Universidad de Concepción

Departamento de Física

DISTRIBUCIÓN DE LLAVE CUÁNTICA RESISTENTE A ATAQUES "SIDE-CHANNEL" A LOS DETECTORES

Tesis para optar al Grado de Magíster en Ciencias con Mención en Física

Autor:
Pablo González G.

Supervisor:
Dr. Wallon Tadaiesky N.

Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Departamento de Física
Concepción, Chile.

Julio 2013

Capítulo 1

Introducción

La criptografía se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad la información en una comunicación entre dos o más entidades con relación a agentes externos al proceso [1]. Actualmente para las transacciones bancarias, comunicaciones que imponen seguridad como las gubernamentales y militares, utilizamos criptografía. Uno de los métodos más conocidos es el RSA (Rivest, Shamir y Adleman) [1, 2]. Esta codificación se basa en la dificultad de poder factorizar números enteros primos con muchos dígitos. Entonces el problema de romper el código y obtener la información se basa en un problema computacional y tecnológico. Mejores computadores y algoritmos podrían romper la seguridad y de esta manera obtener el mensaje enviado. Actualmente en el área de información cuántica se están desarrollando prototipos de computadores cuánticos [3], los que en principio podrían romper las más eficientes formas clásicas de criptografía. Paralelamente al área de computación cuántica, se desarrolló el área conocida como criptografía cuántica, la que aplica los principios de la mecánica cuántica para imponer seguridad en la comunicación [4, 5, 6, 7, 8]. Para establecer esta comunicación entre dos partes necesitamos de un protocolo de distribución de llave cuántica (**QKD**) seguro, con el cual se genera una llave en común.

Hoy en día, el área de invesitigación en **QKD** se enfrenta al hecho de intentar cerrar la brecha entre la teoría y la práctica. La forma de garantizar la seguridad de un protocolo específico de **QKD** se basa en la mecánica cuántica más el modelamiento de las condiciones realistas de la implementación del protocolo [4]. Enfocándonos en los problemas realistas de la implementación, existen distintos tipos de ataques diseñados para obtener parte importante de la información enviada. Uno de los ataques más importantes considerando la implementación del protocolo (por ejemplo: el canal, los detectores, la óptica de control, etc.) es conocido de manera general como "side-channel" [9, 10, 11]. Este tipo de ataque se aprovecha de cualquier información obtenida de la implementación física de un protocolo criptográfico [12] (información de tiempo, consumo de energía, pérdidas electromagnéticas, etc.). Nos enfocaremos en el ataque "side-channel" a los detectores ya que en la presente tesis