COMPARTICIÓN DE SECRETOS EN CRIPTOGRAFÍA

Jorge Villar Santos, Carles Padró Laimón y Germán Sáez Moreno

Profesores del Dpto. de Matemática Aplicada y Telemática.
Universitat Politècnica de Catalunya
e-mail: jvillar@mat.upc.es

En la criptografía clásica, tanto en el ámbito de clave pública como en el de clave privada, los protocolos criptográficos cuentan sólo con dos participantes: el poseedor de la información original y el receptor de dicha información.

En la actualidad, con el desarrollo de las redes informáticas y la necesidad de seguridad y privacidad respecto a la información que éstas cursan, se requiere el uso de protocolos que involucren un número mayor de participantes [Des88]. Un ejemplo sencillo es la realización de una conferencia a tres en la que se requiera privacidad.

Por otra parte, la información secreta no es generada exclusivamente por personas físicas sino por empresas o entidades. En este último caso, no está claro que la responsabilidad sobre la información secreta generada pueda o deba recaer sobre una única persona. Por ejemplo, cualquier movimiento importante de capital en una empresa debería requerir la participación de varios empleados.

1. ESQUEMAS PARA COMPARTIR SECRETOS

Un esquema para compartir secretos es un protocolo criptográfico en el que, como su nombre indica, se divide un determinado secreto en fragmentos que se reparten entre los participantes. Por ejemplo, el secreto podría ser la clave de acceso a una cuenta bancaria.

Este reparto de información se realiza de modo que:

(1) sólo ciertos conjuntos de participantes autorizados pueden reconstruir el secreto original.
(2) un conjunto de participantes no autorizado no puede obtener información alguna sobre el secreto original.

De la segunda condición se desprende que el secreto no se divide literalmente en fragmentos sino que los fragmentos entregados a cada participante resultan de la ejecución de un algoritmo más sofisticado. Asimismo, la reconstrucción del secreto no consistirá en la yuxtaposición de los fragmentos de los participantes sino en la ejecución de cierto algoritmo cuyas entradas sean los fragmentos anteriores.

Los primeros esquemas para compartir secretos fueron introducidos en 1979 por Shamir en [Sha79] y por Blackley en [Bla79]. El primero de ellos está basado en interpolación polinómica sobre un cuerpo finito. Dado un secreto k, se toma un polinomio secreto p de grado no superior a $t-1$, tal que $p(0) = k$. A cada uno de los n participantes, que se caracteriza por cierto número $\xi_i \neq 0$, se le asigna el fragmento $S_i = p(\xi_i)$.

Un protocolo debe ser robusto tanto frente a personas externas al mismo como frente a usos ilícitos de la información repartida

Se puede demostrar que si se reúne una cantidad igual o mayor que t participantes, existe un único polinomio p de grado inferior a t que pase por los puntos (ξ_i, S_i) correspondientes a dichos participantes. Además, el secreto original coincide con $p(0)$.

Por otra parte, dado un conjunto con menos de t participantes, existen varios polinomios q que pasan por los puntos (ξ_i, S_i) correspondientes a dichos participantes y $q(0)$ toma todos los valores posibles con la misma frecuencia. Así, todos los valores posibles del secreto k resultan equiprobables, y los participantes tienen la misma información sobre el secreto que cualquier persona ajena al protocolo.

Este tipo de esquemas en los que se exige un número mínimo de participantes para reconstruir el secreto se denominan esquemas de umbral. Estos esquemas no son los únicos existentes pero sí los más ampliamente estudiados.

2. ESQUEMAS ROBUSTOS FRENTE A MENTIROSOS

En el mundo de la criptografía, un protocolo debe ser robusto tanto frente a personas externas al mismo como frente a usos ilícitos de la información repartida.

Por ejemplo, un participante de un esquema para compartir secretos podría intentar engañar a otros suministrando un fragmento incorrecto durante el proceso de reconstrucción. Si el esquema no cuenta con un algoritmo de verificación de los fragmentos, se reconstruye un secreto incorrecto. En el caso peor, con el fragmento correcto y el secreto incorrecto, el participante tramposo podría recuperar por sí mismo el secreto original. Esto es exactamente el inconveniente del esquema de Shamir.

Un participante de un esquema para compartir secretos podría intentar engañar a otros suministrando un fragmento incorrecto durante el proceso de reconstrucción

Una manera de dotar de cierta robustez al esquema de Shamir es además de repartir el secreto original k, repartir por un procedimiento análogo su cuadrado k^2. Así, a cada participante se le otorgan los fragmentos s_i y t_i correspondientes respectivamente a k y a k^2.

