(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 556 027**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.03.2013 E 13713432 (6)**

(97) Fecha y número de publicación de la concesión europea: **28.10.2015 EP 2853057**

(54) Título: **Dispositivo de compartición de claves y sistema para la configuración del mismo**

(30) Prioridad:

21.05.2012 US 201261649464 P
21.05.2012 EP 12168710
12.06.2012 US 201261658475 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.01.2016

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 5
5656 AE Eindhoven, NL

(72) Inventor/es:

GARCIA MORCHON, OSCAR;
TOLHUIZEN, LUDOVICUS MARINUS GERARDUS MARIA;
GUTIERREZ, JAIME;
KUMAR, SANDEEP SHANKARAN y
GOMEZ, DOMINGO

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Dispositivo de compartición de claves y sistema para la configuración del mismo

Campo de la invención

La invención se refiere a un procedimiento de configuración de un dispositivo de red para la compartición de claves, comprendiendo el procedimiento generar material de claves locales para el dispositivo de red, lo que comprende obtener en forma electrónica un número de identidad para el dispositivo de red, determinar, usando un dispositivo de manipulación polinómica, un polinomio uni-variado a partir de un polinomio bi-variado, sustituyendo el número de identidad en el polinomio bi-variado, y almacenando electrónicamente el material de claves locales generado en el dispositivo de red.

La invención se refiere además a un procedimiento para que un primer dispositivo de red determine una clave compartida, siendo la clave una clave criptográfico, comprendiendo el procedimiento obtener material de claves locales para el primer dispositivo de red en forma electrónica, comprendiendo el material de claves locales un polinomio uni-variado, obtener un número de identidad para un segundo dispositivo de red, siendo el segundo dispositivo de red distinto al primer dispositivo de red, sustituir el número de identidad del segundo dispositivo de red en el polinomio uni-variado y obtener la clave compartida a partir del mismo.

La invención se refiere además a un sistema para configurar un dispositivo de red para la compartición de claves, y a un dispositivo de red configurado para determinar una clave compartida.

Antecedentes de la invención

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 manera de lograr esto está descrita en el artículo de C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro y M. Yung, “Distribución de claves perfectamente segura para conferencias dinámicas”, Notas de Conferencia Springer en Matemática, Vol. 740, págs. 471 a 486, 1993 (mencionado como ‘Blundo’).

Supone una autoridad central, también mencionada como la autoridad de la red o el Tercero Fiable (TTP), que genera un polinomio bi-variado simétrico f(x, y), con coeficientes en el campo finito F con p elementos, en donde p es un número primo o una potencia de un número primo. Cada dispositivo tiene un número de identidad en F y está dotado de material de claves locales por el TTP. Para un dispositivo con identificador η, el material de claves locales son los coeficientes del polinomio f(η, y).

Si un dispositivo η desea comunicarse con el dispositivo η’, usa su material de claves para generar la clave K(η, η’) = f(η, η’). Como f es simétrico, se genera la misma clave.

Un problema de este esquema de compartición de claves tiene lugar si un atacante conoce el material de claves de t+1 o más dispositivos, en donde t es el grado del polinomio bi-variado. El atacante puede luego reconstruir el polinomio f(x, y). En ese momento, la seguridad del sistema está completamente destruida. Dados los números de identidad de dos dispositivos cualesquiera, el atacante puede reconstruir la clave compartida entre este par de dispositivos.

Se hace referencia al artículo “Un esquema multi-polinómico basado en permutaciones para el establecimiento de claves de a pares en redes de sensores” por los autores Song Guo, Victor Leung y Zhuzhong Qian, Conferencia Internacional del IEEE sobre Comunicaciones, 2010. Presenta un esquema multi-polinómico basado en permutaciones para el establecimiento de claves de a pares en redes de sensores inalámbricos. Distinto a Blundo, el esquema presentado en Song no da a cada nodo solamente una prorrata de un polinomio simétrico, sino un grupo de prorratas permutadas.

Sumario de la invención

Sería ventajoso tener un procedimiento mejorado para establecer una clave compartida entre dos dispositivos de red. Se proporcionan un procedimiento de configuración de un dispositivo de red para la compartición de claves y un procedimiento para que un dispositivo de red determine una clave compartida.

El procedimiento de configurar un dispositivo de red para la compartición de claves comprende obtener en forma electrónica un módulo privado, un módulo público y un polinomio bi-variado con coeficientes enteros, la representación binaria del módulo público y la representación binaria del módulo privado son los mismos en al menos los bits consecutivos de longitud de la clave; generar material de claves locales para el dispositivo de red, lo que comprende obtener en forma electrónica un número de identidad para el dispositivo de red, determinar, usando un dispositivo de manipulación polinómica, un polinomio uni-variado a partir del polinomio bi-variado sustituyendo el

número de identidad en el polinomio bi-variado, reducir, módulo el módulo privado, el resultado de la sustitución y almacenar electrónicamente el material de claves locales generado en el dispositivo de red. En una realización, la generación de material de claves locales para el dispositivo de red comprende generar un número ofuscante, p. ej., usando un generador electrónico de números aleatorios y sumar, usando un dispositivo de manipulación polinómica, el número ofuscante a un coeficiente del polinomio uni-variado, para obtener un polinomio uni-variado ofuscado, comprendiendo el material de claves locales generado el polinomio uni-variado ofuscado. Puede ser ofuscado más de un coeficiente, preferiblemente, siendo ofuscados de forma distinta los coeficientes distintos. En una realización, la generación de material de claves locales para el dispositivo de red comprende generar múltiples números ofuscantes, p. ej., usando el generador electrónico de números aleatorios, y sumar, usando el dispositivo de manipulación polinómica, cada número ofuscante, entre los múltiples números ofuscantes, a un respectivo coeficiente entre los coeficientes del polinomio uni-variado, para obtener un polinomio uni-variado ofuscado. En una realización se suma a cada coeficiente del polinomio uni-variado un número ofuscado.

El polinomio bi-variado puede o no ser simétrico. Si el polinomio, o los polinomios, uni-variados son simétricos, dos dispositivos de red cualesquiera pueden obtener una clave compartida. Es interesante que, usando un polinomio bi-variado asimétrico, o uno o más polinomios bi-variados asimétricos, entre múltiples polinomios bi-variados, como material básico de la formación de claves, se permite asimilar la creación de dos grupos de dispositivos, tal como dispositivos; dos dispositivos pertenecientes al mismo grupo no pueden generar una clave común, pero dos dispositivos en distintos grupos sí pueden.

El añadido de la ofuscación es una etapa optativa. Sin la ofuscación, se obtiene todavía la protección contra ataques, porque la obtención del material de claves locales usa un módulo privado que es distinto al módulo público; la relación matemática que estaría presente al trabajar, digamos, en un único campo finito es perturbada. Esto significa que ya no valen las herramientas matemática usuales para analizar polinomios, p. ej., el álgebra finita. Por otra parte, debido a que los módulos privado y público se solapan en un cierto número de bits consecutivos, es probable que dos dispositivos de red que tengan material de claves locales puedan obtener la misma clave compartida. La seguridad puede ser aumentada sumando uno o más números ofuscantes a coeficientes del polinomio uni-variado, para obtener un polinomio uni-variado ofuscado. La etapa de sumar números ofuscantes, sin embargo, es optativa, y puede ser omitida. Añadir ofuscación o no es un compromiso entre la oportunidad de obtener correctamente una clave compartida y la seguridad adicional.

El módulo público es para usar en el dispositivo de red. El procedimiento de configuración de un dispositivo de red para la compartición de claves puede comprender dejar el módulo público disponible para el dispositivo de red, p. ej., almacenando el módulo público junto con el material de claves locales.

El procedimiento de determinación de una clave compartida para un primer dispositivo de red, siendo la clave una clave criptográfica, comprende obtener material de claves locales para el primer dispositivo de red en forma electrónica, comprendiendo el material de claves locales un polinomio uni-variado, posiblemente ofuscado, obtener un número de identidad para un segundo dispositivo de red, siendo el segundo dispositivo de red distinto al primer dispositivo de red, sustituir el número de identidad del segundo dispositivo de red en el polinomio uni-variado ofuscado, reducir el resultado de la sustitución, módulo el módulo público, seguido por una reducción módulo un módulo de clave, y obtener la clave compartida a partir del resultado de la reducción módulo el módulo de clave. En una realización, p. ej., el procedimiento comprende reducir el resultado de la sustitución módulo el módulo público, dividiendo el resultado entre una potencia de dos, y reducir, módulo un módulo de clave.

Cualquier par de dos dispositivos de red, entre los múltiples dispositivos de red que pueden tener cada uno un número de identidad y material de claves locales generado para el número de identidad, son capaces de negociar una clave compartida con pocos recursos. Los dos dispositivos de red necesitan solamente intercambiar sus números de identidad, que no necesariamente deben mantenerse en secreto, y realizar cálculos polinómicos. El tipo de cálculos necesarios no requiere amplios recursos de cálculo, lo que significa que este procedimiento es adecuado para tipos de aplicaciones de bajo coste y gran volumen.

Si el material de claves locales ha sido obtenido a partir de un polinomio simétrico, esto permite a ambos dispositivos de red, en un par de dispositivos de red, obtener la misma clave compartida. Si se ha sumado un número ofuscante al material de claves locales, la relación entre el material de claves locales y el material básico de formación de claves ha sido perturbada. La relación que estaría presente entre el polinomio uni-variado no ofuscado y el polinomio bi-variado simétrico ya no está presente. Esto significa que el ataque directo a un esquema de ese tipo ya no funciona.

Incluso si no se ha usado ninguna ofuscación, se mantiene la dificultad del ataque, porque el módulo público y el módulo (o módulos) privados no son iguales. La reducción módulo el módulo público aumenta la posibilidad de obtener la misma clave compartida, incluso sin ofuscación.

En una realización, la representación binaria del módulo público y la representación binaria del módulo privado son la misma, en al menos los (b) bits consecutivos de la longitud de la clave. Obsérvese que pueden ser usados múltiples módulos privados; pueden ser escogidos de modo que la representación binaria de uno cualquiera de los

múltiples módulos privados del módulo público, y la representación binaria de los módulos privados, sea la misma en al menos los (*b*) bits consecutivos de la longitud de la clave. Para cada módulo privado de los múltiples módulos privados, se escoge un polinomio bi-variado, optativamente simétrico, con coeficientes enteros, para obtener múltiples polinomios bi-variados, y optativamente simétricos.

Debido a que la obtención del material de claves locales usa un módulo privado que es distinto al módulo público, la relación matemática que estaría presente al operar, digamos, en un único campo finito se perturba. Esto significa que las herramientas matemáticas usuales para analizar polinomios, p. ej., el álgebra finita, ya no valen. En el mejor de los casos, un atacante puede usar estructuras mucho menos eficaces, tales como cuadrículas. Además, al obtener la clave compartida se combinan dos operaciones de módulo, que no son compatibles en el sentido matemático usual; por lo que se evita la estructura matemática en dos lugares. El procedimiento permite la generación directa de claves de a pares, y es resistente a la captura de un número muy alto, p. ej., del orden del 10^5 o incluso más alto, de dispositivos de red. Por otra parte, debido a que los módulos privado y público se solapan en un cierto número de bits consecutivos, es probable que dos dispositivos que tienen material de claves locales sean capaces de obtener la misma clave compartida.

Una perspectiva específica del inventor fue que el módulo público no necesariamente debe ser un número primo. En una realización, el módulo público es compuesto. Además, no hay ningún motivo por el cual el módulo público debería ser un número de bits 'todos unos', p. ej., un número que consiste solamente en bits 1, en su representación binaria. En una realización, el módulo público no es una potencia de dos menos 1. En una realización, la representación binaria del módulo público comprende al menos un bit cero (sin contar los ceros iniciales, es decir, la representación binaria del módulo público comprende al menos un bit cero menos significativo que el bit más significativo del módulo público). En una realización, el módulo público es una potencia de dos menos 1 y compuesto.

En una realización, el módulo público es mayor que dichos uno o más módulos privados.

En una realización, al menos los bits consecutivos de la longitud de clave de la representación binaria del módulo público, menos el módulo privado, son todos bits cero. Esta diferencia debería ser evaluada usando la representación numérica con signo del módulo público, menos el módulo privado, y no la representación del complemento a dos. Alternativamente, se puede requerir que al menos los bits consecutivos de longitud de clave de la representación binaria del valor absoluto del módulo público, menos el módulo privado, sean todos bits cero. Hay un conjunto de (b) posiciones consecutivas de la longitud de clave, en las cuales la representación binaria del módulo público concuerda con la representación binaria de todos los módulos privados.

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

Se permite que un módulo privado, entre múltiples módulos privados, sea igual al módulo público; sin embargo, si se usa solamente un módulo privado, entonces esto es indeseable.

Es deseable que los módulos privados introduzcan suficiente no linealidad. En una realización, hay un conjunto de posiciones consecutivas de bits en las cuales el módulo público difiere de cada módulo privado. Además, también se puede imponer que los módulos privados difieran entre sí; una comparación de a pares de la representación binaria del módulo privado también puede diferir en al menos un bit en un conjunto de, digamos, al menos la longitud de la clave, de bits consecutivos, siendo el conjunto igual para todos los módulos privados y, posiblemente, también el mismo para los módulos públicos.

El dispositivo de red puede ser un dispositivo electrónico equipado con comunicación electrónica y medios de cálculo. El dispositivo de red puede ser adosado, p. ej., en forma de una etiqueta RFID, a cualquier objeto no electrónico. Por ejemplo, este procedimiento sería adecuado para la 'Internet de los objetos'. Por ejemplo, los objetos, en particular, los objetos de bajo coste, pueden ser equipados con etiquetas de radio a través de las cuales puedan comunicarse, p. ej., puedan ser identificados. Tales objetos pueden ser inventariados mediante medios electrónicos, tal como un ordenador. Los elementos robados o rotos serían fácilmente rastreados y localizados. Una aplicación especialmente prometedora es una lámpara que comprende un dispositivo de red configurado para determinar una clave compartida. Una lámpara de ese tipo puede comunicar con seguridad su estado; una lámpara de ese tipo podrían ser controlada con seguridad, p. ej., encendida y / o apagada. Un dispositivo de red puede ser uno de múltiples dispositivos de red, comprendiendo cada uno un comunicador electrónico para enviar y recibir un número de identidad, y para enviar un mensaje de estado electrónico, y comprendiendo cada uno un circuito integrado configurado para obtener una clave compartida, siguiendo un procedimiento de acuerdo a la invención.

