(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 798 325**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.10.2017 PCT/EP2017/077843**

(87) Fecha y número de publicación internacional: **11.05.2018 WO18083075**

(96) Fecha de presentación y número de la solicitud europea: **31.10.2017 E 17797894 (7)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3535925**

(54) Título: **Alcance de un acuerdo sobre un valor secreto**

(30) Prioridad:

04.11.2016 EP 16197277

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.12.2020

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 52
5656 AG Eindhoven, NL

(72) Inventor/es:

TOLHUIZEN, LUDOVICUS MARINUS GERARDUS MARIA;
RIETMAN, RONALD y
GARCIA MORCHON, OSCAR

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Alcance de un acuerdo sobre un valor secreto

Campo de la invención

La invención se refiere a un método para ser realizado por un primer dispositivo para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo.

La invención se refiere además a un método a desarrollar por un segundo dispositivo para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo.

La invención se refiere además al primer dispositivo, para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo.

La invención se refiere además a un segundo dispositivo, para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo.

La invención se refiere además a un sistema que comprende un segundo dispositivo para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo y un primer dispositivo.

La invención en particular se refiere a dos dispositivos que ya tienen un acuerdo aproximado sobre un valor secreto, para alcanzar un acuerdo exacto sobre el valor secreto.

Antecedentes de la invención

Muchas aplicaciones actuales hacen uso de un protocolo de intercambio de claves en el que dos partes A y B desean generar un valor compartido. Dichos protocolos pueden estar relacionados con el conocido protocolo de intercambio de claves Diffie-Hellman. Para resistir el criptoanálisis, las partes introducen algunos pequeños errores en los cálculos del protocolo. Como resultado, las partes A y B pueden obtener valores, digamos v_A, v_B que coinciden casi, pero no necesariamente de manera exacta. Para llegar a un acuerdo exacto, una de las partes, digamos A, envía a la otra parte, B, un valor de bit, digamos h, que es indicativo del valor secreto v_A que se ha calculado. La parte A también calcula un valor s_A a partir del valor v_A. La Parte B luego calcula un valor S_B a partir de h y su propio valor v_B. El diseño del sistema puede ser tal que los valores s_A y s_B secretos sean iguales si los valores v_A y v_B estuvieran lo suficientemente cerca uno del otro. Un ejemplo de tal sistema se divulga en J. Ding, X. Xie y X. Lin, "A simple provably secure key exchange scheme based on the learning with errors problem", Archivo de criptología ePrint, Reporte 2012/688, 2012, http://eprint.iacr.org/2012/688.pdf (en lo sucesivo denominado como "Ding").

C. Peikert, "Lattice Cryptography for the Internet", Actas del sexto taller sobre criptografía postcuántica, PQ Crypto 2014, Springer LNCS, vol. 8772, 2014, pp. 197-219 (en lo sucesivo denominado como "Peikert"), divulga un método en el que los valores s_a s_b secretos compartidos generados son estadísticamente imparciales, es decir, se distribuyen uniformemente. En la configuración de Peikert, el valor secreto obtenido por las dos partes es un solo bit.

Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan y Douglas Stebila, "Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE", IACR Archivo de criptología ePrint, Informe 2016/659, https://eprint.iacr.org/2016/659 (en lo sucesivo denominado como "Bos" o "Frodo"), divulga una extensión del método de Peikert para que las partes acuerden sobre un valor secreto que es distribuido uniformemente sobre un conjunto de enteros. En los métodos citados de la técnica anterior, se envía un único bit de reconciliación. Tanto en el método Peikert como en el método Bos, si las partes necesitan ponerse de acuerdo en muchos bits, el método se aplica en paralelo en múltiples instancias para alcanzar un acuerdo. En todas las referencias anteriores, se puede lograr un acuerdo clave exacto si los valores inicialmente obtenidos, v_A, v_B calculados por las dos partes no difieren demasiado.

Erdem Alkim, Leo Ducas, Thomas Pöppelmann, Peter Schwabe, "Post-quantum key exchanges - a new hope", Asociación internacional para la investigación criptográfica, diciembre de 2017, páginas 1-33, modifican el protocolo de Pekert y proponen nuevos parámetros y una distribución de errores más adecuada para Ring-LWE, y codifica un bit clave en cuatro coordenadas del texto cifrado.

Deguchi Kana, Motohiko Isaka, "Approximate performance bound for coding in secret key agreement from the Gaussian channel", IEEE WCNC, marzo de 2015, páginas 458-463, discuten una variante de la codificación asimétrica de Slepian-Wolf, mostrando que el límite derivado proporciona una predicción precisa de la probabilidad de error cuando el recurso ruidoso es el canal Gaussiano de entrada binaria.

Resumen de la invención

Sería ventajoso tener una forma mejorada de alcanzar un acuerdo entre dos dispositivos en un valor secreto. Para abordar mejor esta preocupación, un primer aspecto de la invención proporciona un segundo dispositivo, para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo, que comprende:

un receptor configurado para recibir información indicativa de datos h de reconciliación del primer dispositivo, en donde $0 \leq h < 2^{\delta}$, en donde δ es un entero mayor que 1; y

un procesador configurado para calcular un secreto s común con base en un valor b entero y una ecuación

$$s \equiv \left\lfloor \frac{b+c-h\frac{q}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}+\frac{q}{2^{B+1}}}{\frac{q}{2^{B}}} \right\rfloor \ mod\ 2^{B}\ ,$$

en donde b satisface $0 \leq b < q$, B es un entero positivo, y q es un múltiplo entero de $2^{B+\delta+1}$, en donde q, B, δ, y c son parámetros del sistema.

Como los datos auxiliares están en el rango de $0 \leq h < 2^{\delta}$, en donde δ es un entero mayor que 1, los datos h auxiliares que el primer dispositivo envía al segundo dispositivo consisten en múltiples bits. En este sistema, se puede lograr un acuerdo clave exacto incluso al imponer una condición menos estricta sobre el acuerdo aproximado entre los valores a y b. El dispositivo establecido permite determinar el secreto s común utilizando los datos h auxiliares que el segundo dispositivo recibe del primer dispositivo, de modo que se logra un acuerdo exacto.

Específicamente, se logra un acuerdo exacto cuando el primer dispositivo usa un número a de acuerdo aproximado con el número b, en el sentido de que $a \equiv b + e\ (mod\ q)$, en donde e representa una diferencia entre los números a y b, en donde la restricción $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$ permite una diferencia relativamente grande entre a y b. Esta propiedad permite el uso de un algoritmo de intercambio de claves más seguro.

Como alternativa, para una condición de acuerdo aproximada dada, el sistema se puede usar para alcanzar un acuerdo exacto sobre un valor s secreto que tiene al menos un bit más que es el caso, en por ejemplo, la técnica anterior divulgada en Peikert o Bos.

En un ejemplo particular, el procesador está configurado para calcular b con base en un protocolo de intercambio de claves. Este protocolo de intercambio de claves puede ser, por ejemplo, uno de los protocolos de intercambio de claves descritos en Ding, Peikert y Bos, o una variante del mismo, lo que conduce a un acuerdo aproximado sobre una clave. El dispositivo establecido permite posteriormente alcanzar un acuerdo exacto de una manera eficiente, como se describió anteriormente.

En un ejemplo particular, $q = 2^{m}$ y $\delta = m - B - 1$, en donde m es un entero positivo. Esta configuración permite alcanzar un acuerdo sobre múltiples bits mientras se utilizan relativamente pocos bits de reconciliación.

En un ejemplo particular, el procesador está configurado para calcular el valor b con base en un valor β y una ecuación $b \equiv w\beta\ (\text{mod}\ q)$, en donde wN ≡ 1 (mod q), en donde N es un entero mayor que 1 y es relativamente primo para q. Esto permite soportar una situación en la que el acuerdo aproximado entre el valor α del primer dispositivo y el valor β del segundo dispositivo está presente de acuerdo con una condición α ≡ β + Ne (mod q), en la que $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$.

De acuerdo con otro aspecto de la invención, se divulga un primer dispositivo para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo, en donde el primero comprende:

un procesador configurado para:

determinar un secreto s común con base en un valor a entero y una ecuación

$$s = \left\lfloor \frac{(a+c)\ mod\ q}{\frac{q}{2^{B}}} \right\rfloor ,$$

en donde a satisface 0 ≤ a <q, B es un entero positivo, q es un múltiplo entero de $2^{B+\delta+1}$, en donde δ es un entero mayor que 1, en donde q, B, δ y c son parámetros del sistema, y

determinar un dato h de reconciliación con base en una ecuación

$$h = \left\lfloor \frac{((a+c) mod\ q) mod \left(\frac{q}{2^B}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor;$$

y

un transmisor configurado para transmitir información indicativa de los datos h de reconciliación al segundo dispositivo.

Como los datos h auxiliares están en el rango de $0 \leq h < 2^{\delta}$, en donde δ es un entero mayor que 1, los datos h auxiliares que el primer dispositivo envía al segundo dispositivo consisten en múltiples bits. En este sistema, se puede lograr un acuerdo de clave exacto incluso al imponer una condición menos estricta en el acuerdo aproximado entre los valores a y b del primer dispositivo y el segundo dispositivo. El dispositivo establecido permite generar y transmitir los datos h auxiliares que el segundo dispositivo necesita para determinar el secreto s común, de modo que se logre un acuerdo exacto.

Específicamente, se logra un acuerdo exacto cuando el primer dispositivo usa un número a de acuerdo aproximado con el número b, en el sentido de que $a \equiv b + e \pmod q$, en donde e representa una diferencia entre los números a y b, en donde la restricción $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$ permite una diferencia relativamente grande entre a y b. Esta propiedad permite el uso de un algoritmo de intercambio de claves más seguro.

