Informe eSAMCid sobre estructuras de acceso

Enero de 2017

Resumen

En este documento se ofrece una visión general sobre los esquemas de compartición de secretos con seguridad incondicional realizables mediante algoritmos de eficientes de compartición y de reconstrucción de los secretos compartidos. El objetivo fundamental es mostrar un abanico de posibles alternativas a los clásicos esquemas con estructura de acceso de umbral, que permiten ampliar la aplicabilidad práctica de las claves criptográficas compartidas. Aunque existan multitud de trabajos de investigación enfocados hacia la construcción y evaluación de amplias familias de estructuras de acceso, prácticas o no, el presente informe describe únicamente aquéllas con prestaciones comparables a las ofrecidas por las estructuras de umbral.

Subvencionado por el Ministerio Español de Economía y Universidades mediante el projecto MTM2013-41426-R.

Índice

1. Introducción

Aunque en sus inicios la criptografía se planteaba fundamentalmente para asegurar las comunicaciones entre dos entidades y para preservar la integridad y la confidencialidad de la información privada, el ámbito de aplicación se ha visto vastamente ampliado en las últimas décadas, de modo que en la actualidad, los protocolos criptográficos involucran a conjuntos numerosos de usuarios. Es por ello que la generación conjunta y la compartición de claves criptográficas se han convertido en ingredientes básicos da la mayor parte de los protocolos criptográficos.

Un ejemplo claro de ello es la generación compartida de firmas digitales, que se diferencia de la firma digital convencional en que solamente con la cooperación de varios usuarios autorizados la firma de un documento puede ser generada correctamente. La firma digital no debe concebirse como un mero acto de demostrar la autoría de un archivo o informe, sino como una prueba de la intención y de la aceptación de la acción plasmada en el documento firmado, como en el caso de una transacción económica o de la aceptación de un contrato. En ese sentido, las operaciones a nivel corporativo requieren habitualmente la aceptación concertada de un mínimo de personas autorizadas.

Para distribuir la capacidad de realizar una acción criptogáfica, debe ser posible efectuar la generación de ciertas claves o fragmentos relacionados entre sí de modo que la agrupación de algunos de ellos equivalga a la clave criptográfica que garantiza la ejecución de la acción.

Tanto la seguridad como la funcionalidad de un criptosistema distribuido dependen de qué conjuntos de fragmentos se consideran autorizados para realizar la acción. Por ejemplo, se asume normalmente que un único fragmento nunca será suficiente para realizar la acción, pero también es necesario que ningún usuario pueda vetar completamente la acción al negarse a utilizar su fragmento, o simplemente al destruirlo.

En este informe se efectúa una descripción de las principales estrategias para definir los conjuntos autorizados de fragmentos, mediante las llamadas estructuras de acceso. Dado que la elección de las mismas tiene un impacto significativo en la eficiencia de los protocolos criptográficos, el documento se centrará en aquéllas que resultan de interés práctico.

2. Esquemas para compartir secretos

Los esquemas para compartir secretos son la pieza esencial de la criptografía distribuida, dado que éstos permiten definir políticas de acceso a recursos compartidos por un conjunto de usuarios.

En un esquema para compartir secretos se reparte el valor de un secreto en fragmentos entre los participantes de un conjunto $\mathcal{P} = \{P_1, \ldots, P_n\}$, de forma que sólo ciertos subconjuntos, denominados autorizados, pueden reconstruir el secreto a partir de su información privada.

Los esquemas para compartir secretos se introdujeron de forma independiente por Blackley [4] y Shamir [17] en 1979.

La familia de subconjuntos de $\mathcal{P}$ autorizados Γ se denomina estructura de acceso y es monótona, es decir, si un subconjunto A contiene un subconjunto B autorizado, entonces A también debe ser autorizado.

En un esquema para compartir secretos, con estructura de acceso Γ y conjunto de posibles secretos K, a partir de un valor secreto $s \in K$ y de una cierta elección aleatoria, cada participante P_i recibe privadamente un fragmento $s_i \in S_i$, donde S_i denota el conjunto de posibles fragmentos de P_i. Normalmente, se exige que el esquema de compartir secretos sea perfecto, es decir,

1. Los subconjuntos autorizados, $A \in \Gamma$, pueden reconstruir el valor del secreto s a partir de sus fragmentos $s_A = \{s_i \mid P_i \in A\}$. Es decir, para cualquier $A \in \Gamma$ existe un único valor posible del secreto s compatible con los fragmentos s_A.

