(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 308 725**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06708184 .4**
(96) Fecha de presentación : **10.02.2006**
(97) Número de publicación de la solicitud: **1847062**
(97) Fecha de publicación de la solicitud: **24.10.2007**

(54) Título: **Firmas de pregunta-respuesta y protocolos de seguridad de Diffie-Hellman.**

(30) Prioridad: **10.02.2005 US 651798 P**
07.02.2006 US 348304

(45) Fecha de publicación de la mención BOPI:
01.12.2008

(45) Fecha de la publicación del folleto de la patente:
01.12.2008

(73) Titular/es:
International Business Machines Corporation
New Orchard Road
Armonk, New York 10504, US

(72) Inventor/es: **Krawczyk, Hugo**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Firmas de pregunta-respuesta y protocolos de seguridad de Diffie-Hellman.

Campo de la invención

Aspectos de la presente invención están relacionados en general con firmas que son probadamente seguras para las partes emisora y receptora de un intercambio de información. Más específicamente, un esquema de firmas de preguntas-respuestas posee la propiedad de que tanto el verificador como el firmante pueden calcular la misma firma o firmas relacionadas, el primero porque sabe la pregunta y el segundo porque sabe la clave privada de la firma, permitiendo con ello, en ejemplos de modos de realización, variaciones probadamente seguras de protocolos convencionales de intercambio de claves, incluyendo una variación del muy conocido protocolo MQV.

Descripción de la técnica relacionada

El protocolo 100 de intercambio de claves de Diffie-Hellman (DH) ilustrado en la figura 1, como está propuesto originalmente, se cree que es seguro contra un atacante de escucha solamente. La búsqueda de un protocolo de "Diffie-Hellman autenticado" que resista los ataques activos de intermediarios, ha dado como resultado innumerables propuestas adecuadas, muchas de las cuales han sido destruidas o han demostrado que sufren inconvenientes. Con el desarrollo en los últimos años de rigurosos modelos de seguridad para el intercambio de claves, aquellas personas en el campo de la técnica están ahora en una posición mucho mejor para juzgar la seguridad de estos protocolos, así como para desarrollar diseños que soportan probadamente ataques activos realistas.

Como se esperaba, añadir salvaguardas contra ataques activos da como resultado una complejidad añadida, tanto en términos de comunicaciones adicionales como de cálculos. Esto último es particularmente significativo en protocolos autenticados con técnicas de claves públicas, que requieren normalmente una exponencial de coste acumulado adicional.

Además de la necesidad de una seguridad consistente, las muchas aplicaciones prácticas para el intercambio de claves han dirigido a los diseñadores a mejorar el coste del rendimiento asociado con mecanismos de autenticación, especialmente los basados en una clave pública.

Una línea de investigación, iniciada por Matsumoto, Takashima e Imai en 1986, es la búsqueda de un protocolo DH autenticado con una clave pública (PK), que añadiría una complejidad mínima al protocolo. Idealmente, y hasta el intercambio de claves públicas certificadas, se desea que la comunicación del protocolo parezca exactamente un intercambio básico de DH. En esta técnica, la autenticación del protocolo debe ser obtenida a través del procedimiento de obtención de claves: en lugar de estar de acuerdo con la clave básica g^{xy} de Diffie-Hellman, las partes acordarán una clave que combine g^x, g^y con las claves públicas/privadas de las partes.

Debido en parte a las ventajas prácticas que ofrecería tal protocolo, y en parte al reto matemático detrás de tal diseño, se han desarrollado muchos protocolos bajo este enfoque, denominados a menudo "protocolos de Diffie-Hellman implícitamente autenticados". Este enfoque, no solamente puede generar protocolos que son muy eficientes desde el punto de vista de las comunicaciones, sino que la combinación de la autenticación con el procedimiento de obtención de la clave puede dar potencialmente el resultado de ahorros significativos de cálculo. Por estas razones, se han estandarizado varios de estos protocolos "implícitamente autenticados" por medio de estándares de seguridad principales, tanto nacionales como internacionales.

De estos protocolos, el protocolo MQV parece haber sido ampliamente estandarizado. Este protocolo ha sido estandarizado por muchas organizaciones y ha sido anunciado recientemente por la Agencia Nacional de Seguridad de los Estados Unidos (NSA) como el mecanismo de intercambio de claves que subyace en "la criptografía de la próxima generación para proteger la información del gobierno de los Estados Unidos", que incluye la protección de "información de la seguridad nacional clasificada o crítica para una misión".

El protocolo MQV está descrito en el documento de BLAKE-WILSON S; MENEZES A: "PROTOCOLOS AUTENTICADOS DE ACUERDO DE CLAVES DE DIFFIE-HELLMAN" ÁREAS SELECCIONADAS EN CRIPTOGRAFÍA, 5º TALLER ANUAL INTERNACIONAL, SAC '98. PROCEEDIINGS. SPRINGER-VERLAG, 18 Agosto de 1998 (1998-08-18), páginas 339-361; XP002380813; Kingston, Ont., Canadá; ISBN: 3-540-65894-7.

Además, el MQV parece haber sido diseñado para satisfacer una serie de objetivos de seguridad. Una versión básica del protocolo MQV está explicada, por ejemplo, en la patente de Estados Unidos número 5.761.305, de Vanstone y otros colaboradores.

Pero, a pesar de su atractivo y de su éxito, el MQV ha eludido hasta ahora cualquier análisis formal en un modelo bien definido de intercambio de claves. La presente invención fue motivada por el deseo de proporcionar tal análisis. Al llevar a cabo un estudio, el inventor observó que virtualmente ninguno de los objetivos de los establecidos por MQV puede demostrarse que se cumple, como se lleva a cabo en el modelo de Canetti y Krawczyk de intercambio de claves calculadas, y como se describe en la Solicitud provisional identificada anteriormente.

Este resultado suscitó una preocupación al presente inventor sobre la seguridad de este protocolo convencional. Por tanto, basándose en este análisis de que el protocolo MQV convencional no era probadamente seguro, existe la necesidad de una seguridad adicional para MQV, al tiempo que se retiene preferiblemente su rendimiento y versatilidad existentes.

Sumario de la invención

En vista de lo anterior, y de otros ejemplos de problemas, inconvenientes y desventajas de los sistemas convencionales, es un ejemplo de característica de la presente invención proporcionar un método y una estructura para nuevas variaciones del MQV, denominadas en esta memoria como HMQV, que consiguen, de una manera que puede probarse, los objetivos de seguridad del protocolo MQV.

Es otro ejemplo de característica de la presente invención mostrar un nuevo esquema de firma digital, denominado en esta memoria como "firmas de preguntas-respuestas".

Es otro ejemplo de característica de la presente invención mostrar este esquema de firmas de preguntas-respuestas incluyendo una versión denominada en esta memoria como esquema de firmas de "preguntas-respuestas en forma exponencial" (XCR), obtenido a partir del esquema de identificación de Schnorr, en cuanto que proporciona un mecanismo de protocolos que tiene la propiedad de que tanto el que pregunta como el firmante pueden calcular la misma firma o firmas relacionadas, habiendo elegido el primero la pregunta y sabiendo el segundo la clave privada de la firma.

Por tanto, es un ejemplo de objeto de la presente invención proporcionar una estructura y un método para mejorar la seguridad de los protocolos autenticados de Diffie-Hellman, en los cuales se puede mostrar probadamente la seguridad, implementando en ellos los conceptos del esquema de firma XCR.

En un primer ejemplo de aspecto de la presente invención, para conseguir las características y objetos anteriores, se describe en esta memoria un método de intercambio entre dos partes interconectadas por medio de un dispositivo o una red, incluyendo una parte receptora, en adelante denominada verificador, que elige un valor secreto *x* para calcular un valor $X = F1(x)$, donde *F1* comprende una primera función predeterminada que tiene al menos un argumento, siendo el valor *x* uno de al menos un argumento de *F1*. Una parte firmante, en adelante denominada firmante, elige un valor secreto *y* para calcular un valor $Y = F2(y)$, donde *F2* comprende una segunda función predeterminada que tiene al menos un argumento, siendo el valor *y* uno de al menos un argumento de *F2*. El firmante obtiene el valor *X*, el firmante tiene también una clave privada *b* y una clave pública *B*. El firmante calcula un valor $s = F3(y,b,X)$, donde F3 comprende una tercera función predeterminada que tiene al menos tres argumentos, el valor *y*, la clave privada *b* y siendo el valor *X* tres argumentos de los al menos tres argumentos de *F3*. Existe una cuarta función predeterminada $F4(x,Y,B)$, para calcular un valor $s' = F4(x,Y,B)$, teniendo *F4* al menos tres argumentos, el valor *x*, el valor *Y*, y siendo la clave pública *B* tres argumentos de los al menos tres argumentos de *F4*, pero el valor *s* no es un argumento de *F4*. No existe ningún secreto compartido entre el verificador y el firmante que sirva como base para ningún argumento en ninguna de las funciones F1, F2, F3 y F4. El verificador puede considerar los valores *s* y *s'* como autenticadores válidos si se determina que el valor *s'* está relacionado de una manera predeterminada con el valor *s*.

En un segundo y tercer ejemplos de aspectos de la presente invención, descritos también en esta memoria, hay un aparato que realiza el método descrito en el párrafo precedente y un medio portador de señales que materializa tangiblemente un programa de instrucciones legibles por una máquina y ejecutables por un aparato procesador digital para realizar el método.

En un cuarto ejemplo de aspecto de la presente invención, se describe también en esta memoria un método para establecer una clave autenticada entre dos partes interconectadas por un dispositivo o red. Una primera parte tiene una clave privada a y una clave pública A, siendo la clave privada a un número entero tal que $0 \leq a \leq q-1$, siendo q un entero positivo, siendo g un generador de un grupo finito de orden q, y siendo A un elemento del grupo generado por el valor g y calculado como $A = g^a$. Una segunda parte tiene una clave privada b y una clave pública $B = g^b$, siendo la clave privada b un número entero tal que $0 \leq b \leq q-1$. La primera parte elige un valor secreto *x* para calcular un valor $X = g^x$, siendo x un entero tal que $0 \leq x \leq q-1$, y el valor X es comunicado a la segunda parte. La segunda parte elige un valor secreto *y* para calcular un valor $Y = g^y$, siendo *y* un entero tal que $0 \leq y \leq q-1$, y el valor *Y* es comunicado a la primera parte. La primera parte calcula un valor $s = f_1(Y,B,m)^{\{f2(x,a,m')\}}$, donde *m, m'* comprenden mensajes conocidos, o intercambiados entre las partes, y la segunda parte calcula un valor $s' = f_3(X,A,m')^{\{f4(y,b,m)\}}$. Al menos una de las funciones f_2 y f_4 incluye una función H con al menos un argumento, siendo uno de tales argumentos al menos uno de los mensajes m y m', donde H comprende una función criptográfica que es una entre una función unidireccional, una función de cifrado, y una función criptográfica de un algoritmo de cifrado (hashing o método de troceado). La primera y la segunda partes obtienen una clave compartida a partir de los valores s y s', respectivamente.

Breve descripción de los dibujos

Los anteriores y otros propósitos, aspectos y ventajas se comprenderán mejor a partir de la descripción detallada siguiente de un modo de realización preferido de la invención, con referencia a los dibujos, en los cuales:

La figura 1 muestra el protocolo básico 100 (no autenticado) de Diffie-Hellman;

La figura 2 muestra un protocolo autenticado 200 de Diffie-Hellman, utilizando firmas digitales;

La figura 3 muestra una comparación 300 del cálculo de la clave K de la sesión en el protocolo MQV convencional, con relación al cálculo de la clave de la sesión del protocolo HMQV de la presente invención, mostrando cómo HMQV utiliza el algoritmo de cifrado troceado ("hashing") en un ejemplo de modo de realización que es adicional al "hashing" utilizado en MQV;

La figura 4 muestra una representación gráfica diferente 400 del protocolo HMQV ilustrado en la figura 3;

La figura 5 muestra un ejemplo de cálculo 500 de XCR;

La figura 6 muestra un ejemplo de cálculo 600 de firmas XCR no interactivas;

La figura 7 muestra cálculos 700 de una firma XCR dual por las dos partes;

La figura 8 muestra el HMQV como ejemplo materializado en un protocolo 800 de confirmación de clave de tres mensajes (HMQV-C);

La figura 9 muestra el HMQV como ejemplo materializado en un intercambio 900 de claves de un pase;

La figura 10 ilustra un ejemplo de sistema 1000 de manejo de hardware/información para incorporar en él la presente invención; y

La figura 11 ilustra un medio 1100 de soporte de señales (por ejemplo, un medio de almacenamiento), para almacenar los pasos de un programa de un método, de acuerdo con la presente invención.

