Criptografía Basada en Atributos

Javier Herranz
Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
E-mail: jherranz@ma4.upc.edu

RESUMEN

Con el progreso constante de las tecnologías digitales, se produce un rápido incremento de la información confidencial que debe gestionarse de manera correcta. La criptografía ofrece herramientas seguras y eficientes para asegurar autenticidad, integridad y confidencialidad en el mundo de la información digital. Sin embargo, la criptografía habitual considera un escenario concreto de comunicación entre dos usuarios, un emisor y un receptor.

Este escenario no cubre algunas de las situaciones prácticas que pueden aparecer en aplicaciones reales. Por eso, se están desarrollando nuevas técnicas criptográficas para hacer frente a estos nuevos escenarios. Un ejemplo es la criptografía basada en atributos, que fue introducida en 2005. En este trabajo hablaremos sobre este nuevo concepto: qué es, qué aplicaciones tiene, qué protocolos concretos se han propuesto, qué resultados hemos obtenido en la UPC, qué puntos quedan por resolver, etc.

1. INTRODUCCIÓN

La criptografía es una rama de la ciencia que puede situarse entre las matemáticas y la informática. El objetivo de la criptografía es proporcionar y analizar métodos que ofrezcan confidencialidad, integridad y autenticidad a las comunicaciones (digitales) entre usuarios. Hasta 1976, la criptografía que se utilizaba era simétrica: las dos personas que se comunican de manera confidencial / autentificada deben compartir una clave secreta común, K, que deben haber acordado previamente, de manera segura. Para cifrar y/o autentificar un mensaje, el emisor aplica un algoritmo que depende de K. Para descifrar y/o verificar la autentificación, el receptor aplica otro algoritmo que también depende de K.

La criptografía simétrica tiene ventajas, como su simplicidad conceptual o la existencia de protocolos muy eficientes (por ejemplo, AES) para llevar el concepto a la práctica. Sin embargo, tiene varios inconvenientes que limitan su aplicación directa en un escenario digital tan amplio y ubicuo como el que ofrece Internet. El primer inconveniente tiene que ver con la necesidad de acordar de manera secreta una clave común: ¿cómo puede acordarse una clave secreta, sin un encuentro físico real, en un entorno tan hostil como Internet, donde cada comunicación corre el riesgo de ser escuchada por usuarios deshonestos? El segundo inconveniente, quizás más serio aún, está relacionado con la cantidad de información secreta que debe almacenar cada usuario: si un usuario A debe compartir una clave secreta K_{AB} con cada usuario B, entonces deberá almacenar tantas claves secretas como usuarios con los que quiera comunicarse. En un mundo digital tan global como la Internet actual, esto sería completamente inviable.

Para evitar estos problemas, Diffie y Hellman [3] introdujeron en 1976 el concepto de criptografía *asimétrica* (o *criptografía de clave pública*). Cada usuario A genera un par de claves asociadas: una clave secreta sk_A y una clave pública pk_A. El usuario A almacena sk_A de manera segura (de hecho, ésta es la única información secreta que deberá almacenar), y publica pkA para que el resto de usuarios tengan acceso a ella. Paralelamente, A debe registrar pkA ante una autoridad de certificación, que asegura que la clave es válida mediante la emisión de un certificado digital. Si un usuario B quiere enviar un mensaje confidencial a A, después de verificar que la clave pública pk_A tiene un certificado válido, aplica un algoritmo de cifrado que depende de pk_A. El texto cifrado resultante sólo puede ser descifrado mediante un algoritmo que depende de la clave secreta sk_A; por tanto, A es el único que podrá acceder al mensaje original. De manera similar, si A quiere autentificar un mensaje, puede aplicar un protocolo de firma que depende de sk_A; la firma resultante, como sólo puede haber sido calculada por A, autentifica el mensaje. La corrección de la firma puede ser verificada por cualquier usuario, mediante un protocolo que depende de pk_A.