En una realización, el procedimiento en la invención puede ser usado como un procedimiento criptográfico para protocolos de seguridad tales como IPSec, (D)TLS, HIP o ZigBee. En particular, un dispositivo que usa uno de esos protocolos está asociado a un identificador. Un segundo dispositivo que desea comunicarse con el primer dispositivo

puede generar una clave común de a pares con el primer dispositivo, dado su identificador, y la clave de a pares (o una clave obtenida a partir de esto por medio, p. ej., de una función de obtención de claves) puede ser usada en un procedimiento de los protocolos anteriores, en base a la clave pre-compartida. En particular, el identificador de un dispositivo, según lo definido en esta invención, puede ser una dirección de red tal como la dirección corta de ZigBee, una dirección de IP o el identificador de anfitrión. El identificador también puede ser la dirección de IEEE de un dispositivo o una cadena de bits de propiedad industrial, asociada al dispositivo de modo que un dispositivo reciba algún material de formación de claves locales, asociada a la dirección de IEEE durante la fabricación.

La obtención de una clave compartida puede ser usada por muchas aplicaciones. Habitualmente, la clave compartida será una clave simétrica criptográfica. La clave simétrica puede ser usada para la confidencialidad, p. ej., los mensajes salientes o entrantes pueden ser cifrados con la clave simétrica. Solamente un dispositivo con acceso a ambos números de identidad y a uno de los dos materiales de claves locales (o acceso al material básico de claves) podrá descifrar las comunicaciones. La clave simétrica puede ser usada para la autenticación, p. ej., los mensajes salientes o entrantes pueden ser autenticados con la clave simétrica. De esta manera, puede ser validado el origen del mensaje. Solamente un dispositivo con acceso a ambos números de identidad, y a uno de los dos materiales de claves locales (o acceso al material de claves básicas), podrá crear mensajes autenticados.

El procedimiento de configuración de un dispositivo de red para la compartición de claves será habitualmente ejecutado por una autoridad de la red, p. ej., un tercero fiable. La autoridad de la red puede obtener el material necesario, p. ej., el material de claves básicas, desde otro origen, pero también puede generar esto por sí mismo. Por ejemplo, el módulo público puede ser generado. Por ejemplo, el módulo privado puede ser generado, incluso si el módulo público es un parámetro del sistema y está recibido.

En una realización, el módulo público N se escoge de modo que satisfaga $2^{(a+2)b-1} \leq N \leq 2^{(a+2)b}-1$, en donde *a* representa el grado del polinomio bi-variado y b representa la longitud de clave. Por ejemplo, en una realización $N = 2^{(a+2)b}-1$. La operación de módulo para la última opción puede ser implementada de manera particularmente eficaz.

Tener un módulo público fijo tiene la ventaja de que no necesariamente debe ser comunicado a los dispositivos de red, sino que puede ser integrado, p. ej., con su software de sistema. En particular, el módulo público puede ser escogido usando un generador de números aleatorios.

El módulo público, y el privado, pueden ser representados como una cadena de bits. También pueden ser abreviados, usando cada estructura matemática específica. Por ejemplo, en lugar de almacenar un módulo privado, también se puede almacenar su diferencia con respecto al módulo público, que es mucho más corta.

Tener un módulo privado escogido de manera tal que un número '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 probabilidad de que una clave compartida de un primer dispositivo de red, de un par de dispositivos de red, esté cerca de la clave compartida obtenida en un segundo dispositivo de red del par de dispositivos de red; es decir, la representación binaria del módulo privado tiene los mismos bits en las posiciones menos significativas de la 'longitud de clave' que la representación binaria del módulo público. Por ejemplo, si la longitud de clave es 64, puede escogerse un módulo privado restando un múltiplo de 2^64 al módulo público. En una realización, el módulo público, menos un módulo privado, dividido entre dos a la potencia de la longitud de clave es menor que dos a la potencia de la longitud de clave.

En una realización, los múltiples módulos privados se obtienen o se generan en forma electrónica, para cada módulo privado de los múltiples módulos privados se escoge un polinomio bi-variado simétrico con coeficientes enteros, para obtener múltiples polinomios bi-variados simétricos, de modo que a cada módulo privado corresponda un polinomio bi-variado simétrico. La determinación del polinomio bi-variado comprende sustituir el número de identidad en cada uno de los múltiples polinomios bi-variados simétricos, reduciendo, módulo un módulo privado entre los múltiples módulos privados correspondientes a dicho polinomio bi-variado simétrico, y sumando entre sí los múltiples resultados de las múltiples reducciones. Tener múltiples polinomios bi-variados simétricos para distintos módulos aumenta la seguridad, porque se mezclan adicionalmente estructuras incompatibles. Habitualmente, los módulos privados son distintos. Tener múltiples módulos privados complica adicionalmente el análisis, incluso más si las correspondientes estructuras algebraicas son muy distintas; por ejemplo, escogiéndolos como primos entre sí, en particular, primos entre sí de a pares, e incluso más en particular escogiéndolos como primos distintos.

Tener un módulo privado distinto y, en particular, múltiples módulos privados, complicará el análisis. Para aumentar además la seguridad, son posibles controles adicionales sobre los coeficientes. En una realización, la autoridad que suma entre sí los múltiples polinomios uni-variados resultantes de las múltiples reducciones verifica si el valor de cada uno de los coeficientes resultantes es demasiado pequeño o demasiado grande, p. ej., menos que un umbral mínimo o por encima de un umbral máximo. Esto mejora la seguridad aún más porque, en cualquiera de los dos casos, un atacante podría averiguar los componentes de las múltiples reducciones si son demasiado grandes o demasiado pequeños. Por ejemplo, si el valor de un coeficiente, resultante después de la suma, es igual a 1 y hay solamente dos polinomios uni-variados, entonces un atacante sabe que el correspondiente coeficiente asociado al primer polinomio es 1 y el asociado al segundo polinomio es 0, o al contrario. En particular, la autoridad que genera

el material de claves locales para un dispositivo puede verificar si el valor de cada uno de los coeficientes resultantes del material de formación de claves locales es al menos un 'valor mínimo' y a lo sumo un 'valor máximo'. Esta comprobación puede omitirse, en particular, si el módulo público está relativamente cerca de todos los módulos privados y todos los elementos del material de claves están entre 0 y N-1. Si el TTP es capaz de asignar números de identidad, también podría asignar otro número de identidad al dispositivo, si el TTP detecta coeficientes pequeños o grandes.

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

El módulo público puede ser tanto más grande como más pequeño que el módulo privado. En una realización, la representación binaria del módulo público, menos el módulo privado, tiene al menos todos ceros en los bits de la longitud de clave. Los bits cero, al menos bits cero de la longitud de clave, son consecutivos y pueden estar presentes en cualquier punto en la representación binaria. Tener una cadena de bits cero en la diferencia entre el módulo público y el módulo privado evita que la ofuscación se lleve demasiado lejos. En una realización, hay un parámetro entero 's', de modo que los bits menos significativos de la longitud de clave del módulo público, menos el módulo privado, dividido entre dos a la potencia s, sean todos cero. El parámetro 's' es el mismo para todos los módulos privados.

Por ejemplo, se puede definir un divisor de cadena de bits cero que sea una potencia de dos, de modo que sea cada módulo privado específico tal que los (b) bits de la longitud de clave, de la representación binaria del módulo público, menos el módulo privado específico, dividido entre el divisor de cadena de bits cero, sean todos bits cero. Si los bits menos significativos son ceros, puede tomarse el divisor de cadena de bits cero como igual a 1. En una realización, el divisor de cadena de bits cero es mayor que 1. La división entre una potencia de dos ha de ser interpretada como una división entera, dando el mismo resultado que un desplazamiento de los bits en la dirección de dichos bits menos significativos. Se ignora todo resto de la división.

Para generar la clave compartida de bits de la longitud de clave, los dispositivos de red aplican primero una etapa adicional de división. El primer dispositivo de red evalúa el material de formación de claves en cuanto al número de identidad del segundo dispositivo, módulo los módulos públicos, dividiendo entre 2^s y reduciendo módulo dos a la potencia de la longitud de clave. Obsérvese que esto es equivalente a aplicar primero un módulo 2^(s + longitud de clave) después del módulo público, y dividir luego entre 2^s. Aquí, "dividir" incluye redondear hacia abajo.

En una realización, el módulo privado se genera usando un generador de números aleatorios. En una realización, los múltiples módulos privados se generan de modo que sean primos entre sí de a pares. Por ejemplo, los múltiples módulos privados pueden ser generados verificando iterativamente, para cada nuevo módulo privado, que son primos entre sí de a pares y, si no es así, descartando el último módulo privado generado. Una realización comprende generar iterativamente un módulo candidato, usando el generador de números aleatorios, de modo que los (*b*) bits consecutivos de la longitud de clave, de la representación binaria del módulo público, menos el módulo candidato, sean todos bits cero, p. ej., los bits de la longitud de clave menos significativos, hasta que el módulo candidato satisfaga una prueba de condición de primo, usando un dispositivo de prueba de condición de primo, en el que el módulo candidato así obtenido, que satisfaga la prueba de condición de primo, sea usado como el módulo privado. La prueba de condición de primo puede ser, p. ej., la prueba de condición de primo de Miller-Rabin o la prueba de condición de primo de Solovay-Strassen.

Un polinomio bi-variado simétrico en variables *x* e *y* de grado *a* tiene solamente monomios de la forma $x^j y^j$, con $i \leq a$, $j \leq a$. Además, el coeficiente correspondiente a $x^j y^j$ es el mismo que el coeficiente de $x^j y^j$. Esto puede ser usado para reducir el número de coeficientes almacenados, en alrededor de la mitad. Obsérvese que se usa una definición más informal del grado. Definimos el grado de un monomio como el máximo grado de las variables en el monomio. Por lo que el grado de $x^j y^j$ es max(i, j), es decir, $i \leq a$, $j \leq a$. Así, por ejemplo, lo que llamamos un polinomio de grado 1 tiene una forma general a + bx + cy + dxy (obsérvese que, dado que se consideran solamente polinomios simétricos, tenemos b = c). Obsérvese que, si se desea, se pueden poner restricciones adicionales sobre el polinomio bi-variado, incluyendo, p. ej., que solamente se usen monomios con $i + j \leq a$, pero esto no es necesario.

En una realización, el polinomio bi-variado simétrico es generado por la autoridad de la red. Por ejemplo, el polinomio bi-variado simétrico puede ser un polinomio bi-variado simétrico aleatorio. Por ejemplo, los coeficientes pueden ser seleccionados como números aleatorios, usando un generador de números aleatorios.

Aunque la ofuscación usada aumenta en gran medida la resistencia ante el ataque, en particular, ante ataques de colusión en los que se combinan múltiples materiales de claves locales, tiene un inconveniente potencial. Algunas veces, la clave compartida, obtenida por el primer dispositivo de red, no es idéntica en todos los bits a la clave compartida obtenida por el segundo dispositivo de red. Esto se debe, principalmente, al desajuste en los bits de acarreo después de la suma de los coeficientes de ofuscación. Otro motivo es el efecto faltante de los efectos modulares de cada uno de los módulos privados durante la generación de la clave que afecta a los bits de acarreo generados. Aunque es una molestia, este inconveniente puede ser resuelto de diversas maneras. Escogiendo la ofuscación con más cuidado, la probabilidad de una diferencia y, en particular, la probabilidad de una gran diferencia

pueden ser reducidas significativamente. Además, se halló que es probable que las diferencias, si hubiera alguna, estén situadas en los bits menos significativos de las claves generadas. Luego, eliminando uno o más de los bits menos significativos, puede aumentarse la probabilidad de una clave idéntica compartida. Por ejemplo, en una realización, el procedimiento de determinación de una clave compartida comprende determinar si el primer dispositivo de red y el segundo dispositivo de red han obtenido la misma clave compartida y, si no es así, obtener una clave compartida adicional a partir del resultado de la reducción, módulo el módulo de la clave. Pueden obtenerse claves compartidas adicionales hasta que se halle una que sea igual en ambos lados. Si quedan menos de un número umbral de bits en la clave compartida, el procedimiento puede ser terminado. Para algunas aplicaciones puede aceptarse simplemente que algún porcentaje de los dispositivos de red no puedan comunicarse. Por ejemplo, en redes inalámbricas ad-hoc, en las cuales un mensaje puede ser encaminado a lo largo de diversas rutas, no hay ninguna pérdida de conectividad si algunos de los dispositivos de red no son capaces de comunicarse.

Obsérvese que, sin ofuscación, también puede ocurrir que la clave compartida, obtenida por el primer dispositivo de red, no sea idéntico en todos los bits a la clave compartida obtenida por el segundo dispositivo de red, aunque la probabilidad de esto es menor que en el caso con ofuscación.

En una realización, se eliminan un cierto número de los bits menos significativos de la clave compartida; por ejemplo, el número de bits eliminados puede ser 1, 2 o más, 4 o más, 8 o más, 16 o más, 32 o más, 64 o más. Eliminando más de los bits menos significativos, se reduce la probabilidad de tener claves que no sean iguales; en particular, puede reducirse hasta cualquier umbral deseado. La probabilidad de que las claves compartidas sean iguales puede ser calculada siguiendo las relaciones matemáticas; también puede ser determinada por experimentos.

