(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 788 638**

(51) Int. CI.:

H03M 13/09 (2006.01)
H04L 9/32 (2006.01)
H03M 13/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.07.2016 PCT/EP2016/068151**

(87) Fecha y número de publicación internacional: **23.03.2017 WO17045824**

(96) Fecha de presentación y número de la solicitud europea: **29.07.2016 E 16750131 (1)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2020 EP 3314768**

(54) Título: **Dispositivo y procedimiento para la creación de una suma de comprobación asimétrica**

(30) Prioridad:

16.09.2015 DE 102015217724

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.10.2020

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

ASCHAUER, HANS

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Dispositivo y procedimiento para la creación de una suma de comprobación asimétrica

La invención se refiere a un procedimiento y aparatos para la formación de una suma de comprobación asimétrica y para la verificación de la suma de comprobación asimétrica.

Ocasionalmente se producen errores durante la transmisión de datos, que modifican los datos transmitidos. Para evitar esto, a menudo se calcula una llamada suma de comprobación de los datos y transmite o almacena junto con estos. Cuando se reciben o leen los datos, se calcula de nuevo la suma de comprobación y se compara con la suma de comprobación transmitida. Si las dos sumas de comprobación son iguales, entonces se parte de que existe una alta probabilidad de que no se haya producido ningún error. El nivel de esta probabilidad se puede calcular o estimar en principio a partir de las propiedades del procedimiento de cálculo (función de suma de comprobación) y el modelo de error asumido.

La mayoría de las veces, para aplicaciones específicas existe el requisito de que la función de suma de comprobación se pueda calcular de manera eficiente. Ejemplos de tales funciones de suma de comprobación son CRC16 (verificación de redundancia cíclica 16) o CRC32 (verificación de redundancia cíclica 32). En el caso de aparatos relevantes para la seguridad, los clientes o las normativas a menudo requieren ciertos niveles de integridad de seguridad, como se especifica, por ejemplo, en la norma de seguridad EN 61508. Para ello se requiere una evaluación de riesgos, en cuyo marco también se verifican las funciones de suma de comprobación utilizadas. En este caso, por ejemplo, se debe proporcionar una prueba de que debido un error en la secuencia del programa, a pesar de que la suma de comprobación es realmente errónea, esta se reconoce por error como correcta.

A este respecto existe el problema fundamental aquí de que, según el estado de la técnica, el algoritmo para verificar la suma de comprobación también contiene el algoritmo para calcular la suma de comprobación.

En principio, un receptor de un mensaje tiene que calcular la suma de comprobación por sí mismo, donde el receptor también se denomina a continuación como verificador o aparato verificador. En el caso de un mal funcionamiento del aparato verificador, generalmente se parte de que el aparato verificador calcula de nuevo accidentalmente la suma de comprobación a través de los datos falsificados y compara el resultado de los dos cálculos propios, lo que anula la función de la suma de comprobación, de modo que ya no se pueden detectar errores. Si el verificador reenvía los datos con la suma de comprobación falsificada, otros verificadores ya no podrían reconocer los errores.

Por Helmut Witten et al.: “Kann man RSA vertrauen? Asymmetrische Kryptografie für die Sekundarstufe I”, folleto LOG IN, Informatische Bildung für Computer in der Schule, 1 de diciembre de 2012, páginas 79-91 y disponible en http://bscw.schule.de/pub/bscw.cgi/d1024037/RSA Sekl.pdf así como anónimo: ""RSA-Kryptosystem” - Versionsunterschied-Wikipedia”, 15 de septiembre de 2015, páginas 1-4 y disponible en https://de.wikipedia.org/w/index.php?title=RSA-Kryptosystem&diff=1463057000&oldid=145881181 se conocen procedimientos estándares para la criptografía asimétrica utilizando una función unidireccional.

El objeto de la presente invención es proporcionar un procedimiento y aparatos para el cálculo y verificación de una suma de comprobación asimétrica.

El objetivo se consigue mediante las características indicadas en las reivindicaciones independientes. En las reivindicaciones dependientes están representados perfeccionamientos ventajosos de la invención.

Según un primer aspecto, la invención se refiere a un procedimiento para la creación asistida por ordenador de una suma de comprobación asimétrica por un primer interlocutor de comunicación, en el que un procesador está programado para realizar los pasos del procedimiento. El procedimiento comprende un paso del procedimiento para el cálculo de una suma de comprobación reproducida por medio de un mapeo biyectivo de una primera suma de comprobación, donde la primera suma de comprobación del conjunto de todas las sumas de comprobación posibles por medio una primera función se le asigna respectivamente a un mensaje de un conjunto de todos los mensajes posibles, donde la primera suma de comprobación se prepara para la primera cantidad, en particular mapeando el conjunto de todas las sumas de comprobación posibles, mediante una segunda función. El procedimiento comprende otro paso del procedimiento para la distribución de una información, que define una función inversa para el mapeo biyectivo, a al menos a un segundo interlocutor de comunicación, donde por medio de la función inversa se calcula la primera suma de comprobación a partir de la suma de comprobación asimétrica, donde la primera suma de comprobación del conjunto de todas las sumas de comprobación posibles por medio una primera función se le asigna respectivamente a un mensaje de un conjunto de todos los mensajes posibles, donde la primera suma de comprobación se prepara para la primera cantidad, en particular mapeando el conjunto de todas las sumas de comprobación posibles, mediante una segunda función. El procedimiento comprende otro paso del procedimiento para la distribución de una información, que define una función inversa para el mapeo biyectivo, a al menos a un segundo interlocutor de

comunicación, donde por medio de la función inversa se calcula la primera suma de comprobación a partir de la suma de comprobación asimétrica. El procedimiento comprende otro paso del procedimiento para la transmisión de la suma de comprobación mapeada y el mensaje al menos un segundo interlocutor de comunicación.

En particular, la preparación de la primera suma de comprobación se realiza mapeando el conjunto de todas las sumas de comprobación posibles mediante la segunda función en el primer conjunto antes de que se calcule el mapeo biyectivo.

Con el procedimiento se garantiza que el segundo interlocutor de comunicación, igualmente designado como receptor, verificador o aparato verificador, no calcule por error la suma de comprobación correcta, aunque el mensaje a verificar sea erróneo. Por ejemplo, debido a un error en la secuencia del programa puede ocurrir que, a pesar de que el mensaje o la suma de comprobación son realmente erróneo, estos se reconocen por error como correctos.

Con el procedimiento también se garantiza que el segundo interlocutor de comunicación no esté en posesión de la información para calcular accidentalmente la suma de comprobación mapeada. La información que define la función inversa es suficiente para la verificación de la suma de comprobación. Debido a la estructura asimétrica de la generación de la suma de comprobación y la verificación de la suma de comprobación, el algoritmo de verificación ya no contiene el algoritmo para la generación de la suma de comprobación.

El procedimiento usa preferentemente procedimientos asimétricos no criptográficos para calcular una suma de comprobación asimétrica, para que la suma de comprobación asimétrica se pueda calcular lo más rápido posible. Para que el procedimiento sea lo más eficiente posible, por ejemplo, las longitudes clave de los procedimientos utilizados se pueden elegir muy cortas. Por lo tanto, estas se pueden elegir mucho más cortas de lo que se requeriría para aplicaciones críticas de seguridad.

La preparación del conjunto de todas las sumas de comprobación posibles mediante la segunda función para el primer conjunto puede servir para llevar las sumas de comprobación en primer lugar a un formato con el que solo sea posible un mapeo biyectivo o con el que un mapeo biyectivo sea particularmente fácil de calcular. En una implementación concreta, por ejemplo, la segunda función prepara la primera suma de comprobación antes de que se calcule el mapeo biyectivo.