Descripción detallada de ejemplos de modos de realización de la invención

Haciendo referencia ahora a los dibujos, y más en particular a las figuras 1-11, en ellos se muestran ejemplos de modos de realización de los métodos y estructuras de acuerdo con la presente invención.

Como nota preliminar sobre grupos y notación, todos los protocolos y operaciones estudiados en esta memoria suponen un grupo cíclico G de orden q, típicamente un número primo, generado por un generador g. La longitud en bits de q está indicada por $|q|$ (por ejemplo, $|q| = \lceil \log_2 q \rceil$, que significa el logaritmo de q en base 2, redondeado hacia arriba hasta el entero más próximo), y esta cantidad se utiliza como un parámetro de seguridad implícita. Los parámetros G, g y q se suponen, por simplicidad, que son fijos y conocidos de antemano por las partes, como es común en la práctica. Alternativamente, se podrían incluir estos valores en los certificados, etc.

En esta memoria se utiliza la representación multiplicativa de operaciones en grupo, pero el tratamiento es igualmente aplicable a grupos aditivos, tales como las curvas elípticas, o cualquier otro grupo algebraico o grupos específicos, campos finitos, módulos compuestos, etc. En los protocolos, las claves públicas, indicados por letras en mayúsculas (por ejemplo, A, B), son elementos del grupo G, y las claves privadas, indicadas por las correspondientes letras en minúsculas (por ejemplo, *a, b*), son elementos en Z_q, donde Z_q indica el conjunto de números enteros 0, 1, ..., q-1.

Por ejemplo, una clave pública $A = g^n$ se corresponde con una clave privada a. La parte que tiene A como clave pública será indicada como $\hat{A}$, considerada tradicionalmente como "Alicia" (una segunda parte $\hat{B}$ se considera tradicionalmente como "Bob"). En general, la "notación del sombrero" (circunflejo) se utiliza para indicar las identidades lógicas o "de distinción" de las partes en el protocolo, tal como el nombre, la dirección de e-mail, un protagonismo, etc. En algunos casos, estas identidades pueden ser aumentadas con un certificado digital. Para el más completo análisis matemático proporcionado en la Solicitud provisional, que no se repite aquí, todas las partes del protocolo, incluyendo el atacante, se consideran implementadas por medio de máquinas probabilísticas de polinomios-tiempo. El atacante está indicado también por M, donde M podría significar "malicioso".

Por tanto, como se ilustra en la figura 1, el cálculo de la clave de la sesión para el protocolo básico 100 de Diffie-Hellman no autenticado consiste en un intercambio entre las dos partes, $\hat{A}$ y $\hat{B}$, donde la parte $\hat{A}$ envía su clave $X = g^x$ a la parte $\hat{B}$, y la parte $\hat{B}$ responde entonces transmitiendo su clave $Y = g^y$ a la parte $\hat{A}$, y donde x e y son secretas elegidas por $\hat{A}$ y por $\hat{B}$, respectivamente, aleatoriamente en el conjunto Z_q, y donde la clave compartida de la sesión se calcula como g^{xy}.

Debe observarse que, en esta descripción, el símbolo $_R$ se utiliza a veces para indicar una selección aleatoria. Por ejemplo, $x \in_R Z_q$ significa que se elige el valor x aleatoriamente entre el conjunto de enteros Z_q, utilizando típicamente un generador de números aleatorios o pseudo-aleatorios.

El protocolo MQV

La comunicación en el protocolo MQV es idéntica al protocolo básico 100 DH no autenticado representado en la figura 1, excepto que las identidades $\hat{A}$, $\hat{B}$ pueden incluir información adicional, tal como un certificado de clave pública, o estas identidades pueden ser omitidas todas ellas conjuntamente.

Un primer reto al diseñar un protocolo de intercambio de claves autenticadas de dos mensajes es impedir que tenga éxito un ataque, basándose en la respuesta del primer mensaje del protocolo. Esto es problemático, ya que el primer mensaje no puede incluir ninguna forma de "garantía de frescura" específica de la sesión (por ejemplo, un valor del momento actual o valor DH recién hecho) contribuido por el que responde. Una solución a este problema es proporcionar la frescura por medio del cálculo de la clave de la sesión.

Por ejemplo, el protocolo 200 de dos mensajes de Diffie-Hellman ilustrado en la figura 2, es autenticado utilizando firmas digitales, como se ha adoptado a partir del protocolo 9793 de ISO (Organización Internacional de Estándares). Aunque la inclusión de g^x bajo la firma de $\hat{B}$ proporciona frescura a la autenticación, esta salvaguarda no existe en el mensaje de $\hat{A}$. Aún así, la clave de la sesión, g^{xy}, se garantiza como recién hecha (e independiente de otras claves de la sesión), ya que se hace aleatoria por medio de la *y* recién hecha. Sin embargo, la seguridad del protocolo se rompe si el atacante es capaz de encontrar una sola pareja (x, g^x) utilizada por $\hat{A}$ en una sesión con $\hat{B}$, en cuyo caso el atacante aprende también la firma $\hat{A}(g^x, \hat{B})$. Esto permite al atacante hacerse pasar por $\hat{A}$ a $\hat{B}$ indefinidamente, utilizando el mismo mensaje y su conocimiento de x, y sin tener que aprender nunca la clave de la firma privada de largo plazo de $\hat{A}$.

Esta es una vulnerabilidad seria que viola el principio básico de que la divulgación de la información efímera específica de la sesión (por ejemplo, la pareja (x, g^x)) no debería comprometer otras sesiones. Esto es particularmente serio considerando que muchas aplicaciones calcularán esta pareja (x, g^x) fuera de la línea, y la mantendrá en un almacenamiento menos protegido que, por ejemplo, la clave privada de largo plazo.

Entonces, ¿cómo se puede diseñar un protocolo de dos mensajes que sea inmune a ataques de repetición, incluso cuando se escapa información efímera? La respuesta natural es incluir una clave privada de largo plazo en el cálculo de la clave de la sesión. Este ha sido el enfoque iniciado en el trabajo de 1986 de Matsumoto, Takashima e Ima que motivó muchas de las llamadas variantes "implícitamente autenticadas" de Diffie-Hellman, incluyendo MVQ. En este enfoque, cada parte tiene una clave pública DH de largo plazo y su correspondiente exponente secreto, y las sesiones se generan por combinación de los valores efímeros DH específicos de la sesión, con las claves públicas y privadas de las partes. Por tanto, la seguridad de tal protocolo depende enteramente de los detalles exactos de esta combinación de claves. De manera notable, esta idea aparentemente simple ha sido difícil de implementar con seguridad, y todas las propuestas anteriores han sufrido diversos inconvenientes.

Considerando ahora la solución natural siguiente al problema de combinar claves efímeras y de largo plazo en el cálculo de la clave de la sesión, cuando $\hat{A}$ y $\hat{B}$ desean intercambiar una clave, efectúan un protocolo básico de Diffie-Hellman y calculan la clave de la sesión como $K = g^{(x+a)(y+b)} = (YB)^{x+a} = (XA)^{y+b}$. En este caso, si un atacante aprende *x* pero no *a*, no puede calcular *K*.

Aún así, el protocolo sigue siendo inseguro, como se demuestra con el siguiente ataque simple: *M* elige un valor $x^* \in_R Z_q$, calcula $X^* = g^{x^*}/A$ y envía X^* a $\hat{B}$ como una suplantación de un mensaje inicial de $\hat{A}$. $\hat{B}$ envía $Y = g^y$ y calcula la clave de la sesión $K = (X^*A)^{y+b}$. Desafortunadamente, M puede calcular también *K* como $(BY)^{x^*}$. Por tanto, el protocolo es inseguro.

Más aún, incluso si se cambia el cálculo de K para que sea $K = g^{(x+da)(y+eb)}$ para las constantes *d, e,* el ataque sigue siendo posible. Por otra parte, si se permite que las constantes *d, e* varíen con *X,Y* de una manera tal que el atacante no pueda controlar *e* e *Y* separadamente, el simple ataque anterior puede no funcionar. Esta idea nos lleva de nuevo al diseño de MQV, donde $d = \overline{X}$ y $e = \overline{Y}$.

El cálculo 301, 302 de la clave K de la sesión en MQV está ilustrado en la figura 3, donde la parte $\hat{A}$ posee una clave privada de largo plazo $a \in Z_q$ y la correspondiente clave pública $A = g^a$. De forma similar, la pareja de claves privada/pública de B es *(b, B = g^b),* y los valores efímeros de DH son $X = g^x$ e $Y = g^y$, donde x, y son elegidos por A, B respectivamente. El cálculo de la clave de la sesión utiliza también los valores $d = \overline{X}$ y $e = \overline{Y}$, donde $\overline{X} = 2' + (X \bmod 2')$ e $\overline{Y} = 2' + (Y \bmod 2')$ para $l = |q|/2$.

Debe observarse que el cálculo de la clave de la sesión por $\hat{A}$ implica una exponenciación fuera de línea para calcular $X = g^x$, una exponenciación en línea para calcular B^e, y una exponenciación adicional en línea para $(YB^e)^{x+da}$. Sin embargo, debe observarse también que la segunda exponenciación utiliza un exponente *e* de longitud $|q|/2$ y, por tanto, cuenta como una "media exponenciación" (es decir, la mitad del número de multiplicaciones con respecto a una exponenciación normal de *g*). El mismo cómputo de operaciones es válido para $\hat{B}$.

En su conjunto, el rendimiento de MQV es verdaderamente impresionante: la misma comunicación que en el protocolo básico de DH no autenticado (excepto la posible transmisión de certificados como parte de las identidades de las partes) y justamente media exponenciación más que en el protocolo básico, que es un mero aumento del 25% en el cálculo para conseguir un intercambio autenticado. Esto es significativamente mejor que cualquiera de los protocolos DH probados que confían en firmas digitales o en el cifrado de claves públicas para la autenticación, que implican operaciones más costosas y un aumento en la anchura de banda. También es el más eficaz de los protocolos DH implícitamente autenticados, siendo los más cercanos los protocolos del "Modelo Unificado" que requieren tres exponenciaciones completas, pero que ofrecen características de seguridad sustancialmente menores.

Este rendimiento excepcional y la promesa de seguridad hace de MQV un candidato atractivo cuando se elige un protocolo DH autenticado. Por estas razones, el protocolo ha sido adoptado para muchos estándares y se ha estudiado ampliamente en la literatura. Aún así, una pregunta que todavía no ha sido contestada hasta ahora es cómo es de seguro realmente el protocolo MQV, ya que no se ha efectuado con éxito ningún análisis formal del protocolo MQV en ninguno de los modelos formales de la seguridad de intercambio de claves.

Por otra parte, los diseñadores de MQV han sido explícitos sobre los objetivos de seguridad detrás del diseño. Estos incluyen la seguridad esencial contra la suplantación de personalidad y ataques de claves conocidas (incluyendo la resistencia a los ataques para "compartir claves desconocidas (UKS)", así como características más específicas tales como el envío perfecto de secretos (PFS) y la resistencia a los ataques KCI (suplantación de personalidad con compromiso de claves). La resistencia a los ataques de claves conocidas representa el principio de que la divulgación de información secreta efímera específica de la sesión no debería comprometer la seguridad de otras sesiones.

Las propiedades de PFS y KCI se refieren al confinamiento de daños a la seguridad en el caso de que la clave privada de una parte se escape hacia el atacante *M*. Más específicamente, PFS significa que cualquier clave de sesión establecida entre dos partes no maliciosas no puede ser aprendida por *M*, incluso cuando ambas partes son maliciosas después de haber borrado la clave de la sesión de la memoria de las partes. La resistencia a los ataques KCI requiere que un atacante que aprende una clave privada de largo plazo de una parte Â y, por tanto, podría suplantar la personalidad de Â a otras partes, no pueda suplantar la personalidad de otras partes no maliciosas para Â.

