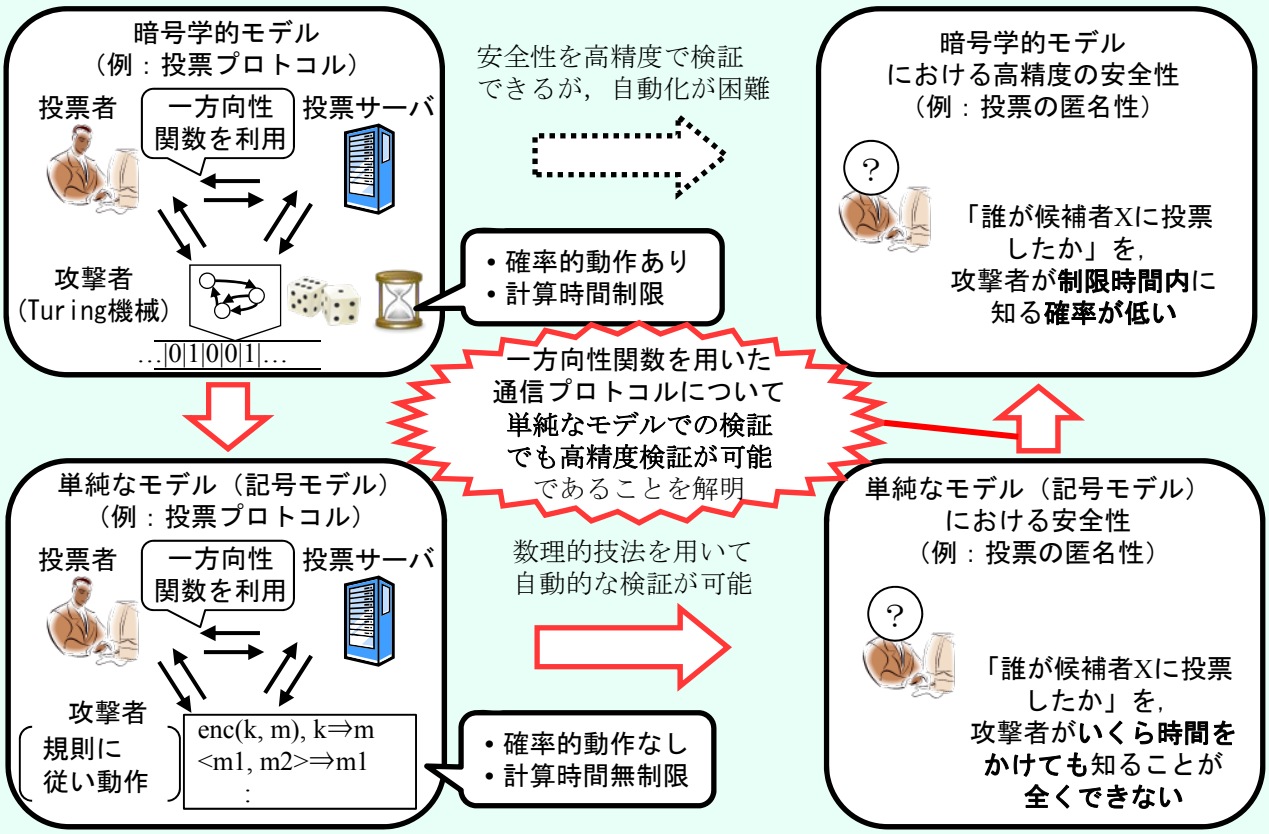
匿名性・プライバシの高精度検証に向かって
―数理的技法と暗号理論の融合による セキュリティ・プロトコルの高精度自動検証―

背景・課題：電子投票や医療に関わる通信などでは，通信プロトコル（通信の仕組み）により匿名性・プライバシなどの安全性が担保される必要があります．通信プロトコルの安全性を人手で正確に検査することは困難であるため，自動的に検証する方法が必要です．

アプローチ：通信プロトコルの安全性は暗号理論の枠組み（暗号学的モデル）を用いて定義されます．この枠組では安全性を高精度で検証できますが自動化が困難です．そこでより単純なモデル（記号モデル）を用いて自動検証を行い，単純なモデルでも高精度検証ができることを暗号理論に基づいて示します．

到達点：未解決問題の，一方向性関数を用いた通信プロトコルの匿名性・プライバシの高精度自動検証を可能にしました．一方向性関数は，パスワードの暗号化などのために非常に多くの通信プロトコルで用いられていますので，従来より多くの通信プロトコルを検証できるようになりました．

概要：



関連文献

H. Comon-Lundh, Y. Kawamoto, and H. Sakurada. Computational and Symbolic Anonymity in an Unbounded Network. JSIAM Letters, Vol.1 (2009), pp.28-31, 2009

H. Comon-Lundh, M. Hagiya, Y. Kawamoto, and H. Sakurada. Computational and Symbolic Anonymity in an Unbounded Network. In Proc. of FCC2009., pp.5-6, 2009

連絡先

櫻田英樹（Hideki Sakurada）

協創情報研究部 情報基礎理論研究グループ