Además, la elección de números ofuscantes puede ser controlada; en una realización, la gama desde la cual se escoge un número ofuscante se reduce para coeficientes correspondientes a monomios de mayor grado. En particular, se puede requerir que $|\varepsilon_{A,i}| < 2^{(a+1-i)b}$, en donde $\in_{A,i}$ indica el número ofuscante para el i-ésimo monomio, *i* indica el grado del monomio correspondiente al coeficiente, *a* representa el grado del polinomio bi-variado y *b* representa la longitud de la clave. *A* representa el dispositivo de red para el cual se genera el material de claves locales. En una realización, se genera un número ofuscante para cada coeficiente, p. ej., usando la fórmula anterior. Una ofuscación distinta puede ser aplicada para distintos dispositivos de red. Por ejemplo, incluso si hay 3 o más dispositivos de red, entonces pueden ser generados distintos números ofuscantes para cada dispositivo de red.

Obsérvese que el número ofuscante puede estar restringido a números positivos, pero esto no es necesario: los números ofuscantes pueden ser negativos. En una realización, los números ofuscantes se generan usando un generador de números aleatorios. Múltiples números ofuscantes pueden ser generados y sumados a coeficientes del polinomio uni-variado para obtener el polinomio uni-variado ofuscado. Uno o más de, y preferiblemente hasta todos, los coeficientes del polinomio uni-variado pueden ser ofuscados de esta manera.

El número de bits en el número de identidad para el dispositivo de red se escoge usualmente como menor o igual a la longitud de la clave. El número de identidad puede ser una cadena de bits, digamos, una cadena de bits de 32 o 64, o más larga. La longitud de clave puede ser de 32 o más, 48 o más, 64 o más, 96 o más, 128 o más, 256 o más. La longitud de clave puede ser escogida como algún número de bits más alto, a fin de reducir un número correspondiente de bits menos significativos de la clave compartida determinada. Por otra parte, en una realización, la longitud del número de identidad es más larga que la longitud de la clave. En este caso, el efecto de las operaciones modulares puede llevar a un mayor efecto sobre los bits menos significativos de los bits de la longitud de clave de la clave generada, por lo que esos bits podrían no ser iguales para un par de dispositivos que desean generar una clave común. Tener una mayor longitud para el identificador puede tener, sin embargo, un efecto positivo en la seguridad, dado que se mezclan entre sí más bits al hacer los cálculos correspondientes.

Un dispositivo de manipulación polinómica puede ser implementado en software que se ejecuta en un ordenador, digamos, en un circuito integrado. Un dispositivo de manipulación polinómica puede ser implementado muy eficazmente en hardware. También es posible una combinación. Por ejemplo, un dispositivo de manipulación polinómica puede ser implementado manipulando formaciones de coeficientes que representan a los polinomios.

El almacenamiento electrónico del material de claves locales generado en el dispositivo de red puede ser implementado enviando electrónicamente el material de claves locales generado al dispositivo de red, p. ej., usando una conexión cableada, o usando una conexión inalámbrica y teniendo el material de claves locales generado almacenado en el dispositivo de red. Esto puede hacerse durante la fabricación o la instalación, p. ej., durante las pruebas, de un circuito integrado en el dispositivo de red. El equipo de pruebas puede comprender, o estar conectado con, la autoridad de la red. Esto también puede ocurrir después de la unión exitosa de un dispositivo con una red de operaciones (es decir, después del acceso a red o el auto-arranque). En particular, el material de claves locales puede ser distribuido como parte de los parámetros operativos de red.

La obtención de material de claves locales para el primer dispositivo de red en forma electrónica puede hacerse recibiendo electrónicamente el material de claves locales desde un sistema, para configurar un dispositivo de red para la compartición de claves, p. ej., un dispositivo de autoridad de red. La obtención de material de claves locales

también puede hacerse extrayendo el material de claves locales desde un almacén local, p. ej., una memoria tal como la memoria flash.

La obtención de un número de identidad para un segundo dispositivo de red puede hacerse recibiendo el número de identidad desde el segundo dispositivo de red, p. ej., directamente desde el segundo dispositivo de red, p. ej., recibiendo inalámbricamente desde el segundo dispositivo de red.

El módulo público y el módulo clave pueden ser almacenados en un dispositivo de red. También pueden ser recibidos desde una autoridad de red. También pueden estar implícitos en el software del dispositivo de red. Por ejemplo, en una realización el módulo clave es una potencia de dos. La reducción módulo un módulo clave de ese tipo puede hacerse descartando todos los bits excepto los bits menos significativos de la longitud de clave. Primero se reduce el resultado de la sustitución, módulo el módulo público, que es luego adicionalmente reducido módulo el módulo clave.

Aunque no se requiere, el módulo público y el módulo clave pueden ser primos entre sí. Esto puede lograrse haciendo que el módulo público sea impar y que el módulo clave sea una potencia de 2. En cualquier caso, se evita que el módulo clave divida al módulo público, ya que entonces podría omitirse la reducción módulo el módulo público.

El procedimiento para el acuerdo de clave entre dos dispositivos puede usar como material básico de formación de claves un cierto número de polinomios bi-variados. Se puede usar el procedimiento para el acuerdo de clave usando x acuerdos entre x partes, usando polinomios de x variables como material básico de formación de claves. En esta extensión, el tercero fiable evalúa los polinomios de x variables en una variable en el anillo correspondiente, y los polinomios resultantes de x-1 variables se suman luego sobre los enteros que generan el material de claves locales almacenado en un dispositivo. Cuando x dispositivos necesitan acordar una clave, un dispositivo evalúa su material de claves locales en los identificadores de los otros x-1 dispositivos. Por ejemplo, se puede usar polinomios multi-variados en un procedimiento de configuración de un dispositivo de red para la compartición de claves, comprendiendo el procedimiento obtener en forma electrónica un módulo privado (p_1), un módulo público (N) y un polinomio multi-variado (f_1) con coeficientes enteros; la representación binaria del módulo público y la representación binaria del módulo privado son la misma en al menos los (b) bits consecutivos de la longitud de clave; generar material de claves locales para el dispositivo de red, que comprende obtener en forma electrónica un número de identidad (A) para el dispositivo de red; determinar, usando un dispositivo de manipulación polinómica, un polinomio a partir del polinomio multi-variado, sustituyendo el número de identidad en el polinomio multi-variado; reducir, módulo el módulo privado, el resultado de la sustitución; y almacenar electrónicamente el material de claves locales generado en el dispositivo de red. El polinomio obtenido por el dispositivo de manipulación polinómica es de una variable menos. Es conveniente para la compartición de clave que la multi-variación sea simétrica en todas las variables. Un procedimiento correspondiente para un primer dispositivo de red, para determinar una clave compartida, siendo la clave una clave criptográfica; comprendiendo el procedimiento obtener material de claves locales para el primer dispositivo de red en forma electrónica, comprendiendo el material de claves locales un polinomio, optativamente ofuscado; obtener un número de identidad para otros múltiples dispositivos de red, siendo el segundo dispositivo de red distinto al primer dispositivo de red; sustituir el número de identidad de los otros dispositivos de red en el polinomio, optativamente ofuscado; reducir el resultado de la sustitución, módulo el módulo público, y reducir, módulo un módulo clave, y obtener la clave compartida a partir del resultado de la reducción módulo el modulo clave. Obsérvese que después de sustituir todos los otros números de identidad, menos uno, el procedimiento se reduce a la situación en la cual se usa un polinomio uni-variado.

En una realización, un primer dispositivo de red recibe múltiples (n) materiales de claves locales, asociados al identificador del dispositivo. La clave generada entre este primer dispositivo y un segundo dispositivo se obtiene como la combinación (p. ej., concatenación) de las múltiples (n) claves obtenidas evaluando cada uno de los múltiples (n) materiales de claves locales del primer dispositivo en el identificador del segundo dispositivo. Esto permite el uso del procedimiento en paralelo.

El uso de polinomios bi-variados asimétricos como material básico de formación de claves, es decir, f(x, y) != f(y, x), permite asimilar la creación de dos grupos de dispositivos, tales como que los dispositivos en el primer grupo reciben KM(Id, y) y los dispositivos en el segundo grupo reciben KM(x, iD), siendo KM el material de claves locales almacenado en un dispositivo. Dos dispositivos pertenecientes al mismo grupo no pueden generar una clave común, pero dos dispositivos en distintos grupos sí pueden. Véase además Blundo.

El número de identidad de un dispositivo de red puede ser calculado como la función unidireccional de una cadena de bits que contiene información asociada al dispositivo. La función unidireccional puede ser una función de troceo criptográfico tal como SHA2 o SHA3. La salida de la función unidireccional puede ser truncada de modo que quepa en el tamaño del identificador. Alternativamente, el tamaño de la función unidireccional es más pequeño que el máximo tamaño de identificador.

En una realización, los polinomios simétricos implican un único monomio de la forma $<ax^iy^j>p_i$, donde $<>p$ represente la operación de 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 hay múltiples módulos privados, algunos pueden ser más grandes que el módulo privado y algunos pueden ser más pequeños.

En una realización del procedimiento de configuración de un dispositivo de red para la compartición de claves, el procedimiento comprende obtener en forma electrónica múltiples módulos privados (p_i) y múltiples polinomios bi-variados simétricos (f_i) con coeficientes enteros, de modo que haya un conjunto de posiciones consecutivas de longitud de clave (b), en las cuales la representación binaria del módulo público es la misma que la representación binaria de todos los módulos privados; generar material de claves locales para el dispositivo de red, lo que comprende obtener en forma electrónica un número de identidad (A) para el dispositivo de red; determinar, usando un dispositivo de manipulación polinómica, un polinomio uni-variado a partir de los múltiples polinomios bi-variados, sustituyendo el número de identidad en cada uno de los múltiples polinomios bi-variados; reducir, módulo un módulo privado de los múltiples módulos privados correspondientes a dicho polinomio bi-variado simétrico; y añadir los múltiples resultados de las múltiples reducciones, y generar un número ofuscante y añadir, usando un dispositivo de manipulación polinómica, el número ofuscante a un coeficiente del polinomio uni-variado, para obtener un polinomio uni-variado ofuscado, comprendiendo el material de claves locales generado el polinomio uni-variado ofuscado; y almacenar electrónicamente el material de claves locales generado en el dispositivo de red. Un polinomio bi-variado de los múltiples polinomios bi-variados (f_i) puede ser representado con coeficientes módulo el correspondiente módulo privado (p_i).

Más en general, el material básico de claves puede ser evaluado sobre cualquier anillo. Es posible usar polinomios de un monomio único tal como Ax^a, en cuyo caso puede usarse un grupo.

Un aspecto de la invención atañe a un sistema para configurar un dispositivo de red para la compartición de claves, p. ej., una autoridad de red, comprendiendo el sistema un obtenedor de materiales 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 bi-variado simétrico con coeficientes enteros; los bits de la longitud de clave de la representación binaria del módulo público, menos el módulo privado, son todos bits cero, posiblemente los bits menos significativos de la longitud de clave; un generador para generar material de claves locales para el dispositivo de red, que comprende un gestor de dispositivos de red para obtener en forma electrónica un número de identidad para el dispositivo de red, y para almacenar electrónicamente el material de claves locales generado en el dispositivo de red, y un dispositivo de manipulación polinómica para determinar un polinomio uni-variado a partir del polinomio bi-variado, sustituyendo el número de identidad en el polinomio bi-variado, reduciendo, módulo el módulo privado, el resultado de la sustitución.

Una realización del sistema comprende un generador de números ofuscantes, p. ej., un generador de números aleatorios, para generar un número ofuscante; el dispositivo de manipulación polinómica está configurado para añadir el número ofuscante a un coeficiente del polinomio uni-variado, para obtener un polinomio uni-variado ofuscado, comprendiendo el material de claves locales generado el polinomio uni-variado ofuscado.

Un aspecto de la invención atañe a un primer dispositivo de red, configurado para determinar una clave compartida, siendo la clave una clave criptográfica, y comprendiendo el primer dispositivo de red un obtenedor de materiales de claves locales, para obtener material de claves locales para el primer dispositivo de red en forma electrónica, comprendiendo el material de claves locales un polinomio uni-variado ofuscado, un receptor para obtener un número de identidad para un segundo dispositivo de red, siendo el segundo dispositivo de red distinto al primer dispositivo de red; un dispositivo de manipulación polinómica para sustituir el número de identidad del segundo dispositivo de red en el polinomio uni-variado ofuscado y reducir el resultado de la sustitución, módulo el módulo público, seguido por la reducción, módulo un módulo clave, siendo el módulo público y el módulo clave primos entre sí; y un dispositivo de obtención de claves para obtener la clave compartida a partir del resultado de la reducción módulo el módulo clave.

Un dispositivo de obtención de claves puede ser implementado como un ordenador, p. ej., un circuito integrado, ejecutando software, en hardware, en una combinación de los dos y similares, configurado para obtener la clave compartida a partir del resultado de la reducción módulo el módulo clave.

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

Múltiples dispositivos de red, teniendo cada uno un número de identidad y el correspondiente material de claves locales, pueden formar conjuntamente una red de comunicación configurada para la comunicación segura, p. ej., confidencial y / o autenticada, entre pares de dispositivos de red.

La generación de claves está basada en Identificadores y permite la generación de claves de a pares entre pares de dispositivos. Un primer dispositivo A puede apoyarse en un algoritmo que obtiene una clave a partir de material de claves locales y un número de identidad.

En una realización, 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 el cifrado de un mensaje y, optativamente, el mismo mensaje. El segundo dispositivo de red puede verificar el cifrado del mensaje. El mensaje puede ser fijo y estar presente en el segundo dispositivo, para evitar la necesidad de enviarlo. El mensaje puede ser aleatorio, u ocasional, etc., en cuyo caso puede ser enviado junto con el cifrado. El segundo dispositivo puede contestar con un mensaje que contiene una indicación si las claves coinciden. El segundo dispositivo también puede contestar con un mensaje propio de confirmación de clave. Si el primer dispositivo, o el segundo, descubre que las claves no son iguales, pueden iniciar un proceso de ecualización de clave, p. ej., borrando los bits menos significativos, etc.