Alternativamente, para una condición de acuerdo aproximada dada, el sistema se puede usar para alcanzar un acuerdo exacto sobre un valor s secreto que tiene al menos un bit más de lo que es el caso, por ejemplo, en la técnica anterior divulgada en Peikert o Bos.

En un ejemplo particular, el procesador está configurado para calcular a con base en un protocolo de intercambio de claves. Este protocolo de intercambio de claves puede ser, por ejemplo, uno de los protocolos de intercambio de claves divulgadas en Ding, Peikert y Bos, o una variante del mismo, lo que conduce a un acuerdo aproximado sobre una clave.

En un ejemplo particular, $q = 2^m$, en donde m es un entero positivo, el secreto s común corresponde a Bits B más significativos de una expansión binaria de $(a + c) \bmod 2^m$, y los datos h de reconciliación corresponden al siguiente bits δ de la expansión binaria. Esta es una representación particularmente atractiva de los componentes de datos que juntos forman a. En un ejemplo aún más específico, δ = m - B - 1. Este valor permite reconciliar múltiples bits a la vez, mientras usa relativamente pocos bits para los datos h auxiliares. Por ejemplo, este valor de δ permite reconciliar un bit más que con el método divulgado en Bos, bajo las mismas condiciones de acuerdo aproximado.

En un ejemplo particular, c = 0. En ese caso, el secreto s común es igual a un cociente de *a* y $\left(\frac{q}{2^B}\right)$, redondeado hacia abajo al entero más cercano.

En un ejemplo particular, $c = \frac{q}{2^{B+1}}$. En ese caso, el secreto s común es igual a un cociente de a y $\left(\frac{q}{2^B}\right)$, redondeado al entero más cercano, en donde el redondeo se desarrolla hacia arriba en caso de empate.

En un ejemplo particular, $c = \frac{q}{2^{B+1}} - 1$. En ese caso, el secreto s común es igual a un cociente de a y $\left(\frac{q}{2^B}\right)$, redondeado al entero más cercano, en donde el redondeo se desarrolla hacia abajo en caso de empate.

En un ejemplo particular, el procesador está configurado para calcular el valor a con base en un valor α y una ecuación $a \equiv w\alpha \pmod q$, en donde $wN \equiv 1 \pmod q$, en donde N es un entero mayor que 1 , en donde N es relativamente primo para q. Esto permite soportar una situación en la que el acuerdo aproximado entre el valor α del primer dispositivo y el valor β del segundo dispositivo está presente de acuerdo con una condición $\alpha \equiv \beta + Ne \pmod q$, en la que $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$.

De acuerdo con otro aspecto de la invención, se presenta un sistema que comprende el primer dispositivo y el segundo dispositivo expuesto anteriormente, en donde el número a está en acuerdo aproximado con el número b, en el sentido de que $a \equiv b + e \ (mod\ q)$, en donde e representa una diferencia entre los números a y b, en la que $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$.

Esto permite que los dos dispositivos, que tienen un acuerdo aproximado sobre los valores a y b, lleguen a un acuerdo exacto sobre un secreto s común, transmitiendo los datos h de reconciliación del primer dispositivo al segundo dispositivo.

De acuerdo con otro aspecto de la invención, un segundo dispositivo debe desarrollar un método para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo, en donde el método comprende:

recibir información indicativa de datos h de reconciliación del primer dispositivo, en donde $0 \leq h < 2^{\delta}$, en el que δ es un entero mayor que 1; y

calcular un secreto s común con base en un valor b entero y una ecuación

$$s \equiv \left\lfloor \frac{b+c-h\frac{q}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}+\frac{q}{2^{B+1}}}{\frac{q}{2^{B}}} \right\rfloor \ mod\ 2^{B},$$

en donde b satisface $0 \leq b < q$, B es un entero positivo, y q es un múltiplo entero de $2^{B+\delta+1}$, en donde q, B, δ, y c son parámetros del sistema.

De acuerdo con otro aspecto de la invención, un primer dispositivo debe desarrollar un método para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo, en donde el método comprende:

determinar un secreto s común con base en un valor a entero y una ecuación

$$s = \left\lfloor \frac{(a+c)\ mod\ q}{\frac{q}{2^{B}}} \right\rfloor,$$

en donde a satisface $0 \leq a < q$, B es un entero positivo, q es un múltiplo entero de $2^{B+\delta+1}$, en donde δ es un entero mayor que 1, en donde q, B, δ y c son parámetros del sistema;

determinar un dato h de reconciliación con base en una ecuación

$$h = \left\lfloor \frac{((a+c) mod\ q) mod \left(\frac{q}{2^{B}}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor;$$

y

transmitir información indicativa de los datos h de reconciliación al segundo dispositivo.

Los expertos en la técnica apreciarán que dos o más de las realizaciones, implementaciones y/o aspectos de la invención mencionados anteriormente se pueden combinar de cualquier manera que se considere útil. Las modificaciones y variaciones de los métodos, que corresponden a las modificaciones y variaciones descritas de los dispositivos, pueden llevarse a cabo por un experto en la técnica sobre la base de la presente descripción.

Breve descripción de los dibujos

Estos y otros aspectos de la presente invención se discutirán con más detalle a continuación, con referencia a los dibujos adjuntos.

La figura 1 muestra un diagrama de bloques de un segundo dispositivo para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo.

La figura 2 muestra un diagrama de bloques de un primer dispositivo para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo.

La figura 3 muestra un diagrama de flujo de un método desarrollado por un segundo dispositivo para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo.

La figura 4 muestra un diagrama de flujo de un método desarrollado por un primer dispositivo para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo.

La figura 5 muestra un diagrama de tiempo de un sistema que comprende un primer dispositivo y un segundo dispositivo para alcanzar un acuerdo sobre un valor secreto.

La figura 6 muestra una descripción de longitud de bits de un identificador utilizado en el sistema.

Descripción detallada de las realizaciones

La siguiente descripción con referencia a los dibujos adjuntos se proporciona para ayudar a una comprensión integral de las realizaciones de ejemplo de la invención tal como se define por las reivindicaciones y sus equivalentes. Incluye diversos detalles específicos para ayudar en esa comprensión, pero estos deben considerarse como simplemente de ejemplo. En consecuencia, los expertos en la técnica reconocerán que se pueden realizar diversos cambios y modificaciones de las realizaciones descritas en este documento sin apartarse del alcance de la invención. Además, las descripciones de funciones y construcciones bien conocidas pueden omitirse para mayor claridad y concisión.

La siguiente notación se utilizará en esta divulgación: Para cualquiera de los dos enteros χ y v, con v ≥ 2, entonces $\langle x \rangle_v$ denota que el entero satisface

$$0 \le \langle x \rangle_v \le v-1 \ y \ \langle x \rangle_v \equiv x \bmod v.$$

Además, para cualquier número real y, la notación $\lfloor y \rfloor$ denota el resultado de redondear y hacia abajo al entero más cercano, y la notación $\lceil y \rceil$ denota el resultado de redondear y hacia arriba al entero más cercano. Por ejemplo:

$$\lfloor \frac{9}{2} \rfloor = 4 , \lceil \frac{9}{2} \rceil = 5 ,$$

y $\lfloor 4 \rfloor = \lceil 4 \rceil = 4$.

En ciertas realizaciones, dos partes, A y B, están utilizando un protocolo particular en el que la parte A calcula un número a y la parte B calcula un número b. El protocolo debe ser tal que, debido a la forma en que se han calculado a y b, estén aproximadamente de acuerdo. Este acuerdo aproximado se expresa en términos de las constantes del sistema q, B y δ, que son conocidos por A y B, donde q, δ y B son enteros positivos, y q es un múltiplo entero de $2^{B+\delta+1}$, de la siguiente manera: a y b son números enteros en el intervalo [0, q) y satisfacen

$$a \equiv b + e \pmod q \qquad \text{(ecuación 1)}$$

en la que

$$|e| \le \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}. \qquad \text{(ecuación 2)}$$

Usando la presente divulgación, las dos partes pueden alcanzar un secreto de bits B común haciendo que una parte, digamos la parte A, transmita bits δ de datos de reconciliación a la parte B. Un parámetro c más del sistema de enteros; su relevancia se divulgará a continuación. Los enteros h y v se definen mediante la siguiente ecuación:

$$\langle a + c \rangle_q = s\frac{q}{2^B} + h\frac{q}{2^{B+\delta}} + v \ , \qquad \text{(ecuación 3)}$$

en la que $0 \le h\frac{q}{2^{B+\delta}} + v \le \frac{q}{2^B} - 1$ y $0 \le v \le \frac{q}{2^{B+\delta}} - 1$.

En particular,

$$s = \lfloor \frac{\langle a + c \rangle_q}{(q/2^B)} \rfloor. \qquad \text{(ecuación 4)}$$

En el caso especial de que $q = 2^m$, el valor s secreto corresponde a los Bits B más significativos de la expansión binaria de $\langle a + c \rangle_{2^m}$, h corresponde a los siguientes bits δ significativos de la expansión binaria de $\langle a + c \rangle_{2^m}$, y v corresponde a los bits menos significativos m - B - δ de $\langle a + c \rangle_{2^m}$.

