論文内容の要旨

論文題目

A Study on Secure Contents Distribution Systems with Advanced Functions to Enrich User Convenience

ユーザの利便性を考慮した効率的でセキュアなコンテンツ配信システムに関する研究

氏名　小川　一人

我々は，コンテンツ配信システムの研究を行い，システムの安全性を保持しつつ，ユーザやコンテンツプロバイダの利便性を増加させるコンテンツ配信システムを開発した．さらに，システムに必要となる効率的な暗号方式を開発したので報告する．ユーザの利便性を高める研究では，３つの機能を有するシステムを提案する．さらに，コンテンツプロバイダの利便性を高める研究では１つの機能を提案する．さらに，コンテンツ配信システムの効率化のための要素技術の研究として，効率的な暗号方式を提案する．

一つ目の項目としては，不正利用者追跡方式(Traitor Tracing)と呼ばれる暗号方式に焦点をあてて研究を行った．不正利用者追跡方式は，重要な暗号方式の一つであり，コンテンツ配信のようなアプリケーションにおいては，コンテンツの著作権を保護するための有効な技術である．特に，通信のインフラやデジタル記録媒体などが進歩し，“海賊版”コンテンツの作成・流通が容易となった今日では必要不可欠な技術となっている．不正利用者追跡方式は，不正利用者による海賊版デコーダの作成を抑止する効果がある．

また，ユーザからは，家の外でも家庭内と同じサービスを享受したいという要望がある．このサービスを実現するには，コンテンツプロバイダがユーザにコンテンツを復号するための鍵（復号鍵）を持ち歩くことを許可しなければならない．反面，このようなシステムでは鍵が漏洩してしまう可能性が生じ，結果として，正規に登録されていないユーザがコンテンツを自由に使用することが可能となり，究極的には海賊版の受信機を作成する可能性が生じる．従って，著作権を所有する放送局などにとっては，受け入れがたいものとなる．そこで我々は，意図的に海賊版受信機を作成するユーザを特定でき，不注意に秘密鍵を使用したた

めに漏洩した場合には，その被害を最小限に食い止めることができる手法を構築することを目的として研究を行った．その結果，適応的な鍵漏洩攻撃に耐性を有する効率的な不正利用者追跡方式(TTaKE）を構築した．この手法は，鍵漏洩耐性を有する公開鍵暗号方式と不正利用者追跡暗号方式の両方の特性を併せ持った暗号方式である．この手法を用いることで，ユーザは秘密鍵を持ち歩き，家庭外でもサービスを享受でき，かつ，意図的に秘密鍵を漏洩させる悪意のある正規ユーザを特定するこができ，ユーザとプロバイダの両方の要求にあったシステムを構築することができる．

二つ目の項目として、ネットワークを経由したコンテンツ配信サービスに焦点をあて研究を行った．第一項目として紹介した不正利用者追跡方式は放送波を利用したサービスに適した方式であり，ネットワークを経由したコンテンツ配信サービスには不十分なところがある．そこで我々は，ネットワークを通じて世界中どこにおいてもサービスを享受でき，しかもセキュアなシステムの構築を目指して研究を行った．この研究では，初めに鍵漏洩に耐性を有するグループ署名方式を構築した．この構築ではTTaKEを基盤技術として使用したため，TTaKEの特性を継承しており，鍵漏洩攻撃に耐性を有し，署名鍵を持ち歩くことが可能となる．そして，ユーザがサービスを家庭外で享受する場合は，ネットワークを通じてリクエストをコンテンツプロバイダに送信するが，その際に，この署名鍵を用いてグループ署名を生成する．グループ署名の利用により，サービスの匿名利用が可能となり，しかも，トークンの利用によりサービス利用回数を制限でき，結果として，ユーザにもプロバイダにも利点があるシステムを構築することができた．

