Criptoanálisis del esquema de dinero cuántico de clave pública de Aaronson y Christiano

Marta Conde Pena, Luis Hernández Encinas
Consejo Superior de Investigaciones Científicas (CSIC)
E-28006 Madrid, Spain
Correo-e: {marta.conde, luis}@iec.csic.es

Raúl Durán Díaz
Departamento de Automática, Universidad de Alcalá
E-28871 Alcalá de Henares, Spain
Correo-e: raul.duran@uah.es

Jean-Charles Faugère, Ludovic Perret
Sorbonne Universités, UPMC Univ Paris 06 POLSYS, UMR 7606, LIP6
F-75005 Paris, France
Correo-e: jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr

***Resumen*—En este trabajo se presenta un criptoanálisis del esquema de dinero cuántico propuesto por Aaronson y Christiano que se deriva de la existencia de algoritmos no cuánticos de tiempo polinómico probabilístico capaces de resolver los problemas de los subespacios ocultos con y sin ruido en que dicho esquema está basado.**

***Palabras clave*—Dinero cuántico, clave pública, problema de los subespacios ocultos, polinomios no lineales en varias variables, bases de Gröbner.**

I. Introducción

El extraordinario crecimiento experimentado durante los últimos años en las telecomunicaciones y en la capacidad para almacenar y procesar información han traído consigo desarrollos quizá inesperados, como por ejemplo, la aparición de alternativas digitales para el dinero contante y sonante. En este ámbito, podemos destacar dos líneas de investigación.

Por un lado, se trabaja en las «criptodivisas», criptomonedas o dinero digital. Ese dinero digital debe ofrecer las mismas propiedades y capacidades que el dinero físico, pero estando disponible solo de manera digital. La idea del dinero digital se remonta a 1982, cuando fue introducida por Chaum [1] y empezaron a surgir las primeras propuestas, como DigiCash, E-gold, o Liberty Reserve. Lamentablemente, todas ellas terminaron fracasando.

Unos años más tarde, la introducción de Bitcoin en 2008 por Nakamoto [2], [3] renovó el interés por la divisa electrónica, que se ha hecho popularmente conocida gracias a él. Anecdóticamente, Nakamoto parece ser un seudónimo que oculta la verdadera personalidad del inventor, quien ha permanecido en la sombra hasta el momento presente.

El otro campo de estudio trata sobre lo que es conocido como dinero cuántico. Contrariamente a lo que ocurre con la divisa electrónica, el dinero cuántico es tangible, no digital, pero trata de servirse de las propiedades derivadas de las leyes cuánticas de la Física para conseguir que una falsificación sea realizable tan solo con una probabilidad despreciable. Los primeros trabajos en esta línea se remontan a Wiesner, que empezó a elaborar una propuesta hacia 1969, aunque no se publicó hasta mucho más tarde [4]. La propuesta de Wiesner presentaba algunos inconvenientes, pero puede considerarse como el fundamento de lo que se ha dado en llamar *dinero cuántico*.

En el año 2009, Aaronson [5] introdujo por vez primera el concepto de «dinero cuántico de clave pública», que aporta como novedad esencial su capacidad de verificación, no tan solo por el emisor, sino por cualquier usuario: es una verificación completamente universal. En un trabajo posterior [6], Aaronson y Christiano proponen un esquema de dinero cuántico que se apoya en la propiedad cuántica de no clonación y la supuesta dificultad para resolver dos problemas novedosos introducidos por los autores: el *problema de los subespacios ocultos* (HSP) y el *problema de los subespacios ocultos con ruido* (NHSP). Los autores conjeturaron que no existían algoritmos cuánticos de tiempo polinómico eficaces para resolver tales problemas.

Esta contribución presenta de manera divulgativa, sin demostraciones rigurosas, un resumen condensado del criptoanálisis realizado por los autores de los esquemas propuestos por Aaronson y Christiano. Nuestro resultado muestra que las conjeturas de Aaronson y Christiano se han revelado erróneas: hacemos ver que, de hecho, existen algoritmos clásicos (ni siquiera cuánticos) que resuelven en tiempo polinómico probabilístico los problemas en que se apoyan, contra lo que ellos habían supuesto. Aunque estos resultados ya han sido publicados [7], [8] nos parecen suficientemente relevantes como para darlos a conocer, resumidamente, en el ámbito del habla española en donde pensamos que estos estudios no son tan populares.

Este trabajo se estructura de este modo: presentamos en la sección II unas ideas orientativas acerca de las propiedades de la Física cuántica que son aprovechadas para crear el dinero cuántico. Equipados con esas ideas, introducimos en la sección III el esquema de dinero cuántico de Aaronson y Christiano. Las secciones siguientes, IV y V, describen los problemas HSP y NHSP junto con los algoritmos que los resuelven, al menos heurísticamente. Con ello se puede considerar criptoanalizada la propuesta de Aaronson y Christiano. Para finalizar, proporcionamos en la sección de conclusiones un resumen de los resultados logrados.

II. Física cuántica y dinero cuántico

Las propiedades cuánticas de la materia pueden ser también aprovechadas para construir *sistemas de información cuánticos*. Típicamente, en un sistema cuántico encontramos dos

estados (cuánticos), a los que es tradicional llamar $|0\rangle$ y $|1\rangle$. La novedad en este caso es que un sistema cuántico puede encontrarse no solo en dos estados definidos, sino en una superposición cualquiera de ellos, que podemos representar como un vector de norma unitaria $|\Psi\rangle = c_0|0\rangle + c_1|1\rangle$, con $c_0, c_1 \in \mathbb{C}$, y $|c_0|^2 + |c_1|^2 = 1$. Este bit, tan especial, se denomina *qubit*.