2. Los participantes de un subconjunto no autorizado no pueden obtener ninguna información sobre el secreto a partir del valor de sus fragmentos. Es decir, si $A \notin \Gamma$ todos los valores posibles del secreto s permanecen equiprobables, aún conociendo los fragmentos s_A.

En algunas ocasiones, la segunda propiedad se relaja, permitiendo que algunos conjuntos no autorizados sean capaces de adquirir cierta información limitada sobre el secreto, pero en este documento solamente trataremos el caso perfecto.

Los primeros esquemas de compartir secretos que se introdujeron utilizaban la llamada estructura de acceso de umbral, en la que un conjunto A es autorizado si el número de participantes que contiene iguala o supera cierto umbral t, independientemente de la identidad de los mismos. A continuación describiremos el esquema de umbral de Shamir, que es quizás el esquema para compartir secretos más ampliamente utilizado.

2.1. El esquema de Shamir

Consideremos el conjunto de participantes $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ y un entero t tal que $1 \leq t \leq n$. La estructura de acceso Γ es la de umbral (t, n), en la que un conjunto A es autorizado si consiste en t o más participantes. El conjunto de posibles secretos es un cuerpo finito, que por simplicidad, vamos a suponer que es el cuerpo primo $\mathbb{Z}_p$, siendo p un número primo. En todo caso, el tamaño del cuerpo, p, debe ser estrictamente mayor que el número de participantes, n.

En la fase inicial, a cada participante se le asigna un elemento x_i del cuerpo $\mathbb{Z}_p$, de modo que los valores x_i son todos no nulos y diferentes entre si. Los valores x_i así como el tamaño del conjunto de secretos, p ,forman parte de la descripción pública del esquema.

Para distribuir un secreto $s \in \mathbb{Z}_p$ se toma al azar un polinomio de grado menor o igual que $t-1$, $r(x)$, tal que $r(0) = s$. Cada participante recibe como fragmento $s_i = r(x_i)$. Debido a que el valor del secreto y los coeficientes del polinomio han de mantenerse secretos, esta fase la lleva a cabo una entidad especial de confianza D llamada distribuidor.

Veamos un ejemplo: En $\mathbb{Z}_{17}$ diseñamos un esquema de umbral $(3, 4)$, los participantes son P_1, P_2, P_3, P_4 y los elementos asignados son $x_1 = 1$, $x_2 = 2$, $x_3 = 3$, $x_4 = 6$, respectivamente. El valor secreto a repartir es $s = 2$ y el polinomio elegido por el distribuidor es $r(x) = 2x^2 - 4x + 2$. Entonces, los fragmentos de cada participante serán $s_1 = 0$, $s_2 = 2$, $s_3 = 8$, $s_4 = 1$, respectivamente. Ahora, los participantes P_1, P_2 y P_3 pueden colaborar entre ellos para construir el único polinomio de grado menor o igual que 3 que pasa por los puntos $(1, 0)$, $(2, 2)$ y $(3, 8)$, que debe coincidir con $r(x)$. El término independiente $r(0)$ es exactamente el secreto compartido.

Por otra parte, si sólo colaborasen los participantes P_1 y P_2, para cualquier valor del secreto s existe un único polinomio de grado menor o igual que 3 que pasa por los puntos correspondientes, $(1, 0)$ y $(2, 2)$, y por el punto $(0, s)$. Por tanto, aún conociendo esos dos fragmentos, el secreto sigue siendo completamente desconocido, ya que todos los valores posibles siguen siendo equiprobables.

A diferencia de otros protocolos criptográficos, la seguridad del esquema de Shamir es incondicional, dado que un adversario con capacidad computacional ilimitada no puede extraer información alguna sobre el secreto s aunque conociese $t-1$ fragmentos del mismo.

2.1.1. Valores extremos del umbral

Los valores extremos del umbral, es decir los esquemas de umbral (n, n) y los de umbral $(1, n)$, merecen atención especial. En el esquema (n, n) la reconstrucción del secreto requiere la colaboración de todos los participantes, lo que admite una construcción sumamente sencilla: Cada participante P_i recibe un fragmento aleatorio $s_i \in \mathbb{Z}_p$, y el secreto compartido es la suma (módulo p) de todos ellos, $s = s_1 + \ldots + s_n$.