Al considerar el módulo de la ecuación (1) $\frac{q}{2^B}$, se deduce que

$$b + c - h\frac{q}{2^{B+\delta}} \equiv v - e(\text{mod } \frac{q}{2^B}). \qquad \text{(ecuación 5)}$$

Como $0 \le v \le \frac{q}{2^{B+\delta}} - 1$ y como se satisface la ecuación (2), se deduce que

$$0 \le v - e - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}} \le \frac{q}{2^B} - 1. \qquad \text{(ecuación 6)}$$

Al combinar la ecuación (5) y la ecuación (6), se deduce que

$$v - e - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}} = \langle b + c - h\frac{q}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}} \rangle_{q/2^B}. \qquad \text{(ecuación 7)}$$

Al combinar la ecuación (1) y la ecuación (3), se deduce que

$$s\frac{q}{2^B} \equiv b + c - h\frac{q}{2^{B+\delta}} - (v - e)(\text{mod } q), \text{ (ecuación 8)}$$

y a partir de la ecuación (8) se deduce que

$$s \equiv \frac{b + c - h\frac{q}{2^{B+\delta}} - (v - e)}{q/2^B} (\text{mod} 2^B). \qquad \text{(ecuación 9)}$$

Al combinar la ecuación (9) y la ecuación (7), y usar la propiedad $s \in [0,2^B)$, se deduce que la parte B puede calcular s usando la ecuación

$$s = \langle \lfloor \frac{b + c - h\frac{q}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}}}{q/2^B} \rfloor \rangle_{2^B}. \qquad \text{(ecuación 10)}$$

Al simplificar la ecuación (10), se deduce que la parte B puede calcular alternativamente s utilizando la ecuación

$$s = \langle \lfloor \frac{b + c}{q/2^B} - \frac{h}{2^\delta} - \frac{1}{2^{\delta+1}} + \frac{1}{2} \rfloor \rangle_{2^B}. \qquad \text{(ecuación 11)}$$

Las ecuaciones (10) y (11) muestran que S puede calcularse a partir de b, h y los parámetros del sistema q, B y δ. Entonces, si la parte A envía información indicativa de h a la parte B, entonces la parte B puede recuperar s, que puede usarse como un secreto común entre la parte A y la parte B.

Como la ecuación (3) implica $0 \le h\frac{q}{2^{B+\delta}} < \frac{q}{2^B}$, se deduce que $0 \le h < 2^\delta$, entonces h puede ser representado por bits δ.

Se observa que si c = 0, la ecuación (4) establece que el secreto s es igual al cociente de a y $(q/2^B)$, redondeado hacia abajo al entero más cercano. Con la opción $c = q/2^{B+1}$, el secreto s es igual al cociente de a y $q/2^B$, redondeado al

entero más cercano (módulo 2^B) (y redondeado hacia arriba en caso de empate, es decir, si a es igual a $k\frac{q}{2^B}+\frac{q}{2^{B+1}}$ para algún entero k). Con la opción c = q/(2^{B+1})-1, el secreto s es igual al cociente de a y q/2^B, redondeado al módulo entero más cercano 2B, con redondeo hacia abajo en caso de empate. Se pueden usar otros valores de c para obtener otro resultado, según se desee. Para estas opciones especiales para c, se puede simplificar el cálculo de s por la parte B. De hecho, la parte B puede obtener s usando la ecuación

$$s=\langle 1+\lfloor \frac{b}{q/2^B}-\frac{h}{2^\delta}-\frac{1}{2^{\delta+1}}\rfloor\rangle_{2^B} \text{ si } c=\frac{q}{2^{B+1}}, \quad \text{(ecuación 12)}$$

y como

$$s=\langle 1+\lfloor \frac{b-1}{q/2^B}-\frac{h}{2^\delta}-\frac{1}{2^{\delta+1}}\rfloor\rangle_{2^B}=\langle \lceil \frac{b}{q/2^B}-\frac{h}{2^\delta}-\frac{1}{2^{\delta+1}}\rceil\rangle_{2^B} \text{ si } c=\frac{q}{2^{B+1}}-1.$$

(ecuación 13)

En caso de que q = 2^m, el secreto s común puede consistir en los Bits B más significativos de a; los datos h auxiliares consisten en los siguientes bits δ de a. Además, si a se distribuye uniformemente, entonces el secreto s común dado los datos h auxiliares también se distribuye uniformemente. Es decir, un adversario no puede obtener información sobre el secreto s común a partir de la observación de los datos h auxiliares.

Se observa que la condición de "acuerdo aproximado" puede generalizarse. Por ejemplo, es posible reemplazar la ecuación (1) por la condición:

$$a \equiv b + Ne \pmod{q} \quad \text{(ecuación 14)}$$

para algún entero N que es relativamente primo para q, es decir, el máximo común divisor de N y q es uno. La condición sobre el valor absoluto de e como se especifica en la ecuación (2) puede mantenerse igual:

$$|e| \leq \frac{q}{2^{B+1}}-\frac{q}{2^{B+\delta+1}}. \quad \text{(ecuación 2)}$$

Por ejemplo, si q = 2^m para algún entero m, entonces N puede ser cualquier número impar. En tal caso, el cálculo de los datos secretos y auxiliares se puede desarrollar utilizando la siguiente derivación. Sea W un entero tal que wN ≡ 1 (mod q). Tal entero existe, porque q y N son relativamente primos. Deje α: = ⟨wa⟩$_q$ y β: = ⟨wb⟩$_q$. Entonces α ≡ β + e (mod q). Por lo tanto, las partes pueden acordar sobre un secreto $s=\lfloor\frac{\alpha+c}{(q/2^B)}\rfloor$ como se explicó anteriormente, usando α y β en lugar de a y b, respectivamente.

Para δ = 1 y q = 2^m, y obteniendo el secreto s como el entero más cercano al cociente de a y 2^{m-B}, se envía un bit h de reconciliación, y las partes pueden acordar un secreto s de bits B siempre que, por ejemplo, |e|≤2^{m-B-2}. Si q = 2^m y δ = m - B - 1, las partes pueden acordar un secreto s de bits B siempre |e|≤2^{m-B-1}-1. Al aumentar el número de bits de reconciliación, las partes pueden acordar sobre un valor secreto que es un bit más largo.

Usando las técnicas descritas en este documento, es posible alcanzar un acuerdo sobre el secreto sin intercambio de información sobre los m - B - δ ≥ 1 bits menos significativos de a. Al variar δ, es posible lograr una compensación entre los requisitos de ancho de banda para enviar datos de conciliación y los requisitos de aproximación para un acuerdo exacto exitoso.

La figura 1 muestra un diagrama de bloques de un ejemplo de un segundo dispositivo 150 para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo 250. El segundo dispositivo 150 comprende una antena 100, un receptor 101, un procesador 102 y una memoria 105. La antena 100 está conectada al receptor 101 para recibir una señal. En funcionamiento, la memoria 105 comprende un bloque 103 de datos y un bloque 104 informático La antena 100 puede usarse para enviar y/o recibir señales de forma inalámbrica usando un estándar de comunicaciones apropiado. En una implementación alternativa, la antena 100 puede ser reemplazada por una conexión por cable (red).

Aunque en la presente divulgación, solo se necesita un receptor 102, las implementaciones prácticas también pueden comprender un transmisor para transmitir señales, por ejemplo usando la antena 100. El procesador 102 controla el funcionamiento del dispositivo, incluido el receptor 101 y la memoria. El bloque 103 de datos de la memoria 105 se puede usar para almacenar diversos datos, incluidos, entre otros, parámetros del sistema (por ejemplo, q, B, δ y c), un secreto s, datos h, de reconciliación recibidos un valor b y otros datos tales como contenidos para ser encriptados o desencriptados. El bloque 104 informático puede comprender un código informático ejecutable que implementa al menos un método para alcanzar un acuerdo sobre un valor secreto con otro dispositivo (por ejemplo, el primer dispositivo 250).

El receptor 101 está configurado para recibir información indicativa de datos h de reconciliación del primer dispositivo, en donde $0 \leq h < 2^{\delta}$, en donde δ es un entero mayor que 1. El procesador 102 está configurado para calcular un secreto s común con base en el valor b entero y una ecuación

$$s \equiv \left\lfloor \frac{b+c-h\frac{q}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}+\frac{q}{2^{B+1}}}{\frac{q}{2^{B}}} \right\rfloor \ mod\ 2^{B}\ .$$

Por ejemplo, se puede elegir s como el valor para el que se cumple la ecuación anterior y en donde $0 \leq s < 2^{B}$.

El valor b satisface $0 \leq b < q$, el parámetro B del sistema es un entero positivo y el parámetro q del sistema es un múltiplo entero de $2^{B+\delta+1}$. Estos parámetros del sistema pueden preprogramarse en el dispositivo o recibirse de una parte confiable, por ejemplo. Estos parámetros del sistema no se mantienen necesariamente en secreto.

El procesador 102 puede configurarse para calcular b antes de calcular el secreto s común. Tal cálculo puede basarse en un protocolo de intercambio de claves. Con ese fin, el segundo dispositivo 150 puede intercambiar más información con el primer dispositivo 250 u otro dispositivo, tal como un tercero intermediario (no mostrado), a través de su receptor 102 o transmisor opcional, de acuerdo con el protocolo de intercambio de claves. Los detalles de este protocolo de intercambio de claves están más allá del alcance de la presente divulgación. Es una propiedad del segundo dispositivo que puede determinar el secreto s común utilizando los datos h de reconciliación, si el primer dispositivo 250 ha calculado los datos h de reconciliación como se divulga a continuación con referencia a la figura 2, siempre que el primer dispositivo 250 usa un número a de acuerdo aproximado con el número b, en el sentido de que $a \equiv b + e \pmod q$, en donde e representa una diferencia entre los números a y b, en la que $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$.

Para valores específicos de c, el cálculo del secreto s común se puede simplificar (véase también las ecuaciones 12 y 13). El procesador 102 del segundo dispositivo se puede configurar para calcular s evaluando una fórmula

$$s = \langle 1 + \left\lfloor \frac{b - \frac{h}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}}}{\frac{q}{2^{B}}} \right\rfloor \rangle_{2^{B}} \ \text{si}\ c = \frac{q}{2^{B+1}}$$

Además, el procesador 102 del segundo dispositivo se puede configurar para calcular s evaluando una fórmula

$$s = \langle 1 + \left\lfloor \frac{b - \frac{h}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}} - 1}{\frac{q}{2^{B}}} \right\rfloor \rangle_{2^{B}} \ \text{si}\ c = \frac{q}{2^{B+1}} - 1$$

que se puede implementar alternativamente como

$$s = \langle \left\lfloor \frac{b-\frac{h}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}}{\frac{q}{2^{B}}} \right\rfloor \rangle_{2^{B}} \ \text{si}\ c = \frac{q}{2^{B+1}} - 1.$$

En un ejemplo particular, $q = 2^m$ y $\delta = m - B - 1$, en donde m es un entero positivo. En este documento,> B + 3.

