliza un módulo privado que es diferente del módulo público; se alteraría la relación matemática que estaría presente digamos, cuando se trabaja en un campo finito individual. Esto significa que las herramientas matemáticas usuales para

analizar polinomios, por ejemplo, álgebra finita, ya no aplican. Por otro lado debido a que el módulo privado y el público se traslapan en un número de bits consecutivos, dos dispositivos de red que tienen material de clave local es probable que sean capaces de derivar la misma clave compartida. La seguridad puede ser aumentada al agregar uno o más números de ofuscación a coeficientes del polinomio univariado para obtener un polinomio univariado ofuscado. El paso de agregar números de ofuscación sin embargo es opcional y puede ser omitido. Si se agrega o no ofuscación es un equilibrio entre la posibilidad de derivar correctamente una clave compartida, y seguridad adicional.

El módulo público es para uso en el dispositivo de red. El método para configurar un dispositivo de red para compartir claves puede comprender poner a disponibilidad el módulo público al dispositivo de red, por ejemplo, almacenar el módulo público junto con el material de clave local.

El método para determinar una clave compartida para un primer dispositivo de red la clave es una clave criptográfica que comprende obtener material de clave local para el primer dispositivo de red en forma electrónica, para el material de clave local que comprende un polinomio univariado, posiblemente ofuscado, 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 dentro del polinomio univariado ofuscado, reducir el resultado del módulo público del módulo de sustitución seguido por módulo de reducción de un módulo de clave, y derivar la clave compartida del resultado del módulo de reducción del módulo de clave. En una modalidad, por ejemplo, el método comprende reducir el resultado del módulo de sustitución del módulo público dividiendo el resultado por una energía de dos, y módulo de reducción de un módulo de clave.

Cualquier par de dos dispositivos de red de múltiples dispositivos de red cada uno que tiene un número idéntico y material de clave local generado para el número de entidad, son capaces de negociar una clave compartida con pocos recursos. Los dos dispositivos de red no necesitan intercambiar únicamente sus números de identidad, que no necesitan mantenerse en secreto, y realizar cálculos de polinomio. El tipo de cálculos necesarios no requiere grandes recursos computacionales, lo que significa que este método es adecuado para tipo de aplicaciones de alto volumen, a bajo costo.

Si se ha obtenido el material de clave local de un polinomio simétrico, esto permite que ambos dispositivos de red en un par de dispositivos de red obtengan la misma clave compartida. Si un número de ofuscación ha sido agregado al

material de clave local, se ha alterado la relación entre el material de clave local y el material de clave de raíz. La relación que estaría presente entre el polinomio univariado no ofuscado y el polinomio bivariado simétrico ya no está presente. Esto significa que el ataque directo en tal esquema ya no funciona.

Incluso si no se ha utilizado ninguna ofuscación, permanece una dificultad de ataque debido a que el módulo público y el módulo privado (o módulos) no son iguales. El módulo de reducción del módulo público aumenta la posibilidad de derivar la misma clave compartida, incluso sin ofuscación.

En una modalidad, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en al menos bits consecutivos de longitud de clave (b). Nota, pueden utilizarse múltiples módulos privados; pueden elegirse de manera que la representación binaria de cualquiera de los múltiples módulos privados del módulo público y la representación binaria del módulo privado sean las mismas en al menos bits consecutivos de longitud de clave (b). Para cada módulo privado de los múltiples módulos privados se elige un polinomio bivariado, opcionalmente simétrico, que tiene coeficientes de número entero para obtener múltiples polinomios bivariados, 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, digamos, en un campo finito individual se altera. Esto significa que las herramientas matemáticas usuales para analizar polinomios, por ejemplo, álgebra finita, ya no aplican. En el mejor de los casos un atacante puede utilizar estructuras mucho menos eficientes, tal como retículos. También cuando se derivan la clave compartida se combinan dos operaciones de módulo que no son compatibles en el sentido matemático usual; así se evita estructura matemática en dos lugares. El método permite generación de clave en pares directa y es resistente a la captura de un número muy alto, por ejemplo, en el orden de 10^5 o incluso superior, de dispositivos de red. Por otro lado debido a que el módulo privado y el público se traslapan en un número de bits consecutivos, dos dispositivos de red que tienen material de clave local es probable que sean capaces de derivar la misma clave compartida.

Una idea particular del inventor fue que el módulo público no necesita ser un número primo. En una modalidad, el módulo público es compuesto. También no existe ninguna razón por la cual el módulo público deba ser un número de bits 'de todos', por ejemplo, un número que únicamente consiste de 1 bit, en su representación binaria. En una modalidad, el módulo público no es una energía de dos menos 1. En una

modalidad, la representación binaria del módulo público comprende al menos un bit cero (sin contar cero líder, es decir, la representación binaria del módulo público comprende al menos un bit cero menos significativo que el bits más significativo del módulo público). En una modalidad, el módulo público es una energía de dos menos 1 y compuesto.

En una modalidad el módulo público es más grande que el uno o más módulos privados.

En una modalidad, al menos bits consecutivos de longitud de clave de la representación binaria del módulo público menos el módulo privado son todos bits cero. La diferencia debe ser evaluada utilizando la representación del número firmada del módulo público menos el módulo privado, no la representación de dos complementos. Alternativamente, uno puede requerir que al menos bits consecutivos de longitud de clave de la representación binaria de valor absoluto del módulo público menos el módulo privado sean todos bits cero. Existe un grupo de posiciones consecutivas de longitud de clave (b) en las cuales la representación binaria del módulo público está de acuerdo con la representación binaria de los módulos privados.

Las posiciones de bit consecutivas en las cuales el módulo público está de acuerdo 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 que no es necesario una división por una energía de dos cuando se deriva la clave compartida.

Se permiten un módulo privado de múltiples módulos privados que es igual al módulo público; sin embargo si únicamente se utiliza un módulo privado entonces esto no es deseable.

Es deseable que los módulos privados introduzcan suficiente falta de linealidad. En una modalidad, existe un grupo de posiciones de bit consecutivo en las cuales el módulo público difiere con cada módulo privado. Además, también se puede imponer que los módulos privados difieran entre ellos mismos; una comparación en pares de la representación binaria del módulo privado también puede diferir al menos en un bit en un grupo de, digamos al menos bits consecutivos de longitud de clave, el grupo es igual para todo el módulo privado, y posiblemente también el mismo para el módulo público.

El dispositivo de red puede ser un dispositivo electrónico equipado con comunicación electrónica y medios de computación. El dispositivo de red puede estar fijado, por ejemplo, en la forma de una etiqueta RFID, a cualquier objeto no electrónico. Por ejemplo, este método sería adecuado para el 'internet de cosas'. Por ejemplo, objetos, en particular

objetos de bajo costo, pueden ser equipados con radio etiquetas a través de las cuales pueden comunicarse, por ejemplo, pueden identificarse. Tales objetos pueden ser inventariados a través de medios electrónicos tal como una computadora. Artículos robados o rotos serían rastreados y localizados fácilmente. Una aplicación particularmente prometedora es una lámpara que comprende un dispositivo de red configurado para determinar una clave compartida. Tal lámpara puede comunicar de manera segura su estado; tal lámpara podría ser controlada de manera segura, por ejemplo, encendida y/o apagada. Un dispositivo de red puede ser uno de múltiples dispositivos de red, cada uno que comprende un comunicador electrónico para enviar y recibir un número de identidad y para enviar un mensaje de estado electrónico, y cada uno que comprende un circuito integrado configurado para derivar una clave compartida siguiendo un método de conformidad con la invención.

En una modalidad, el método en la invención puede utilizarse como un método criptográfico para protocolos de seguridad tal 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 que desea comunicarse con el primer dispositivo puede generar una clave en pares común con el primer dispositivo dado su identificador, y la clave en pares (o una clave derivada de

ésta por medio de, por ejemplo, una función de derivación de clave) puede utilizarse en un método de los protocolos anteriores con base en clave pre-compartida. En particular, el identificador de un dispositivo como se definió en esta invención puede ser una dirección de red tal como la dirección corta de ZigBee, una dirección IP, o el identificador de anfitrión. El identificador también puede ser la dirección de IEEE de un dispositivo o una secuencia de bits de propiedad asociada con el dispositivo para que un dispositivo reciba algún material de clave local asociado con la dirección de IEEE durante fabricación.

Derivar una clave compartida puede utilizarse para muchas aplicaciones. Típicamente, la clave compartida será una clave simétrica criptográfica. La clave simétrica puede ser utilizada para confidencialidad, por ejemplo, mensajes salientes o entrantes pueden ser codificados criptográficamente con la clave simétrica. Unicamente un dispositivo con acceso a ambos números de identidad y uno de los dos materiales de clave local (o acceso al material de clave de raíz) será capaz de decodificar criptográficamente las comunicaciones. La clave simétrica puede utilizarse para autentificación, por ejemplo, mensaje saliente o entrante puede ser autentificado con la clave simétrica. De esta forma puede validarse el origen del mensaje. Unicamente un dispositivo con acceso a ambos números de identidad y uno de

los dos materiales de clave local (o acceso al material de clave de raíz) será capaz de crear mensajes autentificados.

El método para configurar un dispositivo de red para compartir clave típicamente se ejecutará por una autoridad de red, por ejemplo, una tercera parte confiada. La autoridad de red puede obtener el material necesario, por ejemplo, material de clave de raíz desde otra fuente, pero también puede generar éste 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 recibido.

En una modalidad, el módulo público N es elegido para que satisfaga $2^{(a+2)b-1} \leq N \leq 2^{(a+2)b}-1$, en donde, a representa el grado del polinomio bivariado y b representa la longitud de clave. Por ejemplo, en una modalidad $N = 2^{(a+2)b}-1$. La operación de módulo para la última elección puede implementarse particularmente de manera eficiente.

Tener un módulo público fijo tiene la ventaja que no necesita comunicarse a los dispositivos de red, pero puede integrarse, por ejemplo, con su software de sistema. En particular, el módulo público puede ser elegido utilizando un generador de número al azar.

El módulo público y privado puede ser representado como una secuencia de bits. También pueden ser abreviados utilizando cada estructura matemática particular. Por

ejemplo, en lugar de almacenar un módulo privado, uno también puede almacenar su diferencia con el módulo público, que es mucho más corto.

Tener un módulo privado elegido de tal forma que un número de 'longitud de clave' de los bits menos significativos de la representación binaria del módulo público menos el módulo privado sean todos bits cero, aumenta la posibilidad que una clave compartida en un primer dispositivo de red de un par de dispositivo de red esté cerca de la clave compartida 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 módulo privado al restar un múltiplo de 2^64 del módulo público. En una modalidad, el módulo público menos un módulo privado dividido por dos a la energía de la longitud de clave es menor que dos para la energía 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 elige un polinomio bivariado simétrico que tiene coeficientes de número entero para obtener múltiples polinomios bivariados simétricos, para que a cada módulo privado le corresponda un

polinomio bivariado simétrico. Determinar el polinomio univariado comprende sustituir el número de identidad en cada uno de los múltiples polinomios bivariados simétricos, reducir por módulo un módulo privado de los múltiples módulos privados correspondientes a un polinomio bivariado simétrico, y agregar los múltiples resultados de las múltiples reducciones conjuntamente. Tener múltiples polinomios bivariados simétricos para diferentes módulos aumenta la seguridad debido a que se mezclan adicionalmente estructuras incompatibles. Típicamente los módulos privados son distintos. Tener múltiples módulos privados complica adicionalmente análisis incluso más si las estructuras algebraicas correspondientes son muy diferentes; por ejemplo, eligiéndolas relativamente primas, en particular relativamente primas en pares, incluso más en particular al elegirlas como primos distintos.

