Protocolos de reconciliación de información óptimos y no interactivos para distribución cuántica de claves

D. Elkouss, J. Martínez, D. Lancho y V. Martín

Depto. DLSIIS-Análisis Numérico, Facultad de Informática, Universidad Politécnica de Madrid, Campus de Montegancedo, 28660 Boadilla del Monte (Madrid) vicente@fi.upm.es

La reconciliación de información juega un rol esencial en todos los protocolos de distribución cuántica de claves (QKD en adelante). Debido a la inevitable imperfección física —o a la presencia de un espía— de cualquier implementación de un protocolo QKD [1], la cadena compartida tras la transmisión cuántica entre los interlocutores incluye discrepancias. En consecuencia, se requiere una etapa de procesado clásico para extraer una clave final secreta y libre de errores. Para ello se necesita un canal convencional, autenticado y sin ruido. El procesado tiene dos partes: reconciliación de la información y amplificación de la privacidad. En la primera se corrigen los errores entre las cadenas de los extremos de la comunicación (*Alice* y *Bob*), mientras que en la segunda se elimina la información que un espía pudiera conocer sobre la cadena compartida. La información así usada implica la reducción de la cantidad neta de clave: la utilización de un mínimo de información para reconciliar las cadenas de *Alice* y *Bob* maximiza la longitud de clave secreta. Este criterio no es el único a tener en cuenta a la hora de valorar la calidad de un método de reconciliación: la interactividad, medida como el número de intercambios en el canal, es un factor muy importante en la implementación práctica. A medida que el canal clásico tenga mayor latencia, cada uso impondrá una mayor penalización en el tiempo de corrección, siendo el caso extremo el de la QKD con enlaces vía satélite. En la práctica esto puede suponer que el factor limitante en una comunicación QKD no sea la parte cuántica, sino el proceso clásico.

Cascade [2] es el protocolo habitualmente utilizado para reconciliar las cadenas de *Alice* y *Bob*. Presentado por Brassard y Salvail en 1994, fue una de las primeras propuestas de protocolo de reconciliación de errores en un sistema QKD. En aquel momento, el coste computacional de los códigos correctores de errores con gran tamaño de palabra imposibilitaba su utilización práctica. La gran ventaja de Cascade es su simplicidad y la mínima capacidad de cálculo que requiere. Pese a esto, tiene dos importantes defectos: es altamente interactivo y la cantidad de información necesaria para corregir las cadenas es muy superior al límite de Shannon. Las técnicas modernas de corrección de errores son un candidato natural para este problema: por una parte han conseguido alcanzar los límites teóricos en varios tipos de canales y, por otro, requieren una única utilización del canal para corregir. Recientemente [3] se dio un primer paso en esta dirección, identificando como modelo de canal para la corrección el canal binario simétrico (BSC), y adaptando códigos LDPC* a dicho canal. Éstos, son códigos lineales con baja densidad de unos en la matriz de paridad. Su principal ventaja es la existencia de esquemas de decodificación iterativos que permiten su aproximación al límite de Shannon. Los códigos desarrollados tienen límites teóricos cercanos a la capacidad del canal, sin embargo, y a diferencia de Cascade, no se adaptan a diferentes probabilidades de error produciendo un efecto escalón en la cantidad de información necesaria para corregir. Para estar cerca de la capacidad del canal en todas las probabilidades de error posibles se requiere de un número infinito (o extraordinariamente grande) de códigos.

* Low-Density Parity-Check.

En este trabajo presentamos un protocolo que permite construir códigos LDPC de rendimiento variable, y por tanto ajustables a diferentes tasas de error. El procedimiento de ajuste es el siguiente: Se parte de un código de longitud n, información k y redundancia n-k, lo que implica un rendimiento $r_0 = k/n$ (que podría corregir la máxima tasa de error admisible e_0). Una vez estimada la probabilidad de error e (con $e < e0$) se calcula el rendimiento r óptimo con el que un código podría corregir todos los errores (con $r > r_0$). A continuación se calcula la perforación para que el rendimiento equivalente fuera r. Por perforación entendemos el número de bits p del código a eliminar, ya que al ser $e < e_0$ es posible reconciliar las cadenas de *Alice* y *Bob* con menos información. El procedimiento termina dividiendo la cadena intercambiada por *Alice* y *Bob* en bloques de n-p bits y asumiendo que son palabras de las que se han perdido p bits. La figura 1 compara la eficiencia de la reconciliación utilizando Cascade y un único código LDPC perforado. Se observa que a partir de una longitud de 30.000 los códigos LDPC tienen un rendimiento superior a Cascade, con la ventaja adicional de necesitar un único mensaje intercambiado en el canal para conseguir la corrección, lo que en la práctica es muy importante a pesar de incrementar la complejidad computacional. Las simulaciones muestran que los códigos LDPC tienen un comportamiento similar a Cascade para palabras pequeñas, mientras que en las de gran tamaño son netamente superiores, manteniendo la ventaja de no ser interactivos. Estos resultados demuestran que la sustitución de Cascade por códigos LDPC permite incrementar la cantidad neta de clave secreta obtenida en un sistema QKD a la vez que disminuye drásticamente la sobrecarga de comunicaciones asociadas al protocolo.

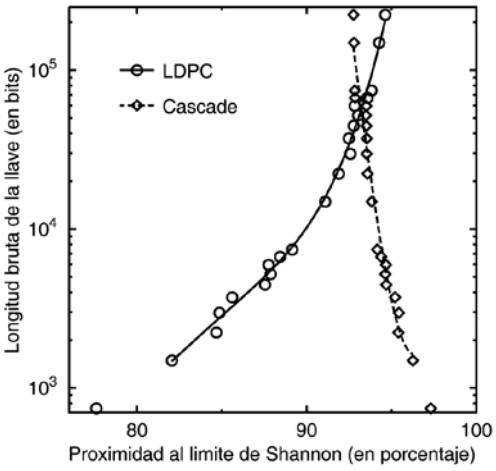

Figura 1. *Comparativa de la proximidad al límite de Shannon utilizando Cascade y códigos LDPC adaptables.*

Los autores agradecen la financiación del Ministerio de Ciencia e Innovación del Gobierno de España a través del Centro para el Desarrollo Tecnológico Industrial, CDTI, y del proyecto Segur@ CENIT-2007, así como del proyecto UPM 178/Q06 1005-127.

Referencias

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Int. Conf. on Comp., Sys. and Signal Proc, pp. 175–179, 1984.

[2] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion", Lecture Notes in Computer Science, vol. 765, pp. 410–423, 1994.

[3] D. Elkouss, A. Leverrier, R. Alleaume and J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution", IEEE International Symposium On Information Theory, 2009.