Protocolos de distribución cuántica de claves

D. Elkouss[1] y J. García-López[1]

Dep. Matemática Aplicada, E.U. Informática, U. Politécnica de Madrid

Resumen. Este estudio muestra como realimentar con seguridad informacional una clave compartida entre Alicia y Bernardo. Partiendo de una semilla común se pretende realimentar una clave a través de un protocolo cuántico de distribución de clave. Alicia y Bernardo deben de tener cuidado a fin de evitar la paradoja de utilizar métodos basados en seguridad computacional, por ejemplo la criptografía de clave pública, para obtener seguridad informacional.

Palabras clave: BB84, autenticación, criptografía de clave privada, criptografía cuántica, distribución de claves privadas.

1 Introducción

Hasta mediados de los años 80, la utilización del cuaderno de un solo uso de Vernam, único método conocido que garantiza independencia estadística del criptograma con respecto al mensaje, fue escasa o nula. Así fue, dado que el intercambio de la clave secreta se basaba, como en gran medida sigue siendo el caso, en mecanismos con seguridad computacional, como pueda ser el método de Diffie y Hellman que descansa sobre la dificultad de calcular logaritmos discretos. Una vez la clave en sí no es totalmente aleatoria o desconocida para el espía, el cuaderno de un solo uso no ofrece seguridad absoluta.

Este panorama no cambió hasta 1984, año en que Bennett y Brassard presentaron su protocolo [1]. Utilizando un canal cuántico y aprovechando sus características, una pareja de interlocutores puede intercambiar una clave totalmente secreta y aleatoria con la garantía de que cualquier intento de escucha por parte de un espía será detectado.

La segunda parte revisa el protocolo BB84 y presenta el modelo de espía para a continuación estudiar la seguridad del protocolo. En la tercera parte se muestra una construcción explícita que permite realimentar una semilla previa compartida por dos interlocutores Alicia y Bernardo. Se muestra en particular que no es necesario recurrir a mecanismos de seguridad computacional para obtener una nueva clave.

2 Estudio de seguridad de BB84

Un criptosistema es informacionalmente seguro si su seguridad deriva exclusivamente de la teoría de la información. Esto es, si no hace ninguna hipótesis sobre la dificultad de un problema matemático. Un criptosistema informacionalmente seguro es, en consecuencia, seguro incluso si un adversario tuviera capacidad de cálculo ilimitada.

La idea de este estudio es implementar BB84 en la práctica de manera que el protocolo completo tenga seguridad informacional. Como modelo de partida se tiene dos interlocutores, Alicia y Bernardo, que quieren intercambiar una clave. Disponen para ello de un canal clásico, de un canal cuántico y de una clave compartida previa. Una espía, Eva, trata de interceptar la clave sin ser percibida, dispone para ello de una capacidad ilimitada de computación y acceso tanto pasivo como activo al canal clásico y al cuántico.

2.1 El protocolo BB84

A continuación se describe de manera resumida cada una de las fases del protocolo BB84.

1. Alicia genera una cadena aleatoria de unos y ceros, $a_1, ..., a_i, ..., a_N$ con $a_i \in \{0, 1\}$

2. Para cada bit de la cadena Alicia elige aleatoriamente entre dos bases (B_+, B_x) y envía el bit codificado en dicha base. Representando B_+ por 1 y B_x por 0, la cadena de bases es una cadena α de unos y ceros, $\alpha_1, ..., \alpha_i, ..., \alpha_N$ con $\alpha_i \in \{0, 1\}$

3. Cuando Bernardo recibe el bit elige aleatoriamente la base con la que medir de entre las dos anteriores. La cadena que representa la base elegida es β, una cadena de longitud N equivalente a α. La medida genera una cadena b de unos y ceros, $b_1, ..., b_i, ...b_N$ con $b_i \in \{0, 1\}$.