La interpretación física es que el qubit en el estado $|\Psi\rangle$ puede encontrarse en *ambos estados* con probabilidades $|c_0|^2$ y $|c_1|^2$. Medir el qubit equivale a proyectar el vector sobre la base estándar, con lo que obtendremos como resultado el valor $|0\rangle$ con probabilidad $|c_0|^2$ y el valor $|1\rangle$ con probabilidad $|c_1|^2$.

En principio, un qubit podría realizarse con cualquier sistema biestado como, por ejemplo, dos estados de polarización de un fotón con polarización lineal $|V\rangle$, $|H\rangle$, o circular $|L\rangle$, $|R\rangle$; dos estados de espín, en un núcleo o en un electrón; o dos niveles energéticos de estado de un átomo.

La propuesta de Wiesner para crear dinero cuántico consiste en dotar a cada billete de un número de serie, s, y un estado cuántico, $|\Psi_s\rangle$, que puede consistir en n fotones polarizados en direcciones elegidas aleatoriamente con igual probabilidad entre los estados $\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$. Para poder medir cada qubit, es necesario usar la base correcta: cuando se trate de los dos primeros, ha de usarse la base $\{|0\rangle, |1\rangle\}$; para los dos últimos, ha de usarse, en cambio, $\{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$. Solo quien sepa cuáles son los bits los medirá con la base apropiada. Si se mide con la base equivocada, el valor obtenido es perfectamente aleatorio, pues las bases están giradas 45^{o}.

El banco emisor del billete debe mantener una base de datos que relacione s con una descripción *clásica* del estado cuántico. Para verificar la autenticidad del billete, el tenedor ha de llevarlo al banco emisor que, tras consultar su base de datos, mide cada qubit en la base adecuada y comprueba si se obtiene lo correcto. El teorema de no clonación asegura que es imposible crear una copia perfecta de un estado cuántico arbitrario desconocido. Como se demuestra en [9], quien no conozca las bases podría llegar a conseguir falsificar un billete con una probabilidad de solo $(3/4)^n$ en el mejor de los casos, siendo n el número de fotones en el billete.

Aunque la idea de Wiesner es atractiva, también presenta varios inconvenientes: solo el banco emisor puede verificar los billetes; el proceso de verificación puede dar lugar a un ataque *on-line*; y, en fin, la base de datos crecería enormemente.

III. Esquema de Aaronson y Christiano

Para crear un billete, el banco toma el número de serie, s, y la descripción clásica de un cierto subespacio, A, con la cual prepara un estado cuántico $|A\rangle$ y, finalmente, publica $(s, |A\rangle)$. La verificación propuesta se apoya en llamadas a un oráculo clásico que comprueba la pertenencia del estado a los espacios A o su ortogonal $A^\perp$. El oráculo propuesto se basa en propiedades de sistemas de polinomios no lineales en varias variables. Dada una colección de polinomios $p_1, \ldots, p_m \in \mathbb{F}_2[\mathbf{x}]$, donde $\mathbf{x} = (x_1, \ldots, x_n)$, resulta *difícil*, en términos generales, hallar un punto $v \in \mathbb{F}_2^n$ que anule simultáneamente los m polinomios; sin embargo, es bien sencillo comprobarlo para un punto dado. La idea de los autores es «ocultar» el subespacio A detrás de ese conjunto de polinomios, $p_1, \ldots, p_m$ elegidos aleatoriamente de entre los que se anulan en todo punto de A. Análogamente, $A^\perp$ se «oculta» tras un conjunto de polinomios $q_1, \ldots, q_m \in \mathbb{F}_2[\mathbf{x}]$. Naturalmente, estos conjuntos de polinomios son públicamente conocidos, lo que garantiza la verificabilidad universal. Los autores hablan entonces del *problema de los subespacios ocultos* o HSP, por sus iniciales en inglés.

Incidentalmente, el problema HSP se relaciona estrechamente con el problema del isomorfismo de polinomios (IP), introducido por Patarin en 1996 [10], que es relevante precisamente en criptografía cuadrática multivariante [11].

Para mayor seguridad, los autores proponen añadir a los polinomios mencionados otros elegidos de modo totalmente aleatorio que, obviamente, ya no se anulan ni en A ni en su complementario ortogonal: son polinomios que introducen *ruido* que, en principio, puede hacer el problema más difícil aún de resolver. Hablamos entonces del problema de los subespacios ocultos con ruido o NHSP.

En relación con este problema NHSP, los autores conjeturan [6, Conj. 6.7] que, dado un subespacio A, no existe ningún algoritmo cuántico de tiempo polinómico que permita recuperar A o $A^\perp$ (es decir, resolver el NHSP) con probabilidad $\Omega\left(2^{-n/2}\right)$ donde Ω representa la función asintótica estándar.

Con esta comunicación pretendemos difundir nuestros trabajos en relación con ambos problemas, HSP y NHSP, y su aplicación al dinero cuántico. En [7] obtenemos resultados para el caso HSP. En particular, demostramos que cuando el cuerpo base es un cuerpo primo $\mathbb{F}_t$, con $t \neq 2$, la conjetura anterior queda totalmente desechada y que para el caso $\mathbb{F}_2$ también queda descartada suponiendo cierta una conjetura que la experimentación confirma ampliamente. El caso del problema NHSP está tratado en [8] en donde explicamos que existe un algoritmo clásico de tiempo polinómico probabilístico que tiene éxito con probabilidad $\Omega\left(2^{-n/2}\right)$ cuando la proporción de polinomios ruidosos se mantiene dentro de cierto rango: con ello queda también descartada la conjetura de Aaronson y Christiano para el caso NHSP.

