要 旨

ワンタイムパスワード認証方式を用いた
鍵共有方式の検討

中 山　優

インターネットの普及に伴い，近年では，個人情報や金銭情報などの秘匿すべき情報がインターネット上で扱われている．これらの情報を安全に扱うためには，暗号化通信技術が必要である．既存の暗号化通信技術では，暗号化通信に用いる鍵の共有に，価格コストや処理コストが必要となる．これらのコストを抑えた鍵共有方式として，ワンタイムパスワード認証方式を用いた鍵共有方式が提案されている．しかしながら，先行研究では，一つの OTP 認証方式についてのみ検討されており，他の方式については述べられていない．また，ワンタイムパスワード認証方式を鍵共有方式に応用した際の安全性についても十分に議論されていない．

そこで本論文では，既存のワンタイムパスワード認証方式を用いた鍵共有方式について検討した．検討内容として，12 種類のワンタイムパスワード認証方式に対して，本論文で定義した性質を満たすかどうかを確認した．その結果，1 種類のワンタイムパスワード認証方式が鍵共有方式として適していることが分かった．さらに，鍵共有方式として適しているワンタイムパスワード認証方式の特徴を，抽出することができた．そして，これらの検討結果から，鍵共有方式に適したワンタイムパスワード認証方式を提案した．

キーワード　個人情報, ワンタイムパスワード認証方式, 暗号化通信, 鍵共有

Abstract

A Key Sharing Scheme with a One-Time Password Authentication Protocol

Yu NAKAYAMA

Various information are sent on public networks. Cryptosystems are necessary for protect these information. Existing key sharing scheme need money costs and processing costs. A key sharing scheme with a one-time password authentication protocol is proposed. However, safety of key sharing scheme with a one-time password authentication protocol is not studied enough.

In this paper, we studied about key sharing scheme with a one-time password authentication protocol. We defined key sharing condition for one-time password authentication protocol. As a result, we discovered characteristic of one-time password authentication protocol that can share the key. And, we proposed one-time password authentication protocol to share the key.

key words personal information, one–time password authentication, encryption communication, key sharing