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

Un procedimiento de acuerdo a la invención puede ser implementado en un ordenador como un procedimiento implementado por ordenador, o en hardware dedicado, o en una combinación de ambos. El código ejecutable para un procedimiento de acuerdo a la invención puede ser almacenado en un producto de programa de ordenador. Los ejemplos de productos de programa de ordenador incluyen dispositivos de memoria, dispositivos de almacenamiento óptico, circuitos integrados, servidores, software en línea, etc. Preferiblemente, el producto de programa de ordenador comprende medios de código de programa, no transitorio, almacenados en un medio legible por ordenador para realizar un procedimiento de acuerdo a la invención cuando dicho producto de programa es ejecutado en un ordenador.

En una realización preferida, el programa de ordenador comprende medios de código de programa de ordenador, adaptados para realizar todas las etapas de un procedimiento de acuerdo a la invención cuando el programa de ordenador es ejecutado en un ordenador. Preferiblemente, el programa de ordenador es realizado en un medio legible por ordenador.

Para completar, se menciona la solicitud internacional WO2010032161 con título “Un procedimiento para la comunicación segura en una red, un dispositivo de comunicación, una red y un programa de ordenador para el mismo”, que se refiere a un procedimiento para comunicaciones seguras en una red de comunicación.

Hay un cierto número de diferencias con respecto a esa solicitud, que incluyen: el uso de operaciones modulares, en particular, la combinación de operaciones modulares con módulos público y privado distintos, operaciones modulares repetidas, p. ej., una reducción módulo un módulo público, seguida por una reducción módulo un módulo clave, el uso de la ofuscación y el uso de polinomios enteros.

Se proporcionan un procedimiento de configuración de un dispositivo de red para la compartición de claves y un procedimiento para que un primer dispositivo de red determine una clave compartida. El procedimiento de configuración usa un módulo privado (p1), un módulo público (N) y un polinomio bi-variado (f1) con coeficientes enteros, y la representación binaria del módulo público y la representación binaria del módulo privado son la misma en al menos los (b) bits consecutivos de la longitud de clave. El material de claves locales para un dispositivo de red es generado sustituyendo un número de identidad en el polinomio bi-variado y reduciendo, módulo el módulo privado, el resultado de la sustitución para obtener un polinomio uni-variado. La seguridad puede ser aumentada añadiendo (440) uno o más números ofuscantes a los coeficientes del polinomio uni-variado, para obtener un polinomio uni-variado ofuscado. En una fase de uso, el dispositivo de red determina una clave criptográfica compartida, sustituyendo (530) el número de identidad de otro dispositivo de red en el polinomio uni-variado y reduciendo módulo el módulo público, y reduciendo módulo un módulo clave.

Breve descripción de los dibujos

Estos y otros aspectos de la invención son evidentes a partir de, y serán esclarecidos con referencia a, las realizaciones descritas a continuación en la presente memoria. En los dibujos,

la Figura 1 es un diagrama de bloques esquemáticos que lustra un generador de materiales de claves básicas,
la Figura 2 es un diagrama de bloques esquemáticos que ilustra un generador de materiales de claves locales,
la Figura 3 es un diagrama de bloques esquemáticos que ilustra una red de comunicación,
la Figura 4 es un diagrama de flujo esquemático que ilustra la generación de material de claves locales,
la Figura 5 es un diagrama de flujo esquemático que ilustra la generación de una clave compartida,
la Figura 6 es un diagrama esquemático de secuencias que ilustra la generación de una clave compartida.

Debería observarse que los elementos que tienen los mismos números de referencia en distintas Figuras tienen las mismas características estructurales y las mismas funciones, o son las mismas señales. Allí donde la función y / o la

estructura de un elemento de ese tipo ha sido explicado, no hay ninguna necesidad de una explicación repetida del mismo en la descripción detallada.

Lista de números de referencia:

100	un obtenedor de material de clave básica
110	un elemento de módulo público
112	un elemento de grado de polinomio
114	un elemento de longitud de clave
116	un elemento de número de polinomios
122	un gestor de módulos privados
124	un gestor de polinomios bi-variados simétricos
200	un generador de material de claves locales
210	un elemento de material público
220	un elemento de material privado
240	un dispositivo de manipulación de polinomios
250	un gestor de dispositivos de red
260	un generador de números ofuscantes
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 polinomios
344	un obtenedor de material de claves locales
346	un dispositivo de obtención de claves
348	un ecualizador de claves
350	un elemento criptográfico

Realizaciones detalladas

Si bien esta invención es susceptible de realización en muchas formas distintas, se muestran en los dibujos y serán descritas en detalle en la presente memoria, una o más realizaciones específicas, entendiéndose que la presente divulgación ha de ser considerada como ejemplar de los principios de la invención, y no como concebida para limitar la invención a las realizaciones específicas mostradas y descritas.

Más adelante se describe una realización del procedimiento de compartición de claves. El procedimiento tiene una fase de establecimiento y una fase de uso. La fase de establecimiento puede incluir etapas de iniciación y etapas de registro. Las etapas de iniciación no implican a los dispositivos de red.

Las etapas de iniciación seleccionan parámetros del sistema. Las etapas de iniciación pueden ser realizadas por el tercero fiable (TTP). Sin embargo, los parámetros del sistema pueden también ser considerados como dados por datos de entrada. En ese caso, el tercero fiable no necesita generarlos, y las etapas de iniciación pueden ser omitidas. Por ejemplo, el tercero fiable puede recibir los parámetros del sistema desde un fabricante de dispositivos. El fabricante de dispositivos puede haber realizado las etapas de iniciación para obtener los parámetros del sistema. Por comodidad de exposición, nos referiremos al tercero fiable como el realizador de las etapas de iniciación, teniendo en mente que esto no es necesario.

Etapas de iniciación

Se selecciona la longitud de clave deseada para la clave que será compartida entre dispositivos en la fase de uso; esta longitud de clave se menciona como '*b*'. Un valor típico para una aplicación de baja seguridad puede ser 64 u 80. Un valor típico para seguridad a nivel de consumidor puede ser 128. Las aplicaciones sumamente secretas pueden preferir 256 o valores incluso mayores.

Se selecciona el grado deseado; el grado controla el grado de ciertos polinomios. El grado será mencionado como '*a*', y es al menos 1. Una elección práctica para *a* es 2. Una aplicación más segura puede usar un valor mayor de *a*, digamos 3 o 4, o incluso mayor. Para una aplicación sencilla también es posible a = 1. El caso *a* = 1 está relacionado con el llamado 'problema del número oculto'; los valores mayores de "a" están relacionados con el problema extendido del número oculto, lo que confirma que estos casos son difíciles de resolver.

Se selecciona el número de polinomios. El número de polinomios será mencionado como '*m*'. Una elección práctica para *m* es 2. Una aplicación más segura puede usar un valor mayor de *m*, digamos, 3 o 4, o incluso mayor. Obsérvese que una aplicación de baja complejidad, digamos, para dispositivos acotados en recursos, puede usar *m* = 1.

Valores mayores de los parámetros de seguridad *a* y *m* aumentan la complejidad del sistema y aumentan en consecuencia su intratabilidad. Los sistemas más complicados son más difíciles de analizar y por tanto más resistentes al criptoanálisis.

En una realización, se selecciona un módulo público *N* que satisfaga $2^{(a+2)b-1} \leq N$ y, más preferiblemente, también $N \leq 2^{(a+2)b}-1$. Las cotas no son estrictamente necesarias; el sistema también podría usar un valor mayor / menor de N, aunque esa no es considerada como la mejor opción.

A menudo la longitud de la clave, el grado y el número de los polinomios estarán predeterminados, p. ej., por un diseñador del sistema, y proporcionados al tercero fiable como datos de entrada. Como elección práctica se 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, si $a = 2$, $b = 128$, entonces *N* puede ser $N = 2^{512}-1$. Escoger para *N* la cota superior o inferior del intervalo anterior tiene la ventaja del cálculo fácil. Para aumentar la complejidad se puede escoger un número aleatorio dentro de la gama para *N*.

Se seleccionan un cierto número de *m* módulos privados $p_1, p_2, ..., p_m$. Los módulos son enteros positivos. Durante las etapas de registro, cada dispositivo será asociado a un número de identidad. Cada módulo privado seleccionado es mayor que el mayor número de identidad usado. Por ejemplo, se puede acotar los números de identidad requiriendo que sean menores o iguales a $2^b - 1$, y que los módulos privados seleccionados sean mayores que $2^b - 1$. Cada número seleccionado satisface la siguiente relación $p_j = N + \gamma_j \cdot 2^b$. En donde los γ_j son enteros tales que $|\gamma_j| < 2^b$. Una manera práctica de seleccionar números que satisfagan este requisito es escoger un conjunto de m números aleatorios γ_j tales que $-2^b + 1 \leq \gamma_j \leq 2^b - 1$ y calcular los módulos privados seleccionados a partir de la relación $p_j = N + \gamma_j \cdot 2^b$. Puede admitirse tener los $|\gamma_j|$ un poco más grandes; sin embargo, puede ocurrir un problema en cuanto a que la operación modular vaya demasiado lejos, por lo que las claves compartidas podrían no ser iguales.

Para $m > 1$, el sistema es más complicado, y por tanto más seguro, dado que las operaciones de módulo para distintos módulos están combinadas, incluso aunque tales operaciones no sean compatibles en el sentido matemático usual. Por este motivo, es ventajoso escoger los módulos privados seleccionados como distintos de a pares.

Se genera un número de *m* polinomios bi-variados simétricos $f_1, f_2, ..., f_m$ de grados a_j. Todos los grados satisfacen $a_j \leq a$, y más preferiblemente, $a = MAX\{a_1, ..., a_m\}$. Una elección práctica es tomar cada polinomio de grado *a*. Un polinomio bi-variado es un polinomio de 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 los enteros módulo p_j, obtenido calculando en módulo p_j. Los enteros en módulo p_j forman un anillo finito con p_j elementos. En una realización, el polinomio f_j está representado con coeficientes desde 0 hasta $p_j - 1$. Los polinomios bi-variados pueden ser seleccionados al azar, p. ej., seleccionando coeficientes aleatorios dentro de estas cotas. Obsérvese que algunos de, o todos, los polinomios bi-variados pueden ser generados asimétricamente, lo que lleva a un sistema con dos grupos. Supondremos, para simplificar, que todos los polinomios seleccionados son simétricos.

La seguridad de la compartición de claves depende de estos polinomios bi-variados, ya que son el material de formación de claves básicas del sistema; por tanto, preferiblemente, se toman medidas estrictas para protegerlos, p. ej., procedimientos de control, dispositivos resistentes a la alteración y similares. Preferiblemente, los enteros seleccionados $p_1, p_2, ..., p_m$ también se mantienen en secreto, incluyendo el valor γ_j correspondiente a p_j, aunque esto es menos crítico. Nos referiremos a los polinomios bi-variados también de la siguiente forma: para j = 1, 2, ..., m, escribimos

$$f_j(x,y) = \sum_{i=0}^{a} f_{i,j}(x)y^i.$$

La realización anterior puede ser variada de un cierto número de maneras. Las restricciones sobre los módulos públicos y privados pueden ser escogidas en una amplia variedad de formas, de modo que sea posible la ofuscación del polinomio uni-variado, pero que, sin embargo, las claves compartidas obtenidas en dispositivos de red permanezcan suficientemente cercanas entre sí suficientemente a menudo. Como se ha explicado, lo que sea suficiente dependerá de la aplicación, del nivel de seguridad requerido y de los recursos de cálculo disponibles en los dispositivos de red. La realización anterior combina enteros positivos de modo que las operaciones modulares que se llevan a cabo al generar las particiones polinómicas sean combinadas de forma no lineal cuando son sumadas sobre los enteros, creando una estructura no lineal para el material de claves locales almacenado en un dispositivo de red. La elección anterior para *N* y p_j tiene la propiedad de que: (i) el tamaño de *N* está fijado para todos los dispositivos de red y vinculado con *a*; (ii) el efecto no lineal aparece en los bits más significativos de los coeficientes que forman el material de claves almacenado en el dispositivo. Debido a esa forma específica, la clave compartida puede ser generada reduciendo en módulo 2^b después de la reducción en módulo *N*.

Estos conceptos de diseño pueden ser aplicados de una manera más general para mejorar los aspectos (i) y (ii), según lo mencionado en el último párrafo. A continuación se dan estructuras generales distintas para escoger los módulos públicos y privados. Para abordar el primer punto (i), esta estructura para *N* y p_j se adecua a una expresión más general, donde escribimos $p_j = 2^X + \gamma_j 2^{Y_j} - 1$, de modo que, para cada j, $Y_j + b\alpha_j = X$ y $|\gamma_j| < 2^b$. Esta expresión admite una forma más variable p_j, asegurando a la vez un efecto máximo al introducir efectos no lineales. Obsérvese

que también se puede hacer $Y_j + b\alpha_j \approx X$, donde la diferencia entre los lados izquierdo y derecho es una fracción de la longitud de la clave.