En el procedimiento se le envía, además del mensaje y la suma de comprobación mapeada, la primera suma de comprobación al segundo interlocutor de comunicación.

Mediante el envío de la primera suma de comprobación al segundo interlocutor de comunicación se mejora aún más la verificación de la corrección del mensaje. Esto se logra porque se compara la primera suma de comprobación adicionalmente con la suma de comprobación, que se calcula por el segundo interlocutor de comunicación.

En otras formas de realización del procedimiento, el cálculo de la suma de comprobación mostrada forma un secreto que se conoce por el primer interlocutor de comunicación.

Dado que solo el primer interlocutor de comunicación conoce cómo se calcula la suma de comprobación mapeada, es extremadamente improbable que mediante un error de programación para un mensaje erróneo se calcule por error una suma de comprobación correcta.

En otras formas de realización del procedimiento, la preparación de la primera suma de comprobación con la segunda función se realiza en un primer paso de preprocesamiento antes del cálculo de la suma de comprobación mapeada, donde el mapeo biyectivo es en particular un mapeo del primer conjunto sobre sí mismo.

Según un otro aspecto, la invención se refiere a un procedimiento para la verificación asistida por ordenador de un mensaje por medio de una suma de comprobación asimétrica por un segundo interlocutor de comunicación, en el que un procesador está programado para realizar los pasos del procedimiento. El procedimiento comprende un paso del procedimiento para la recepción de información, que define una función inversa para un mapeo biyectivo, de un primer interlocutor de comunicación. El procedimiento comprende otro paso del procedimiento para la recepción de una suma de comprobación mapeada y un mensaje de un primer interlocutor de comunicación. El procedimiento comprende otro paso del procedimiento para el cálculo de una segunda suma de comprobación por medio de la función inversa usando la suma de comprobación mapeada, donde la segunda suma de comprobación del conjunto de todas las posibles sumas de comprobación por medio de una primera función se le asigna respectivamente a un mensaje de un conjunto de todos los mensajes posibles, donde el conjunto de todos las sumas de comprobación posibles se mapean a un primer conjunto con una segunda función, donde el mapeo biyectivo es un mapeo del primer conjunto sobre sí mismo. El procedimiento comprende otro paso del procedimiento para el cálculo de una tercera suma de comprobación sobre del mensaje. El

procedimiento comprende otro paso del procedimiento para la constatación de una corrección del mensaje si la segunda suma de comprobación presenta una concordancia con la tercera suma de comprobación.

En el procedimiento, además del mensaje y la suma de comprobación asimétrica se recibe una primera suma de comprobación del primer interlocutor de comunicación, donde la primera suma de comprobación se compara adicionalmente con la segunda suma de comprobación y/o la tercera suma de comprobación y donde se determina la corrección del mensaje si la primera suma de comprobación presenta una concordancia con la segunda suma de comprobación y/o la tercera suma de comprobación.

Mediante la recepción de la primera suma de comprobación del primer interlocutor de comunicación se mejora aún más la verificación de la corrección del mensaje. Esto se logra porque se compara la primera suma de comprobación adicionalmente con la suma de comprobación, que se calcula por el segundo interlocutor de comunicación.

En otras formas de realización del procedimiento, la preparación de la tercera suma de comprobación con la segunda función se realiza en un segundo paso de preprocesamiento antes de la constatación de la corrección del mensaje, donde el mapeo biyectivo es en particular un mapeo del primer conjunto sobre sí mismo.

En general, mediante la preparación de una suma de comprobación por la segunda función se puede llevar, por ejemplo, la suma de comprobación a una forma con la que sea posible primeramente un mapeo biyectivo, el mapeo biyectivo sea más fácil de calcular o el mapeo biyectivo cumpla ciertas propiedades predefinidas, como condiciones matemáticas. La información sobre la segunda función se le puede transmitir al segundo interlocutor de comunicación por separado o estar contenida en la información sobre la función inversa.

En otras formas de realización del procedimiento, la segunda función mapea una suma de comprobación de 64 bits en una suma de comprobación de 32 bits o la segunda función es la identidad.

El mapeo se puede calcular de manera muy eficiente mediante un procesador en diferentes arquitecturas de ordenador. A este respecto, su uso como segunda función es particularmente adecuado, ya que esta se puede calcular rápidamente simplemente cortando los bits sobrantes.

La identidad se puede utilizar, por ejemplo, para casos de aplicación en los que la segunda función no debe modificar la cantidad de todas las sumas de comprobación posibles o la primera suma de comprobación.

En otras formas de realización del procedimiento, el primer conjunto o el conjunto de todas las sumas de comprobación posibles es un monoide, donde el monoide comprende el elemento uno como elemento neutro y está definida una operación de combinación para el monoide, donde el primer interlocutor de comunicación selecciona un elemento invertible del monoide, donde el primer interlocutor de comunicación calcula un elemento invertido para el elemento invertible, donde la suma de comprobación mapeada se forma por medio del mapeo biyectivo en forma de combinación de la primera suma de comprobación con el elemento invertible, donde la información comprende el elemento invertido, y donde la combinación, en particular, del elemento invertible y la suma de comprobación asimétrica produce el elemento uno.

Una implementación del procedimiento en base a un monoide ofrece la ventaja de que el procedimiento se puede implementar de manera muy eficiente. Se puede utilizar, por ejemplo, en sistemas con capacidad de cálculo limitada, como las tarjetas con chip, de modo que la tarjeta con chip pueda generar la suma de comprobación asimétrica.

En otras formas de realización del procedimiento, la segunda suma de comprobación se calcula por medio de la función inversa en la forma de la comprobación del elemento invertido con la suma de comprobación mapeada.

Una implementación del procedimiento en base a un monoide ofrece la ventaja de que el procedimiento se puede implementar de manera muy eficiente. Se puede utilizar, por ejemplo, en sistemas con capacidad de cálculo limitada, como las tarjetas con chip, de modo que la tarjeta con chip pueda verificar la suma de comprobación asimétrica.

En otras formas de realización del procedimiento, el primer conjunto o el conjunto de todas las sumas de comprobación posibles es un espacio vectorial, donde el primer interlocutor de comunicación forma una matriz invertible a partir del espacio vectorial, donde el primer interlocutor de comunicación forma una matriz invertida a partir de la matriz invertible, donde la información comprende la matriz invertida, y donde la suma de comprobación asimétrica se forma por medio del mapeo biyectivo en forma de multiplicación matricial de la primera suma de comprobación con la matriz.

Una implementación del procedimiento en base a matrices y una multiplicación matricial ofrece la ventaja de que el procedimiento se puede calcular extremadamente rápido en arquitecturas informáticas, que están optimizadas

con respecto a los vectores y cálculos matriciales. Estos pueden ser, por ejemplo, ordenadores vectoriales o tarjetas gráficas.

En otras formas de realización del procedimiento, la segunda suma de comprobación se calcula por medio de la función inversa en forma de multiplicación matricial, en tanto que la matriz invertida se multiplica por la suma de comprobación mapeada.

Una implementación del procedimiento en base a matrices y una multiplicación matricial ofrece la ventaja de que el procedimiento se puede calcular extremadamente rápido en arquitecturas informáticas, que están optimizadas con respecto a los vectores y cálculos matriciales. Estos pueden ser, por ejemplo, ordenadores vectoriales o tarjetas gráficas.

En otras formas de realización del procedimiento, el primer interlocutor de comunicación forma una primera tabla, en la que se asigna respectivamente una suma de comprobación asimétrica a todas las sumas de comprobación posibles, donde el primer interlocutor de comunicación forma una segunda tabla, en la que se asigna una suma de comprobación respectivamente a una suma de comprobación asimétrica, donde la primera tabla es el mapeo biyectivo y la segunda tabla es la función inversa del mapeo biyectivo, y donde la información sobre una función inversa comprende la segunda tabla.