Tener un módulo privado diferente, y en particular múltiples módulos privados, complicará el análisis. Para aumentar adicionalmente la seguridad son posibles controles adicionales en los coeficientes. En una modalidad, la autoridad que agrega los múltiples polinomios univariados resultantes de las múltiples reducciones verifica conjuntamente si el valor de cada uno de los coeficiente resultantes es muy pequeño o muy grande, por ejemplo, menor que un umbral mínimo o por encima de un umbral máximo. Esto

mejorar seguridad incluso adicionalmente debido a que en cualquiera de los dos casos, un atacante puede averiguar los componentes de las múltiples reducciones si son demasiado grandes o demasiado pequeños. Por ejemplo, si el valor de un coeficiente que resulta de la adición es igual a uno y solo existen dos polinomio univariados, entonces un atacante sabe que el coeficiente correspondiente asociado con el primer polinomio es 1 o el asociado con el segundo polinomio es 0, o de otra forma. 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 de clave local es al menos 'valor mínimo' y máximo 'valor máximo'. Esta revisión puede omitirse, en particular, si 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 bits de longitud de clave (*b*) menos significativos de la representación binaria del módulo público menos el módulo privado específico son todos bits cero.

El módulo público puede ser tanto más grande como

más pequeño que el módulo privado. En una modalidad la representación binaria del módulo público menos el módulo privado tiene al menos bits de longitud de clave todos cero. Los bits cero de al menos bits cero de longitud de clave son consecutivos y pueden estar presentes en cualquier punto en la representación binaria. Tener una secuencia de bits cero en la diferencia entre el módulo público y el módulo privado evita que la ofuscación se lleve demasiado lejos. En una modalidad, existe un parámetro de número entero 's', de manera que bits menos significativos de longitud de clave del módulo público menos el módulo privado, divididos por dos a la energía s se han todos cero. El parámetro 's' es el mismo para todos los módulos privados.

Por ejemplo, uno puede definir un divisor de secuencia de bits cero que es una energía de dos, de manera que cada módulo privado específico sea tal que los bits de longitud de clave (*b*) de la representación binaria del módulo público menos el módulo privado específico dividido por el divisor de secuencia de bits cero sean todos bits cero. Si los bits menos significativos son cero, el divisor de secuencia de bits cero puede ser tomado para ser 1. En una modalidad el divisor de secuencia de bits cero es mayor que 1. La división por una energía de dos se va a interpretar como una división de número entero, dando el mismo resultado que un desplazamiento de los bits en la dirección de los bits

menos significativos. Se ignora cualquier resto de la división.

Para generar la clave compartida de bit de longitud de clave, los dispositivos de red primero aplican un paso de división adicional. El primer dispositivo de red evalúa el material de clave para el número de identidad del segundo módulo de dispositivo de los módulos públicos, dividiendo por 2^s y reduciendo el módulo dos a la energía de la longitud de clave. Obsérvese que esto es equivalente aplicar primero un módulo 2^(s+longitud de clave) después del módulo público, y entonces al dividir por 2^s. Aquí "dividir" incluye redondeo hacia abajo.

En una modalidad, el módulo privado es generado utilizando un generador de número al azar. En una modalidad, se generan múltiples módulos privados de manera que sean relativamente primos en pares. Por ejemplo, los múltiples módulos privados pueden generarse de manera interactiva verificando para cada nuevo módulo privado que aún son relativamente primos en pares, y si no desechar el último módulo privado generado. Una modalidad comprende generar de manera iterativa un módulo candidato como utilizando el generador de número al azar, de manera que bits consecutivos de longitud de clave (*b*) de la representación binaria del módulo público menos el módulo candidato sean todos bits cero, por ejemplo, los bits de longitud de clave menos

significativos, hasta que el módulo candidato satisface una prueba del número primo utilizando un dispositivo de prueba de número primo, en donde el módulo candidato así obtenido que satisface la prueba de número primo se utiliza como el módulo privado. La prueba de número primo puede, por ejemplo, ser la prueba de número primo de Miller-Rabin, o la prueba de número primo de Solovay-Strassen.

Un polinomio bivariado simétrico en variables de x y y de grado a, tiene únicamente monomios de la forma x^iy^j, con $i \leq a, j \leq a$. Además el coeficiente correspondiente a x^iy^j es el mismo que el coeficiente de x^jy^i. Esto puede utilizarse para reducir el número de coeficientes almacenados por aproximadamente la mitad. Obsérvese que se utiliza una definición más relajada del grado. Definimos el grado de un monomio, como el grado máximo de las variables en el monomio. Así el grado de x^jy^i es max(i,j), es decir, que $i \leq a, j \leq a$. Así que por ejemplo lo que llamamos un polinomio de grado 1 tiene una forma general a + bx + cy + dxy, (obsérvese que ya que se consideran únicamente polinomios simétricos, tenemos que b=c). Obsérvese que si se desea uno se pueden colocar restricciones adicionales sobre el polinomio bivariado, incluyendo, por ejemplo, que se utilizan únicamente monomios con $i + j \leq a$, pero esto no es necesario.

En una modalidad, se genera el polinomio bivariado simétrico por la autoridad de red. Por ejemplo, el polinomio

bivariado simétrico puede ser un polinomio bivariado simétrico al azar. Por ejemplo, los coeficientes pueden seleccionarse como números al azar utilizando un generador de número al azar.

Aunque la ofuscación utilizada aumenta ampliamente la resistencia contra ataque, en particular contra ataques de colusión en donde se combinan múltiples materiales de clave local, tiene una desventaja potencial. Algunas veces la clave compartida derivada por el primer dispositivo de red no es en todos los bits idéntica a la clave compartida derivada por segundo dispositivo de red. Esto es principalmente debido a la falta de coincidencia en los bits de transporte después de la adición de los coeficientes de ofuscación. Otra razón es el efecto faltante de los efectos modulares de cada uno de los módulos privados durante la generación de la clave que afecta los bits generados de transporte. Aunque es una molestia puede resolverse esta desventaja en varias formas. Al elegir la ofuscación con más cuidado puede reducirse significativamente la posibilidad de una diferencia y en particular la posibilidad de una gran diferencia. Además, se encontró que diferencias, si existen, es probable que estén localizadas en los bits menos significativos de las claves generadas. Así que al remover uno o más de los bits menos significativos puede aumentar la posibilidad de una clave compartida idéntica. Por ejemplo, en una modalidad del método

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

Obsérvese que sin ofuscación también puede suceder que la clave compartida derivada por el primer dispositivo de red no sea en todos los bits idéntica a la clave compartida derivada por el segundo dispositivo de red, aunque la posibilidad de esto es menor que el caso con ofuscación.

En una modalidad, se remueve un número de los bits menos significativos de la clave compartida; 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 posibilidad de tener claves que no sean iguales; en particular puede reducirse a

cualquier umbral deseado. Puede calcularse la posibilidad de claves compartidas que son iguales, al seguir las relaciones matemáticas, también se puede determinar por experimento.

También la elección de números de ofuscación puede controlarse, en una modalidad, el rango del cual se elige un número de ofuscación se reduce para coeficientes correspondientes a monomios de grado superior. En particular, uno puede requerir que $|\epsilon_{A,i}| < 2^{(a+1-i)b}$, en donde $\epsilon_{A,i}$ denote número de ofuscación para el monomio i-ésimo, i denote el grado del monomio correspondiente al coeficiente, a representa el grado del polinomio bivariado y b representa la longitud de clave. A representa el dispositivo de red para el cual se generó el material de clave local. En una modalidad, se genera un número de ofuscación para cada coeficiente, por ejemplo, utilizando la fórmula anterior. Puede aplicarse diferente ofuscación para diferentes dispositivos de red. Por ejemplo, incluso si existen tres o más dispositivos de red, que para cada dispositivo de red, pueden generarse diferentes números de ofuscación.

Obsérvese que el número de ofuscación puede estar restringido a números positivos pero esto no es necesario, los números de ofuscación pueden ser negativos. En una modalidad, se generan los números ofuscados utilizando un generador de número al azar. Pueden generarse múltiples números de ofuscación y agregarse coeficiente del polinomio

univariado para obtener el polinomio univariado ofuscado. Uno o más, preferiblemente incluso todos los coeficientes del polinomio univariado pueden ser ofuscados de esta forma.

El número de bits en el número de identidad para el dispositivo de red se elige usualmente como menor o igual que la longitud de clave. El número de identidad puede ser una secuencia de bits, digamos una secuencia de bits de 32 ó 64, o más larga. La longitud de clave puede ser 32 o más, 48 o más, 64 o más, 96 o más, 128 o más, 256 o más. La longitud de clave puede ser elegida de algún número de bits superior con el fin 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 clave. En este caso, el efecto de operaciones modulares puede llevar a un efecto superior sobre los bits menos significativos de los bits de longitud de clave de la clave generada de manera que esos bits pueden no ser iguales para un par de dispositivos que desean generar una clave común. Tener una longitud mayor para el identificador, sin embargo, puede tener un efecto positivo en la seguridad ya que se mezclan más bits conjuntamente cuando se hacen los cálculos correspondientes.

Puede implementarse un dispositivo de manipulación de polinomio en software que se ejecuta en una computadora, digamos en un circuito integrado. Un dispositivo de

manipulación de polinomio puede ser implementado muy eficientemente en hardware. También es posible una combinación. Por ejemplo, puede implementarse un dispositivo de manipulación de polinomio al manipular disposiciones de coeficientes que representan los polinomios.

Almacenar electrónicamente el material de clave local generado en el dispositivo de red puede implementarse al enviar electrónicamente el material de clave local generado al dispositivo de red, por ejemplo, utilizando una conexión por cable, o utilizando una conexión inalámbrica y teniendo el materia de clave local generado almacenado en el dispositivo de red. Esto puede hacerse durante fabricación o instalación, por ejemplo, durante prueba, de un circuito integrado en el dispositivo de red. El equipo de prueba puede comprender o ser conectado a la autoridad de red. Esto puede suceder después de una unión exitosa de un dispositivo a una red de operación (por ejemplo, después de acceso a red o arranque). En particular, el material de clave local puede ser distribuido como parte de parámetros de red operativos.

Obtener material de clave local para el primer dispositivo de red en forma electrónica puede hacerse al recibir electrónicamente el material de clave local de un sistema para configurar un dispositivo de red para compartir clave, por ejemplo, un dispositivo de autoridad de red. Obtener material de clave local también puede hacerse al

recuperar el material de clave local de un almacenamiento local, por ejemplo, una memoria tal como memoria flash.

Obtener un número de identidad para un segundo dispositivo de red, puede hacerse al recibir el número de identidad del segundo dispositivo de red, por ejemplo, directamente del segundo dispositivo de red, por ejemplo, al recibir inalámbricamente desde el segundo dispositivo de red.

El módulo público y el módulo de clave pueden almacenarse en un dispositivo de red. También pueden recibirse desde una autoridad de red. También pueden estar implícitos en software del dispositivo de red. Por ejemplo, en una modalidad el módulo de clave es una energía de dos. Puede hacerse módulo de reducción tal como un módulo de clave al descartar todo los bits excepto bits menos significativos de longitud de clave. Primero se redujo por módulo el resultado de la sustitución del módulo público que entonces redujo por módulo adicionalmente el módulo de clave.

Aunque no se requiere, el módulo público y el módulo de clave pueden ser relativamente primos. Esto puede lograrse al tener la posibilidad de módulo público y el módulo de clave una energía de 2. En cualquier caso, se evita que el módulo de clave divida el módulo público, ya que entonces podría omitirse el módulo de reducción del módulo público.