Para abordar el segundo punto, la forma anterior para N y p_j se adecua a una expresión incluso más general, en la cual $p_j = \beta 2^X + \gamma_j 2^{Y_j} + \xi_j 2^{Z_j}$. Fijando, p. ej., $\xi_j = -1$, $\beta = 1$ y $Z_j = 0$ $\forall j$, obtenemos la expresión previa, en la cual los distintos valores de γ_j introducen un efecto no lineal en los bits más significativos de los coeficientes del material de claves almacenado en un dispositivo de red. En este caso, el módulo público constante (N) es $N = 2^X - 1$, mientras que la parte variable privada usada en la generación de distintos enteros positivos implicados en las operaciones modulares es $\gamma_j 2^{Y_j}$. Alternativamente, podemos fijar $\gamma_j = 1$, $\beta = 1$, $Z_j = 0$, $Y_j = (\alpha_j + 1)b$, $X = (\alpha_j + 2)b$ $\forall j$, mientras que los ξ_j son distintos para distintos j, de modo que $|\xi_j| < 2^b$. En este caso, las diferencias en ξj permiten introducir un efecto no lineal en los bits menos significativos de los coeficientes del material de claves locales almacenado en un nodo. La construcción de la parte pública en este caso también es distinta, 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 que, en este caso, el efecto no lineal está en la parte más baja y, debido a la condición para el máximo efecto de mezcla mencionado antes, entonces la diferencia entre $Y_j - Z_j - \log_2(\xi_j)$ debe ser $\alpha_j b$. De manera similar, pueden ser definidas otras estructuras siguiendo el mismo concepto.

Etapas de registro

En la etapa de registro cada dispositivo de red tiene asignado material de formación de claves (KM). Un dispositivo de red está asociado a un número de identidad. El número de identidad puede ser asignado a petición, p. ej., por parte del TTP, o puede ya estar almacenado en el dispositivo, p. ej., ser almacenado en el dispositivo en la fabricación, etc.

El TTP genera un conjunto de material de formación de claves para un dispositivo A de la siguiente manera:

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

En donde $KM^A(X)$ es el material de formación de claves de un dispositivo con número de identidad A; X es una variable formal. Obsérvese que el material de formación de claves es no lineal. La notación < ... > p_j indica reducción módulo p_j de cada coeficiente del polinomio entre los corchetes. La notación '$\varepsilon_{A,i}$' indica un entero aleatorio, que es un ejemplo de un número ofuscante, de modo que $|\varepsilon_{A,i}| < 2^{(a+1-i)b}$. Obsérvese que uno cualquiera de los enteros aleatorios puede ser positivo o negativo. Los números aleatorios ε son generados de nuevo para cada dispositivo. El término $\sum_{i=0}^{a} \epsilon_{A,i} X^i$ representa por tanto un polinomio en X de grado a, en el cual la longitud de coeficientes es más corta al aumentar el grado. Alternativamente, una condición más general, pero más complicada, es que $\sum_{i=0}^{a} |\epsilon_{A,i}| \cdot 2^{b+i}$ sea pequeño, p. ej., < 2a. Obsérvese que la etapa de añadir ofuscación es optativa y puede ser omitida, pero se prefiere para obtener un mayor nivel de seguridad. Supondremos que se usa la ofuscación.

Todas las otras adiciones pueden usar bien la aritmética entera natural, o bien (preferiblemente) usan la adición módulo N. Por lo que la evaluación de cada uno de los polinomios uni-variados $\sum_{j=1}^{m} < f_j(x, A) >_{p_j}$ se hace individualmente módulo un módulo p_j más pequeño, pero la suma de estos mismos polinomios uni-variados reducidos se hace, preferiblemente, módulo N. Además, la adición del polinomio ofuscante $2^b \sum_{i=0}^{a} \epsilon_{A,i} X^i$ puede hacerse usando la aritmética entera natural o, preferiblemente, módulo N. El material de formación de claves comprende los coeficientes C_i^A, con i = 0, ..., a. El material de formación de claves puede ser presentado como un polinomio, como en lo que antecede. En la práctica, el material de formación de claves puede ser almacenado como una lista, p. ej., una formación, de los enteros C_i^A. El dispositivo A también recibe los números N y b. La manipulación de los polinomios puede ser implementada, p. ej., como manipulación de formaciones que contienen los coeficientes, p. ej., enumerando todos los coeficientes en un orden predeterminado. Obsérvese que los polinomios pueden ser implementados, en otras estructuras de datos, p. ej., como una formación asociativa (también conocida como un 'mapa'), que comprende una colección de pares de (grado, coeficiente), preferiblemente de modo que cada coeficiente aparezca a lo sumo una vez en la colección. Los coeficientes C_i^A que se proporcionan al dispositivo están, preferiblemente, en la gama 0, 1, ... N-1.

En el caso en que se usa la estructura más general para N y para los números enteros p_j, el polinomio ofuscante necesita ser adaptado de modo que los números aleatorios $\in$ afecten a distintas partes de los coeficientes. Por ejemplo, si el efecto no lineal es introducido en los bits menos significativos de los coeficientes del material de claves almacenado en los dispositivos de red, entonces los números aleatorios deberían afectar solamente a la parte más alta de los coeficientes y a un número variable de bits en la parte más baja de los coeficientes. Esto es una extensión directa del procedimiento descrito anteriormente, y son factibles otras extensiones.

Fase de uso

Una vez que dos dispositivos A y B tienen un número de identidad y que han recibido su material de formación de claves desde el TTP, pueden usar su material de formación de claves para obtener una clave compartida. El dispositivo A puede realizar las siguientes etapas para obtener su clave compartida. Primero, el dispositivo A obtiene el número de identidad *B* del dispositivo B, luego A genera la clave compartida calculando 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 formación de claves, visto como un polinomio entero, para el valor B; el resultado de la evaluación del material de formación de claves es un entero. Luego, el dispositivo A reduce el resultado de la evaluación, primero, módulo el módulo público *N*, y luego, módulo el módulo clave 2^b. El resultado será mencionado como la clave compartida de A, y es un entero en la gama desde 0 hasta $2^b - 1$. Por su parte, el dispositivo B puede generar la clave compartida B' evaluando su material de clave para la identidad *A* y reduciendo el resultado módulo *N*, y luego, módulo 2^b.

En línea con la descripción anterior, si se usa una expresión más general de N y de los enteros positivos p_j, entonces el procedimiento para obtener la clave de los b bits necesita una pequeña adaptación. En particular, si el efecto no lineal es introducido en los bits más bajos de los coeficientes del material de claves almacenado en los dispositivos de red, mientras el segundo término en la expresión de N es Y_j, entonces la clave se genera de la siguiente manera:

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

Debido a que los polinomios bi-variados en el material de claves básicas son simétricos, la clave compartida de A y la clave compartida de B son frecuentemente, aunque no siempre necesariamente, iguales, Los requisitos particulares sobre los enteros $p_1, p_2, ..., p_m$ y sobre los números aleatorios (optativos) $\in$ son tales que las claves son a menudo iguales y casi siempre cercanas entre sí, módulo dos a la potencia de la longitud de clave. Si A y B han obtenido la misma clave compartida, entonces pueden usarla como una clave simétrica que es compartida entre A y B; por ejemplo, puede ser usada para una amplia variedad de aplicaciones criptográficas, por ejemplo, pueden intercambiar uno o más mensajes cifrados y / o autenticados, usando la clave compartida. Preferiblemente, se aplica un algoritmo de obtención de claves a la clave compartida, para protección adicional de la clave maestra, p. ej., puede ser aplicada una función de troceo.

Si A y B no han obtenido la misma clave compartida, entonces es casi seguro que estas claves están cercanas entre sí; eliminando un cierto número de los bits menos significativos de las claves, las claves generadas pueden hacerse iguales casi siempre. A y B pueden verificar si sus claves compartidas son iguales realizando una confirmación de clave, por ejemplo, A puede enviar a B un mensaje que contiene el par (m, E(m)), en el que m es un mensaje, digamos, una cadena fija o un número aleatorio, y E(m) es el cifrado, usando la clave compartida de A.

Al descifrar E(m) usando la clave compartida de B, B puede verificar si las claves son iguales. Si lo son, B puede responder a A informándole de la situación.

Si las claves no son iguales, A y B pueden participar en un protocolo de ecualización de claves. Por ejemplo, pueden hacer uso del hecho de que dos claves sean aritméticamente cercanas entre sí. Por ejemplo, los dispositivos de red A y B pueden eliminar iterativamente un bit menos significativo y enviar un mensaje de confirmación de clave hasta que las claves sean iguales. Después de obtener claves iguales, A y B pueden llevar a cabo un algoritmo de obtención de claves para recuperar claves de una longitud normal de clave.

Los *m* módulos seleccionados $p_1, p_2, ..., p_m$ son preferiblemente primos entre sí de a pares. Si estos números son primos entre sí de a pares, aumenta la falta de compatibilidad entre las operaciones de módulo. La obtención de números primos entre sí de a pares puede lograrse seleccionando los enteros en orden, probando, para cada nuevo entero, si todos los pares de números distintos son todavía primos entre sí; y si no lo son, el número recién seleccionado se elimina del conjunto. Este procedimiento continúa hasta que estén seleccionados todos los *m* números.

La complejidad aumenta aún más al requerir que los *m* módulos privados seleccionados $p_1, p_2, ..., p_m$, sean números primos distintos. En ese caso, puede requerirse que cada número primo tenga la forma $p_j = N + \gamma_j \cdot 2^b$. En donde los γ_j son enteros tales que $|\gamma_j| < 2^b$. Los experimentos han confirmado que estos primos están fácilmente disponibles. Por ejemplo, se puede seleccionar repetidamente un γ_j aleatorio y probar el p_j resultante hasta que se halle un primo. Lo mismo vale si se aplica una expresión más general, según lo descrito anteriormente. En efecto, se deduce del teorema de números primos para progresiones aritméticas que, mientras *a* tenga alrededor del mismo orden de magnitud que *b*, en particular, para $a < b$, tales primos son abundantes. En particular, para cualquier combinación de

longitudes de clave en el grupo 64, 128, 196, 256, y de grados en el grupo 2,3, confirmamos por experimentación que muchos números primos de esta forma podrían ser generados usando el algoritmo anterior con límites temporales prácticos. Al usar números primos, cada polinomio f_j se toma por tanto en el campo finito con p_j elementos.

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

Como se ha indicado, la diferencia entre $Y_j - Z_j - \log_2(\xi_j)$ puede ser $\alpha_j b$. De manera similar, pueden ser definidas otras estructuras siguiendo el mismo concepto. En particular, podemos escribir $p_j = \beta 2^X + \gamma_j 2^{Yj} + \delta 2^W + \xi_j 2^{Zj}$ para los módulos privados y $N = \beta 2^X + \delta 2^W$ para el módulo público. Una instanciación específica de esta estructura es $p_j = 2^{2(a+1)b} + \gamma_j 2^{(a+1)b} + 2^{ab} + \xi_j$ y $N = 2^{2(a+1)b} + 2^{ab}$. En este caso, el valor absoluto de los términos γ_j y β_j es más pequeño que 2^b, y están encargados de crear un efecto no lineal en los MSB y los LSB de los coeficientes del material de claves locales almacenadas en un dispositivo. Obsérvese que, dado que los identificadores de dispositivo son alrededor de b bits de largo, γ_j (β_j) afecta los MSB (LSB) de los coeficientes de la partición polinómica evaluada en el anillo de enteros, módulo p_j. Después, durante la generación del material de claves locales para un dispositivo, los coeficientes de las particiones polinómicas en distintos anillos son sumados sobre los enteros, de modo que se oculte el origen de las contribuciones.

La clave puede ser generada de la siguiente manera: $K_{AB} = < \frac{< KM^A(x)|_{x=B} >_N}{2^{Y_j}} >_{2^b}$, pero si se usa la expresión aún más general de p_j y N, que permite introducir un efecto no lineal tanto en los MSB como en los LSB, entonces la división después de la reducción módulo N es entre 2 a la potencia de W, donde 2^W es la más alta potencia entera de 2 de la cual N es un múltiplo entero. Otras estructuras de N y p_j pueden requerir una división entre otra potencia de dos. Debido a que los polinomios bi-variados en el material de la clave básica son simétricos, la clave compartida de A y la clave compartida de B son a menudo, aunque no necesariamente siempre, iguales.

Confirmación de clave.

Puede ser deseable, para uno entre A y B, enviar un mensaje de confirmación de clave a la otra parte. Un denominado mensaje de confirmación de clave (KC) permite al destinatario 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 de compartición de claves para el cual se conoce que la clave establecida por ambas partes puede diferir, un mensaje de confirmación de clave puede ser usado tanto como una confirmación de que ambos han establecido la misma clave, como, si no es así, para determinar una clave compartida igual. Por ejemplo, en general, un MAC (código de autenticación de mensaje) basado en la clave establecida puede servir como el mensaje de confirmación, p. ej., un HMAC basado en SHA2 o SHA3, o un CMAC basado en AES, y similares. También puede usarse una función de troceo criptográficamente potente, p. ej., un troceo de la clave establecida puede usarse como el mensaje de confirmación de clave. El troceo puede ser calculado sobre la misma clave. El MAC puede ser calculado sobre datos que son conocidos por B, o que están incluidos en el mensaje de confirmación de clave, p. ej., un mensaje ocasional, etc.

Sin embargo, los mensajes generales de confirmación de clave criptográficamente potentes requieren algunos recursos, posiblemente más recursos que un algoritmo de compartición de claves, de acuerdo a los principios anteriores. Los esquemas de compartición de claves dados anteriormente admiten funciones más sencillas que requieren muchos menos recursos de cálculo que los esquemas de confirmación de clave de propósito general.

Los dispositivos A y B calculan las claves $K_A(B)$ y $K_B(A)$. Puede mostrarse, siguiendo las relaciones matemáticas, que existe un entero Δ, según los parámetros de diseño, tal que

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

Nuevamente, $< x >_m$ indica el entero entre 0 y m-1 tal que $x - < x >_m$ es un múltiplo de m. Definamos una función de la siguiente manera: $h(x) = < x >_{2^r}$, donde r es un entero predeterminado tal que $2^r \geq 2\Delta + 1$. En comparación con la realización general, no hay ninguna necesidad de que los dispositivos calculen funciones de troceo posiblemente complicadas; la desventaja es que alguna información sobre la clave que se está usando se envía por un canal de comunicación observable. Se prefiere usualmente que un mensaje de confirmación de clave no filtre ninguna, o filtre una cantidad despreciable, de información sobre la clave para la cual se calcula. Esta desventaja puede ser contrarrestada dividiendo la clave establecida entre 2^r, después de que se haya hallado una clave que sea la misma tanto para A como para B. Más en general, en una segunda realización, $h(x) = <x>_v$, donde $v \geq 2\Delta+1$, es tal que 2^b

es un múltiplo de v, o bien $< 2^b >_v \geq 2\Delta+1$. En ambos casos, $h(K_A(B))$ puede ser usado por A como un mensaje de confirmación de clave.

