Polibits

ISSN: 1870-9044

polibits@nlp.cic.ipn.mx

Instituto Politécnico Nacional

México

Molina Vilchis, María Aurora; Silva Ortigoza, Ramón; Bracho Molina, Eleazar

Criptografía Cuántica: Un Nuevo Paradigma

Polibits, núm. 36, 2007, pp. 30-35

Instituto Politécnico Nacional

Distrito Federal, México

Criptografía Cuántica: Un Nuevo Paradigma

Maria Aurora Molina Vilchis
Ramón Silva Ortigoza
CIDETEC IPN
Eleazar Bracho Molina
UAMI, Licenciatura en Computación.

La criptografía cuántica, a diferencia de la criptografía clásica, resuelve los problemas de cifrado de los mensajes para ocultar la información, así como la distribución de la clave, donde cada bit puede estar en un estado discreto y alternativo a la vez; la unidad fundamental de almacenamiento es el bit cuántico, cada uno de los cuales puede tener múltiples estados simultáneamente en un instante determinado, con lo que se reduce el tiempo de ejecución de algunos algoritmos de miles de años a apenas segundos.

La criptografía cuántica está basada en las interacciones del mundo sub-atómico, y tiene elementos como el bit cuántico, las compuertas cuánticas, los estados confusos, la tele transportación cuántica, el paralelismo cuántico y la computación cuántica.

Podemos decir que los métodos actuales de encriptación se basan en operaciones matemáticas, que modifican el mensaje para ocultar su significado, hasta que el destinatario que conoce las claves invierte el proceso y redescubre el mensaje. La fragilidad de este método radica en la transmisión de las claves, que pueden ser interceptadas en el trayecto, sin que el emisor y el receptor lo sepan. La criptografía cuántica supera en teoría ambas limitaciones, ya que la información se sitúa en las partículas de luz o fotones que son emitidos, de uno en uno, en un estado previamente conocido por el destinatario, quien de esta forma puede recuperar el mensaje. Si uno de los fotones es interceptado, su estado queda alterado y el receptor detecta el ataque al mensaje.

Criptografía es la ciencia matemática de las comunicaciones secretas, con una larga y distinguida historia de uso militar y diplomático que se remonta a los antiguos Griegos. Fue un elemento importante y decisivo durante la segunda guerra mundial, y hoy en día su uso es muy común y necesario, para brindar seguridad en las transacciones comerciales, comunicaciones, y privacidad; que se llevan a cabo mediante la Internet. Dados M y f, donde M es un mensaje y f una función de encriptación, tenemos $C = f(M)$, C entonces es el mensaje encriptado. C es enviado al receptor mediante un canal público, este obtiene el mensaje original con f^{-1}, haciendo $M = f^{-1}(C)$. Si f^{-1} es conocido y C es interceptado en el canal público, entonces se puede obtener M. La seguridad de f depende de la dificultad con que pueda obtenerse f^{-1}.

La factorización es un aspecto muy importante en la criptografía moderna, debido a que la seguridad del mecanismo de criptografía RSA de clave pública se basa en la dificultad de factorizar números grandes. El mejor algoritmo para hallar los factores aún sigue siendo el de las divisiones sucesivas. Así M, R_1 y R_2, mediante el mecanismo de RSA se define una función p, tal que $C_1 = p(Q_1, P_1, M_1)$ y $C_2 = p(Q_2, P_2, M_2)$, donde P_1 y P_2 son claves públicas generadas en base a Q_1 y Q_2 que son claves privadas pertenecientes a A y B respectivamente. A y B comparten sus respectivas claves públicas P_1 y P_2, y ambos pueden obtener y descifrar sus mensajes mediante p^{-1}, de tal modo *que* $M_1 = p^{-1}(Q_1, P_1, M^1)$ y $M_2 = p^{-1}(Q_2, P_2, M_2)$.