IV. Problema de los subespacios ocultos (HSP)

De manera más formal, fijemos algunas notaciones. Denotamos por $\mathbb{F}_t$ un cuerpo finito de orden primo, t, y por $\mathbb{F}_t[\mathbf{x}]$ el anillo de polinomios en n variables (n se asume siempre par) sobre $\mathbb{F}_t$, con $\mathbf{x} = (x_1, \ldots, x_n)$. Definimos $(\mathbf{p}, \mathbf{q}) = ((p_1, \ldots, p_m), (q_1, \ldots, q_m)) \in \mathbb{F}_t[\mathbf{x}]^m \times \mathbb{F}_t[\mathbf{x}]^m$ como un par compuesto de m-tuplas de polinomios, $n \leq m \leq 2n$, cada uno de ellos en el anillo $\mathbb{F}_t[\mathbf{x}]$, de grado $d \geq 3$.

IV-A. *Computación de una base de Gröbner*

En este trabajo uno de los ingredientes clave está constituido por sistemas de polinomios no lineales en varias variables, para los que resulta de mucho interés una herramienta denominada *bases de Gröbner*. Para explicarla, supongamos un sistema de s polinomios en n variables sobre $\mathbb{F}_t$ y definamos el ideal polinómico generado por tales polinomios como $\mathcal{I} = \langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^s f_i h_i \mid h_1, \ldots, h_s \in \mathbb{F}_t[\mathbf{x}]\}$. A partir de un ideal, definimos la variedad algebraica $\mathcal{V}_t(\mathcal{I})$ como el conjunto de puntos de $\mathbb{F}_t^n$ que son ceros comunes a todos los polinomios de $\mathcal{I}$, es decir, $\mathcal{V}_t(\mathcal{I}) = \{\mathbf{x} \in \mathbb{F}_t^n \mid f_i(\mathbf{x}) = 0, 1 \leq i \leq s\}$. El teorema de la base de Hilbert (véase, por ejemplo, [12, Th. 4, §5, Ch. 2]) garantiza

que todo ideal polinómico admite siempre una base finita de polinomios generadores. Pues bien, una base de Gröbner para un ideal proporciona un conjunto nuevo de generadores para tal ideal (y, por ende, para la misma variedad) con «mejores propiedades» para trabajar computacionalmente con el ideal y la variedad.

El algoritmo original para calcular una base de Gröbner se debe a Buchberger, pero a día de hoy existen métodos más eficientes, como el F_5 [13]. Este método itera un proceso que va reduciendo a forma diagonal una matriz cuyas filas son los coeficientes de $m_j f_{i_j}$, $1 \leq j \leq s$, ordenados según un orden lexicográfico elegido, donde los m_j son monomios tales que en cada paso del algoritmo el grado de $m_j f_{i_j}$ es menor o igual que cierto $\bar{r}$. El algoritmo termina cuando la matriz está diagonalizada: en ese momento contiene los coeficientes de una base de Gröbner. El valor máximo que haya alcanzado $\bar{r}$ a lo largo de la ejecución del algoritmo se denomina *grado de regularidad*, r, y es de interés porque la complejidad computacional del F_5 es $\mathcal{O}\left(n^{r\omega}\right)$.

El valor $2 \leq \omega \leq 3$ recibe el nombre de *exponente de multiplicación de matrices* puesto que influye de manera exponencial en el tiempo de computación empleado para multiplicar dos matrices. Concretamente, indica que existe un algoritmo capaz de multiplicar dos matrices $k \times k$ en tiempo computacional $\mathcal{O}(k^\omega)$ (ver, por ejemplo, [14, cap. 12]).

IV-B. Algoritmo para el HSP$_t$

Con las notaciones anteriores, definimos el problema de los subespacios ocultos sin ruido en $\mathbb{F}_t$ (HSP$_t$) de la siguiente manera: dados dos conjuntos de polinomios, $(\mathbf{p}, \mathbf{q}) \in \mathbb{F}_t[\mathbf{x}]^m \times \mathbb{F}_t[\mathbf{x}]^m$, encontrar un subespacio $A \subset \mathbb{F}_t^n$ de dimensión $n/2$ tal que $p_i(A) = 0$, $q_j(A^\perp) = 0$ para todo $i, j \in \{1, \ldots, m\}$, donde $A^\perp$ es el complemento ortogonal de A con respecto al producto escalar estándar.

Para el caso en que $t > d \geq 3$, tenemos el siguiente resultado [7, Th. 3]:

Teorema 1: Existe un algoritmo de tiempo polinómico probabilístico que resuelve el problema HSP$_t$, para $t > d$, con complejidad computacional $\mathcal{O}\left(n^{2\omega}\right)$ y probabilidad de éxito

$$\frac{\gamma_t(n/2)\gamma_t(m)}{\gamma_t(m - n/2)},$$

donde la función $\gamma_t(k)$ es la probabilidad de que una matriz $k \times k$ con valores en $\mathbb{F}_t$ elegidos aleatoriamente sea invertible. Su expresión es

$$\gamma_t(k) = \prod_{i=1}^{k} \left(1 - \frac{1}{t^i}\right),$$

que resulta del orden de $1 - 1/t$ para k grande.

El resultado del Teorema 1 resuelve en negativo la conjetura [6, Conj. 6.7] para el caso HSP$_t$, con t suficientemente grande.

Para demostrar el Teorema 1 los autores fijan una instancia de grado d del problema HSP$_t$ y a continuación demuestran que si A es una solución del HSP$_t$, entonces también $S \cdot A$ es una solución, con $S \in GL_{n/2}(\mathbb{F}_t)$: es decir, cualquier transformación lineal de A también será solución del HSP$_t$. Eso les permite suponer que, salvo en pocos casos, la matriz A se podrá escribir como $A = (I|G)$, donde $G \in GL_{n/2}(\mathbb{F}_t)$ y la matriz I es la identidad de tamaño $n/2 \times n/2$. También se verifica que $A^\perp = (-G^T|I)$.