La aparición de la criptografía de clave pública supuso una auténtica revolución, puesto que permitió solucionar los problemas más graves de la criptografía clásica. Sólo faltaba encontrar protocolos concretos que llevasen el concepto a la práctica. La primera propuesta, en 1978, fue el sistema RSA [4]. Desde entonces, han aparecido muchos otros protocolos de cifrado de clave pública (confidencialidad) y de firma digital (integridad y autenticidad). Todos ellos deben satisfacer unas ciertas propiedades de seguridad; por ejemplo, que sea imposible (o inviable con la capacidad de cálculo actual)

descifrar un texto cifrado sin el conocimiento de la clave secreta correspondiente. Los protocolos no pueden satisfacer estas propiedades de manera absoluta; lo que se demuestra es que romper estas propiedades de seguridad (y atacar así el protocolo) es equivalente a resolver algún problema matemático computacional que se considera extraordinariamente difícil / costoso. Por ejemplo, el problema de factorizar un número entero que sea el producto de dos números primos muy grandes, o el problema de calcular el logaritmo discreto en un grupo cíclico con orden muy grande.

La criptografía de clave pública ofrece soluciones a muchas situaciones prácticas de hoy en día. Por ejemplo, el sistema RSA se utiliza en programas para cifrar y firmar correos electrónicos, para pago seguro por Internet, para conexión segura a servidores web, etc. Sin embargo, el uso masivo de las tecnologías de la información digitales, en ámbitos muy diversos, da pie a nuevas situaciones y nuevos problemas en los que hay que proteger información confidencial, pero en un escenario diferente al clásico escenario de un emisor y un receptor. Consideremos el siguiente ejemplo. Un consorcio de hospitales desea mantener un sistema informático para almacenar y gestionar los datos médicos de los pacientes: sus diagnósticos, tratamientos, resultados de análisis, etc. Evidentemente, se trata de información confidencial que debe estar al alcance de algunos actores (médicos, enfermeros) solamente, y no siempre: un enfermero de un hospital no debería tener acceso a la información sobre pacientes que no estén a su cargo, o incluso a alguna parte de la información de sus propios pacientes. La solución debe utilizar algún tipo de mecanismo criptográfico para cifrar la información. Sin embargo, si se consideran esquemas de cifrado de clave pública convencionales, únicamente, el sistema resultante es muy ineficiente. Veamos un ejemplo: supongamos que la totalidad de la información relativa a un paciente P_i, con problemas coronarios, ingresado en un cierto hospital H_j, debe estar al alcance de:

- el médico de H_j que es responsable de P_i,

- médicos de cualquier otro hospital del consorcio que sean especialistas en enfermedades coronarias,

- los directores de todos los hospitales del consorcio.

A su vez, una parte de la información relativa a P_i (por ejemplo, el tratamiento a seguir) debe estar al alcance de los enfermeros que se ocupan de P_i, y también de los encargados de la sección farmacéutica del hospital H_j.

Si pensamos en una solución basada en criptografía de clave pública convencional, donde cada actor tiene su par de claves secreta y pública, cada vez que se introdujese información en el sistema, debería cifrarse con las claves públicas de todos los actores autorizados. Es decir, los resultados de los análisis de P_i, su diagnóstico, su tratamiento, etc. deberían cifrarse con las claves públicas del médico responsable de P_i, de todos los especialistas en enfermedades coronarias, de todos los directores de hospitales. La información relativa al tratamiento también se debería cifrar con las claves públicas de los enfermeros que se ocupan de P_i y de los farmacéuticos de H_j. Como resultado, el sistema debería almacenar una cantidad de información cifrada demasiado elevada, lo cual haría bastante inviable su implementación.

