Análisis en torno a los esquemas de compromiso digital y su aplicación en seguridad de red

Por Javier y Ana Areitio Bertolín

Prof. Dr. Javier Areitio Bertolín
jareitio@eside.deusto.es
Catedrático de la Facultad de Ingeniería. ESIDE.
Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.
Prof. Dra. Ana Areitio Bertolín
ana.areitio@ehu.es
Laboratorio de Informática Aplicada. Universidad del País Vasco (UPV / EHU)

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto LEFIS-APTICE (financiado por Socrates 2005-2007. European Commission).

En el presente artículo se analiza la tecnología de los esquemas de compromiso que pueden considerarse como primitivas criptográficas y constituyen el núcleo de construcción de protocolos de mayores dimensiones. Pueden emplearse para un número creciente de aplicaciones, por ejemplo, en comercio electrónico, en autenticación basada en contraseñas, en compras utilizando Web, para la difusión anónima de mensajes, para la votación electrónica, para las transacciones con dinero digital, para la síntesis de nuevas primitivas de protocolo, para la firma electrónica de contratos on-line/off-line, para la firma digital a ciegas y/o tipo camaleón, en casinos virtuales, para correos electrónicos certificados, en aplicaciones de conocimiento cero, en computación multi-parte, para procesos de concatenación en paralelo de firma digital y cifrado (para conseguir cifrado autenticado), en pujas y subastas, para poker mental (esquema de compromiso para jugar al poker sin intercambiar físicamente las cartas), en lanzamiento de monedas a través de Internet, en MCF (Mental Coin Flipping) (esquema de compromiso que permite tomar una decisión binaria), en CFOtTP (Coin Flipping Over the Telephone Problem), para juegos on-line y en el desarrollo de otras muchas aplicaciones de seguridad y privacidad para comunicaciones de red.

Un esquema de compromiso (o commitment scheme) es un método que permite enviar información secreta de modo que no pueda alterarse en una etapa posterior ni por el emisor ni por el receptor. En general los esquemas de compromiso constan de una fase de compromiso y una fase de apertura. La idea es que en la fase de compromiso una entidad A se compromete con una entidad destino B sobre un valor que no puede cambiar posteriormente, mientras aún mantenga el valor oculto. En la fase de apertura el valor se lo muestra a otra entidad B. Los esquemas de compromiso deben ser vinculantes de modo que la entidad A no puede cambiar el valor después de la fase de compromiso y deben ser ocultos, es decir una entidad destino B no puede averiguar el valor antes de la fase de apertura.

El esquema de compromiso más básico en criptografía es el BC (Bit Commitment) donde las entidades A y B desean alcanzar una decisión binaria utilizando un único bit. Es comparable a tratar de lanzar una moneda sin encontrarse de hecho físicamente y ver evolucionar la moneda. El BC permite establecer el valor de un único bit. Una generalización de los esquemas BC son los esquemas SC (String Commitment) en los que el valor o compromiso secreto es una cadena de N bits.

Un esquema de compromiso puede considerarse como la analogía digital de enviar mensajes secretos dentro de una caja cerrada; una vez que llega la caja al receptor, el emisor no puede cambiar su contenido y el contenido está oculto al receptor hasta que en una fase posterior (fase de revelación) el emisor revela el mensaje enviando la llave o clave para abrir la caja. En los esquemas de compromiso estadísticamente ocultos, el emisor no es factible desde el punto de vista computacional que pueda cambiar el mensaje, así mismo, el receptor es imposible estadísticamente que pueda saber nada acerca del mensaje hasta la fase de revelación. Es decir, permite probar cualquier declaración NP con conocimiento cero estadístico, de modo que un probador puede convencer a un verificador de la validez de la declaración de tal forma que no es factible desde el punto de vista computacional convencer al verificador de una declaración falsa y es imposible estadísticamente para el verificador aprender ningún conocimiento adicional acerca del contenido de la citada declaración a parte de su validez.