Denotemos las componentes lineales de la instancia $(\mathbf{p}, \mathbf{q})$ bajo consideración como

$$p_i^{(1)}(\mathbf{x}) = \lambda_i^{\mathbf{p}}\mathbf{x}, \quad q_i^{(1)}(\mathbf{x}) = \lambda_i^{\mathbf{q}}\mathbf{x}, \quad \forall i \in \{1, \ldots, m\}$$

donde $\lambda_i^{\mathbf{p}} = (\lambda_{i,1}^p, \ldots, \lambda_{i,n}^p) \in \mathbb{F}_t^n$, y $\lambda_i^{\mathbf{q}} = (\lambda_{i,1}^q, \ldots, \lambda_{i,n}^q) \in \mathbb{F}_t^n$. Entonces, cuando se realiza la transformación apuntada, $A = (I|G)$, aparece el siguiente sistema puramente lineal:

$$\begin{cases} \lambda_{i,k}^p & + & \sum_{j=1}^{n/2} \lambda_{i,j+n/2}^p g_{k,j}, \\ \lambda_{i,k+n/2}^q & - & \sum_{j=1}^{n/2} \lambda_{i,j}^q g_{j,k}, \end{cases} \tag{1}$$

para valores $i \in \{1, \ldots, m\}$, $k \in \{1, \ldots, n/2\}$. Este sistema debe resolverse para encontrar los $n^2/4$ elementos de G (es decir, los $g_{i,j}$). Observemos que disponemos de $2mn/2 = mn$ ecuaciones; como $m \geq n$ se tiene que $mn \geq n^2$, por lo que el sistema está sobre-determinado. Para tener éxito solamente necesitamos que la matriz $m \times n/2$ formada por los coeficientes lineales de la instancia tenga rango máximo, lo cual ocurre con probabilidad

$$\frac{\gamma_t(m)}{\gamma_t(m - n/2)},$$

valor que tiende rápidamente a 1, incluso para valores bajos de t. La Figura 1 presenta el algoritmo, relativamente sencillo, con que resuelve el HSP$_t$.

ENTRADA:	$p_1, \ldots, p_m, q_1, \ldots, q_m \in \mathbb{F}_t[\mathbf{x}]$.
SALIDA:	Subespacio A o fallo del algoritmo.

1. [Inicialización]
   01: Construcción del sistema lineal (ecuación (1)).
2. [Comprobación]
   02: Comprobación del rango de la matriz $\{\lambda_{i,j}\}$
3. [Resolución y salida]
   03: **if** rango($\{\lambda_{i,j}\}$) es máximo **then**
   04: **return** solución del sistema A
   05: **else**
   06: **print** "El algoritmo ha fallado"
   07: **end if**

Figura 1. Algoritmo para resolver el HSP$_t$

IV-C. Algoritmo para el HSP$_2$ y criptoanálisis del esquema de Aaronson y Christiano

El caso verdaderamente interesante es el problema HSP$_2$ por ser el oráculo clásico usado en la propuesta de Aaronson y Christiano. En este caso, el resultado es conjetural, pero la conjetura está soportada por una serie de argumentos teóricos y goza de un amplio respaldo experimental. Por ello, el algoritmo representa un criptoanálisis práctico del esquema de Aaronson y Christiano.

La conjetura que necesitamos admitir está relacionada con el tiempo de computación de una base de Gröbner, que es la sustancia del algoritmo, y se enuncia así, para una instancia de HSP$_2$ de grado d [7, Conj. 1]:

Conjetura 2: El grado de regularidad está acotado superiormente por $d + 1$.

Con tal conjetura, el resultado alcanzado se enuncia así [7, Th. 4]:

Teorema 3: Existe un algoritmo de tiempo polinómico probabilístico que resuelve el problema HSP_2, con complejidad computacional $\mathcal{O}\left(n^{2\omega(d+1)}\right)$ con probabilidad de éxito $\gamma_2(n/2)$.

Para valores altos de n, la probabilidad de éxito del algoritmo es, aproximadamente, $1/2$. El valor ω representa nuevamente el *exponente de multiplicación de matrices* (véase subsección IV-A).

Este resultado no es tan fuerte como el anterior pues en característica 2 ya no es posible obtener ecuaciones lineales debido a la restricción que impone la reducción polinómica con las ecuaciones del cuerpo, por la que en ningún polinomio puede aparecer una variable elevada a una potencia superior a 1. Sin embargo, el sistema está tan sobre-determinado que la computación de la base de Gröbner termina siendo eficiente a pesar de todo.

El resultado teórico que apoya la anterior afirmación, enunciado en forma de corolario en [7, Cor. 1], dice así:

Corolario 4: Sea $(\mathbf{p},\mathbf{q}) = ((p_1,\ldots,p_m),(q_1,\ldots,q_m)) \in \mathbb{F}_2[\mathbf{x}]^m \times \mathbb{F}_2[\mathbf{x}]^m$ una instancia de HSP_2 de grado d. Es fácil generar $\mathcal{O}(m^2)$ ecuaciones de grado $d-1$ que son combinaciones lineales de las ecuaciones de grado d del sistema original.

Experimentalmente, se ve que se encuentran m^2 ecuaciones de grado $d-1$ en cuanto los parámetros superan valores bajos.