El otro caso extremo es trivial, ya que la estructura de umbral $(1, n)$ justamente indica que cada participante puede individualmente recuperar el secreto. Por ello, el esquema consiste en entregar directamente dicho secreto a cada participante, es decir, $s_i = s$.

Debemos observar que en las dos construcciones anteriores desaparece la limitación sobre el tamaño del cuerpo, p, ya que puede ser ahora arbitrariamente pequeño (incluso $p = 2$) e independiente del número de participantes.

Los dos casos extremos de estructuras de umbral resultan especialmente útiles como piezas auxiliares en la definición de estructuras de acceso más complejas y versátiles, como veremos en secciones posteriores.

2.1.2. Propiedades homomórficas

Un aspecto a tener en cuenta en algunos esquemas de compartición de secretos es la posibilidad de efectuar operaciones básicas sobre distintos secretos sin tener que reconstruirlos previamente, es decir, operando únicamente sobre los fragmentos. Concretamente, un esquema para compartir secretos es aditivamente homomórfico sobre $\mathbb{Z}_p$ si cada participante P_i puede combinar los fragmentos $s_i^{(a)}$ y $s_i^{(b)}$ recibidos en la compartición de dos secretos $s^{(a)}$ y $s^{(b)}$, respectivamente, para obtener un nuevo fragmento del secreto suma $s^{(a)} + s^{(b)}$.

El esquema de Shamir disfruta de esa propiedad, dado que la suma de los fragmentos de dos secretos repartidos con el mismo umbral t equivale a la compartición de la suma de los dos secretos, también con el mismo umbral. En efecto, cada secreto se reparte por medio de un polinomio aleatorio, de modo que la suma de polinomios corresponderá tanto a la suma de los secretos como a la suma de los fragmentos de cada participante.

El esquema también puede dotarse de propiedades homomórficas multiplicativas, pero ello requiere añadir comunicaciones adicionales entre los participantes.

2.2. Eficiencia de los esquemas para compartir secretos

Existen varias medidas sobre la eficiencia de un esquema para compartir secretos. Enumeramos a continuación los aspectos más relevantes a tener en cuenta desde el punto de vista de las aplicaciones de los mismos:

- El tamaño de los fragmentos recibidos por los participantes, que es la medida de la cantidad de información secreta que éstos deben custodiar. Puede cuantificarse de varias maneras, que comúnmente son el máximo de los tamaños, o el valor promedio entre los distintos participantes.
- La complejidad del algoritmo de generación de los parámetros públicos del esquema y de los fragmentos. Para algunas estructuras de acceso diferentes de las de umbral solamente se conocen esquemas de compartición de secretos que o bien son imprácticos por su complejidad, o bien éstos requieren la costosa construcción de ciertos objetos combinatorios especiales en el proceso de inicialización.
- La complejidad del algoritmo de reconstrucción del secreto. En una aplicación práctica de los esquemas para compartir secretos, una excesiva complejidad de cálculo en el algoritmo de reconstrucción del secreto puede degradar sustancialmente las prestaciones de un protocolo criptográfico. Por ejemplo, la reconstrucción del secreto, o un procedimiento relacionado con la misma, es requerida durante la generación de una firma digital conjunta entre varios participantes.
- El tamaño mínimo requerido para el conjunto de secretos. Por ejemplo, el esquema de Shamir descrito anteriormente impone una seria restricción en el tamaño mínimo del conjunto de secretos en función del número de participantes. Esto puede tener un impacto sustancial en protocolos criptográficos con un elevado número de participantes en los que se comparten números aleatorios secretos pequeños, o incluso bits.

Se demuestra que en un esquema para compartir secretos perfecto, el tamaño de los fragmentos no puede ser inferior al del secreto. Si se da la igualdad, el esquema se denomina ideal.

No todas las estructuras de acceso admiten esquemas ideales, por lo que la eficiencia del esquema estará limitada en particular por la estructura de acceso que pretenda implementar. Como se desprende de la propia existencia del esquema de Shamir, las estructuras de umbral admiten esquemas ideales.

3. Estructuras de acceso no de umbral

En esta sección hacemos una descripción de las principales familias de estructuras de acceso con aplicabilidad práctica que generalizan el concepto de estructura de acceso de umbral.

3.1. Composición de estructuras de acceso

Es posible componer varios esquemas de umbral para obtener estructuras de acceso más generales sin sacrificar excesivamente la eficiencia del esquema resultante. Los ejemplos más sencillos son las composiciones por conjunción y por disyunción.