El método para acuerdo de clave entre dos

dispositivos puede utilizar como material de clave de raíz un número de polinomios bivariados. Uno puede utilizar el método para acuerdo x entre x partes al utilizar polinomios x-variados como material de clave de raíz. En este grado, la tercera parte confiada evalúa los polinomios x-variados en una variable en el anillo correspondiente, los polinomios variados x-1 resultantes entonces se agregan sobre los números enteros generando el material de clave local almacenado en un dispositivo. Cuando x dispositivos necesitan estar de acuerdo en una clave, el dispositivo evalúa su material de clave local en identificadores de los otros dispositivos x-1. Por ejemplo, uno puede utilizar polinomios multivariados en un método para configurar un dispositivo de red para compartir clave, el método comprende obtener en forma electrónica un módulo privado (p_1), un módulo público (N), y un polinomio multivariado (f_1) que tiene coeficientes de número entero, la representación binaria y el módulo público y la representación binaria del módulo privado son iguales en al menos bits consecutivos de longitud de clave (b), generar material de clave local para el dispositivo de red que comprende obtener en forma electrónica un número de identidad (A) para el dispositivo de red, determinar utilizando un dispositivo de manipulación de polinomio del polinomio multivariado al sustituir el número de identidad dentro del polinomio multivariado, reducir por módulo el

módulo privado que resulta en la sustitución, y almacenar electrónicamente el material de clave local generado en el dispositivo de red. El polinomio obtenido por el dispositivo de manipulación de polinomio está por encima de una variable menor. Es conveniente para compartir clave sí el multivariado es simétrico en todas las variables. Un método correspondiente para que un primer dispositivo de red determine una clave compartida, la clave es una clave criptográfica, el método comprende, obtener material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende un polinomio opcionalmente ofuscado, obtener un número de identidad para múltiples dispositivos de red diferentes, el segundo dispositivo de red es diferente del primer dispositivo de red, sustituir el número de los otros dispositivos de red dentro del polinomio opcionalmente ofuscado, reducir el resultado del módulo de sustitución del módulo público y reducir por módulo un módulo de clave, y derivar la clave compartida del resultado del módulo de reducción del módulo de clave. Obsérvese que después de sustituir todos excepto uno de los otros números de identidad, el método se reduce a una situación en la cual se utiliza un polinomio univariado.

En una modalidad, un primer dispositivo de red recibe múltiples (n) materiales de clave local asociados con el identificador del dispositivo. La clave generada entre

este primer dispositivo y un segundo dispositivo se obtiene como la combinación (por ejemplo, concatenación) de las múltiples (n) claves obtenidas al evaluar cada uno de los múltiples (n) materiales de clave local del primer dispositivo en el identificador del segundo dispositivo. Esto permite uso del método en paralelo.

El uso de polinomios bivariados asimétricos como material de clave de raíz, es decir, f(x,y) !=f(y,x), permite adaptar la creación de dos grupos de dispositivos de manera que dispositivos en el primer grupo reciban KM(ld,y) y dispositivos en el segundo grupo reciban 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 estos dispositivos en diferentes grupos pueden hacerlo. Ver adicionalmente Blundo.

El número de identidad del dispositivo de red puede ser calculado como la función unidireccional de una secuencia de bits que contiene información asociada con el dispositivo. La función unidireccional puede ser una función hash criptográfica tal como SHA2 o SHA3. La salida de la función unidireccional puede ser truncada de manera que se ajusta el tamaño del identificador. Alternativamente, el tamaño de la función unidireccional es menor que el tamaño del identificador máximo.

En una modalidad, los polinomios simétricos

involucran un monomio individual de la forma $(ax^iy^i)_{pj}$ en donde $<>_p$ representa la operación del módulo. 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 existen múltiples módulos privados, puede ser más grande que el módulo privado y algunos pueden ser más pequeños.

En una modalidad del método para configurar un dispositivo de red para compartir clave, el método comprende obtener de forma electrónica múltiples módulos privados (p_i), y múltiples polinomios bivariados simétricos (f_i) que tienen coeficientes de número entero, de manera que exista un grupo de posiciones consecutivas de longitud de clave (b) en el cual la representación binaria del módulo público es la misma que la representación binaria de todos los módulos privados, generar material de clave local para el dispositivo de red que comprende obtener en forma electrónica un número de identidad (A) por el dispositivo de red, determinar utilizando un dispositivo de manipulación de polinomio un polinomio univariado de los múltiples polinomios bivariados al sustituir el número de identidad en cada uno de los múltiples polinomios bivariados, reducir por módulo un módulo privado de los múltiples módulos privados correspondientes a un polinomio bivariado simétrico, y agregar los múltiples resultados de las múltiples reducciones, y generar un número

de ofuscación y agregar utilizando un dispositivo de manipulación de polinomio, el número de ofuscación a un coeficiente del polinomio univariado para obtener un polinomio univariado ofuscado, el material de clave local generado comprende el polinomio univariado ofuscado, y almacenar electrónicamente el material de clave local generado en el dispositivo de red. Un polinomio bivariado de los múltiples polinomios bivariados (f_i) puede ser representado como teniendo coeficientes que modulan el módulo privado correspondiente (p_i).

Más generalmente, el material de clave de raíz, puede ser evaluado sobre cualquier anillo. Es posible utilizar polinomios de un monomio individual tal como Ax^a, en cuyo caso puede utilizarse un grupo.

Un aspecto de la invención se refiere a un sistema para configurar un dispositivo de red para compartir clave, por ejemplo, una autoridad de red, el sistema comprende un obtentor de material de clave para obtener en forma electrónica un módulo privado, un módulo público, que puede o no ser más grande que el módulo privado, y un polinomio bivariado simétrico que tiene coeficientes de número entero, bits de longitud de clave de la representación binaria del módulo público menos el módulo privado son todos bits cero, posiblemente los bits menos significativos de longitud de clave, un generador para generar material de clave local para

el dispositivo de red que comprende un administrador de dispositivo 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, y un dispositivo de manipulación de polinomio para determinar un polinomio univariado del polinomio bivariado al sustituir el número de identidad en el polinomio bivariado, modular por reducción el resultado de la sustitución del módulo privado.

Una modalidad del sistema comprende un generador de número de ofuscación, por ejemplo, un generador de número al azar, para generar un número de ofuscación, el dispositivo de manipulación de polinomio está configurado para agregar el número de ofuscación a un coeficiente del polinomio univariado para obtener un polinomio univariado ofuscado, el material de clave local generado comprende polinomio univariado ofuscado.

Un aspecto de la invención se refiere a un primer dispositivo de red configurado para determinar una clave compartida, la clave es una clave criptográfica, el primer dispositivo de red comprende, un obtentor de material de clave local para obtener material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende un polinomio univariado ofuscado, 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 de polinomio para sustituir el número de identidad del segundo dispositivo de red dentro del polinomio univariado ofuscado y reducir el resultado del módulo de sustitución del módulo público seguido por reducir por módulo un módulo de clave, el módulo público y de clave son relativamente primos, un dispositivo de derivación de clave para derivar la clave compartida del resultado del módulo de reducción del módulo de clave.

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

Derivar la clave compartida del resultado del módulo de reducción del módulo de clave, puede incluir la aplicación de una función de derivación de clave, por ejemplo la función KDF, definida en la Especificación de 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 agregar, restar, o concatenar un número entero (antes de aplicar la función de derivación de clave).

Cada una de múltiples dispositivos de red que tienen un número de identidad y material de clave local correspondiente juntos pueden formar red de comunicación configurada para asegurar, por ejemplo, comunicación confidencial y/o autentificada, entre pares de dispositivos de red.

La generación de clave se basa en ID y permite la generación de claves entre pares de dispositivos. Un primer dispositivo A puede confiar en un algoritmo que deriva una clave del material de clave local y un número de identidad.

En una modalidad, un primer dispositivo de red envía un mensaje de confirmación de clave al segundo dispositivo de red. Por ejemplo, un mensaje de confirmación puede comprender la codificación criptográfica de un mensaje, y opcionalmente el mismo mensaje. El segundo dispositivo de red puede verificar la codificación criptográfica del mensaje. El mensaje puede ser fijo y estar presente del segundo dispositivo, para evitar la necesidad de enviarlo. El mensaje puede ser al azar, o un código generado al azar, etc., en cuyo caso puede enviarse junto con la codificación criptográfica. El segundo dispositivo puede responder con un mensaje que contiene una indicación si las claves están de acuerdo. El segundo dispositivo también puede responder con un mensaje de confirmación de clave propio. Si el primer y segundo dispositivos encuentran que las claves no son iguales

pueden iniciar un proceso de igualación de clave, por ejemplo, al eliminar 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 por computadora, o en hardware dedicado, o en una combinación de ambos. Código ejecutable para un método de conformidad con la invención puede almacenarse en un producto de programa de computadora. Ejemplos de productos de programa de computadora incluyen dispositivos de memoria, dispositivos de almacenamiento óptico, circuitos integrados, servidores, software en línea, etc. Preferiblemente, el producto de programa de computadora comprende medios de código de programa no transitorios almacenados en un medio legible por computadora para realizar un método de conformidad con la invención cuando se ejecuta el producto de programa en una computadora.

En una modalidad preferida, el programa de computadora comprende medios de código de programa de computadora adaptados para realizar todos los pasos de un método de conformidad con la invención cuando se ejecuta el programa de computadora en una computadora. Preferiblemente, el programa de computadora está representado en un medio legible por computadora.

Para integridad, la solicitud internacional WO2010032161 con título "A method for secure communication in a network, a communication device, a network and a computer program therefor", se menciona, y se refiere a un método para asegurar comunicaciones en redes de comunicación.

Existe número de diferencias con esa aplicación, incluyendo: el uso de operaciones modulares, en particular combinar operaciones modulares con un módulo público y privado diferente, operaciones modulares repetidas, por ejemplo un módulo de reducción de un módulo público seguido por un módulo de reducción de módulo de clave, el uso de ofuscación, el uso de polinomios enteros.

Se proporciona un método para configurar un dispositivo de red para compartir clave y un método para que un primer dispositivo de red determine una clave compartida. El método para configuración utiliza un módulo privado (p_1), un módulo público (N), y un polinomio bivariado (f_1) que tiene coeficientes de número entero, la representación binaria del módulo público y la representación binaria del modelo privado son iguales en al menos bits consecutivos de longitud de clave (b). El material de clave local para un dispositivo de red se genera al sustituir un número de identidad en el polinomio bivariado y al reducir por módulo el resultado del módulo privado de la sustitución para obtener un polinomio univariado. Puede aumentar la seguridad

al agregar (440) uno o más números ofuscación a coeficientes del polinomio univariado para obtener un polinomio univariado ofuscado. En una fase de uso, el dispositivo de red determina una clave criptográfica compartida, al sustituir (530) el número de identidad de otro dispositivo de red dentro del polinomio univariado y al reducir por módulo el módulo público y al reducir por módulo un módulo de clave.

BREVE DESCRIPCION DE LAS FIGURAS

Estos y otros aspectos de la invención son evidentes a partir de y se aclararán con referencia a las modalidades descritas aquí en lo sucesivo. En las figuras,

la Figura 1 es un diagrama de bloque esquemático que ilustra un generador de material de clave de raíz,

la Figura 2 es un diagrama de bloque esquemático que ilustra un generador de material de clave local,

la Figura 3 es un diagrama de bloque esquemático que ilustra una red de comunicación,

la Figura 4 es un cuadro de flujo esquemático que ilustra generar material de clave local,

la Figura 5 es un cuadro de flujo esquemático que ilustra generar una clave compartida,

la Figura 6 es un diagrama de secuencia esquemático que ilustra generar una clave compartida.

Obsérvese artículos 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 se ha explicado la función y/o estructurales de tal artículo, no hay necesidad de explicación repetida de la misma en la descripción detallada.

LISTA DE NUMEROS DE REFERENCIA:

100 un obtentor de material de clave de raíz

110 un elemento de módulo público

112 un elemento de grado de polinomio

114 un elemento de longitud de clave

116 un módulo de elemento de polinomios

122 un administrador de módulo privado

124 un administrador de polinomio bivariado simétrico

200 un generador de material de clave local

210 un elemento de material público

220 un elemento de material privado

240 un dispositivo de manipulación de polinomio

250 un administrar de dispositivo de red

260 un generador de número de ofuscación

300 una red de comunicación

310 un primer dispositivo de red

320 un segundo dispositivo de red

330 un transceptor

342 un dispositivo de manipulación de polinomio

344 un obtentor de material de clave local

346 un dispositivo de derivación de clave

348 un ecualizador de clave

350 un elemento criptográfico

DESCRIPCION DETALLADA DE LA INVENCION

Aunque la invención es susceptible de llevarse a cabo en muchas formas diferentes, se muestra en las figuras y se describirá aquí en detalle una o más modalidades específicas, con el entendimiento de que la presente invención se va a considerar como ilustrativa de los principios de la invención y no pretende limitar la invención a las modalidades específicas mostradas y descritas.

A continuación se describe una modalidad del método para compartir clave. El método tiene una fase de configuración y una fase de uso. La fase de configuración puede incluir pasos de inicio y pasos de registro. Los pasos de inicio no involucran los dispositivos de red.