V. Problema de los subespacios ocultos con ruido (NHSP)

Informalmente, la idea del esquema ruidoso es añadir sobre un esquema ordinario de tipo HSP un cierto número de polinomios que no se anulan ni en A ni en $A^\perp$, de modo que sirvan de «señuelo» para así confundir al posible criptoanalista.

V-A. Definición del NHSP_t

Dado un cuerpo primo $\mathbb{F}_t$, sean polinomios de grado $d \geq 3$ $(\mathbf{p},\mathbf{q}) = ((p_1,\ldots,p_m),(q_1,\ldots,q_m)) \in \mathbb{F}_t[\mathbf{x}]^m \times \mathbb{F}_t[\mathbf{x}]^m$, con $m = \lceil \beta n \rceil$, $\beta \geq 3/(1-2\epsilon)^2$ y $0 \leq \epsilon < 1/2$. Se define el problema NHSP_t como el de encontrar un subespacio $A \subset \mathbb{F}_t^n$ de dimensión $n/2$ (o su complemento ortogonal $A^\perp$) tal que

$$p_i(A) = 0,\ \forall i \in I_{\mathbf{p}} \text{ y } q_j(A^\perp) = 0,\ \forall j \in I_{\mathbf{q}},$$

para ciertos $I_{\mathbf{p}}, I_{\mathbf{q}} \subset \{1,\ldots,m\}$ con $\#I_{\mathbf{p}} = \#I_{\mathbf{q}} = \lceil (1-\epsilon)m \rceil$. Por consiguiente, un polinomio $p_i \in \mathbf{p}$ (o bien $q_i \in \mathbf{q}$) es no ruidoso si $i \in I_{\mathbf{p}}$ (o bien $i \in I_{\mathbf{q}}$) y ruidoso en caso contrario.

Los polinomios no ruidosos se eligen de manera aleatoria de entre los que se anulan en A (o en $A^\perp$). Por su parte, un polinomio ruidoso, p_i con $i \notin I_{\mathbf{p}}$, se elige aleatoriamente de entre los polinomios que se anulan en un espacio $A_i^{\mathbf{p}}$ elegido también aleatoriamente en $\mathbb{F}_t^n$. Análogamente, un polinomio ruidoso q_i con $i \notin I_{\mathbf{q}}$, se elige aleatoriamente de entre los polinomios que se anulan en un espacio $A_i^{\mathbf{q}}$ elegido también aleatoriamente en $\mathbb{F}_t^n$. Observemos que en este caso no existe ninguna relación de ortogonalidad entre $A_i^{\mathbf{p}}$ y $A_i^{\mathbf{q}}$. Por tanto, en el conjunto de los m polinomios $\mathbf{p}$ y los m polinomios $\mathbf{q}$ tenemos una fracción ϵ que no se relaciona en absoluto con los espacios A y $A^\perp$: su presencia sirve puramente para confundir al criptoanalista.

Para simplificar la notación en los resultados que expondremos sucesivamente, dada una instancia $(\mathbf{p},\mathbf{q})$ del problema NHSP_t, definimos el *peso* de un vector $v \in \mathbb{F}_t^n$ con respecto a $\mathbf{p}$, denotado como $w_t^{\mathbf{p}}(v)$ como el cardinal del conjunto

$$W_v^{\mathbf{p}} = \{p_i : p_i(v) \neq 0\},$$

es decir, $w_t^{\mathbf{p}}(v) = |W_v^{\mathbf{p}}|$. Definimos también el conjunto $Z_t^{\mathbf{p}} \subset \mathbb{F}_t^n$ como

$$Z_t^{\mathbf{p}} = \{v \in \mathbb{F}_t^n : w_t^{\mathbf{p}}(v) < \epsilon\beta n\}.$$

Estas definiciones pueden escribirse de modo análogo para $\mathbf{q}$. Equipados con estas definiciones, presentamos el siguiente resultado:

Lema 5: [6, Lemma 6.5] Sea $(\mathbf{p},\mathbf{q})$ una instancia de NHSP_2 tal como se explica más arriba. Entonces se verifica que $A \subseteq Z_2^{\mathbf{p}}$ y, además, $\Pr[A = Z_2^{\mathbf{p}}] = 1 - 2^{-\Omega(n)}$, donde $\Pr[\cdot]$ denota la probabilidad de un evento $[\cdot]$.

Este resultado permite comprobar fácilmente si un elemento de $\mathbb{F}_2^n$ pertenece a A. El resultado del Lema 5 se puede extender al caso de un cuerpo primo $\mathbb{F}_t$, con $t > 2$.

V-B. Algoritmo para el NHSP_t con $t > d$

El primer resultado del criptoanálisis del problema NHSP concierne el caso en que $t > d$ y resuelve en negativo la Conjetura 6 enunciada por Aaronson y Christiano, pues somos capaces de dar un algoritmo de tiempo polinómico para resolver el problema NHSP_2 que, además, es puramente clásico.

La conjetura tal como la enuncian los autores es la siguiente:

Conjetura 6: [6, Conj. 6.7] Sea $\epsilon < 1/2$ y $\beta = 3/(1-2\epsilon)^2$, y sea $(\mathbf{p},\mathbf{q}) \in \mathbb{F}_2[\mathbf{x}]^m \times \mathbb{F}_2[\mathbf{x}]^m$ una instancia de grado d del problema NHSP_2. En estas condiciones, no existe ningún algoritmo cuántico de tiempo polinómico que pueda resolver el NHSP_2 con probabilidad de éxito mayor de $\Omega(2^{-n/2})$.