Para resolver este tipo de problemas, se ha introducido recientemente el concepto de criptografía basada en atributos. La idea es la siguiente: cada usuario del sistema tiene un conjunto de atributos *AT*, y recibe de un servidor central una cierta clave secreta sk_{AT} que depende de dichos atributos. Por ejemplo, un médico M_t especialista en enfermedades coronarias que trabaje en el hospital H_s recibirá una clave secreta para los atributos at_1='identidad Mt', at_2='hospital H_s', at_3='especialista enfermedades coronarias'. Después, cuando haya que cifrar la información confidencial de los pacientes, se escogerá para cada tipo de información una política de descifrado: qué atributos (como mínimo) debe poseer un usuario para poder descifrar y obtener la información confidencial. En nuestro ejemplo, para los resultados de los análisis médicos del paciente P_i, si el médico encargado de P_i es M_p, la política sería: 'identidad M_p' Ó 'especialista enfermedades coronarias' Ó 'director de hospital'. Para el tratamiento a seguir por el paciente P_i, si E_a y E_b son los enfermeros a cargo de P_i, a la política de descifrado previa habría que añadir: Ó 'enfermero E_a' Ó 'enfermero E_b' Ó ('farmacéutico' Y 'hospital H_j').

En este trabajo discutiremos el concepto de criptografía basada en atributos, dando un enfoque que pretende ser mínimamente formal y divulgativo a la vez. Repasaremos los protocolos que forman parte en un sistema de cifrado basado en atributos; explicaremos qué requisitos de seguridad deben exigirse a estos sistemas; haremos un resumen de las propuestas que se han hecho hasta ahora, enfatizando los aspectos a mejorar; mencionaremos los resultados sobre este tema que hemos obtenido desde el grupo MAK–UPC, así como las líneas de investigación que tenemos abiertas actualmente; por último, mostraremos cómo el concepto de criptografía basada en atributos podría utilizarse para implementar sistemas de

control de acceso que preserven el anonimato de los clientes.

2. CIFRADO BASADO EN ATRIBUTOS

Un sistema de cifrado basado en atributos (para simplificar, escribiremos ABE, del inglés '*attribute-based encryption*') consiste en los siguientes protocolos.

- Inicialización: se generan los parámetros públicos *pms* que van a ser comunes a los usuarios del sistema (por ejemplo, el conjunto total de atributos *U*), así como la clave secreta, *msk*, del servidor autorizado que repartirá las claves secretas a los usuarios.

- Obtención de claves: un usuario demuestra al servidor autorizado que posee un subconjunto *AT* de atributos. Como respuesta, obtiene una clave secreta sk_{AT}.

- Cifrado: un usuario que quiere esconder una información o mensaje confidencial *m* escoge una política de descifrado, que siempre puede describirse como una familia Γ de subconjuntos de *U*: aquellos subconjuntos de atributos que, en caso de ser poseídos por un usuario, permitirán el descifrado correcto. El resultado del protocolo de cifrado es un texto cifrado *C*.

- Descifrado: un usuario cuyo subconjunto de atributos *AT* pertenece a la familia Γ puede utilizar su clave secreta sk_{AT} para descifrar *C* y recuperar la información original *m*.

2.1. Propiedades de Seguridad Requeridas

Como todos los sistemas de cifrado, un esquema ABE debe satisfacer una condición básica de seguridad: los usuarios que en teoría no están autorizados a descifrar un texto cifrado no deben obtener ninguna información sobre el mensaje que ha sido cifrado. Para formalizar este requisito, se considera la situación más ventajosa para un adversario que intentase atacar el sistema de cifrado: se supone que el adversario escoge dos mensajes m_0 y m_1, y que el texto cifrado corresponde a uno de esos dos mensajes; el adversario, que no conoce las claves secretas necesarias para descifrar correctamente el texto cifrado, debe intentar adivinar cuál de los dos mensajes ha sido cifrado. Si existe algún adversario que acierta con probabilidad significativamente superior a ½ (esta probabilidad se obtiene trivialmente con una elección al azar), eso quiere decir que el sistema de cifrado está filtrando alguna información, y por tanto se considera que no es seguro.