Si tenemos dos estructuras de acceso Γ_1 sobre $\mathcal{P}_1$ y Γ_2 sobre $\mathcal{P}_2$, la conjunción de ambas es una estructura de acceso $\Gamma_1 \wedge \Gamma_2$ sobre la unión de los conjuntos de participantes $\mathcal{P}_1 \cup \mathcal{P}_2$ en la que un conjunto A es autorizado si $A \cap \mathcal{P}_1 \in \Gamma_1$ y $A \cap \mathcal{P}_2 \in \Gamma_2$, es decir, si los participantes de A forman un conjunto autorizado en ambas estructuras de partida. Claramente, la conjunción de dos estructuras es en general más restrictiva que las estructuras originales.

A partir de dos esquemas que realicen las estructuras Γ_1 y Γ_2 puede definirse fácilmente (si se da alguna restricción técnica adicional) un esquema que realice la conjunción de ambas. Para ello, un secreto s se reparte entre dos participantes ficticios $\widetilde{P}_1, \widetilde{P}_2$ mediante un esquema de umbral $(2, 2)$. Cada uno de los dos fragmentos resultantes, $\widetilde{s}_1, \widetilde{s}_2$, se reparte entre los participantes reales utilizándolos como secretos en los esquemas que realizan Γ_1 y Γ_2, respectivamente.

Observemos que la construcción anterior requiere que el conjunto de los posibles secretos de los dos esquemas originales sean idénticos, para que podamos tomar $s = s_1 + s_2$, de modo que s_1 y s_2 sean variables aleatorias uniformes e independientes. Si las dos estructuras originales, Γ_1, Γ_2, son estructuras de umbral (t_1, n_1) y (t_2, n_2) respectivamente, y se utilizan esquemas de Shamir para realizarlas sobre el mismo cuerpo finito $\mathbb{Z}_p$, entonces el esquema resultante para la estructura $\Gamma_1 \wedge \Gamma_2$ sería el siguiente: El secreto $s \in \mathbb{Z}_p$ se descompone aleatoriamente en suma de $\widetilde{s}_1, \widetilde{s}_2 \in \mathbb{Z}_p$. Se construyen polinomios aleatorios $r_1(x)$ y $r_2(x)$, de grado menor o igual que t_1 y t_2 respectivamente, tales que $r_1(0) = \widetilde{s}_1$ y $r_2(0) = \widetilde{s}_2$. Finalmente, cada participante $P_i \in \mathcal{P}_j$ recibe el fragmento $s_{i,j} = r_j(x_{i,j})$, donde $x_{i,j}$ es el elemento público asociado a P_i en el esquema de Shamir sobre el conjunto $\mathcal{P}_j$, con $j = 1, 2$. De este modo, cada participante de la intersección $\mathcal{P}_1 \cap \mathcal{P}_2$

recibirá dos fragmentos independientes, mientras que los demás solamente recibirán uno de los dos fragmentos.

En el algoritmo de reconstrucción del secreto, se recuperan independientemente los secretos parciales $\widetilde{s}_1$ y $\widetilde{s}_2$ por medio de la interpolación de Lagrange, y posteriormente se suman ambos para obtener s.

La construcción descrita puede generalizarse de modo natural a la conjunción de un número $m > 2$ de estructuras básicas. En el caso peor, un participante recibirá m fragmentos, uno por casa esquema básico en el que participa, que tendrá que custodiar en secreto hasta la reconstrucción. Por ello, para no degradar significativamente la eficiencia, m debe ser un número reducido.

En algunos casos, los conjuntos $\mathcal{P}_1$ y $\mathcal{P}_2$ son disjuntos, y la eficiencia de la conjunción es la misma que la de los esquemas originales. Un ejemplo de ello es un esquema en el que hay dos clases de participantes, y cada una de ellas tiene privilegios de reconstrucción diferentes, como el caso en el que el secreto puede ser recuperado siempre que un conjunto A contenga como mínimo t_1 participantes de $\mathcal{P}_1$ y como mínimo t_2 participantes de t_2.