Una implementación del procedimiento en base a tablas permite una realización del procedimiento en sistemas extremadamente débiles en cálculo, como los chips RFID. Las tablas se pueden implementar como tablas de búsqueda (LUT) o tablas de conversión. El uso de tablas tiene en particular la ventaja de que no es necesario un cálculo de una suma de comprobación mapeada en tiempo de ejecución.

En otras formas de realización del procedimiento, la segunda suma de comprobación se calcula por medio de la función inversa en la forma de la segunda tabla.

Una implementación del procedimiento en base a tablas permite una realización del procedimiento en sistemas extremadamente débiles en cálculo, como los chips RFID. Las tablas se pueden implementar como tablas de búsqueda (LUT) o tablas de conversión. El uso de tablas tiene en particular la ventaja de que no es necesario calcular la segunda suma de comprobación en tiempo de ejecución.

En otras formas de realización del procedimiento, una suma de comprobación mapeada se implementa como un número o como un valor alfanumérico.

Las tablas se pueden generar de una manera particularmente simple mediante la representación de la suma de comprobación mapeada como un número o como un valor alfanumérico.

Según otro aspecto, la invención se refiere a un primer interlocutor de comunicación para la generación de una suma de comprobación asimétrica. El primer interlocutor de comunicación presenta un primer dispositivo de cálculo y un dispositivo de transmisión. El primer dispositivo de cálculo calcula con un procesador una suma de comprobación reproducida por medio de un mapeo biyectivo de una primera suma de comprobación, donde la primera suma de comprobación del conjunto de todas las sumas de comprobación posibles por medio una primera función se le asigna respectivamente a un mensaje de un conjunto de todos los mensajes posibles, donde la primera suma de comprobación se prepara para la primera cantidad, opcionalmente en particular mapeando el conjunto de todas las sumas de comprobación posibles, mediante una segunda función. El dispositivo de transmisión envía información, que define una función inversa para el mapeo biyectivo, a al menos un segundo interlocutor de comunicación de forma distribuida, donde la primera suma de comprobación se calcula a partir de la suma de comprobación mapeada por medio de la función inversa y el dispositivo de transmisión transmite la suma de comprobación mapeada, la primera suma de comprobación y el mensaje al menos un segundo interlocutor de comunicación.

En una primera forma de realización del primer aparato de comunicación, el primer aparato de comunicación es un primer aparato de comunicación virtualizado.

Un primer aparato de comunicación virtualizado tiene la ventaja de que se puede usar de manera económica en un sistema de cálculo virtualizado y prescinde del hardware costoso.

Según otro aspecto, la invención se refiere a un segundo interlocutor de comunicación para la verificación de un mensaje por medio de una suma de comprobación asimétrica, que presenta un dispositivo receptor y un segundo dispositivo de cálculo. El dispositivo receptor recibe información, que define una función inversa para un mapeo biyectivo, de un primer interlocutor de comunicación y el dispositivo receptor recibe una suma de comprobación mapeada, una primera suma de comprobación y un mensaje del primer interlocutor de comunicación. El segundo dispositivo de cálculo calcula con un procesador una segunda suma de comprobación por medio de la función inversa usando la suma de comprobación mapeada. El segundo dispositivo de cálculo calcula con el procesador una tercera suma de comprobación sobre el mensaje, donde la tercera suma de comprobación del conjunto de

todas las sumas de comprobación posibles por medio una primera función se le asigna respectivamente a un mensaje de un conjunto de todos los mensajes posibles, donde la tercera suma de comprobación se prepara para la primera cantidad, en particular mapeando el conjunto de todas las sumas de comprobación posibles, mediante una segunda función. El segundo dispositivo de cálculo constata una corrección del mensaje si la segunda suma de comprobación presenta una concordancia con la tercera suma de comprobación y, adicionalmente, el segundo dispositivo de cálculo constata la corrección del mensaje si la primera suma de comprobación presenta una concordancia con la segunda suma de comprobación y/o la tercera suma de comprobación.

En una primera forma de realización del segundo aparato de comunicación, el segundo aparato de comunicación es un segundo aparato de comunicación virtualizado.

Un segundo aparato de comunicación virtualizado tiene la ventaja de que se puede usar de manera económica en un sistema de cálculo virtualizado y prescinde del hardware costoso.

Además, un circuito integrado, por ejemplo una FPGA o un ASIC, se reivindica con las características según la invención mencionadas. Además, se reivindica un circuito integrado que se equipa con pasos de configuración para la realización del procedimiento mencionado según la invención o está configurado con pasos de configuración, de modo que el circuito integrado presente las características según la invención del primer dispositivo de comunicación o del segundo dispositivo de comunicación.

Además se reivindica un producto de programa informático con instrucciones de programa para la realización del procedimiento mencionado según la invención. Además, se reivindica un dispositivo de facilitación para el almacenamiento y/o facilitación de una estructura de datos que comprende el producto del programa informático. El dispositivo de facilitación es, por ejemplo, un soporte de datos que almacena y/o facilita el producto de programa informático. Alternativamente, el dispositivo de facilitación es, por ejemplo, un sistema informático, un sistema de servidor, una red, un sistema de cálculo basado en la nube y/o un sistema de cálculo virtual que almacena y/o proporciona el producto del programa informático. Esta facilitación se realiza preferentemente como una descarga del producto completo del programa informático, pero también se puede realizar, por ejemplo, como una descarga parcial, que consta de varias partes y se descarga en particular a través de una red de igual a igual. Un producto de programa informático semejante se lee, por ejemplo, usando el dispositivo de facilitación en forma del soporte de datos en un sistema y ejecuta las instrucciones de programa, de modo que el procedimiento según la invención se lleva a un ordenador para la ejecución.

Las propiedades, características y ventajas descritas anteriormente de esta invención, así como el modo y manera en cómo se consiguen se harán comprensibles de forma más clara y obvia en relación con la siguiente descripción de ejemplos de realización que se explican más en detalle en relación con las figuras. A este respecto muestran:

Fig. 1 un diagrama de flujo de un ejemplo de realización para la generación de una suma de comprobación asimétrica;

Fig. 2 un diagrama de flujo de un ejemplo de realización para la verificación de una suma de comprobación asimétrica;

Fig. 3 una representación esquemática de un ejemplo de realización de un primer interlocutor de comunicación;

Fig. 4 una representación esquemática de un ejemplo de realización de un segundo interlocutor de comunicación; y

Fig. 5 una representación esquemática de un ejemplo de realización de un sistema informático con un primer interlocutor de comunicación y un segundo interlocutor de comunicación.

En las figuras los elementos iguales funcionalmente se proveen de las mismas referencias, siempre y cuando no se indique lo contrario.

La fig. 1 es un diagrama de flujo de un ejemplo de realización para la generación de una suma de comprobación asimétrica.

Para calcular una suma de comprobación asimétrica, que también se designa como la suma de comprobación mapeada c', para un mensaje m, por medio de la primera función F_1, por ejemplo, una función de suma de comprobación se puede asignar en primer lugar a cada mensaje individual del conjunto de todos los mensajes M suma de comprobación c del conjunto de todas las sumas de comprobación C:

$$F_1: M \rightarrow C \qquad \text{(Fórmula 1)}$$

Para un mensaje m se calcula por consiguiente en primer lugar una primera suma de comprobación c_1 por medio de la primera función.