第三の項目として，有料放送の匿名化に焦点をあて研究を行った．現在，ユーザが有料放送を視聴する場合，放送事業者と契約を結ばなければならない．すなわち，ユーザが視聴するコンテンツが放送事業者に知らされており，ユーザのプライバシー保護の観点からは，完全なシステムではない．そこで，匿名で有料放送を視聴でき，しかも，コンテンツプロバイダには正規の収入が分配されるシステムを構築することを目的として研究を行った．我々が考案したシステムでは，準同形暗号にマスク機能を付加した暗号方式を使用する．この暗号方式は，準同形暗号化されたデータに乱数でマスクをかけた方式だが，準同形暗号の特性を妨害しない形態でマスクをかける方式になっている．この暗号の準同形性により，プロバイダ間での正当な収入分配が可能となる．さらに，マスク機能により不正を行う構成員を特定，もしくは，不正なプロセスを検知することができる．これらの機能の結果，有料放送を匿名で視聴でき，しかも，放送事業者に正規の収入分配が可能なシステムを構築できた．

4つ目の項目として，コンテンツプロバイダの利便性を高めるために研究を行った．現存するほとんどのコンテンツ配信サービスでは，コンテンツはサービスプロバイダに一旦集められる．そして，サービスプロバイダはコンテンツを暗号化し，復号鍵をユーザに分配する．このシステムでは，コンテンツプロバイダの数が増加するに従い，サービスプロバイダの負荷が大きくなる．そして，さらなるコンテンツプロバイダが同じサービスプロバイダを利用できない状況が起こりえる．多くのPCユーザが誰でもコンテンツプロバイダになりえる今日

では，このような状況は好ましくない．そこで我々は，コンテンツプロバイダの利便性を良くすることを目的として研究を行った．すなわち，サービスプロバイダの重い負荷を複数の組織で独立に行うことができるDRM方式を考案した．より詳しく述べると，“分割暗号方式(SENC)”を開発し，SENCを用いたコンテンツ配信方式を開発した．分割暗号方式では，暗号鍵と復号鍵を独立に管理できる．従って，この方式を用いたシステムでは，コンテンツを暗号化するコンテンツサーバと復号鍵を生成・発行するライセンスサーバの独立運用が可能となる．さらに，ID-Based暗号方式(IBE)と分割暗号方式が同じセキュリティ要素技術であることを証明し，現実に開発されたID-Based暗号方式を用いてSENCが構成できることを示した．ここで用いられたID-Based暗号方式はランダムオラクルモデルの上で安全な方式であるため，そのID-Based暗号方式を用いて作られたSENCもランダムオラクルモデル上での安全な方式となる．そこで我々は，より実用的な方式を求めて，スタンダードモデルでの安全性を有する別のSENCを構成した．これらの機能により，サービスプロバイダの重い負荷を分散できるコンテンツ配信システムを構築することができた．

最後に，セキュリティシステムの効率化に目を向けた研究を行った．先にも述べたが，不正利用者追跡方式は，悪意のある正規ユーザによる海賊版デコーダの作成を抑止する有効な手段であり，多くの方式が提案されてきた．その中で，総ユーザ数をN人，ｋ人の結託攻撃に耐性を有する(k,N)-不正利用者追跡方式に焦点をあてて効率化を目指した．今日まで，適応的な鍵漏洩攻撃と線形攻撃の両方に対し耐性を持ち，多項式を用いてユーザの秘密鍵と対応する公開鍵を生成するタイプの(k,N)-不正利用者追跡方式を構成するには，次数が2k-1次の多項式が2つ必要であると信じられてきた．すなわち，|q|をセキュリティパラメータとした際，約4k|q|ビットの秘密情報を鍵管理センタに所持する必要があった．しかし，我々はｋ次の多項式が2つあれば同じ安全性を有する(k,N)-不正利用者追跡方式を構成できることを示した．すなわち，鍵管理センタが所持する秘密情報のサイズは先ほどの半分である約2k|q|ビットに削減でき，この不正利用者追跡方式を利用することでシステムの効率化が可能であることを示した．