Los pasos de inicio seleccionan parámetros de sistema. Los pasos de inicio pueden ser realizados por la tercera parte confiada. Sin embargo, los parámetros de sistema no obstante también pueden considerarse como proporcionados como entradas. En este caso la tercera parte confiada no necesita generarlos, y puede saltarse el paso de inicio. Por ejemplo, la tercera parte confiada puede recibir los parámetros de sistema de un fabricante de dispositivo. El fabricante del dispositivo pudo haber realizado los pasos de

inicio para obtener los parámetros de sistema. Para conveniencia de exposición nos referiremos a la tercera parte confiada como realizando los pasos de inicio, teniendo en mente que esto no es necesario.

Pasos de Inicio

La longitud de clave deseada para la clave que será compartida entre dispositivos en la fase de uso se selecciona; esta longitud de clave es indicada como '*b*'. Un valor típico para una aplicación de baja seguridad puede ser 64 u 80. Un valor típico para una seguridad de nivel de consumidor puede ser 128. Aplicaciones altamente secretas pueden preferir 256 o incluso valores superiores.

Se selecciona el grado deseado; el grado controla el grado de ciertos polinomios. El grado se indicará como '*a*', es al menos 1. Una elección práctica de *a* es 2. Una aplicación más segura puede utilizar un valor superior de *a*, digamos 3 ó 4, o incluso superior. Para una aplicación simple también es posible a=1. El caso *a* = 1 está relacionado con el denominado 'problema de número oculto'; valores de "a" superiores se relacionan con el problema de número oculto confirmando que estos casos son difíciles de romper.

Se selecciona el número de polinomios. El número de polinomio se indicará como '*m*'. Una elección práctica de *m* es 2. Una aplicación más segura puede utilizar un valor superior de *m*, digamos 3 ó 4, o incluso superior. Obsérvese que una

aplicación de baja complejidad, digamos para dispositivos limitados a recurso puede utilizar $m = 1$.

Valores superiores de parámetros de seguridad a y m aumenta la complejidad del sistema y por consiguiente aumentan su inviabilidad. Sistemas más complicados son más difíciles de analizar y de esa forma son más resistentes a análisis crítico.

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

Frecuentemente se predeterminará la longitud de clave, grado y número de polinomios, por ejemplo, mediante un diseñador de sistema, y se proporcionará la parte confiada como entradas. Como una elección práctica uno puede tomar $N = 2^{(a+2)b}-1$. Por ejemplo si $a = 1, b = 64$, entonces N puede ser $N = 2^{192}-1$. Por ejemplo sí $a = 2, b = 128$ entonces N puede ser $2^{512}-1$. Elegir para N el límite superior o inferior del intervalo anterior tiene la ventaja de cálculo fácil. Para aumentar complejidad uno puede elegir un número al azar con el rango para N.

Se selecciona un número de m módulos privados $p_1, p_2, \ldots, p_m$. Los módulos son números enteros positivos. Durante los pasos de registro cada dispositivo estará asociado con un

número de identidad. Cada módulo privado seleccionado es mayor que el número de identidad más grande utilizado. Por ejemplo, uno puede limitar números de identidad al requerir que éstos 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 $p_j = N + y_j \cdot 2^b$. En donde el y_j son números enteros de manera que $|y_j| < 2^b$. Una forma práctica de seleccionar números que satisfagan este requisito es elegir un grupo de m números enteros al azar y_j de manera que $-2^b + 1 \leq y_j \leq 2^b - 1$ y para calcular los módulos privados seleccionados de la relación $p_j = N + y_j \cdot 2^b$. Puede permitirse tener $|y_j|$ un bit más grande, sin embargo, puede ocurrir un problema en cuánto a que la operación modular va mucho más allá de manera que claves compartidas puede no ser iguales.

Para $m > 1$, el sistema es más complicado, y de esa forma más seguro, ya que la operación de módulo para diferentes módulos se combina incluso aunque tales operaciones no son compatibles en el sentido matemático usual. Por esta razón es ventajoso elegir los módulos privados seleccionados como distintos en pares.

Un número de m polinomios bivariados simétricos $f_1, f_2, \ldots, f_m$ de grados a_j se generan. Todos los grados satisfacen $a_j \leq a_j$, muy preferiblemente $a = MAX\{a_1, \ldots, a_m\}$. Una elección práctica es tomar cada polinomio de grado a. Un

polinomio bivariado es un polinomio en dos variables. Un polinomio simétrico f satisface $f(x,y) = f(y,x)$. Cada polinomio f_j es evaluado en el anillo finito formado por el módulo de números enteros p_j, obtenido al calcular el módulo p_j. El módulo de números enteros p_j forma un anillo finito con elementos p_j. En una modalidad de polinomio f_j es representado con coeficientes desde 0 hasta p_j - 1. Los polinomios bivariados pueden seleccionarse al azar, por ejemplo, al seleccionar coeficientes al azar con estos límites. Obsérvese que algunos o todos los polinomios bivariados pueden generarse asimétricamente, lo que lleva a un sistema con dos grupos. Asumiremos para simplicidad que todos los polinomio seleccionados son simétricos.

La seguridad de compartir clave depende de estos polinomios bivariados ya que son el material de clave de raíz del sistema; así que se tomaron medidas preferiblemente fuertes para protegerlos, por ejemplo, procedimientos de control, dispositivos resistentes a alteración, y similares. Preferiblemente los números enteros seleccionados $p_1, p_2, \ldots, p_m$ también se mantienen secretos, incluyendo el valor y_j correspondiente a p_j, aunque esto es menos crítico. Haremos referencia a los polinomios bivariados también en la siguiente forma: para J=1,2,…,m, escribimos $f_j(x,y)=$ $\sum_{i=1}^{a} f_{i,j}(x) y^i$

La modalidad anterior puede ser variada en un número de formas. Las restricciones sobre los módulos

privados y públicos pueden elegirse en una variedad de formas, de manera que ofuscación de polinomio univariado sea posible, incluso que las claves compartidas obtenidas en dispositivos de red permanezcan suficientemente cerca entre sí suficientemente lo suficientemente frecuente. Como se explicó, lo que es suficiente dependerá de la aplicación, el nivel de seguridad requerido y los recursos de cómputo disponibles en los dispositivos de red. La modalidad anterior combina números enteros positivos de manera que las operaciones modulares que se llevan a cabo cuando se generan las porciones de polinomios se combinen en una forma no lineal cuando se agregan sobre los números 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 que: (i) el tamaño de N es fijo para todos los dispositivos de red y enlazado a a; (ii) el efecto no lineal aparece en los bits más significativos de los coeficientes formando el material de clave almacenado en el dispositivo. Debido a esa forma específica la clave compartida puede generarse al reducir el módulo 2^b después del módulo de reducción N.

Estos conceptos de diseño pueden ser aplicados en una forma más general para mejorar en aspectos (i) y (ii) como se mencionó en el último párrafo. A continuación se proporcionan diferentes construcciones generales para elegir

los módulos públicos y privados. Para abordar el primer punto (i) esta estructura para N y p_j se ajusta a una expresión más general en donde escribimos $p_j = 2^X + y_j 2^{Y_j} - 1$ de manera que cada uno j, $y_j + ba_j = X$ y $|y_j| < 2^b$. Esta expresión permite una forma más variable p_j mientras asegura un efecto máximo cuando introduce efectos no lineales. Obsérvese que uno también puede hacer, $y_j + ba_j \approx X$, 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 incluso más general en donde $p_j = \beta 2^X + \gamma_j 2^{Y_j} + \zeta_j 2^{Z_j}$. Al establecer, por ejemplo, ζ_j = -1, β = 1, y $Z_j = 0 \ \forall j$ obtenemos la expresión previa en la cual diferentes valores y_j introduce un efecto no lineal en los bits más significativos de los coeficientes del material de clave almacenados en un dispositivo de red. En este caso, el módulo público constante (N) es $N = 2^X - 1$, mientras la parte variable privada utilizada en la generación de diferentes números enteros positivos involucrados en las operaciones modulares es $\gamma_j 2^{Y_j}$. Alternativamente, podemos establecer

$$Y_j = 1, \beta = 1, Z_j = 0, \ Y_j = (\alpha_j + 1)b, X = (\alpha_j + 2)b \ \forall \ j$$

mientras ζ_j son diferentes para diferente j de manera que $|\zeta_j|$. En este caso, las diferencias en ζ_j permiten introducir un efecto no lineal en los bits menos significativos de los

coeficientes del material de clave local almacenado en un nodo. La construcción de la parte pública en este caso también es diferente e igual a $N = \beta_j 2^{X_j} + \gamma_j 2^{Y_j} = 2^X + 2^{b(\alpha_j+1)}$ es decir, las partes que permanecen constantes. Obsérvese en este caso que el efecto no lineal está en la parte más baja, y debido a la condición para el efecto de mezcla máximo mencionado anteriormente, entonces la diferencia entre Y_j - Z_j - $\log_2$ debe ser $\alpha_j b$. En una forma similar, pueden definirse otras construcciones siguiendo el mismo concepto.

Pasos de Registro

En el paso registro cada dispositivo de red es asignado con material de clave (KM). Un dispositivo de red está asociado con un número de identidad. El número de identidad puede estar asignado a demanda, por ejemplo mediante la TTP, o ya puede estar almacenado en el dispositivo, por ejemplo, almacenado en el dispositivo en fabricación, etc.

La TTP genera un grupo de material de clave para un dispositivo A como a continuación:

$$KM^A(X) = \sum_{j=1}^{m} < f_j(x, A) >_{p_j} + 2^b \sum_{i=0}^{a} \epsilon_{A,i} X^i = \sum_i C_i^A x^i$$

en donde $KM^A(X)$ es el material de clave de un dispositivo con número de identidad A; X es una variable formal. Obsérvese que el material de clave no es lineal. La anotación $<\ldots>_{pj}$ denota reducir por módulo p_j cada coeficiente del polinomio entre los corchetes. La anotación '$\epsilon_{A,i}$' denota un número entero al azar, que es un ejemplo de un número de ofuscación, de manera que $|\epsilon_{A,i}| < 2^{(a+1-i)b}$. Obsérvese que cualquiera de los números enteros al azar puede ser positivo o negativo. Los números al azar ϵ son generados de nuevo para cada dispositivo. El término $\sum_{i=0}^{a} \epsilon_{A,i} X^i$ de esa forma representa un polinomio en X de grado a, del cual la longitud del coeficiente es más corta con grado creciente. Alternativamente, una condición más general, pero más complicada es que $\sum_{i=0}^{a} |\epsilon_{A,i}| \cdot 2^{b+i}$ es pequeño, por ejemplo, $< 2a$. Obsérvese que el paso de agregar ofuscación es opcional y puede ser omitido, pero se prefiere para obtener un nivel de seguridad superior. Asumiremos que se utiliza ofuscación.

Todas las otras adiciones pueden utilizar la aritmética de número entero natural, o (preferiblemente) utilizan módulo de adición N. Así que la evaluación de los polinomios univariados $\sum_{j=1}^{m} < f_j(x,A) >_{p_j}$ se realiza cada uno individualmente por módulo a un módulo más pequeño p_j pero la suma de estos mismos polinomios univariados reducidos preferiblemente se hace por módulo N. También agregar el polinomio de ofuscación $2^b \sum_{i=0}^{a} \epsilon_{A,i} X^i$ puede hacerse utilizando

aritmética de número entero natural o, preferiblemente, módulo N. El material de clave comprende los coeficientes C_i^A con $i = 0, \ldots, a$. El material de clave puede ser presentado como un polinomio como anteriormente. En la práctica, el material de clave puede ser almacenado como una lista, por ejemplo, una disposición, de los números enteros C_i^A. El dispositivo A también recibe los números N y b. Puede implementarse manipulación de polinomios, por ejemplo, como manipulación de disposiciones que contienen los coeficientes, por ejemplo, enlistando todo el coeficiente en un orden predeterminado. Obsérvese que pueden implementarse polinomios, en otras estructuras de datos, por ejemplo, como una posición asociativa (también conocida como un 'mapa') que comprende una colección de pares (grado, coeficiente), preferiblemente de manera que cada coeficiente aparezca máximo una vez en la colección. Los coeficientes C_i^A que se proporcionan al dispositivo están preferiblemente en el rango 0, 1, .. N-1.