Desafortunadamente, los resultados del análisis del presente inventor, como se ha descrito con más detalle en la Solicitud provisional antes descrita, indican que ninguna de estas propiedades, cuando se estudian formalmente, sea satisfecha por el protocolo MQV. Específicamente, se demuestra que, en el modelo de seguridad de Canetti y Krawczyk, el protocolo está abierto a una gama de ataques que contradicen las propiedades de seguridad antes descritas, y que se alega que son satisfechas por MQV.

El protocolo HMQV

El protocolo HMQV ("H" puede ser considerada con el significado de "Hash" (algoritmo de cifrado troceado)) es una variante sencilla pero potente de MQV que, en varios ejemplos de modos de realización, puede incluir el algoritmo "hashing", tal como se ilustra en el paso 303 de la figura 3, adicional a los protocolos MQV convencionales, ilustrados en el paso 302 para comparación. Sin embargo, debe observarse también, como asunto inicial, que el paso o pasos del "hashing" de estos ejemplos de modos de realización no son un prerrequisito para la presente invención, ya que hay modos de realización alternativos, tanto sin "hashing" como utilizando técnicas distintas al "hashing", que se estudian en esta memoria y que son incluidos también en los conceptos de la invención. Un concepto más fundamental de la presente invención está relacionado con el esquema de firmas de preguntas-respuestas a partir del cual evolucionaron varias aplicaciones y modos de realización, incluyendo los ejemplos de versiones hechas con el algoritmo de "hashing" del protocolo MQV.

El algoritmo "hashing", como es bien sabido en la técnica, implica utilizar una función "hash" (troceado) para convertir una cadena de caracteres en un número, un cadena de longitud fija (es decir, un troceado o recopilación de mensajes), etc., como una salida. La funcionalidad básica de las funciones "hash" en criptografía es proporcionar una transformación "unidireccional" o "irreversible", lo que significa que debería no ser factible recuperar los datos originales, y también no factible para construir un bloque de datos que coincida con un valor dado de "hash". Las funciones "hash" pueden variar desde simples funciones "mezcladoras" a transformaciones que asemejan un cifrado puramente aleatorio. Estas últimas son denominadas "funciones hash criptográficamente fuertes" y son modeladas a menudo en el análisis criptográfico por funciones aleatorias ideales (u "oráculos aleatorios").

Se utilizan ampliamente varias funciones hash para un fuerte método de troceado criptográfico (hashing). Por ejemplo, MD5 toma un bloque de datos de tamaño arbitrario como entrada y produce un hash de 128 bits (16 bytes) utilizando operaciones en base a bits, suma y una tabla de valores basados en la función seno, para procesar los datos en bloques de 64 bytes. Otra importante función hash es el Algoritmo Hash Seguro (SHA) del NIST (Instituto Nacional de Estándares y Tecnología), que proporciona un hash de 160 bits.

Típicamente, las funciones hash no se usan directamente para el cifrado, sino que las funciones de cifrado proporcionan una transformación unidireccional y son, por tanto, aplicables a algunos usos del hashing, incluyendo algunos ejemplos de modos de realización de la presente invención. Las funciones hash son también muy adecuadas para la autenticación de datos y se utilizan para tales fines conjuntamente con claves secretas (en estos ajustes son denominadas a menudo MAC, que significa Códigos de Autenticación de Mensajes, o PRF, que significa Funciones Pseudos-Aleatorias) o esquemas de firmas (donde los valores hash se utilizan para las "recopilaciones de mensajes").

Diversos ejemplos de modos de realización de la presente invención utilizan al menos una función hash H que es resumida como un oráculo aleatorio ideal en el análisis de seguridad descrito con más detalle en la Solicitud Provisional antes mencionada. Dos tareas para las cuales se utiliza la función H en estos ejemplos de modos de realización son las siguientes: primera, el cálculo de los exponentes d, e; y segunda, la obtención de la propia clave de la sesión.

La primera tarea utiliza de manera ejemplar dos argumentos para H y entrega una cadena de longitud |q|/2, mientras que la segunda aplica *H* a un solo argumento y entrega una clave de una longitud especificada (por ejemplo, 128 bits).

Para simplificar la notación, se utiliza el mismo símbolo *H* para indicar ambas aplicaciones de las funciones hash. En la práctica, se utilizaría una sola *H*, por ejemplo SHA-1, que pueda manejar entradas de longitud variable y cuyo tamaño de salida pueda ser sintonizado para ajustarse a las dos tareas, utilizando posiblemente alguna combinación de truncamiento/expansión al producir el resultado de hash.

Sin embargo, debe observarse también que si se utiliza el hashing en la primera tarea, no estaría necesariamente confinado a dos argumentos, ya que argumentos adicionales, tales como una marca de tiempos, la presente ocasión, etc., podrían ser incluidos como entradas en la función de hash, en lugar de efectuar el hashing solamente en un mensaje o una identidad de una parte.

Cuando se utiliza el hashing, la función hash utilizada para generar los exponentes d, e (típicamente con l = |q|/2 bits de salida) es indicada a menudo como $\overline{H}$ y la función hash aplicada a los σ valores con *k* bits de salida es indicada como *H*. En la práctica, se puede utilizar la misma función hash con distintas longitudes de salida, y por tanto el símbolo H se utiliza algunas veces en lugar del $\overline{H}$. Como regla nemotécnica, la barra en $\overline{H}$ indica que la salida de la función se utiliza como un exponente.

Como en el MQV, la comunicación del protocolo HMQV es idéntica al intercambio básico DH ilustrado anteriormente en la figura 1, con la posible adición de certificados. Como en el ejemplo de la figura 3, el cálculo de la clave K de la sesión difiere del de MQV en el cálculo de los valores d y e, que implica el hashing del valor DH poseído por la parte y la identidad del homólogo. Una salida típica de este hash es l = |q|/2 bits. Además, en un ejemplo de modo de realización, HMQV especifica el hashing de los valores $\sigma_{\hat{A}} = \sigma_{\hat{B}}$ en claves de *k* bits, donde *k* es la longitud de la clave de la sesión deseada. En modos de realización alternativos, una o ambas funciones no han sido objeto de hash.

A partir de esta descripción, se puede observar que el HMQV conserva el notable rendimiento de MQV tanto en términos de comunicaciones como de cálculo. Al mismo tiempo, el HMQV supera todos los inconvenientes de seguridad del MQV que se estudian en la Solicitud provisional de patente antes mencionada, en la mayor medida posible de un protocolo de dos mensajes, como se estudia con más detalle y se prueba en esa Solicitud. Un relato más completo de las propiedades de seguridad y ventajas del HQMV y sus variantes, se presenta más adelante en esta solicitud.

Firmas de preguntas-respuestas

Aunque debe estar claro ahora cómo difiere el protocolo HMQV del protocolo MQV, existe otro aspecto de la presente invención que es, en un sentido, incluso más fundamental: una herramienta técnica principal que se erige en el diseño básico y elemento de análisis detrás del HMQV, es una nueva forma de firmas interactivas, denominada "firmas de preguntas-respuestas", que es implementada sobre la base de una nueva variante de esquema de identificación de Schnorr, utilizando la metodología de Fiat-Shamir. Como resultado, se obtienen las firmas de "preguntas-respuestas exponenciales" (XCR) de la presente invención. La relación entre las metodologías de Schnorr y Fiat-Shamir y las firmas XCR se estudia a continuación.

Estas firmas XCR son seguras en el modelo del oráculo aleatorio (bajo la suposición del Diffie-Hellman Computacional, o CDH, véase más adelante) y tiene la propiedad de que tanto el verificador como el firmante pueden calcular, como ejemplo, la misma firma. El primero consigue esto conociendo la pregunta, y el segundo pude hacerlo al saber la clave privada de la firma. Las variaciones de cálculo de idéntica firma incluyen el cálculo de firmas diferentes, pero relacionadas, por el firmante y por el verificador.

Por ejemplo, el valor de la firma calculada por uno puede ser una variante hash de la firma calculada por el otro, o pueden estar relacionadas por alguna propiedad algebraica particular, etc. Las diversos protocolos HMQV de la presente invención son un ejemplo de mecanismo que utiliza estas firmas XCR, donde proporcionan autenticación (de valores DH y de la identidad del homólogo) así como el cálculo de la clave de la sesión.

Por tanto, las firmas XCR, así como su "versión dual" (por ejemplo DCR) que se van a estudiar en breve, proporcionan una interpretación natural, tanto técnica como conceptual, de las ideas subyacentes en el diseño y el análisis del HMQV.

Además, debe observarse que las firmas XCR pueden ser utilizadas también en aplicaciones más allá del protocolo HMQV. En su forma básica, las firmas XCR no proporcionan la funcionalidad clásica de las firmas digitales, ya que son interactivas, específicas de la pregunta y no transferibles. Es decir, no pueden ser utilizadas para fines de no rechazo.

Por otra parte, proporcionan una "autenticación" negable, una propiedad importante para algunas aplicaciones, incluyendo el intercambio de claves, por medio del cual el receptor de una firma XCR puede estar seguro del origen e integridad de un mensaje o una clave, pero no puede probar este origen a ninguna tercera parte. En particular, estos protocolos de intercambio de firmas y clave resultante son idealmente adecuados para comunicaciones "confidenciales" y protección privada. Además, existen versiones no interactivas de XCR, como se estudia a continuación y, en algunos casos, proporcionan alternativas a los esquemas de firmas establecidos, tales como el muy conocido Algoritmo de Firma Digital (DSA).

Como en un esquema normal de firmas digitales, en un esquema de firmas de preguntas-respuestas, un firmante tiene una pareja de claves, privada y pública, utilizadas para la generación y verificación, respectivamente, de firmas, y se supone que el verificador obtiene la clave pública auténtica del firmante. En particular, se supone que las partes no comparten un secreto antes de iniciar el protocolo de firmas, ni tal secreto compartido está implicado en el cálculo de las firmas. Sin embargo, como contraste a las firmas normales, en su forma básica, las firmas de preguntas-respuestas son interactivas y requieren que el receptor (es decir, el verificador) de la firma emita una pregunta al firmante antes de que éste último pueda generar la firma para un mensaje dado. Un esquema seguro de firmas de preguntas-respuestas necesita garantizar que ningún otro excepto el firmante legítimo sea capaz de generar una firma que convenza al que pregunta para que acepte la firma como válida. En particular, una firma no solamente es específica del mensaje, sino también específica de la pregunta.

Por otra parte, es de interés asegurar la capacidad de verificación de la firma por el que pregunta, y por tanto, no hay suposiciones o requisitos relativos a la capacidad de transferencia, o la capacidad de verificación, por una tercera parte, de la firma. Más aún, el esquema específico descrito a continuación tiene la propiedad de que la parte que elige la pregunta siempre puede generar una firma, en cualquier mensaje, que es válido con respecto a la pregunta en particular. Lo que es aún más importante para la presente solicitud, y lo que diferencia este esquema de otras firmas interactivas, es el hecho de que el verificador pueda calcular, utilizando una pregunta, la misma cadena de firmas (o relacionada con ella) que el firmante.

Como antes, g es el generador de un grupo G de orden q (usualmente primo). Además, H es una función hash que entrega $|q|/2$ bits ($|q| = \lceil \log_2 q \rceil$), pero, nuevamente, el uso de "orden primo" y la longitud específica de la salida de H son solamente ejemplos de detalles de diseño de ejemplos de modos de realización, y no son esenciales para la invención.

Definición del esquema de firmas XCR

El esquema exponencial 500 de firmas de preguntas-respuestas (XCR), ilustrado en la figura 4, se define como sigue: El firmante en un esquema XCR, indicado como $\hat{B}$, posee una clave privada $b \in_R Z_q$ y una clave pública $B = g^b$. Un verificador (o el que pregunta), indicado como $\hat{A}$ proporciona una pregunta inicial X que $\hat{A}$ calcula como $X = g^x$, para $x \in_R Z_q$, donde x se elige y se mantiene en secreto por $\hat{A}$. La firma de $\hat{B}$ en un mensaje dado m, utilizando la pregunta X, se define como la pareja $(Y, X^{y+\overline{H}(Y,m)b})$, donde $Y = g^y$ e $y \in_R Z_q$, son elegidos por $\hat{B}$ y el exponente $y+\overline{H}(y,m)b$ es un módulo q reducido. El verificador $\hat{A}$ acepta una pareja de firmas (Y,σ) como válida (para el mensaje m y la pregunta $X = g^x$) si, y solamente si, se mantiene que $(YB^{\overline{H}(Y,m)})^x = \sigma$.