4. Bernardo envía β a Alicia por un canal público.

5. Por el mismo canal público, Alicia envía α a Bernardo.

6. Alicia y Bernardo borran de sus cadenas los bits en los que se han usado bases diferentes.

7. A continuación Alicia envía a Bernardo una lista de posiciones junto a su valor para estimar la tasa de error.

8. Si la tasa de error es inferior a un cierto umbral, se da por válido el intercambio; si es superior, Bernardo comunica a Alicia que hay que abortar el protocolo.

2.2 Modelo de espía

En este estudio se va a dotar al espía, Eva, de la capacidad de realizar ataques individuales sobre los qubits. Es decir: para cada qubit Eva elige si lo intercepta o no. En caso de interceptarlo, Eva mide el qubit en una base de su elección,

guarda el resultado de la medida y reenvía a Bernardo el qubit resultante. Esta estrategia de espionaje es conocida como interceptar-reenviar, para una demostración del caso general ver [2]. Después de realizar su ataque Eva obtiene una secuencia de bits e de longitud N con $e_i \in \{0, 1\}$, cada bit tendrá una cierta probabilidad de ser igual al bit de Alicia. A esta probabilidad la llamamos información de Eva sobre Alicia, I. Obtener esta información implica introducir una discrepancia en la cadena compartida por Alicia y Bernardo, D. Llamamos ataque sobre un qubit a un par D, I. Para una D dada existe una máxima I alcanzable.

$$I = \sum_{i=1}^{N} P(a_i = e_i / \alpha_i = \beta_i) \tag{1}$$

$$D = \sum_{i=1}^{N} P(a_i \neq b_i / \alpha_i = \beta_i) \tag{2}$$

Analizaremos ahora el canal clásico. En la literatura es habitual encontrar la hipótesis de partida de una canal autenticado, o de una semilla previa que se usa para autenticar los mensajes [5]. Es una hipótesis razonable al no ser muy costosa, ya que la clave necesaria para autenticar un mensaje es proporcional a $log(N)$ siendo N el tamaño del mensaje [3], siempre con seguridad informacional. Vamos a estudiar ahora si esta hipótesis es necesaria, o si existe algún paso que se puede enviar en claro. Recordamos que Eva es libre de realizar cualquier manipulación sobre la información. En particular es libre de:

a)Manipular β y por tanto manipular la secuencia de bases con las que Alicia piensa que Bernardo midió. Manipular β es equivalente a realizar un ataque complementario y no aporta ningún beneficio a Eva.

b)Manipular α. Una vez recibe β, Alicia descarta las posiciones en las que las bases no coinciden y envía α por el canal público, manipular α es equivalente a elegir las posiciones que Bernardo descarta.

De una manera intuitiva se puede razonar que para un ataque simétrico, Eva tiene la misma información sobre todos los bits, un cambio en las posiciones que Bernardo descarta no aportará ningún beneficio a Eva. Teniendo en cuenta que además se alcanza la información máxima para una distorsión dada sólo con un ataque simétrico, en principio Eva no deberá ganar nada manipulando las posiciones de Bernardo.

Para un ataque no simétrico la situación es más complicada, existen ciertos ataques que dan a Eva toda la información de Alicia, permiten conocer con exactitud la mitad de los bits de Bernardo, y no saber nada de la otra mitad.

La idea clave aquí es que para reducir la distorsión Eva necesitaría poder descartar más bits que la mitad. Para apoyar esta idea se ha estudiado el efecto que tiene un ataque de suplantación por parte de Eva:

1. Alicia genera su cadena aleatoria a_i codificando cada bit en la base también generada aleatoriamente α_i.

2. Eva intercepta todos los qubits y los mide según una secuencia de bases generada aleatoriamente ϵ_i. El espía guarda el resultado de la medición y reenvía a Bernardo el qubit resultante.