En el caso del cifrado basado en atributos, un buen sistema debe ser capaz de resistir *ataques* por *coalición*. Es decir, si varios usuarios no cumplen, por separado, la política de descifrado, pero juntando sus atributos sí que se cumple dicha política, tampoco deben ser capaces de descifrar un texto cifrado que corresponda a esa política, aunque compartan sus claves secretas. En nuestro ejemplo de la Sección 1, supongamos que un enfermero que trabaja en el hospital H_j, pero que no es ni E_a ni E_b (los enfermeros a cargo del paciente P_i) confabula con un farmacéutico del hospital H_s, donde $s \neq j$. Por separado, ninguno de estos dos usuarios tienen derecho a acceder al tratamiento del paciente P_i, pero si juntasen sus atributos, se obtendría el subconjunto 'farmacéutico' Y 'hospital H_j', que sí que pertenece a la política de descifrado. El diseño del sistema debe asegurar que estos dos usuarios no serán capaces de obtener ninguna información sobre el tratamiento del paciente P_i, aunque se intercambien sus claves secretas.

Estos requisitos que hemos explicado informalmente en estos dos párrafos se pueden formalizar con un experimento entre un retador y un adversario *Adv*. El adversario puede obtener claves secretas para todos los subconjuntos de atributos que quiera, siempre que ninguno de estos subconjuntos pertenezca a la política de descifrado, naturalmente. Al otorgar esta información al adversario, se modela la situación de un ataque por coalición. El objetivo es que el adversario sea incapaz de adivinar qué mensaje se ha cifrado, entre los dos que escoge él mismo. El juego es el siguiente:

(1) El adversario *Adv* escoge una política de descifrado Γ que quiere atacar.
(2) El retador ejecuta el protocolo de Inicialización, mantiene *msk* en secreto y envía a *Adv* la información pública pms.
(3) *Adv* puede pedir al retador las claves secretas correspondientes a subconjuntos de atributos AT_i de su elección, siempre que AT_i no pertenezca a Γ. El retador ejecuta el protocolo de obtención de claves, y envía a *Adv* las claves sk_{ATi} correspondientes.
(4) *Adv* escoge dos mensajes m_0 y m_1.
(5) El retador escoge al azar un número *b* (ó el 0 ó el 1), y ejecuta el protocolo de cifrado para el mensaje mb y la política de descifrado Γ. El texto cifrado resultante, C*, se envía a *Adv*.
(6) El paso (3) se repite.
(7) Finalmente, *Adv* devuelve un valor *b'* (ó 0 ó 1).

Un adversario tiene éxito en dicho experimento si su probabilidad de acertar, es decir, de obtener *b'=b*, es significativamente mayor a ½. Si un sistema ABE cumple que ningún adversario con capacidad de cálculo razonable puede tener éxito en este

experimento, entonces el sistema ABE se considera seguro.

3. ESTADO DEL ARTE EN SISTEMAS ABE

El concepto de cifrado basado en atributos fue introducido por Sahai y Waters en [5]. En ese artículo, propusieron un sistema ABE pero que funciona sólo para políticas de descifrado de tipo umbral (es decir, se necesita poseer como mínimo *t* atributos para poder descifrar) y además el umbral *t* se fija al principio y no se puede cambiar según la información que se desee cifrar. Por tanto, el sistema no tiene suficiente flexibilidad como para ser usado en situaciones prácticas (como nuestro ejemplo hospitalario).

El primer sistema ABE que admitía políticas de descifrado más flexibles fue propuesto por Bethencourt, Sahai y Waters en [1]. Las políticas que admite este esquema son las que pueden representarse mediante un árbol en el que las hojas representan los atributos, y cada nodo interno representa una puerta de tipo umbral. De hecho, las políticas de descifrado de nuestro ejemplo hospitalario pertenecen a este tipo, puesto que un 'Ó' puede representarse mediante una puerta de umbral en la que el umbral es igual a 1, y un 'Y' puede representarse como una puerta de umbral en la que el umbral es igual al número de inputs que tiene la puerta. Sin embargo, este sistema tiene la limitación que, en los árboles que representan la política de descifrado, cada atributo (hoja del árbol) puede colgar sólo de un nodo-puerta de umbral. Esto hace que sea imposible, por ejemplo, realizar una política de acceso como $\Gamma = (at_1$ Y at_2 Y $at_3)$ Ó $(at_2$ Y at_4 Y $at_5)$ Ó $(at_3$ Y $at_5)$.

