A cryptographic communication by an almost secure message transmission

KINOSHITA Lab. KURIYAMA Tomoya (200602825)

Abstract

A public key cryptosystem needs a trusted third party that proves the legitimacy of public keys. However,an n-channel secure message transmission (SMT) scheme does not need one, because a sender and a receiver can transmission without sharing any prior key. In this paper,we study an n-channel SMT scheme, which is a scheme to securely transmit a document through n channels. There are two kind of SMT called PSMT and ASMT. We propose and mount a improved protocol that improves the wire traffic of basic protocol.

従来の公開鍵暗号方式では公開鍵の正当性を証明するために信頼できる第三者機関が必要であった。それに対して n チャネルメッセージ伝送方式では事前の鍵が不要なため第三者機関も必要がない。そこで本論文では n チャネルメッセージ伝送方式に着目している。n チャネルメッセージ伝送方式とは文書を n 本の通信路を使用して安全に送信する暗号化通信方式である。n チャネルメッセージ伝送方式には PSMT と ASMT という 2 つの方式があり、本論文では ASMT に着目している。Basic プロトコルの通信効率を改善した改良プロトコルを提案実装する。