3. Bernardo comunica por el canal clásico público la secuencia de bases de medida.

4. Eva intercepta este mensaje y envía a Alicia su propia secuencia de bases de medida.

En este momento Eva ha conseguido una secuencia de bits exactamente igual a la de Alicia y conoce de Bernardo la mitad de las posiciones, exactamente aquellas en las que las bases son coincidentes. Si Eva dispusiera de cuatro posiciones para encajar cada bit de Alicia, conseguiría reducir la distorsión a cero. Asignando sólo las posiciones que conoce:

$$\overline{l} = \frac{1}{4}1 + \frac{3}{4}\frac{1}{4}2 + \frac{3}{4}\frac{3}{4}\frac{1}{4}3 + \ldots = \sum_{1}^{\infty} \frac{1}{4} i \left(\frac{3}{4}\right)^{i-1} \tag{3}$$

y usando la relación $\frac{d}{dr}\sum_0^\infty r^i = \frac{d}{dr}\frac{1}{1-r} = \frac{1}{(1-r)^2}$:

$$\overline{l} = \sum_{1}^{\infty} \frac{1}{4} i \left(\frac{3}{4}\right)^{i-1} = \frac{1}{4}\frac{1}{\left(1-\frac{3}{4}\right)^2} = 4 \tag{4}$$

Sin embargo, Eva no dispone de cuatro posiciones para encajar cada posición de Alicia, dispone de dos. Una estrategia razonable para el Espía es intentar emparejar el bit i de Alicia de manera correcta con un bit de Bernardo hasta una posición cercana a $2i + j$, usando un valor correcto o uno aleatorio hasta una posición $2i + k$ y finalmente emparejar con b_{2i+k} independientemente de su valor, la figura 1 muestra los resultados para $k \in [-2, 2]$, aunque se consigue un descenso de la distorsión introducida, esta mejora tiene un límite equivalente al de un ataque simétrico.

Por último se muestra (figura 1) un estudio de la variación de la distorsión en función de k para una longitud fija comprobando que tiene un mínimo para k cercana a 0.

3 Realimentando una semilla con BB84

Los costosos protocolos de distribución cuántica de clave tienen como objetivo mejorar la seguridad ofrecida por los sistemas de criptofrafía clásica que descansan en la seguridad computacional. A fin de no caer en la paradoja de tener que recurrir a estos sistemas vamos a analizar los distintos métodos utilizables con seguridad informacional.

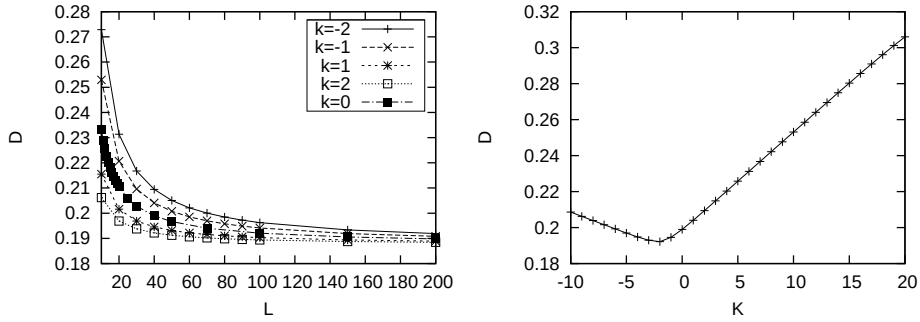

Figura 1. A la izquierda: Distorsión D en función de la longitud de la clave L. A la derecha: Distorsión D en función de k para una longitud de clave fija de 40 bits.

3.1 Autenticación

Para autenticar los mensajes recurriremos a códigos de autenticación no secretos incondicionalmente seguros. Propuestos originalmente por Wegman y Carter [8], han sido estudiados ampliamente en los últimos años [7].

Se tiene un estado fuente s, corresponde al mensaje plano, que es concatenado con un autenticador a para así obtener el mensaje $m = (s, a)$ que se envía por el canal.

Supongamos que Eva tiene la habilidad de introducir mensajes en el canal y/o de modificar mensajes existentes. Se llama impersonación a la introducción de un nuevo mensaje $m' = (s', a')$, a la modificación de un mensaje $m = (s, a)$ por otro $m' = (s', a')$ se le denomina sustitución. En los dos casos la dificultad que tiene Eva es hallar $a' = h(s', e)$ sin conocer e.