En caso de que se utilice la construcción más general para N y los números enteros p_j, el polinomio de ofuscación necesita ser adaptado de manera que los números al azar ϵ afecten diferentes partes de los coeficientes. Por ejemplo, si se introduce el efecto no lineal en los bits menos significativos de los coeficientes del material de clave almacenados en los dispositivos de red, entonces los

números al azar deben afectar únicamente la parte más alta de los coeficientes y un número variable de bits en la parte más baja de los coeficientes. Esta es una extensión directa del método descrito anteriormente y son factibles otras extensiones.

Fase de Uso

Una vez que dos dispositivos A y B tienen un número de identidad y recibieron su material de clave desde la TTP, pueden utilizar su material de clave para obtener una clave compartida. El dispositivo A puede realizar los siguientes pasos para obtener su clave compartida. En primer lugar, el dispositivo A obtiene el número de identidad *B* del dispositivo B, entonces A genera la clave compartida al calcular lo siguiente:

$$K_{AB} = << KM^A(x)|_{x=B} >_N >_{2^b} = \ll \sum_i C_i^A B^i >_N >_{2^b}$$

Es decir, A evalúa su material de clave, visto como un polinomio de número entero, para el valor B; el resultado de evaluar el material de clave es un número entero. Después el dispositivo A reduce el resultado de la evaluación por primer módulo del módulo público *N* y entonces por el módulo del módulo de clave 2^b. El resultado será indicado como clave compartida de A, es un número entero en el rango de 0 hasta $2^b - 1$. Para su parte, el dispositivo B puede generar clave compartida de B al evaluar su material con clave para identidad *A* y al reducir el módulo de resultado *N* y entonces

el módulo 2^b.

En línea con la descripción anterior, si se utiliza una expresión más general de N y los números enteros positivos p_j, entonces el método para obtener la clave de bits b necesita una pequeña adaptación. En particular, si el efecto no lineal es introducido en los bits más bajos de los coeficientes del material de clave almacenado en los dispositivos de red mientras el segundo término en la expresión de N es Y_j, entonces la clave es generada como a continuación:

$$K_{AB} = < \frac{< KM^A(x)|_{x=B} >_N}{2^{Y_j}} >_{2^b}$$

Debido a que los polinomios bivariados en el material de clave de raíz son clave compartida de A simétrica y clave compartida de B simétricas son frecuentemente, aunque no necesariamente siempre, iguales. Los requisitos particulares sobre los números enteros $p_1, p_2, \ldots, p_m$, y sobre los números al azar (opcionales) ϵ son tales que las clave son frecuentemente iguales y casi siempre cerca una de otra modulan dos a la energía de la longitud de clave. Si A y B han obtenido la misma clave compartida, entonces pueden utilizarla como una clave simétrica que es compartida entre A y B; por ejemplo, puede utilizarse para una variedad de aplicaciones criptográficas, por ejemplo, pueden intercambiar uno o más mensajes codificados criptográficamente y/o

autentificados utilizando la clave compartida. Preferiblemente, 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 hash.

Si A y B no han obtenido la misma clave compartida, entonces casi es cierto que estas claves están cerca entre sí, al remover un número de estos bits menos significativos de las claves, las claves generadas casi siempre pueden hacerse iguales. A y B pueden verificar si sus claves compartidas son iguales al realizar una confirmación de clave, por ejemplo, A puede enviar a B un mensaje que contiene el par (m, E(m)), en donde m es un mensaje, digamos una secuencia fija o un número al azar, y E(m) es la codificación criptográfica utilizando la clave compartida de A.

Al decodificar criptográficamente E(m) utilizando la clave compartida de B, B puede verificar si 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 ecualización de clave. Por ejemplo, pueden hacer uso del hecho que las dos claves están aritméticamente cerca una de otra. Por ejemplo, el dispositivo de red A y B puede remover de manera iterativa un bit menos significativo y enviar un mensaje de confirmación

de clave hasta que las claves son iguales. Después de obtener claves iguales, A y B pueden realizar un algoritmo de derivación de clave para recuperar claves de una longitud de clave usual.

Los m módulos privados seleccionados, $p_1, p_2, \ldots, p_m$, son relativamente primos en pares. Si estos números son relativamente primos en pares aumenta la falta de compatibilidad entre las operaciones de módulo. Obtener números relativamente primos en pares puede obtenerse al seleccionar los números enteros en orden, al probar para cada número entero si todos los pares de diferentes números aún son relativamente primos, si no se remueve el número que se acaba de seleccionar del grupo. Este procedimiento continúa hasta que se seleccionaron todos los m números.

La complejidad aumenta incluso más al requerir que los m módulos privados seleccionados, $p_1, p_2, \ldots, p_m$, sean números primos distintos. En ese caso cada número primo puede ser requerido para tener la forma $p_j = N + Y_j \cdot 2^b$. En donde el y_j son números enteros de manera que $|y_j| < 2^b$. Experimentos han confirmado que estos números primos están fácilmente disponibles. Por ejemplo, uno puede seleccionar repetidamente un y_j al azar y probar el p_j resultante hasta que se encuentra un número primo. Lo mismo aplica si se aplica una expresión más general, como se describió anteriormente. De hecho continúa del teorema de número primo para progresos

aritméticos que siempre y cuando a sea de aproximadamente el mismo orden de magnitud que b, en particular para a < b, tales primos son abundantes. En particular, para cualquier combinación de longitud de clave en el grupo 64, 128, 196, 256 y el grado en el grupo 2, 3, confirmamos por experimento que muchos números primos de esta forma podrían generarse utilizando el algoritmo anterior dentro de límites de tiempo prácticos. Cuando se utilizan números primos cada polinomio f_j de esa forma es tomado en el campo finito con p_j elementos.

Muchas variantes son posibles para elegir los varios parámetros utilizados durante las fases de registro y de uso. Por ejemplo, en una modalidad simplificada, los módulos privados son más pequeños que los módulos públicos y satisfacen la relación $p_j = N - \beta_j \cdot 2^b$. En donde el β_j son números enteros positivos de manera que $\beta_j < 2^b$. Una forma práctica para seleccionar números que satisfacen este requisito es para elegir un grupo de m números enteros positivos al azar β_j de manera que $\beta_j < 2^b$ y calcular los módulos privados seleccionados de la relación $p_j = N - \beta_j \cdot 2^b$.

Como se observó, la diferencia entre $Y_j - Z_j - \log_2(\zeta_j)$ puede ser $\alpha_j b$. En una forma similar, pueden definirse otras construcciones después del 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. Un inicio 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 términos y_j y β_j es menor que 2^b y están a cargo de crear un efecto no lineal sobre el MSB y LSB de los coeficientes del material de clave almacenado local en un dispositivo. Obsérvese que ya que los identificadores de dispositivo son de aproximadamente b bits de largo, $y_j(\beta_j)$ afecta el MSB (LSB) de los coeficientes y la porción polinomio evaluada en el anillo de módulo de números enteros p_j. Después de eso, durante la generación del material de clave local para un dispositivo, se agregan los coeficientes de las porciones de polinomio en diferentes anillos sobre los números enteros de manera que se oculte el origen de las contribuciones.

La clave puede ser generada como a continuación: $K_{AB} = <\frac{<KM^A(x)|_{x=B}>_N}{2^{Y_j}}>_{2^b}$, pero si la expresión incluso más general de p_j y N se utiliza y permite introducir un efecto no lineal sobre ambos MSB y LSB, entonces la división después del módulo de reducción N es por 2 a la energía de W, en donde 2^w es la energía de número entero más alta de 2 de la cual N es un múltiplo de número entero. Otras construcciones de N y p_j pueden requerir una división por otra energía de 2. Debido a que los polinomios bivariados en el material de clave de raíz son clave compartida de A y clave compartida de B simétricas son frecuentemente, pero no necesariamente siempre, iguales.

Confirmación de Clave

Puede ser deseable que uno de A y B envíe un mensaje de confirmación de clave a la otra parte. Un denominado mensaje de confirmación de clave (KC, por sus siglas en inglés) permite al receptor del mensaje de confirmación de clave verificar que ha calculado la misma clave que el remitente del mensaje de confirmación de clave. En particular en un esquema para compartir clave para el cual se sabe que la clave establecida por ambas partes puede diferir, puede utilizarse un mensaje de confirmación de clave tanto como una confirmación que ambas han establecido la misma clave, y si no es así, determinar una clave compartida igual. Por ejemplo, en general un código de autentificación de mensaje (MAC, por sus siglas en inglés) con base en la clave establecida puede servir como el mensaje de confirmación, por ejemplo un MAC con base en SHA2 o SHA3, o un CMAC con base AES, y similares. También puede utilizarse una función hash criptográficamente fuerte, por ejemplo, puede utilizarse hash de la clave establecida como el mensaje de confirmación de clave. El hash puede calcularse sobre la misma de clave. El MAC puede calcularse sobre datos que se conocen por B o incluidos en el mensaje de confirmación de clave, por ejemplo, un código generado al azar, etc.

Sin embargo, mensajes de confirmación de clave criptográficamente fuertes generales requieren los mismos

recursos, posiblemente más recursos que un algoritmo para compartir clave de conformidad con los principios anteriores. Los esquemas para compartir clave proporcionados anteriormente permiten funciones más simples que requieren mucho menos recursos de computación que esquemas de confirmación de clave de propósito general.

Dispositivos A y B calculan claves $K_A(B)$ y $K_B(A)$. Se puede mostrar, por las siguientes relaciones matemáticas, que existe un número entero Δ, dependiendo de los parámetros de diseño, de manera que:

$$K_A(B) \in \{< K_B(A) + j >_{2^b} \mid -\Delta \leq j \leq \Delta\},$$

De nuevo, $< x >_m$ denota el número entero entre 0 y m-1 de manera que $x - < x >_m$ sea un múltiplo de m. Definir una función como a continuación: $h(x) = < x >_{2^r}$ donde r es un número entero predeterminado de manera que $2^r \geq 2\Delta + 1$. Comparado con la modalidad general, no hay necesidad de que los dispositivos calculen funciones hash posiblemente complicadas; la desventaja es que algo de información en la clave que se está utilizando se envía sobre un canal de comunicación observable. Usualmente se prefiere que un mensaje de confirmación de clave no se filtre o una cantidad insignificante, de información en la clave para la cual se calcula. Esta desventaja puede ser contrarrestada al dividir la clave establecida por 2^r, después que se ha encontrado que una clave es la misma tanto para A como para B. Más

generalmente en una segunda modalidad, $h(x) = \langle x \rangle$ en donde $v \geq 2\Delta+1$ es tal que 2^b es un múltiplo de v o $\langle 2^b \rangle_v \geq 2\Delta+1$. En ambos casos, $h(K_A(B))$ puede utilizarse por A como un mensaje de confirmación de clave.

Además de enviar un mensaje de confirmación de clave, uno puede disminuir la diferencia entre $K_A(B)$ y $K_B(A)$ al dividir ambas claves por una energía de 2. $K_A(B)$ y $K_B(A)$ son claves de bit b, removiendo entonces los I bits menos significativos de las claves generadas por bit b de manera que una clave de bits b-I, que corresponde a los bits más significativos b-I de la clave generada, se utilice para asegurar la comunicación. Sí b es relativamente grande (digamos, 100) y I es también grande (digamos 50), la probabilidad de que los bits más significativos b-I sean iguales es muy alta, es decir, aproximadamente $1 - \frac{2\Delta}{2^{b-I}}$. Este acercamiento no requiere el intercambio de cualquier información, se remueven I bits de la clave generada original, y la clave resultante puede utilizarse para la comunicación. Sin embargo, esto tiene una desventaja debido a que se reduce el tamaño de clave, potencialmente en una forma considerable para asegurarse que todos los dispositivos en una red compartirán una clave de bit b-I común con probabilidad muy alta.

Obsérvese que remover bits menos significativos puede combinarse con un mensaje de confirmación de clave. Por

ejemplo, después de remover I bits, se calcula y envía un mensaje de confirmación de clave a la otra parte. Este acercamiento tiene la ventaja que, incluso si la remoción de bits menos significativos no fue suficiente para establecer una clave común, será más fácil encontrar tal clave común.