La disjunción de estructuras (y de esquemas) se define de manera análoga a la conjunción. La disjunción $\Gamma_1 \vee \Gamma_2$ de dos estructuras de acceso Γ_1 y Γ_2 sobre $\mathcal{P}_1$ y $\mathcal{P}_2$ respectivamente, es una estructura de acceso definida sobre $\mathcal{P}_1 \cup \mathcal{P}_2$ en la que un conjunto A es autorizado si o bien $A \cap \mathcal{P}_1 \in \Gamma_1$ o bien $A \cap \mathcal{P}_2 \in \Gamma_2$, es decir, si los participantes de A forman un conjunto autorizado en alguna de las dos estructuras de partida. La disyunción de dos estructuras es en general más amplia que las estructuras originales.

La construcción de un esquema para $\Gamma_1 \vee \Gamma_2$ a partir de esquemas para cada una de las estructuras originales es análoga a la de la conjunción salvo que ahora se utiliza un esquema de umbral $(1, 2)$ para combinarlos. Concretamente, se toma $\widetilde{s}_1 = \widetilde{s}_2 = s$. Las consideraciones sobre la eficiencia del esquema resultante son exactamente las mismas que en el caso anterior.

Existen construcciones aún más generales basadas en principios similares, en las que m estructuras de acceso básicas, $\Gamma_1, \ldots, \Gamma_m$, se ensamblan en una estructura más compleja por medio de otra estructura de referencia Γ_0 con m participantes $\widetilde{\mathcal{P}} = \{\widetilde{P}_1, \ldots, \widetilde{P}_m\}$. Como antes, cada participante ficticio $\widetilde{P}_i$ se asocia a la estructura Γ_i sobre un conjunto de participantes reales $\mathcal{P}_i$. El secreto s primero se reparte según un esquema que realice Γ_0, obteniendo fragmentos $\widetilde{s}_1, \ldots, \widetilde{s}_m$ asociados a los participantes ficticios. Finalmente, esos fragmentos se toman como secretos a compartir entre los usuarios reales, según las estructuras $\Gamma_1, \ldots, \Gamma_m$, respectivamente. En la reconstrucción se procede, como en la conjunción y en la disyunción, en el orden contrario: primero se reconstruyen algunos de los fragmentos de

los participantes ficticios, y luego a partir de ellos se reconstruye el secreto real.

3.2. Estructuras de acceso generales

Las técnicas de conjunción y disyunción de estructuras permiten obtener construcciones generales (llamadas circuitales) válidas para cualquier estructura de acceso. Para ello, bastaría con expresar cualquier estructura de acceso como una composición conjunciones y disyunciones de estructuras de umbral. Un modo de hacerlo es asociar a cada estructura de acceso una fórmula booleana que de como resultado si un determinado conjunto de participantes es o no autorizado. Puede demostrarse que para cualquier estructura de acceso existe siempre una fórmula que utiliza únicamente los operadores lógicos de conjunción y de disyunción, pero no el de negación. En la construcción del esquema de compartir secretos, cada operación lógica en la fórmula corresponderá a una conjunción o una disyunción de estructuras de acceso.

Por ejemplo, si $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ y los conjuntos autorizados son aquéllos que o bien contienen a P_1 y a P_2, o bien a P_2 y a P_3 o bien a P_1, a P_3 y a P_4, entonces la estructura de acceso Γ puede asociarse a la fórmula booleana

$$f_\Gamma(x_1, x_2, x_3, x_4) = (x_1 \wedge x_2) \vee (x_2 \wedge x_3) \vee (x_1 \wedge x_3 \wedge x_4).$$

de lo que se deduce que $\Gamma = \Gamma_{1,2} \vee \Gamma_{2,3} \vee \Gamma_{1,3,4}$, donde $\Gamma_{1,2}, \Gamma_{2,3}$ son estructuras de umbral $(2, 2)$ y $\Gamma_{1,3,4}$ es de umbral $(3, 3)$.

Sin embargo, esas construcciones generales son completamente imprácticas para la mayor parte de las estructuras de acceso posibles, por lo que conviene hacer un estudio de familias de estructuras particulares, suficientemente flexibles, que permitan construcciones eficientes de esquemas para compartir secretos que las realicen. En las siguientes secciones describiremos las familias conocidas más importantes.

3.3. Estructuras de umbral con pesos

En esta sección se describe la primera generalización natural de la estructura de acceso de umbral, en la que los participantes dejan de ser equivalentes para asociarles un peso distinto a cada uno de ellos. De este modo, la estructura permite diferenciar participantes con desigual relevancia en el procedimiento de reconstrucción del secreto. En particular, a cada participante P_i se le asigna un peso entero positivo w_i, de modo que un conjunto

de participantes se considera autorizado si la suma de los pesos de sus elemento supera cierto umbral t.