- **Resolución del problema *CFOtTP* (*Coin Flipping Over the Telephone Problem*) utilizando un esquema *BC* (*Bit Commitment*) simple basado en criptografía de clave pública.**
- **En los esquemas *BC* genéricos la entidad A realiza un compromiso con otra entidad B acerca de un cierto valor secreto que posteriormente lo revela.**

FASES DEL PROTOCOLO BC

- Las entidades A y B se encuentran separadas físicamente, no se ven, desconfían mutuamente y sin embargo deben lanzar una moneda al aire para poder acordar y decidir quién gana cierto activo, fruto del resultado del azar.
- Las entidades A y B acuerdan que si el resultado es 1, entonces A gana la apuesta, si es 0 entonces gana B.
- La entidad A establece un esquema de cifrado de clave pública. Genera un par de claves pública-privada (e, d) y publica la clave pública e. Selecciona de forma aleatoria un bit b_A y se compromete con B. Para ello envía a B cifrado con su clave pública e, es decir envía a B: $E_e(b_A)$.
- La entidad B genera de forma aleatoria un bit b_B y se lo envía a la entidad A.
- La entidad A revela su clave privada d a la entidad B y las entidades A y B proceden a calcular el resultado de la operación: $b = (b_A + b_B) \bmod 2$.

Figura 1. Resolución del problema CFOtTP, utilizando un esquema BC. Bit Commitment

Figura 2. Resolución del problema CFOtTP utilizando un esquema de transferencia trascordada estilo Rabin

Métodos de síntesis de esquemas de compromiso

Existen diversas formas de garantizar criptográficamente, es decir de forma robusta, un compromiso. Esto significa que pueden construirse esquemas de compromiso utilizando:

(1) Funciones criptográficas unidireccionales o hash (sin puerta trasera).

Si una entidad A desea comprometerse con una cierta información con otra entidad remota B puede utilizar una función hash para calcular el valor hash de la información y enviarla a la otra entidad B. Una vez que la información se libera, la entidad B puede calcular el valor hash y verificar el compromiso de la entidad A. La entidad A no puede alterar su compromiso sin alterar el valor hash.

(2) Cifradores asimétricos o de clave pública.

Se supone que una entidad A desea comprometerse con una entidad B sobre una cierta información. La entidad A puede generar un par de claves criptográficas pública/privada y cifrar la información objeto del compromiso con la clave privada y sólo publicar la clave pública una vez que la información necesita ser verificada por la entidad B. Pueden basarse en el problema del logaritmo discreto (criptosistemas ElGamal, ECC, etc.), en la dificultad de la factorización de números enteros (criptosistemas estilo RSA), en esquemas Rabin que tienen en cuenta las propiedades de los residuos cuadráticos, etc.

(3) Generadores criptográficos de números pseudoaleatorios.

Sea F un generador de números pseudoaleatorios cuya entrada son n bits y la salida son 3n bits. Supongamos que la entidad A desea comprometer un bit b frente a la entidad B. El proceso es el siguiente:

(i) La entidad B selecciona un valor aleatorio r de 3n bits y se lo envía a la entidad A.

(ii) La entidad A selecciona un valor aleatorio z de n bits y le aplica F para calcular un valor de 3n bits, es decir calcula F(z).

- **Resolución del problema *CFOtTP* (*Coin Flipping Over the Telephone Problem*) utilizando un esquema no obvio de transferencia trascordada de Rabin.**
- **Este esquema está basado en las propiedades de los residuos cuadráticos.**
- **La entidad A sabe resolver la ecuación: $t^2 = a \bmod n$, en cambio la entidad B no, debido a que A conoce como factorizar n**

FASES DEL PROTOCOLO

- Las entidades A y B se encuentran separadas físicamente, desconfían mutuamente y sin embargo deben lanzar una moneda al aire para poder acordar y decidir quién gana cierto objeto, fruto del resultado del azar.
- La entidad A genera dos números primos p y q y publica su producto n = p . q. Por ejemplo: p = 31, q = 23 → n = 713.
- La entidad B genera un número aleatorio x tal que $0 < x < n$ y el máximo común divisor *mcd* (x, n) = 1. Calcula $a = x^2 \bmod n$ y se lo envía a A. Por ejemplo: si x = 220 → $a = 220^2 \bmod 713 = 629$.
- La entidad A resuelve la ecuación congruencial: $t^2 = a \bmod n$ y encuentra dos pares distintas de soluciones: {x, - x} y {y, - y}. La entidad A elige un par y se lo envía a B. En el ejemplo numérico considerado, los resultados obtenidos son: {220, 493} y {654, 59}; la entidad A elige uno de los dos pares.
- Si A elige {x, -x} habrá ganado, en caso contrario B gana y para probarlo revela el valor x. En el ejemplo numérico considerado si A elige {220, 493} gana, si elige {654, 59} la entidad B gana. Todo lo que tiene que hacer B es revelar el valor 220 a la entidad A.