En un acercamiento diferente el problema de que se establezcan claves potencialmente diferentes por partes A y B es el siguiente: Autoridad central tiene toda la información para calcular de antemano si cualquiera de dos dispositivos puede derivar diferentes claves. Por ejemplo, la autoridad central puede iniciar con identificador A individual y material de clave calculado para A. Se agregan dispositivos a un grupo de dispositivo de manera iterativa. Cuando se va a agregar un nuevo dispositivo B' al sistema, la TTP calcula material de clave para B'. La TTP, verifica para cada combinación de B' y los dispositivos ya en el grupo si llegarían a la misma clave común. Por ejemplo, la TTP puede verificar que encuentran la misma clave directamente. La TTP también puede verificar que B' y cualquier otro dispositivo llegará a una clave común al acoplarse en un protocolo de acuerdo de clave adecuado para reparar una posible clave diferente; por ejemplo, al dividir mediante una energía de 2 y/o al enviar uno o más mensajes de confirmación de clave. En vista del acercamiento probabilístico anterior, es muy poco probable que una elección al azar para B' haga {A,B'} válido

para todo A si el número de dispositivos A es relativamente pequeño.

Si resulta que B' no llegara a una clave común con algunos de los dispositivos en el grupo, la TTP asigna un nuevo identificador a B' o calcula un nuevo material de clave, pero con diferentes elecciones al azar. Aunque revisar esta condición representa un gran gasto, es posible para dispositivos de redes relativamente pequeños (digamos ~ $O(10^4)$ ó $O(10^5)$).

También puede aplicarse un acercamiento relacionado en grupos de dispositivos. En particular, en algunos entornos no todos los dispositivos pueden requerir hablar entre sí, por ejemplo, si dispositivos son estáticos y son desplegados en grupos (por ejemplo, en un edificio). En este caso, la verificación realizada por la TTP cuando se agrega un nuevo dispositivo B' para revisar los dispositivos que pertenecen al grupo al cual se agregará B'. Por ejemplo, la TTP puede verificar si todos los dispositivos en un grupo dado genera una clave si I LSB de la clave es removido. Obsérvese que este método también permite el diseño de esquemas jerárquico más avanzados de manera que todos los dispositivos pertenezcan al grupo principal en un primer nivel, los dispositivos están divididos en un número de grupos en un segundo nivel, dispositivos en un grupo en un segundo nivel además están divididos en un número de subgrupos. En tal

organización jerárquica, la TTP puede verificar si todos los dispositivos en un grupo dado en el nivel w generan una clave común después de la remoción de I_w bits. En tal sistema, grupos a un nivel más profundo pueden requerir la remoción de un número menor de bits mientras grupos en niveles altos pueden requerir la remoción de más bits para asegurar la generación de claves comunes.

La TTP puede realizar estas revisiones en cualquier momento que se agrega un nuevo dispositivo, pero puede crear también de manera proactiva un grupo de identificadores de dispositivo y material de clave de manera que cada par de identificadores de este grupo dé una clave común válida.

Por ejemplo, la TTP puede limitarse a pares de dispositivos válidos $\{A,B\}$, en donde un par es válido si:

$$\left\lfloor \frac{K_B(A)}{2^l} \right\rfloor = \left\lfloor \frac{K_A(B)}{2^l} \right\rfloor$$

en donde I se refiere a I bits correspondientes a I Bits menos significativos de $K_A(B)$ y $K_B(A)$. Esta condición, en general, muestra una forma para verificar que las claves que se utilizarán realmente son iguales. Otra condición es que se admite un nuevo B sí, y únicamente si para todo A, los I bits menos significativos de $K_A(B)$ y $K_B(A)$ corresponden a un número en $[\Delta, 2^l - 1 - \Delta]$.

La Figura 1 es un diagrama de bloque esquemático que ilustra un generador de material de clave de raíz. Un

obtentor de material de clave está configurado para proporcionar datos de entrada, excepto un número de identidad, necesario por un generador de material de clave local para generar material de clave local. Un generar de clave es un ejemplo de un obtentor de material de clave. En lugar de generar todos o parte de los datos de entrada, algunos parámetros también pueden obtenerse por el generador de material de clave de raíz al recibirlos; por ejemplo el obtentor de clave puede comprender un receptor electrónico para recibir datos de entrada, por ejemplo, un módulo público y privado. Un obtentor 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, recibidos y el módulo público y los módulos privados y polinomios bivariados simétricos correspondientes son generados. En una modalidad también se predetermina el módulo público, por ejemplo, recibido.

El generador de clave de raíz 100 comprende un elemento de grado de polinomio 112, un elemento de longitud de clave 114 y un número de elemento de polinomio 116 configurado para proporcionar el grado de polinomio, la longitud de clave y el número de polinomios, es decir, a, b y m respectivamente. Aunque estos elementos pueden ser generados, por ejemplo, deteniendo de las circunstancias, típicamente se eligen estos parámetros por un diseñador de

sistema. Por ejemplo, los elementos pueden ser diseñados como memorias no volátiles, o como receptores para recibir los valores de elemento, o como memorias volátiles conectadas a un receptor, etc. Una elección adecuada incluye $a = 2, b = 128, m = 2$. Cualquiera de los números puede aumentar o disminuir para obtener un sistema más o menos seguro.

El generador de clave de raíz 100 comprende un elemento de módulo público 110 configurado para proporcionar el módulo público N. El módulo público puede o no ser elegido por un diseñador de sistemas. Por ejemplo, el módulo público puede ser establecido a un número conveniente permitiendo reducción rápida (cerca o igual de una energía 2). El módulo público es elegido con un rango determinado por los elementos 112 y 114.

El generador de clave de raíz 100 comprende un administrador de módulo privado 112 configurado para proporcionar el módulo privado p, o múltiples módulos privados $p_1, \ldots, p_m$,. Por ejemplo, se eligen al azar dentro de los límites apropiados.

El generador de clave de raíz 100 comprende un administrador de polinomio bivariados simétricos 114 configurado para proporcionar el polinomio bivariados simétricos f, o múltiples polinomios bivariados simétricos $f_1, \ldots, f_m$,. Cada polinomio bivariado simétrico es elegido con coeficientes de módulo al azar del módulo privado

correspondiente, es decir, el módulo privado que tiene el mismo índice. Los coeficientes pueden ser elegidos dentro del rango 0 a p - 1, y pueden ser elegidos al azar.

Pueden elegirse módulos privados al agregar o restar un múltiplo de dos a la energía de la longitud de clave al módulo público. Esto resultará en módulos privados de manera que la diferencia con el módulo público termina en una serie de ceros consecutivos. Uno puede elegir también un módulo público y uno o más módulos privados de manera que una serie de ceros consecutivos de longitud de clave ocurre no al final si no en otra posición, digamos posición de 's', contando desde el bit menos significativo.

La Figura 2 es un diagrama de bloque esquemático que ilustra un generador de material de clave local 200. El generador de material de clave 100 y generador de material de clave local 200 juntos forman un sistema para configurar un dispositivo de red para compartir clave.

El generador de material de clave local 200 comprende un dispositivo de manipulación de polinomio 240. El generador de material de clave local 200 comprende un elemento de material público 210 para proporcionar parámetros públicos a,N al dispositivo de manipulación de polinomios 240. El generador de material de clave local 200 comprende un elemento de material privado 220 para proporcionar los parámetros privados p_1, f_1 y m al dispositivo de manipulación

de polinomio 240. Los elementos 210 y 220 pueden ser implementados por los elementos correspondientes de generador de material de clave 100; estos elementos también pueden ser memorias o conductores comunes para conectarse al generador de material de clave 100.

El generador de material de clave local 200 comprende un generador de número de ofuscación 260 para proporcionar un número de ofuscación '$\epsilon_{A,i}$' al dispositivo de manipulación de polinomio 240. El número ofuscado puede ser un número al azar, por ejemplo, generado con el generador de número al azar. El generador de número de ofuscación 260 puede generar múltiples números de ofuscación para múltiples coeficientes del polinomio univariado. En una modalidad se determina un número de ofuscación para cada coeficiente del polinomio univariado.

El generador de material de clave local 200 comprende un administrar de dispositivo 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 configurarse 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 al azar, en serie o de código generado al azar. En el último caso el número de identidad se envía junto con el material de clave

local al dispositivo de red.

El dispositivo de manipulación de polinomio 240 obtiene, posiblemente múltiples polinomios univariados al sustituir el número de identidad del administrador 250 en cada uno de los polinomios bivariados y al reducir por cada módulo el módulo privado correspondiente. Se agregan múltiples polinomios univariados reducidos resultantes, en forma de coeficiente, con adición aritmética natural. También agregados están uno o más números de ofuscación. Preferiblemente, se redujo el resultado, de nuevo en forma de coeficiente, módulo del módulo público; los coeficientes del último pueden representarse en el rango 0 a N - 1.

El polinomio univariado ofuscado es parte del material de clave local correspondiente al número de identidad. Si se necesitan, el módulo público, grado y la longitud de clave también se envían al dispositivo de red.

La Figura 3 es un diagrama de bloque esquemático que ilustra una red de comunicación 300 que comprende múltiples dispositivos de red; se muestra un primer dispositivo 310 y un segundo dispositivo 320. Ilustraremos el primer dispositivo de red 310. El segundo dispositivo de red 320 puede ser el mismo, o trabajar a lo largo de los mismos principios.

El dispositivo de red 310 comprende un receptor 330 que combina un remitente y un receptor para o recibir

mensajes en formato electrónico, por ejemplo, digital, en forma por cable e inalámbricamente desde y hacia el segundo dispositivo de red 320. Posiblemente, también se utiliza el transceptor 330 para recibir el material de clave local desde la autoridad de red 200. A través del transceptor 330 se recibe 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 obtentor de material de clave local 344. El obtentor de material de clave local 344 puede ser implementado como memoria local, por ejemplo, memoria no volátil tal como memoria flash para almacenar el material de clave local. El obtentor de material de clave local 344 también puede configurarse para obtener el material de clave local del generador 200, por ejemplo, a través del transceptor 330. El obtentor de material de clave local 344 está configurado para proporcionar al dispositivo de manipulación de polinomio con los parámetros necesarios.

El dispositivo de red 310 comprende un dispositivo de manipulación de polinomio 342 configurado para sustituir el número de identidad del segundo dispositivo de red dentro del polinomio univariado ofuscado, y para realizar dos reducciones sobre el resultado: Reducir primero el resultado del módulo de sustitución del módulo público y el segundo módulo de reducción de un módulo de clave. Obsérvese que incluso si se utilizaron múltiples módulos privados,

únicamente se necesitaría un módulo público. Obsérvese que para algunas combinaciones de N y módulo privado, se requiere una división por una energía 2 antes que se reduzca por módulo el resultado de un módulo de clave.

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

El dispositivo de red 310 comprende un ecualizador de clave 348 opcional. Obsérvese que puede suceder que la clave compartida derivada en el primer dispositivo de red no sea igual a la clave derivada en el segundo dispositivo de red (con base en el número de identidad del primer dispositivo de red). Si esto es considerado no deseable, puede seguirse un protocolo de ecualización de clave.

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 decodificar criptográficamente o autentificar un mensaje del primer

dispositivo de red con la clave compartida antes de enviarla al segundo dispositivo de red, digamos un estado de mensaje. Por ejemplo, el elemento criptográfico 350 puede decodificar criptográficamente o verificar la autenticidad de un mensaje recibido del segundo dispositivo de red.

Típicamente, un sistema para configurar un dispositivo de red para compartir clave 200, y un primer dispositivo de red configurado para determinar una clave compartida 310, cada uno comprende un microprocesador (no mostrados) que ejecuta software apropiado almacenado en los dispositivos respectivos, por ejemplo, cuyo software pudo haber sido descargado y almacenado en una memoria correspondiente, por ejemplo RAM (no mostrada).