El resultado que hemos obtenido en relación con la Conjetura 6 se enuncia como sigue:

Teorema 7: Existe un algoritmo de tiempo polinómico probabilístico que resuelve el problema NHSP_t de grado d, cuando $t > d$, con complejidad computacional $\mathcal{O}(m^\omega)$ y una probabilidad de éxito de, al menos,

$$\frac{\gamma_t\left(\lceil (1-\epsilon)m \rceil\right)}{\gamma_t\left(\lceil (1-\epsilon)m \rceil - n/2\right)} \cdot \sum_{i=\lceil (1-\epsilon)m \rceil}^{m} \binom{m}{i} \left(1 - \frac{1}{t^n}\right)^i \left(\frac{1}{t^n}\right)^{m-i}.$$

Para alcanzar este resultado se siguen dos pasos. En primer lugar, en [6, Claim 6.10] los propios autores presentan un ataque al NHSP_2 en el caso de grado $d = 1$, capaz de recuperar A en tiempo polinómico. La clave es observar que

$$q_i \text{ se anula en } A^\perp \iff q_i(\mathbf{x}) = \lambda_i^{\mathbf{q}}\mathbf{x} \text{ para algún } \lambda_i^{\mathbf{q}} \in A.$$

Esta propiedad implica que existen exactamente tantos elementos $\lambda_i^{\mathbf{q}} \in A$ como polinomios no ruidosos que se anulan en $A^\perp$, es decir, $\lceil (1-\epsilon)m \rceil$. Pero decidir si un elemento cualquiera de $\mathbb{F}_2^n$ está en A se puede hacer eficientemente, así que podemos recuperar $\mathcal{O}\left(\lceil (1-\epsilon)m \rceil\right)$ elementos de

A, entre los que habrá $n/2$ linealmente independientes con probabilidad

$$\frac{\gamma_2\left(\lceil(1-\epsilon)m\rceil\right)}{\gamma_2\left(\lceil(1-\epsilon)m\rceil - n/2\right)} = \prod_{i=\lceil(1-\epsilon)m\rceil-n/2+1}^{\lceil(1-\epsilon)m\rceil}\left(1-\frac{1}{t^i}\right).$$

Aunque este resultado está enunciado para un cuerpo binario, es perfectamente aplicable a un cuerpo primo $\mathbb{F}_t$, con $t > 2$.

Para dar el segundo paso, la clave es observar que una instancia de NHSP$_t$ de grado $d > 1$ puede reducirse a una instancia de grado $d = 1$. Notemos que cualquier elemento del subespacio $A \subset \mathbb{F}_t^n$ puede escribirse como $\mathbf{y}A$, donde $\mathbf{y} = \left(y_1, \ldots, y_{n/2}\right) \in \mathbb{F}_t^{n/2}$ es un vector de variables formales y A representa (abusando de la notación) una matriz base del subespacio A. Puesto que para todo $i \in I_{\mathbf{p}}$, el polinomio p_i se anula en $\mathbf{y}A$ y recordando que $t > d$, necesariamente ocurre que todos los coeficientes de $p_i\left(\mathbf{y}A\right)$ se anulan. En particular, $p_i^{(1)}\left(\mathbf{y}A\right) = 0$ para todo $i \in I_{\mathbf{p}}$. Con esto queda reducido el problema al caso de grado $d = 1$ y se aplica el resultado anterior.

Sea $(\mathbf{p}, \mathbf{q}) \in \mathbb{F}_t[\mathbf{x}]^m \times \mathbb{F}_t[\mathbf{x}]^m$ una instancia de grado $d \geq 3$ del problema NHSP$_t$, $m = \lceil \beta n \rceil$, con $\beta \geq 3/(1-2\epsilon)^2$, y $0 \leq \epsilon < 1/2$. Si denotamos las componentes lineales de $\mathbf{p}$ y $\mathbf{q}$ como

$$p_i^{(1)}\left(\mathbf{x}\right) = \lambda_i^{\mathbf{p}}\mathbf{x}, \quad q_i^{(1)}\left(\mathbf{x}\right) = \lambda_i^{\mathbf{q}}\mathbf{x}, \quad \forall i \in \{1, \ldots, m\}$$

donde $\lambda_i^{\mathbf{p}}, \lambda_i^{\mathbf{q}} \in \mathbb{F}_t^n$, el algoritmo mostrado en la Figura 2 resuelve el problema NHSP$_t$:

ENTRADA: $q_1, \ldots, q_m \in \mathbb{F}_t[\mathbf{x}]$.
SALIDA: Subespacio A o fallo del algoritmo.

1. [Inicialización]
   01: $E_A \leftarrow \emptyset$
2. [Lazo]
   02: **for** $j := 1$ to m **do**
   03: $c \leftarrow w_t^{\mathbf{p}}\left(\lambda_j^{\mathbf{q}}\right)$
   04: **if** $(m - c \geq \lceil(1-\epsilon)\rceil m)$ **then**
   05: $E_A \leftarrow E_A \cup \{\lambda_j^{\mathbf{q}}\}$
   06: **end if**
   07: **end for**
3. [Comprobación y salida]
   08: **if** $(\dim(\text{span}(E_A)) = n/2)$ **then**
   09: $A \leftarrow \text{span}(E_A)$
   10: **return** A
   11: **else**
   12: **print** "El algoritmo ha fallado"
   13: **end if**

Figura 2. Algoritmo para resolver el NHSP$_t$

El algoritmo presentado funciona para instancias del problema NHSP$_t$ en que haya al menos $\lceil(1-\epsilon)m\rceil$ polinomios en $\mathbf{q}$ (o en $\mathbf{p}$) con términos lineales para poder aplicar el paso anteriormente descrito. La probabilidad de que ello suceda en un polinomio aleatoriamente elegido es precisamente

$$\sum_{i=\lceil(1-\epsilon)m\rceil}^{m}\binom{m}{i}\left(1-\frac{1}{t^n}\right)^i\left(\frac{1}{t^n}\right)^{m-i},$$

lo que justifica que la probabilidad total de éxito del algoritmo sea la enunciada en el Teorema 7.