Además de enviar un mensaje de confirmación de clave, se puede reducir la diferencia entre $K_A(B)$ y $K_B(A)$ dividiendo ambas claves entre una potencia de 2. $K_A(B)$ y $K_B(A)$ son claves de b bits; luego, la eliminación de los l bits menos significativos de las claves generadas de b bits, que corresponden a los b-l bits más significativos de la clave generada, se usa para asegurar la comunicación. Si b es relativamente grande (digamos, 100) y l también es grande (digamos, 50), la probabilidad de que los b-l bits más significativos sean iguales es muy alta, es decir, de alrededor de $1 - \frac{2\Delta}{2^{b-l}}$. Este enfoque no requiere ningún intercambio de información alguna, se eliminan L bits de la clave original generada y la clave resultante puede ser usada para la comunicación. Sin embargo, esto tiene un inconveniente, porque se reduce el tamaño de la clave, en potencia, de forma considerable, para asegurar que todos los dispositivos en una red compartan una clave común de b-l bits con muy alta probabilidad.

Obsérvese que la eliminación de bits menos significativos puede ser combinada con un mensaje de confirmación de clave. Por ejemplo, después de eliminar l bits, se calcula un mensaje de confirmación de clave y se envía a la otra parte. Este enfoque tiene la ventaja de que, incluso si la eliminación de bits menos significativos no fuera suficiente para establecer una clave común, facilitará hallar una clave común de ese tipo.

En un enfoque distinto, el problema de que claves potencialmente distintas sean establecidas por las partes A y B es el siguiente: la autoridad central tiene toda la información para calcular de antemano si dos dispositivos cualesquiera pueden obtener claves distintas. Por ejemplo, la autoridad central puede comenzar con un único identificador A y material de formación de claves calculado para A. Se añaden dispositivos a un fondo común de dispositivos iterativamente. Cuando ha de añadirse un nuevo dispositivo B' al sistema, el TTP calcula material de formación de claves para B'. El TTP verifica, para cada combinación de B' y los dispositivos ya en el fondo común, si llegarán a la misma clave común. Por ejemplo, el TTP puede verificar que hallen la misma clave directamente. El TTP también puede verificar que B' y cualquier otro dispositivo llegarán a una clave común participando en un protocolo adecuado de acuerdo sobre claves para reparar una clave posiblemente distinta; p. ej., dividiendo entre una potencia de 2 y / o enviando uno o más mensajes de confirmación de clave. A la vista del precedente enfoque probabilístico, es muy probable que una elección aleatoria para B' haga que {A, B'} sea válido para todo A si el número de dispositivos A es relativamente pequeño.

Si resulta que B' no llegará a una clave común con algunos de los dispositivos ya en el fondo común, el TTP asigna un nuevo identificador a B' o calcula nuevo material de formación de claves, pero con distintas elecciones aleatorias. Aunque comprobar esta condición representa un buen sobregasto, esto es posible para redes relativamente pequeñas (digamos, dispositivos ~ O (10^4) o O (10^5)).

Un enfoque relacionado también puede ser aplicado en grupos de dispositivos. En particular, en algunas configuraciones no todos los dispositivos podrían requerir hablarse entre sí, p. ej., si los dispositivos son estáticos y se despliegan en grupos (p. ej., en un edificio). En este caso, la verificación realizada por el TTP cuando se añade un nuevo dispositivo B' se limita a comprobar los dispositivos pertenecientes al grupo al cual se añadirá B'. Por ejemplo, el TTP puede verificar si todos los dispositivos en un grupo dado generan o no una clave si se eliminan los l LSB de la clave. Obsérvese que este procedimiento también admite el diseño de esquemas jerárquicos más avanzados, de modo que todos los dispositivos pertenezcan al grupo principal en un primer nivel, los dispositivos sean divididos entre un cierto número de grupos a un segundo nivel, y los dispositivos en un grupo en un segundo nivel sean adicionalmente divididos en un cierto número de sub-grupos. En una tal organización jerárquica, el TTP podría verificar si todos los dispositivos en un grupo dado de nivel w generan o no una clave común después de la eliminación de l_w bits. En tal sistema, los grupos en un nivel más profundo podrían requerir la eliminación de un menor número de bits, mientras que los grupos en niveles altos podrían requerir la eliminación de más bits para asegurar la generación de claves comunes.

El TTP puede realizar estas comprobaciones toda vez que se añade un nuevo dispositivo, pero también crear pro-activamente un fondo común de identificadores de dispositivo y material de formación de claves, de modo que cada par de identificadores de este fondo común dé una clave común válida.

Por ejemplo, el TTP puede limitarse a pares de dispositivos válidos {*A, B*}, donde un par es válido si:

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

donde l se refiere a l bits correspondientes a los l Bits Menos Significativos de $K_A(B)$ y $K_B(A)$. Esta condición, en general, muestra una forma de verificar que las claves que efectivamente se usarán son iguales. Otra condición es que se admite un nuevo B si y solamente si, para todo A, los l 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 bloques esquemáticos que ilustra un generador de material de claves básicas 100. Un obtenedor de material de claves está configurado para proporcionar datos de entrada, excepto un número de identidad, que necesita un generador de material de claves locales para generar material de claves locales. Un generador de claves es un ejemplo de un obtenedor de material de claves. En lugar de generar todos, o parte de, los datos de entrada, algunos parámetros también pueden ser obtenidos por el generador de material de claves básicas, recibiéndolos; por ejemplo, el obtenedor de claves puede comprender un receptor electrónico para recibir datos de entrada, p. ej., un módulo público y un módulo privado. Un obtenedor de material de claves obtiene todos los parámetros necesarios, excepto los números de identidad, desde un origen externo. En una realización, *a, b, m* están predeterminados, p. ej., recibidos, y el módulo público y los módulos privados y los correspondientes polinomios bi-variados simétricos están generados. En una realización, también el módulo público está predeterminado, p. ej., recibido.

El generador de claves básicas 100 comprende un elemento de grado polinómico 112, un elemento de longitud de clave 114 y un cierto número de elementos polinómicos 116, configurados para proporcionar el grado polinómico, la longitud de clave y el número de polinomios, es decir, *a, b* y *m*, respectivamente. Aunque estos elementos pueden ser generados, p. ej., según las circunstancias, habitualmente estos parámetros son escogidos por un diseñador del sistema. Por ejemplo, los elementos pueden ser diseñados como memorias no volátiles, o como receptores para recibir los valores de elementos, o como memorias volátiles conectadas con un receptor, etc. Una elección adecuada incluye $a = 2$, $b = 128$, $m = 2$. Uno cualquiera de los números puede ser aumentado o disminuido para obtener un sistema más o menos seguro.

El generador de claves básicas 100 comprende un elemento de módulo público 110 configurado para proporcionar el módulo público *N*. El módulo público puede o no ser escogido por un diseñador del sistema. Por ejemplo, el módulo público puede ser fijado en un número conveniente que admita la reducción rápida (cercana o igual a una potencia de dos). El módulo público se escoge dentro de una gama determinada por los elementos 112 y 114.

El generador de claves básicas 100 comprende un gestor de módulos privados 122 configurado para proporcionar el módulo privado *p*, o múltiples módulos privados $p_1, ..., p_m$. Por ejemplo, se escogen al azar dentro de las cotas adecuadas.

El generador de claves básicas 100 comprende un gestor de polinomios bi-variados simétricos 124 configurado para proporcionar el polinomio bi-variado simétrico *f*, o múltiples polinomios bi-variados simétricos $f_1, ..., f_m$. Cada polinomio bi-variado simétrico se escoge con coeficientes al azar, módulo el correspondiente módulo privado, es decir, el módulo privado que tiene el mismo índice. Los coeficientes pueden ser escogidos dentro de la gama 0 a $p-1$, y pueden ser escogidos al azar.

Los módulos privados pueden ser escogidos añadiendo o restando al módulo público un múltiplo de dos a la potencia de la longitud de la clave. Esto dará como resultado módulos privados tales que la diferencia con el módulo público acaba en una serie de ceros consecutivos. También se puede escoger un módulo público y uno o más módulos privados, de modo que una serie de ceros consecutivos de la longitud de la clave aparezca, no al final sino en otra posición, digamos la posición 's', contando desde el bit menos significativo.

La Figura 2 es un diagrama de bloques esquemáticos que ilustra un generador de material de claves locales 200. El generador de material de claves 100 y el generador de material de claves locales 200 forman juntos un sistema para configurar un dispositivo de red para la compartición de claves.

El generador de material de claves locales 200 comprende un dispositivo de manipulación de polinomios 240. El generador de material de claves locales 200 comprende un elemento de material público 210 para proporcionar los parámetros públicos *a, N* al dispositivo de manipulación de polinomios 240. El generador de material de claves locales 200 comprende un elemento de material privado 220 para proporcionar los parámetros privados p_i, f_i y *m* al dispositivo de manipulación de polinomios 240. Los elementos 210 y 220 pueden ser implementados por los correspondientes elementos del generador de material de claves 100; estos elementos también pueden ser memorias o buses para conectar el generador de material de claves 100.

El generador de material de claves locales 200 comprende un generador de números ofuscantes 260, para proporcionar un número ofuscante '$\varepsilon_{A,i}$' al dispositivo de manipulación de polinomios 240. El número ofuscado puede ser un número aleatorio, p. ej., generado con el generador de números aleatorios. El generador de números ofuscantes 260 puede generar múltiples números ofuscantes para múltiples coeficientes del polinomio uni-variado. En una realización, un número ofuscante está determinado para cada coeficiente del polinomio uni-variado.

El generador de material de claves locales 200 comprende un gestor de dispositivos de red 250 configurado para recibir un número de identidad, para el cual debe generarse material de claves locales, p. ej., desde un dispositivo de red, y está configurado para enviar el material de claves locales al dispositivo de red correspondiente al número de identidad. En lugar de recibir un número de identidad, puede también ser generado, p. ej., como un número aleatorio, en serie u ocasional. En este último caso, el número de identidad es enviado junto con el material de claves locales al dispositivo de red.

El dispositivo de manipulación de polinomios 240 obtiene polinomios uni-variados, posiblemente múltiples, sustituyendo el número de identidad procedente del gestor 250 en cada uno de los polinomios bi-variados y reduciendo a cada uno, módulo el correspondiente módulo privado. Los múltiples polinomios uni-variados reducidos resultantes se suman, según los coeficientes, con la suma aritmética natural. También se suman dichos uno o más números ofuscantes. Preferiblemente, el resultado es reducido, nuevamente según los coeficientes, módulo el módulo público; los coeficientes de este último pueden ser representados en la gama 0 a $N - 1$.

El polinomio uni-variado ofuscado es parte del material de claves locales correspondiente al número de identidad. Si es necesario, el módulo público, el grado y la longitud de la clave también son enviados al dispositivo de red.

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

El dispositivo de red 310 comprende un transceptor 330 que combina un remitente y un receptor para enviar y recibir mensajes en formato electrónico, p. ej., digital, por cable o inalámbricamente, desde y a un segundo dispositivo de red 320. Posiblemente, el transceptor 330 también se usa para recibir el material de claves locales 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, el del segundo dispositivo de red 320.

El dispositivo de red 310 comprende un obtenedor de material de claves locales 344. El obtenedor de material de claves locales 344 puede ser implementado como memoria local, p. ej., memoria no volátil tal como memoria flash, para almacenar el material de claves locales. El obtenedor de material de claves locales 344 también puede ser configurado para obtener el material de claves locales desde el generador 200, p. ej., mediante el transceptor 330. El obtenedor de material de claves locales 344 está configurado para proporcionar el dispositivo de manipulación de polinomios los parámetros necesarios.

El dispositivo de red 310 comprende un dispositivo de manipulación de polinomios 342, configurado para sustituir el número de identidad del segundo dispositivo de red en el polinomio uni-variado ofuscado, y para realizar dos reducciones sobre el resultado: primero, reducir el resultado de la sustitución módulo el módulo público y, segundo, reducir módulo un módulo clave. Obsérvese que incluso si se usaran múltiples módulos privados, solamente sería necesario un módulo público. Obsérvese que, para algunas combinaciones de N y módulo privado, se requiere una división entre una potencia de 2 antes de que el resultado sea reducido módulo un módulo clave.

El dispositivo de red 310 comprende un dispositivo de obtención de claves 346, para obtener la clave compartida a partir del resultado de la reducción módulo el módulo clave. Por ejemplo, el dispositivo de obtención de claves 346 puede eliminar uno o más bits menos significativos. El dispositivo de obtención de claves 346 también puede aplicar una función de obtención de claves. También es posible usar el resultado de la segunda reducción sin procesamiento adicional.

El dispositivo de red 310 comprende un ecualizador de claves optativo 348. Obsérvese que puede ocurrir que la clave compartida obtenida en el primer dispositivo de red no sea igual a la clave obtenida en el segundo dispositivo de red (en base al número de identidad del primer dispositivo de red). Si esto se considera indeseable, se puede seguir un protocolo de ecualización de claves.

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

Habitualmente, un sistema para configurar un dispositivo de red para la compartición de claves 200, y un primer dispositivo de red configurado para determinar una clave compartida 310, comprenden, cada uno, un microprocesador (no mostrado) que ejecuta el software adecuado almacenado en los respectivos dispositivos, p. ej., software que puede haber sido descargado y almacenado en una correspondiente memoria, p. ej., RAM (no mostrada).