Una segunda función F_2 prepara la primera suma de comprobación c_1 en un primer paso de preprocesamiento. Este paso de preprocesamiento es opcional, es decir, no obligatoriamente necesario, pero tiene la ventaja de que la primera suma de comprobación c_1, por ejemplo, para llevarlo a una representación, solo es posible primeramente para un mapeo biyectivo. También se puede seleccionar una representación en la que el mapeo biyectivo sea más fácil de calcular o el mapeo biyectivo cumpla ciertas propiedades predefinidas, por ejemplo, condiciones matemáticas. Estos cálculos también se pueden realizar preferentemente por el segundo interlocutor de comunicación igualmente para que este último pueda verificar la suma de comprobación mapeada transmitida c'. Los detalles de esto se explican en el ejemplo de realización correspondiente en la figura 2.

Expresado de manera más general, la segunda función F_2 se utiliza para mapear el conjunto de todas las sumas de comprobación posibles C para un primer conjunto C', donde de este modo se mapea la primera suma de comprobación c_1. Por lo tanto, la primera suma de comprobación c_1 antes del primer paso de preprocesamiento es un elemento del conjunto de todas las sumas de comprobación posibles C y después de usar la segunda función F_2 la primera suma de comprobación es, por lo tanto, un elemento del primer conjunto C'. La primera suma de comprobación c_1 también se puede designar como una primera suma de comprobación preparada después de este primer paso de preprocesamiento.

$$F_2: C \rightarrow C' \qquad \text{(Fórmula 2)}$$

En una variante, la segunda función F_2 es una función que mapea una suma de comprobación de 64 bits cortando los bits en una suma de comprobación de 32 bits.

En otra variante, la segunda función F_2 es una función que mapea el conjunto de todas las sumas de comprobación posibles C sin cambios en el primer conjunto C'. Esto puede ser útil, por ejemplo, para poner a disposición el conjunto de todas las posibles sumas de comprobación C sin cambios para cálculos posteriores.

En otras palabras, también es posible, por ejemplo, aplicar la segunda función F_2 siempre en la primera suma de comprobación c_1. En escenarios de aplicación en los que la primera suma de comprobación c_1 o el conjunto de todas las sumas de comprobación posibles C se debe proporcionar sin cambios o sin preparación para otros pasos de cálculo, para la segunda función F_2 se puede seleccionar, por ejemplo, una función de identidad o un mapeo idéntico del conjunto de todas las sumas de comprobación posibles C en el primer conjunto C'.

Para calcular la suma de comprobación mapeada c’ para un mensaje m por un primer interlocutor de comunicación en un primer paso del procedimiento 105, se usa un mapeo biyectivo G del primer conjunto C' o del conjunto de todas las posibles de comprobación sumas sobre sí mismo. En otras palabras, el mapeo biyectivo G es una función que realiza una permutación de las sumas de comprobación mostradas c', donde la primera suma de comprobación c_1 es un parámetro de entrada para el mapeo biyectivo G.

Por consiguiente se puede calcular fácilmente la suma de comprobación mapeada c’ para la primera suma de comprobación c_1.

$$c' = G(c_1) \qquad \text{(Fórmula 3)}$$

Con la ayuda de una función inversa G^{-1} para el mapeo, la primera suma de comprobación c_1, que se puede haber preparado mediante la segunda función F_2 o la primera suma de comprobación preparada, se puede calcular de nuevo a partir de la suma de comprobación mapeada c'.

$$c_1 = G^{-1}(c') \qquad \text{(Fórmula 4)}$$

Mediante el mapeo biyectivo G o la suma de comprobación asimétrica c’ se evita que el mapeo biyectivo G genere el mismo resultado que la función inversa G^{-1} o la función inversa G^{-1} genere el mismo resultado que el mapeo biyectivo G. En particular, para el mapeo biyectivo G y la función inversa G^{-1} está excluida una involución. En otras palabras, se excluye de este modo que concuerden el mapeo biyectivo G y la función inversa G^{-1}. Un ejemplo de tal involución sería una operación O-exclusiva de la primera suma de comprobación c_1 con una constante a.

$$G(c_1) = c_1 \text{ xor } a \qquad \text{(Fórmula 5)}$$

Según del modelo de cálculo o la arquitectura de cálculo, ciertas variantes del cálculo se excluyen del mapeo biyectivo. En particular, se excluyen los cálculos del siguiente tipo:

$$G(c_1) = c_- + a \bmod 2^{32} \qquad \text{(Fórmula 6)}$$

donde mod es la operación de módulo. Tal cálculo de la suma de comprobación mapeada es problemático porque la función inversa G^{-1} presenta para la fórmula 6

$$G^{-1}(c') = c' - a \bmod 2^{32} \qquad \text{(Fórmula 7)}$$

una sustracción. En este sentido, esto es problemático porque la sustracción en la mayoría de las unidades aritméticas difiere de la adición solo en un bit, es decir, un simple interruptor.

En otras palabras, para el mapeo biyectivo G y la función inversa G^{-1} está excluida preferentemente una involución. Además, el mapeo biyectivo G y la función inversa G^{-1} satisfacen preferentemente la condición de que el cálculo del mapeo biyectivo G y la función inversa G^{-1} es tan diferente en cada caso que los errores de bit triviales no proporcionan un resultado idéntico para las dos funciones. Esto se aplica en particular a la operación de adición y la operación de sustracción.

Para que un segundo interlocutor de comunicación pueda verificar la suma de comprobación mapeada c', a este se le proporciona información en un segundo paso del procedimiento 110 que define la función inversa G^{-1}. Esta disposición puede tener lugar en un momento anterior, por ejemplo, de modo que esta información se pueda utilizar para muchas de las sumas de comprobación mapeadas.

En un tercer paso del procedimiento 115, la suma de comprobación mapeada c' y el mensaje m se le transmiten al segundo interlocutor de comunicación.

La fig. 2 es un diagrama de flujo de un ejemplo de realización para la verificación de una suma de comprobación asimétrica. Las reglas de cálculo y las condiciones matemáticas, que ya se han explicado en la descripción de la figura 1, también son aplicables a las siguientes explicaciones de las figuras 2 - 5.

Para verificar la suma de comprobación asimétrica por un segundo interlocutor de comunicación, en un cuarto paso del procedimiento 150, la información que define la función inversa G^{-1} para el mapeo biyectivo G, se recibe por el primer interlocutor de comunicación.

En un quinto paso del procedimiento 155, la primera suma de comprobación mapeada c' y el mensaje m se reciben por el primer interlocutor de comunicación.

En un sexto paso del procedimiento 160, una segunda suma de comprobación c_2 se calcula por medio de la función inversa G^{-1} usando la suma de comprobación mapeada c' y usando, por ejemplo, un procesador. A este respecto, la segunda suma de comprobación c_2 corresponde a la primera suma de comprobación c_1, que se puede haber preparado por la segunda función F_2. Si la segunda función F_2 prepara la primera suma de comprobación c_1, entonces la segunda función F_2 se conoce preferentemente por el segundo interlocutor de comunicación.

En un séptimo paso del procedimiento 165 se calcula entonces una tercera suma de comprobación c_3 sobre el mensaje m. Para ello, se usa la primera función F_1 para que se use el mismo algoritmo para el cálculo de la suma de comprobación respectivamente a través del mensaje m. Además, la segunda función F_2 se aplica en un segundo paso de preprocesamiento en la tercera suma de comprobación c_3, análogamente a la aplicación de la segunda función F_2 en la primera suma de comprobación c_1. Sin embargo, el segundo paso de preprocesamiento solo se realiza si esto es realmente necesario, es decir, el primer paso de preprocesamiento se ha realizado en la generación de la suma de comprobación mapeada c'. La tercera suma de comprobación se puede designar después de la aplicación de la segunda función F_2 también como la tercera suma de comprobación preparada.

En una octava etapa del procedimiento 170 se constata la corrección del mensaje m si la segunda suma de comprobación c_2 presenta una concordancia suficiente con la tercera suma de comprobación c_3.

