審査の結果の要旨

論文提出者氏名　　山中　晋爾

本論文は「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」と題し，ヒューマンクリプトを構成する２つの基盤技術に関して提案を行ったものである. ヒューマンクリプトでは, 人に安全と同時に安心を与えることが重要とされる. 安心を与えるための基本的な要素技術として, プライバシーを守るための匿名通信技術, バイオメトリクスを利用した暗号化技術が挙げられる. 本論文では, これら二つの技術を実際に用いる場合に生じる重要な問題を指摘し, その解決策を提案している．すなわち，匿名通信技術に関しては，①ネットワーク構造の変化に適応可能な匿名通信路の構成, バイオメトリクスに基づく暗号化技術に関しては, ②バイオメトリクスを利用した暗号文復号用秘密鍵の漏洩対策，をそれぞれ示している．本論文は「序論」を含め７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, 研究の動機と目的について言及し, 研究の位置付けについて整理している.

第２章は「現代暗号技術」と題し，以下で用いる暗号技術の基礎的な方式を紹介している. すなわち，共通鍵暗号，公開鍵暗号，電子署名方式について例示して説明している.

第３章は「匿名通信技術」と題し，ネットワーク上でメッセージの送信者や受信者の匿名性を維持するために近年提案された匿名通信方式を紹介している. 匿名通信方式は, 送信者からのメッセージを受信者に送信する際に, 複数の中継ノードを経由させることで, 送信者と受信者のつながりを絶つ（すなわち匿名性を維持する）ことができる．本章では特にミックスネット，オニオン・ルーティング，クラウズ方式についてその詳細を示し，同時にネットワーク構造の変化に対する適応能力の不備を指摘している.

第４章は「通信路変化耐性・匿名通信路の構成方法」と題し，オニオン・ルーティング方式をベースとした提案方式の詳細を示している. 既存方式では１つの経路情報のみをメッセージに添付する手法が一般的であったが, 提案方式では, メッセージが複数の経路情報を保持する仕組みとなっている．この結果，提案方式は，ネットワーク構造が変化した場合にデータの転送が失敗する確率が，既存方式と比較して減少する．また，匿名性・メッセージ量・通信回数といった要素について，既存方式との比較を行っている.

第５章は「秘密鍵漏洩対策技術」と題し，既存の公開鍵暗号方式における秘密鍵漏洩に耐性を持つ方式を紹介している．特に，threshold encryption 方式や，forward secure encryption 方式, key-insulated encryption 方式, そして intrusion-resilient encryption 方式について概説し, 各方式の利点と欠点を提示している.

第６章は「バイオメトリクス秘密鍵更新方式」と題し，ユーザのバイオメトリクス情報を用いて秘密鍵を更新するという秘密鍵漏洩に対処し得る方式を提案している. 秘密鍵更新方式の一つである key-insulated encryption 方式は，IC カードのような携帯型デバイスに記憶したマスター鍵を利用して秘密鍵を定期的に更新することにより, 秘密鍵が漏洩した場合にその影響の範囲をある期間に限定する方式である．しかし，key-insulated encryption 方式はその安全性がマスター鍵の安全性に依存しており，IC カードの盗難やそれにともなう成りすまし問題には対処で

きない．本章では，IC カードを利用する代わりに，バイオメトリクスを利用する秘密鍵更新方式を提案している．バイオメトリクスはユーザ個人に起因する情報であるため，本人以外に秘密鍵の更新を行うことが難しく，成りすましも防止しやすい．ここでは，提案方式の具体的なモデルおよび実装例を示した上で，実証実験の結果を示している．

最後に第７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，ヒューマンクリプトを構成する基盤技術としての匿名通信技術およびバイオメトリクスを利用した暗号化技術を実際に用いる場合に生じるネットワーク構造変化や秘密鍵漏洩問題に対する解決策を明示したものであり，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．