En el proceso de reconstrucción, se recuperan ambos secretos k_1 y k_2. Si todos los participantes son honrados, resulta $k_1 = k$ y $k_2 = k^2$. En caso contrario, con alta probabilidad sucederá que $k_1^2 \neq k_2$, y los participantes deducirán que el secreto k_1 reconstruido no es válido. Por otra parte, un participante no puede (salvo casualidad improbable) modificar sus fragmentos s_j y t_j de modo que se cumpla la relación $k_1^2 = k_2$, sin conocer previamente los fragmentos de t-1 participantes más.

Esta mejora del esquema de Shamir fue introducida por Padró en [Pad96].

Existen otros requisitos de robustez más severos que el anterior que, por ejemplo, consiguen llegar a identificar al participante tramposo a partir de los fragmentos suministrados [Car95]. En general, cuanto más robusto es un esquema para compartir secretos, mayor resulta el tamaño de los fragmentos repartidos a los participantes. En el esquema de Padró, el tamaño de los fragmentos es el doble del tamaño del secreto. Se puede demostrar que este tamaño es casi el mínimo posible [Oga96].

Los esquemas para compartir secretos pueden aparecer como un componente de otros protocolos criptográficos como la generación compartida de firmas digitales o la verificación compartida de la autenticidad de un documento [Soe90, Fra95]. En ambos casos se evita concentrar toda la responsabilidad de un acto determinado en una única persona.

Otra aplicación de los esquemas para compartir secretos se halla en los sistemas de votación electrónica, en los que la apertura de la urna requiere la reconstrucción de una clave secreta compartida entre los miembros de la mesa electoral.

3. SEGURIDAD COMPUTACIONAL VS. INCONDICIONAL

Además de los esquemas para compartir secretos descritos anteriormente y denominados incondicionalmente seguros, existe una versión menos estricta de los mismos, denominados computacionalmente seguros.

Las exigencias de un esquema tal son:

(1) sólo ciertos conjuntos de participantes autorizados pueden reconstruir el secreto original.

(2) un conjunto de participantes no autorizado no puede obtener información alguna sobre el secreto original, usando los recursos computacionales actuales.

En este tipo de esquemas se asume la existencia de una función f unidireccional, es decir, calculable con relativa facilidad y cuya inversa no se puede calcular a partir de los recursos computacionales actuales. Un ejemplo de función unidireccional es la exponenciación $f(x) = g^x$ en un cuerpo finito.

Por ejemplo, dado el fragmento s_i entregado a cada participante en un esquema incondicionalmente seguro, podemos publicar $S_i = f(s_i)$ sin revelar el valor concreto de s_i. De este modo, si un participante intenta dar un fragmento falso s^*_i, éste sería inmediatamente detectado dado que $S_i \neq f(s^*_i)$.

Los esquemas computacionalmente seguros son, en general, más versátiles que los incondicionalmente seguros dado que permiten añadir dinámicamente participantes sin tener que modificar los fragmentos repartidos, así como reutilizar los fragmentos para compartir un segundo secreto [Cac95, Gho97].

Para las mismas prestaciones, los fragmentos de un esquema computacionalmente seguro tienen menor tamaño que los fragmentos de un esquema incondicionalmente seguro.

Por último, la seguridad computacional demuestra ser suficiente para las aplicaciones prácticas.

4. CRIPTOGRAFIA VISUAL

Recientemente se ha introducido una generalización de los esquemas para compartir secretos que se conoce como criptografía visual [Nao94]. En este caso, tanto el

secreto compartido como los fragmentos que se entregan a los participantes son imágenes en blanco y negro. La restricción que se introduce es que en el proceso de reconstrucción los fragmentos se superponen como si fueran transparencias. Es decir, el resultado de superponer dos imágenes es la «OR» lógica punto a punto de ambas, considerando el color negro (opaco) como «1» y el color blanco (transparente) como «0» lógico.

Desde el punto de vista de esquemas para compartir secretos, lo que se hace es descomponer la imagen secreta en un conjunto de bits, cada uno correspondiente a un pixel de la imagen. Cada bit se reparte independientemente de los demás bits de la imagen, de modo que los fragmentos tienen un tamaño fijo de *m* bits por pixel original. De este modo, los fragmentos requieren una resolución mayor que la imagen secreta original.

