諏訪東京理科大学
コンソーシアム専用

諏訪東京理科大学
「一技(ひとわざ) シーズ」PRシート

分類No：A-3

ひとわざ(一技)シーズ名： 数理との融合によって生まれた新暗号方式

1. シーズ概要(200字目安) 研究技術内容　　セールスポイント

東京理科大学 理工学部 情報科学科 大矢雅則教授の研究チームと、イタリア・ローマII大学のアカルディ教授のグループが、20年以上にわたる数学(非可換解析学・非可換確率論など)の研究をベースとして、開発した新しい暗号方式。

(1) 独自の数学理論を基にして、他方式に比べ非常に高い品質の乱数を生成することができる。
(2) 暗号の解を見つける確率がゼロになることが数学的に証明されており、従来方式と比べ非常に高い安全性を有している。
(3) 従来の方法に比べ、鍵交換、鍵生成アルゴリズムが圧倒的に速い(従来比1万倍以上の速さ)。

2.写真・図(技術要点説明)

独自の数学理論に基づく新しい疑似乱数生成アルゴリズム

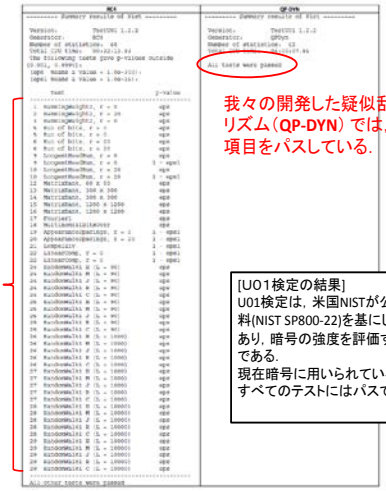
- 疑似乱数・・・一見，乱数列のように見えるが，実際はある特定の計算アルゴリズムによって求めた数列のこと．

疑似乱数は，次の性質を持たなければならない．

① 無作為性	統計的な偏りがなく，でたらめな数列になっているという性質
② 予測不可能性	過去の数列から，次の数を予測できないという性質

⇒ ある数列が，これらの性質を満たしているかを確認するには，様々な項目について統計テストを行わなければならない．

様々なランダム性評価テストが存在しているが，**最も厳しいテストと言われているのがU01検定である．**



3.産業への活用方向　　(適応業界・分野等)

Streaming(デモ有) 音声・動画などのマルチメディア・ファイルを安全にかつ高速に転送する。
Strong Identification (デモ有)自動車のキーレスエントリーなどへの応用．etc

4.関係する大学・企業等

東京理科大学 総合研究機構 量子生命情報研究部門(部門長：大矢雅則教授)
ローマ大学II ボルテラ・センター(センター長：ルイジ・アカルディー教授)

5. 研究室概要

学 科 名	経営情報学科	研 究 分 野	研 究 者 名
		数理情報、数理物理、数理経済	松岡 隆志
主研究テーマ	量子情報理論、非可換確率論、作用素代数論、ゲーム理論		
主要キーワード	量子エントロピー、エンタングルメント、量子相関、アダプティブ・ダイナミクス、ミクロ・マクロ双対性、公平性を取り入れた効用モデル、etc.		

特記事項
①特許取得・各種認証等取得状況(予定含む)：本件における非対称公開鍵暗号方式をイタリアにて特許出願中．日本でも同様な出願を行う予定．
②シーズの熟度(基礎研究 技術開発 実証開発 実用化開発段階等)：本暗号方式を用いたいくつかの試作品(イモビライザー，暗号化ソフトなど)がある．また、現在，実用化に向けてパートナー企業と製品を開発中．

備考：本研究は、当該研究者が所属する研究グループの共同研究者たちによる成果であり、現在のところ、当該研究者は本研究に関連した論文による実績はありません。ご興味をお持ちの方には、当該研究者が実質の研究メンバーを紹介します。