En otro ejemplo, el procesador 102 está configurado para calcular el valor b con base en un valor β y una ecuación $b \equiv w\beta \pmod q$, en donde $wN \equiv 1 \pmod q$, en donde N es un entero mayor que 1 y es relativamente primo para q. Esto permite soportar una diferencia mayor entre a y b, tal como se explicó anteriormente con respecto a la ecuación 14.

La figura 2 muestra un diagrama de bloques que ilustra un ejemplo de un primer dispositivo 250 para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo 150. El primer dispositivo 250 comprende una antena 200, un transmisor 201, un procesador 202 y una memoria 205. La antena 200 está conectada al transmisor 201 para recibir una señal. En funcionamiento, la memoria 205 comprende un bloque 203 de datos y un bloque 204 informático. La antena 200 puede usarse para enviar y/o recibir señales de forma inalámbrica usando un estándar de comunicaciones apropiado. En una implementación alternativa, la antena 200 puede ser reemplazada por una conexión por cable (red). Aunque para la descripción de la presente divulgación, solo se necesita un transmisor 202, las implementaciones prácticas también pueden comprender un receptor para recibir señales, por ejemplo usando la antena 200. El procesador 202 controla el funcionamiento del dispositivo, incluido el transmisor 201 y la memoria 205. El bloque 203 de datos de la memoria 205 puede usarse para almacenar diversos datos, incluidos, entre otros, los parámetros del sistema (por ejemplo, q, B, δ y c), un secreto s, datos h de reconciliación, un valor b, y otros datos, tales como los contenidos que se deben encriptar o desencriptar. El bloque 204 informático puede comprender un código ejecutable por ordenador que implementa al menos un método para alcanzar un acuerdo sobre un valor secreto con otro dispositivo (por ejemplo, el segundo dispositivo 150).

En una implementación práctica, el procesador 202 puede configurarse para determinar un secreto s común con base en un valor a entero y una ecuación

$$s = \left\lfloor \frac{(a + c) \bmod q}{\frac{q}{2^B}} \right\rfloor$$

Esto puede escribirse alternativamente como:

$$s = \left\lfloor \frac{\langle a + c \rangle_q}{\frac{q}{2^B}} \right\rfloor$$

en donde el valor a satisface 0 ≤ a <q, el parámetro B del sistema es un entero positivo, el parámetro q del sistema es un múltiplo entero de $2^{B+\delta+1}$, y el parámetro δ del sistema es un entero mayor que 1.

Antes o después de determinar el secreto s común (o simultáneamente), el procesador 202 puede determinar un dato h de reconciliación con base en una ecuación

$$h = \left\lfloor \frac{\left((a + c) \bmod q\right) \bmod \left(\frac{q}{2^B}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor$$

Esto puede escribirse alternativamente como:

$$h = \left\lfloor \frac{\langle \langle a + c \rangle_q \rangle_{\frac{q}{2^B}}}{\frac{q}{2^{B+\delta}}} \right\rfloor$$

El transmisor 201 puede estar configurado para transmitir, bajo el control del procesador 202, información indicativa de los datos h de reconciliación al segundo dispositivo. Por ejemplo, la información indicativa de los datos h de reconciliación puede ser una representación binaria de los datos h de reconciliación o una representación codificada de los datos h de reconciliación.

En un ejemplo particular, el procesador 202 está configurado para calcular a con base en un protocolo de intercambio de claves. Con ese fin, el primer dispositivo 250 puede intercambiar más información con el segundo dispositivo 150, u otro dispositivo, tal como una tercera parte intermediaria (no mostrado), de acuerdo con el protocolo de intercambio de claves, usando el transmisor 201 o un receptor opcional. Los detalles de este protocolo de intercambio de claves están más allá del alcance de la presente divulgación. Es una propiedad del primer dispositivo 250 que puede proporcionar al segundo dispositivo 150 los datos h de reconciliación adicionales. El segundo dispositivo 150 puede determinar el secreto s común utilizando los datos h de reconciliación, combinando los datos h de reconciliación con el número b de la manera descrita en este documento con referencia a la figura 1, siempre que el primer dispositivo 250 use un número a en acuerdo aproximado con el número b que usa el segundo dispositivo 150, en el sentido de que $a \equiv b + e \pmod{q}$, en donde e representa una diferencia entre los números a y b, en la que $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$.

En un ejemplo de implementación particular, $q = 2^m$, en donde m es un entero positivo, el secreto s común corresponde a Bits B más significativos de una expansión binaria de $(a + c) \bmod 2^m$, y los datos h de reconciliación corresponden a siguientes bits δ más significativos de la expansión binaria de $(a + c) \bmod 2^m$. Por ejemplo, $\delta = m - B - 1$ puede proporcionar un número relativamente grande de bits que se pueden conciliar al tiempo que permite una restricción relativamente relajada con respecto a qué tan aproximado debe ser el acuerdo entre a y b, y transmitir relativamente pocos bits δ de datos de conciliación. Sin embargo, este valor solo se presenta como un ejemplo.

El secreto s pueden derivarse del valor a de varias maneras diferentes. Por ejemplo, se puede realizar un comportamiento diferente variando el parámetro c del sistema. El mismo valor de los parámetros del sistema (incluido c) debe usarse tanto en el primer dispositivo como en el segundo dispositivo para un desarrollo óptimo. Por ejemplo, se puede elegir c = 0 para que el secreto s común sea igual a un cociente de a y $(\frac{q}{2^B})$, redondeado hacia abajo al entero más cercano. Alternativamente, $c = \frac{q}{2^{B+1}}$ puede elegirse, de modo que el secreto s común sea igual a un cociente de a y $(\frac{q}{2^B})$, redondeado al entero más cercano, en donde el redondeo se desarrolla hacia arriba en caso de empate. Sin embargo, alternativamente, $c = \frac{q}{2^{B+1}} - 1$ se elige, de modo que el secreto s común sea igual a un cociente de a y $(\frac{q}{2^B})$, redondeado al entero más cercano, en donde el redondeo se desarrolla hacia abajo en caso de empate.

En un ejemplo de implementación particular, el procesador está configurado para calcular el valor a con base en un valor α y una ecuación $a \equiv w\alpha \pmod{q}$, en donde $wN = 1 \pmod{q}$, en donde N es un entero mayor que 1, en donde N es relativamente primo para q. Esto permite soportar una diferencia mayor entre a y b, tal como se explicó anteriormente con respecto a la ecuación 14.

Los procesadores 102 y 202 pueden ser cualquier tipo de procesador de ordenador, capaz de ejecutar un programa almacenado en la memoria y controlar periféricos tales como un transmisor, receptor, memoria y similares. Por ejemplo, el procesador 102 o 202 puede ser un microcontrolador o un microprocesador. Tal procesador es un dispositivo electrónico que es bien conocido en la técnica. Además, el procesador 102, 202 puede comprender una pluralidad de subprocesadores que pueden cooperar para desarrollar ciertas tareas en paralelo. La memoria 105 o 205 puede ser cualquier tipo de memoria que sea capaz de almacenar datos digitales, ya sea de manera volátil o no volátil. La memoria 105 o 205 es legible por ordenador, y puede ser utilizada por el procesador 102, 202 respectivo para recuperar y/o almacenar datos. Tal memoria 105, 205 es un dispositivo electrónico. Ejemplos bien conocidos incluyen una memoria Flash, una memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM) y una unidad magnética u óptica. Se puede usar una combinación de estos tipos de memoria en cada dispositivo.

En un ejemplo particular, un dispositivo contiene todos los componentes y la funcionalidad tanto del primer dispositivo como del segundo dispositivo. Por ejemplo, el dispositivo puede conmutar roles entre el rol del primer dispositivo y el segundo dispositivo.

La transmisión de datos desde el primer dispositivo al segundo dispositivo puede realizarse mediante comunicación directa. Alternativamente, la transmisión puede realizarse a través de una red, y los datos de reconciliación pueden pasar varios nodos en la red antes de alcanzar al segundo dispositivo. Por ejemplo, la transmisión de datos puede usar tecnología de red de datos Wi-Fi, Bluetooth, 3G, 4G, LTE.

La figura 3 ilustra un método a desarrollar por un segundo dispositivo para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo. La figura 4 ilustra un método que debe desarrollar el primer dispositivo para alcanzar un acuerdo sobre un valor secreto con el segundo dispositivo. La figura 5 ilustra cómo el primer dispositivo 501 y el segundo dispositivo 502 pueden cooperar para alcanzar un acuerdo. Los pasos ilustrados en la figura 5 que corresponden a los pasos ilustrados en la figura 3 y la figura 4 se han indicado utilizando los mismos numerales de referencia.

