論文の要旨

題目：「動的環境における双方向性匿名通信路の構築とその応用に関する研究」

氏名：　田村　仁

本学位論文では，動的環境における双方向性匿名通信路の実現に不可欠な要素技術を暗号基盤，通信路及びアプリケーションの各層から提案し構築する．動的環境とは，エンティティ同士の信頼度や，ネットワークの中では特に近年普及しつつある無線系ネットワーク等，変化に富む環境を指す．また双方向性匿名通信路とは匿名性を保ったまま双方向のデータ送受信を行える通信路のことである．

まず，暗号基盤に関しては公開鍵暗号基盤（Public Key Infrastructure 以下，PKI）を前提とした．ここでいうPKIとは認証局や公開鍵証明書等から成り立ついわゆる”狭義のPKI”のことではなく，各エンティティが鍵ペア（公開鍵及び秘密鍵）を有する事のみを前提とする”広義のPKI”のことである(当然，広義のPKIは狭義のPKIを含む）．人々が電子決済やネットバンキングなどでPKIを安心して使用できるためには技術的基盤や法律的基盤の他，信頼的基盤が不可欠である．つまり，PKIにおける暗号化による秘匿性や署名による否認／改ざん防止等の技術的保証あるいは電子署名法等による法律的保証も，フィッシング詐欺等が示すようにそもそも鍵の使用者が正規の所有者でなければこれらも全く意味をなさない．狭義のPKIにおいてはこの信頼的部分もできる限り技術あるいは法律でカバーすべく，信頼ある第三者としての認証局を設け，そこからトップダウン式に認証を行い，各エンティティは認証局から発行された公開鍵証明書（X.509)を保有することで，利用者がその都度検証する仕組みを設けている．しかしながら近年数多くの認証局が設置されている中では，そうしたトップの認証局を信頼できるかどうか等信頼に関わる問題は避けられず，また，こうしたトップダウンの仕組みをその場的なグループにまでその都度導入するには各エンティティ等にかかる負担があまりに大きいといえる．そこで，PGP(Pretty Good Privacy)などに代表されるような，エンティティ同士がフラットに認証しあいながらその信頼の輪(Web of Trust）を活用する方式が導入された．こうした中でターゲットのエンティティの信頼度を定量化する研究をトラストメトリックスと呼ぶ．PGPを始めとする信頼度推測型トラストメトリックスでは，信頼度を開示しない変わりにユーザが推測して全て割り当てなくてはいけない等，定量化過程の問題があり，一方，研究の主流である信頼度参照型のトラストメトリックスではお互いの信頼度を全て開示しなくてはいけないプライバシの問題があった．こうした諸々の問題点を本論文第2章で指摘し，我々は新たに，秘密計算とコミットメントを組み合わせることで，定量化に必要な信頼度の計算を互いに信頼度を隠したまま行い，更にあらかじめコミットしておいた情報を参照することにより計算結果を検算できる，コミットメント参照型トラストメトリックスの概念を提案し，更に実際に信頼度参照型BBK手法からコミットメント参照型BBK手法への適用例を示す．

また，通信路構築には，通常データの可用性は大前提となるが，匿名通信路を動的な環境において可用性を高めるにあたって，通常の通信路との難しさの決定的な違いは，特に返信の際，送信元すら送信先をわからないままの動的な対応が求められる点にある．こうした変化には，従来静的ネットワークを前提として提案されてきたような，送信時に経路上の中継ノードに前後の隣接ノードを記憶させる方式では到底対応ができない．そこで我々は本論文第３章において，これまでの多重暗号化による隣接ノード記憶の手法ではなく，ノードごとのルーティングテーブルを各々の公開鍵で単暗号化することで，匿名性を保ったまま可用性を高められることを示し，従来手法との比較による検証を行う．

更に双方向性匿名通信路で動く応用アプリケーションとして，匿名カウンセリングや社内告発システム等の他，プライベート情報検索等の二者間暗号プロトコルが挙げられる．プライベート情報検索とは情報を漏洩することなくユーザが選択したデータを検索することができる暗号プロトコルであり，例えば特許の先願調査等の用途が挙げられる．このプロトコルを双方向性匿名通信路と組み合わせることにより「誰が」「何を」検索したのかの双方を秘匿する，一層匿名性の高いインフラを実現できる．しかしながら一般に，動的ネットワークにおいては個々のノードの計算能力や通信能力は低く，更に返信までのタイムラグが大きいほど可用性は低下するので，こうしたプロトコルにおけるラウンド数（つまりデータ往復の回数）や通信コスト及び計算コストの削減は急務である．我々は1データベース1ラウンドモデルにおいて初めての通信コストが$\log^2$オーダーであったLFCPIR手法を改良し，通信コスト$\log$オーダーの新たな手法を第４章で提案する．

これら階層別の課題に取り組み，またそれらを解決する手法を各章で提案する．これにより，ユビキタスという超動的なネットワーク環境の到来に向け極めて運用性の高いプライバシ保護インフラを示すことができた．

本学位論文が各提案方式としての意義だけでなく，プライバシ保護技術が実際に盛んに使われる社会における運用基盤の研究としての意義を持っていくことを期待する．