様式 1-4-2 (2019-1)

平成 30 年度研究開発成果概要書

採 択 番 号　　：202A01
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

（1）研究開発の目的

超長期間にわたって機密性と完全性を確保し、且つ事業継続性計画を高めるためには、秘密分散によるセキュアな分散データ保管が最適である。この秘密分散には物理乱数源による真性乱数が大量に求められる。この社会的なニーズに答えるために、以下の利用シーンの要件を満たした物理乱数源の研究開発を実施する。

- 多様な製品へ搭載可能な回路組み込みを前提とした物理乱数チップ
- 多様な社会ニーズに適用するため小型・可搬型を前提とした物理乱数ドングル
- サーバ等で大量のデータを処理するためラック搭載・高速リアルタイム生成を前提とした高速物理乱数生成装置

（2）研究開発期間

平成 30 年度から平成 32 年度（3 年間）

（3）実施機関

株式会社ワイ・デー・ケー

（4）研究開発予算（契約額）

総額４５百万円（平成 30 年度１５百万円）　※百万円未満切り上げ

（5）研究開発項目と担当

研究開発項目１：物理乱数チップの開発
1. 製品プロトタイプの設計・試作・評価（株式会社ワイ・デー・ケー）.
研究開発項目２：物理乱数ドングルの開発
1. 製品プロトタイプの設計・試作・評価（株式会社ワイ・デー・ケー）
2. 秘密分散ソフトとの結合評価（株式会社ワイ・デー・ケー）
研究開発項目３：高速物理乱数生成装置の開発
1. 製品プロトタイプの設計・試作・評価（株式会社ワイ・デー・ケー）
2. 秘密分散ソフトとの結合評価（株式会社ワイ・デー・ケー）

（6）特許出願、論文発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表	研究論文	0	0
	その他研究発表	0	0
	プレスリリース・報道	0	0
	展示会	0	0
	標準化提案	0	0

（7）具体的な実施内容と成果

研究開発項目１：物理乱数チップの開発

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を実現するために、検討・考案・設計を実施した結果、以下の成果を得た。

マルチ化構造を実現するために、メイン基板とサブ基板による二段構成を採用した。メイン基板は外部インタフェース機能、乱数抽出処理機能を有し共通化する。複数のエントロピー源を認識し、制御を自動的に可変する機能も有する。サブ基板は各種エントロピー源に対応し、異なる回路仕様を吸収する。

低容量な乱数抽出処理を実現するために、自己鍛錬型エクストラクタのランダム行列を Toeplitz 行列で実現する。これによって、乱数圧縮性能は同等で、回路規模を大幅に縮小することが可能となった。

研究開発項目２：物理乱数ドングルの開発

研究開発項目１の物理乱数チップを実装した可搬型物理乱数生成源を実現するために、検討・設計を実施した結果、以下の成果を得た。

樹脂筐体 120mm×70 mm×21 mm 以下に物理乱数チップ、各種メモリ、USB3.0 回路等を搭載し、可搬型モデルの実現が可能となった。USB3.0 給電の他、外部 DC 給電と併用できる機能も有する。

物理乱数データ、分散データを保存する不揮発性メモリとして SSD メモリを採用し、各々32GB 以上の格納領域を用意する。各 SSD メモリは USB コントローラ、USB ハブ経由で USB3.0 インタフェースと接続され、回路構成として 1Gbps 以上の転送性能を見込む。

研究開発項目３：高速乱数生成装置の開発

機構が提供する量子乱数発生回路を小型化搭載し、物理乱数生成速度の高速化を目指すために、検討・設計を実施した結果、以下の成果を得た。

量子乱数発生回路を機構と連携して省スペース実装検討を重ねた結果、19 インチラック 2U 構造のラック搭載一体型として実現が可能となった。

乱数生成性能の高速化を実現するために、信号処理用高速 AD コンバータはサンプリング速度 2.5GSPS/分解能 12bit とし、後段自己鍛錬型エクストラクタはランダム行列を Toeplitz 行列で実現することによって、低コストで並列化・高速化を実現することが可能となった。

秘密分散ソフトとのインタフェースは物理乱数ドングルと共通の USB3.0 と決定した。