La estructura de acceso es fácilmente implementable mediante una sencilla modificación de un esquema de umbral (n', t), donde n' es ahora la suma de los pesos de todos los participantes, $n' = w_1 + \ldots + w_n$. Concretamente, a cada participante real P_i le son entregados w_i fragmentos del esquema de umbral (n', t). Dado que durante la reconstrucción del secreto, los participantes aportan sus fragmentos, un conjunto será autorizado si el número total de fragmentos que acumula (es decir, la suma de los pesos de sus participantes) alcanza el umbral t.

El esquema funciona como si cada participante P_i real jugase el papel de w_i participantes virtuales diferentes en un esquema de umbral (n', t).

Si bien la modificación anterior es muy simple, la eficiencia del esquema resultante se puede reducir considerablemente si los pesos adquieren un valor muy elevado. En particular, la cantidad de información secreta que recibirá el participante P_i será proporcional a su peso w_i. Por ello, la aplicabilidad práctica del esquema se reduce a casos en los que la estructura de acceso deseada puede realizarse con valores muy reducidos de los pesos.

3.4. Estructuras multipartitas o compartimentadas

Una amplia familia de estructuras de acceso que contiene numerosos ejemplos de estructuras útiles en la práctica y que además son eficientemente implementables son las denominadas multipartitas o compartimentadas. En ellas, el conjunto de participantes está dividido en cierto número m de clases disjuntas, $\mathcal{P}_1, \ldots, \mathcal{P}_m$. Denotaremos por $n_1, \ldots, n_m$ el número de participantes en cada una de dichas clases. En una estructura multipartita un conjunto A es autorizado o no dependiendo únicamente del número de participantes de A en cada una de las clases. Es decir, serán los cardinales de $A \cap \mathcal{P}_1, \ldots, A \cap \mathcal{P}_m$, que denotaremos por $a_1, \ldots, a_m$ respectivamente, los que determinarán si $A \in \Gamma$. La definición anterior implica que en los esquemas multipartitos, los participantes pertenecientes a la misma clase son indistinguibles, sin importar la identidad particular de ninguno de ellos.

Este tipo de estructuras resulta muy natural cuando el secreto se reparte entre un colectivo numeroso y heterogéneo, pero divisible en un número reducido de clases o estamentos.

Por ejemplo, consideremos la siguiente estructura tripartita en la que un conjunto A es autorizado si $a_1 \geq t_1$ y $a_1 + a_2 \geq t_2$ o bien basta con que $a_3 \geq t_3$. Utilizando varios esquemas de Shamir ensamblados adecuadamen-

te puede construirse un esquema razonablemente eficiente que implemente la estructura de acceso anterior. Concretamente, podemos combinar esquemas de Shamir de umbral (t_1, n_1) en $\mathcal{P}_1$, de umbral $(t_2, n_1 + n_2)$ en $\mathcal{P}_1 \cup \mathcal{P}_2$, y de umbral (t_3, n_3) en $\mathcal{P}_3$. Para repartir un secreto $s \in \mathbb{Z}_p$, lo dividimos aleatoriamente en la suma $s = \widetilde{s}_1 + \widetilde{s}_2$, con $\widetilde{s}_1, \widetilde{s}_2 \in \mathbb{Z}_p$, y utilizamos como secretos a compartir $\widetilde{s}_1$, $\widetilde{s}_2$ y s respectivamente en los tres esquemas de Shamir mencionados. Claramente, los participantes de $\mathcal{P}_1$ recibirán dos fragmentos de Shamir, mientras que es resto recibirán un único fragmento.

El ejemplo anterior podría utilizarse en situaciones como la de limitar el acceso a cierta información sensible en una empresa, de modo que se requiere la participación de como mínimo tres trabajadores de los que como mínimo uno tiene que ser responsable de proyecto, o bien basta con que sean dos auditores.

Una ventaja importante de este tipo de esquemas es que resulta sencillo incorporar nuevos participantes, simplemente generando nuevos fragmentos correspondientes a su clase, sin tener que cambiar ninguno de los fragmentos ya existentes. De todos modos, no todas las modificaciones naturales de la estructura pueden ser efectuadas de modo tan simple. Por ejemplo, si un participante cambia de una clase a otra, éste acumularía los privilegios de acceso de la nueva clase a la que pertenece a los que ya estaban en su poder. La revocación de privilegios de acceso requiere, en general, la renovación de todos los fragmentos y del secreto.

