電子署名付き音声ストリームを用いたIP電話システム

1. 背景

ブロードバンド時代に突入し、高速な有線もしくは無線による安価な常接回線が各家庭にも設置され、その付加的なサービスとしてIP電話が普及しつつある。IP電話は既存の公衆回線網との相互接続が可能であり、通話料金が非常に安価であることから、今後は全世界的に電話の主流となっていくと考えられる。本提案はIP電話の会話内容に対する効率の良い電子署名方式である。現在のIP電話は既存の公衆回線電話の代替として使用されているだけであり、デジタル音声が送受信されているにも関わらず、その特徴がセキュリティに生かされていないといえる。そこで当該開発ではIP電話の音声ストリームに対して、送受信遅延をできるだけ抑えつつ公開鍵署名を施すことで、通話内容の認証を可能とするシステムを提案する。

2. 目的

本研究は、音声通話における通信経路の暗号化と誤解されやすいが、本研究が目指すものは通信経路の暗号化でも通信相手の認証でもなく、通話内容の認証である。

電話の通話内容に電子署名を施すことが可能になれば、電話での注文や契約がより安全に行えるようになる。現在でも問題になっている、いわゆる言った言わない問題も、会話内容が署名されていれば送信者、受信者ともに都合の良い編集は不可能になる。また、勧誘の方法が不当な場合や、脅迫まがいの契約、電話詐欺などを防止することもできる。現在の電話でも会話中の音声を録音することは可能であるが、会話内容を都合のいいように編集し、途中を消去して自分に不利な部分だけ削り落としたり、順番を入れ替えたりするといったような操作を加えることも不可能ではない。デジタル映像やデジタル音声に関しては、品質（画質・音質）が非常に良い状態であれば、編集の継ぎ目が露見したりするなど、完全な偽造加工が難しいとされているが、署名方式を用いれば、品質の悪い映像や音声でも編集の痕跡を消すことは不可能であり、証拠となる映像や音声を高圧縮の状態で保存できるため、長時間の録画や録音にも向いている。

3. 開発の内容

当該開発のIP電話プログラムはWin32が使用可能な全てのWindows上で動作すると思われる。なお、ユーザインタフェース部のグラフィックは全てプログラムのリソースとして定義しているため実行ファイル単体で動作し、インストール作業などはとくに必要としない。当該開発におけるユーザインタフェースのコンセプトとしては、署名や認証の難しい理論と

は関係なく一般ユーザにわかりやすく使いやすいものにするということを一番に考慮した。当該開発で実装した IP 電話のユーザインタフェースを図 1 に示す。

図 1: IP 電話のユーザインタフェース

当該開発の IP 電話は、通常のアプリケーションと同様、Windows 上で IP 電話プログラムのアイコンをダブルクリックするなどすれば起動する。操作画面はシンプルであり、基本的な操作は電話番号のボタンと通話ボタンによって行われる。

電話を掛けたいユーザは相手の端末の IP アドレスを、番号ボタンを押して入力する。今回の開発では、IP 電話の電話番号と IP アドレスの変換を行う基地局などを設けていないため、相手の IP アドレスを入力する仕様になっているが、通常の IP 電話が 050 から開始される電話番号を所有しているため、本格的にサービスを稼働させるのであれば、電話番号と IP アドレスの変換テーブルを持つなんらかのサーバと交信し、相手の IP アドレスを取得することが望ましいと思われる。当該開発の実装では、電話を掛けるための制御信号は音声通話とは別に TCP/IP によるコネクションにより送信しているため、通話開始前に TCP/IP によるコネクションをサーバと確立し、電話番号を IP アドレスに変換した結果を得た後に相手に通話のコネクションを張るようにすることは難しいことではない。また、当該開発では認証局を実装していないため、公開鍵署名に使用される公開鍵が本人の物であるという証明書を確認していないが、実運用の段階になれば、今までに着信を受けたことのない人から初めて電話が掛かってきた場合は、通話開始前に認証局に相手の公開鍵の証明をしても

らうため、認証局との接続が必要となる。なお、「CLR」ボタンを押すと、誤入力した番号を 1 文字消去することが可能である。

相手の IP アドレスを入力した後、「通話」ボタンを押すことにより、相手の IP 電話に対して TCP/IP による接続が行われ、呼び出し先の電話からは着信音が鳴る。着信を受けた電話の利用者は、「通話」ボタンを押せば電話に出ることができる。この時点で相互通話が開始され、通常の電話による通話と同じように利用できる。