Para los cálculos o para la primera función F_1 de la primera suma de comprobación c_1 y de la tercera suma de comprobación c_3 se utiliza la misma función de suma de comprobación. Igualmente para la segunda función F_2 se usa respectivamente igualmente el mismo algoritmo, siempre que el primer paso de preprocesamiento se haya realizado durante la generación de la suma de comprobación mapeada c'. A este respecto, la segunda suma de comprobación c_2 corresponde a la primera suma de comprobación c_1.

La información sobre la primera función F_1 y segunda función F_2 puede ser conocida en general, intercambiarse entre los socios de comunicación a través de un mensaje separado, configurarse por un administrador y/o estar contenida en la información de la función inversa G^{-1}.

La secuencia básica del procedimiento entre el primer interlocutor de comunicación y el segundo interlocutor de comunicación se explica a continuación.

La regla de cálculo para formar el mapeo biyectivo G está implementada del lado del primer interlocutor de comunicación. La regla de cálculo para la función inversa G^{-1} está implementada del lado del segundo interlocutor de comunicación. El primer interlocutor de comunicación calcula la primera suma de comprobación c_1 a través del mensaje m, prepara la primera suma de comprobación c_1 con la segunda función F_2 y luego forma la suma de comprobación mapeada asociada c'. Además de la primera suma de comprobación c_1 (o, en un ejemplo que no está dentro del alcance de la invención, en lugar de la primera suma de comprobación c_1) se transmite entonces la suma de comprobación mapeada c'.

El mensaje m y la suma de comprobación adicional mapeada c' llegan al segundo interlocutor de comunicación. El segundo interlocutor de comunicación ahora calcula la tercera suma de comprobación c_3 y luego aplica la segunda función F_2 en la tercera suma de comprobación c_3 en. Además, calcula la segunda suma de comprobación c_2 y compara el resultado con la tercera suma de comprobación c_3. Si no se han producido errores de transmisión, la segunda suma de comprobación c_2 y la tercera suma de comprobación c_3 son idénticas. Si adicionalmente se ha transmitido la primera suma de comprobación c_1, la primera suma de comprobación c_1 concuerda con la segunda suma de comprobación c_2 si la suma de comprobación mapeada c' se ha transmitido sin errores.

Si se han producido errores de transmisión, la segunda suma de comprobación c_2 y la tercera suma de comprobación c_3 no son iguales con una probabilidad elevada.

Dado que el segundo interlocutor de comunicación no conoce el mapeo biyectivo G, el segundo interlocutor de comunicación no puede calcular la primera suma de comprobación c_1 y, por lo tanto, no usar accidentalmente (o incluso reenviar) una suma de comprobación falsa sin que esto se note más adelante.

A este respecto, a diferencia de los procedimientos criptográficos, es irrelevante para la aplicación mencionada si se puede calcular de manera eficiente el mapeo biyectivo G a partir de la función inversa G^{-1}. Es suficiente que el cálculo del mapeo biyectivo G a partir de la función inversa G^{-1} sea lo suficientemente no trivial, por ejemplo, requiera un algoritmo que no se implementa del lado del segundo interlocutor de comunicación, de modo que este cálculo no se pueda realizar "accidentalmente".

En una variante de los ejemplos de realización descritos, el mapeo biyectivo G y la función inversa G^{-1} se implementa por medio de una combinación monoide.

A este respecto, el primer conjunto C' es un monoide, es decir, un semigrupo con elemento neutral 1 y combinación "*". Si la segunda función F_2 no se ha aplicado al conjunto de todas las sumas de comprobación C, el monoide es el conjunto de todas las sumas de comprobación C.

El primer interlocutor de comunicación selecciona un elemento invertible a del monoide, donde es válido

$$a * a_{inv} = 1 \qquad \text{(Fórmula 8)}$$

a_{inv} es el elemento invertido respecto al elemento invertible a. El primer interlocutor de comunicación distribuye el elemento invertido a_{inv} al segundo interlocutor de comunicación y mantiene el elemento invertible a.

El mapeo biyectivo es dado por

$$G(c_1) = c_1 * a \qquad \text{(Fórmula 9)}$$

Y la función inversa G^{-1} es dada por

$$G^{-1}(c') = c' * a_{inv} \qquad \text{(Fórmula 10)}$$

Una posible implementación por medio de un monoide se explica en detalle a continuación.

A continuación, el monoide es dado por el conjunto {0x0, 0x1, 0x2,..., Oxffffffff} junto con el módulo de multiplicación 0x100000000. Esta multiplicación modular se puede implementar de manera muy eficiente, dado que del resultado de la multiplicación normal simplemente se usan los 32 bits menos significativos.

En este monoide se puede invertir cualquier número impar. Por ejemplo, si el elemento invertible es a = 0xc0c17487, entonces el elemento invertido es a_{inv} = 0xa4751137. Esto se puede calcular, por ejemplo, con ayuda del algoritmo euclidiano. El producto del elemento invertible a y del elemento invertido a_{inv} es

$$a \bullet a_{inv} = 0x7bd4140700000001$$
$$= 1 \bmod 0x100000000 \qquad \text{(Fórmula 11)}$$

donde "•" es la multiplicación de números enteros.

La primera función es F_1 es una función de suma de comprobación, por ejemplo, la función CRC32. Aquí es posible seleccionar como segunda función F_2 el mapeo idéntico, ya que el conjunto de imágenes de CRC32 concuerda con el monoide.

Ahora, por ejemplo, sea la primera suma de comprobación c_1 = 0x82441710 la suma de comprobación CRC32 de un mensaje adecuado m para el que se ha aplicado la segunda función F_2, entonces la suma de comprobación mapeada c' está definida por

$$c' = c * a = 0xef6b6970 \qquad \text{(Fórmula 12)}$$

Este número se le transmite al segundo interlocutor de comunicación junto con el mensaje m.

El segundo interlocutor de comunicación ahora calcula la tercera suma de comprobación c_3 con la ayuda de la función CRC 32 sobre el mensaje m y luego aplica la segunda función F_2 en esto. Además, se calcula la segunda suma de comprobación c_2:

$$c_2 = c' * a_{inv} = 0x82441710 \qquad \text{(Fórmula 13)}$$

Sin concuerda la segunda suma de comprobación c_2 y la tercera suma de comprobación c_3, el mensaje m se considera libre de errores. Sin embargo, el segundo interlocutor de comunicación no podría calcular la suma de comprobación mapeada c' ya que no conoce el elemento invertible a y el algoritmo euclidiano no se ha implementado.

Además del módulo de multiplicación de una potencia de 2 descrito anteriormente para la construcción del monoide, también sería concebible, por ejemplo, un módulo de multiplicación de un número primo p. El monoide resultante es entonces un grupo si se excluye el 0. De ello se desprende que cada elemento es invertible. El cálculo del inverso se realiza nuevamente con ayuda del algoritmo euclidiano. Dado que el número primo p es una constante, la multiplicación modular se puede implementar de manera eficiente, por ejemplo calculando previamente 1/p con suficiente precisión, por lo que se simplifica la división en una multiplicación.

En una variante de los ejemplos de realización descritos, el mapeo biyectivo G y la función inversa G^{-1} se implementa por medio de matrices y la multiplicación matricial.

El primer conjunto C' o el conjunto de todas las sumas de comprobación C es un espacio vectorial y el primer interlocutor de comunicación forma una matriz A invertible a partir del espacio vectorial.

$$A = C' * C' \qquad \text{(Fórmula 14)}$$

El primer interlocutor de comunicación calcula una matriz invertida $A.^{-1}$ a la matriz invertible A y la distribuye al segundo interlocutor de comunicación.

El mapeo biyectivo es dado por

$$G(c_1) = A * c_1 \qquad \text{(Fórmula 15)}$$

donde "*" es la multiplicación matricial.