El tiempo que requeriría el realizar la factorización se estima en aproximadamente $4x10^{16}$ años. Sin embargo en 1994 se logró desarrollar un algoritmo, usando recursos en redes, donde la factorización únicamente tomo 8 meses, el equivalente a 4,000 MIPS-años. [Hughes94]. Se estima que los algoritmos cuánticos de factorización realizarían este cálculo en segundos. Utilizando claves privadas, es posible – al menos en teoría – tener un algoritmo de encriptación imposible de romper. El emisor cada vez que envía un mensaje M, genera aleatoriamente una diferente clave privada P, y mediante una función de encriptación E se codifica el mensaje de tal modo que $C = E(P, M)$. El receptor necesita la clave privada P para poder realizar el proceso inverso $M = E^{-1}(P, C)$. Actualmente, este mecanismo es utópico, debido a la gran dificultad que surge en la distribución de la clave privada P, debido a que necesita un canal muy seguro para su entrega.

La criptografía cuántica hace posible la distribución de la clave privada P. Esta clave es transmitida mediante un canal cuántico. Cualquier intento de medir P será

detectado, debido a que es imposible observar un *qubit* (bit cuántico) sin dejar rastro.

Este artículo presenta una introducción al nuevo paradigma en la criptografía de cara a la computación cuántica. En la sección 2 describe *grosso modo* los fundamentos de la criptografía cuántica. En la sección 3 se describe el criptosistema cuántico. Por último, en la sección 4 se listan las principales empresas comerciales que actualmente están incursionando en este nuevo campo de la criptografía.

2. *Fundamentos de la Criptografía Cuántica*

La comunidad científica dedicada a investigar tópicos en el ámbito de la criptografía cuántica, ha logrado enormes avances teóricos, al demostrar que es posible reducir drásticamente los recursos computacionales requeridos en la ejecución de algoritmos. Los algoritmos requieren un inmenso poder de cómputo aún en las computadoras más avanzadas de la actualidad. Algoritmos matemáticos tales como la búsqueda de números primos, y algoritmos de manejo de información tales como la búsqueda en bases de datos no ordenadas han sido teóricamente desarrollados con mucho éxito, utilizando los fundamentos de la criptografía cuántica.

La teoría de la criptografía cuántica está basada en las interacciones del mundo atómico y en futuras implementaciones de las computadoras cuánticas. Dichas computadoras aún están en los laboratorios de investigación pero ya se tienen resultados alentadores, como el desarrollo de la computadora Cuántica de cinco qubits desarrollada por Steffen et al [Steffen01].

2.1 Fundamentos de la Criptografía Cuántica

La Criptografía cuántica se basa en las propiedades de la interacción cuántica entre las partículas subatómicas, tales como la superposición simultánea de dos estados en una sola partícula subatómica. Esta propiedad fundamental de la interacción cuántica, es ampliamente aprovechada para el desarrollo teórico de los algoritmos cuánticos, logrando una capacidad de procesamiento exponencial.

La superposición Cuántica permite mantener simultáneamente múltiples estados en un bit cuántico, es decir "0" y "1" a la vez; a diferencia del bit – elemento fundamental en la criptografía actual – que únicamente es capaz de mantener un estado discreto alternativo a la vez, el "0" o "1" lógico. La criptografía cuántica aprovecha la superposición cuántica para lograr el paralelismo cuántico y el paralelismo cuántico masivo. Cualquier interacción con el mundo subatómico producirá un cambio en este, es decir, cualquier medición o lectura traerá indefectiblemente un cambio. Este fenómeno cuántico es aprovechado en la tele transportación cuántica para la transmisión de qubits, y asimismo es utilizada como mecanismo de seguridad en la criptografía cuántica.

2.2 Elementos básicos de la Criptografía cuántica

2.2.1 El bit cuántico "qubit"

El elemento básico de la criptografía cuántica es el bit cuántico o qubit[1] (*quantum bit* por sus siglas en inglés), un qubit representa ambos estados simultáneamente, un "0" y un "1" lógico, dos estados ortogonales de una sub partícula atómica, como es representada en la figura 1. El estado de un qubit se puede escribir como $\{|0\rangle, |1\rangle\}$, describiendo su múltiple estado simultáneo.