Una modalidad interesante se obtiene para $a = 1$, especialmente en combinación con valores superiores de m, digamos superiores a 1, 2 o superiores, 4 o superior. La manipulación de polinomio requerida se reduce a una multiplicación o reducción individual, dando una implementación especialmente simple. Sin embargo, incluso para este caso simple recuperar los polinomios bivariados originales no es directo, y se vuelve cada vez más complicado con valores superiores de m. Aunque no se conoce ningún ataque viable para $a = 1$, la estructura lineal puede ser un punto de partida para análisis futuro, de manera que uno puede desear restringirse a $a > 1$, por esta razón.

La Figura 4 es un cuadro de flujo esquemático que ilustra un método para generar material de clave local 400. El método comprende obtener 410 un módulo público y privado, y un polinomio bivariado simétrico, obtener 420 un número de identidad de un dispositivo de red, sustituir 430 el número de identidad en el módulo de polinomio bivariado con el módulo privado, agregar 450 un número de ofuscación a un coeficiente, y almacenar 450 el polinomio univariado ofuscado en el dispositivo de red.

La Figura 5 es un cuadro de flujo esquemático que ilustra un método para generar una clave compartida 500. El método comprende obtener 510 número de identidad externo de otro dispositivo de red, enviar 520 el número de identidad local a otro dispositivo de red, sustituir 530 número de identidad externo dentro del módulo de polinomio univariado ofuscado del módulo público, reducir 540 por módulo el módulo de clave, derivar 550 una clave compartida, enviar 560 un mensaje de confirmación de clave al otro dispositivo de red, determinar 570 si se confirmó 570 la clave, y una aplicación criptográfica 580. Si no se confirmó la clave en el paso 570 entonces el método continuo en el paso 550 con derivar una nueva clave. Por ejemplo, el paso 550 puede remover un bit menos significativo adicional cada vez que se confirma la clave.

Los pasos 550, 560 y 570 juntos forman un protocolo de ecualización de clave. Por ejemplo, en el paso 560 un código generado al azar y codificación criptográfica de

código generado al azar bajo la clave compartida derivados en el paso 570 pueden enviarse al segundo dispositivo. En el paso 560 se recibe un mensaje desde el segundo dispositivo. El mensaje recibido puede simplemente decir que el mensaje de confirmación de clave recibido mostró que las claves no son iguales. El mensaje recibido también puede contener un mensaje de confirmación de clave. En el último caso, el primer dispositivo de red verifica el mensaje de confirmación de clave y establece si las claves son iguales. Si no es así se deriva una nueva clave, por ejemplo, al eliminar al menos un bit significativo.

Son posibles muchas formas diferentes para ejecutar el método, como será evidente para un técnico en la materia. Por ejemplo, el orden de los pasos puede variar o pueden ejecutarse algunos pasos en paralelo. Sin embargo, entre pasos pueden insertarse otros pasos de método. Los pasos insertados pueden representar refinaciones del método tal como se describió aquí, o pueden no estar relacionados con el método. Por ejemplo, los pasos 410 y 420, o 510 y 520, pueden ejecutarse, al menos parcialmente, en paralelo. Además, un paso dado puede no haber terminado completamente antes que se inicie un siguiente paso.

Un método de conformidad con la invención puede ser ejecutado utilizando software, que comprende instrucciones para causar que un sistema de procesador realice el método

400 ó 500. Software únicamente puede incluir aquellos pasos tomados por una sub-entidad particular del sistema. El software puede ser almacenado en un medio de almacenamiento adecuado, tal como un disco duro, un disco flexible, una memoria, etc. El software puede ser enviado como una señal a lo largo de un cable, o inalámbricamente, o utilizando una red de datos, por ejemplo, Internet. El software puede ponerse a disponibilidad para descarga y/o para uso remoto en un servidor.

La Figura 6 muestra en forma esquemática una posible secuencia de mensaje entre dos dispositivos de red, dispositivo A y B, mientras están generando una clave compartida. El tiempo se acaba. En el paso 610, el dispositivo de red 600 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 clave para la clave compartida (K1) que derivó con base en número de identidad A y su material de clave local. En el paso 630, el dispositivo A encontró que no generaron la misma clave. El dispositivo A ha eliminado un bit menos significativo (digamos número entero dividido por 2) para obtener la clave K2. En el paso 630 el dispositivo A envía un nuevo mensaje de confirmación de clave. De esta forma A y B intercambian mensajes de confirmación de clave 640 hasta que llegan a la misma clave en el paso 650. En el paso 650 el dispositivo A envía un mensaje de confirmación de clave al dispositivo B.

El dispositivo B fue capaz de verificar que llegaron en la misma clave. En el paso 660 envía una confirmación de lo mismo, ésta puede ser un mensaje autentificado o un mensaje de confirmación de clave, etc. En el paso 670 el dispositivo A envía un mensaje M1 que es codificado criptográficamente (digamos utilizando AES) y/o autentificado (digamos utilizando HMAC) utilizando la clave compartida ahora igual.

El algoritmo a continuación proporciona una implementación posible de este acercamiento, es decir, un protocolo para acuerdo de clave mutuo y derivación de clave de sesión ejecutados por el Dispositivo A y el Dispositivo B.

```
Establecer I = L
Establecer continuar = VERDADERO
Establecer Longitud = b-I
Generar una Clave de b-bit k
Mientras (Continuar y (Longitud Mayor>MINIMUN_LENGH)){
K = K>>|
Realizar Saludo de Mano de Autentificación Mutua con B con Base en K
si el saludo de manos fue exitoso, Entonces {
continuar = FALSO
}también{
Longitud = b-I
}
```

El protocolo remueve un número de bits de la secuencia de bits generada con un algoritmo para compartir clave, tal como se describió, y realiza un saludo de manos de autentificación, por ejemplo, respuesta de desafío. El saludo de manos de autentificación puede comprender un mensaje de confirmación de clave. Si no es exitoso, se removieron pocos bits adicionales, y así sucesivamente hasta que el saludo de mano se realiza exitosamente o la clave se vuelve muy corta. El protocolo puede ser modificado en un número de formas, por ejemplo, el remover un número de bits variable dependiendo de la iteración de requerir siempre un número fijo de pasos de manera que un espía que observa la ejecución del protocolo no obtiene ninguna información sobre la longitud de la clave común compartida entre A y B. Ese acercamiento tiene la ventaja que se asegura que las claves compartidas son tan largas como sea posible; sin embargo, tiene la desventaja potencial que requiere un número de intercambios para el acuerdo sobre la clave común. Porto lado, para la mayoría de las aplicaciones no habrá un gran problema debido a que para la mayoría de los pares de dispositivos las claves serán iguales o diferirán únicamente pocos bits y únicamente un par de bits llegará a claves con un número relativamente alto de diferentes bits menos significativos. Esto continúa de propiedades de las propiedades de las claves generadas.

Existen otras formas para llegar a una misma clave

para ambos dispositivos. De nuevo aseguramos que los dispositivos A y B calculan claves $K_A(B)$ y $K_B(A)$. Los protocolos a continuación aplican para cualquier esquema para compartir clave para el cual existe un número entero Δ, dependiendo de los parámetros de diseño, de manera que:

Por ejemplo, los esquemas para compartir clave aquí descritos tienen esta propiedad. Las claves generadas son representadas como números enteros b-bits. Así que pueden considerarse claves como elementos del grupo $\{0,1,2,\ldots,2^b-1\}$. Por ejemplo, si $\Delta=2$, y $K_B(A)=1$, entonces $K_A(B)$ está en $\{1,2,3,0,2^b-1\}$ (obsérvese que $< 1 - 2>_{2^b} = 2^b - 1$). Para parámetros de diseño de sistema apropiadamente elegidos, Δ es relativamente pequeño. La invención asegura que se genera la misma clave siempre debido a una falla para generar una clave común que puede recuperarse desde ahí.

De conformidad con este método, en Dispositivo A envía al dispositivo B un valor de función $h(K_A(B))$. Aquí h es una función hash adecuada, por ejemplo, una función hash criptográfica. El dispositivo B calcula h(i) para todo i en $\{< K_B(A) + j >_{2^b} \mid -\Delta \leq j \leq \Delta\}$ y utiliza, para comunicaciones futuras, el número entero i para el cual h(i) coincide con el valor recibido de $h(K_A(B))$. Si Δ es demasiado grande, los dispositivos A y B pueden dividir primero sus claves por una energía de 2 para reducir el tamaño de Δ.

Se apreciará que la invención también se extiende para calcular programas, particularmente programas de computadora sobre o dentro de un portador, adaptado para colocar la invención en práctica. El programa puede estar en la forma de código de fuente, código de objeto, o fuente intermedia de código y código de objeto tal como forma parcialmente recopilada, o en cualquier otra forma adecuada para uso en la implementación del método de conformidad con la invención. Una modalidad que se refiere al producto de programa de computadora comprende instrucciones ejecutables por computadora correspondientes a cada uno de los pasos de procesamiento de al menos uno de los métodos descritos. Estas instrucciones pueden estar subdivididas en subrutinas y/o almacenadas en uno o más archivos que pueden estar enlazados estáticamente o dinámicamente. Otra modalidad que se refiere a un programa de computadora comprende instrucciones ejecutables por computadora correspondientes a cada uno de los medios de al menos uno de los sistemas y/o productos descritos.

Debemos observar que las modalidades mencionadas anteriormente ilustran en lugar de limitar la invención, que aquellos técnicos en la materia serán capaces de diseñar muchas modalidades alternativas. En las reivindicaciones, cualquier signo de referencia colocado entre paréntesis no deben interpretarse como limitando la invención. El uso del

verbo "comprenden" y sus conjugaciones no excluyen la presencia de elementos o pasos diferentes a aquellos mencionados en la reivindicación. El artículo "un" o "uno" precedente a un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede ser implementada por medios de hardware que comprenden varios elementos distintos, y por medio de una computadora adecuadamente programada. En la reivindicación de dispositivo que enumera varios medios, varios de los medios pueden ser representados por un mismo artículo de hardware. El simple hecho que se mencionen ciertas características en reivindicaciones dependientes mutuamente diferentes no indica que no puede utilizarse una combinación de estas medidas para tener ventaja.

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 para configurar un dispositivo de red para compartir clave, caracterizado porque comprende:

obtener en forma electrónica un módulo privado, un módulo público, y un polinomio bivariado que tiene coeficientes de número entero, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas en al menos bits consecutivos de longitud de clave,

generar material de clave local para el dispositivo de red, el paso de generación comprende obtener en forma electrónica un número de identidad para el dispositivo de red, y determinar utilizando un dispositivo de manipulación de polinomio un polinomio univariado del polinomio bivariado al sustituir el número de identidad dentro del polinomio bivariado, reducir por módulo el resultado de módulo privado de la sustitución, y

almacenar electrónicamente el material de clave local generado en el dispositivo de red, y almacenar el módulo publico en el dispositivo de red.

2.- Un método de conformidad con la reivindicación

1, caracterizado porque generar material de clave local para el dispositivo de red comprende generar un número de ofuscación y agregar utilizando un dispositivo de manipulación de polinomio, el número de ofuscación a un coeficiente del polinomio univariado para obtener un polinomio univariado ofuscado, el material de clave local generado comprende el polinomio univariado ofuscado.

3.- Un método de conformidad con cualquiera de las reivindicaciones 1 ó 2, caracterizado porque el polinomio bivariado es un polinomio simétrico.

4.- Un método de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque los bits de longitud de cadena menos significativos en la representación binaria del módulo público son los mismos que los bits de longitud de cadena menos significativos del módulo privado.

5.- Un método de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque además comprende

generar el módulo privado utilizando un generador de número al azar electrónico, y/o

generar el polinomio bivariado utilizando un generador de número al azar electrónico al generar uno o más coeficientes al azar para el polinomio bivariado.

6.- Un método de conformidad con cualquiera de las

reivindicaciones precedentes, caracterizado porque el módulo público satisface $2^{(a+2)b-1} \leq N$, en donde N representa el módulo público, a representa el grado del polinomio bivariado y b representa la longitud de clave.