Y la función inversa G^{-1} es dada por

$$G^{-1}(c') = A^{-1} * c' \qquad \text{(Fórmula 16)}$$

En otra variante de los ejemplos de realización descritos, el mapeo biyectivo G y la función inversa G^{-1} se implementa por medio de tablas.

El mapeo biyectivo G o la suma de comprobación mapeada c' se forma en este caso por una primera tabla en la que está almacenado un valor adecuado para su mapeo biyectivo G o G(c) para cada suma de comprobación c. Aquí, las sumas de comprobación también pueden haberse preparado mediante la segunda función F_2 antes de ser procesadas. La primera suma de comprobación c_1 se utiliza como valor de entrada, por ejemplo, para una

tabla de conversión, a fin de calcular la suma de comprobación mapeada c'. La función inversa G^{-1} o la segunda suma de comprobación c_2 se calcula mediante una segunda tabla que contiene la suma de comprobación apropiada para cada suma de comprobación mapeada. En otras palabras, la suma de comprobación mapeada c' se usa como el valor de entrada para la segunda tabla, a fin de obtener la segunda suma de comprobación c_2.

La figura 3 es una representación esquemática de un ejemplo de realización de un primer interlocutor de comunicación 200, que también se denomina aparato de generación o transmisor. El aparato de generación presenta un primer dispositivo de cálculo 210 y un dispositivo de transmisión 220, que están conectados entre sí en comunicación a través de un bus 230.

El primer dispositivo de cálculo 210 calcula con un procesador 211 una suma de comprobación reproducida por medio de un mapeo biyectivo de una primera suma de comprobación, donde la primera suma de comprobación del conjunto de todas las sumas de comprobación posibles por medio una primera función se le asigna respectivamente a un mensaje de un conjunto de todos los mensajes posibles, donde la primera suma de comprobación se prepara para la primera cantidad, en particular mapeando el conjunto de todas las sumas de comprobación posibles, mediante una segunda función.

El dispositivo de transmisión 220 distribuye una información, que define una función inversa del mapeo biyectivo, a al menos un segundo interlocutor de comunicación, que también se denomina verificador o aparato de verificación, donde por medio de la función inversa se calcula la primera suma de comprobación a partir de la suma de comprobación mapeada. El dispositivo de transmisión 220 transmite adicionalmente la suma de comprobación mostrada y el mensaje al menos un segundo interlocutor de comunicación.

La figura 4 es una representación esquemática de un ejemplo de realización de un segundo interlocutor de comunicación 300, que también se denomina emisor, verificador o aparato verificador. El aparato verificador presenta un dispositivo receptor 310 y un segundo dispositivo de cálculo 320, que están conectados entre sí en comunicación a través de un bus 350.

El dispositivo receptor 310 recibe una información, que define una función inversa a un mapeo biyectivo, de un primer interlocutor de comunicación, que también se denomina aparato de generación. Adicionalmente, el dispositivo receptor 310 recibe una suma de comprobación mapeada y un mensaje del primer interlocutor de comunicación.

El segundo dispositivo de cálculo 320 calcula con un procesador 321 una segunda suma de comprobación por medio de la función inversa usando la suma de comprobación mapeada.

El segundo dispositivo de cálculo 320 calcula adicionalmente preferentemente con el procesador 321 una tercera suma de comprobación sobre el mensaje, donde la tercera suma de comprobación del conjunto de todas las sumas de comprobación posibles por medio una primera función se le asigna respectivamente a un mensaje de un conjunto de todos los mensajes posibles, donde la tercera suma de comprobación se prepara para la primera cantidad, en particular mapeando el conjunto de todas las sumas de comprobación posibles, mediante una segunda función.

Además, el segundo dispositivo de cálculo 320 constata una corrección del mensaje si la segunda suma de comprobación presenta una concordancia suficiente con la tercera suma de comprobación.

La fig. 5 es una representación esquemática de un ejemplo de realización de un sistema informático 500.

El sistema informático 500 comprende un primer interlocutor de comunicación 200 como se describe en la figura 3, por ejemplo en forma de una primera ordenador, por ejemplo un ordenador personal compatible con IBM con un sistema operativo Linux. El primer interlocutor de comunicación 200 está conectado a través de una red, por ejemplo, una red Ethernet o una red de anillo de token, con un segundo interlocutor de comunicación 300 según la descripción de la figura 4 en forma de una segunda ordenador, por ejemplo un Apple iMac®.

El primer interlocutor de comunicación 200 y el segundo interlocutor de comunicación 300 comprenden, por ejemplo, respectivamente componentes de hardware disponibles comercialmente, tales como un aparato de visualización, preferentemente en forma de monitor TFT, en particular al menos un aparato de entrada, preferentemente en forma de un ratón de ordenador y/o teclado, al menos un soporte de datos, preferentemente en forma de disco duro de estado sólido y/o una unidad de lectura y/o escritura de DVD, un procesador, preferentemente un procesador compatible con Intel x86, una interfaz de red, preferentemente una interfaz Ethernet, memoria, preferentemente DDR SDRAM (*Double Data Rate Synchronous Dynamic Random Access Memory*), y/u otro hardware o dispositivos periféricos conocidos por el experto en la materia.

Los componentes de hardware del primer interlocutor de comunicación 200 están conectados entre sí por comunicación, por ejemplo, a través de una placa de circuitos impresos principal y un bus de datos. Los componentes de hardware del segundo interlocutor de comunicación 300 están conectados igualmente entre sí

por comunicación, por ejemplo, a través de una placa de circuitos impresos principal y un bus de datos. Las placas de circuitos impresos principales respectivas del primer interlocutor de comunicación 200 y el segundo interlocutor de comunicación 300 disponen preferentemente de al menos una ranura u otras interfaces, por ejemplo un bus serie universal (USB) o una interfaz FireWire, para conectar un dispositivo periférico al procesador a través del bus de datos. La ranura está diseñada preferentemente como un bus expreso de interconexión de componentes periféricos (PCIe).

El procedimiento que se ha explicado en la descripción de las figuras 2 y 3 se implementa, por ejemplo, por medio de un dispositivo o varios dispositivos que están configurados como una tarjeta enchufable o aparato USB. Esta tarjeta enchufable se inserta, por ejemplo, en la ranura y, por lo tanto, presenta una conexión en comunicación con los componentes de hardware y/o periféricos adicionales.

En una variante, el procedimiento se implementa por medio de un código de programa que se ejecuta por el procesador.

En otra variante, el primer interlocutor de comunicación 200 ejecuta, por ejemplo, al menos un ordenador virtualizada que presenta una tarjeta enchufable virtualizada que implementa el procedimiento, o implementa el procedimiento por código de programa que se ejecuta por el procesador virtualizado.

En una otra variante, el procedimiento se implementa, por ejemplo, por un servidor de terminal por medio de una tarjeta enchufable o código de programa, donde el servidor de terminal puede ser igualmente un servidor de terminal virtualizado. Luego, el servidor terminal sirve a un cliente terminal de modo que un usuario u otro programa pueda ejecutar el procedimiento.

En otra variante, el primer interlocutor de comunicación es un primer proceso o un primer programa y el segundo interlocutor de comunicación es un segundo proceso o un segundo programa que se ejecuta en un ordenador.

En una otra variante, un circuito integrado, por ejemplo una FPGA o un ASIC, puesto en un estado por medio de comandos de programa, se puede llevar a un estado a fin de ejecutar el procedimiento según la invención.

Aunque la invención se ha ilustrado y descrito más en detalle mediante los ejemplos de realización, así la invención no está limitada por los ejemplos dados a conocer y se pueden derivar otras variaciones por parte del experto en la materia sin abandonar el alcance de protección de la invención.