Un vector de dos qubits representa simultáneamente los estados 00, 01, 10 y 11; un vector de tres qubits, representa simultáneamente los estados 000, 001, 010, 011, 100, 101, 110, y 111; y así sucesivamente. Es decir, un vector de n qubits representa a la vez 2^n estados.

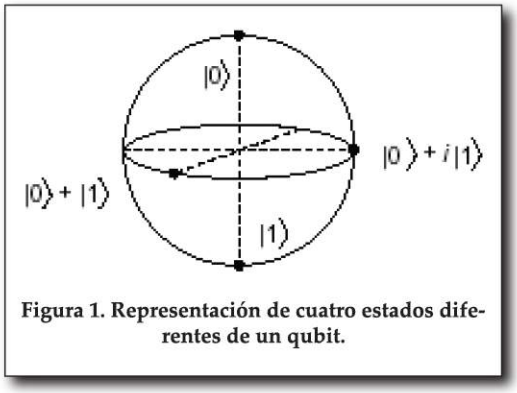

Figura 1. Representación de cuatro estados diferentes de un qubit.

Cualquier sistema cuántico con dos estados discretos distintos puede servir como qubit, un espín de electrón que apunta arriba o abajo, o un espín de fotón con polarización horizontal o vertical. En la figura anterior se tiene una representación gráfica de cuatro diferentes estados basado en el espín de un núcleo atómico, por lo que puede ser usado como un qubit. Un qubit no puede ser clonado, no puede ser copiado, y no puede ser enviado de un lugar a otro.

1 "qubit" término acuñado por Schumacher en 1995.

2.2.2 Compuertas Cuánticas

Las compuertas lógicas son operaciones unarias sobre qubits. La compuerta puede ser escrita como $P(\theta)=|0\rangle\langle 0| + \exp(i\theta) + |1\rangle\langle 1|$, donde $\theta = \omega t$. A continuación algunas compuertas Cuánticas elementales [Steane97]:

$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| =$ identidad
$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0| =$ NOT
$Z \equiv P(\pi)$
$Y \equiv XZ$
$H \equiv (1/\sqrt{2})[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]$

Donde I es la identidad, X es el análogo al clásico NOT, Z cambia el signo a la amplitud, y H es la transformación de Hadamard. Esas compuertas forman uno de los más pequeños grupos de la criptografía cuántica. La tecnología de la física Cuántica puede implementar esas compuertas eficientemente. Todos, excepto el CNOT, operan en un simple qubit; la compuerta CNOT opera en dos qubits. Una compuerta de dos qubits en especial interesante, es la conocida como "U controlada", [Steane97] $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$ son operadores actuando sobre dos qubits, donde I es la operación de identidad sobre un qubit, y U es una compuerta. El estado del qubit U es controlado mediante el estado del qubit I. Por ejemplo, el NOT controlado (CNOT) es:

$|00\rangle \rightarrow |00\rangle$; $|01\rangle \rightarrow |01\rangle$; $|10\rangle \rightarrow |11\rangle$; $|11\rangle \rightarrow |10\rangle$

2.2.3 *Procesamiento*

La capacidad computacional de procesamiento paralelo de la criptografía cuántica, es enormemente incrementada por el procesamiento masivamente en paralelo, debido a una interacción que ocurre durante algunas millonésimas de segundo. Este fenómeno de la mecánica cuántica es llamado *entanglement*. Debido a esto es que dos partículas subatómicas permanecen indefectiblemente relacionadas entre sí, si han sido generadas en un mismo proceso; por ejemplo, la desintegración en un positrón y un electrón. Estas partículas forman subsistemas que no pueden describirse separadamente. Cuando una de las dos partículas sufre un cambio de estado, repercute en la otra. Dicha característica se desencadena cuando se realiza una medición sobre una de las partículas [White00].

