SANTANDER, 19-23 DE SEPTIEMBRE DE 2011

XXXIII

Reunión Bienal de la Real Sociedad Española de Física

tomo IV

21º Encuentro Ibérico para la Enseñanza de la Física

Astrofísica
Física de Plasmas
Física de la Materia Blanda
Física Médica
Información Cuántica

PUbliCan Ediciones

Reunión bienal de la
Sociedad Española
de Física

21º Encuentro Ibérico para la Enseñanza de la Física

M.ª Teresa Barriuso Pérez (Editora)

XXXIII Reunión Bienal
de la
Real Sociedad Española de Física

21.er Encuentro Ibérico para la Enseñanza de la Física

Santander, 19-23 de septiembre de 2011

Resúmenes de las Comunicaciones

[Tomo IV]
Astrofísica, Física de Plasmas
Física de la Materia Blanda
Física Médica, Información Cuántica

PUbliCan
Ediciones
Universidad de Cantabria

Real Sociedad Española de Física. Reunión Bienal (33ª : 2011 : Santander)
XXXIII Reunión Bienal de la Real Sociedad Española de Física ; 21er Encuentro Ibérico para la Enseñanza de la Física. -- Santander : PUbliCan, Ediciones de la Universidad de Cantabria, 2011.

Reuniones celebradas en el Palacio de la Magdalena de Santander del 19 al 23 de septiembre de 2011.

ISBN 978-84-86116-40-8 (O.C.)
ISBN 978-84-86116-41-5 (T.1)
ISBN 978-84-86116-42-2 (T.2)
ISBN 978-84-86116-43-9 (T.3)
ISBN 978-84-86116-44-6 (T.4)

Física-- Congresos.
Física-- Didáctica-- Congresos.
Encuentro Ibérico para la Enseñanza de la Física (21º : 2011 : Santander)

53(063)
53:37.02(063)

ISBN: 978-84-86116-40-8 (obra completa)
ISBN: 978-84-86116-44-6
DL: S. 1.171-2011

Impreso de España - *Printed in Spain*

Imprenta KADMOS
Salamanca

Reconciliación de errores mínimamente interactiva en distribución cuántica de claves

J. Martinez-Mateo, D. Elkouss, A. Ciurana, D. Espino, V. Martín[1]

[1]G. investigación Información y Computación Cuánticas, Universidad Politécnica de Madrid; Facultad de Informática, Campus de Montegancedo, Boadilla del Monte 28660, Madrid. vicente@fi.upm.es.

Introducción

La criptografía cuántica, o más concretamente la distribución cuántica de claves (QKD), es una disciplina de la información cuántica en auge desde el punto de vista industrial. A las en su día pioneras idQuantique y MagicQ, se le han añadido empresas grandes como Toshiba, NEC, NTT o Mitsubishi que trabajan en el desarrollo de dispositivos QKD comerciales. Esta disciplina también continúa avanzando desde el punto de vista teórico, en los últimos años destacan las propuestas de nuevos protocolos para QKD (e.g. COW o DPS entre otros) así como nuevos mecanismos para mejorar la seguridad de estos sistemas (e.g. los estados señuelo). También son destacables los trabajos recientes acerca de los nuevos protocolos independientes de los dispositivos, nuevas pruebas de seguridad y estimaciones más precisas de la seguridad de la clave intercambiada en situaciones reales. Sin embargo, independientemente de todos estos progresos, el intercambio de una clave a través de un protocolo QKD está, en todo momento, intrínsecamente asociado con un proceso clásico de destilación de la misma. Dicho proceso de destilación se descompone a su vez en dos subprocesos secuenciales generalmente tratados de forma independiente: (1) un primer proceso de corrección de errores, o reconciliación de información, donde se elimina toda posible discrepancia entre los bits de clave intercambiados y (2) un segundo proceso de amplificación de la privacidad, donde la clave corregida o reconciliada es acortada con el objetivo de reducir la información que haya podido ser obtenida por un hipotético espía o atacante. El primero de estos procesos, la reconciliación de la información, es clave tanto para la estimación de la tasa final de clave secreta como para el cálculo de la tasa de clave secreta generada por unidad de tiempo, que es fundamental para el rendimiento del sistema.