Recientemente, otros artículos han propuesto sistemas ABE que solucionan este problema, puesto que permiten realizar políticas de descifrado más generales, de hecho cualquier política de descifrado Γ que sea monótona creciente: si un subconjunto AT_1 pertenece a Γ, y AT_2 contiene a AT_1, entonces AT_2 debe pertenecer a Γ, también. Estos sistemas ABE, propuestos por Waters [7] y por Daza, Herranz, Morillo y Ràfols [2], utilizan como herramienta el concepto de los esquemas para compartir secretos [6].

3.1. Problemas Abiertos

Todos los sistemas ABE que hemos mencionado en la sección anterior tienen diversos inconvenientes, entre los que se pueden destacar tres.

(1) La longitud de los textos cifrados C siempre depende (como mínimo, de manera lineal) del número total de atributos que aparecen en la política de descifrado Γ. Por ejemplo, si una política umbral de descifrado se define como 'poseer al menos *t* atributos de entre una lista (amplia) de *n* atributos', entonces los textos cifrado de los esquemas existentes hasta ahora contendrán al menos *n* elementos (o 2(*n*-*t*) elementos, en el caso del esquema en [2]). Esto es un problema en el caso de querer cifrar información para políticas de descifrado complejas en las que estén involucrados muchos atributos.

(2) En el diseño de todos los sistemas ABE propuestos hasta ahora, se usa un tipo de objeto matemático, los emparejamientos bilineales (*bilinear pairings*, en inglés). Son un tipo de aplicación entre grupos matemáticos, e: $G \times G \rightarrow G_T$, donde G y G_T son grupos con el mismo orden q, que cumplen que $e(g^a,g^b)=e(g,g)^{ab}$, para cualquier elemento $g \in G$ y cualquier par de números $a,b \in \{0,1,...,q-1\}$. Los emparejamientos bilineales se han utilizado mucho en los últimos años para diseñar nuevos protocolos criptográficos, ya que permiten obtener funcionalidades que no se saben implementar sin ellos. El cifrado basado en atributos es un ejemplo. Sin embargo, los emparejamientos bilineales tienen aspectos negativos de cara a la implementación de estos sistemas: sólo se conocen ejemplos de emparejamientos bilineales en grupos asociados a algunas curvas elípticas, y son conceptualmente muy complicados. Esta complicación se traduce en el hecho de que calcular un emparejamiento para dos elementos de G es bastante ineficiente, y por tanto la eficiencia global de los sistemas ABE actuales no es del todo satisfactoria.

(3) La seguridad de los sistemas ABE propuestos hasta ahora se demuestra en relación a la dificultad de resolver algunos problemas matemáticos computacionales (como siempre en criptografía moderna) que no son muy conocidos, sino que han ido apareciendo 'on-line' a la vez que se diseñaban los sistemas ABE. Por tanto, aún no ha habido tiempo para estudiar estos problemas matemáticos detenidamente, para convencerse de que son realmente difíciles de resolver.

Desde el grupo de Matemática Aplicada a la Criptografía (MAK), http://www-ma4.upc.edu/mak , del Departamento de Matemática Aplicada IV de la Universitat Politècnica de Catalunya (UPC) estamos trabajando para intentar solucionar alguno de estos inconvenientes. En un trabajo que está actualmente bastante avanzado, junto con Carla Ràfols (MAK-UPC) y Fabien Laguillaumie (Université de Caen, Francia), estamos diseñando un sistema ABE que produce

textos cifrados C de longitud constante, independientemente del número de atributos involucrados en la política de descifrado. Disponemos ya de un sistema seguro para el caso de políticas de umbral (con un umbral t flexible que puede elegir la persona que cifra cada vez), y ahora estamos intentando adaptarlo para que funcione con políticas de descifrado más expresivas, por ejemplo las que se pueden representar mediante un árbol con puertas de umbral.

