審 査 の 結 果 の 要 旨

氏　名　　田 村　仁

本論文は、「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」と題し、プライバシー意識の高い社会において不可欠なプライバシー保護技術、とくに近年普及しつつある動的環境においても実現可能な双方向性匿名通信路について、暗号基盤、通信路及びアプリケーションの各層から要素技術を提案して具体的な構築方法を提示している。ここで動的環境とは、遠隔エンティティ同士の信頼度や無線系ネットワーク等、変化に富む環境を指し、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が可能な通信路のことを指している。論文の構成は「序論」を含め５章からなる。

第１章は「序論」で、本研究の背景を明らかにした上で、本研究の前提となっている公開鍵暗号基盤（PKI）を含めた関連技術や運用方式を述べ、更に第２章で扱うトラストメトリックス（信頼度の定量化尺度）の定義やPKIにおけるその重要な役割について記述している。

第２章は「コミットメント参照型トラストメトリックス」と題し、これまでのトラストメトリックスの既存方式が、PGPをはじめとする信頼度推測型トラストメトリックス、もしくは、BBKをはじめとする信頼度参照型トラストメトリックスのどちらかであり、信頼度推測型トラストメトリックスではユーザが全ノードの信頼度を推測することによる精度の問題があり、信頼度参照型トラストメトリックスでは他のユーザの信頼度を参照することで精度の面はカバーされているものの、信頼度を他に開示しなくてはいけないプライバシーの問題があることを指摘した上で、これらのトレードオフを解決するコミットメント参照型トラストメトリックスという新しい概念を提案している。コミットメント参照型トラストメトリックスとは、秘密計算とコミットメントを組み合わせることにより、定量化に必要な信頼度の計算は互いに信頼度を隠したまま行い、必要に応じて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の検算を行うという着想に基づいた手法である。更に本章では、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手法への変換適用例が示され、その有効性が評価されている。

第３章は「動的環境に適した双方向性匿名通信路の構築」と題し、これまで困難であった、動的環境において匿名性も可用性も保ったまま送受信が可能な匿名通信路の構築手法について述べている。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、送信元にすら送信先を秘匿したままの動的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「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」では到底対応できなかった。しかし本章では、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が示され、更に従来手法との比較による評価がおこなわれている。その結果、

現実的な攻撃者の能力の範囲において、匿名性を損なうことなく可用性を著しく高めることに成功したことが示されている。

第４章は「高効率・プライベート情報検索スキーム」と題し、前章までで述べた双方向性匿名通信路上で動くアプリケーションの効率化手法について述べられている。双方向性の匿名通信路を構築したことで二者間暗号プロトコルとの組み合わせが可能となり、多様な応用へ道が開ける。中でも、プライベート情報検索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、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、極めて匿名性の高いインフラを実現可能である。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が低下することは明白であり、効率化が研究開発の主たる課題となっていた。具体的には、1データベース1ラウンドモデルを初めて実現し従来最良の手法であったLFCPIR手法ですら、通信コストは対数の二乗オーダーであった。こうした背景から、本章では、プロトコルにおけるラウンド数や通信コスト及び計算コストの削減をおこない、LFCPIR手法と同じく1データベース1ラウンドモデルのもとで、通信コストが対数オーダーという世界トップ性能のプライベート情報検索スキームを提案している。

最後に第５章は、「結論」で、本研究の総括を行い、併せて将来展望について述べている。

以上これを要するに、本論文は、今後ますます重要性を増していくであろう動的環境に適した、匿名性、可用性及び効率性の高いプライバシー保護基盤技術の構築手法とその応用について有意義な提案を行いそれらの評価を示したものであり、電子情報学、特に情報セキュリティ工学上貢献するところが少なくない。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。