会議レポート

CoSyProofs 2009 参加報告

2009 年 4 月 6 日から 9 日にかけて，暗号の計算論的・記号的安全性証明に関するスプリングスクール＆ワークショップ（Spring School and Workshop on Computational and Symbolic Proofs of Security, CoSyProofs 2009）に参加した．本会議は，NTT コミュニケーション科学基礎研究所と産総研情報セキュリティ研究センターの主催で，今回がはじめての開催である．会場は静岡県の熱川ハイツ，眼前に相模湾，遠くに伊豆七島をのぞむ風光明媚なロケーションであった．

会議の参加者は約 60 名で，その半数ほどが海外からの参加だった．講演数は 24 件，そのうちの半分が招待講演，のこりが一般講演で，この分野の基礎的な知識から最新動向までをいっきに俯瞰できる構成となっていた．

会議の内容は，もちろん暗号の計算論的・記号的安全性証明に関するものである．セキュリティプロトコルの記号的（あるいは形式的）な安全性証明の方法論についての研究は，いわゆる Dolev-Yao モデルを用いた秘匿性／認証性の研究など，80 年代初頭からさかんに行われてきた．しかし，そこで用いられる形式化・抽象化の正当性を実際の暗号システムの性質に関連付けて議論すること（計算論的健全性と呼ばれる）は，潜在的にはその必要性が認識されつつも，長らく手つかずのままだった．一方暗号研究の分野では，複雑化する暗号システムの安全性証明をいかに正しく行うか（あるいは理解しやすくするか）という問題意識から，証明の記述法を様式化したり，さらには計算機によって自動化したりすることに興味が持たれつつあった．これら 2 つの研究分野の融合が，本会議のテーマである．

まず招待講演の内容から紹介すると，初日は，記号的安全性証明の計算論的健全性研究の嚆矢となるいわゆる Abadi-Rogaway 理論についての講演が，M. Abadi 氏自身によってなされた．またその発展であり，能動的な攻撃者の取扱いや mapping soundness に関する講演を B. Warinschi 氏が行った．さらに D. Pointcheval 氏が，近年暗号分野で注目されているゲームに基づくセキュリティ証明の方法論について話した．

2 日目には，Protocol Composition Logic（PCL）とその計算論的モデルについての講演が，J. Mitchell 氏と A. Datta 氏からあった．また，M. Berg 氏が，Backes-Pfitzmann-Waidner（BPW）モデルについて講演した（M. Backes 氏急病のため代理）．どちらも，計算論的に健全性な記号的安全性証明の方法論であり，かつセキュリティシステムの性質を compositional に導出できる，つまり個々の部品の性質からそれらを組み合わせたものの性質を導くことができる方法論として知られている．

3 日目は暗号分野からの講演で，汎用的結合可能性について O. Pereira 氏が，さらにそれに関連して Joint State 定理などに関する新たな結果とそれを可能にする IITM 計算モデルについて R. Kusters 氏が話をした．また電通大の太田先生から，MD ハッシュの証明可能安全性に関する講演があった．

最終日は，先に述べたゲームに基づく議論を直接的に形式化することによって計算論的に健全性な記号的安全性証明の方法論を得るという話題について，R. Segala 氏が確率 I/O オートマトンを用いたアプローチを，B. Blanchet 氏が確率プロセス計算に基づく検証ツールを，それぞれ紹介した．

一般講演については，紙面の都合から詳しくは述べないが，Abadi-Rogaway 理論や PCL を発展させた話題について，それぞれ数件の発表があった．ゲーム，および汎用的結合可能性に基づく議論を形式化するという発表も各 1 件あった．また，Hoare 論理を暗号の安全性証明に適用するというアプローチも紹介された．さらには，E-cash の安全性や，F# という関数型プログラミング言語で書かれたプロトコルの直接検証など，システム寄りの発表も数件あった．

以上のように，概要をかいつまんで説明するのも困難なほど，中身の濃い会議であった．次回の開催予定はアナウンスされていないが，何らかの形でまたこのような会議が開かれることを期待したい．

（真野　健／ NTT コミュニケーション科学基礎研究所）

講演の様子

Workshop dinner の様子