数理解析研究所講究録
第1712巻 2010年 p.170

確率様相論理による秘匿性の証明

竹内泉† 真野健‡
†産業技術総合研究所
‡NTT コミュニケーション科学基礎研究所

A proof of secrecy by probabilistic modal logic

Takeuti Izumi† & Ken Mano‡
† National Institute of Advanced Industrial Science and Technology
‡ NTT Communication Science Laboratories, NTT Corporation

情報を秘匿するプロトコルの中には，確率変数によって秘匿性が保証されるものがある．そのようなプロトコルに対して，公理的体系の中で情報の秘匿性を証明することを目的とする．そのための，確率変数を扱うことの出来る公理的な論理体系を設計することを目標とする．確率変数によって情報を秘匿するプロトコルに於いても，確率変数ではない変数は存在する．それはプロトコルの開始以前に値の決まっている変数である．このような変数は確率変数ではなく，非決定性過程によって値の定まる変数と見做さなければならない．本発表で提案する論理体系は命題変数と二階量化と確率様相が登場する量化様相命題論理である．そこでは，二階量化によって束縛される命題変数と確率様相によって束縛される命題変数がある．二階量化によって束縛される命題変数は非決定性過程によって値の決まる変数を表す．確率様相によって束縛される命題変数は確率変数である．意味論は可能世界意味論で与え，その意味論に対し健全な公理系を与える．その公理系は完全かどうかは分からない．公理系は完全であることが望ましいが，健全であって必要な定理が証明出来る程度に強力なものであれば，完全でなくとも有用である．本稿では例題として暗号学者の会食問題を採り上げ，そのプロトコルの情報の秘匿をこの論理体系によって証明する．