REIVINDICACIONES

1. Procedimiento para la creación asistida por ordenador y la transmisión de una suma de comprobación asimétrica para un mensaje (m) por un primer interlocutor de comunicación (200), en el que un procesador (211) realiza los siguientes pasos del procedimiento:

- cálculo (105) de la suma de comprobación asimétrica (c') a partir de una primera suma de comprobación (c_1) por medio de un mapeo biyectivo (G) de un primer conjunto (C')

- la primera suma de comprobación (c_1) de un conjunto de todas las sumas de comprobación posibles (C) por medio de una primera función (F_1) se le asigna al mensaje (m) a partir de un conjunto de todos los mensajes posibles (M),

- la primera suma de comprobación (c_1) se prepara para la primera cantidad (C'), en particular mapeando el conjunto de todas las sumas de comprobación posibles (C), mediante una segunda función (F_2);

- distribución (110) de una información, que define una función inversa (G^{-1}) para el mapeo biyectivo (G), a al menos a un segundo interlocutor de comunicación (300), donde por medio de la función inversa (G^{-1}) se calcula la primera suma de comprobación (c_1) a partir de la suma de comprobación asimétrica (c'); y

- transmisión (115) de la suma de comprobación asimétrica (c') y el mensaje (m) al menos un segundo interlocutor de comunicación (300);

caracterizado porque además del mensaje (m) y la suma de comprobación asimétrica (c'), la primera suma de comprobación (c_1) se le envía al segundo interlocutor de comunicación (300).

2. Procedimiento según la reivindicación 1, donde el cálculo de la suma de comprobación asimétrica (c') forma un secreto que es conocido por el primer interlocutor de comunicación (200).

3. Procedimiento según cualquiera de las reivindicaciones anteriores, donde

- la preparación de la primera suma de comprobación (c_1) con la segunda función (F_2) se realiza en un primer paso de preprocesamiento antes del cálculo de la suma de comprobación asimétrica (c'), y

- el mapeo biyectivo (G) es en particular un mapeo del primer conjunto (C') sobre sí mismo.

4. Procedimiento para la verificación asistida por ordenador de un mensaje por medio de una suma de comprobación asimétrica por un segundo interlocutor de comunicación (300), en el que un procesador (321) está programado para realizar los siguientes pasos:

- recepción (150) de una información, que define una función inversa (G^{-1}) para un mapeo biyectivo (G) de un primer conjunto (C'), de un primer interlocutor de comunicación (200);

- recepción (155) de la suma de comprobación asimétrica (c') y el mensaje (m) de un primer interlocutor de comunicación (200);

- cálculo (160) de una segunda suma de comprobación (c_2) por medio de la función inversa (G^{-1}) utilizando la suma de comprobación asimétrica (c');

- cálculo (165) de una tercera suma de comprobación (c_3) sobre el mensaje (m), donde

  - la tercera suma de comprobación (c_3) del conjunto de todas las sumas de comprobación posibles (C) por medio de una primera función (F_1) se le asigna al mensaje (m) a partir de un conjunto de todos los mensajes posibles (M),

  - la tercera suma de comprobación (c_3) se prepara para la primera cantidad (C'), en particular mapeando el conjunto de todas las sumas de comprobación posibles (C), mediante una segunda función (F_2); y

- constatación (170) de una corrección del mensaje (m) si la segunda suma de comprobación (c_2) presente una concordancia con la tercera suma de comprobación (c_3);

caracterizado porque además del mensaje (m) y la suma de comprobación asimétrica (c') se recibe una primera suma de comprobación (c_1) del primer interlocutor de comunicación, donde la primera suma de

comprobación (c_1) se compara adicionalmente con la segunda suma de comprobación (c_2) y/o la tercera suma de comprobación (c_3) y donde se determina la corrección del mensaje (m) si la primera suma de comprobación (c_1) presenta una concordancia con la segunda suma de comprobación (c_2) y/o la tercera suma de comprobación (c_3).

5. Procedimiento según cualquiera de las reivindicaciones anteriores, donde

- la preparación de la tercera suma de comprobación (c_3) con la segunda función (F_2) se realiza en un segundo paso de preprocesamiento antes de la constatación de la corrección del mensaje (m),

- el mapeo biyectivo (G) es en particular un mapeo del primer conjunto (C') sobre sí mismo.

6. Procedimiento según la reivindicación 5, donde

- la segunda suma de comprobación (c_2) corresponde a la primera suma de comprobación (c_1) que se ha preparado por la segunda función (F_2), y

- la primera suma de comprobación (c_1) y la tercera suma de comprobación (c_3) son, en particular, respectivamente un elemento del primer conjunto (C').

7. Procedimiento según cualquiera de las reivindicaciones anteriores, donde la segunda función (F_2) mapea una suma de comprobación de 64 bits en una suma de comprobación de 32 bits o es la identidad.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, donde

- el primer conjunto (C') o el conjunto de todas las sumas de comprobación posibles (C) es un monoide,

- el monoide comprende el elemento uno como elemento neutro y está definida una operación de combinación para el monoide,

- el primer interlocutor de comunicación (200) selecciona un elemento invertible (a) del monoide;

- el primer interlocutor de comunicación (200) calcula un elemento invertido (a_{inv}) para el elemento invertible (a);

- la suma de comprobación mapeada (c') se forma por medio del mapeo biyectivo (G) en forma de combinación de la primera suma de comprobación (c_1) con el elemento invertible (a),

- la información comprende el elemento invertido (a_{inv}); y

- la combinación, en particular, del elemento invertible (a) y la suma de comprobación asimétrica (c') produce el elemento uno.

9. Procedimiento según la reivindicación 8, donde la segunda suma de comprobación (c_2) se calcula por medio de la función inversa (G^{-1}) en forma de combinación del elemento invertido (a_{inv}) con la suma de comprobación asimétrica (c').

10. Procedimiento según cualquiera de las reivindicaciones 1 - 7, donde

- el primer conjunto (C') o el conjunto de todas las sumas de comprobación posibles (C) es un espacio vectorial;

- el primer interlocutor de comunicación (200) forma una matriz invertible (A) a partir del espacio vectorial;

- el primer interlocutor de comunicación (200) forma una matriz invertida (A^{-1}) a partir de la matriz invertible (A);

- la información comprende la matriz invertida (A^{-1}); y

- la suma de comprobación asimétrica (c') se forma por medio del mapeo biyectivo (G) en forma de multiplicación matricial de la primera suma de comprobación (c_1) con la matriz (A).

11. Procedimiento según la reivindicación 10, donde la segunda suma de comprobación (c_2) se calcula por medio de la función inversa (G^{-1}) en forma de multiplicación matricial, en tanto que la matriz invertida (A^{-1}) se multiplica por la suma de comprobación asimétrica (c').

12. Procedimiento según cualquiera de las reivindicaciones 1 - 7, donde

- el primer interlocutor de comunicación (200) forma una primera tabla, en la que se asigna respectivamente una suma de comprobación asimétrica (c') a todas las sumas de comprobación posibles (C);

- el primer interlocutor de comunicación (200) forma una segunda tabla, en la que se asigna una suma de comprobación respectivamente a una suma de comprobación asimétrica (c');

- la primera tabla es el mapeo biyectivo (G) y la segunda tabla es la función inversa (G^{-1}) del mapeo biyectivo; y

- la información sobre una función inversa comprende la segunda tabla.

13. Procedimiento según la reivindicación 12, donde la segunda suma de comprobación (c_2) se calcula por medio de la función inversa (G^{-1}) en la forma de la segunda tabla.

14. Procedimiento según la reivindicación 12 o 13, donde la suma de comprobación asimétrica (c') se implementa como una cifra o como un valor alfanumérico.