Por lo que respecta a la complejidad computacional del algoritmo, observemos que el coste de la computación del lazo en los pasos 02–07 corresponde esencialmente a m evaluaciones de la función $w_t^{\mathbf{p}}$, lo supone un coste de $\mathcal{O}(m^2 n)$ multiplicaciones. Obtener la matriz diagonal para encontrar $n/2$ vectores linealmente independientes es el objetivo de la comprobación final y salida en los pasos 08–13, lo que tiene un coste de $\mathcal{O}(\lceil(1-\epsilon)m\rceil^\omega)$ multiplicaciones. Por tanto el coste total es $\mathcal{O}(m^\omega)$ multiplicaciones.

Es de notar que este ataque se podría evitar si los parámetros del sistema se toman diferentes de los propuestos por los autores de [6], eligiendo, por ejemplo, instancias con polinomios de grado homogéneo.

V-C. Algoritmo para el NHSP$_2$

También para el problema ruidoso el caso binario resulta el más interesante, pues el trabajo de Aaronson y Christiano se centra precisamente en este caso. El resultado que vamos a presentar resuelve en negativo la Conjetura 6 presentada más arriba.

Para conseguir este resultado combinamos una búsqueda exhaustiva junto con el algoritmo que resuelve el caso HSP$_2$. Dada una instancia del NHSP$_2$, $(\mathbf{p}, \mathbf{q}) \in \mathbb{F}_t[\mathbf{x}]^m \times \mathbb{F}_t[\mathbf{x}]^m$, de grado d, la idea es elegir aleatoriamente n polinomios de los de $\mathbf{p}$ y confiar en que sean justamente no ruidosos. Si tenemos suerte, el algoritmo HSP$_2$ funcionará y tendremos una solución también para NHSP$_2$. Si no funciona, repetimos el proceso. Se trata, pues, de un algoritmo probabilístico.

Nos interesa, en primer lugar, saber qué probabilidad tenemos de acertar con n polinomios no ruidosos si los elegimos aleatoriamente. No es difícil ver que tal probabilidad viene dada por este cociente:

$$P_n^{\epsilon,\beta} = \frac{\binom{\lceil(1-\epsilon)\beta n\rceil}{n}}{\binom{\lceil\beta n\rceil}{n}},$$

en donde debemos recordar que $m = \beta n$. Utilizando una aproximación debida a Stirling se puede dar una expresión asintótica como sigue:

$$P_n^{\epsilon,\beta} = \left[\left(\frac{\beta-1}{\beta}\right)^{\beta-1}\cdot\left(1+\frac{1}{(\epsilon-1)\,\beta}\right)^{(\epsilon-1)\beta}\cdot\left(1-\epsilon-\frac{1}{\beta}\right)\right]^n.$$

Combinando lo anterior, expresamos formalmente el resultado obtenido mediante el siguiente:

Teorema 8: Dada una instancia del NHSP$_2$, $(\mathbf{p}, \mathbf{q}) \in \mathbb{F}_t[\mathbf{x}]^m \times \mathbb{F}_t[\mathbf{x}]^m$, de grado d, existe un algoritmo probabilístico de tiempo polinómico que resuelve el problema NHSP$_2$ con probabilidad

$$\gamma_2\left(n/2\right) \cdot P_n^{\epsilon,\beta}.$$

Observemos que elegir n polinomios de $\mathbf{p}$ toma, ciertamente, tiempo polinómico $\mathcal{O}(n)$. Además, ejecutar el algoritmo HSP$_2$ toma también tiempo polinómico, por lo que el conjunto de ambos procesos también lo hará.

Por lo que respecta a la probabilidad, tener éxito y elegir justamente n polinomios no ruidosos tiene una probabilidad de $P_n^{\epsilon,\beta}$. Como el HSP$_2$ tiene una probabilidad de éxito de $\gamma_2(n/2)$, el resultado final es el producto de ambas.

Para finalizar, establecemos el resultado que resuelve definitivamente la Conjetura 6, a saber, que nuestro algoritmo tiene éxito con probabilidad $\Omega(n/2)$, con tal que la proporción de polinomios ruidosos no supere cierto límite. Expresémoslo formalmente mediante el siguiente teorema:

Teorema 9: Sea $\beta = 3/(1-2\epsilon)^2$. Dada una instancia del NHSP_2 de grado d, $(\mathbf{p},\mathbf{q}) \in \mathbb{F}_2[\mathbf{x}]^m \times \mathbb{F}_2[\mathbf{x}]^m$ el algoritmo muestra una probabilidad asintótica de éxito de

$$ {c_\epsilon}^{-n/2}, \quad \text{con } c_\epsilon < 2, $$

para $\epsilon \in (0, \epsilon_\beta]$, con

$$ \epsilon_\beta = 0{,}28363360679073705 \pm 0{,}00000000000000005. $$

Para entender el anterior resultado, observemos que, fijado un cierto ϵ, la expresión $P_n^{\epsilon,\beta}$ depende solo de n. Por otro lado, $\lim_{n\to\infty} \gamma_2(n/2) \approx 0{,}288788$ (es decir, podemos tomarlo como un valor constante) con lo que la probabilidad de éxito del algoritmo será $\Omega(2^{-n/2})$ si y solo si $P_n^{\epsilon,\beta}$ es $\Omega(2^{-n/2})$, es decir, si $P_n^{\epsilon,\beta} > 2^{-n/2}$. Si resolvemos esta última desigualdad numéricamente, llegamos a que esto ocurre justamente cuando $0 \le \epsilon \le \epsilon_\beta$, y ϵ_β toma el valor expresado arriba.