7.- Un método de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque comprende obtener en forma electrónica múltiples módulos privados, y múltiples polinomios bivariados teniendo módulo de coeficientes p_i, de manera que exista un grupo de posiciones consecutivas de longitud de bit en las cuales la representación binaria del módulo público está de acuerdo con la representación binaria de todos los módulos privados,

determinar el polinomio univariado comprende sustituir el número de identidad dentro de cada uno de los múltiples polinomio bivariados, reducir por módulo un módulo privado de los múltiples módulos privados correspondientes a un polinomio bivariado simétrico, y agregar los múltiples resultados de las múltiples reducciones.

8.- Un método de conformidad con cualquiera de las reivindicaciones precedentes, caracterizado porque el número de ofuscación es generado de manera que

$$|\epsilon_{A,i}| < 2^{(a+1-i)b}$$

en donde $\epsilon_{A,i}$ denota el número de ofuscación, i denota el monomio correspondiente al coeficiente, a representa el grado del polinomio bivariado y b representa la

longitud de clave.

9.- Un método para un primer dispositivo de red configurado por un método para configurar un dispositivo de red para compartir clave de conformidad con la reivindicación 1 para determinar una clave compartida, la clave es una clave criptográfica, caracterizado porque comprende:

obtener material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende un polinomio opcionalmente ofuscado, univariado,

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 opcionalmente ofuscado, univariado,

reducir al resultado del módulo de sustitución del módulo público y reducir por módulo un módulo de clave; y

derivar la clave compartida del resultado del módulo de reducción del módulo de clave.

10.- Un método de conformidad con la reivindicación 9, caracterizado porque además comprende

determinar si el primer dispositivo de red y el segundo dispositivo de red han derivado la misma clave compartida, y si no es así derivar una clave compartida

adicional del resultado del módulo de reducción del módulo de clave.

11.- Un método de conformidad con cualquiera de las reivindicaciones 9 ó 10, caracterizado porque además comprende dividir el resultado del módulo de sustitución del módulo público por un divisor de secuencia de bits cero que es una energía de dos, el divisor de secuencia de bits cero es mayor que 1.

12.- Un sistema para configurar un dispositivo de red para compartir clave, caracterizado porque comprende:

un obtentor de material de clave para obtener en forma electrónica un módulo privado, un módulo público, y un polinomio bivariado simétrico que tiene coeficientes de número entero, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas que al menos en bits consecutivos de longitud de clave,

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

un administrador de dispositivo 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 del dispositivo de red, y almacenar el módulo público en el dispositivo de red, y

un dispositivo de manipulación de polinomio para determinar un polinomio univariado del polinomio bivariado al

sustituir el número de identidad en el polinomio bivariado reduciendo por módulo el resultado del módulo privado de la sustitución.

13.- Un primer dispositivo de red configurado para determinar una clave compartida de conformidad con la reivindicación 1, la clave es una clave criptográfica, caracterizado porque comprende:

un obtentor de material de clave local para obtener material de clave local para el primer dispositivo de red en forma electrónica, el material de clave local comprende un polinomio opcionalmente ofuscado, univariado,

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 de polinomio para sustituir el número de identidad del segundo dispositivo de red en el polinomio opcionalmente ofuscado, univariado y reduciendo por módulo un módulo de clave, y

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

14.- Un programa de computadora caracterizado porque comprende medios de código de programa adaptados para realizar todos los pasos de conformidad con cualquiera de las reivindicaciones 1 a 11, cuando el programa de computadora se

ejecuta en una computadora.

15.- Un programa de computadora de conformidad con la reivindicación 14, caracterizado porque es representado en un medio legible por computadora.

RESUMEN DE LA INVENCION

Se proporcionan un método para configurar un dispositivo de red para compartir clave y un método para un primer dispositivo de red para determinar una clave compartida. El método para configurar usos de módulo privado (p_j), un módulo público (N), y un polinomio bivariado (f_j) que tienen coeficientes de número entero, la representación binaria del módulo público y la representación binaria del módulo privado son las mismas al menos en bits consecutivos de longitud de clave (b). Se genera material de clave local para un dispositivo de red al sustituir un número de identidad en el polinomio bivariado y al reducir por módulo el resultado del módulo privado de la sustitución para obtener un polinomio univariado. Puede aumentar seguridad al agregar (440) uno o más números de ofuscación a coeficientes del polinomio univariado para obtener un polinomio univariado ofuscado. En una fase de uso, el dispositivo de red determina una clave criptográfica compartida, al sustituir (530) el número de identidad de otro dispositivo de red dentro del polinomio univariado y al reducir por módulo el módulo público y al reducir por módulo un módulo de clave.

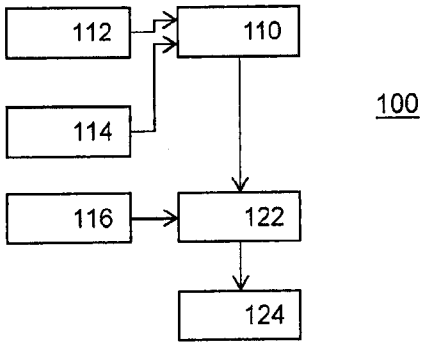

FIGURA 1

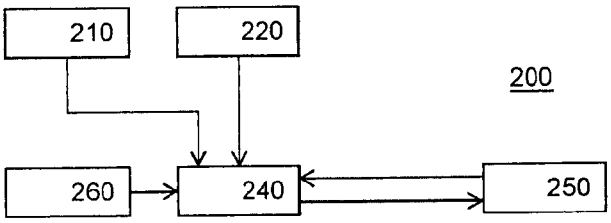

FIGURA 2

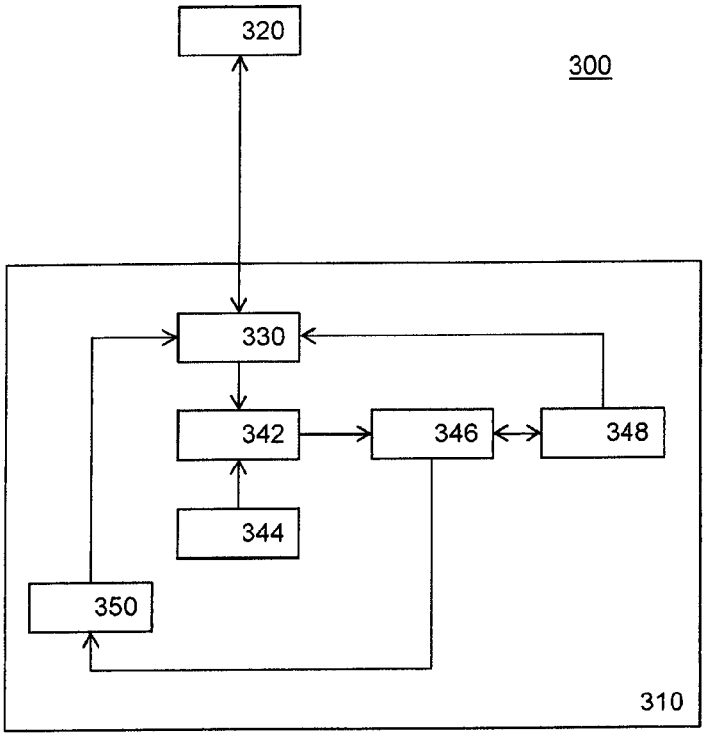

FIGURA 3

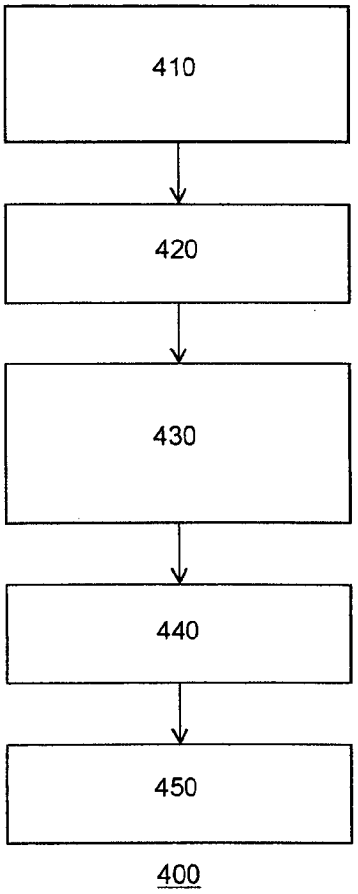

FIGURA 4

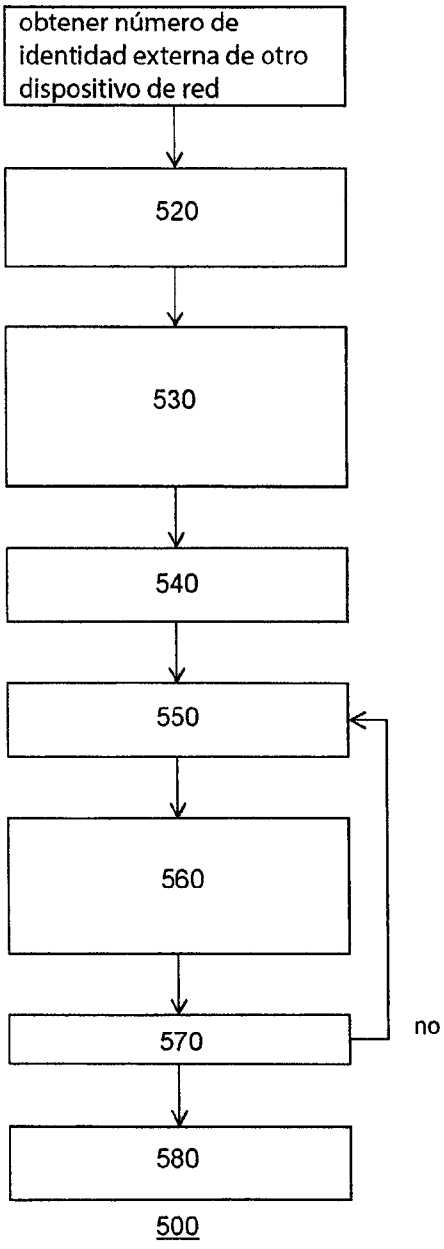

FIGURA 5

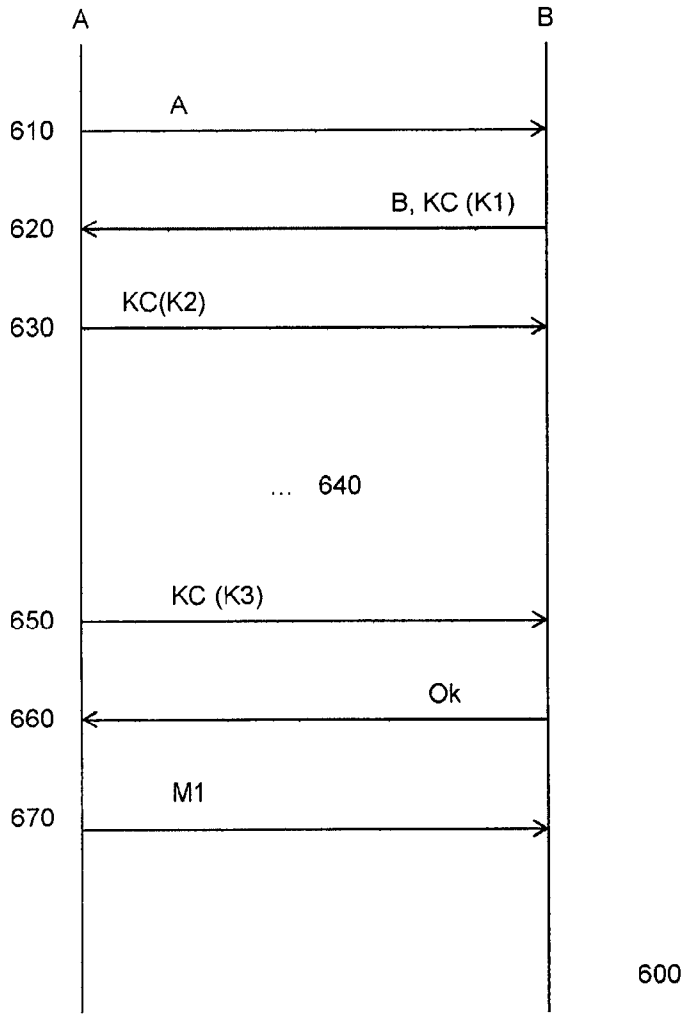

FIGURA 6