Además, junto con Paz Morillo, Carla Ràfols, Àlex Escala y Carlos Luna (MAK-UPC) estamos intentando diseñar un sistema ABE que no utilice emparejamientos bilineales. Da la impresión que se trata de un problema realmente difícil, todo un reto para nosotros, pero el tema es apasionante y los conceptos matemáticos que estamos investigando en nuestros intentos son realmente interesantes.

4. OTRA APLICACIÓN DE LOS SISTEMAS ABE: CONTROL DE ACCESO ANÓNIMO

En esta última sección del artículo vamos a explicar otro ejemplo de una situación real en la que se pueden utilizar los sistemas de cifrado basados en atributos para obtener una solución satisfactoria. Se trata de diseñar un sistema de control de acceso en el que se preserve el anonimato del cliente (autorizado) que accede a determinados recursos. Por ejemplo, en muchos sitios web (clubs, tiendas, foros), los usuarios tienen acceso a diferentes partes / recursos del sitio, en función de su status, de la cuota que hayan pagado, de su edad, etc. La solución habitual es que cada usuario debe completar un proceso de registro, en el que se verifica que dicho usuario cumple los requisitos que dice cumplir. Se guarda un perfil del usuario, de manera que en el futuro, cuando el usuario accede al sitio, debe identificarse (normalmente mediante un nombre de usuario y una contraseña). El servidor detecta el perfil del usuario y automáticamente el sitio web queda personalizado para que el usuario tenga acceso sólo a los recursos para los que está autorizado según su perfil. Desafortunadamente, esta solución no proporciona ningún nivel de anonimato / privacidad al usuario, puesto que el servidor del sitio web controla completamente qué usuario está accediendo en ese momento a qué recursos.

En un sistema ideal, el servidor no debería ser capaz de identificar al usuario; sólo debería estar seguro de que los usuarios que están accediendo a determinados recursos tienen realmente derecho a hacerlo. Es decir, un usuario que accede a un sitio web no tendría que dar más información que la estrictamente necesaria, y que en este caso no es otra que el hecho de cumplir los requisitos necesarios para acceder a esos recursos. Por ejemplo, para acceder a recursos reservados a personas mayores de edad, un usuario sólo tendría que demostrar que tiene más de 18 años, sin tener que difundir su nombre ni su DNI ni su fecha de nacimiento.

La criptografía basada en atributos ofrece una solución a este problema. El servidor encargado del sitio web hace el trabajo del servidor autorizado que reparte las claves secretas. Cada usuario completa inicialmente un proceso de registro con el servidor, en el que se le asigna una clave secreta en función de sus atributos; algunos ejemplos de atributos en esta situación podrían ser 'mayor de edad', 'miembro del club con categoría A / B / C', 'persona con tarjeta de crédito registrada', etc. Después, para acceder a cada recurso protegido del sitio web, un usuario deberá superar un reto propuesto por el servidor (de manera automatizada, claro): el servidor habrá definido anteriormente una política de acceso para ese determinado recurso, incluyendo los atributos mínimos que debe poseer un usuario para poder acceder. Entonces, se escoge un mensaje m al azar y se cifra mediante el sistema ABE, tomando como política de descifrado la política de acceso correspondiente. Si el usuario es capaz de descifrar y dar como respuesta el mensaje m, entonces el servidor estará convencido que el usuario posee los atributos necesarios, y por tanto está autorizado a acceder a ese recurso. De esta manera, el servidor no obtiene ninguna información sobre la identidad de los usuarios que están intentando acceder al sitio, ni sobre qué atributos en concreto posee cada uno de ellos.