Utilizamos la notación siguiente: para un mensaje dado m, pregunta X y valor Y, definimos $XSIG_B(Y,m,X) = X^{y+\overline{H}(Y,m)b})$, es decir, $XSIG_{\hat{B}}$ indica el segundo elemento en una pareja de firmas XCR. Como nota general, merece la pena observar que el uso anterior de la palabra "mensaje" es representativo de cualquier forma de datos o información que pueda ser representada por una cadena de bits, incluyendo los datos transmitidos, ficheros, medios, etc., y puede ser por sí mismo una versión hash de un mensaje más largo. Este mensaje puede ser introducido a las partes como se ilustra en la figura 5, o puede ser transmitido desde una parte a la otra, o puede ser proporcionado por una tercera parte, una fuente externa, etc.

Como se describe en esta Solicitud, las ventajas de las firmas XCR incluyen: consistencia analítica (capacidad de ser probada), capacidad de ser calculada tanto por el verificador como por el que la prueba, dualidad (un solo cálculo que representa el conjunto de firmas por dos o más partes), capacidad de "hashing" (es decir, la capacidad de funcionar y verificar las firmas con hashing), obtención de claves o valores comunes, no posibilidad de transferencia y capacidad de rechazo, posibilidad de conversión (de firmas negables en firmas tradicionales no rechazables), proporcionando una alternativa más robusta que el DSS (especialmente en entornos interactivos), y la existencia de variantes no interactivas.

Puede ser ilustrativo motivar el diseño del esquema XCR a través de su relación con el esquema de identificación de Schnorr, a partir del cual se obtienen las firmas XCR. El esquema de identificación (interactiva) de Schnorr consiste en una prueba de conocimiento del logaritmo discreto b para una entrada dada $B = g^b$. Indiquemos con $\hat{B}$ el probador en este esquema (que posee b) y con $\hat{A}$ el verificador (al que se le da la entrada B). La identificación básica de Schnorr consiste en tres mensajes:

(i) $\hat{B}$ elige $y \in_R Z_q$, y envía $Y = g^y$ a $\hat{A}$;

(ii) $\hat{A}$ responde con un valor aleatorio $e \in_R Z_q$; y

(iii) $\hat{B}$ envía a $\hat{A}$ el valor s = y + eb. $\hat{A}$ acepta si, y solamente si, se mantiene que $g^x = YB^e$.

Este protocolo es una prueba de conocimiento cero de acuñamiento público del conocimiento (de b) contra un verificador honrado $\hat{A}$ (por ejemplo, uno que elija e uniformemente al azar). Por tanto, se puede transformar a través de la muy conocida metodología de Fiat-Shamir en un esquema de firmas, es decir, $SIG_{\hat{B}}(m) = (Y, y + H(Y, m)b)$, que es probadamente seguro en el modelo del oráculo aleatorio.

Considérese ahora la siguiente variante de cuatro mensajes del protocolo de Schnorr, en el cual se añade un primer mensaje desde $\hat{A}$ hasta $\hat{B}$. En este primer mensaje, $\hat{A}$ envía a $\hat{B}$ un valor $X = g^x$. Entonces, siguen los tres mensajes del

esquema de Schnorr, excepto que en el mensaje (iii), es decir, el cuarto en el protocolo modificado, en lugar de enviar $s = y + eb$ a Â, B̂ envía $S = X^S$. Â acepta si, y solamente si, $S = (YB^e)^x$. Se puede demostrar que este protocolo es un prueba de la "capacidad" de B̂ de calcular el valor de Diffie-Hellman CDH(*B,X*) para cualquier valor de *XG*.

Más aún, el protocolo es de conocimiento cero contra un verificador Â que elija *e* al azar, mientras que *X* puede ser elegido arbitrariamente.

Aplicando la transformación de Fiat-Shamir a este protocolo, se obtiene la firma XCR de preguntas-respuestas de la presente invención. Esto explica también por qué se utiliza el término "exponencial" en el nombre del esquema XCR: se refiere a la sustitución de $s = y + eb$ en el esquema de Schnorr por X^S en el último mensaje del protocolo.

En la Solicitud provisional anteriormente identificada, se estudian aspectos adicionales de la seguridad del esquema de firmas de XCR, bajo la suposición CDH.

Para explicar alguna parte de la terminología anterior, para dos elementos $U = g^u$, $V = g^v$ en *G*, indicamos con *CDH(U,V)* el resultado de aplicar el cálculo U y V de Diffie-Hellman (es decir, $CDH(U,V) = g^{uv}$). Un cierto algoritmo se llama "solucionador CDH para G", cuando toma como parejas de entradas de los (U,V) en G y entrega el resultado *CDH(U,V)* de Diffie-Hellman. La principal suposición de capacidad interactiva utilizada en el análisis proporcionado adicionalmente en la Solicitud provisional, es la suposición de Cálculo de Diffie-Hellman (CDH). Se puede decir que la suposición CDH se mantiene en el grupo G si, para todos los solucionadores CDH eficaces para *G*, la probabilidad de que, en una pareja (U,V), para $U,V \in_R G$, el solucionador calcule el valor correcto de *CDH(U,V)* es despreciable (la probabilidad tomada sobre las acuñaciones aleatorias del solucionador y la elección de *U, V* independientemente al azar en *G*).

El número de bits en $\overline{H}(Y,m)$.

Sea *l* el número de bits en la salida de $\overline{H}(Y,m)$. Claramente, cuanto menor es *l*, más eficiente es el esquema de firmas. Por otra parte, una *l* muy pequeña implica un límite de seguridad malo, ya que el exponente $\overline{H}(Y,m)$ es predecible, el esquema de firmas es inseguro. Pero, ¿cómo de grande se necesita *l* para fines de seguridad?

Se puede demostrar (véase la discusión en la Solicitud provisional antes referenciada) que el ajuste $l = 1/2\ |q|$ proporciona un buen equilibrio entre la seguridad y el rendimiento y, por tanto, este valor se utiliza en el ejemplo de especificación de las firmas XCR (y para su ejemplo de aplicación al protocolo HMQV de la presente invención).

Cambio del orden de interacción con B

En algunas aplicaciones de las firmas XCR, en particular cuando se aplican al análisis del protocolo HMQV, puede cambiarse el orden de interacción entre el que pregunta Â y el firmante B̂.

En la definición anterior del esquema XCR, Â presenta a B̂ el mensaje *m* al mismo tiempo que proporciona la pregunta X a B̂, permitiendo así a B̂ responder inmediatamente con la pareja de firmas (Y, $XSIG_{\hat{B}}(Y, m, X)$). En la versión modificada ahora considerada, existe el siguiente orden de interacción:

(i) Â presente el mensaje m a B̂ y B̂ entrega Y, después, en algún momento posterior,

(ii) Â proporciona (Y,m,X) a B̂, y B̂ entrega $XSIG_{\hat{B}}(Y, m, X)$.

Ahora, supóngase que una parte F solicita a B̂ que admita esta orden modificada. En particular, F puede intercalar distintas interacciones con B̂, es decir, F puede ejecutar distintos ejemplos del paso (i) antes de ejecutar el correspondiente paso (ii). Esto requiere que B̂ mantenga su condición después del paso (i), con los valores de *Y, y* y *m*. Cuando F presente más tarde *(Y,m,X)* en el paso (ii), B̂ comprueba que tiene la pareja *(Y, m)* en su estado y, si es así, responde con $XSIG_{\hat{B}}(Y, m, X)$ y elimina *(Y, m)* de su estado (si B̂ no tuviera la pareja *(Y, m)* en su estado, no emite la firma).

Obsérvese que esta especificación de las acciones de B̂ asegura que B̂ nunca utilizará el mismo valor de *Y* para dos firmas diferentes. Se puede verificar fácilmente que la prueba de seguridad de las firmas XCR permanece válida para este orden modificado, simplemente porque la simulación de la elección de *Y* por B̂ no requiere el conocimiento de *X*, sino solamente el valor de *m* necesario para determinar $\overline{H}(Y,m)$.

Una variante con hash de XCR (HCR)

Es posible sustituir las parejas de firmas XCR (Y, σ) por parejas (Y, H(σ)), donde H es una función hash, y tales firmas de "XCR con hash" se abrevian como "HCR". Obsérvese que, debido a la propiedad de XCR por medio de la cual el verificador es capaz de recalcular σ, dada Y, entonces puede calcular también H(σ) y, por tanto, es capaz de verificar la firma HCR modificada.

Las firmas HCR tienen una gama de propiedades que son importantes en algunos ajustes. Por ejemplo, pueden ser más cortas que las firmas XCR normales, pueden dar como resultado valores aleatorios o pseudos-aleatorios, pueden impedir que un atacante aprenda cualquier estructura algebraica en σ, etc.

En particular, en entornos de autenticación interactivos y específicos del verificador (tales como en los protocolos de intercambio de claves), las firmas HCR ofrecen una alternativa más segura a las firmas DSA. En realidad, aunque en DSA, la divulgación de un solo exponente efímero (por ejemplo, k en el componente $r = g^k$ de una firma DSA) hace que el esquema de firmas sea totalmente inseguro al revelar la clave de firma privada, las firmas HCR son infalsificables incluso si se revela el exponente efímero y al atacante (siempre que, en este caso, el firmante compruebe el orden de la pregunta X o utilice una exponenciación de factores cooperantes para forzar que el valor sea del orden de al menos q).

Una variante no interactiva de XCR

Las firmas XCR (y HCR) pueden hacerse no interactivas, pero específicas del verificador, poniendo $X = A$, donde A es una clave pública del verificador, como se ilustra en la figura 6. Esto proporciona un mecanismo de autenticación negable muy eficiente, no interactivo y específico del verificador. En una variante, en lugar de utilizar una clave pública única A de una parte Â, esta última puede hacer pública (por ejemplo, poniéndola en una página web) una o más preguntas para ser utilizadas por el firmante, haciendo así que estas preguntas estén disponibles incluso cuando el propio Â no este disponible en el momento de la firma.

Firmas XCR convertibles

Una destacada propiedad de las firmas XCR (que, en particular, las diferencia de otros mecanismos "negables" de preguntas-respuestas, incluyendo aquellos que están basados en secretos compartidos y cifrado de claves públicas), es la capacidad de "convertir" estas firmas en firmas normales, no rechazables. Las firmas convertibles poseen la propiedad de la autenticación negable, es decir, pueden ser verificadas solamente por el receptor de destino, pero también permiten al firmante probar eventualmente que es el autor de una firma dada, sin revelar su clave de firma privada.

Esta capacidad de conversión desde una firma privada a una pública puede ser necesaria, por ejemplo, para la comunicación oficial confidencial que, tras varios años, debe ser convertida en un registro público verificable. En el caso de firmas XCR, una firma (Y, σ) en un mensaje m bajo una pregunta X, puede ser convertida por el firmante legítimo en una firma normal no rechazable, revelando el valor $y+\underline{H}(Y,m)b$.

Aunque en la literatura específica se han presentado otras firmas convertibles (específicas del receptor), ninguna de éstas permiten al receptor de destino (o entidad que pregunta) volver a calcular la firma por sí misma y, por tanto, no comparten las muchas ventajas que esta propiedad de re-calcular proporciona a las firmas XCR, como se muestra en los ejemplos de las siguientes firmas XCR Duales.

Firmas XCR Duales (DCR)

Una propiedad importante de las firmas XCR es que el que pregunta, una vez elegida la pregunta, puede calcular la firma por sí mismo. En este caso se muestra cómo aprovechar esta propiedad con el fin de obtener un esquema de firmas de preguntas-respuestas relacionado (que se denomina en este caso como "esquema XCR dual", o brevemente DCR) con la propiedad de que dos partes cualesquiera, Â, B̂ pueden interactuar mutuamente con los protagonismos duales del que pregunta y del firmante, y cada uno puede producir una firma que no puede ser falsificada por un tercero. Más aún, y esto es lo que hace al esquema significativo para el protocolo HMQV, las firmas resultantes por Â y B̂ tienen el mismo valor. Más precisamente, tienen el mismo componente *XSIG* en una pareja de firmas XCR.