音声通話が行われている時に、相手の音声データの署名が確認できていれば、「署名 ON」のランプが明滅する。「署名間隔」欄にはその時点で使用されている署名間隔が表示される。利用者は本開発による電話の詳しい署名の原理などを知らずとも、「署名 ON」のランプの点灯を見れば相手の音声の署名が正しく確認できていることを認識できる。

相手との通話中に「録音」ボタンを押すと、通話内容を録音できる。この録音は、音声部分だけを記録するのではなく、受信したパケットをそのまま記録するものである。

相手との通話を終了した後に「再生」ボタンを押せば、最後に記録した音声が再生できる。なお、改竄されたパケットがあったとしてもそのまま記録されてしまうが、認証が成功しないパケットは実際の通話時にも録音した音声の再生時にも音声として再生されないため、通話時に聞こえた音と同様の音が再生されるため問題ない。

もし、受信者が記録したデータの音声部分を、パケットの順番を入れ替えたり他の音声に置き換えるなどして改変したりした場合、パケットに含まれているハッシュ値および公開鍵署名が一致しなくなり、正しく再生されない。この記録データは、電子署名法により裁判での証拠として署名捺印した紙面と同等の法的効力を持つ。

4. 従来の技術との相違

本開発では、IP 電話などの音声通話に使用するための、リアルタイム性を重視したストリーミングメディアの署名方式を提案する。

ストリーミング転送においては、一般的な公開鍵署名では、データ全体を受信し終えるまで署名の確認が行えないという欠点が生じる。受信者はデータ全体のハッシュダイジェストを計算する必要があるため、途中まで受信したデータに対してはハッシュ計算が行えない。最も簡単な解決策は、データを分割して署名する方法であるが、データの分割数が少なければデータをバッファリングする時間が長くなるため遅延が大きくなり、データの分割数を増やせば署名の計算数が増加してしまうという問題が発生する。公開鍵署名の計算は非常に遅く、限られた演算性能の中では大量の計算を行うことは難しい。

関連研究としては、Rosario Gennaro、Pankaj Rohatgi らが提案したハッシュチェーン、Chung Kei Wong、Simon S. Lam らが考案したパケットグループによるストリーミング転送の認証方式などが挙げられる。これらはストリーミング転送における効率の良い署名方法の提案である。しかし、これらの手法は送受信時のバッファリングに時間が多く掛かってしまい、IP 電話のような遅延を極力少なくする必要がある用途には適さない。

そこで本開発では、ハッシュと公開鍵を組み合わせ、遅延時間を少なくすることに特化し

た音声ストリーム署名方式を提案し、IP 電話に実装した。

5. 期待される効果

本開発プロジェクトでは、IP 電話に使用することを想定し、送受信遅延を最小限に抑えることを重視しつつ、ストリーミングメディアの転送時に電子署名法で定められた強度をもつ公開鍵署名を効率よく施す手法を提案した。これにより、IP 電話を用いてお互いの会話内容を公開鍵による署名が施された信頼度で認証し合うことが可能となり、電話での商品注文などの利用に役立つと思われる。本提案の手法は、従来の電話音声の認証方法のように認証サーバを介した音声認証を行う必要がないため、維持コストを非常に安価に抑えることが可能である。このため、商用で大規模な電子商取引のみではなく、一般の利用者が安価な製品の購入に利用する用途にも使用でき、我が国の高度情報通信社会にふさわしい安全で便利な生活を提供する技術の一端を担えるのではないかと考えられる。

6. 普及の見通し

将来的に IP 電話が広く普及すれば、IP 電話を行う端末は低消費電力で演算性能の低いモバイル端末に波及することは明白であり、最終的には携帯電話自体が IP 電話の技術を取り入れたものになってゆくのではないかと想像される。

技術の進歩により通信速度が向上し、通信料金がさらに安価になったとしても、端末の小型化はさらに進み、無線通信が利用できる範囲もさらに拡張されてゆくため、通信品質の不安定による送受信遅延の揺らぎや端末の演算性能に関する問題は今後も残っていくと推測される。

本提案は、通信品質に応じて署名演算の負荷を変更することが可能であり、パケットロスに対する署名の耐性も有するため、これからのユビキタス社会における様々な状況に対応できる署名方式であると考えられる。

7. 開発者名

宇田 隆哉（東京工科大学 コンピュータサイエンス学部 uda@cs.teu.ac.jp）
高田 和泉（慶應義塾大学大学院 理工学研究科）