2.2.4 Tele transportación Cuántica

La tele transportación Cuántica es descrita por Stean [Steane97] como la posibilidad de "transmitir qubits sin enviar qubits". En la criptografía tradicional, para transmitir bits, estos son clonados o copiados y luego enviados a través de diferentes medios como el cobre, fibra óptica, ondas de radio y otros. En la criptografía cuántica no es posible clonar, copiar, o enviar qubits de un lugar a otro como se hacen con los bits.

Si enviamos un qubit $|\varnothing\rangle$ donde $\varnothing$ es un estado desconocido, el receptor no podrá leer su estado con certidumbre; cualquier intento de medida podría modificar el estado del qubit, por lo tanto se perdería su estado, imposibilitando su recuperación. La tele transportación Cuántica, resuelve este problema; esta se basa en el *entanglement* para poder transmitir un qubit sin necesidad de enviarlo. El emisor y el receptor poseen un par de qubits "enredados" (*entangled*). Entonces el qubit es transmitido desde el emisor, desaparece del emisor y el receptor tiene el qubit tele transportado. Este fenómeno es posible debido a un mecanismo conocido como el efecto EPR[2]. En la tele transportación Cuántica primero dos qubits E y R son "enredados" y luego separados, el qubit R es ubicado en el receptor y el qubit E es ubicado en el emisor junto al qubit original Q a ser transmitido; al realizar la lectura del estado de los dos qubits Q y E, estos cambian su estado a uno aleatorio debido a la interacción. La información leída es enviada al receptor, donde esta información es utilizada para un tratamiento que es aplicado al qubit R, siendo ahora R una réplica exacta del qubit Q [Nayak02] [Ambainis02].

2.2.5 El paralelismo cuántico

La superposición Cuántica permite un paralelismo exponencial o paralelismo cuántico en el cálculo, mediante el uso de las compuertas lógicas de qubits. [Steffen01] Los qubits, a diferencia de los bits, pueden existir en un estado de superposición, representado por $a|0\rangle + b|1\rangle$, donde a y b son números complejos que satisfacen la relación $|a|^2 + |b|^2 = 1$.

Dada una compuerta lógica de un qubit *f*, que transforma el estado $|a|$ en el estado $|f(x)|$, cuando el qubit de entrada tiene en el estado $(1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$ [Steffen01] una superposición igual de $|0\rangle$ y $|1\rangle$.

Por linealidad de la mecánica Cuántica [Steffen01], la compuerta lógica *f* transforma el estado del qubit a

$$(1/\sqrt{2})|f(0)\rangle + (1/\sqrt{2})|f(1)\rangle$$

2 La "correlación de Einstein-Podolsky-Rosen (EPR)" o *entanglement*, ha sido al menos en parte conocido desde los 1930s cuando fue discutido en un famoso paper por Albert Einsten, Boris Podolsky, y Nathan Rosen

El estado resultante es la superposición de los 2 valores de salida, siendo *f* evaluado para los 2 valores de entrada en paralelo. Para una compuerta lógica *g* de 2 qubits, que tienen dos qubits de entrada en superposición de $|0\rangle$ y $|1\rangle$, tendríamos una superposición de 4 estados $c_0|\mathbf{0}\rangle + c_1|\mathbf{0}\rangle + c_2|\mathbf{0}\rangle + c_3|1\rangle$.

La compuerta lógica *g* transforma el estado de entrada a $c_0|g(\mathbf{0})\rangle + c_1|g(\mathbf{0})\rangle + c_2|g(\mathbf{0})\rangle + c_3|g(1)\rangle$ [Steffen01] así *g* es evaluado en un solo paso para 4 valores de entrada. En una compuerta lógica *h* de 3 qubits, se tienen 3 qubits de entrada en superposición de $|0\rangle$ y $|1\rangle$, juntos hacen una superposición de 8 estados, que son evaluados en paralelo. Por cada qubits adicional la cantidad de estados se duplica.