Definición: El esquema dual (exponencial) de firmas de preguntas-respuestas (DCR). Sean Â, B̂ dos partes con claves públicas $A = g^a$, $B = g^b$, respectivamente. Sean m_1, m_2 dos mensajes. La firma XCR dual (brevemente, DCR) de Â y B̂ en los mensajes m_1, m_2, respectivamente, se define como una tripleta de valores: X, Y y $DSIG_{Â,B̂}(m_1,m_2,X,Y)$ $\underline{B}g^{(x+da)(y+eb)}$, donde $X = g^x$ e $Y = g^y$ son preguntas elegidas por Â, B̂, respectivamente, y los símbolos d y e indican $\underline{H}(X,m_1)$ y $\underline{H}(Y,m_2)$, respectivamente. (Véase la figura 7).

De esa manera, una propiedad fundamental de una firma DCR es que, tras intercambiar los valores X e Y (siendo x e y elegidos por Â y B̂, respectivamente), tanto Â como B̂ pueden calcular (y verificar) la misma firma $DSIG_{Â,B̂}(m_1,m_2,X,Y)$. Esto puede observarse a partir de las siguientes equivalencias:

$$DSIG_{Â,B̂}(m_1,m_2,X,Y) = g^{(x+da)(y+eb)} = (YB^e)^{x+da} = (XA^d)^{y+eb}$$

donde $x+da$ e $y+eb$ son módulo q reducido.

Más aún, un atacante no puede calcular factiblemente esta firma, como se demuestra en el estudio de la Solicitud provisional antes mencionada.

Hablando en términos generales, una firma dual es una firma XCR por Â sobre el mensaje m_1, bajo la pregunta YB^e, y al mismo tiempo, una firma XCR por B̂ sobre el mensaje m_2, bajo la pregunta XA^d. Más precisamente, como los valores *d* y *e* se determinan durante el proceso de firma (a través de la elección posiblemente adversa de los mensajes m_1, m_2), se puede demostrar entonces que una firma DCR de B̂ es segura con respecto a cualquier valor $A = g^a$ no elegido por el atacante.

Descripción formal del protocolo básico HMQV

El protocolo HMQV, en su intercambio básico de dos mensajes, consiste en un intercambio entre las partes Â y B̂, de los valores de Diffie-Hellman $X = g^x$ e $Y = g^y$ que sirven como preguntas a partir de las cuales ambas partes calculan la firma XCR dual $DSIG_{\hat{A},\hat{B}}$ *("Â", "B̂", X, Y)* $= g^{(x+da)(y+eb)}$. La clave de la sesión se obtiene entonces efectuando el hash sobre este valor. De esta manera, la propia firma no necesita ser transmitida: es la exclusividad de la firma la que asegura un valor obtenido común de la clave de la sesión, y es la capacidad exclusiva de calcular la clave (equivalentemente, la firma) la que proporciona una prueba de que el intercambio se ha llevado a cabo por las partes que lo alegan Â, B̂.

Fundamentalmente, como los mensajes m_1, m_2 sobre los cuales se calcula la firma, son identidades de la pareja (es decir, de Â, B̂), ambas partes tienen la seguridad de que la clave que han calculado está limitada exclusivamente a las identidades correctas. Esta inclusión de las identidades de las partes, no simplemente los valores efímeros de Diffie-Hellman, bajo la firma (en particular, en el cálculo de los valores d y e), es esencial para evitar algunos fallos de autenticación, tales como los ataques UKS.

Por tanto, una sesión del protocolo HMQV entre dos partes Â, B̂ consiste en un intercambio básico de Diffie-Hellman de los valores DH de $X = g^x$ e $Y = g^y$ (figura 1) con la clave de la sesión calculada como $H(\pi)$, donde $\pi = DSIG_{\hat{A},\hat{B}}$ (m_1 = B̂, m_2 = Â, *X, Y)*. Esto es, π se calcula como la firma dual de Â y B̂ en la identidad mutua. La firma anterior se indica por la abreviatura π(Â, B̂, X, Y), es decir:

$$\pi(\hat{A}, \hat{B}, X, Y) \text{ B } DSIG_{\hat{A},\hat{B}} (m_1 = \hat{B}, m_2 = \hat{A}, X, Y) = g^{(x+da)(y+eb)}$$

donde d = $\overline{H}$(X,B̂), e = $\overline{H}$(Y,Â) y $A = g^a$, $B = g^y$ son las claves públicas de las partes Â, , respectivamente. Debe observarse en este punto que π(Â, B̂, X, Y) = π(B̂, Â, Y, X). En una variante, $H(\pi)$ puede ser sustituida por una función diferente de π, en particular el hashing puede incluir información adicional tal como las identidades de las partes, etc.

El protocolo HMQV se ejecuta típicamente en una red de múltiples partes, donde cualquiera de las partes puede ser invocada para ejecutar el protocolo. Cada invocación del protocolo en una parte crea una sesión (un estado local que contiene información relativa a este ejemplo específico del protocolo), que puede producir mensajes salientes y la salida de una clave de sesión al terminar. Durante una sesión, una parte puede ser activada con tres tipos de activaciones, como sigue (en la descripción siguiente, Â indica la identidad de la parte que se está activando y B̂ indica la identidad del homólogo al que se destina la sesión).

1. *Iniciar (*Â, B̂*):* Â genera un valor $X = g^x$, $x \in_R Z_q$ crea una sesión local del protocolo HMQV que identifica como la sesión (incompleta) *(*Â, B̂, *X)* y entrega el valor X como su mensaje saliente.

El significado de esta activación es que Â ha sido activado como el iniciador de una sesión con B̂, y X es el mensaje destinado a entregarse al homólogo B̂ como parte de esta sesión. La parte Â será llamada "titular" (o "propietario") de la sesión, B̂ el homólogo de la sesión, y X el valor saliente (DH).

2. *Responder (*Â, B̂, *Y):* Â comprueba que Y ≠ 0. Si es así, genera un valor $X = g^x$, $x \in_R Z_q$, entrega X y completa una sesión con el identificador *(*Â, B̂, *X, Y)* y la clave de la sesión $H(\pi((\hat{A}, \hat{B}, X, Y))$. En este caso, Â se está activando como el que contesta en la sesión con el homólogo B̂ y el valor entrante Y. En este caso, Â completa inmediatamente su sesión (no hay mensajes entrantes adicionales). Obsérvese que, si el valor entrante Y es cero, Â ignora la activación.

3. *Completar (*Â, B̂, *X, Y)*: Â comprueba que $Y \neq 0$ y que tiene una sesión abierta con el identificador *(*Â, B̂, *X)*. Si falla alguna de estas condiciones, Â ignora la activación; en otro caso, completa la sesión con el identificador *(*Â, B̂, *X, Y)* y la clave de la sesión K = $H(\pi((\hat{A}, \hat{B}, X, Y))$. Esto representa la entrega del segundo mensaje en el protocolo con el valor entrante Y, que es la respuesta (alegada) desde el homólogo B̂.

El protocolo HMQV-C de tres mensajes

El protocolo HMQV-C de tres mensajes (donde C quiere decir "Confirmación de clave"), está representado en la figura 8. El protocolo disfruta de todas las propiedades de seguridad de HMQV y esencialmente el mismo coste de cálculo. Sin embargo, añade un tercer mensaje al protocolo y un ligero aumento de la longitud de los mensajes del protocolo.

A cambio, el HMQV-C proporciona algunas propiedades que faltan en el protocolo HMQV básico, incluyendo la confirmación de claves, PFS, y la capacidad de composición universal.

Confirmación de clave

El protocolo HMQV proporciona una convicción fundamental a una parte Â que completa una sesión con el homólogo B̂ y una clave de sesión *K*: si B̂ no es malicioso, entonces solamente sería posible que B̂ conociera *K*. Lo que el protocolo no proporciona es ninguna convicción a Â de que B̂ haya completado la sesión o haya calculado la clave de la sesión. Más aún, B̂ podría no haber estado "vivo" durante la ejecución de la sesión.

Esto no es un inconveniente solamente para HMQV, ya que será cierto para cualquier protocolo basado en clave pública de dos mensajes (suponiendo, como en el escenario típico de claves públicas, que no se había creado un estado compartido anterior, en una comunicación previa entre Â y B̂). Además, como ha indicado Shoup, el objetivo aparentemente natural de que ambas partes tengan la convicción de que su homólogo completó la sesión antes de que cada uno empiece a utilizar la clave, no puede conseguirse por ningún protocolo de intercambio de claves. En realidad, un atacante siempre puede impedir esta convicción mutua deteniendo el último mensaje del protocolo para que no alcance su destino.

Aún así, se consigue la convicción más débil para cada una de las partes de que el homólogo fue capaz de calcular la clave (aunque no necesariamente que entrega la clave a la aplicación invocadora) y es denominada en la literatura como la propiedad de confirmación de la clave. Aunque no es crucial para la seguridad básica de un intercambio de claves (por ejemplo, la falta de confirmación de la clave no es una amenaza para la privacidad o autenticidad de las comunicaciones protegidas con la clave), esta propiedad puede proporcionar una "comprobación de salud operativa" para algunas aplicaciones.

En este caso, el protocolo HMQV-C es más adecuado que el HMQV, ya que los valores añadidos de MAC proporcionan la confirmación de la clave. Más aún, la validación de los MAC confirma que la implicación activa del homólogo identificado para la sesión, así como el hecho de que este homólogo posee una sesión de adaptación (es decir, con los mismos homólogos, y la misma clave de la sesión). Obsérvese que con el fin de conseguir estas propiedades, los MAC en HMQV-C no necesitan ser aplicados a ninguna información específica de la sesión, sino simplemente a un solo bit utilizado para indicar la "dirección" del mensaje y para impedir la reflexión. También merece observarse que el protocolo consistente en solamente los dos primeros mensajes en HMQV-C ya proporciona la confirmación de la clave al iniciador (que puede añadir una característica útil al HMQV sin aumentar el número de mensajes del protocolo).

En muchas aplicaciones del intercambio de claves, la falta de confirmación de la clave puede conducir a una forma de ataque de "negación del servicio" (DoS), en el cual una parte Â comienza utilizando la clave, por ejemplo para enviar una información protegida a B̂, mientras que B̂ no es capaz de procesar esta información, ya que no ha establecido todavía la clave. Como se ha dicho, esta situación no puede ser evitada por completo, ya que no se puede conseguir la confirmación mutua de "culminación de la sesión".

Además, hay formas más serias de ataques DoS contra protocolos basados en operaciones con claves públicas, en las cuales una parte está forzada a gastar ciclos de cálculo significativos (y a crear el estado de la sesión) antes de descubrir la invalidez del homólogo. Existen algunas contra-medidas útiles pero de alcance limitado para los ataques DoS, que pueden ser aplicadas a cualquier protocolo de intercambio de claves (incluyendo el HMQV) a costa de mensajes de protocolo añadidos.

Secreto perfecto de reenvío (PFS)

El secreto perfecto de reenvío es una propiedad muy deseada de los protocolos de intercambio de claves, por medio de los cuales el compromiso de claves privadas de largo plazo no pone en peligro la seguridad de las claves de sesiones antiguas. De una manera más formal, si una parte no maliciosa Â establece una sesión con intercambio de claves con un homólogo B̂ no contaminado, la clave *K* de la sesión permanece segura incluso si el atacante contamina a Â después de haber expirado *K* en Â, o contamina a B̂ después de haber expirado K en B̂. Ningún protocolo de dos mensajes con autenticación implícita, incluyendo HMQV, puede proporcionar un secreto perfecto de reenvío contra atacantes activos. En lugar de eso, lo mejor que puede esperarse es la débil forma de PFS proporcionada por HMQV. La ventaja principal de HMQV, con respecto al HMQV básico de dos mensajes, es que eleva esta limitación inherente de HMQV y proporciona un PFS completo, como se explica con más detalle en la Solicitud provisional.