Figura 3. Comparativa entre los esquemas-protocolos BC y los protocolos de transferencia trascordada (OT y 1-2OT)

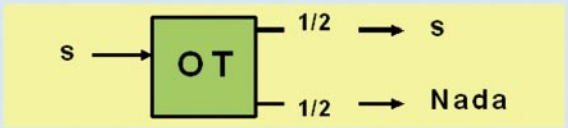
Esquemas *BC* (*Bit Commitment*).

- Dados dos entidades A emisor y B receptor.
- La entidad A escribe el valor de un bit b en un papel y lo mete en una caja cerrada con candado. Le da la caja cerrada a una entidad B.
- Si la entidad A desea, puede revelar su compromiso abriendo la caja delante de la entidad B. Evidentemente desde que A da a B la caja, el compromiso o contenido no lo puede variar A y B lo ignora.

Transferencia trascordada (*OT: Oblivious Transfer*) → Dos tipos: OT y 1-2 OT

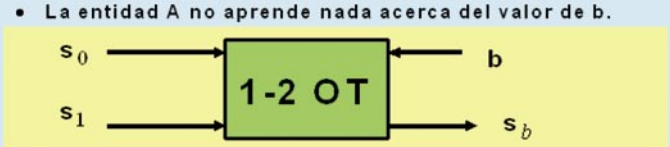
Dadas dos entidades A y B. La entidad A tiene un secreto s. Al final del protocolo de transferencia trascordada uno de los dos siguientes eventos ocurren, cada uno con una probabilidad 1/2 :

- La entidad B conoce el secreto s.
- La entidad B no obtiene información adicional alguna acerca del secreto s.



Dadas dos entidades A y B. La entidad A tiene dos secretos s_0 y s_1. La entidad B tiene un bit de selección b. Al final del protocolo de transferencia trascordada 1-2 OT, se cumplen las tres siguientes condiciones:

- La entidad B conoce el secreto s_b.
- La entidad B no obtiene información adicional alguna acerca del secreto s_{1-b}.
- La entidad A no aprende nada acerca del valor de b.



(iii) Si b = 1 la entidad A envía F(z) a B, en caso contrario envía a la entidad B el valor: (r + F(z)) mod 2.

(iv) Para la fase de revelación la entidad A envía a B el valor z, de modo que B pueda comprobar que recibió F(z) o (r + F(z)) mod 2. En este esquema, A no puede hacer trampas con probabilidad mayor de dos elevado a la menos n.

(4) Cifradores simétricos o de secreto compartido.

Estos pueden ser de bloque como AES, 3DES, IDEA o de flujo con características de mayor rapidez, por ejemplo para redes de banda ancha que operan incluso a decenas de Gbps.

Un commitment (o compromiso) es similar a una nota colocada dentro de una caja fuerte. En la etapa de compromiso una entidad A escribe una nota, la coloca dentro de una caja fuerte y envía la caja fuerte cerrada a una entidad destinataria B. Existe una etapa posterior de revelación en la que la entidad A proporciona a la entidad B la combinación de dicha caja fuerte. Ejemplos de mecanismos físicos de compromiso son las cajas fuertes con combinación. Posibles mecanismos criptográficos para sintetizar esquemas de compromiso pueden estar basados en el problema del logaritmo discreto:

(i) Esquema de compromiso de Pedersen.

En este caso dado el compromiso:

$$com\ (r, b) = (g^r h^b)$$

se trata de revelar (b, r).

(ii) Esquema de compromiso estilo ElGamal.

En este caso:

$$com\ (r, b) = (g^r h^{r+b})$$

No pueden existir r y r' tales que:

$$com\ (r, b) = com\ (r', 1 - b)$$

para b con valor 0 o 1.