3. *Criptosistemas Cuánticos*

La Criptografía cuántica es propuesta a principios de los 70 por Stephen Weisner, denominada *Conjugate Coding* y publicada eventualmente el 1983. Bennet y Brassard, quienes compartían ideas de Weisner, proponen el protocolo para la criptografía cuántica denominado "BB84" en 1984. No fue sino hasta 1989, en un laboratorio del Centro de Investigaciones de IBM (*International Business Machines*), que el primer prototipo experimental basado en este protocolo fue operable, la primera transmisión de señales Cuánticas fue a una distancia de 32 cm. En 1995, investigadores de la Universidad de Ginebra lo consiguieron utilizando una fibra óptica de 23 kilómetros de longitud. En 1997, Zbinden et al [Zbinden98] lograron distribuir Cuánticamente una clave a través de 23 Km de fibra bajo el lago Génova. Más adelante, el laboratorio de Los Álamos logró una distancia de 50 kilómetros.

Actualmente, ingenieros de la compañía Toshiba en Gran Bretaña han conseguido enviar un mensaje a más de 100 kilómetros por un cable de fibra óptica utilizando criptografía cuántica a la velocidad de 2 kilobits por segundo, lo que permitirá comercializar esta tecnología, incluso podría utilizarse la QKD (*Quantum Key Distribution*).

Los sistemas criptográficos cuánticos aprovechan el Principio de Incertidumbre de Heisenberg, el cual al medir un sistema cuántico en general lo perturba, ofreciendo información distinta a la de su estado antes de la medida. El escuchar detrás de las puertas en un canal de comunicaciones cuántico causa un disturbio inevitable. Los elementos del intercambio de información del quantum son observaciones del mismo; los fotones son puestos típicamente en un estado particular por el remitente y después observados por el destinatario. Debido al principio de incertidumbre, cierta información del quantum ocurre como conjugaciones que no se puedan medir simultáneamente. Dependiendo de cómo se realiza la observación, diversos aspectos del sistema pueden ser medidos – por ejemplo, las polarizaciones de fotones se pueden expresar en cualquiera de tres diversas bases: rectilíneo, circular y diagonal – pero observado en una base seleccionada al azar.

Así, si el receptor y el remitente no concuerdan en que base de un sistema del quantum están utilizando, el receptor puede destruir la información del mensajero sin ganar cualquier cosa útil. Éste, entonces, es el acercamiento total a la transmisión del quantum de la información: el remitente lo codifica en estados del quantum, el receptor observa estos estados y entonces, por la discusión pública de las observaciones, el remitente y el receptor convienen un cuerpo de la información que comparten (con probabilidad arbitrariamente alta). Su discusión se ocupa de los errores, mismos que se pueden introducir por ruido al azar o por *eavesdroppers*, pero debe ser en general para no comprometer la información. Mientras que la criptografía clásica emplea varias técnicas matemáticas para restringir a los indiscretos, en la teoría Cuántica la información es protegida por las leyes de la física. En la criptografía clásica una seguridad absoluta de la información no puede ser garantizada, mientras que el principio del enredo y la incertidumbre de Heisenberg se puede explotar en un sistema de la comunicación segura.

La criptografía del quantum proporciona los medios para que dos participantes intercambien una llave de codificación sobre un canal privado con completa seguridad. Hay por lo menos tres tipos principales de Criptosistemas para la distribución de llaves, estos son: **a)** Criptosistema con la codificación basada en dos observadores que no conmutan, propuestos por S. Wiesner, C.H. Bennett y G. Brassard, **b)** Criptosistema con la codificación construida sobre el enredo del quantum y el teorema de Bell, propuesto por A.K. Ekert, y **c)** Criptosistema con la codificación basada en dos vectores no ortogonales, propuestos por C.H. Bennett.