Seguridad de Composición Universal

El modelo de Canetti/Krawczyk para el intercambio de claves, que es la base para el análisis del MQV y del HMQV en la Solicitud provisional, ha sido ampliado a un modelo más ambicioso con el objetivo de asegurar la seguridad de los protocolos de intercambio de claves, cuando se ejecutan concurrentemente con otras aplicaciones, como es el caso de los entornos del mundo real. Este modelo es conocido como el modelo de Composición Universal (UC) del intercambio de claves.

Se puede demostrar que, para el HMQV-C, cuando la primera parte entrega su clave de sesión para completar una sesión, el estado del homólogo solamente contiene información que puede ser "simulada" a partir de la información pública en el protocolo y en la clave de la sesión. Canetti-Krawczyk demostraron que esta propiedad, junto con las demás propiedades de seguridad de HMQV ilustradas en la Solicitud provisional, es suficiente para garantizar la capacidad de composición universal del protocolo HMQV.

HMQV de un pase

Un protocolo de intercambio de claves de un pase, ilustrado en la figura 9, consiste en un simple mensaje enviado desde un emisor Â a un receptor B̂, a partir del cual ambas partes, utilizando sus claves privadas y públicas, obtienen una clave exclusiva que solamente es posible que conozcan Â y B̂, siempre que ambas partes y la sesión no estén contaminadas como se define a continuación.

Los requisitos de la clave establecida son los mismos que en el protocolo de intercambio de claves normal, excepto por la posibilidad de que el mensaje recibido por B̂ sea una repetición de un mensaje más antiguo desde Â. Esta repetición es inevitable en un protocolo de un pase, aunque puede ser detectable por otros medios, tales como tiempo sincronizado o estado compartido.

Además, tal protocolo no puede proporcionar PFS, ya que por falta de una entrada específica de la sesión desde B̂, la clave debe ser computable con solamente el conocimiento de la clave privada de B̂.

En un modo de realización de la presente invención, el protocolo HMQV de un pase entre las partes Â y B̂, con las claves públicas $A = g^a$, $B = g^b$, respectivamente, consiste en un solo valor de $X = g^x$ transmitido desde Â a B̂, donde $x \in_R Z_q$ es elegido por Â. La clave K de la sesión es calculada por Â como

(i) Indiquemos como (Â, B̂) un mensaje que incluye las dos identidades Â *y* B̂, y fijemos *d* como el resultado de $d = \overline{H}(X,(\hat{A},\hat{B}))$;

(ii) Calcular $\sigma_{\hat{A}} = XSIG_{\hat{A}}(X,(\hat{A}, \hat{B}),B) = B^{x+da}$;

(iii) Fijemos $K = H(\sigma\ \hat{A})$, donde H entrega un número de bits igual a la longitud de la clave requerida. La misma clave k se calcula por B̂, tras comprobar que $X \neq 0$, como $K = H((XA^d)^b)$. En una variante, $K = H(\sigma, \hat{A}, \hat{B})$.

En otras palabras, la clave en este modo de realización del HMQV de un pase se obtiene a partir de una firma XCR no interactiva, utilizando la clave pública de B̂ como la pregunta.

También ha de observarse que el protocolo de un pase puede ser utilizado como un esquema de cifrado seguro de texto cifrado elegido autenticado (CCA). Es decir, Â puede transmitir un mensaje *m* a B̂ cifrado (contra ataques de texto cifrado elegido), así como autenticado (por Â). En un modo de realización, Â enviaría una tripleta *(X,c,t),* donde $X=gx$, *c* es un texto cifrado obtenido como un cifrado seguro simétrico de solo texto elegido (CPA) del mensaje m bajo una clave K_1, y *t* un valor MAC calculado sobre *c* bajo la clave K_2. Las claves K_1, K_2 se obtienen a partir de una clave *K* calculada a partir de X, como en el protocolo HMQV de un pase.

Todo el coste de este procedimiento son dos exponenciaciones de Â (uno fuera de línea) y 1,5 para B̂. Esto es justamente 1/2 exponenciación más para B̂ en comparación con los esquemas de cifrado CCA alternativos, tales como el DHIES (Esquema de Cifrado Integrado de Diffie-Hellman), pero, a cambio de eso, proporciona una autenticación desde Â (con DHIES), esa autenticación devolvería una firma completa adicional desde Â). Este eficaz cifrado CCA autenticado es muy atractivo para aplicaciones de "almacenar y enviar", tales como la popular aplicación "Privacidad Bastante Buena" (PGP, y es significativamente más económica que el paradigma normal de firmar y cifrar. La única advertencia en este caso es que la identidad Â (y posiblemente su certificado) necesita ser transmitida fuera de sospechas, ya que es necesaria para la operación de descifrado.

Una propiedad más del protocolo anterior que merece observarse, es que puede ser utilizado simplemente como una firma específica del verificador de Â en un mensaje *m*, sin añadir necesariamente la parte de cifrado. Sin embargo, esta firma es específica del receptor y, por tanto, no proporciona el no-rechazo. En lugar de eso, proporciona la capacidad de la negación, una característica muy valiosa en muchas aplicaciones, tales como PGP.

Debe observarse que muchos de los estándares que han adoptado el MQV, también han adoptado la variante del mismo de un pase. Para los estándares interesados en adoptar el HMQV en sus distintas formas (uno, dos y tres mensajes), podría tener sentido definir la obtención de la clave en un protocolo de un pase, de manera similar a la obtención en las demás variantes de HMQV.

Específicamente, al sustituir *Y* por *B* en las firmas duales que definen el protocolo HMQV, se obtienen los siguientes valores para la clave de un pase: Â y B̂, respectivamente, calculan $\sigma_{\hat{A}} = (BB^e)^{x+da}$ *y* $\sigma_{\hat{B}} = (XA^d)^{b+eb}$, y fijan la clave *K* en el algoritmo hash de estos valores (iguales). Obsérvese que, en este caso, el exponente *e* no añade ningún valor al protocolo, excepto para hacerlo compatible con las demás variantes. Realmente devalúa de alguna manera la eficiencia del protocolo.

Aún así, permanece una discrepancia adicional entre el valor de $d = \overline{H}(X,(\hat{A},\hat{B}))$ en la versión de un pase y $d = \overline{H}(X,\hat{B})$ en la versión de dos mensajes de HMQV. Una manera de proporcionar la compatibilidad entre los tres modos sería tener en todos ellos $d = \overline{H}(X,\hat{B})$, $e = d = H(Y,\hat{A})$ donde y=B en el caso de un pase, y añadir las identidades Â, B̂ a la función de obtención de la clave de la sesión: es decir, $K = H(\sigma, \hat{A}, \hat{B})$ (definiendo el orden de Â y B̂ utilizando algún criterio fijo). Esto sustituye la necesidad de añadir Â en el cálculo de *d*. También tiene la ventaja de reforzar HMQV

en el caso de escape de valores DH precalculados y evitando ataques potenciales desconocidos de compartición de claves.

Resumen de los Aspectos de Seguridad de HMQV

Comparado con el protocolo MQV convencional, el protocolo HMQV proporciona diversas ventajas de rendimiento, incluyendo las siguientes. HMQV dispensa probadamente la necesidad de pruebas costosas de orden principal en los valores DH transmitidos en el protocolo. Como se ha demostrado en la Solicitud provisional, la única manera de que un atacante se pueda beneficiar de la elección de valores maliciosos de DH es eligiendo que esos sean cero y, así, una simple comprobación de distintos de cero es todo lo que se requiere en HMQV. Por tanto, no hay necesidad de pruebas de orden principal o de un factor cooperante *h* utilizado actualmente en el protocolo MQV.

Lo que sigue es una lista de propiedades que consigue el protocolo HMQV de una manera que puede probarse matemáticamente:

(1) HMQV es seguro en el modelo de intercambio de claves fuertes formales de Canetti y Krawczyk;

(2) HMQV resiste la suplantación de atacantes que no tienen acceso a las claves privadas de las partes;

(3) HMQV establece una unión exclusiva entre las claves y las identidades de las partes para el intercambio, aplicando una firma XCR a estas identidades, evitando así el UKS y otros ataques de autenticación;

(4) HMQV es seguro también en presencia de un compromiso parcial de las claves de la sesión y otra información de la sesión; en otras palabras, HMQV es resistente a los denominados ataques de "clave conocida". En particular, se garantiza que distintas claves de sesiones sean "de cálculo independiente" entre sí.

(5) El protocolo proporciona un nivel de protección adicional, conocido como resistencia a los ataques de "suplantación del compromiso de claves (KCI)", es decir, impide que un atacante que aprende la clave privada de una parte A sea capaz de suplantar a otras partes frente a A;

(6) El protocolo HMQV de 3 mensajes con confirmación de claves proporciona un secreto de reenvío perfecto (PFS) que puede ser probado, es decir, aún cuando se divulguen eventualmente las claves privadas de largo plazo de las dos partes, las claves de la sesión creadas por esas partes antes del compromiso permanecen seguras;

(7) El protocolo de tres mensajes con confirmación de claves disfruta de la ventaja de seguridad adicional de los denominados protocolo de intercambio de claves "que pueden componerse universalmente", es decir, puede ser compuestos con seguridad con otros protocolos;

(8) La seguridad de HMQV no depende de pruebas especiales en la forma y estructura de las claves públicas estáticas, ni requiere la denominada "posesión de la prueba", de las correspondientes claves privadas. Estas ventajas del HMQV sobre protocolos similares, incluyendo el MQV, liberan a las autoridades de certificación (CA) de la carga de realizar estas comprobaciones especiales sobre claves públicas registradas, proporcionando así una convicción de seguridad más realista y práctica, en particular, ya que muchas CA locales no son capaces o no están configuradas para hacer estas comprobaciones. Más aún, merece observarse que la propia ejecución de tales pruebas (por ejemplo, pruebas de posesión) por el CA, abre los protocolos a vulnerabilidades de seguridad adicionales;

(9) Los protocolos HMQV de dos mensajes y de tres mensajes no necesitan comprobar el orden de las claves publicas efímeras (es decir, los valores X e Y), evitando así una prueba que podría ser costosa en algunos casos. Sin embargo, estas pruebas son necesarias si la seguridad del protocolo es resistir los atacantes que puedan aprender las claves secretas efímeras de las partes. Esta prueba es necesaria también para la seguridad del protocolo HMQV de un pase.

Igual que con el MQV, estas pruebas pueden ser sustituidas por la "exponenciación de factores cooperantes" de los valores σ en el protocolo. Se pueden requerir pruebas adicionales en elementos del grupo, tales como la pertenencia a un grupo predeterminado, dependiendo de los grupos algebraicos subyacentes.

Una ventaja significativa del protocolo HMQV de la presente invención es que es argumentadamente el protocolo de intercambio de claves de Diffie-Hellman autenticado de la manera más eficiente en existencia, con una amplia gama de propiedades de seguridad que puede probarse que se mantienen de una manera matemática formal. En realidad, esta capacidad de prueba formal es una distinción principal entre el HMQV y su predecesor MQV.

El MQV, no solamente falla en cuanto que no tiene una prueba d seguridad, sino que han surgido con el tiempo debilidades explícitas del protocolo (por ejemplo, el trabajo de Kaliski y el informe de Rogaway y otros colaboradores), incluyendo algunas debilidades que fueron descritas por primera vez en la solicitud provisional antes mencionada. Estas debilidades, o ataques, han invalidado algunas de las reivindicaciones de seguridad del MQV hechas por sus inventores y, en particular, demuestran que no puede probarse que MQV sea seguro.

Comparación de las firmas XCR con las "Firmas Implícitas" de MQV

A modo de comparación, merece observarse que el MQV, como se describe en las patentes y documentos académicos, utiliza también una noción de firmas en el diseño y descripción del protocolo. Éstas son denominadas "firmas implícitas" en el contexto de MQV y siguen la noción más convencional de las firmas digitales, en las cuales el valor de la firma solamente puede ser producido por el propietario de la clave privada de la firma (específicamente, MQV se refiere a las firmas similares a ElGamal, formadas por combinaciones lineales de la clave de firma privada, y las claves efímeras secretas y públicas). Sin embargo, el protocolo deja pronto de utilizar totalmente las propiedades de estas firmas. En particular, el protocolo MQV no utiliza las firmas como una forma de autenticar explícitamente las identidades de las partes del protocolo, lo cual conduce a fallos severos de autenticación tales como los famosos ataques para "compartir claves desconocidas (UKS)", descubiertos por Kaliski.

