恩を忘れない

金沢 史明　特許庁

〔受賞論文〕
・送信者に認証機能を付加したブロードキャスト暗号とその応用
・金沢史明，岡本健（筑波大学大学院システム情報工学研究科），猪俣敦夫（（独）科学技術振興機構），岡本栄司（筑波大学大学院システム情報工学研究科）
・情報処理学会論文誌，Vol.47, No.11, pp.2992-3004 (2006)

このたび，論文賞という名誉ある賞を頂戴した．当然のことながら，受賞の通知を受けるまで，論文賞のことは頭になかった．それだけに嬉しさは大きかった．特に，他の共著者との共同受賞である点が嬉しい．昨年受賞した山下記念研究賞では，受賞対象が口頭発表者のみであったため，嬉しさの中に後ろめたい気持ちもあった．今回の論文賞では，受賞対象が共著者全員であり，気兼ねなく喜びを分かち合うことができた．

受賞論文の概要

ブロードキャスト暗号とは，多数のユーザが存在する中で，送信者が選択したユーザのみに対し，ブロードキャストチャネルを通して安全かつ効率的にデータを配布する技術であり，有料放送などの著作物の配信に有効である．受賞論文では，送信者が自身の秘密鍵を用いて暗号文を生成することにより，受信者が送信者の本人認証とメッセージ認証を行うことができる方式を提案した．さらに，提案方式を応用し，1-out-of-n 署名と検証者指定署名の特徴を併せた電子署名方式を構築した．両方式は，いずれも暗号文や署名のサイズがユーザの数に依存せず固定長となり，チャネルの帯域が制限された環境に適している．

受賞に至るまで

ブロードキャスト暗号という研究テーマは，修士時代の恩師，宮地充子 JAIST 助教授（現・教授）からの紹介によるものである．その後，博士後期課程進学と同時に，筑波大の岡本栄司教授の研究室へ移った．研究テーマを変更しようかと悩んでいた矢先，受賞論文の主引用文献となる Boneh らの論文“Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys”に出会った．この論文は，国際暗号学会（IACR）の電子テクニカルレポート集（暗号技術の研究者の間では，単に e-print と呼ばれている）に掲載されたばかりの論文で，暗号文サイズと秘密鍵サイズを固定長に抑えたという点で画期的な論文だった．今振り返れば，この論文と早めに出会っていたことが，受賞に至った最大の鍵だったのかもしれない．その後，この提案方式の構造を分析し，岡本健講師（現・筑波技術大准教授）と猪俣敦夫 JST 研究員（現・NAIST 特任准教授）との議論を重ねた．その結果，Boneh らの方式の特長を活かしたまま，送信者認証機能を付加することに成功した．さらに，岡本講師独自の研究と絡ませ，電子署名方式も構築した．これらの方式を論文にまとめ，2005 年コンピュータセキュリティシンポジウム（CSS2005）にて発表した．この発表内容は，情報処理学会論文誌へ推薦されることとなり，さらに山下記念研究賞を与えられるものとなった．そして，論文誌に掲載されたその推薦論文が今回の受賞論文となった．この過程の要所で，先輩学生であった左瑞麟氏（現・国立政治大学（台湾）助理教授），情報セキュリティ大学院大の土井洋教授と大川直人氏より，安全性に対する大変有意義なご指摘とご提案を頂戴している．以上の方々を含め，お世話になった方々に深く感謝申し上げたい．

今後へ向けて

博士後期課程において，研究に対するモチベーションを保つことは，非常に難しいことであった．研究能力に限界を感じ，後期課程進学を選択した自分を責め続けていた．就職の道を選んでおけば良かったと何度後悔したか分からない．睡眠時間を削って研究を進めていると，次第に考え方がおかしくなり，自暴自棄になったこともあった．自分の提案した暗号方式が破られたときは，特に辛かった．「能力の限界は自分が勝手に設定したものだ」といわれることがある．自分が感じた限界もその一種だったかもしれないが，周囲の方々は常に自分を支えてくださった．その方々の恩を忘れず，今後も産業の発達に寄与していきたい．

（平成 20 年 4 月 30 日受付）

金沢　史明（正会員）　kfumiaki@ieee.org
2003 年東京理科大学理学部応用数学科卒業．2005 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．2008 年筑波大学大学院システム情報工学研究科博士後期課程修了．博士（工学）．同年特許庁入庁．