IPSJ Best Paper Award

匿名ユーザを失効させる別発想からのアプローチ

米沢祥子　NEC 共通基盤ソフトウェア研究所
佐古和恵　NEC 共通基盤ソフトウェア研究所

〔受賞論文〕
・ OMSP レスポンダ：グループ署名における失効メンバ確認モデル
・ 米沢祥子，佐古和恵（NEC インターネットシステム研究所）
・ 情報処理学会論文誌，Vol.47, No.3, pp.932-944 (2006)

このたび，表記の論文において本会論文賞をいただくことになり，大変光栄に思っております．

我々の研究グループではここ数年来，グループ署名と呼ばれる暗号技術の研究を続けています．グループ署名技術はセキュリティとプライバシを両立できる革新的な技術であり，個人情報保護が不可欠となる社会の中で重要な役割を果たすものと期待されています．

グループ署名はたとえばこのように利用されます．A 大学の学生は B 書店で割引サービスを受けることができます．A 大学の学生であることを示すためには A 大学の学生証を書店に見せればよいのですが，そうすると B 書店の店員さんに氏名や学籍番号などの個人情報が知られてしまいます．グループ署名を利用すると，「A 大学の学生」であることは確認できるが，A 大学の誰であるか店員さんには分からないディジタル署名を作成することができます．ただし，トラブルが起こったときのために，大学の学生課では署名した学生を特定できるようになっています．つまり，グループ署名ではユーザのプライバシを守りつつユーザの権限を確認することができ，同時に匿名性の悪用に対するセキュリティも担保できるのです．

このような利用シーンを考えるときに重要なのは，A 大学を卒業・退学した学生が引き続き割引サービスを利用できないようにすることです．これをグループ署名技術では「メンバの失効」と呼びます．グループ署名におけるメンバの失効は学術的にも難しい問題でした．たとえば，通常のディジタル署名で用いられる証明書失効リスト（CRL: Certificate Revocation List）では，失効したユーザに対応する公開鍵証明書を CRL として公開することにより，検証者はユーザの公開鍵が失効されているかどうかを確認することができます．しかしグループ署名では，ユーザ個人の秘密鍵はそれぞれ異なるものの，公開鍵はグループで共通です．そのため，グループ署名では CRL をそのまま適用することができません．グループ署名の安全性を満たしながら CRL のような方法で失効機能を実現する研究も発表されていますが，アルゴリズムが複雑になったり，鍵更新が必要になったりします．

そこで我々は，メンバ失効に対して別方向からのアプローチを試みました．それは，ディジタル署名の失効確認に利用されている OCSP（Online Certificate Status Protocol）レスポンダの発想をグループ署名に応用することです．本論文では，グループ署名システムにオンラインサーバ OMSP レスポンダを導入した「OMSP レスポンダモデル」を提案しました．OMSP とは Online Membership Status Protocol の略で，OMSP レスポンダはオンラインでグループのメンバ状態を検証者に応答する信頼機関です．このモデルにより，失効機能を持たないグループ署名方式にも簡単に失効機能を追加できることを示しました．

暗号プロトコルを考えるときは，そのプロトコルが満たす安全性を定義し証明する必要があります．OMSP レスポンダを導入したグループ署名方式では，攻撃者が OMSP レスポンダを自由に利用できるため，攻撃者はグループメンバの状態（有効／失効）に関する情報を得ることができます．そのため，このような攻撃モデルにおけるグループ署名方式の安全性を見直す必要がありました．そのため本論文では，OMSP レスポンダを用いたグループ署名方式が満たす安全性を改めて定義し，提案方式がその安全性を満たすことを示しました．

最後に，本論文に関して貴重なコメントをくださった査読者の皆様をはじめ，本研究を進めるにあたり数々の有益な議論をしてくださった関係各位に心より感謝いたします．

（平成 19 年 5 月 25 日受付）

米沢　祥子（正会員）　s-yonezawa@da.jp.nec.com
平成 15 年東京大学大学院情報理工学系研究科電子情報学専攻修士課程修了．同年日本電気（株）入社．現在，同社共通基盤ソフトウェア研究所にて，グループ署名技術の研究開発に従事．

佐古　和恵（正会員）　k-sako@ab.jp.nec.com
日本電気（株）入社後，電子投票・電子入札・電子抽選など暗号プロトコルの研究に従事．現在，同社共通基盤ソフトウェア研究所主席研究員．博士（工学）．電子情報通信学会，IACR 各会員．