3.5. Estructuras jerárquicas

Las estructuras de acceso jerárquicas son casos particulares de estructuras multipartitas que, por su especial estructura, admiten esquemas de compartir secretos ideales. Existen dos tipos de estructuras jerárquicas: las conjuntivas y las disyuntivas.

En todas las estructuras jerárquicas consideramos las m clases disjuntas de participantes, $\mathcal{P}_1, \ldots, \mathcal{P}_m$, con $n_1, \ldots, n_m$ participantes respectivamente, y consideramos una secuencia entera de umbrales $0 < t_1 < \cdots < t_m$.

En la estructura jerárquica disyuntiva un conjunto A es autorizado si existe algún número entero k, $1 \leq k \leq m$, tal que $a_1 + \ldots + a_k \geq t_k$, donde a_i denota el número de participantes en $A \cap \mathcal{P}_i$.

De modo análogo, en la estructura jerárquica conjuntiva A es autorizado si para todo k, $1 \leq k \leq m$, se cumple que $a_1 + \ldots + a_k \geq t_k$.

4. Esquemas lineales

El esquema de Shamir mostrado en la sección 2.1 puede verse como un caso particular de los denominados esquemas lineales. En estos esquemas, a cada participante P_i se le asocia un subespacio vectorial F_i de dimensión d_i dentro de un espacio vectorial E de dimensión d. Fijando bases públicas B_i de cada subespacio F_i, y un vector adicional $\mathbf{v}_0$ para el secreto, la generación aleatoria de los fragmentos y del propio secreto se realiza del siguiente modo: Se toma un vector aleatorio $\mathbf{r}$ uniformemente distribuido en el espacio vectorial. El secreto generado es el producto escalar $s = \mathbf{r} \cdot \mathbf{v}_0$, mientras que a cada participante P_i le son entregados los productos escalares de $\mathbf{s}$ con los vectores de la base B_i de su subespacio. Es decir, P_i recibe el fragmento $s_i = \{\mathbf{r} \cdot \mathbf{v}_j \mid \mathbf{v}_j \in B_i\}$

Un conjunto A será autorizado si el vector $\mathbf{v}_0$ puede expresarse como combinación lineal de los vectores de las bases de sus participantes. El algoritmo de reconstrucción consiste en recuperar el secreto mediante la misma combinación lineal calculada ahora con los fragmentos. Concretamente, si $B_A = \bigcup_{P_i \in A} B_i$, entonces

$$\mathbf{v}_0 = \sum_{\mathbf{v}_j \in B_A} \lambda_j \mathbf{v}_j \quad \Rightarrow \quad s = \mathbf{r} \cdot \mathbf{v}_0 = \sum_{\mathbf{v}_j \in B_A} \lambda_j \, \mathbf{r} \cdot \mathbf{v}_j = \sum_{\mathbf{v}_j \in B_A} \lambda_j s_{i,j}.$$

En el esquema de Shamir, el espacio vectorial utilizado es $\mathbb{Z}_p^t$, que tiene dimensión igual al umbral t, y cada participante P_i está asociado a un único vector $\mathbf{v}_i = (1, x_i, x_i^2, \ldots, x_i^{t-1})$. El vector del secreto es $\mathbf{v}_0 = (1, 0, \ldots, 0)$, y el vector aleatorio elegido es el vector de los coeficientes del polinomio r, $\mathbf{r} = (a_0, a_1, \ldots, a_{t-1})$, donde $r(x) = a_0 + a_1 x + \ldots a_{t-1} x^{t-1}$. La interpolación de Lagrange utilizada en el esquema de Shamir es equivalente al cálculo de los coeficientes λ_j del esquema lineal.

De modo similar a lo que ocurre con los esquemas de umbral con pesos, la eficiencia de los esquemas lineales decrece cuando las dimensiones d_i de los subespacios de los participantes aumenta. Sin embargo, existe una variedad considerable de estructuras de acceso diferentes de la de umbral que son realizables incluso si todos los d_i valen 1 (estructuras ideales), igualando la eficiencia del esquema de Shamir en lo que respecta al tamaño de la información secreta custodiada por los participantes.

Aunque los esquemas lineales permiten realizar cualquier estructura de acceso, la determinación de la asignación de subespacios a los participantes que asegure una realización eficiente de una estructura arbitraria es un problema combinatorio de difícil solución. Por ello, las construcciones usuales

se restringen a familias concretas bien estudiadas, pero que aportan flexibilidad suficiente para la mayor parte de las aplicaciones.