Propiedades de los esquemas criptográficos de compromiso

Los esquemas criptográficos de compromiso pueden presentar las siguientes propiedades, que ordenadas por grado de robustez son:

(1)Vinculante (que obliga)

Es un requisito básico de seguridad. Después de dar la caja fuerte a la entidad B, la entidad A no puede alterar la nota escrita dentro. La probabilidad de que la entidad A pueda abrir-generar dos compromisos diferentes con éxito es despreciable.

(2) Oculto

Es otro requisito básico de seguridad. La entidad B no puede determinar el contenido de la nota o notas dentro de la caja fuerte hasta que conozca la contraseña de dicha caja fuerte. La entidad B no puede adivinar información alguna hasta la fase de apertura.

(3) Corrección

Es otro requisito básico de seguridad. La probabilidad de que la honestidad de A falle al abrir un compromiso es despreciable.

(4) Equivocabilidad (Puerta trasera)

Existe una puerta trasera que podría permitir a un emisor alterar el valor del compromiso. Por ejemplo, en el contexto de los logaritmos discretos si $h = g^s$, sea el compromiso: com $= (g^r h^x)$, entonces al abrir se revela (x, r). Si se equivoca a x', se revela (x', r') donde $r' = r + s\ (x - x')$.

(5) No maleable (Intuición) basados o no en tags

La entidad A hace un compromiso com a un valor desconocido v. Un adversario no debería poder producir un nuevo compromiso com' a un valor v' relacionado con v con una probabilidad mejor no despreciable después de ver com que antes de ver com. Los compromisos pueden tener asociada una etiqueta o tag.

(6) UA (Universal Composability).

Deben tener las propiedades de equivocabilidad, no maleable y extractibilidad (este requisito aumenta la complejidad).

(7) Solidez y resistencia a la simulación

(8) Compromiso homomórfico.

Para definir esta propiedad consideremos el esquema de compromiso de Pedersen, dado el compromiso $com_1(r, x) = g^r h^x$, donde

❖ **Protocolo 1-1 *OT* (*Oblivious Transfer*) de Rabin.**

- Dados dos entidades A (emisor) y B (receptor).
- La entidad A genera una clave RSA (e, d, n) y publica la clave pública (e, n).
- La entidad A cifra un valor secreto s y se lo envía a la entidad B: $E_{(e,n)}(s)$.
- La entidad B genera un valor aleatorio x y calcula $a = x^2 \bmod n$ y se lo envía a la entidad A.
- La entidad A obtiene las cuatro raíces cuadradas del valor a mod n. Elige el valor y de forma aleatoria de entre todos ellos y se lo envía a la entidad B.
- Si el valor y es una raíz cuadrada de a mod n distinta de x y – x entonces la entidad B puede factorizar n y descomponer la clave RSA para revelar el secreto s.
- La entidad A no tendrá idea alguna de si la entidad B ha aprendido del valor y.

❖ **Transferencia trascordada 1-n *OT***

- Dada una entidad A con n secretos: $m_0, \ldots, m_{n-1}$.
- La entidad B que elige selecciona un valor de selección v.
- Al final del protocolo 1-n OT la entidad B conoce el secreto m_v.
- La entidad B no obtiene información sobre el resto de (n – 1) secretos. La entidad emisora A no sabrá con que secreto se ha hecho la entidad B.

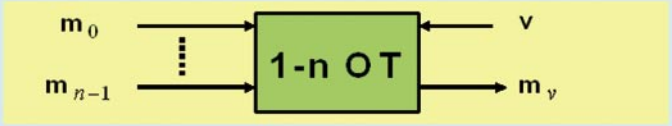


Figura 4. Protocolos de transferencia trascordada: 1-1 OT y 1-n OT

r es un residuo cuadrático en Z_n y x pertenece a Z_n . Este esquema posee la propiedad homomórfica aditiva ya que:
$[com_1(r,x).com_1(r',x')]=com_1(r+r', x+x')$

Esta propiedad es útil en computación multi-parte, puede utilizarse como bloque de construcción para la síntesis de esquemas de elecciones seguras, durante la fase de votación los votantes colocan sus votos en compromisos homomórficos y durante la fase de recuento, los votantes se cuentan tomando el producto de todos los compromisos.