Se llama estrategia de autenticación a la distribución de probabilidad escogida para E dada la distribución de probabilidad de S. Elegida la estrategia, se pueden calcular P_{d_0} y P_{d_1} que representan respectivamente la probabilidad de Eva de realizar con éxito un ataque de impersonación y sustitución.

De aplicación directa a las necesidades de la distribución cuántica de clave es el siguiente resultado [7].

Teorema 1. *Sean a y b enteros, definimos* $s = b + \lceil log\ log\ a \rceil$ *e* $i = \lceil log(a/s) \rceil$. *Existe un código de autenticación para una fuente de a bits que tiene un autenticador de b bits y requiere* $(i + 1)s + b$ *bits de clave, con* $p_{d_0} = 1/2^b$ *y* $p_{d_1} \leq 1/2^{b-1}$

Adicionalmente el código es equivalente al array ortogonal $OA(2^b, 2^a, 2^{a-b})$ [7], lo que proporciona una construcción explícita al teorema 1. Siguiendo esta construcción, si se elige $a = 1024$, $b = 20$, se necesitará una clave de 236 bits para autenticar, que proporcionará una probabilidad de impersonación $p_{d_0} = 2^{-20}$ y una probabilidad de sustitución de $p_{d_1} \leq 2{-}19$. Para conseguir estas mismas probabilidades con $a = 2^{20}$ hará falta una clave de 445 bits.

3.2 Transmisión segura

Según se analizó en la sección 2 tanto la secuencia de bases medidas por Bernardo como la secuencia de posiciones a descartar pueden ser enviadas en claro por el canal clásico.

El paquete envíado por Alicia consta de tres secciones: la secuencia de posiciones, la secuencia de valores y el autenticador. Se proponen dos opciones de env'io: 1)Encriptar y autenticar (tabla 1); las dos primeras secciones se codifican sumando posición a posición con la clave privada previa común a Alicia y a Bernardo, y la secuencia de autenticación se envía en claro. 2)Sólo autenticar; igual a 1), pero no es necesario sumar la clave a las dos primeras secciones.

Tabla 1. Formato de mensaje y de resultado del protocolo

$p_0, \cdots, p_i$	$v_0, \cdots, v_j$	$a_0, \cdots, a_k$
posiciones $\oplus$ clave	valores $\oplus$ clave	autenticador $\oplus$ 0
$p_0 \oplus c_0, \cdots, p_i \oplus c_i$	$v_0 \oplus c_{i+1}, \cdots, v_j \oplus c_{i+j+2}$	$a_0, \cdots, a_k$

resultado autenticador	
b	$a_0 \ldots a_{61}$

Bernardo sólo tiene que enviar un bit para informar a Alicia del resultado del protocolo, con valor 1 para continuar, con valor 0 para abortar.

3.3 Compresión

El teorema de Shannon de codificación sin ruido [6] muestra que la cantidad mínima de bits para transmitir N variables aleatorias X idénticamente distribuidas caracterizadas por una entropía $H(X)$ es de $N \cdot H(X)$. No es posible comprimir los valores de las posiciones reveladas ya que son totalmente aleatorios.

Es especialmente importante en el caso en el que se quiere cifrar cada posición con el cuaderno de un solo uso. La descripción de una posición en una cadena de N bits toma $\lceil log_2 N \rceil$ bits para ser descrita, el valor de cada bit toma 1 bit y finalmente cada bit revelado es un bit perdido de clave bruta. Si se usa un 10 % de la clave para medir la discrepancia, la clave consumida es mayor que la clave bruta para $N \geq 256$.

Para evitar esta situación, las posiciones pueden codificarse, no como su posición en la secuencia sino como la diferencia con la posición precedente. Esta codificación ofrece ventajas ya que estas diferencias tenderán a tener como media n/N, si n es el total de posiciones a revelar y N el total de bits de clave bruta.

