KSRP 北九州学術研究都市
Kitakyushu Science and Research Park

北九州学術研究都市
大学研究シーズ集

(公財) 北九州産業学術推進機構
Kitakyushu Foundation for the Advancement of Industry, Science and Technology
FAIS

擬似乱数性器の設計法と乱数性評価

研究課題

【課題橋渡しガイド】
■サイバーセキュリティ対策技術 ■IoTネットワークの高信頼化 ■セキュリティ対策
■DX（IoT・デジタル化） ■見える化・数値化・センシング

ボタン電池で駆動可能なマイクロPC等でも，使用される無線通信において正しい情報を遅延なく取得することが必要である．

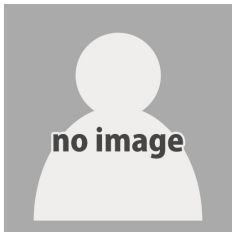
私の研究

【研究キーワード】
・小規模実装・解読不可能性・予測不可能性

【技術コンセプト】
計算資源が乏しいＰＣにおいて安全に安定して通信するための擬似乱数生成法を提案し，その乱数性について評価する．

【研究内容】
計算資源が乏しいＰＣにおいても安全性や安定性が重要視されている．使用メモリが少なく，計算負荷の少ないアルゴリズム必要であり，また乱数性の高い鍵生成も必要である．本研究では，以上の条件に適した写像にシフト演算や排他的論理和といった低負荷の処理を加えて乱数性を高めている．評価については，一般的な統計的乱数性による評価の他に予測し難さや解読し難さの指標となる評価法について検討している．

研究者



【プロフィール】
北九州市立大学国際環境工学部・大学院国際環境工学研究科
情報システム工学科（セキュリティ）
上原　聡（ウエハラ　サトシ）

【特許】
登録No.6678958 （擬似乱数生成装置及び擬似乱数生成プログラム）