Clasificación de los esquemas de compromiso

Un esquema de compromiso consta de dos fases una de compromiso después de la que el emisor se compromete con otra entidad receptora en un cierto valor y la fase de revelación o apertura del compromiso, durante la que el valor comprometido se revela al receptor. Pueden identificarse dos tipos de esquemas de compromiso:

(1) Esquema de compromiso estándar

Protege contra emisores poderosos en recursos. Dicho esquema oculta desde el punto de vista computacional y vincula desde el punto de vista teórico la información.

(2) Esquema de compromiso perfecto.

Son más difíciles de construir. Protege contra receptores poderosos en recursos. Dicho esquema es vinculante desde el punto de vista computacional y oculta la información desde el punto de vista teórico.

Protocolos BC basados en criptosistemas simétricos-asimétricos y en funciones hash

Supongamos que una entidad A afirma que posee un método capaz de predecir los resultados de los partidos de fútbol, que desea vender a una entidad B. La entidad B solicita a la entidad A que pruebe que su método de hecho predice los resultados de los partidos de la próxima semana. La entidad A se niega y le dice a B que mejor sería para que compruebe que el sistema funciona correctamente que puede predecir los resultados de la próxima semana. El problema que se plantea es que A desea enviar a B un bit b (0 o 1) pero con los siguientes requisitos:
(a) La entidad B no puede determinar el valor del bit sin la ayuda de A.
(b) La entidad A no puede cambiar el bit una vez que se lo haya enviado.

La solución mecánica es que A ponga el bit en una caja cerrada y se lo envíe a B. Cuando B desee conocer el valor del bit, A le dará la llave o clave para abrirla. La entidad A no puede cambiar el bit una vez enviado en una caja a B.

En este apartado se sintetizan métodos similares pero utilizando tecnología criptográfica:

(1) Bit commitment utilizando criptografía simétrica

La entidad A crea un mensaje con el bit b que desea comprometerse, por ejemplo el resultado de partido de fútbol futuro. Cifra con una clave aleatoria K utilizando un cierto algoritmo de cifrado de clave secreta y envía a la entidad B el resultado
$E_K(b)$. Ahora la entidad B solicita a la entidad A que revele el bit b. Para ello A envía a B la clave K, entonces la entidad B descifra $D_KE_K(b)=b$. En este método la entidad A puede hacer trampas y cambiar el bit b, para ello encuentra dos claves K1 y K2 tales que: $D_{K1}E_K(b) = 1$ y $D_{K2}E_K(b) = 0$. Como la salida es binaria la entidad A puede averiguar las claves y tiene un 50% de probabilidades de hallar la respuesta. Dependiendo del bit que desee

DIFERENTES TIPOS DE FUNCIONES HASH CON Y SIN CLAVE

- Dado el valor x → $H(x) = (7x^{21} + 3x^3 + 13x^2 + 1) \bmod (2x^{15} - 1)$.
- Dado el valor x y la clave (y, z) → $H(x, y, z) = (x + y + z) \bmod p$.
- Dad el valor x → $H(x) = x \bmod 65537$.
- Dado el valor x y la clave (a, b) → $H(x, a, b) = (ax^2 + b) \bmod p$.
- Dado el valor x y la clave (c, d, e) → $H(x, c, d, e) = (cx^e + d) \bmod p$.
- Dado el texto x formado por un conjunto de n caracteres ASCII, se agrupan sus códigos decimales a_i de tres en tres y se aplica la expresión: $c_i = (a_i - a_{i+1}).\ a_{i+2}$ desde i = 1 con i = (i + 3) hasta que i = (n – 2). Seguidamente se suman algebraicamente (teniendo en cuenta los signos) los c_i y el resultado es la *función hash* sin clave buscada: $H(x) = (c_1 + c_4 + c_7 + \ldots + c_{n-2}) = \sum_{\substack{j=1 \\ j=j+3}}^{n-2} c_j$. El número de sumandos es el total de grupos de tres caracteres. Si n = 15, existirán cinco grupos de tres caracteres.

