

Quantum Insecurity of Classical Security; A Descriptive Example

Robabeh Rahimi^{* 1}

* PhD, Postdoctoral fellow

¹ Department of physics, Kinki University, 3-4-1 Kowakae, Higashi Osaka, Osaka 577-8502, Japan

Abstract Type: Descriptive

Keywords: *Quantum computing, Security, RSA, Factorizing, Shor's algorithm*

Background and Aim :Background; The articles about classical security. Aim; A quantum computer is more powerful than a classical one.

Discussion and Conclusions: Discus.; With an easy numerical example fragility of classical security is shown. Conclus.; understanding of quantum computer is necessary and useful.

The technology of computers has been developing very fast so that our life wouldn't appear easily possible without assistance from the current advanced computers. These computers are called classical computers since they are developed based on classical physics. Classical computers are developed to fancy tiny sizes with numerous computational powers but still there are some problems that remain intractable for a classical computer. A significant example is the problem of finding prime factors for an integer. Consequently, the prime factorizing problem has been used for producing secure keys in algorithms such as RSA; publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT. Then, RSA security has been used for years for encrypting messages such as remote purchase through the Net. If one finds a solution for prime factorizing problem then RSA would be broken in its security.

Recently scientists tend to make computers based on quantum laws of physics hence called quantum computers. Speaking about the power of a quantum computer in comparison to a classical computer, there is an algorithm, namely Shor's algorithm that gives an efficient solution for prime factorizing problem. Then, it is expected that by realizing a working quantum computer and employing Shor's algorithm, then the RSA security will not be secure anymore. Instead one may hang on a new security protocol that can be quantum cryptography. In this talk, with a simple numerical example, I explain how RSA works and why it is fragile against quantum computation.