卒業論文　　2009年度 (平成21年度)

量子鍵配送を用いたIPsecのための Internet Key Exchangeの設計と実装

慶應義塾大学 総合政策学部

氏名：永山 翔太

指導教員

慶應義塾大学 環境情報学部

村井 純

徳田 英幸

楠本 博之

中村 修

高汐 一紀

重近 範行

Rodney D. Van Meter III

植原 啓介

三次 仁

中澤 仁

平成25年12月10日

卒業論文要旨 - 2009 年度 (平成 21 年度)

量子鍵配送を利用したIPsecのための IKEプロトコルの設計と実装

本研究では，量子鍵配送で共有した鍵を用いて IPsec を行うための Internet Key Exchange の拡張システムを構築した．

現在開発中である量子コンピュータは，素因数分解を効率的に解くこと可能であり，Diffie-Hellman 秘密鍵共有方式を無力化することが示されている．量子コンピュータが開発された後も暗号化通信を実現するためには，素因数分解に依らない安全性を持つ秘密鍵共有アルゴリズムを用いた暗号化通信システムが必要である．

本研究では，量子力学により数学的に安全性が保証されている量子鍵配送を用いた IPsec を行うための，Internet Key Exchange の拡張を行った．本研究により，

Internet Key Exchange は，システム外で共有した鍵を用いることが可能となり，は，量子技術を用いた新しい共有秘密鍵共有アルゴリズムである．量子鍵配送は，

キーワード
1．量子鍵配送, 2．Internet Key Exchange, 3．IPsec

慶應義塾大学 総合政策学部

永山 翔太

Abstract of Bachelor's Thesis

Academic Year 2008

Designing and Implementation of IP Multicast Dvrelay to Adapt the communications quality

Keywords :
1. STREAMING, 2. adaptive communication, 3. IP Multicast

Keio University, Faculty of Environmental Information

Gen Mineki

目 次

図 目 次

表 目 次

第1章　序論

本章では，本論文の背景，目的を明らかにする．また，本論文の構成を示す．

1.1　背景

インターネットは登場以来，コンピュータの発展と共に機能の拡張を続け，今や人々の生活に欠かせないインフラストラクチャーとなっている．その用途は多岐に渡り，民間サービスも公共サービスもインターネットを利用しない物はもはやないと言ってよいだろう．インターネットを介する情報の高速転送は，情報化社会の立役者である．しかしながら，インターネットの利用は何の危険も伴わないというわけではない．インターネット上には様々な脅威が存在し，その多くは，データの盗難やサービス不能を目的としている．脅威からデータやコンピュータを守るため，暗号化通信や認証，ファイアウォールなどのセキュリティ技術が考案され実際に運用されている．

暗号化通信は，データの漏洩を防ぐために存在する．通信パケットを盗み見られても，データに暗号化が施されていれば，盗聴者にはデータの内容を知る事が出来ないのである．暗号化通信は，暗号化するための鍵と暗号化アルゴリズムによって実現される．暗号の強度は，暗号化鍵の安全性と暗号化アルゴリズムの強度に影響される．このどちらかが破られれば，暗号は解かれ，通信内容は漏洩してしまうのである．

現在，暗号化鍵の共有には，公開鍵暗号と Diffie-Hellman 暗号化鍵共有アルゴリズムが利用されている．これらは，共に素因素分解問題を利用したアルゴリズムである．ノイマン型コンピュータは巨大数の素因数分解を効率的に解く事が不可能であることに安全性の根拠を置いており，素因数分解を解くアルゴリズムが見つからない限り今後も安全であると考えられる．

[1]

1.2　本研究の目的

1.3 本論文の構成

第2章　要素技術

2.1　量子鍵配送

量子鍵配送は，量子情報によって実現される新しい秘密乱数共有アルゴリズムである．量子鍵配送の特徴は，量子の観測するまで状態が確定せずなおかつ観測すると必ず状態が一意に確定する性質に依り，第三者に因る盗聴を確実に検知できる点である．