Como contraste, el HMQV introduce dos importantes elementos en su diseño. Uno es el uso de XCR, que es una versión exponencial de las firmas de ElGamal. Más específicamente, es una versión exponencial de las firmas de Schnorr, las cuales, a su vez, son ejemplos particulares de las firmas de ElGamal. El otro es la firma explícita de la identidad del homólogo, que asegura una unión segura de una clave de la sesión a los homólogos de la sesión y, en particular, impide los fallos de autenticación tales como el UKS.

Una novedad clave de las firmas XCR es la propiedad de que tanto el firmante como el verificador (o el que pregunta) pueden calcular la misma firma. Esta propiedad se encuentra normalmente en mecanismos de autenticación basados en criptografía de claves compartidas (es decir, en casos en los que tanto el firmante como el verificador tienen una clave compartida *a priori*) pero es nueva en las firmas basadas en claves públicas. Las firmas XCR no solamente son perfectamente adecuadas para la obtención de claves compartidas, como en HMQV, sino que presentan una diversidad de ventajas como herramientas de autenticación, algunas de las cuales han sido descritas anteriormente.

Debe quedar claro para un experto normal en la técnica que la presente invención cubre una diversidad de modos de realización.

Así, en un ejemplo de modo de realización, hay dos partes, un verificador V y un firmante S. El firmante S tiene una clave privada b y un clave pública B, y el verificador V se supone que posee u obtiene (por ejemplo, a través de un certificado digital enviado desde S) la clave pública auténtica B de S. El protocolo de autenticación para un mensaje m dado incluye:

(1) V elige un valor secreto x y calcula un valor $X = F_1(x)$, donde F_1 es una función dada, y envía X a S.

(2) S elige un valor secreto y y calcula un valor $Y = F_2(y)$, donde F_2 es una función dada, y envía Y a V.

(3) S calcula un valor $s = F_3(y,b,X,m)$, donde F_3 es una función dada, y envía s a V.

(4) V calcula un valor $s' = F_4(x,Y,B,m)$, y decide sobre la autenticidad de m sobre la base del valor s' y su relación con el valor s recibido.

Algunos ejemplos de variantes de este modo de realización incluyen:

(a) F_1, F_2 son funciones unidireccionales. En XCR, estas funciones unidireccionales son $X = g^x$ e $Y = g^y$.

(b) En las firmas XCR, las funciones $s = F_3(y,b,X,m) = X^{y+\overline{H}(Y,m)b)}$ y $s' = F_4(x,Y,B,m) = (YB^{(\overline{H}(Y,m))})^x$.

(c) Aceptando m como una autenticación si, y solamente si, $s' = s$. Esta última variante hace uso de la propiedad de las firmas típicas de XCR, por medio de las cuales el verificador puede re-calcular la firma porque conoce el secreto que encierra la pregunta X.

(d) Calcular $s = F_3(y,b,X,m) = {}^{y+\overline{H}(Y,m)b)}$ y comprobar que H(s') = s, etc.

En al menos un modo de realización de la aplicación de XCR a HMQV, el valor s calculado por S en el paso (3) nunca es enviado a V. En lugar de eso, V calcula el valor s', el cual debe ser idéntico a s (excepto si S es un impostor), y utiliza s (que es σ en HMQV) para obtener una clave de sesión a partir de ella. En particular, V nunca lleva a cabo una verificación explícita. En este modo de realización, en lugar de ser un método para verificar la autenticidad de un mensaje m, sería un método por medio del cual ambas partes calculan un "valor autenticado" común (es decir, un valor que ambas partes, y solamente ellas, pueden calcular), y por medio del cual este valor está unívocamente unido a sus identidades (una condición esencial en los típicos protocolos de intercambio de claves conseguidos en HMQV por la firma, a través de las firmas XCR duales, de las identidades de las partes).

En el texto anterior y en las reivindicaciones se describen variaciones adicionales.

Ejemplo de implementación por hardware

La figura 10 ilustra una configuración típica de hardware de un sistema de gestión de información/informático, de acuerdo con la invención, y que preferiblemente tiene al menos un procesador o unidad central de proceso (CPU) 1011.

Las CPU 1011 están interconectadas a través de un bus 1012 del sistema, a una memoria de acceso aleatorio (RAM) 1014, una memoria de sólo lectura (ROM) 1016, un adaptador 1018 de entrada/salida (E/S) (para conectar dispositivos periféricos tales como unidades 1021 de disco y unidades 1040 de cinta, al bus 1012), un adaptador 1022 de interfaz de usuario (para conectar un teclado 1024, un ratón 1026, un altavoz 1028, un micrófono 1032 y/o otros dispositivos de interfaz de usuario al bus 1012), un adaptador 1034 de comunicaciones para conectar un sistema de gestión de información a una red de proceso de datos, a Internet, a una Intranet, a una red de área personal (PAN), etc., y un adaptador 1036 de pantalla para conectar el bus 1012 a un dispositivo 1038 de pantalla y/o una impresora 1039 (por ejemplo, una impresora digital o similar).

Además del entorno de hardware/software descrito anteriormente, un aspecto diferente de la invención incluye un método implementado por ordenador para realizar el método anterior. Como ejemplo, este método puede ser implementado en el entorno particular, como se ha estudiado anteriormente.

Tal método puede ser implementado, por ejemplo, manejando un ordenador, que esté materializado por un aparato digital de proceso de datos, para ejecutar una secuencia de instrucciones legibles por máquina. Estas instrucciones pueden residir en diversos tipos de medios de soporte de señales.

Por tanto, este aspecto de la presente invención está dirigido a un producto programado, que comprende medios de soporte de señales que incorporan tangiblemente un programa de instrucciones legibles por máquina ejecutables por un procesador digital de datos, que incorpora la CPU 1011 y el hardware anterior, para realizar el método de la invención.

Estos medios de soporte de señales pueden incluir, por ejemplo, una RAM contenida dentro de la CPU 1011, como se representa por el almacenamiento de acceso rápido, por ejemplo. Alternativamente, las instrucciones pueden estar contenidas en otros medios de soporte de señales, tal como un disquete 1100 de almacenamiento magnético de datos (figura 11), directa o indirectamente accesibles por la CPU 1011.

Estén o no contenidas en el disquete 1100, en el ordenador/CPU 1011, o en cualquier otro sitio, las instrucciones pueden estar almacenadas en una diversidad de medios de almacenamiento de datos legibles por máquina, tal como un almacenamiento DASD (por ejemplo, un “disco duro” convencional o una agrupación RAID), cinta magnética, memoria electrónica de sólo lectura (por ejemplo, ROM, EPROM o EEPROM), un dispositivo de almacenamiento óptico (por ejemplo, un CD-ROM, WORM, DVD, cinta digital óptica, etc.), tarjetas “perforadas” de papel, u otros medios adecuados de soporte de señales, incluyendo medios de transmisión, tales como enlaces de comunicaciones digitales y analógicas e inalámbricas. En un modo de realización ilustrativo de la invención, las instrucciones legibles por máquina pueden comprender código objeto de software.

REIVINDICACIONES

1. Un método de intercambio entre dos partes interconectadas por un dispositivo o red, comprendiendo dicho método:

una parte receptora, en adelante denominada verificador, que elige un valor secreto x para calcular un valor $X = F1(x)$, donde $F1$ comprende una primera función predeterminada que tiene al menos un argumento, siendo dicho valor x uno de al menos un argumento de $F1$;

una parte firmante, en adelante denominada firmante, elige un valor secreto y para calcular un valor $Y = F2(y)$, donde $F2$ comprende una segunda función predeterminada que tiene al menos un argumento, siendo dicho valor y uno de dicho al menos un argumento de $F2$;

obteniendo dicho firmante dicho valor X, teniendo dicho firmante una clave privada b y una clave pública B; y

calculando el firmante un valor $s = F3(y,b,X)$, donde F3 comprende una tercera función predeterminada que tiene al menos tres argumentos, siendo dicho valor y, dicha clave privada b y dicho valor X tres argumentos de dichos al menos tres argumentos de $F3$,

donde existe una cuarta función predeterminada $F4$ para calcular un valor $s' = F4(x,Y,B)$, teniendo $F4$ al menos tres argumentos, siendo dicho valor x, dicho valor Y, y dicha clave pública B tres argumentos de los al menos dichos tres argumentos de $F4$, pero dicho valor s no es un argumento de $F4$,

no existe ningún secreto compartido entre dicho verificador y dicho firmante que sirva como base para ningún argumento en ninguna de dichas F1, F2, F3 y F4, y

dicho verificador puede considerar dichos valores s y s' como autenticadores válidos si se determina que el valor s' está relacionado de una manera predeterminada con el valor s.

2. El método de la reivindicación 1, en el que:

dicha clave pública $B = g^b$, siendo g un generador de un grupo finito de orden q, siendo dicha clave privada b un número entero tal que $0 \leq b \leq q-1$;

dicho valor $X = g^x$, siendo x un entero tal que $0 \leq x \leq q-1$, y dicho valor $Y = g^y$, siendo y un entero tal que $0 \leq y \leq q-1$, y

dicho firmante calcula dicho valor $s = f_1{}^{f_2(m,Y,y,b)}$, f_1 comprende una primera función matemática y f_2 comprende una segunda función matemática, y el argumento m comprende un mensaje.

3. El método de la reivindicación 2, en el que q es primo.

4. El método de la reivindicación 2, en el que dicho mensaje m se estima que está autenticado si dicho valor s determina que está relacionado de dicha manera predeterminada con dicho valor s'.

5. Un medio (1100) de soporte de señales, que materializa tangiblemente un programa de instrucciones legibles por máquina, ejecutables por un aparato digital (1000) de proceso, para realizar los paso del método descrito en la reivindicación 1.

6. Un aparato (1000) que comprende:

un calculador adaptado para calcular las funciones F2 y F3 para el firmante, con el fin de llevar a cabo el método de la reivindicación 1.

7. Un método para establecer una clave autenticada entre dos partes interconectadas por un dispositivo o una red, comprendiendo dicho método:

dada una primera parte que tiene una clave privada a y una clave pública A, siendo la clave privada a un número entero tal que $0 \leq a \leq q-1$, siendo q un entero positivo, siendo g un generador de un grupo finito de orden q, y siendo A un elemento del grupo generado por dicho valor g y calculado como $A = g^a$ y

dada una segunda parte que tiene una clave privada b y una clave pública $B = g^b$, siendo dicha clave privada b un número entero tal que $0 \leq b \leq q-1$,

eligiendo dicha primera parte un valor secreto *x* para calcular un valor $X = g^x$, siendo x un entero tal que $0 \leq x \leq q-1$, y siendo comunicado dicho valor X a dicha segunda parte,

eligiendo dicha segunda parte un valor secreto *y* para calcular un valor $Y = g^y$, siendo *y* un entero tal que $0 \leq y \leq q-1$, y siendo comunicado dicho valor *Y* a dicha primera parte;

calculando dicha primera parte un valor $s = f_1(Y,B,m)^{f_2(x,a,m')}$ donde *m, m'* comprenden mensajes conocidos, o intercambiados entre las partes, y la segunda parte calcula un valor $s' = f_3(X,A,m')^{f_4(y,b,m)}$;

incluyendo al menos una de las funciones f_2 y f_4 una función H con al menos un argumento, siendo uno de tales argumentos al menos uno de los mensajes m y m', donde H comprende una función criptográfica que es una entre una función unidireccional, una función de cifrado, y una función criptográfica de un algoritmo "hash";

obteniendo dicha primera y segunda partes una clave compartida a partir de los valores s y s', respectivamente.

8. El método de la reivindicación 7, en el que al menos uno de los siguientes:

(i) el cálculo de dichos valores x y X incluye la clave privada de dicha primera parte y las claves públicas de una o más de dichas partes; y

(ii) el cálculo de dichos valores y e Y incluye la clave privada de dicha segunda parte y las claves públicas de una o más de dichas partes.

9. El método de la reivindicación 7, en el que dicha obtención de una clave compartida a partir de s y s' comprende una función criptográfica que es una entre una función unidireccional, una función de cifrado y una función criptográfica con "hash".