- **EJEMPLO:**

Sea el texto sobre el que deseamos calcular su *función hash*: x = {En un rincón de} → es un texto ASCII de 15 caracteres. Lo pasamos a sus códigos ASCII incluyendo los blancos: x = (69, 110, 32, 117, 110, 32, 114, 105, 110, 99, 243, 110, 32, 100, 101). Agrupamos de tres en tres desde la izquierda y aplicamos la expresión: [(1° – 2°).3°] → Obtenemos (69, 110, 32) → – 1312, (117, 110, 32) → 224, (114, 105, 110) → 990, (99, 243, 110) → –15840, (32, 100, 101) → – 6868. Por tanto:
H(x) = – 1312 + 224 + 990 – 15840 – 6868 = – 22806.
Cualquier ligera modificación en el texto x provoca un cambio importante en la *función hash* H(x). Por ejemplo, al sustituir rincón por rincon sin acento, el valor del *hash* pasa de – 22806 a – 8286, ya que: (99, 111, 110) → – 1320 → H(x) = – 1312 + 224 + 990 – 1320 – 6868 = – 8286.

Figura 5. Funciones Hash con clave y sin clave para construir esquemas de compromiso BC/SB

revelar a B puede enviarle K1 o K2. Para resolver este problema B genera una cadena de bits aleatoria R y se la envía a la entidad A. La entidad A crea un mensaje con el bit b que desee comprometerse y R, por ejemplo concatenando las dos cadenas de bits. La entidad A cifra con una clave aleatoria K y envía a B el resultado $E_K(R, b)$. Posteriormente B pide a la entidad A que revele el bit b, la entidad A envía a B la clave secreta K, entonces B descifra:

$$D_K E_K(R, b) = (R, b)$$

Si R es largo de más de 128 o 512 bits y el algoritmo de cifrado es robusto la probabilidad de trampas es despreciable.

(2) Bit commitment utilizando criptografía asimétrica.

Supongamos que A y B acuerdan que si el resultado final es 1 entonces A gana un premio y si es 0 el premio se lo queda B. Las fases del mecanismo son:

(a) La entidad A genera un par de claves pública y privada (e, d) y publica la clave pública e. La entidad A selecciona de forma aleatoria un bit b_A y se compromete enviando a B el valor cifrado con la clave pública: $E_e b_A$.

(b) La entidad B selecciona de forma aleatoria un bit b_B y se lo envía a la entidad A.

(c) La entidad A revela a B su clave privada d y entonces ambas entidades A y B pueden calcular $b = (b_A + b_B) \bmod 2$.

(3) Bit commitment utilizando funciones criptográficas unidireccionales o hash

Las fases de mecanismo son:

(a) La entidad A genera dos cadenas de bits aleatorios R1 y R2.

(b) La entidad A crea un mensaje formado por la terna (R1, R2, b).

(c) La entidad A aplica una función unidireccional H al mensaje y se lo envía a la entidad B junto con una de las cadenas de bits aleatorias, es decir: H(R1, R2, b), R1. La entidad B no puede encontrar el bit b debido a la naturaleza unidireccional de la función H( ) y su ignorancia de R2.

(d) La entidad A revela su compromiso enviando a B el mensaje original (R1, R2, b).

(e) La entidad B calcula la función hash: H(R1, R2, b) y compara con el mensaje previo enviado por A. Si coinciden, el compromiso de A se habrá confirmado. La entidad A no puede hacer trampas y cambiar su compromiso ya que no puede encontrar otro mensaje (R1, R2', b') tal que: H(R1, R2', b') = H(R1, R2, b) si esto fuese posible significaría que la función H presenta colisión; las funciones H profesionales no presentan colisión. Por otro lado si A envía R1 y R2 en la fase (c), entonces B podría haber calculado H(R1, R2, 0) y H(R1, R2, 1) y comparado con el valor original y haber encontrado el valor del bit b.

