電子署名付き音声ストリームを用いたIP電話システム

宇田 隆哉（東京工科大学）
高田 和泉（慶應義塾大学大学院）

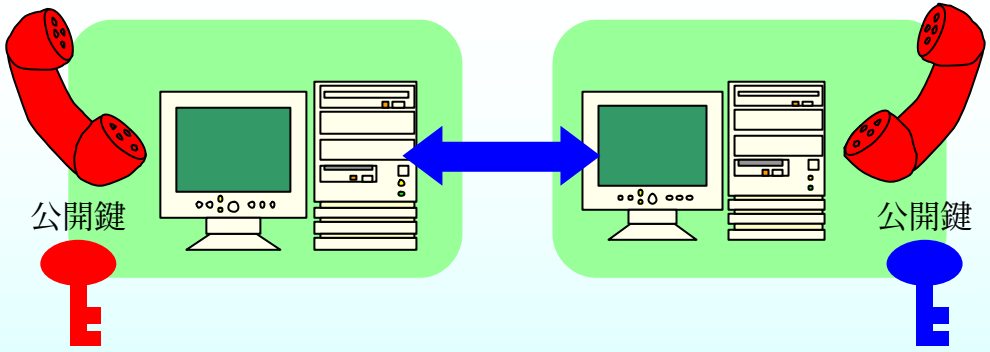
音声通話内容に対して電子署名を添付することにより、録音された音声を証拠能力の高い資料として使用可能

話し手：話した内容の否認ができない
聞き手：相手が話した内容を都合の良いように編集できない

認証局により認証された公開鍵を所有していれば、通話データは認証サーバを介さずに直接相手の端末に送信されるため、サーバを介して記録することにより通話内容の証明を行うシステムと比較して安価にサービスを提供可能。

本システムを利用して通話される電話の音声には、公開鍵による電子署名が添付されており、電子署名法に基づくセキュリティ強度を保ちつつ、リアルタイムな通話が可能。本システムでは、通話時に認証サーバを介さずに音声ストリームを認証するため、電話による安価な商取引などを低コストに実現可能である。また、使用する電話端末の演算性能や、ネットワークの品質に応じて署名の負荷やパケットロス耐性を変化させることができ、無線通信を用いた小型端末による通話など、ユビキタスな環境での使用にも適している。

通話中は認証サーバを介すことなくP2Pにて認証可能



- ***言った、言わない」問題の解決***
- ***不当な勧誘、脅迫、詐欺の抑制***
- ***都合の良い音声編集の防止***
- ***高圧縮低品質な音声データの証拠能力向上***

ネットワークによる遅延時間、通信帯域、通信品質などから公開鍵署名の間隔を決定し、ハッシュと組み合わせることにより演算の効率化を図る。バーストロス、ランダムロスのいずれの場合にもパケットロス耐性を持ち、電子署名の確認が途切れることなくシームレスな音声通話を実現。