3.1 Criptosistema de quantum

El criptosistema de quantum se puede explicar con el ejemplo siguiente: el sistema incluye un transmisor y un receptor; un remitente puede utilizar el transmisor para enviar los fotones en una de cuatro polarizaciones:

0°, 45°, 90° o 135°, mientras que un recipiente en el otro extremo utiliza el receptor para medir la polarización. Según las leyes mecánicas del quantum, el receptor puede distinguir entre las polarizaciones rectilíneas (0° y 90°), o puede ser configurado rápidamente de nuevo para discriminar entre las polarizaciones diagonales (45° y 135°), pero nunca distinguir ambos tipos. La distribución dominante requiere varios pasos: el remitente envía los fotones con una de las cuatro polarizaciones que se liguen al azar; para cada fotón entrante, el receptor elige al azar el tipo de medida, rectilíneo o diagonal. El receptor registra las medidas y las mantiene secretas. El receptor posteriormente anuncia públicamente el tipo de medida (no los resultados) y el remitente dice al receptor que medidas estaban del tipo correcto. El remitente y receptor guardan todos los casos en los cuales las medidas del receptor son del tipo correcto. Estos casos se traducen en trozos (unos y ceros) y de tal modo se convierte en una llave. Un *eavesdropper* esta limitado para producir errores a esta transmisión , por que no sabe por adelantado el tipo de polarización de cada fotón, y la mecánica del quantum no permite que adquiera valores agudos de dos observadores que no conmuten (polarizaciones rectilíneas y diagonales). Los dos usuarios legítimos prueban el quantum para escuchar detrás de la puerta, revelando un subconjunto de azar de trozos dominantes y comprobando (en público) la tasa de error. Aunque no pueden evitar escuchar detrás de las puertas, un *eavesdropper* nunca los engañará, porque el esfuerzo sutil y sofisticado de golpear ligeramente el canal será detectado.

3.2 Criptosistema del enredo del quantum y el teorema de Bell

La idea principal de este criptosistema está basada en una secuencia de los pares correlacionados que la partícula genera, con un miembro de cada par que es detectado por cada partido (por ejemplo, un par de los fotones supuestos de Einstein Podolsky-Rosen, que polarizaciones son medidas por los partidos). Un *eavesdropper* en esta comunicación tendría que detectar una partícula para leer la señal, y retransmitirla en la orden para que su presencia siga siendo desconocida. Sin embargo, el acto de la detección de una partícula de un par destruye su correlación del quantum con la otra, y los partidos pueden verificar fácilmente si esto ha sido hecho, sin revelar los resultados de sus propias medidas, por el excedente de la comunicación en un canal abierto.

4. Compañías Comerciales Relacionadas

La criptografía cuántica teóricamente ha logrado evolucionar de forma satisfactoria y tiene definidos sus fundamentos con base en la interacción subatómica y sus elementos como el bit cuántico, compuertas Cuánticas, tele transportación de código, paralelismo cuántico y encriptación Cuántica. [Steane97] [Bennett98]. Aunque no se ha logrado implementar una comunicación Cuántica aún, se tienen grandes avances como la definición de una arquitectura Cuántica ampliamente aceptado por los investigadores [Oskin02], la implementación de pequeños prototipos como la computadora de 5 bits cuánticos desarrollada por Steffen et al [Steffen01], y el desarrollo de tecnologías Cuánticas comerciales [Johnson02a].

Las principales compañías que actualmente están realizando estrategias de desarrollo y comercialización con la criptografía cuántica son:

- MagiQ Technologies
- IdQuantique
- BBN Technologies
- D-Wave Systems
- IBM
- Hewlett-Packard,

IdQuantique quien actualmente tiene en el mercado el generador de números aleatorios cuánticos. En el futuro se espera que la criptografía cuántica, esté completamente desarrollada (aproximadamente entre el 2020 a 2025), y tome el lugar de las Criptografías actuales. Una muestra de lo que ocurrirá es *Magiq*, la primera empresa que lanzará al mercado tecnología de Encriptación Cuántica, capaz de codificar flujos de datos y enviarlos a altas velocidades por las troncales de Internet, de forma similar a los trabajos experimentales desarrollados por Prem Kumar y Horace Yuen, profesores de la Universidad Northwestern [Johnson02a] [Johnson02b].