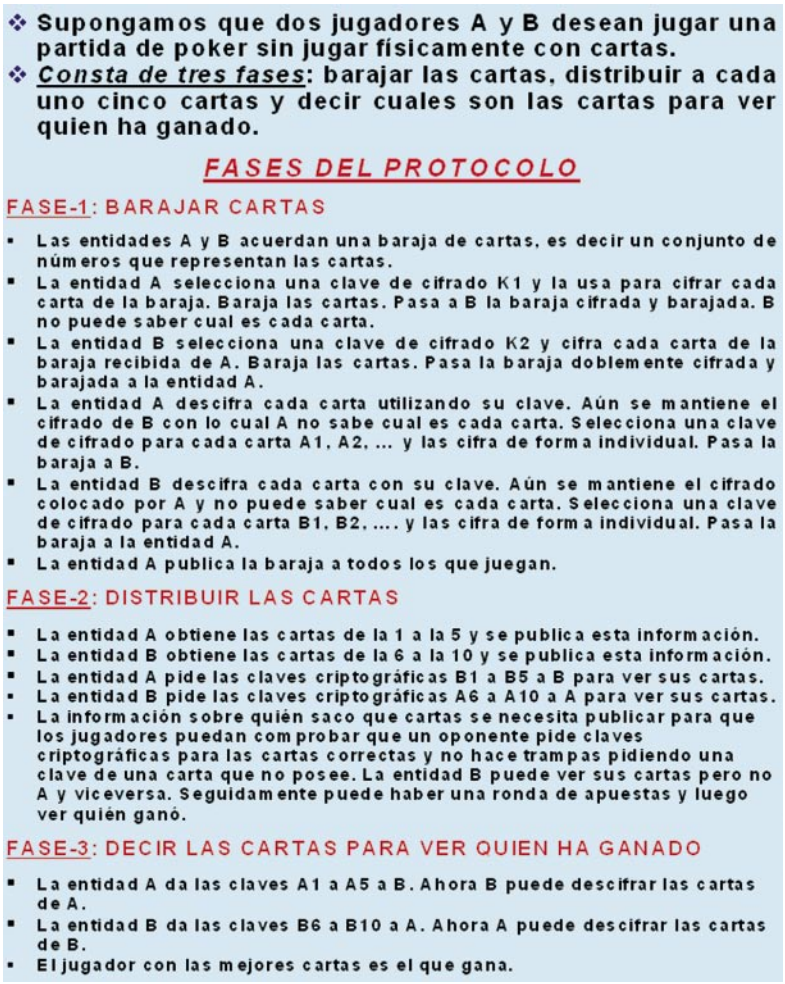


Figura 6. Resolución del problema MP (Mental Poker) utilizando un esquema criptográfico de compromiso

Aplicaciones de los esquemas de compromiso

Examinemos algunas aplicaciones de los esquemas de compromiso:

(1) Aplicación en pujas y subastas

Un comprador potencial B desea comprar un cierto producto gastando una cantidad menor del precio de compra denominado b. Un vendedor potencial A desea vender un cierto producto por un precio mayor que el precio de venta denominado a. Supongamos que el valor a es menor o igual que el valor b y que las cantidades a y b las guardan en secreto las entidades A y B.

Se trata de que A y B acuerden un protocolo con equidad que permita que el producto se comercialice al precio medio p = (a + b)/2. Un protocolo o esquema de compromiso puede resolver este problema; operaría de la siguiente forma:

(i) La entidad A comunica a la entidad B el compromiso a en forma de función oculta f(a).

