諏訪東京理科大学
コンソーシアム専用

諏訪東京理科大学
「一技(ひとわざ) シーズ」PRシート

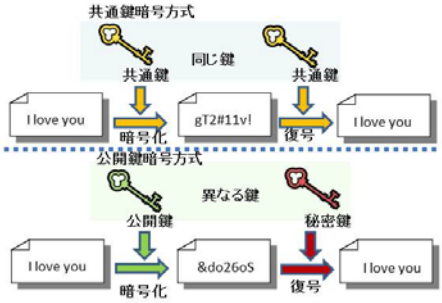
分類No：A-3

ひとわざ(一技)シーズ名： 暗号技術、アドホックセキュリティ技術

1. シーズ概要(200字目安) 研究技術内容　　セールスポイント

近年暗号技術が注目を集めています。その中で最新技術として、①共通鍵暗号技術(小規模高速共通鍵暗号等)②公開鍵暗号技術(IDベース公開鍵暗号等)③認証アルゴリズム④セキュリティプロトコル(SSL等)(タイムカプセル暗号等)、等が注目されています。これら技術を新規に適用することで、従来には無かった機能が実現できます。またそれら技術の応用として当研究室ではアドホックセキュリティ技術を研究開発しています。従来アドホックネットワークにおける問題点としては、①利用者の端末が攻撃されたりするセキュリティの問題②「他者の通信を中継しない」という「セルフィッシュ・ノード(自分勝手なノード)」を排除する問題③P to Pネットワークで起こっているように，ユーザーの使っている携帯電話機からウイルスが拡散するような可能性、等がありましたが暗号技術の適用でこれらを解決することができます。

2.写真・図(技術要点説明)



主要な技術
・共通鍵暗号技術
・公開鍵暗号技術
・認証アルゴリズム
・セキュリティプロトコル(SSL等)

最新技術の適用
・共通鍵暗号技術
(小規模高速共通鍵暗号等)
・公開鍵暗号技術
(IDベース公開鍵暗号等)
・認証アルゴリズム
・セキュリティプロトコル(SSL等)
(タイムカプセル暗号等)

3.産業への活用方向　　(適応業界・分野等)

情報通信、医療システム

4.関係する大学・企業等

各大学の電気情報通信系の学科、電気、情報通信系、医療システム系の企業

5. 研究室概要

学　科　名	コンピュータメディアエ学科	研　究　分　野	研　究　者　名
		ネットワーク・セキュリティ	杉田　誠
主研究テーマ	ネットワーク・セキュリティ技術の研究		
主要キーワード	ネットワーク、セキュリティ、ワイヤレス、暗号		

特記事項