15. Primer interlocutor de comunicación (200) para la creación y transmisión de una suma de comprobación asimétrica para un mensaje, que presenta:

- un primer dispositivo de cálculo que con un procesador (211) calcula la suma de comprobación asimétrica (c') a partir de una primera suma de comprobación (c_1) por medio de un mapeo biyectivo (G) de un primer conjunto (C'), donde

  - la primera suma de comprobación (c_1) del conjunto de todas las sumas de comprobación posibles (C) por medio de una primera función (F_1) se le asigna al mensaje (m) a partir de un conjunto de todos los mensajes posibles (M),

  - la primera suma de comprobación (c_1) se prepara para la primera cantidad (C'), en particular mapeando el conjunto de todas las sumas de comprobación posibles (C), mediante una segunda función (F_2);

- un dispositivo de transmisión (220) que

  - distribuye una información, que define una función inversa (G^{-1}) para el mapeo biyectivo (G), a al menos a un segundo interlocutor de comunicación (300), donde por medio de la función inversa (G^{-1}) se calcula la primera suma de comprobación (c_1) a partir de la suma de comprobación asimétrica (c'); y

  - la suma de comprobación asimétrica (c') y el mensaje (m) se le transmiten al menos un segundo interlocutor de comunicación (300),

caracterizado porque el dispositivo de transmisión, además de la suma de comprobación asimétrica (c') y el mensaje (m), envía la primera suma de comprobación (c_1) al menos un segundo interlocutor de comunicación (300).

16. Primer interlocutor de comunicación (200) según la reivindicación 15, donde el primer interlocutor de comunicación (200) es un primer aparato de comunicación virtualizado.

17. Segundo interlocutor de comunicación (300) para verificar un mensaje por medio de una suma de comprobación asimétrica, que comprende:

- un dispositivo receptor (310) que

  - recibe una información, que define una función inversa (G^{-1}) para un mapeo biyectivo (G) de un primer conjunto (C'), de un primer interlocutor de comunicación;

  - recibe la suma de comprobación asimétrica (c') y el mensaje (m) del primer interlocutor de comunicación;

- un segundo dispositivo de cálculo (320), que con un procesador (321)

- calcula una segunda suma de comprobación (c_2) por medio de la función inversa (G^{-1}) utilizando la suma de comprobación asimétrica (c');

- calcula una tercera suma de comprobación (c_3) sobre el mensaje (m), donde

- la tercera suma de comprobación (c_3) del conjunto de todas las sumas de comprobación posibles (C) por medio de una primera función (F_1) se le asigna al mensaje (m) a partir de un conjunto de todos los mensajes posibles (M),

- la tercera suma de comprobación (c_3) se prepara para una primera cantidad (C'), en particular mapeando el conjunto de todas las sumas de comprobación posibles (C), mediante una segunda función (F_2); y

- constata una corrección del mensaje (m) si la segunda suma de comprobación (c_2) presenta una concordancia con la tercera suma de comprobación (c_3), **caracterizado porque** el dispositivo receptor, además del mensaje (m) y la suma de comprobación asimétrica (c'), recibe una primera suma de comprobación (c_1) del primer interlocutor de comunicación y el segundo dispositivo de cálculo compara adicionalmente la primera suma de comprobación (c_1) con la segunda suma de comprobación (c_2) y/o la tercera suma de comprobación (c_3) y se constata la corrección del mensaje (m) si la primera suma de comprobación (c_1) presenta una concordancia con la segunda suma de comprobación (c_2) y/o la tercera suma de comprobación (c_3).

18. Segundo interlocutor de comunicación (300) según la reivindicación 17, donde el segundo interlocutor de comunicación (300) es un segundo aparato de comunicación virtualizado.

19. Sistema informático (500) que presenta

- un primer aparato de comunicación (200) según la reivindicación 15 o 16, y

- un aparato de comunicación (300) según la reivindicación 17 o 18.

20. Circuito integrado que se equipa con pasos de configuración para realizar el procedimiento según cualquiera de las reivindicaciones 1-14 o está configurado con pasos de configuración de manera que el circuito integrado presenta las características del primer dispositivo de comunicación según la reivindicación 15 o 16, o del segundo dispositivo de comunicación según la reivindicación 17 o 18.

21. Producto de programa informático con instrucciones de programa para la realización del procedimiento según cualquiera de las reivindicaciones 1-14.

22. Dispositivo de facilitación para el producto de programa informático según la reivindicación 21, donde el dispositivo de facilitación almacena y/o proporciona el producto de programa informático.

FIG 1

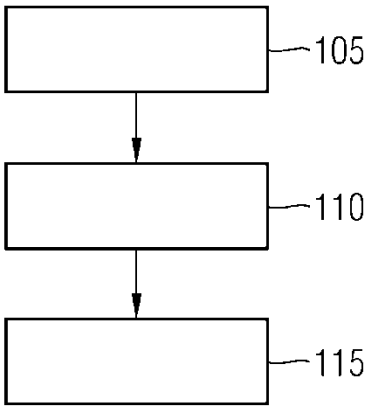

FIG 2

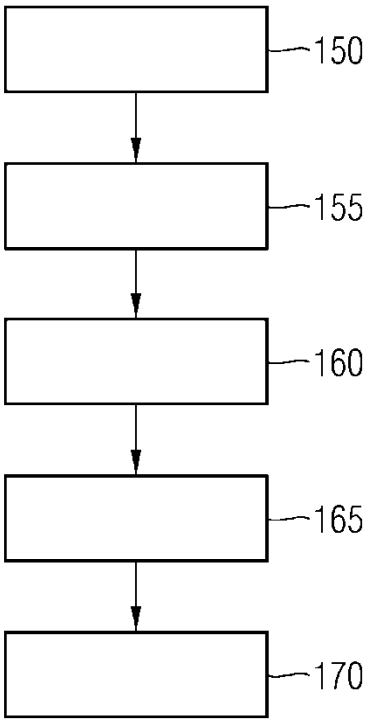

FIG 3

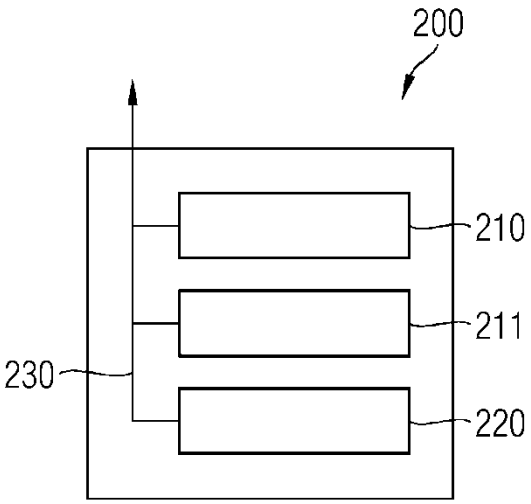

FIG 4

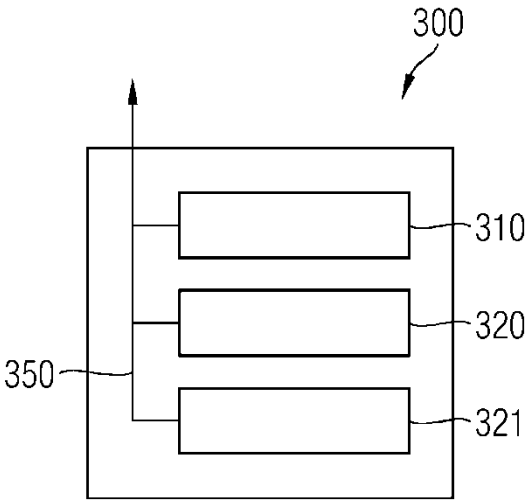

FIG 5