VI. Conclusiones

Por medio de esta comunicación hemos tratado de divulgar el conocimiento de esquemas criptográficos basados en propiedades cuánticas, campo de creciente actualidad. En particular, hemos descrito en términos sencillos el esquema de dinero cuántico propuesto por Aaronson y Christiano. Este esquema se apoya en unos problemas novedosos, también propuestos por los mismos autores, que ellos denominaron el *problema de los subespacios ocultos* (HSP) y el *problema de los subespacios ocultos con ruido* (NHSP).

Los problemas HSP y NHSP no son cuánticos, sino puramente clásicos. En su trabajo, Aaronson y Christiano conjeturaron que no existía ningún algoritmo cuántico de tiempo polinómico capaz de resolverlos sobre $\mathbb{F}_2$.

A lo largo de esta comunicación hemos tratado de mostrar que, de hecho, esa conjetura se revela falsa, pues hemos sido capaces de diseñar algoritmos puramente clásicos y de tiempo polinómico probabilístico que resuelven los problemas HSP y NHSP. Los algoritmos obtenidos cubren los siguientes casos:

- Un algoritmo de tiempo polinómico probabilístico que resuelve el problema HSP_t, para $t > d$.
- Un algoritmo heurístico de tiempo polinómico probabilístico que resuelve el problema HSP_2.
- Un algoritmo de tiempo polinómico probabilístico que resuelve el problema NHSP_t de grado d, cuando $t > d$.
- Un algoritmo de tiempo polinómico probabilístico que resuelve el problema NHSP_2.

Por tanto, las conjeturas que Aaronson y Christiano habían presentado han resultado falsas, no solo frente a los algoritmos cuánticos, sino incluso en el ámbito de los puramente clásicos. Esto no invalida por completo el esquema original de los autores, pero exige redefinir algunos parámetros para garantizar su seguridad.

Aunque por falta de espacio no hemos incluido el código en esta comunicación, todos estos algoritmos han sido implementados de manera práctica usando el sistema de álgebra computacional Magma [15] y hemos obtenido tiempos de computación para valores bajos de los parámetros totalmente congruentes con lo esperado por la teoría.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el Ministerio de Economía, Industria y Competitividad (MINECO), la Agencia Estatal de Investigación (AEI) y el Fondo Europeo de Desarrollo Regional (FEDER, UE), a través del proyecto COPCIS, referencia TIN2017-84844-C2-1-R, y por la Comunidad de Madrid (Spain) a través del proyecto CYNAMON, referencia P2018/TCS-4566-CM, también cofinanciado con fondos FEDER de la Unión Europea.

Referencias

[1] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA: Springer US, 1983, pp. 199–203.

[2] S. Nakamoto. (2008) Bitcoin P2P e-cash paper. http://nakamotoinstitute.org/bitcoin/. [Online]. Available: http://nakamotoinstitute.org/bitcoin/

[3] ——. (2009) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[5] S. Aaronson, "Quantum copy-protection and quantum money," in *Proceedings of the 2009 24th Annual IEEE Conference on Computational Complexity*, ser. CCC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 229–242.

[6] S. Aaronson and P. Christiano, "Quantum money from hidden subspaces," *Theory of Computing*, vol. 9, pp. 349–401, 2013.

[7] M. Conde Pena, J.-C. Faugère, and L. Perret, "Algebraic cryptanalysis of a quantum money scheme: The noise-free case," in *Public-Key Cryptography – PKC 2015*, J. Katz, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 194–213.

[8] M. Conde Pena, R. Durán Díaz, J.-C. Faugère, L. Hernández Encinas, and L. Perret, "Non-quantum cryptanalysis of the noisy version of Aaronson-Christiano's quantum money scheme," *IET Information Security*, vol. 13, no. 4, pp. 362–366, 7 2019.

[9] A. Molina, T. Vidick, and J. Watrous, "Optimal counterfeiting attacks and generalizations for Wiesner's quantum money," in *Theory of Quantum Computation, Communication, and Cryptography*, ser. Lecture Notes in Computer Science, K. Iwama, Y. Kawano, and M. Murao, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, vol. 7582, pp. 45–64.

[10] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *Advances in Cryptology - EUROCRYPT 1996*, ser. Lecture Notes Comput. Sci., U. Maurer, Ed., vol. 1070. Springer Berlin Heidelberg, 1996, pp. 33–48.

[11] M. Conde Pena, R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué, "The isomorphism of polynomials problem applied to multivariate quadratic cryptography," in *International Joint Conference SOCO'13-CISIS'13-ICEUTE'13*, ser. Advances in Intelligent Systems and Computing, Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, A. C. de Carvalho, P. G. Bringas, I. Zelinka, H. Quintián, and E. Corchado, Eds., vol. 239. Springer International Publishing, 2014, pp. 567–576.

[12] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, 3rd ed., ser. Undergraduate Texts in Mathematics, S. Axler, F. Gehring, and K. Ribet, Eds. New York, USA: Springer, 2007.

[13] J.-C. Faugère, "A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)," in *International Symposium on Symbolic and Algebraic Computation-ISAAC 2002*, A. Press, Ed., 2002, pp. 75–83.

[14] J. v. z. Gathen and J. Gerhard, *Modern Computer Algebra*, 2nd ed. Cambridge, UK: Cambridge University Press, 2003.

[15] W. Bosma, J. J. Cannon, and C. Playoust, "The Magma Algebra System I: The user language," *Journal of Symbolic Computation*, vol. 24(3-4), pp. 235–265, 1997.