Una realización interesante se obtiene para $a = 1$, especialmente en combinación con valores mayores de m, digamos, mayores que 1, 2 o mayores, 4 o mayores. La manipulación de polinomios requerida se reduce a una única multiplicación y reducción, dando una implementación especialmente sencilla. Sin embargo, incluso para este caso sencillo, la recuperación de los polinomios bi-variados originales no es inmediata, y se torna crecientemente complicada con valores mayores que m. Aunque no se conoce ningún ataque viable incluso para $a = 1$, la estructura lineal puede ser un punto de partida para el análisis futuro, por lo que se puede querer restringir a $a > 1$, por este motivo.

La Figura 4 es un diagrama de flujo esquemático que ilustra un procedimiento de generación de material de claves locales 400. El procedimiento comprende obtener 410 un módulo público y un módulo privado, y un polinomio bi-variado simétrico, obtener 420 un número de identidad de un dispositivo de red, sustituir 430 el número de identidad en el polinomio bi-variado, módulo el módulo privado, añadir 440 un número ofuscante a un coeficiente y almacenar 450 el polinomio uni-variado ofuscado en el dispositivo de red.

La Figura 5 es un diagrama de flujo esquemático que ilustra un procedimiento de generación de una clave compartida 500. El procedimiento comprende obtener 510 el número de identidad externo de otro dispositivo de red, enviar 520 el número de identidad local a otro dispositivo de red, sustituir 530 el número de identidad externo en el polinomio uni-variado ofuscado, módulo el módulo público, reducir 540 módulo el módulo de clave, obtener 550 una clave compartida, enviar 560 un mensaje de confirmación de clave al otro dispositivo de red, determinar 570 si la clave está confirmada 570 y una aplicación criptográfica 580. Si la clave no es confirmada en la etapa 570, entonces el procedimiento continúa en la etapa 550 con la obtención de una nueva clave. Por ejemplo, la etapa 550 puede eliminar un bit menos significativo adicional cada vez que la clave no se confirma.

Las etapas 550, 560 y 570 forman juntas un protocolo de ecualización de clave. Por ejemplo, en la etapa 560, un mensaje ocasional, y el cifrado del mensaje ocasional según la clave compartida obtenida en la etapa 550, pueden ser enviados el segundo dispositivo. En la etapa 560 se recibe un mensaje desde el segundo dispositivo. El mensaje recibido puede decir simplemente que el mensaje recibido de confirmación de clave mostró que las claves no son iguales. El mensaje recibido también puede contener un mensaje de confirmación de clave. En este último caso, el primer dispositivo de red verifica el mensaje de confirmación de clave y establece si las claves son iguales. Si no lo son, se obtiene una nueva clave, por ejemplo, borrando un bit menos significativo.

Son posibles muchas formas distintas de ejecutar el procedimiento, como será evidente para una persona experta en la técnica. Por ejemplo, el orden de las etapas puede ser variado, o algunas etapas pueden ser ejecutadas en paralelo. Además, entre las etapas pueden ser insertadas otras etapas del procedimiento. Las etapas insertadas pueden representar refinamientos del procedimiento, tales como los descritos en la presente memoria, o pueden no estar relacionadas con el procedimiento. Por ejemplo, las etapas 410 y 420, o 510 y 520, pueden ser ejecutadas, al menos parcialmente, en paralelo. Además, una etapa dada puede no haber acabado por completo antes de que se inicie una nueva etapa.

Un procedimiento de acuerdo a la invención puede ser ejecutado usando software, que comprende instrucciones para provocar que un sistema procesador realice el procedimiento 400 o 500. El software solamente puede incluir aquellas etapas adoptadas por una sub-entidad específica del sistema. El software puede ser almacenado en un medio de almacenamiento adecuado, tal como un disco rígido, un disco flexible, una memoria, etc. El software puede ser enviado como una señal a lo largo de un cable, o inalámbricamente, o usando una red de datos, p. ej., Internet. El software puede dejarse disponible para su descarga y / o para su uso remoto en un servidor.

La Figura 6 muestra en forma esquemática una posible secuencia de mensajes entre dos dispositivos de red, los dispositivos A y B, mientras están generando una clave compartida. El tiempo fluye hacia abajo. En la etapa 610, el dispositivo de red A envía su número de identidad al dispositivo B. En la etapa 620 el dispositivo B envía su número de identidad y un mensaje de confirmación de clave para la clave compartida (K1) que obtuvo en base al número de identidad A y a su material de claves locales. En la etapa 630, el dispositivo A halló que no generaron la misma clave. El dispositivo A ha borrado un bit menos significativo (digamos, por división entera entre 2) para obtener la clave K2. En la etapa 630, el dispositivo A envía un nuevo mensaje de confirmación de clave. De esta manera, A y B intercambian mensajes de confirmación de clave 640 hasta que llegan a la misma clave en la etapa 650. En la etapa 650, el dispositivo A envía un mensaje de confirmación de clave al dispositivo B. El dispositivo B fue capaz de verificar que habían llegado a la misma clave. En la etapa 660 envía una confirmación del mismo, y esto puede ser un mensaje autenticado o un mensaje de confirmación de clave, etc. En la etapa 670 el dispositivo A envía un mensaje M1 que está cifrado (digamos, usando AES) y / o autenticado (digamos, usando HMAC) usando la clave compartida, ahora igual.

El algoritmo a continuación da una posible implementación de este enfoque, es decir, un protocolo para el acuerdo mutuo de clave y la obtención de clave de sesión, ejecutado por el Dispositivo A y el Dispositivo B

```
Fijar l = L
Fijar continuar = VERDAD
Fijar Longitud = b-l
Generar una clave K de b bits
Mientras (continuar Y (Longitud > LONGITUD_MÍNIMA)){
        K=K>>l
        Efectuar saludo mutuo de autenticación con B en base
a K
        Si saludo es_exitoso, entonces {
                continuar = FALSO
} en caso contrario {
```

Longitud = b-I

}

El protocolo elimina un cierto número de bits de la cadena de bits generada con un algoritmo de compartición de clave, tal como el descrito en la presente memoria, y realiza un saludo mutuo de autenticación, p. ej., de reto-respuesta. El saludo mutuo de autenticación puede comprender un mensaje de confirmación de clave. Si no es exitoso, se eliminan unos pocos bits adicionales, y así sucesivamente hasta que el saludo mutuo sea efectuado con éxito o la clave se quede demasiado corta. El protocolo puede ser modificado de un cierto número de formas, p. ej., eliminando un número variable de bits, según la iteración, o requiriendo siempre un número fijo de etapas a fin de que un mirón que observe la ejecución del protocolo no obtenga ninguna información acerca de la longitud de la clave común compartida entre A y B. Este enfoque tiene la ventaja de que asegura que las claves compartidas sean tan largas como sea posible; sin embargo, tiene la desventaja potencial de que requiere un cierto número de intercambios para el acuerdo sobre la clave común. Por otra parte, para la mayoría de las aplicaciones, esto no será un gran problema porque, para la mayoría de los pares de dispositivos, las claves serán iguales, o diferirán solamente en unos pocos bits, y solamente unos pares de dispositivos llegarán a claves con un número relativamente alto de bits menos significativos distintos. Esto se deduce de las propiedades de las claves generadas.

Hay otras maneras de llegar a la misma clave para ambos dispositivos. Nuevamente suponemos que los dispositivos A y B calculan las claves $K_A(B)$ y $K_B(A)$. Los protocolos más adelante valen para cualquier esquema de compartición de claves para el cual exista un entero Δ, según los parámetros de diseño, tal que:

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

Por ejemplo, los esquemas de compartición de clave descritos en la presente memoria tienen esta propiedad. Las claves generadas están representadas como enteros de b bits. Por lo que las claves pueden ser consideradas como elementos del conjunto {0, 1, 2, ..., 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 $< 1\text{-}2 >_{2^b} = 2^b - 1$). Para parámetros de diseño de sistemas debidamente escogidos, Δ es relativamente pequeño. La invención supone que la misma clave es generada siempre, porque es posible recuperarse de un fallo para generar una clave.

De acuerdo a este procedimiento, el Dispositivo A envía al dispositivo B un valor de función $h(K_A(B))$. Aquí h es una función de troceo adecuada, p. ej., una función de troceo criptográfico. El dispositivo B calcula h(i) para todo i en $\{< K_B(A) + j >_{2^b} \mid -\Delta \leq j \leq \Delta\}$ y usa, para comunicaciones futuras, el 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 entre una potencia de 2 para reducir el tamaño de Δ.

Se apreciará que la invención también se extiende a programas de ordenador, en particular, programas de ordenador sobre, o en, una portadora, adaptada para poner la invención en práctica. El programa puede estar en forma de código fuente, código objeto, un código intermedio entre fuente y objeto, tal como una forma parcialmente compilada, o en cualquier otra forma adecuada para su uso en la implementación del procedimiento de acuerdo a la invención. Una realización referida a un producto de programa de ordenador comprende instrucciones ejecutables por ordenador, correspondientes a cada una de las etapas de procesamiento de al menos uno de los procedimientos enunciados. Estas instrucciones pueden ser subdivididas en sub-rutinas y / o ser almacenadas en uno o más ficheros que pueden estar enlazados estáticamente o dinámicamente. Otra realización referida a un producto de programa de ordenador comprende instrucciones ejecutables por ordenador, correspondientes a cada uno de los medios de al menos uno de los sistemas y / o productos enunciados.

Debería observarse que las realizaciones mencionadas anteriormente ilustran, en lugar de limitar, la invención, y que los expertos en la técnica podrán diseñar muchas realizaciones alternativas. En las reivindicaciones, todo signo de referencia colocado entre paréntesis no será interpretado como limitador de la reivindicación. El uso del verbo “comprender” y sus conjugaciones no excluye la presencia de elementos o etapas distintas a las indicadas en una reivindicación. El artículo “un” o “uno”, precediendo a un elemento, no excluye la presencia de una pluralidad de tales elementos. La invención puede ser implementada por medio de hardware que comprende varios elementos distintos, y por medio de un ordenador adecuadamente programado. En la reivindicación de dispositivo que enumera varios medios, varios de estos medios pueden ser realizados por un mismo elemento de hardware. El mero hecho de que ciertas medidas estén reveladas en reivindicaciones dependientes, mutuamente distintas, no indica que una combinación de estas medidas no pueda ser usada con ventaja.

REIVINDICACIONES

1. Un procedimiento de configuración de un dispositivo de red para la compartición de claves, comprendiendo el procedimiento:

obtener (410) en forma electrónica un módulo privado (p_1), un módulo público (N) y un polinomio bi-variado (f_1) con coeficientes enteros; la representación binaria del módulo público y la representación binaria del módulo privado son la misma en al menos los (b) bits consecutivos de la longitud de clave,
generar material de claves locales para el dispositivo de red, comprendiendo la etapa de generación obtener (420) en forma electrónica un número de identidad (A) para el dispositivo de red, y determinar, usando un dispositivo de manipulación polinómica, un polinomio uni-variado a partir del polinomio bi-variado, por sustitución (430) del número de identidad en el polinomio bi-variado, reduciendo, módulo el módulo privado, el resultado de la sustitución, y
almacenar electrónicamente (450) el material generado de claves locales en el dispositivo de red, y almacenar el módulo público en el dispositivo de red.

2. Un procedimiento según lo reivindicado en la Reivindicación 1, en el que la generación del material de claves locales para el dispositivo de red comprende generar un número ofuscante y sumar (440), usando un dispositivo de manipulación polinómica, el número ofuscante a un coeficiente del polinomio uni-variado, para obtener un polinomio uni-variado ofuscado, comprendiendo el material generado de claves locales el polinomio uni-variado ofuscado.

3. Un procedimiento según lo reivindicado en la Reivindicación 1 o 2, en el que el polinomio bi-variado (f_1) es un polinomio simétrico.

4. Un procedimiento según lo reivindicado en una cualquiera de las reivindicaciones precedentes, en el que los (b) bits menos significativos de la longitud de clave de la representación binaria del módulo público son los mismos que los (b) bits menos significativos de la longitud de clave del módulo privado.

5. Un procedimiento según lo reivindicado en una cualquiera de las reivindicaciones precedentes, que comprende además
generar el módulo privado (p_1) usando un generador electrónico de números aleatorios, y / o
generar el polinomio bi-variado usando un generador electrónico de números aleatorios, generando uno o más coeficientes aleatorios para el polinomio bi-variado.

6. Un procedimiento según lo reivindicado en una cualquiera de las reivindicaciones precedentes, en el que el módulo público satisface $2^{(a+2)b-1} \leq N$, en el que N representa el módulo público, a representa el grado del polinomio bi-variado y b representa la longitud de clave.

7. Un procedimiento según lo reivindicado en una cualquiera de las reivindicaciones precedentes, que comprende obtener en forma electrónica múltiples módulos privados (p_i), y múltiples polinomios bi-variados (f_i) con coeficientes módulo p_i, de modo que haya un conjunto de (b) posiciones consecutivas de longitud de clave, en las cuales la representación binaria del módulo público concuerda con la representación binaria de todos los módulos privados,
determinar el polinomio uni-variado comprende sustituir el número de identidad en cada uno de los múltiples polinomios bi-variados (f_i), reducir, módulo un módulo privado de los múltiples módulos privados correspondientes a dicho polinomio bi-variado simétrico, y sumar los múltiples resultados de las múltiples reducciones.

8. Un procedimiento según lo reivindicado en una cualquiera de las reivindicaciones precedentes, en el que el número ofuscante es generado de modo que

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

en el que $\varepsilon_{A,i}$ indica el número ofuscante, i indica el grado del monomio correspondiente al coeficiente, a representa el grado del polinomio bi-variado y b representa la longitud de clave.