A pesar de que hemos usado como ejemplo ilustrativo el caso de un sitio web, existen muchas otras situaciones en las que un sistema de control de acceso anónimo es deseable, por ejemplo para gestionar el control de acceso a infraestructuras que pueden ser críticas: empresas, aeropuertos, edificios gubernamentales, instalaciones militares, etc. En estos casos, el sistema podría implementarse mediante lectores de tarjetas inteligentes o dispositivos RFID que se repartirían entre los usuarios, con las claves secretas ya integradas, dependiendo de sus atributos. Puesto que estos dispositivos tienen unas capacidades computacionales y de memoria bastante más limitadas que un ordenador convencional (usado por los clientes en el ejemplo de los sitios web), cualquier avance en el diseño de sistemas ABE más eficientes será bienvenido. La eficiencia se mide por la longitud de los parámetros públicos pms, la longitud de las claves secretas sk_{AT}, la longitud de los textos cifrados

C, y el número de operaciones para cifrar y descifrar.

5. CONCLUSIONES

Este artículo pretende ser una aproximación divulgativa pero precisa al concepto de la criptografía basada en atributos. Como hemos podido observar, este tipo de esquemas puede ser una herramienta muy potente para implementar soluciones satisfactorias a problemas de la vida real que tratan con información y recursos confidenciales.

La criptografía basada en atributos es un concepto que ha sido introducido recientemente, y por tanto hay muchas posibilidades abiertas para trabajar y obtener nuevos resultados que mejoren el estado del arte. Es lo que estamos haciendo (o intentando) desde el grupo de investigación MAK de la Universitat Politècnica de Catalunya.

REFERENCIAS

[1] J. Bethencourt, A. Sahai y B. Waters. 'Ciphertext-policy attribute-based encryption'. En Proceedings of IEEE Symposium on Security and Privacy, IEEE Society Press, pág. 321-334 (2007).

[2] V. Daza, J. Herranz, P. Morillo y C. R\'afols. 'Extended access structures and their cryptographic applications'. Manuscrito disponible en http://eprint.iacr.org/2008/502 (2008).

[3] W. Diffie y M.E. Hellman. 'New directions in cryptography'. En IEEE Transactions on Information Theory, vol. 22, núm. 6, pág. 644-654 (1976).

[4] R.L. Rivest, A. Shamir y L. Adleman. 'A method for obtaining digital signatures and public key cryptosystems'. En Communications of the ACM, vol. 21, pág. 120-126 (1978).

[5] A. Sahai y B. Waters. 'Fuzzy identity-based encryption'. En Proceedings of Eurocrypt'05, Lecture Notes in Computer Science 3494, Springer-Verlag, pág. 457-473 (2005).

[6] J.L. Villar, C. Padró y G. Sáez. 'Compartición de secretos en criptografía'. En la revista BURAN, Student Section of IEEE (1997).

[7] B. Waters. 'Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization'. Manuscrito disponible en http://eprint.iacr.org/2008/290 (2008).

AUTOR

Javier Herranz es licenciado en Matemáticas por la Universitat Politècnica de Catalunya (FME, 2000) y Doctor en Matemática Aplicada por la misma universidad (FME, 2005). Ha trabajado como investigador post-doctoral en la École Polytechnique (LIX; Palaiseau, Francia, 2005), en el Centrum voor Wiskunde en Informatica (CWI; Amsterdam, Holanda, 2006) y en el Institut d'Investigació en Intel•ligència Artificial (IIIA-CSIC; Bellaterra, España, 2007-08). Desde enero de 2009 trabaja como profesor e investigador en el grupo de Matemàtica Aplicada a la Criptografia (MAK) del Departament de Matemàtica Aplicada IV de la UPC, con un contrato Ramón y Cajal. Su investigación se centra en aspectos relacionados con la criptografía, en particular con el diseño y análisis de protocolos criptográficos de firma y cifrado que tengan algunas propiedades especiales: firmas distribuidas, firmas de anillo, cifrado basado en atributos, cifrado con propiedades homomórficas, etc. Más información sobre sus trabajos puede encontrarse en su web personal: http://www-ma4.upc.edu/~jherranz/