Con referencia a la figura 3 y la figura 5, el segundo dispositivo inicia el método en el paso 301. El inicio puede ser activado, por ejemplo, por una señal interna o externa apropiada, o una entrada proporcionada por un usuario. Por ejemplo, el método comienza cuando un primer dispositivo intenta establecer una comunicación con el segundo dispositivo. En el paso 302, se determinan los parámetros q, B, δ y c del sistema. Por ejemplo, estos parámetros del sistema se recuperan de la memoria 103. Opcionalmente, como se indica mediante la flecha 503, este paso puede implicar negociar entre el primer y el segundo dispositivo acerca de los parámetros del sistema que se utilizarán; por ejemplo, se pueden intercambiar mensajes sobre un conjunto de parámetros admitidos por ambos dispositivos. B es un entero positivo, δ es un entero mayor que 1, y q es un múltiplo entero de $2^{B+\delta+1}$. En el paso 303, se determina el número b. Por ejemplo, este número se calcula a partir de los datos que están disponibles para el segundo dispositivo. Alternativamente, el número b se recibe de una fuente externa, por ejemplo, una parte confiable, preferiblemente en forma cifrada. El número b podría obtenerse como parte de un protocolo de intercambio de claves con base en la red. Como se indica por la flecha 504, el valor b está en acuerdo aproximado con un valor correspondiente a del primer dispositivo 501. En el paso 304, el segundo dispositivo recibe la información indicativa de los datos h de reconciliación, como se indica por la flecha 505. La información puede ser transmitida al segundo dispositivo en forma cifrada, y ser descifrada por el segundo dispositivo, por ejemplo. Los datos de reconciliación están en el rango de $0 \leq h < 2^{\delta}$. En el paso 305, el segundo dispositivo calcula s con base en una ecuación

$$s \equiv \left\lfloor \frac{b + c - h\frac{q}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}}}{\frac{q}{2^{B}}} \right\rfloor \ mod\ 2^{B}$$

Por ejemplo,

$$s = \left\langle \left\lfloor \frac{b + c - h\frac{q}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}}}{\frac{q}{2^{B}}} \right\rfloor \right\rangle_{2^{B}}$$

Otras representaciones de s también son posibles.

En el paso 306, opcionalmente se determina una clave con base en el secreto s común. Luego, el método finaliza en el paso 307. Opcionalmente, el segundo dispositivo ahora puede comenzar a usar el secreto s común y/o la clave con base en el secreto s común. Los posibles usos pueden ser por uno o más de muchos, incluido el procesamiento criptográfico de datos, tales como el contenido, por ejemplo, cifrado, descifrado, creación de firma digital y verificación. Por ejemplo, el secreto s común puede usarse para el intercambio seguro de mensajes entre el primer dispositivo y el segundo dispositivo, como se indica por la flecha 506. Además, el secreto s común y/o la clave derivada de los mismos pueden almacenarse en la memoria del segundo dispositivo para su uso posterior.

Con referencia a la figura 4 y la figura 5, el primer dispositivo inicia el método en el paso 401. El inicio puede ser activado, por ejemplo, por una señal interna o externa apropiada, o una entrada proporcionada por un usuario. Por ejemplo, el método comienza cuando un segundo dispositivo intenta establecer comunicación con el primer dispositivo. En el paso 402, se determinan los parámetros q, B, δ y c del sistema. Por ejemplo, estos parámetros del sistema se recuperan de la memoria. Opcionalmente, como se indica con la flecha 503, este paso puede implicar negociar entre el primer y el segundo dispositivo sobre los parámetros del sistema que se utilizarán; por ejemplo, los mensajes se pueden intercambiar para determinar un conjunto de parámetros admitidos por ambos dispositivos. B es un entero positivo, δ es un entero mayor que 1, y q es un múltiplo entero de $2^{B+\delta+1}$. En el paso 403, el primer dispositivo determina un número a. Esta determinación puede basarse, por ejemplo, en un protocolo de intercambio de claves. Por ejemplo, este número a se calcula a partir de los datos que están disponibles para el primer dispositivo. Alternativamente, el número a se recibe de una fuente externa, por ejemplo, una parte confiable, preferiblemente en forma cifrada. El número a podría obtenerse como parte de un protocolo de intercambio de claves con base en la red. Como se indica mediante la flecha 504, el valor a está en acuerdo aproximado con un valor b correspondiente del segundo dispositivo 502. En el paso 404, el primer dispositivo determina los datos h de reconciliación. Estos datos de conciliación pueden basarse en la ecuación

$$h = \left\lfloor \frac{((a + c) mod\ q) mod \left(\frac{q}{2^B}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor$$

Los datos de reconciliación pueden estar en el rango de $0 \leq h < 2^{\delta}$. En el paso 405, el primer dispositivo transmite información indicativa de los datos h de reconciliación, como se indica mediante la flecha 505, al segundo dispositivo. La información puede cifrada por el primer dispositivo para transmitir la información al segundo dispositivo en forma cifrada, por ejemplo. En el paso 406, el primer dispositivo determina el secreto s común. Este paso puede desarrollarse antes que los otros pasos. En una implementación alternativa, el secreto s común se pueden determinar antes de determinar el número a, en donde el primer dispositivo puede derivar el número a del secreto s común. El secreto s común se pueden calcular con base en una ecuación

$$s = \left\lfloor \frac{(a + c)\ mod\ q}{\frac{q}{2^B}} \right\rfloor$$

En otra notación,

$$s = \left\lfloor \frac{\langle a + c \rangle_q}{\frac{q}{2^B}} \right\rfloor$$

Otras representaciones de s también son posibles. En el paso 407, opcionalmente se determina una clave con base en el secreto s común. Alternativamente el secreto s común puede estar basado en una clave determinada de antemano. Luego, el método finaliza en el paso 408. Opcionalmente, el primer dispositivo puede usar el secreto s común y/o la clave. Los posibles usos pueden ser por uno o más de muchos, incluido el procesamiento criptográfico de datos, tal como el contenido, por ejemplo, cifrado, descifrado, creación de firma digital y verificación. Por ejemplo, el secreto s común o la clave se pueden usar para el intercambio seguro de mensajes entre el primer dispositivo y el segundo dispositivo, como se indica con la flecha 506. Además, el secreto s común y/o la clave se pueden almacenar en la memoria del segundo dispositivo para su uso posterior.

La figura 6 muestra un ejemplo que ilustra conceptualmente una posible relación entre a, s, h, m, B y q para el caso específico de $q = 2^m$ y c = 0. En el dibujo, la representación binaria de a es ilustrada, desde el bit más significativo (en el lado izquierdo) hasta el bit más significativo (en el lado derecho). En el numeral 601, se ilustra que el secreto s común está representado por los Bits B más significativos de a. En el numeral 602, se ilustra que los datos h de reconciliación están representados por bits (B + 1)ésimo a (B + δ) ésimo más significativos de a. En el numeral 603, se ilustra que los bits restantes (B + δ + 1)ésimo a q-ésimo, es decir, los bits m - B - δ menos significativos de a, no están representados ni en el secreto s común ni en los datos h de reconciliación. Esta característica puede permitir un ahorro de datos con respecto al número de bits de los datos h de reconciliación y/o una mayor tolerancia con respecto al acuerdo aproximado entre a y b.

En esta divulgación, se presenta un método de reconciliación que puede enviar más de un bit de reconciliación. Las técnicas divulgadas en este documento pueden usarse, por ejemplo, para hacer que las partes acuerden un número particular de bits, mientras imponen condiciones menos estrictas sobre "cuán aproximado" debería ser el acuerdo aproximado. Permitir condiciones menos estrictas en el acuerdo aproximado puede mejorar la seguridad del sistema. Alternativamente, con aproximadamente las mismas condiciones de aproximación (es decir, con garantías de seguridad similares), una instancia del método permite que las dos partes acuerden sobre un valor secreto que es un bit más largo. A continuación, se divulgan algunas de las ventajas del método y su impacto mediante ejemplos numéricos.

Bos divulga un método de intercambio de claves de seguridad cuántico. Una parte envía a otra parte una pequeña semilla y una matriz $n \times \overline{n}$ con elementos de Z_q. En respuesta, se envían una matriz $\overline{m} \times n$ y una matriz binaria $n \times \overline{m}$ con bits de reconciliación. Ambas partes construyen una matriz $n \times \overline{m}$; de cada entrada de dicha matriz, se extraen Bits B comunes. El número total de bits extraídos (etiquetados como "longitud" en las tablas a continuación) es igual a $\overline{n} \cdot \overline{m} \cdot B$, mientras que el número total de bits transmitidos es igual a

$$n(\overline{n} + \overline{m}) \lceil \log_2(q) \rceil + \overline{m} \cdot \overline{n}.$$

La tabla 1 es una versión condensada de las instancias propuestas en la tabla 2 de Bos.

Esquema	n	q	B	*n*	*m*	Longitud	Ancho de banda
Desafío	352	2^{11}	1	8	8	64	7,57 KB
Clásico	592	2^{12}	2	8	8	128	14,22 KB
Recomendado	752	2^{15}	4	8	8	256	22,57 KB
Paranoico	864	2^{15}	4	8	8	256	25,93 KB
Tabla 1: Opciones de parámetros del papel Bos							

De acuerdo con Bos, en caso de que se envíe un bit de reconciliación, se garantiza que las partes acuerden un secreto B-bits común si sus números difieren menos de 2^{m-B-2} (donde m es tal que $q = 2^m$). Los resultados con las técnicas divulgadas en este documento muestran que, bajo la misma condición, las dos partes pueden acordar un secreto de B + 1 bits si se envían δ = m - B - 2 bits de reconciliación. La cantidad de datos de reconciliación es igual a $\log_2(q) - B - 2$ bits por entrada de matriz, y el ancho de banda total utilizado es igual a $\log_2(q)n(\overline{n}+\overline{m})+\overline{m}\cdot\overline{n}\cdot(\log_2(q)-B-2)$. Como en las técnicas divulgadas en este documento, el número de bits que se acuerda es mayor que en la divulgación de Bos, es posible reducir $\overline{n}$ y/o $\overline{m}$ y, por lo tanto, reducir el uso de ancho de banda general. Usando las técnicas divulgadas en este documento, se obtuvieron los resultados en la tabla 2. La columna más a la derecha (etiquetada "Relación") muestra la proporción del ancho de banda utilizado del esquema de reconciliación propuesto y la del sistema divulgado en Bos.