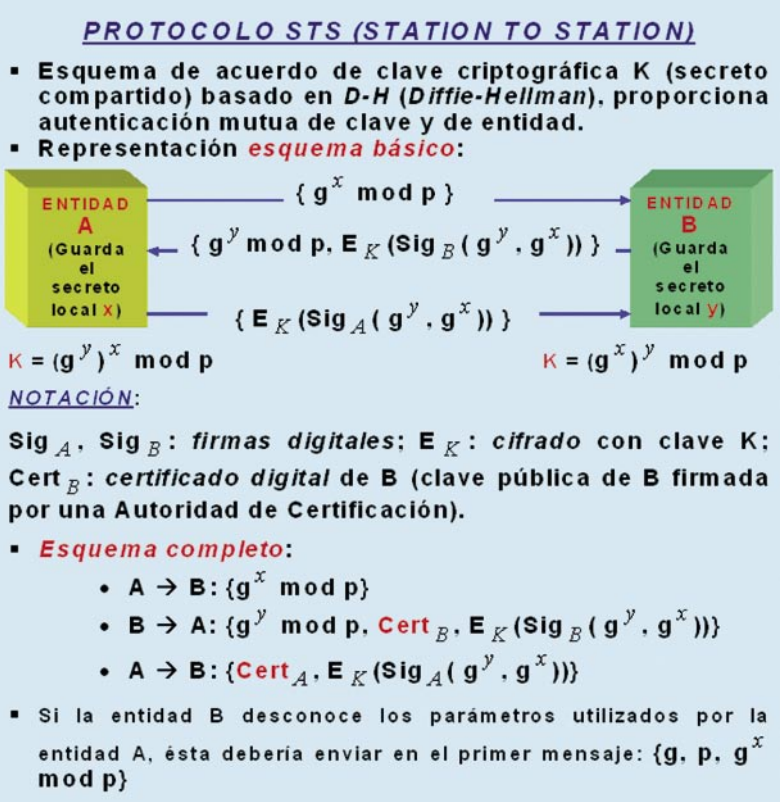


Figura 7. Especificación del protocolo STS (Station-To-Station) para protegerse en redes con ataque MIMT (Man-In-The_Middle)

(ii) La entidad B comunica a A el valor b.
(iii) La entidad A abre su compromiso dándole a B la clave para sacar a de f(a).
(iv) Ambas entidades A y B calculan el valor medio p = (a+b)/2 como se quería. Este caso puede generalizarse para situaciones más complicadas como son las subastas.

(2) Aplicación de los esquemas BC al MCF (Mental Coin Flipping)

Un posible protocolo BC presenta las siguientes fases:
(i) La entidad A se compromete con el valor b = 0 o b = 1. Cifra el valor utilizando una clave secreta K y lo envía a la entidad B y lo publica como $E_K(b)$.
(ii) La entidad B anuncia públicamente y le envía a la entidad A, el valor de c que puede ser 0 o 1.
(iii) La entidad A publica la clave K.

Tanto las entidades A como B pueden calcular: $[D_K E_K(b)+c] \bmod 2$.

Consideraciones finales

Nuestro grupo de investigación trabaja desde hace doce años en la implantación de esquemas de compromiso en muy diversos campos de aplicación. También ha participado en la valoración de riesgos de protocolos BC/SC preestablecidos y su reforzamiento con contramedidas frente a amenazas de nueva generación. La flexibilidad y potencia que ofrecen los esquemas de compromiso permite aplicarlos en nuevas áreas de actividad de muy alta tecnología como es el caso de la criptografía cuántica para cifrar las comunicaciones intercambiadas a través de redes de fibra óptica por ejemplo de tipo monomodo. Así mismo el campo de las aplicaciones e-business y de protección para casinos virtuales demanda un creciente número de soluciones de esquemas de compromiso.

Bibliografia

- Areitio, J. y Areitio, A. "Determinación del ROI/ROSI, elemento clave del análisis de riesgos de seguridad de la información". R E de Electrónica. Nº 589. Diciembre 2003.
- Areitio, J. y Areitio, A. "Tipificación de amenazas, identificación de contramedidas de seguridad en el ámbito de gestión de redes y sistemas". R E de Electrónica. Nº 613. Diciembre 2005.
- Areitio, J. "Identificación y análisis del anonimato en comunicaciones electrónicas". REDE. Nº 627. Febrero 2007.
- Areitio, J. "Identificación y análisis en torno a la PKI y su relación con los certificados digitales y la firma electrónica avanzada". Revista Española de Electrónica. Nº 596. Julio 2004.
- Areitio, J. "Seguridad de la Información: Redes, Informática y Sistemas de Información". Cengage Learning Paraninfo. 2008.
- Shostack, A. and Stewart, A. "The New Scholl of Information Security". Addison-Wesley Professional. 2008.
- Reese, R. "Network Security". John Wiley & Sons, Inc. 2007.
- Huang, S. MacCallum, D. and Du, D.Z. "Network Security". Springer. 2008.
- NcNsab, C. "Network Security Assessment". O'Reilly. 2007.