5. Conclusiones

Dos limitaciones importantes enfrenta la implementación de la criptografía cuántica: 1) la presencia de elementos en estado líquido y gaseoso en el proceso de interacción subatómica, que hacen muy difícil el lograr modelos donde intervengan miles de bits cuánticos. 2) no se puede realizar una lectura sin producir cambios en ella, limitación dada por la naturaleza de las interacciones

con los elementos subatómicos. Estos cambios son impredecibles y se propagan a lo largo de todo el sistema, por lo que es necesario integrar complejos mecanismos de corrección de errores que agregan sobrecarga en proporciones exponenciales. No obstante, en las próximas décadas serán realidad y de uso cotidiano los criptosistemas cuánticos en las redes como la Internet, gracias a los avances tecnológicos de la computación cuántica.

Agradecimientos

MAMV agradece el apoyo recibido del programa EDD del IPN.

RSO agradece el soporte económico recibido por la Secretaría de Investigación y Posgrado del IPN (SIP-IPN), a través del proyecto 20071024 y del programa EDI, así como del Sistema Nacional de Investigadores (SNI-México).

Referencias

[Ambainis02] Ambainis, A., Smith, A., Yang, K., "Extracting Quantum Entanglement", in Proceedings of the 17th IEEE Annual Conference on Computational Complexity" (2002).

[Bennett98] Bennett, C., Shor, P., "Quantum information theory", in Information Theory, IEEE Transactions (Volume: 44 Issue: 6 , Oct. 1998), Page(s): 2724 -2742.

[Beth00] Beth, T., "Quantum Computing: An Introduction", in ISCAS 2000 – IEEE International Symposium on Circuits and Systems (May 28-31, 2000, Genova, Switzerland).

[Hughes94] Hughes, R., J., "Quantum Cryptography", (1994).

[Johnson02a] Jonson, R., "Magiq employs quantum technology for secure encryption", in EETIMES, http://www.eetonline.com/at/news/OEG20021105S0019 (November 6, 2002).

[Johnson02b] Jonson, R., "Quantum encryption secures high-speed data stream", in http://www.eetonline.com/at/news/OEG20021107S0031 (November 8, 2002).

[Keyes01] Keyes, R., "Fundamental limits of silicon technology", in Proceedings of the IEEE (Volume: 89 Issue: 3, March 2001), Page(s): 227 -239.

[Nayak02] Nayak, A., Salazman, J., "On Communication over an Entanglement-Assisted Quantum Channel", in Proceedings of the 34th Annual ACM Symposium on Theory of Computing (2002).

[Oskin02] Oskin, M., Chong, F., Chuang, I., "A Practical Architecture for Reliable Quantum Computers", in Computer (Volume: 35 Issue: 1, Jan. 2002), Page(s): 79 -87.

[Steane97] Steane, A., "Quantum Computing", in Department of Atomic and Laser Physics (University of Oxford, , England, July, 1997).

[Steffen01] Steffen, M., Vandersypen, L., Chuang, I., "Toward Quantum Computation: A Five-Qubit Quantum Processor", in IEEE MICRO (Volume: 21 Issue: 2, March-April 2001). Page(s): 24 -34.

[Svennson01] Svennson, C., "Future of CMOS – physical limits, trends, and perspectives", in QNANO Workshop (2001).

[White00] White, A., James, D., Munro, W., Kwiat, P., "Measuring entanglement and entanglement measures", in Quantum Electronics and Laser Science Conference (2000), Page(s): 163 -163.

[Zbinden98] Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., Zbinden, H., "Automated 'plug and play' quantum key distribution", Electronics Letters (Volume: 34 Issue: 22 , 29 Oct. 1998), Page(s): 2116 -2117.