Tabla 2: Mejora que puede lograrse mediante el esquema de reconciliación divulgado en este documento

Esquema	n	q	B	$\overline{n}$	$\overline{m}$	Longitud	Ancho de banda	Relación
Desafío	352	2^{11}	2	6	6	72	5,84 KB	0,76
Clásico	592	2^{12}	3	7	7	147	12,48 KB	0,88
Recomendado	752	2^{15}	5	7	8	280	21,22 KB	0,94
Paranoico	864	2^{15}	5	7	8	280	24,37 KB	0,94

Se apreciará que la invención también se aplica a programas informáticos, particularmente programas informáticos sobre o en un portador, adaptados para poner en práctica la invención. El programa puede tener la forma de un código fuente, un código objeto, un código fuente intermedio y un código objeto tal como en una forma parcialmente compilada, o en cualquier otra forma adecuada para usar en la implementación del método de acuerdo con la invención. También se apreciará que dicho programa puede tener muchos diseños arquitectónicos diferentes. Por ejemplo, un código de programa que implementa la funcionalidad del método o sistema de acuerdo con la invención puede subdividirse en una o más subrutinas. El experto en la técnica verá muchas formas diferentes de distribuir la funcionalidad entre estas subrutinas. Las subrutinas pueden almacenarse juntas en un archivo ejecutable para formar un programa autónomo. Dicho archivo ejecutable puede comprender instrucciones ejecutables por ordenador, por ejemplo, instrucciones de procesador y/o instrucciones de intérprete (por ejemplo, instrucciones de intérprete de Java). Alternativamente, una o más o todas las subrutinas pueden almacenarse en al menos un archivo de biblioteca externo y vincularse con un programa principal, ya sea estática o dinámicamente, por ejemplo, en tiempo de ejecución. El programa principal contiene al menos una llamada al menos a una de las subrutinas. Las subrutinas también pueden comprender llamadas entre sí. Una realización relacionada con un producto de programa informático comprende instrucciones ejecutables por ordenador que corresponden a cada paso de procesamiento de al menos uno de los métodos establecidos en este documento. Estas instrucciones pueden subdividirse en subrutinas y/o almacenarse en uno o más archivos que pueden vincularse estática o dinámicamente. Otra realización relacionada con un producto de programa de ordenador comprende instrucciones ejecutables por ordenador que corresponden a cada medio de al menos uno de los sistemas y/o productos establecidos en este documento. Estas instrucciones pueden subdividirse en subrutinas y/o almacenarse en uno o más archivos que pueden vincularse estática o dinámicamente.

El portador de un programa de ordenador puede ser cualquier entidad o dispositivo capaz de llevar el programa. Por ejemplo, el portador puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo, una CD ROM o una ROM de semiconductores, o un medio de grabación magnética, por ejemplo, una unidad flash o un disco duro. Además, el portador puede ser un portador transmisible tal como una señal eléctrica u óptica, que puede transmitirse a través de un cable eléctrico u óptico o por radio u otros medios. Cuando el programa se incorpora a dicha señal, el portador puede estar constituido por dicho cable u otro dispositivo o medio. Alternativamente, el portador puede ser

un circuito integrado en el que está incrustado el programa, el circuito integrado está adaptado para desarrollar, o para ser utilizado en el desarrollo del método relevante.

Debe 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 sin apartarse del alcance de las reivindicaciones adjuntas. En las reivindicaciones, los signos de referencia colocados entre paréntesis no se interpretarán como limitativos de la reivindicación. El uso del verbo "comprender" y sus conjugaciones no excluye la presencia de elementos o pasos distintos de los establecidos en una reivindicación. La expresión "un" o "uno, una" que precede a un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede implementarse por medio de hardware que comprende varios elementos distintos, y por medio de una ordenador adecuadamente programado. En la reivindicación del dispositivo que enumera varios medios, varios de estos medios pueden estar incorporados por uno y el mismo ítem de hardware. El mero hecho de que ciertas medidas se mencionen en reivindicaciones dependientes mutuamente diferentes no indica que una combinación de estas medidas no pueda usarse con ventaja.

REIVINDICACIONES

1. Un segundo dispositivo, para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo, que comprende:

un receptor (101) configurado para recibir información indicativa de datos h de reconciliación del primer dispositivo, en donde $0 \leq h < 2^{\delta}$, en donde δ es un entero mayor que 1; y

un procesador (102) configurado para calcular un secreto s común con base en un valor b entero y una ecuación

$$s \equiv \left\lfloor \frac{b+c-h\frac{q}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}+\frac{q}{2^{B+1}}}{\frac{q}{2^{B}}} \right\rfloor \ mod\ 2^{B}\ ,$$

en donde b satisface $0 \leq b < q$, B es un entero positivo, y q es un múltiplo entero de $2^{B+\delta+1}$, en donde q, B, δ, y c son parámetros del sistema.

2. El segundo dispositivo de la reivindicación 1, en donde el procesador (102) está configurado para calcular b con base en un protocolo de intercambio de claves.

3. El segundo dispositivo de la reivindicación 1, en donde el primer dispositivo tiene un número a de acuerdo aproximado con el número b, en el sentido de que a ≡ b + e (mod q), en donde e representa una diferencia entre los números a y b en donde

$$|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}\ .$$

4. El segundo dispositivo de la reivindicación 1, en donde $q = 2^{m}$ y δ = m - B - 1, en donde m es un entero positivo.

5. El segundo dispositivo de la reivindicación 1, en donde el procesador (102) está configurado para calcular el valor b con base en un valor β y una ecuación b ≡ wβ (mod q), en donde wN = 1 (mod q), en donde N es un entero mayor que 1 y es relativamente primo para q.

6. Un sistema que comprende el segundo dispositivo de la reivindicación 1 y un primer dispositivo, en donde el primer dispositivo comprende:

un procesador (202) configurado para:

determinar un secreto s común con base en un valor a entero y una ecuación

$$s = \left\lfloor \frac{(a+c)\ mod\ q}{\frac{q}{2^{B}}} \right\rfloor ,$$

en donde a satisface $0 \leq a < q$, B es un entero positivo, q es un múltiplo entero de $2^{B+\delta+1}$, en donde δ es un entero mayor que 1, en donde q, B, δ y c son parámetros del sistema, y

determinar un dato h de reconciliación con base en una ecuación

$$h = \left\lfloor \frac{((a+c) mod\ q) mod \left(\frac{q}{2^{B}}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor ;$$

y

un transmisor (201) configurado para transmitir información indicativa de los datos h de reconciliación al segundo dispositivo,

en donde el número a está en acuerdo aproximado con el número b, en el sentido de que a ≡ b + e (mod q), en donde e representa una diferencia entre los números a y b, en donde $|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}$.

7. Un primer dispositivo para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo, que comprende:

un procesador (202) configurado para:

determinar un secreto s común con base en un valor a entero y una ecuación

$$s = \left\lfloor \frac{(a+c) \bmod q}{\frac{q}{2^B}} \right\rfloor,$$

en donde a satisface 0 ≤ a <q, B es un entero positivo, q es un múltiplo entero de $2^{B+\delta+1}$, en donde δ es un entero mayor que 1, en donde q, B, δ y c son parámetros del sistema, y

determinar un dato h de reconciliación con base en una ecuación

$$h = \left\lfloor \frac{((a+c) \bmod q) \bmod \left(\frac{q}{2^B}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor;$$

y

un transmisor (201) configurado para transmitir información indicativa de los datos h de reconciliación al segundo dispositivo.

8. El primer dispositivo de la reivindicación 7, en donde el procesador (202) está configurado para calcular a con base en un protocolo de intercambio de claves.

9. El primer dispositivo de la reivindicación 7, en donde el segundo dispositivo tiene un número b de acuerdo aproximado con el número a en el sentido de que $a \equiv b + e \pmod q$, en donde e representa una diferencia entre los números a y b, en donde

$$|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}.$$

10. El primer dispositivo de la reivindicación 7, en donde $q = 2^m$, en donde m es un entero positivo, el secreto s común corresponde a bits B más significativos de una expansión binaria de (a + c) mod 2^m, y los datos h de reconciliación corresponden a los siguientes bits δ de la expansión binaria.

11. El primer dispositivo de la reivindicación 10, en donde δ = m - B - 1.

12. El primer dispositivo de la reivindicación 7, en donde al menos uno de:

c = 0 para que el secreto s común sea igual a un cociente de a y $\left(\frac{q}{2^B}\right)$, redondeado hacia abajo al entero más cercano;

$c = \frac{q}{2^{B+1}}$, para que el secreto s común sea igual a un cociente de a y $\left(\frac{q}{2^B}\right)$, redondeado al entero más cercano, en donde el redondeo se desarrolla hacia arriba en caso de empate; y

$c = \frac{q}{2^{B+1}} - 1$, para que el secreto s común sea igual a un cociente de a y $\left(\frac{q}{2^B}\right)$, redondeado al entero más cercano, en donde el redondeo se desarrolla hacia abajo en caso de empate.

13. El primer dispositivo de la reivindicación 7, en donde el procesador (202) está configurado para calcular el valor a con base en un valor α y una ecuación $a \equiv w\alpha \pmod q$, en donde $wN = 1 \pmod q$, en donde N es un entero mayor que 1, en donde N es relativamente primo para q.