10. El método de la reivindicación 7, en el que:

$f_1(Y,B,m) = YB^{H(Y,m)}$,

$f_2(x,a,m') = (x+H(X,m')a) \bmod q$,

$f_3(X,A,m') = XA^{H(X,m')}$,

$f_4(y,b,m) = (y+H(Y,m)b) \bmod q$, y

H es una función de al menos dos argumentos que comprenden una función criptográfica que es una función unidireccional, una función de cifrado y una función "hash" criptográfica.

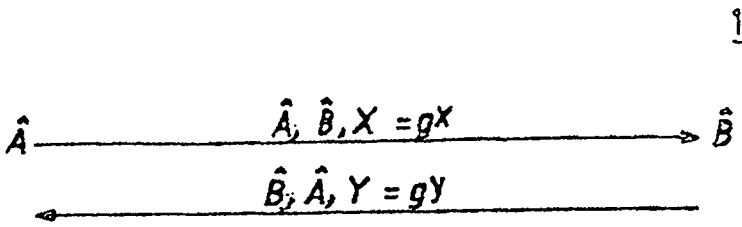

FIG. 1

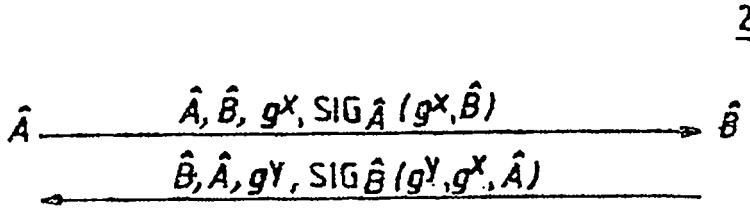

FIG. 2

300

Entradas : $\hat{A}$: Clave privada a, clave pública $A = g^a$, B clave pública de $\hat{B}$

$\hat{B}$: Clave privada b, clave pública $B = g^b$, A clave pública de $\hat{A}$

Ambos protocolos : $\hat{A}$ y $\hat{B}$ ejecutan un intercambio básico de Diffie-Hellman — 301

$\hat{A}$ calcula $\sigma_{\hat{A}} = (Y B^e)^{x + da}$, $\hat{B}$ calcula $\sigma_{\hat{B}} = (X A^d)^{y + eb}$

MQV: $d = \bar{X} \stackrel{def}{=} 2^l + (X \bmod 2^l)$ $e = \bar{Y} \stackrel{def}{=} 2^l + (Y \bmod 2^l)$ $l = |q|/2$ — 302

$K = \sigma_{\hat{A}} = \sigma_{\hat{B}}$

HMQV: $d = \bar{H}(X, \hat{B})$, $e = \bar{H}(Y, \hat{A})$ — 303

$K = H(\sigma_{\hat{A}}) = H(\sigma_{\hat{B}})$

FIG. 3

400

Entradas : $\hat{A}$: Clave privada a, clave pública $A = g^a$, B clave pública de $\hat{A}$

$\hat{B}$: Clave privada b, clave pública $B = g^b$, A clave pública de $\hat{B}$

$\hat{A}$ ——— $\hat{A}, \hat{B}, X = g^x$ ———→ $\hat{B}$

$\hat{B}, \hat{A}, Y = g^y$ ←———

$\sigma_{\hat{A}} = (Y B^{\bar{H}(Y,\hat{A})})^x + \bar{H}(X,\hat{B})a$ $\sigma_{\hat{B}} = (X A^{\bar{H}(X,\hat{B})})^y + \bar{H}(Y,\hat{A})b$

$K = H(\sigma_{\hat{A}})$ $K = H(\sigma_{\hat{B}})$

FIG. 4

500

Entradas Firmante $\hat{B}$: Clave privada b, clave pública $B = g^b$, mensaje m

Verificador $\hat{A}$: A clave pública de $\hat{B}$, mensaje m

Protocolo de firma

$\hat{A}$ $\hat{B}$

$x \in_R Z_q$ $X = g^x$ →

$Y = g^y, \sigma = X^y + \bar{H}(Y,m)^b$ ← $y \in_R Z_q$

Verifica:

$\sigma = (Y B^{\bar{H}(Y,m)})^x$

e $Y \neq 0$

FIG. 5

600

Entradas : Firmante $\hat{B}$: Clave privada b, clave pública $B=g^b$, A clave pública de $\hat{A}$, mensaje m

Verificador $\hat{A}$: Clave privada a, clave pública $A=g^a$, B clave pública de $\hat{B}$, mensaje m

Protocolo de firma

$\hat{A}$ $\qquad$ $\hat{B}$

$y \in_R Z_q$

$Y=g^y,\ \sigma = A^y \cdot \bar{H}(Y,m)^b$ ←

Verifica

$\sigma = (YB^{\bar{H}(Y,m)})^a$

FIG. 6

700

Inputs: $\hat{A}$ Clave privada a, clave pública $A=g^a$, B clave pública de $\hat{B}$, mensajes m_1, m_2

$\hat{B}$ Clave privada b, clave pública $B=g^b$, A clave pública de $\hat{A}$, mensajes m_1, m_2

Protocolo de firma

$\hat{A}$ $\qquad$ $\hat{B}$

$x \in_R Z_q$ $\qquad$ $X=g^x$ →

$y \in_R Z_q$

$Y=g^y$ ←

$\sigma = (YB^{\bar{H}(Y,m_2)})^x \cdot \bar{H}(X,m_1)^a$ $\qquad$ $\sigma = (XA^{\bar{H}(X,m_1)})^y \cdot \bar{H}(Y,m_2)^b$

FIG. 7

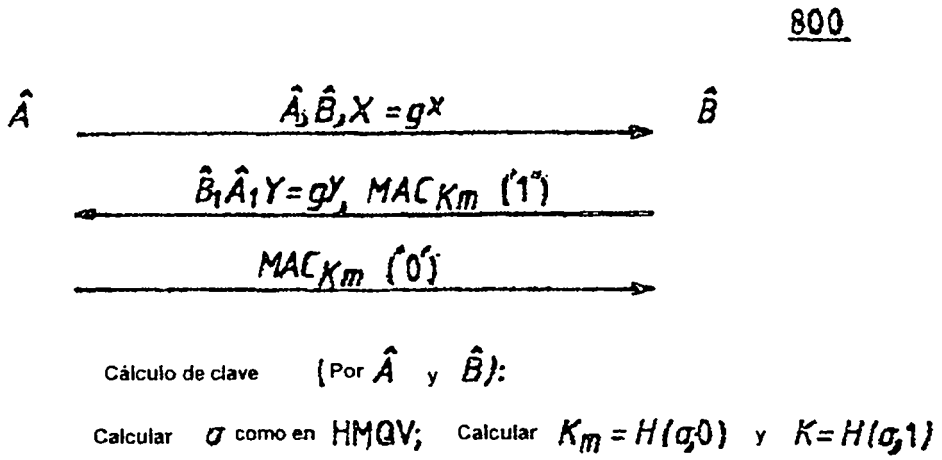
800
$\hat{A}$
$\hat{A}, \hat{B}, X = g^x$
$\hat{B}$
$\hat{B}, \hat{A}, Y = g^y$, MAC_{Km} ("1")
MAC_{Km} ("0")
Cálculo de clave (Por $\hat{A}$ y $\hat{B}$):
Calcular σ como en HMQV; Calcular $K_m = H(\sigma, 0)$ y $K = H(\sigma, 1)$

FIG. 8

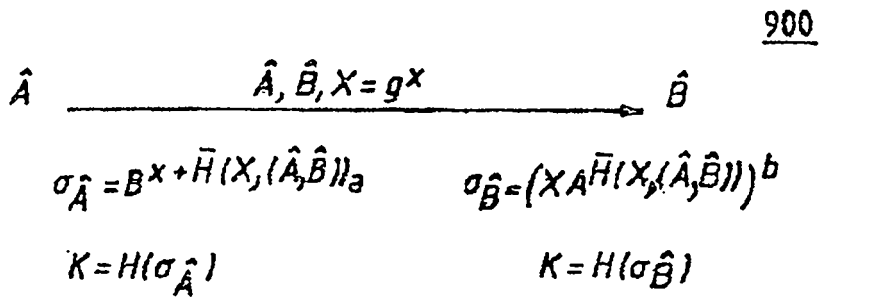
900
$\hat{A}$
$\hat{A}, \hat{B}, X = g^x$
$\hat{B}$
$\sigma_{\hat{A}} = B^{x + \bar{H}(X, (\hat{A}, \hat{B}))a}$
$\sigma_{\hat{B}} = (XA^{\bar{H}(X, (\hat{A}, \hat{B}))})^b$
$K = H(\sigma_{\hat{A}})$
$K = H(\sigma_{\hat{B}})$

FIG. 9

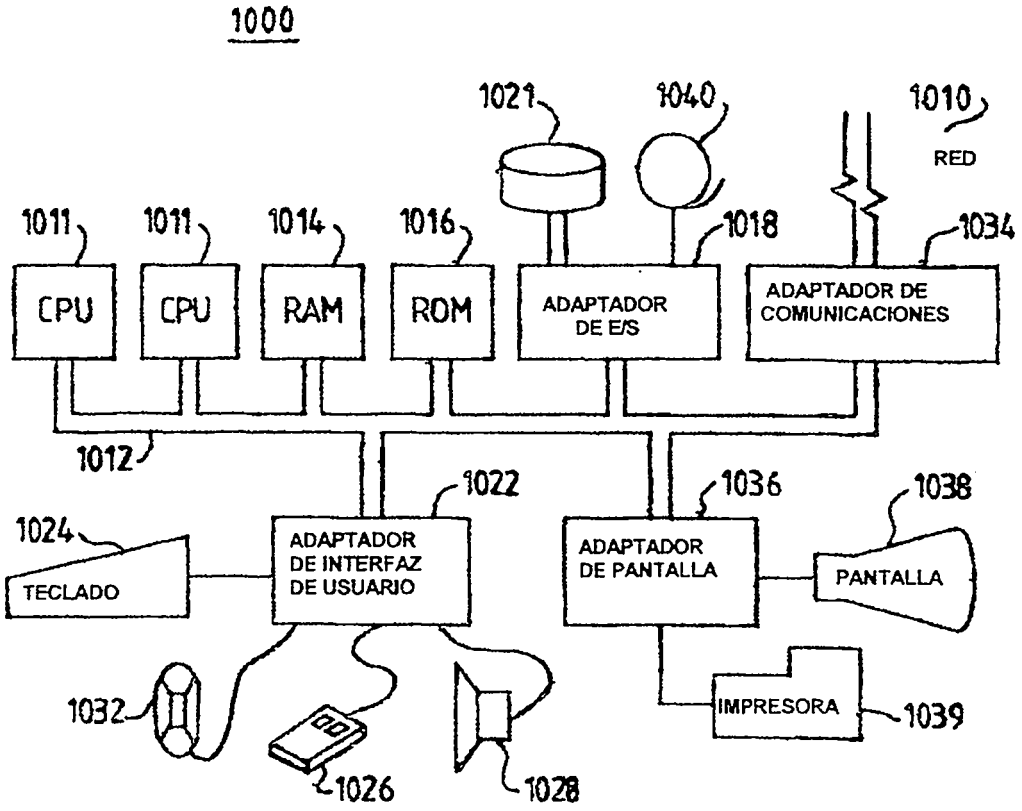
1000
1021
1040
1010
RED
1011
1011
1014
1016
1018
1034
CPU
CPU
RAM
ROM
ADAPTADOR DE E/S
ADAPTADOR DE COMUNICACIONES
1012
1022
1036
1038
1024
TECLADO
ADAPTADOR DE INTERFAZ DE USUARIO
ADAPTADOR DE PANTALLA
PANTALLA
IMPRESORA
1039
1032
1026
1028

FIG. 10

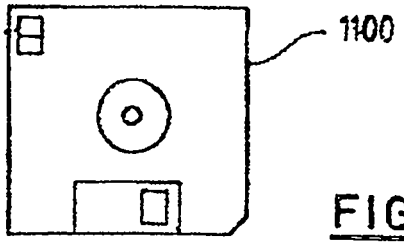
1100

FIG. 11