平成30年度研究開発成果概要図 （目標・成果と今後の研究計画）

１．研究課題・受託者・研究開発期間・研究開発予算

◆研究開発課題名：超長期セキュア秘密分散保管システム技術の研究開発　課題A　物理乱数源の研究開発
◆副題　　：秘密分散の基盤となる小型・高速・安全な物理乱数源の開発とシステム総合評価
◆実施機関　　：株式会社ワイ・デー・ケー
◆研究開発期間：平成30年度から平成32年度（3年間）
◆研究開発予算：総額45百万円（平成30年度15百万円）

２．研究開発の目標

真性乱数を安定的に生成できる乱数抽出アルゴリズムを適用し、利用シーン別に3種類の物理乱数生成製品のプロトタイプを研究開発する。多様な製品へ搭載可能な回路組み込みを前提とした①物理乱数チップ、様々な社会ニーズに適用するため小型・可搬型を前提とした②物理乱数ドングル、サーバ等で大量のデータを処理するためラック搭載型・高速リアルタイム生成を前提とした③高速物理乱数生成装置とする。

３．研究開発の成果

①物理乱数チップ

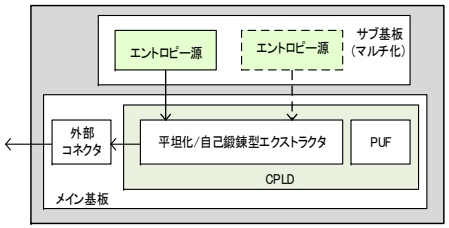
研究開発目標

複数のエントロピー生成源を搭載可能とするマルチ化構造とし、後段の乱数抽出回路により、真性乱数を安定的に生成できる機能の設計
・複数のエントロピー源を搭載可能なマルチ化構造
・低容量な圧縮・自己鍛錬型ランダム行列

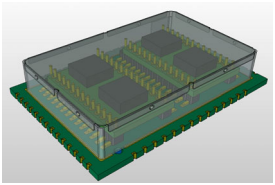
研究開発成果

〇二段構成を採用
メイン基板とサブ基板により、外部インタフェースの共通化、複数のエントロピー源を搭載可能とするマルチ化を実現
〇Toeplitz行列を採用
乱数圧縮性能は同等で、回路規模を大幅に縮小。廉価デバイスでの実現可能。

機能ブロックイメージ



概観イメージ

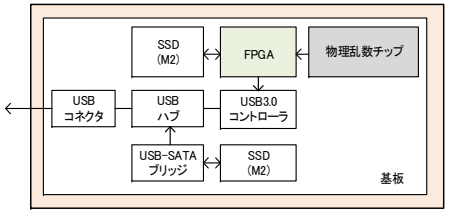


②物理乱数ドングル

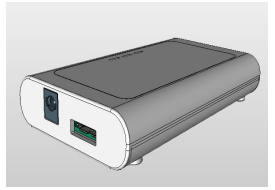
物理乱数チップ（①）を実装した可搬型物理乱数源の設計
・可搬型として樹脂筐体120mm×70 mm×21 mm
・乱数/分散データを各々10Gbit以上格納
・USB3.0によるデータ入出力性能1Gbps以上
・消費電力900mW以下

〇樹脂筐体120mm×70 mm×21 mm
物理乱数チップ、各種メモリ、USB3.0回路等を搭載し、可搬型物理乱数源を実現
〇不揮発メモリM.2 SSD採用
乱数/分散データを各々32GB以上格納し、小型化を実現。高速アクセス可能でUSB3.0による1Gbps転送性能を見込む。

機能ブロックイメージ



概観イメージ

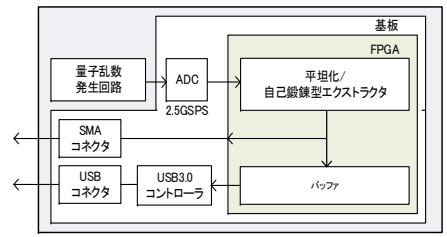


③高速物理乱数生成装置

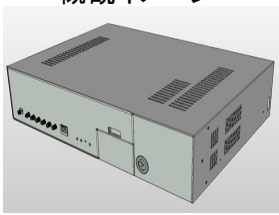
量子乱数発生回路を小型化搭載し、物理乱数生成速度を高速化する設計
・量子乱数発生回路を搭載し、19インチラック2U構造
・高速な圧縮・自己鍛錬型ランダム行列構造の実現
・乱数生成性能1.244Gbps以上、LVDSでリアルタイム出力

〇量子乱数発生回路搭載
量子乱数発生回路を省スペース実装し、19インチラック2U構造のラック搭載一体型として実現
〇Toeplitz行列を採用
乱数圧縮性能は同等で、回路規模を大幅に縮小。低コストで並列化・高速化を実現

機能ブロックイメージ



概観イメージ



4. 特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	プレスリリース 報道	展示会	標準化提案
0 （0）	0 （0）	0 （0）	0 （0）	0 （0）	0 （0）	0 （0）

※成果数は累計件数、（ ）内は当該年度の件数です。

5. 今後の研究開発計画

平成30年度の研究開発成果により、物理乱数チップ、物理乱数ドングル、高速物理乱数生成装置の試作機を製作し、機能評価を実施する。評価結果を基に改善を図る。