14. Un método que debe desarrollar un segundo dispositivo para alcanzar un acuerdo sobre un valor secreto con un primer dispositivo, el método comprende:

recibir (304) información indicativa de datos h de reconciliación del primer dispositivo, en donde $0 \leq h < 2^{\delta}$, en donde δ es un entero mayor que 1; y

calcular (305) un secreto s común con base en un valor b entero y una ecuación

$$s \equiv \left\lfloor \frac{b+c-h\frac{q}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}+\frac{q}{2^{B+1}}}{\frac{q}{2^{B}}} \right\rfloor \ mod\ 2^{B}\ ,$$

en donde b satisface 0 ≤ b <q, B es un entero positivo, y q es un múltiplo entero de $2^{B+\delta+1}$, en donde q, B, δ, y c son parámetros del sistema.

15. Un método que debe desarrollar un primer dispositivo para alcanzar un acuerdo sobre un valor secreto con un segundo dispositivo, el método comprende:

determinar (406) un secreto s común con base en un valor a entero y una ecuación

$$s = \left\lfloor \frac{(a+c)\ mod\ q}{\frac{q}{2^{B}}} \right\rfloor ,$$

en donde a satisface 0 ≤ a <q, B es un entero positivo, q es un múltiplo entero de $2^{B+\delta+1}$, en donde δ es un entero mayor que 1, en donde q, B, δ y c son parámetros del sistema;

determinar (404) un dato h de reconciliación con base en una ecuación

$$h = \left\lfloor \frac{((a+c) mod\ q) mod \left(\frac{q}{2^{B}}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor ;$$

y

transmitir (405) información indicativa de los datos h de reconciliación al segundo dispositivo.

Fig. 1

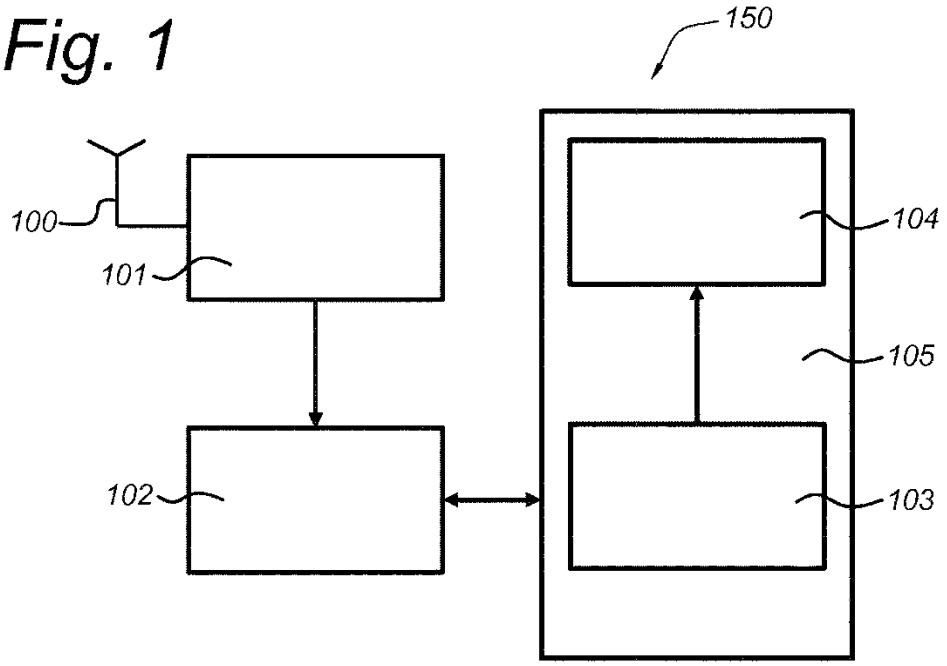


Fig. 2

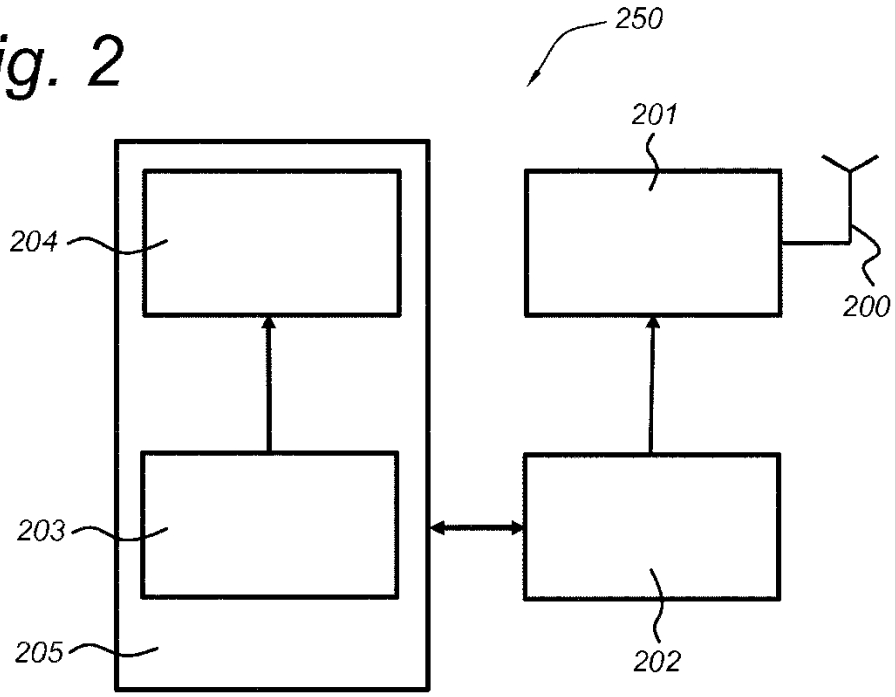


Fig. 3

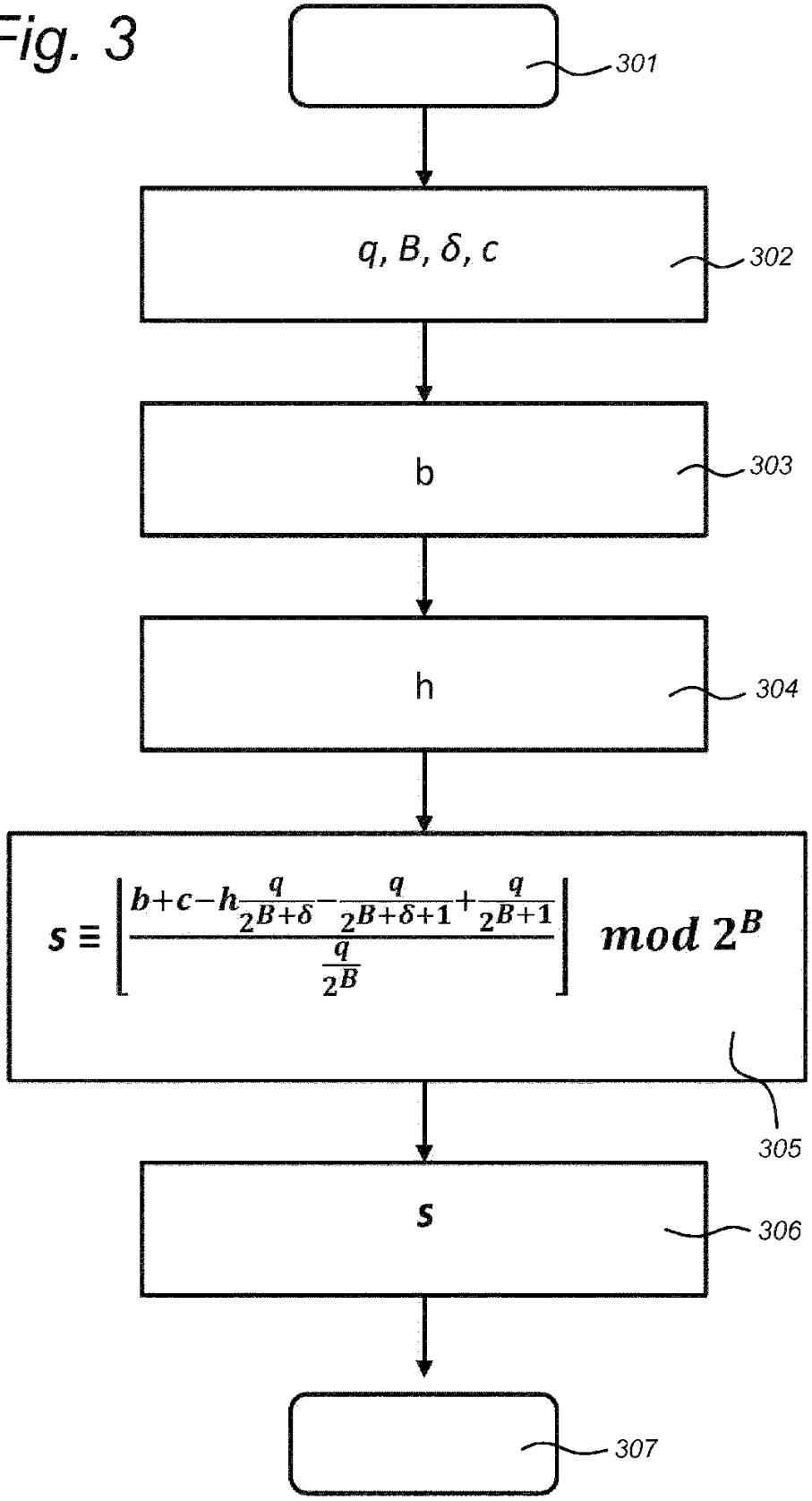

301
q, B, δ, c
302
b
303
h
304
$s \equiv \left\lfloor \frac{b+c-h\frac{q}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}+\frac{q}{2^{B+1}}}{\frac{q}{2^B}} \right\rfloor \mod 2^B$
305
s
306
307

