論 文 内 容 の 要 旨

博士論文題目

電子透かしと暗号技術を用いたネットワークサービス構成法に関する研究

氏　名　北川　隆

コンピュータネットワークの普及により、多様なサービスがネットワーク上で提供されるようになっている。この際、ネットワーク上を流通するコンテンツの著作権情報や利用者のプライバシ保護が大きな問題となる。そこで、不正者による盗聴・改ざん・なりすましなどが行われた場合でも、利用者のプライバシが保護され、システムが正しく動作するように、暗号技術やネットワーク技術を用いてサービスを設計する必要がある。

本論文では、安全なネットワークサービス実現のために必要となる技術について考察されている。第2章では、電子透かしに関する研究について述べられている。はじめに、コンピュータソフトウェアに対する電子透かし法について、透かしの安全性が形式的に定義され、その安全性を満たす電子透かしの構成法が提案されている。次に、電子透かし用の結託耐性符号化法（結託に耐性をもつ符号でユーザ ID を符号化してメディアに埋め込む方法）について議論されている。本論文ではこれまで性能がよいと考えられていた結託耐性符号に対し新しい結託攻撃が示されている。さらに、そのような攻撃に対しても安全な符号が提案され、その符号の安全性が計算機シミュレーションにより示されている。第3章では、ソフトウェアの回数券型課金法が提案されている。ソフトウェアを利用した分だけ代金を支払う方式が実現できれば、ユーザの負担が減り、ソフトウェアを利用しやすくなる。提案方式では、ソフトウェアの難読化技術と電子署名法を組み合わせることで回数券型課金方式を実現している。第4章では、匿名アンケートプロトコルが提案されている。近年、多くの大学で学生による講義評価が行われている。講義評価アンケートを電子化することで、集計の手間の削減が期待できるが、安易な匿名アンケートシステムを利用すると、その匿名性によりアンケートの回答率が減少する。本論文ではこの問題を解決するために、匿名かつ未回答者の特定が可能なアンケートプロトコルが提案されている。さらに、提案プロトコルを実装することにより行われた実証実験により、回答率が大幅に上昇することが示されている。

氏 名	北川 隆

（論文審査結果の要旨）

計算機ネットワーク上で多くのサービスが提供される今日、サーバ（サービス提供者）、ユーザ双方の観点から、計算機システムの安全性、配信コンテンツの著作権保護、ユーザのプライバシー保護を実現するための基盤技術の確立が急務となっている。本論文は以上の問題意識のもと、安全なネットワークサービスを実現するための要素技術である電子透かしに関する研究成果、ならびに、具体的なサービス実現法に関する研究成果をまとめたものである。本論文の主な結果は以下の通りである。

1. 要素技術としての電子透かし法に関する研究：電子透かしとは、コンテンツの不正コピーを抑止することを目的とし、コンテンツ中に正規ユーザを特定できる情報を埋込む技術である。本研究では電子透かしに関する以下の成果がまとめられている。
(1) プログラムに対する電子透かし法：画像や音声データは冗長度が高いため、電子透かしを埋込むことは比較的容易である。これに対し、プログラムは冗長度が低く、その内容の一貫性や完全性が強く要求される。本論文では、プログラムに対する電子透かし法の満たすべき条件について考察し、改変不可能性、消去不可能性、偽造不可能性という3条件として定式化している。さらに、これらの条件を満たす具体的な透かし法が提案されている。
(2) 結託攻撃耐性をもつ電子透かし用符号：複数のユーザが結託して電子透かしを比較することにより、透かし情報の改竄が可能な場合がある。このような結託攻撃に耐性をもつ符号として、c-secure CRT 符号が知られている。本論文ではまず、c-secure CRT 符号において、結託したユーザを特定するためのトレースアルゴリズムを悪用した新しい攻撃法が示されている。この攻撃法がなぜ効果的であるかの考察を通し、randomized c-secure CRT 符号と呼ばれる新しい符号化法が提案されている。計算機シミュレーションにより、提案符号化法が従来の c-secure CRT 符号と比較して高い安全性をもつことが実証されている。

2. 具体的なサービス実現法に関する研究：暗号、難読化、ディジタル署名等の要素技術を利用した二つのネットワークサービス構築法がまとめられている。
(1) ソフトウェアに対する回数券型ライセンス方式：有料ソフトウェアには、買取り方式とペイパーユース (PPU) 方式がある。高価で使用頻度が少ないソフトウェアの場合、ユーザにとって PPU 方式が望ましい。本論文では、回数券型 PPU 方式を想定し、特殊なデバイスやサーバとの常時接続を必要としない新しいソフトウェアライセンス方式を提案している。ユーザの不正を防止するため、暗号化と難読化を効果的に利用することにより、ユーザの利便性を損ねず、サーバにとっても安全なサービス提供を可能としている。
(2) 回答証明が可能な匿名アンケートプロトコルとその実現：本論文では、要素技術として、暗号化、一方向性関数とディジタル署名（特にブラインド署名）を利用することにより、回答証明が可能な匿名アンケートプロトコルが提案されている。さらに、本プロトコルの応用例として、本学情報科学研究科において、学生による授業評価アンケート集計システムを実現している。約半年間本システムを集計に用いたところ、単純なアンケート収集方式と比較して回答率が大きく向上し、本方式の有効性が実証された。

本論文で提案する手法と得られた結果は、ネットワークサービスにおける情報セキュリティに関する重要な知見を与えており、その発展に寄与するところが大きい。従って、博士 (工学) の学位論文として価値あるものと認める。