要 旨

低処理負荷端末向け双方向 VoIP 暗号化通信システムの構築

幸 地　勇 明

近年，スマートフォンの普及により，携帯端末上で様々なアプリケーションを手軽に実行できるようになった．また，公衆無線 LAN サービスの普及により屋外で無線 LAN サービスを利用できるようになった．スマートフォンにおいて VoIP 通信を実現することで，ユーザは手軽に安価で音声通話を行うことができる．しかし，公衆無線 LAN を用いた VoIP 通話は第三者によって盗聴されてしまう危険がある [1]．この問題に対する先行研究として，本研究室の小野らによる VoIP を用いた音声通話アプリケーション SAS-Phone が挙げられる [2].

SAS-Phone が採用している SAS-2 は計算コストが少なく高速な鍵交換が可能 [3] であり，非常に秘匿性の高い VoIP 通信を実現している．しかし，SAS-Phone では，技術的な課題により双方向通信が実現できていなかった．また，片側の通信に約 600ms の遅延が発生している．この値は ITU-T によって規定されている許容遅延時間を超えているため，SAS-Phone は VoIP アプリケーションとして実用的であるとは言えない.

本研究では小野らの研究を引き継ぎ，アルゴリズムや実装方法の最適化を行うことで，双方向通信が可能で，より実用的な SAS-Phone を開発した．これにより実用的で秘匿性の高い音声通話が可能になった.

キーワード　VoIP, 携帯端末，暗号化, ワンタイムパスワード, SAS-2

Abstract

The development of a bidirectional VoIP communication system for handheld devices

Kouchi, Takeaki

Today's expanding of smartphone made possible to execute various applications easily on mobile devices. And, increasing of public wireless LAN service made possible to use Wireless LAN service in larger area of outside. By actualizing VoIP communication on smartphone, users can use voice call easier and more inexpencive.

There is a previous research on voice call application using VoIP named SAS-Phone made by Ono at our lab. But, cause of technical reason, the previous research: SAS-Phone couldn't implement duplex communication. And, it delays about 600ms for one side communication. The acceptable latancy of VoIP is known as under 400ms. Therefore current SAS-Phone is not practical as a VoIP application.

In this research, I developed duplex communicatable and more practical SAS-Phone, by inheritancing the research by Ono et al. and optimize its algorithm and implimentation. It make possible to use voice call that is practical and secure.

key words VoIP,mobile device, Encryption, One-time password, SAS-2