La diferencia entre posiciones se puede codificar usando un código Huffman [4]. De manera empírica se obtiene un código de Huffman con una longitud media de 4.71 bits, muy inferior a $\lceil log_2 \rceil 1000 = 10$ bits que se necesitarían para codificar la posición bruta.

3.4 Balance de información

Vamos a analizar ahora cuatro protocolos, en el protocolo A se parte con una clave generada por el protocolo de distribución cuántico de 1000 bits de longitud, se usa el código Huffmann para comprimir la información de las posiciones, que posteriormente es encriptada con el cuaderno de un solo uso y autenticada. Se puede observar que el balance es positivo, pero la ganancia neta de clave secreta es mínima.

Tabla 2. Balance de información de los protocolos

Protocolo A:	clave bruta	+1000 bits
	cifrado posiciones	$-4{,}71 \cdot 100$ bits
	cifrado valores	$-1 \cdot 100$ bits
	posiciones reveladas	$-1 \cdot 100$ bits
	autenticación posiciones y valores	236 bits
	autenticación resultado	63 bits
	total	30 bits
Protocolo B:	clave bruta	+1000 bits
	posiciones reveladas	$-1 \cdot 100$ bits
	autenticación posiciones y valores	236 bits
	autenticación resultado	63 bits
	total	601 bits
Protocolo C:	clave bruta	+1000000 bits
	cifrado posiciones	$-4{,}72 \cdot 100000$ bits
	cifrado valores	$-1 \cdot 100000$ bits
	posiciones reveladas	$-1 \cdot 100000$ bits
	autenticación posiciones y valores	445 bits
	autenticación resultado	63 bits
	total	327402 bits
Protocolo D:	clave bruta	+1000000 bits
	posiciones reveladas	$-1 \cdot 100000$ bits
	autenticación posiciones y valores	445 bits
	autenticación resultado	63 bits
	total	899492 bits

El protocolo B es equivalente al A, pero las secuencia de posiciones y valores están solamente autenticadas. Los protocolos C y D muestran el balance de información para una clave bruta de 1000000 bits con y sin cifrar las secuencias

de posiciones y valores respectivamente. En todos estos protocolos se consigue expandir satisfactoriamente la clave inicial.

4 Conclusión

En este trabajo se ha mostrado como realimentar una semilla existente con seguridad informacional utilizando el protocolo BB84. Por una parte se ha estudiado las partes de BB84 que necesitan encriptación o al menos autenticación para el éxito del protocolo. Para encriptar se ha utilizado el cuaderno de un solo uso y para autenticar una familia de códigos de autenticación desarrollada por Stinson [7].

El tipo de encriptación utilizado para los mensajes no se puede mejorar sin relajar la seguridad del protocolo. Sin embargo, en lo que respecta a la autenticación, una vez fijada p_{d_1} no es descartable que nuevas familias de códigos de autenticación puedan ofrecer la misma seguridad con un número de bits de clave inferior.

Queda abierto un estudio menos idealizado del protocolo que incorpore la fase de corrección de errores debido a las imperfecciones de los dispositivos físicos, y de igual manera la fase de amplificación de la privacidad donde se elimina la información mostrada en la corrección de errores.

Referencias

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computers, Systems and Signal Processing*, Dec. 1984, pp. 175–179.

[2] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," 1999.

[3] P. Gemmell and M. Naor, "Codes for interactive authentication," *Lecture Notes in Computer Science*, vol. 773, pp. 355–??, 1994.

[4] D. A. Huffman, "A method for the construction of minimum-redundancy codes," *Proceedings of the IRE*, vol. 40, no. 9, pp. 1098–1101, 1952.

[5] R. Renner, "Security of quantum key distribution," PhD, Zurich Institute of technology, 2005.

[6] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, 1948.

[7] D. R. Stinson, "Universal hashing and authentication codes," *Lecture Notes in Computer Science*, vol. 576, pp. 74–85, 1991.

[8] M. N. Wegman and C. J. L., "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, pp. 265–279, June 1981.