数理解析研究所講究録
1093 巻 1999 年 155-155

無証拠複数者間計算
Receipt-Free Multiparty Computation

櫻井 幸一
Kouichi Sakurai

九州大学大学院 システム情報科学研究科 情報工学専攻
〒 812-8581 福岡市東区箱崎 6-10-1
sakurai@csce.kyushu-u.ac.jp

概要： 本稿では、複数者間計算プロトコルにおける安全性を無証拠性の立場から検討する。

キーワード： 複数者間計算, 無証拠性, 否認可能暗号, 暗号プロトコル, 電子選挙

複数者間計算 (Multiparty computation)

暗号プロトコルの代表的計算モデルとして複数者間計算 (Multiparty computation) がある。最近の話題は、より高い安全性をもつ複数者間計算の設計である。この背景には、インターネット社会において公開鍵暗号が基盤技術としての地位を確立しつつあり、複数者間計算における暗号技術の利用法をもう一度見直しているという状況がある。

従来の複数者間計算 [CCD88, GMW87] では、静的・受動的外敵に対する安全性を議論していたが、現在では、より強力な動的・能動的・適応的な攻撃者までも考慮したプロトコルの研究が行なわれている [CDNO97, CFGN96]。

電子選挙の無証拠性

暗号論的複数者間計算プロトコルの応用例として電子選挙がある [CFSY96]。電子選挙における課題として証拠性 (Receipt-Free) がある。投票した事実の証拠が保存可能であれば、票売買への悪用や強制投票などの問題が生じる。したがって、(誰に) 投票したという事実を残さない" 無証拠性" を考慮した電子投票方式が検討されている [BT97a]。

無証拠性 対 非強制性

Canetti ら [CFGN96] は複数者間計算プロトコルの適応的な攻撃者に対する安全性と非強制性との関係を指摘している。

本研究では、Canetti らが提案した非強制性複数者間計算プロトコルの解析を通じて

1. 複数者間計算における無証拠性と非強制性との差 (形式的差と実質的差)
2. 無証拠複数者間計算プロトコルの設計
3. 複数者間計算の無証拠性に対応する安全性

を議論する。

参考文献

[BT97a] J. Benaloh and D. Tuinstra. "Receipt-free secret-ballot elections," Proc. STOC '94, pages 544–553.

[BT97b] J. Benaloh and D. Tuinstra. "Uncoercible communication," Clarkson Univ. TR-MCS-94-1 (Mar. 94).

[CFSY96] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung. "Multiauthority secret ballot elections with linear work," Proc. EUROCRYPT '96.

[CCD88] D. Chaum, C. Crepeaú and I Damgard, "Multiparty unconditionally secure protocols", 20th STOC, 1988.

[CG96] R. Canetti and R. Gennaro. "Incoercible multiparty computation" Proc. FOCS' 96.

[CFGN96] R. Canetti, U. Feige, O. Goldreich and M. Naor, "Adaptively Secure Computa-tion", 28th STOC, 1996.

[CDNO97] Canetti, Dwork,Naor, and Ostrovsky, "Deniable Encryption," Proc. CRYPTO'97.

[GMW87] O. Goldreich, S. Micali and A. Wigderson, "How to Play any Mental Game", 19th STOC, 1987.

[NR94] Niemi and Renvall, "How to prevent buying of votes in computer elections," Proc. Asiacrypt'94.

"Receipt-Free Mix-type voting scheme," Proc. Eurocrypt'95.