量子鍵配送は既に実現されており，今現在実装されている量子鍵配送装置は全て量子状態伝達素子に光子を用い，光ファイバーの中を通して通信を行うものである．光子の量子状態を変更しないために，この光ファイバーにはアンプを入れる事はできない．また，既存のネットワーク機器を入れる事も出来ず，量子鍵配送のルーティングのためには専用の量子ネットワークを構成する必要がある．

2009 年 12 月現在 NTT Communications に因る 20km 間 10Mb/s が最速である．

2.2　IPsec

IPsec は，OSI7 階層中第 3 層ネットワーク層で通信を暗号化する暗号化プロトコルである．IPsec は通信に秘匿性，完全性，認証を与えることが可能である．IPsec によって作られた暗号化通信路は Security Association(SA) と呼ばれるパラメータの集合によって認識される．SA には暗号化鍵の他に，暗号化プロトコルや SA のライフタイムなどのパラメータを持っている．

IPsec の運用形態はトンネルモードとトランスポートモードの二種類があり，トンネルモードは拠点間における暗号化通信に，トランスポートモードは拠点ネットワークと単体間における暗号化通信に利用される．

2.3　Internet Key Exchange

Internet Key Exchange(IKE) は，IPsec をマネジメントするためのプロトコルである．IKE の主な役割は以下の二つである．

- 暗号化鍵の共有
- 鍵の使い方の調整

IKE は暗号化鍵の共有に Diffie-Hellman 鍵共有アルゴリズムを用いる．IKE は IPsec を行うために二種類の SA を管理する．一つは CHILD_SA と呼ばれる SA で，この SA を用いて実際にやり取りしたいデータの暗号化通信を行う．もう一つは IKE_SA と呼ばれる SA で，IKE_SA は新しい SA の折衝や IKE の状態管理を行うための SA である．

IKE は図 2.1 のような動作シーケンスから成る．

ぬるぽ

図 2.1: IKE 動作シーケンス図

2.4 Diffie-Hellman 鍵共有アルゴリズム

Diffie-Hellman 鍵共有アルゴリズムは，素因数分解には効率的なアルゴリズムが見つかっていない事に基づく，離れた二者間で共有秘密鍵を共有するためのアルゴリズムである．Diffie-Hellman 鍵共有アルゴリズムは，図 2.2 にある計算式で秘密鍵を計算する．

ぬるぽ

図 2.2: Diffie-Hellman 鍵共有アルゴリズム計算式

第3章　関連研究と問題点

ほげ

第4章　アプローチ

本論文では，量子鍵配送で共有された乱数を，IKEv2 によって管理して IPsec の暗号化鍵に用いることを目的とする．

4.1　新構造と前提

本研究に於けるネットワークは図 4.1 のように構成される．

図 4.1: IPsec with QKD ネットワーク図

まず，両サイドにそれぞれ一つずつ IPsec Gateway と量子鍵配送装置 IPsec Gateway は IP ネットワークを通じて逆サイドの IPsec Gateway と繋がっている．また，量子鍵配送装置は量子ネットワークを通して逆サイドの量子鍵配送装置と繋がっている．両サイドに於いて，IPsec gateway と量子鍵配送装置はローカル接続されている．この接続は確実に

安全でなければならず，つまりは認証されておりなおかつ送受信に於いて信頼性が確認されておらねばならない．この接続は物理的には専用線が望ましい．

量子鍵配送装置は，共有した秘密乱数を IPsec Gateway に供給する．本研究においては，本ネットワーク中に存在する量子鍵配送装置で共有される秘密乱数は全て本ネットワーク中の IPsec Gateway で利用されることとする．

4.2 IKE 拡張モデルに対する要求事項

4.3 量子鍵配送を用いるための拡張切り分け

ほげ

第5章　設計

ほげ

第6章　実装

ほげ

第7章　評価

ほげ

第8章　結論

ほげ

謝辞

参考文献

[1] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *IEEE*, 1994.

付 録A　Appendix

IPsec Maintenance and Extensions S. Nagayama
Internet-Draft R. Van Meter
Intended status: Experimental Keio University
Expires: April 22, 2010 October 19, 2009

IKE for IPsec with QKD
draft-nagayama-ipsecme-ipsec-with-qkd-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 22, 2010.

Copyright Notice