Otra propiedad interesante de los esquemas lineales es que, al igual que el esquema de Shamir, éstos son aditivamente homomórficos. En efecto, si dos secretos han sido compartidos utilizando la misma asignación pública de vectores a los participantes, entonces sumar los vectores aleatorios es equivalente a sumar los secretos y los fragmentos de cada participante. Esto hace que gran número de protocolos criptográficos diseñados para funcionar con el esquema de umbral de Shamir puedan ser generalizados a cualquier esquema lineal, o como mínimo a cualquier esquema lineal ideal (es decir, donde $d_i = 1$).

Referencias

[1] A. Beimel. “Secret-sharing schemes: A survey”. Coding and Cryptology **6639**, 11–46, 2011.

[2] A. Beimel, T. Tassa, E. Weinreb. “Characterizing Ideal Weighted Threshold Secret Sharing”. SIAM J. Discrete Math. **22**, 360–397, 2008.

[3] A. Beimel, E. Weinreb. “Monotone Circuits for Monotone Weighted Threshold Functions”. Information Processing Letters **97**, 12–18, 2006.

[4] G.R. Blakley. “Safeguarding cryptographic keys”. En Proc. AFIPS **48**, 313–317, 1979. 2

[5] E.F. Brickell. “Some ideal secret sharing schemes”. J. Combin. Math. and Combin. Comput. **9**, 105–113, 1989.

[6] M.J. Collins. “A Note on Ideal Tripartite Access Structures”. Cryptology ePrint Archive: Report 2002/193. 2002. Online: `http://eprint.iacr.org/2002/193`.

[7] O. Farràs, J. Martí-Farré, C. Padró. “Ideal Multipartite Secret Sharing Schemes”. En Proc. EUROCRYPT 2007, Lecture Notes in Computer Science **4515**, 448–465. Springer, 2007.

[8] O. Farràs, C. Padró. “Ideal Hierarchical Secret Sharing Schemes”. En Proc. TCC 2010, Lecture Notes in Computer Science **5978**, 219–236. Springer, 2010.

[9] H. Ghodosi, J. Pieprzyk, R. Savavi-Naini. “Secret Sharing in Multilevel and Compartmented Groups”. En Proc. ACISP 98, Lecture Notes in Computer Science **1438**, 367–378. Springer, 1998.

[10] J. Herranz, G. Sáez. “New Results on Multipartite Access Structures”. En Proc. IEE Proceedings of Information Security 153, 153–162, 2006.

[11] M. Ito, A. Saito, T. Nishizeki. “Secret sharing scheme realizing any access structure”. En Proc. IEEE Globecom 1987, 99–102, IEEE Computer Society, Washington, DC, USA, 1987.

[12] E.D. Karnin, J.W. Greene, M.E. Hellman. “On secret sharing systems”. IEEE Trans. Inform. Theory **29**, 35–41, 1983.

[13] P. Morillo, C. Padró, G. Sáez, J.L. Villar. “Weighted Threshold Secret Sharing Schemes”. Inf. Process. Lett. **70**, 211–216, 1999.

[14] S.L. Ng. “Ideal secret sharing schemes with multipartite access structures”. IEE Proc.-Commun. **153**, 165–168, 2006.

[15] C. Padró, G. Sáez. “Secret sharing schemes with bipartite access structure”. IEEE Trans. Inform. Theory **46**, 2596–2604, 2000.

[16] C. Padró, G. Sáez. “Correction to Secret Sharing Schemes With Bipartite Access Structure”. IEEE Trans. Inform. Theory **50**, 1373–1373, 2004.

[17] A. Shamir. “How to share a secret”. Commun. of the ACM **22**, 612–613, 1979. 2

[18] G.J. Simmons. “How to (Really) Share a Secret”. En Proc. CRYPTO 1988, Lecture Notes in Computer Science **403**, 390–448. Springer, 1990.

[19] D.R. Stinson. “An explication of secret sharing schemes”. Des. Codes Cryptogr. **2**, 357–390, 1992.

[20] T. Tassa. “Hierarchical Threshold Secret Sharing”. J. Cryptology **20**, 237–264, 2007.

[21] T. Tassa, N. Dyn. “Multipartite Secret Sharing by Bivariate Interpolation”. J. Cryptology **22**, 227–258, 2009.