Reconciliación de información

Una de las propuestas originales para la reconciliación de errores en QKD es el protocolo conocido como *Cascade* [1]. Este protocolo continúa siendo utilizado en implementaciones actuales de dispositivos QKD debido a su sencillez y relativamente buena eficiencia en entornos con bajas tasas de error. Sin embargo, este protocolo es ineficiente debido a que: (1) es un protocolo altamente interactivo, puesto que requiere un número considerable de transmisiones a través de un canal de comunicación clásico, y (2) el porcentaje de información revelada con respecto al mínimo de información requerida se degrada para ratios de error elevados. Algunos trabajos recientes han desarrollado varias alternativas a *Cascade*, entre las cuales destacan aquellas basadas en el uso de técnicas de codificación modernas. Por ejemplo, a través del uso de códigos Low-Density Parity-Check (LDPC) hoy día encontramos varias propuestas que permiten mejorar la eficiencia de la reconciliación de clave para ratios de error elevados. Al utilizar códigos LDPC tan sólo se requiere un único uso del canal de comunicación.

Estas propuestas se basan en una técnica conocida como "codificación de síndrome" que permite aplicar métodos de corrección de errores para reconciliar cadenas aleatorias correlacionadas. En una de estas propuestas aplicamos dos técnicas conocidas en codificación, cómo son la perforación y el acortado de símbolos, para adaptar en tiempo real el ratio de información proporcionado por el síndrome intercambiado [2].

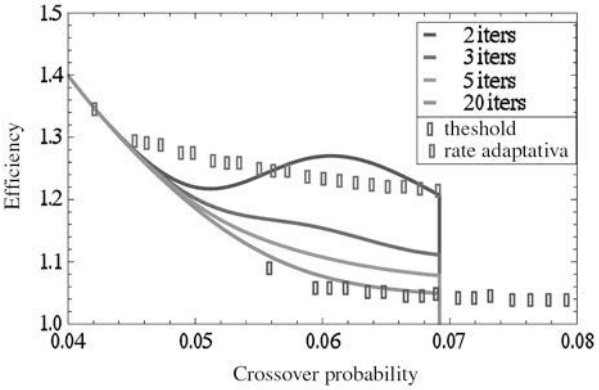

Figura 1. Comparación entre la eficiencia teórica (threshold) y la eficiencia simulada de un protocolo de reconciliación basado en la adaptación de la tasa de información (rate-adaptive). Eficiencias promedio de la versión interactiva con 2, 3 5 y 20 usos del canal para reconciliación.

En Ref. [2] pasamos de utilizar un protocolo altamente interactivo a un protocolo no interactivo sin analizar el rendimiento de soluciones intermedias. En este trabajo estudiamos las mejoras en el rendimiento del protocolo si permitimos usos adicionales del canal clásico de comunicaciones. La Fig. 1 muestra el impacto del número de usos permitidos del canal en el rendimiento del protocolo.

Conclusiones

El uso de una solución intermedia, un protocolo mínimamente interactivo para la reconciliación de errores, basada en técnicas modernas de codificación permite mejorar la eficiencia y el rendimiento promedio de las técnicas clásicas de reconciliación de errores aplicadas a los protocolos de acuerdo de clave secreta.

Los autores agradecen la financiación de la Comunidad de Madrid a través del proyecto Quantum Information Technologies in Madrid (QUITEMAD), así como los recursos proporcionados por el Centro de Supercomputación de Madrid (CeSViMa) y la Red Española de Supercomputación.

Referencias

1. Brassard G, Salvail L., *Lecture Notes in Computer Science*, **765**, 410 – 423 (1994)
2. Elkouss D., Martinez-Mateo J., Martin .V, *Quantum Inform. Comput.*, **11**, 226 – 238 (2011)
3. Martinez-Mateo J., Elkouss D., Martin V., *6th Int. Symposium on Turbo Codes & Iterative Information Processing*, 270 – 274 (2010)