Modifying IKE to use Quantum Key Distribution

永山 翔太
kurosagi@sfc.wide.ad.jp
慶應義塾大学

Rodney Van Meter
rdv@sfc.wide.ad.jp
慶應義塾大学

概 要

量子コンピュータの持つ能力が明らかになるに連れて，既存のセキュリティシステムが受ける影響もまた明らかになって来ている．量子コンピュータの巨大数を効率的に因数分解する能力は，Diffie-Hellman 鍵共有アルゴリズムや，公開鍵暗号系の技術を無力化することが既に分かっている．また，量子鍵配送 [1] は，物理的に安全性が証明されているため Diffie-Hellman 鍵共有アルゴリズムが無力化された後も利用できる秘密鍵共有アルゴリズムである，本研究では Internet Key Exchange（IKE）の，量子鍵配送を用いる新しいプロトコルを提案する．本研究の結果，量子コンピュータが実現した後も使用できる暗号化通信が実現する．

問題点

暗号化通信技術は既に人々の生活基盤となり，欠く事ができない物となっている．これらの暗号化通信技術に用いられる Diffie-Hellman 鍵共有アルゴリズムや公開鍵暗号は，巨大数の因数分解には効率的に解決するアルゴリズムが存在せず，計算に膨大な時間が必要となることに安全性の根拠を置いている．そのような中で，量子コンピュータは，巨大数を効率的に因数分解できることが Peter Shor によって示された [2]．これは，量子コンピュータが開発された後には，現在利用されている暗号化通信技術が安全性の根拠を失うため利用できなくなることを意味している．鍵暗号が無力化される前に，因数分解の困難性に依らない暗号化通信システムの構築が必要である．

量子鍵配送は，量子力学の不確定性原理に安全性の根拠を置いている鍵共有技術であり，数学的に安全性が証明されている．量子鍵配送を行う専用機器は，鍵を作成する相手側の量子鍵配送機器を認証し，鍵の生成を行う．本研究では，公開鍵暗号の代わりに量子鍵配送を用いて既存のインターネットで暗号化通信を行うためのプロトコルを提案する．

手法

IKEv2 では，最初に IKE 同士の通信・管理用の IKE_SA（Security Association）を張り，その後 IKE_SA 内で，暗号データを送受信するための IPsec _SA のステータスや鍵を交換する．よって，IKE_SA の暗号化鍵に量子鍵配送で作成した鍵を用いる事により，暗号データの送受信に際しても量子鍵配送の安全性で通信を行うことが出来る．本研究では，IKE_SA の作成に量子鍵配送の鍵を利用することを目的とする．

量子鍵配送には専用の機器と，間に増幅器などを挟まない一本の専用光ファイバーが必要である．本研究では，IKE に WIDE プロジェクトの racoon2 を用い，量子鍵配送機器に NEC 社の QUICS を利用した．図 1 にネットワーク構成を示す．

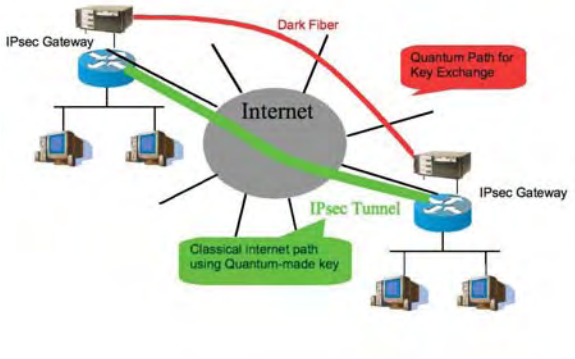

図 1: 量子鍵配送を利用する IPsec におけるネットワーク構成

量子鍵配送を用いる際に，IKE が折衝しなければならない点が二つある．一点目は，量子鍵配送で順次作られる鍵のうちどれを用いるかの折衝で，これは IKE_SA 内に量子鍵配送ペイロードを作成し行う．二点目は，鍵の作成速度を利用速度が上回ってしまった場合の方策である．鍵の生成そのものについては量子鍵配送機器が行う，鍵の管理については鍵を利用する側で考えなければならない．

謝辞

本研究を行うにあたり，機材提供をしてくださった NEC 様に感謝致します．

参考文献

[1] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE, December 1984.

[2] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc. 35th Symposium on Foundations of Computer Science*, pages 124–134, Los Alamitos, CA, 1994. IEEE Computer Society Press.