La reconstrucción por superposición de los fragmentos no es exacta pero el ojo humano es capaz de distinguir la imagen original si esta no es excesivamente recargada. La ventaja de este protocolo es que el algoritmo de reconstrucción no requiere realizar cálculo alguno.

BIBLIOGRAFÍA

[Bei94] A. Beimel y B. Chor «Interaction in key distribution schemes» Advances in Cryptology, Crypto '93 444-457 (1994)

[Bla79] G.R. Blakley «Safeguarding cryptographickeys» AFIPS Conference Proceedings 48 313-317 (1979)

[Cac95] C. Cachin y C. Boyd «On-line secret sharing» Cryptography and Coding, IMA '96 190-198 (1995)

[Car95] M. Carpentieri «A perfect threshold secret sharing scheme to identify cheaters» Design, Codes and Cryptography 5 183-187 (1995)

[Des88] Y. Desmedt «Society and group oriented cryptography: A new concept» Advances in Cryptology, Crypto '87 120-127 (1988)

[Fra95] M.K. Franklin y M.K. Reiter «Verifiable signature sharing» Advances in Cryptology, EUROCRYPT '9550-63 (1995)

[Gho97] H. Ghodosi, J. Pieprzyk, G.R. Chaudhry y J. Seberry «How to prevent cheating in Pinch's scheme» Electronics Letters 33 (1997) 1453-1454

[Nao94] M. Naor y A. Shamir «Visual cryptography» Advances in Cryptology, EUROCRYPT '94 1-12 (1994)

[Oga96] W. Ogata y K. Kurosawa «Optimum Secret Sharing Scheme Secure against Cheating» Advances in Cryptology, EUROCRYPT '96 200-211 (1996)

[Pad96] C. Padró, G. Sáez y J.L. Villar «Detection of cheaters in vector space secret sharing schemes» Proc. of the 1st Int. Conf. on the Theory and Appl. of Cryptology, PRAGOCRYPT '96 (1996) 359-369

[Sha79] A. Shamir «How to share a secret» Commun. of the ACM 22 612-613 (1979)

[Soe90] M. de Soete, J.J. Quisquater y K. Vedder «A signature with shared verification scheme» Advances in Cryptology, Crypto '89 253-262 (1990)

VENTANA AL CAMPUS

Inauguramos en este número una sección en la cual trataremos temas relacionados con el Campus. Os invitamos a colaborar enviando vuestras sugerencias a la edición de la revista.

Como ya sabéis, una de las características del Campus Nord de la UPC es la existencia de un centro comercial que está situado entre los edificios C3, C4 y B4. Este hecho, tan habitual en las universidades del resto del mundo, se está reproduciendo en los nuevos campus, como el de la Autónoma y el de la Vall d'Hebron, pero en ninguno de estos casos se ha conseguido una integración urbana como en el caso de La CUP.

Se ofrecen servicios de todo tipo, unos más directamente relacionados con la vida estudiantil (Self Sevice PoliMenu, la librería técnica Díaz de Santos, cooperativa de papelería Abacus, Cooperativa de Publicaciones del Campus Nord CPET), y otros que nos ayudan a encontrar más cómoda y agradable nuestra estancia en el campus, permitiéndonos ahorrarnos el incómodo trayecto al centro de la ciudad (como puede ser el RACC, una óptica, una peluquería, oficinas bancarias, agencias de viajes, servicio de fotocopias, servicio de limpieza, servicio de mensajería, una tienda de deportes, restaurantes y un quiosco).

La intención de los gestores de La CUP ha sido siempre la de mejorar la calidad de vida en el Campus. Como hemos podido apreciar, no solo nos han acercado los servicios comerciales, sino que también participan en las actividades culturales y sociales, apoyando las iniciativas de los estudiantes, ya sea para realizar fiestas, revistas, congresos, etc. En parte, gracias a ellos se mantiene el espíritu universitario, tan necesario para desconectar de la rutina estudiantil.

La CUP pone a disposición de los estudiantes (que en el fondo somos sus clientes) un despacho a donde podemos acudir siempre que surja cualquier problema con locales de La CUP, o tengamos alguna sugerencia o queja al respecto (recordemos el caso del Nyam-Nyam). Desde aquí os animamos a descubrir lo que La CUP nos ofrece, no sólo sus comercios, sino también su apoyo a nuestras iniciativas.