論文の内容の要旨

論文題目　　秘密鍵漏洩およびネットワーク変化に対応できる匿名通信路の研究

氏　名　　山中　　晋爾

本論文では，暗号用秘密鍵漏洩およびネットワーク変化に対応できる匿名通信路を提案する．匿名通信路とは，あるネットワークにおいて，ある参加者同士が互いに通信をおこなっている際に，通信をおこなっていない第三者からは誰と誰が通信をおこなっているかがわからない，というような仕組みをもつ通信路である．言い換えれば，通信データ(の内容)の秘匿のみならず，データの送信元と送信先の関連付けも取れなくする通信路である．

匿名通信路に関しては，D.Chaumによって1981年に提案されたUntraceable Electronic Mailに始まり，さまざまな構成方法が提案されてきた．Mix-net，Onion Routing，Crowdsなどの匿名通信路は定評のある方式である．しかしながら，これらの方式は，(1)ネットワーク構造の動的な変化に対応できない，(2)秘密鍵の漏洩に対して脆弱である，という問題を内包している．

そこで，本論文ではこの２つの問題を解決する新しい匿名通信路構成方法を提案する．すなわち，提案手法は次の２つの特徴を持つ．

a)　ネットワーク構造が動的に変化するようなネットワーク，例えば，peer-to-peer(P2P)環境やアドホック・ネットワークにおいて，匿名通信が利用しやすくなる．

b)　匿名通信路を構成するのに必要な公開鍵暗号系における，秘密鍵漏洩問題に対処する手法を備えている．

これまでの匿名通信路の研究では，ネットワーク上の各ルータは静的な状態にある(ネットワークの構造が変化しない)ことを前提にしていた．このため，既存の方式をP2P環境などで利用すると，プロトコルの途中でネットワークの接続・構成が突然変更された場合に大きな問題が生じた．例えば，匿名通信路の形成に失敗するだけではなく，通信路の形成に失敗したという事実をメッセージ送信者に伝えることも困難になる場合もあった．

Mix-netは，メッセージの送信経路が完全に固定されており，そもそも構成要素であるノード(Mixサーバ)が一つでもオフラインになると，匿名通信機能が利用できない．また，Crowdsは，その性質上，経路上のノード(Crowdsメンバ)に送信先が知られてしまうという欠点がある．オニオン・ルーティングは，Mix-netよりはノード(オニオン・ルータ)の選択において柔軟性があり，送信先も隠蔽されているのでCrowdsよりは匿名性が高い．

そこで，提案手法は，オニオン・ルーティングに用いられた多重暗号化の概念を利用した新しい匿名通信路方式を考案した．具体的には，これまでのオニオン・ルーティング手法で仮定していた，ステイトフル(パケットなどの情報をある程度記憶すること)なノードを用いる代わりに，オニオン・データパケット自身に対して予備

の経路情報(バックトラック・オニオン)を付加した．この結果，ネットワークの構造(トポロジ)が動的に変化する場合においても，付加した情報を利用することによりそれに対応できるようになった．すなわち，切断された経路や，オフラインになったノードを回避することが可能になり，その結果送信先にメッセージを送ることに成功する可能性を増大することができた．さらに，匿名性をより強固なものとするために，どのようなパケット構造が適切であるかも検討し，具体的な方策を提示した．

秘密鍵漏洩問題とは，公開鍵暗号系における秘密鍵(これには，署名用秘密鍵と暗号文復号用秘密鍵が存在するが，本論文では後者の復号用秘密鍵を指す)が第三者に漏洩してしまう問題である．秘密鍵が漏洩してしまうと，その鍵の正当な所有者ではない者が，暗号文を復号できてしまうことになり，暗号の持つ秘匿性が完全に失われてしまう．証明書失効リスト(CRL)を利用するにしても，公開鍵-秘密鍵のペアを再生成する必要があり，またそれをメッセージの送信者に告知する労力も馬鹿にならない．

この問題に対抗するために，秘密鍵の管理に工夫をする方式が提案されている．例えば，Threshold Encryption，Forward Secrue Encryption，Key-Insulated Encryption，そしてIntrusion-Resilient Public-key Encryptionといった方式があげられる．この中でも，Key-insulated encryption(KIE)方式は，方式実現のための仮定が比較的小さい反面，秘密鍵漏洩に対してそれなりの耐性がある．しかしながら，KIE方式はマスター秘密鍵と呼ばれる”親”秘密鍵を安全な場所に保存しておく必要があり，同方式においては安全性を仮定した秘密鍵保存デバイスの存在を前提条件としている．

本論文では，秘密鍵漏洩問題に対処する手法として，パーソナル・エントロピーを利用して秘密鍵の更新を行う手法を提案した．KIEに即して述べるならば，パーソナル・エントロピーを用いてマスター秘密鍵を作成する方式を考案した．ここで述べるパーソナル・エントロピーとは，個人的な特徴を基にした秘密情報の総称である．具体的には，バイオメトリクス情報およびグラフィカルパスワードを利用して，個人の秘密鍵を作成する方法を提案した．

この方式では，従来の秘密鍵更新方式において必要とされていた，安全性を仮定した秘密鍵保存デバイスが不要となった．すなわち，方式を安全に保つための仮定のひとつを取り除くことに成功した．さらに，正当なユーザ(本人)以外にバイオメトリクス鍵を生成することは困難であるため，秘密鍵を更新するタイミングにおけるなりすまし攻撃も難しい．そして，バイオメトリクス情報(鍵)は，特定のデバイス内に保存しない仕組みにするため，これが漏洩することは考えなくて良い．また，提案した秘密鍵生成手法は，同じニーズがある他のアプリケーションにも応用が可能な，適用範囲の広い手法といえる．