Fig. 4

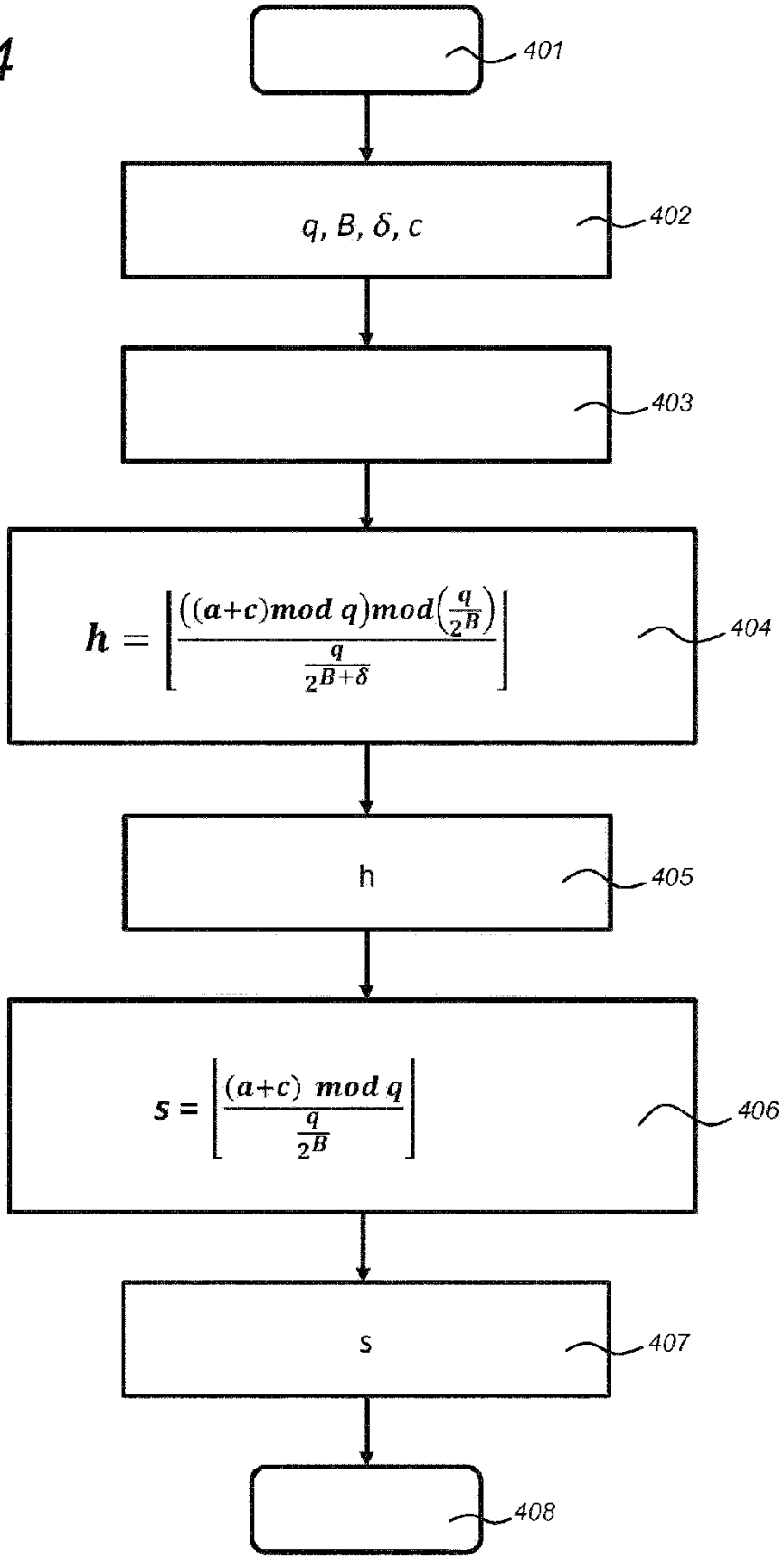

401
q, B, δ, c
402
403
$h = \left\lfloor \frac{((a+c) \bmod q) \bmod \left(\frac{q}{2^B}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor$
404
h
405
$s = \left\lfloor \frac{(a+c) \bmod q}{\frac{q}{2^B}} \right\rfloor$
406
s
407
408

Fig. 5

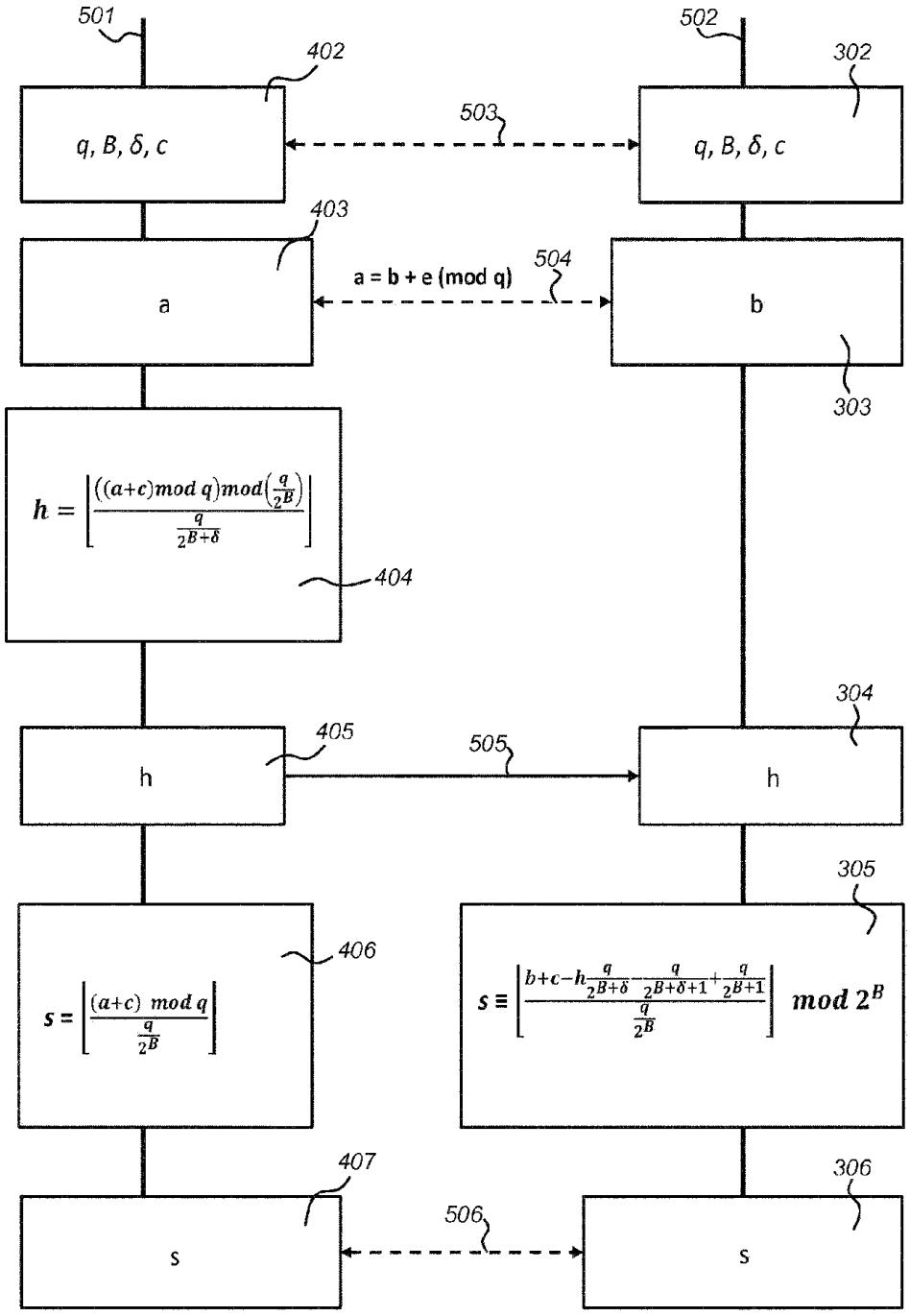
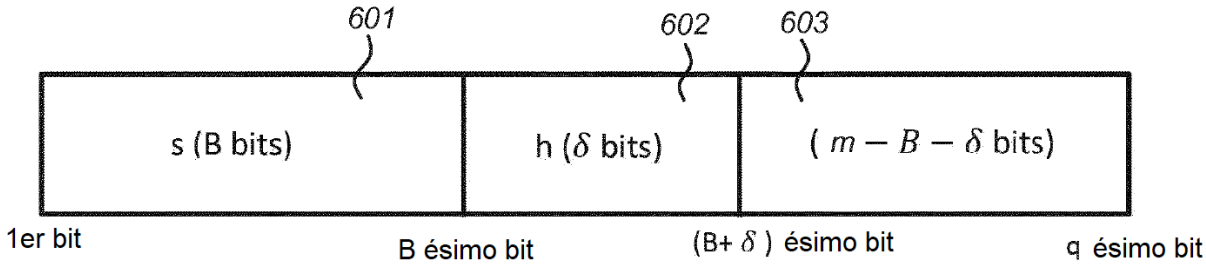

501
402
q, B, δ, c
503
502
302
q, B, δ, c
403
a
a = b + e (mod q)
504
b
303
$h = \left\lfloor \frac{((a+c) \bmod q) \bmod \left(\frac{q}{2^B}\right)}{\frac{q}{2^{B+\delta}}} \right\rfloor$
404
304
405
h
505
h
305
406
$s = \left\lfloor \frac{(a+c) \bmod q}{\frac{q}{2^B}} \right\rfloor$
$s \equiv \left\lfloor \frac{b+c-h\frac{q}{2^{B+\delta}}-\frac{q}{2^{B+\delta+1}}+\frac{q}{2^{B+1}}}{\frac{q}{2^B}} \right\rfloor \bmod 2^B$
407
306
506
s
s

Fig. 6


601
602
603
s (B bits)
h (δ bits)
($m - B - \delta$ bits)
1er bit
B ésimo bit
(B+ δ) ésimo bit
q ésimo bit