Faculty of Engineering
Tokushima University

並列・軽量デバイスのための暗号技術

キーワード：暗号理論，軽量化，並列化　**講師　河内 亮周**

現代社会に大きな影響を与えたインターネットをはじめとする情報通信技術は新たな局面を迎えようとしている．従来インターネットに接続されている多くの機器がメモリ・処理能力が十分ある計算機であったが，低性能な計算能力しか持たないスマートフォン，家庭用電化製品なども近年では同じネットワークに接続されており，またそのような機器でもマルチコア化が進んでいる．

機器の低性能・並列性を前提として従来の計算機ネットワークと同等の情報セキュリティを保証できる暗号システムを発展させていくことは次世代ネットワークの基盤技術として非常に重要である．

本研究では非常に少ないメモリでも暗号化などの処理が可能，かつその処理の並列化が容易に可能となる基本的な暗号システム（公開鍵暗号，デジタル署名，対話型認証など）を構成し，そのセキュリティを数理科学的に解析する．またその構成可能性や性能に関する理論的限界を明らかにする．

分野：情報学

専門：暗号理論

E-mail: kawachi@is.tokushima-u.ac.jp

Tel. : 088-656-9446

HP : https://sites.google.com/site/akinorikawachi