9. Un procedimiento para un primer dispositivo de red, configurado por un procedimiento de configuración de un dispositivo de red para la compartición de clave, como en la Reivindicación 1, para determinar una clave compartida, siendo la clave una clave criptográfica, comprendiendo el procedimiento:

obtener material de claves locales para el primer dispositivo de red en forma electrónica, comprendiendo el material de claves locales un polinomio uni-variado, optativamente ofuscado,
obtener (510) un número de identidad para un segundo dispositivo de red, siendo el segundo dispositivo de red distinto al primer dispositivo de red,
sustituir (530) el número de identidad del segundo dispositivo de red en el polinomio uni-variado, optativamente ofuscado,
reducir el resultado de la sustitución, módulo el módulo público, y reducir (540), módulo un módulo clave, y
obtener (550) la clave compartida a partir del resultado de la reducción módulo el módulo clave.

10. Un procedimiento según lo reivindicado en la reivindicación 9, que comprende además
determinar (560, 570) si el primer dispositivo de red y el segundo dispositivo de red han obtenido la misma clave compartida y, si no es así, obtener una clave compartida adicional a partir del resultado de la reducción módulo el módulo clave.

11. Un procedimiento según lo reivindicado en las Reivindicaciones 9 o 10, que comprende además dividir el resultado de la sustitución, módulo el modulo público, entre un divisor de cadena de bits cero que sea una potencia de dos, siendo el divisor de cadena de bits cero mayor que 1.

12. Un sistema para configurar un dispositivo de red para la compartición de claves, comprendiendo el sistema:

un obtenedor de material de claves (100) para obtener en forma electrónica un módulo privado (122,p_1), un módulo público (110, N) y un polinomio bi-variado simétrico (124, f_1) con coeficientes enteros, y la representación binaria del módulo público y la representación binaria del módulo privado son la misma en al menos (b) bits consecutivos de la longitud de clave,
un generador (200) para generar material de claves locales para el dispositivo de red, que comprende
un gestor de dispositivos de red (250) para obtener en forma electrónica un numero de identidad (A) para el dispositivo de red, y para almacenar electrónicamente el material generado de claves locales en el dispositivo de red, y almacenar el módulo público en el dispositivo de red, y
un dispositivo de manipulación polinómica (240) para determinar un polinomio uni-variado a partir del polinomio bi-variado, sustituyendo el número de identidad en el polinomio bi-variado, y reduciendo, módulo el módulo privado, el resultado de la sustitución.

13. Un primer dispositivo de red (310) configurado para determinar una clave compartida como en la Reivindicación 1, siendo la clave una clave criptográfica, y comprendiendo el primer dispositivo de red:

un obtenedor de material de claves locales (344) para obtener material de claves locales para el primer dispositivo de red, en forma electrónica, comprendiendo el material de claves locales un polinomio uni-variado, optativamente ofuscado,
un receptor (330) para obtener un número de identidad para un segundo dispositivo de red, siendo el segundo dispositivo de red distinto al primer dispositivo de red,
un dispositivo de manipulación polinómica (342) para sustituir el número de identidad del segundo dispositivo de red en el polinomio uni-variado, optativamente ofuscado, y reducir el resultado de la sustitución, módulo el módulo público, seguido por una reducción, módulo un módulo clave, y
un dispositivo de obtención de clave (346) para obtener la clave compartida a partir del resultado de la reducción módulo el módulo clave.

14. Un programa de ordenador que comprende medios de código de programa de ordenador, adaptados para realizar todas las etapas de una cualquiera de las reivindicaciones 1 a 11 cuando el programa de ordenador es ejecutado en un ordenador.

15. Un programa de ordenador según lo reivindicado en la reivindicación 14, realizado en un medio legible por ordenador.

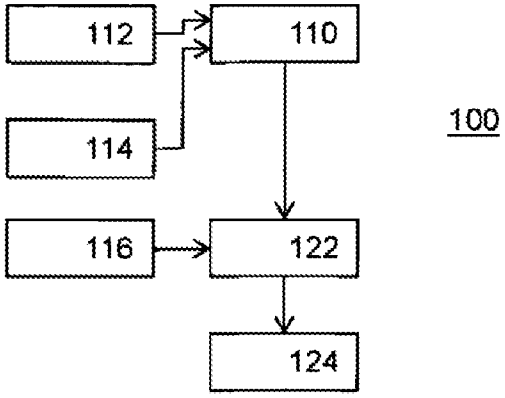

Figura 1

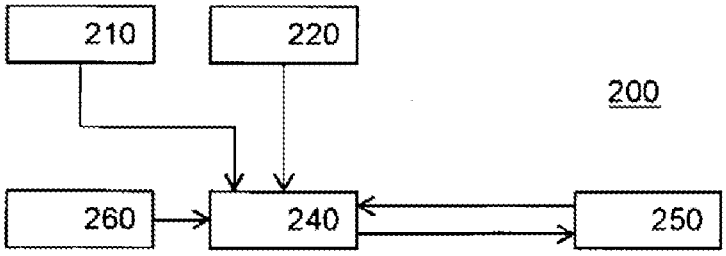

Figura 2

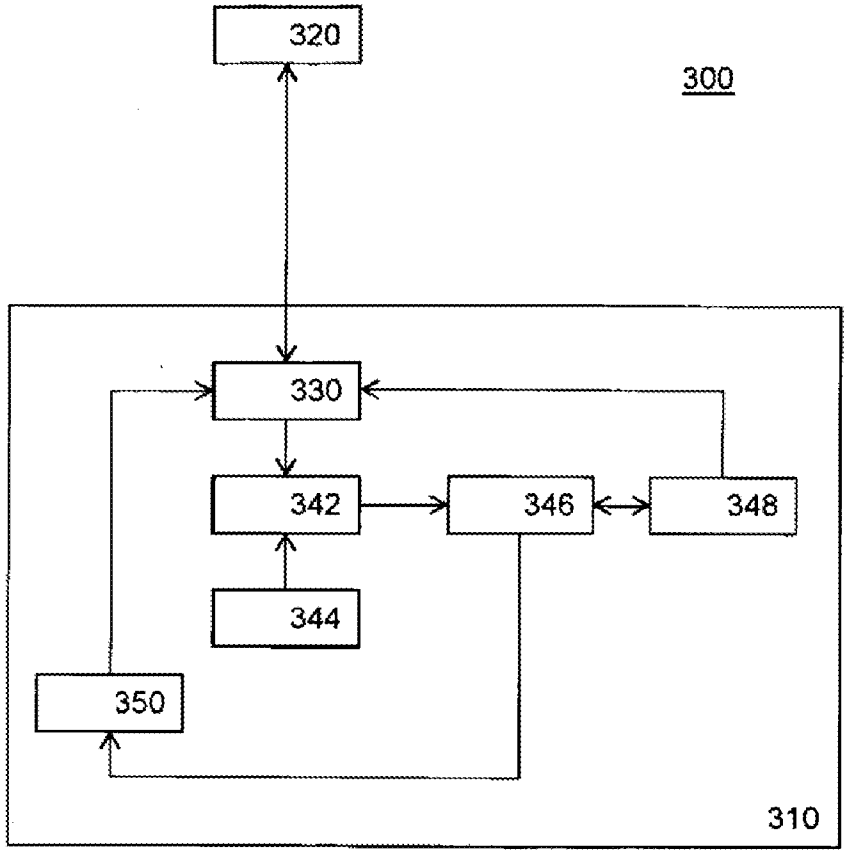

Figura 3

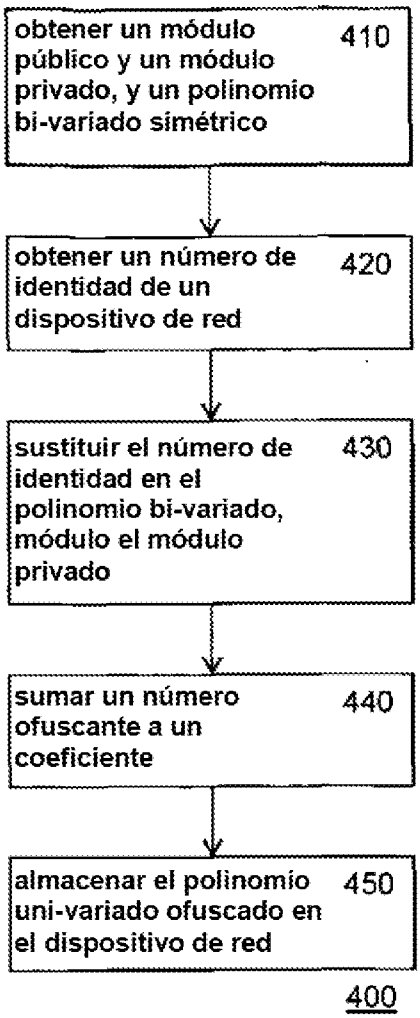

Figura 4

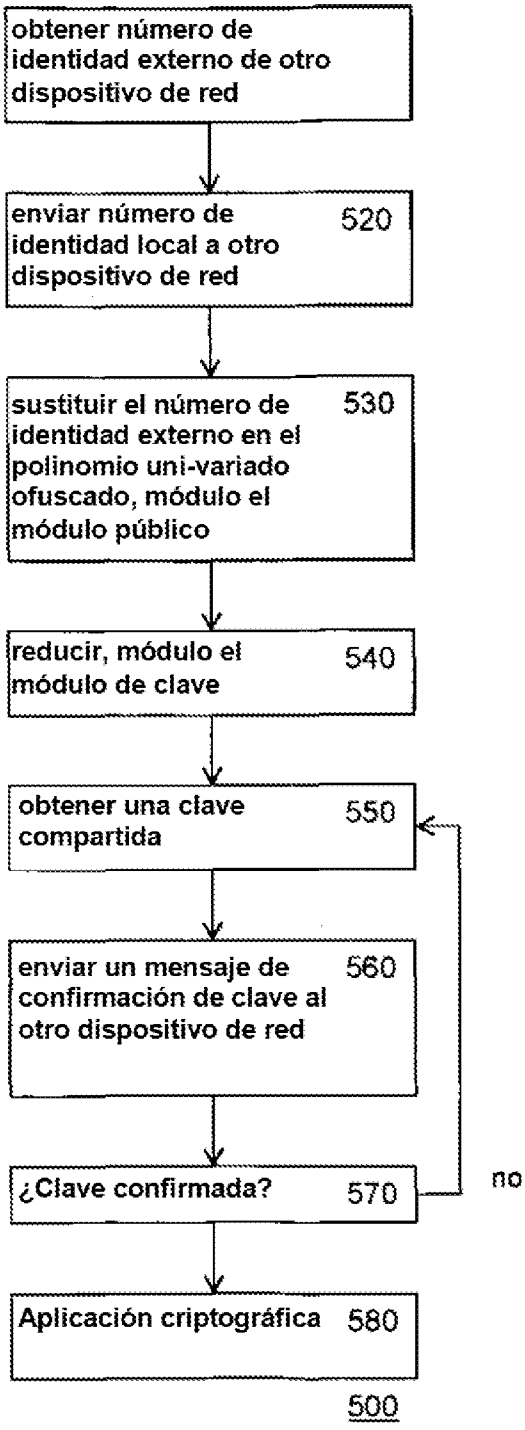

Figura 5

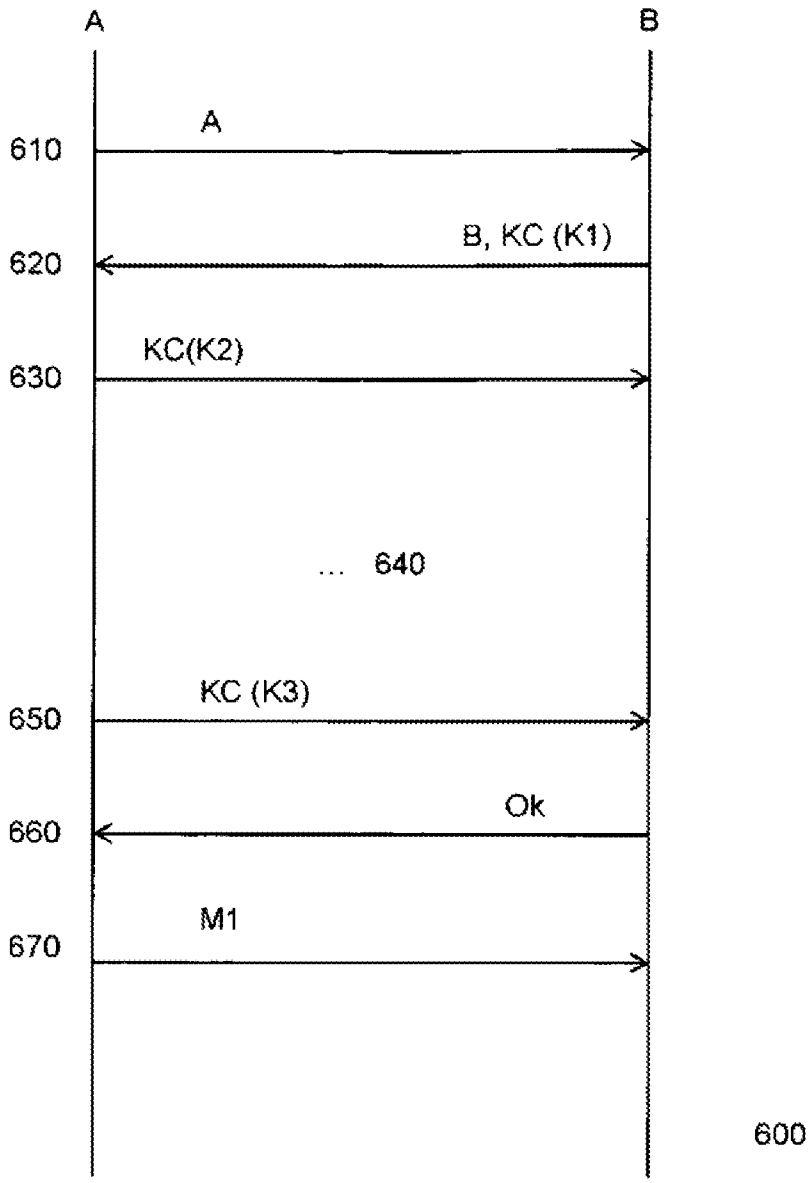

Figura 6