様式 1-4-2 (2022-1)

令和４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 年度から令和４年度（5 年間）

（３）受託者

株式会社ワイ・デー・ケー ＜代表研究者＞

（４）研究開発予算（契約額）

平成 30 年度から令和４年度までの総額 71 百万円（令和４年度 12 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）
2.高速化改良設計（株式会社ワイ・デー・ケー）
3.製造要領・評価法の構築（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・総合評価（株式会社ワイ・デー・ケー）
3.製造要領・評価法の構築（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・総合評価（株式会社ワイ・デー・ケー）
3.製造要領・評価法の構築（株式会社ワイ・デー・ケー）

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	2	2
	外国出願	0	0
外部発表等	研究論文	0	0
	その他研究発表	1	0
	標準化提案・採択	0	0
	プレスリリース・報道	1	0
	展示会	3	2
	受賞・表彰	0	0

（7）具体的な実施内容と最終成果

研究開発項目１：物理乱数チップの開発

1－1．製品プロトタイプの設計・試作・評価

メイン基板とサブ基板構造を採用することで、マルチ化/ミックス化構造を実現した。乱数抽出回路には Toeplitz 行列による低容量化を実現し、廉価デバイスを採用した。セキュリティ機構の検討と改良を図り、階層構造によるセキュリティ強化を実現した。

1－2．高速化改良設計

エントロピー源（サブ基板）のデュアル構造を利用し、後段の乱数抽出回路への入力データを多重化処理することで、乱数生成性能の高速化（倍速）を実現した。

1－3．製造要領・評価法の構築

適用する品質マネジメントシステムを検討し、品質保証体系図/QC 工程表へのマッピングを実施した。セキュアな工程については適用するサイバーセキュリティ規格を検討し、方針を決定した。乱数性の評価には NIST 検定や安全性パラメータを適用し、評価を実施した。

研究開発項目２：物理乱数ドングルの開発

2－1．製品プロトタイプの設計・試作・評価

樹脂筐体による小型・軽量な可搬型物理乱数源を実現した。不揮発性メモリを搭載し、乱数保存 2GB を格納することで、低速な乱数生成性能を補うことが可能となる。また、分散データ 16GB が格納でき、分散データを持ち運ぶストレージとしての機能も有する。秘密分散ソフトが動作する PC とのインタフェースとして、USB3.0 を採用し、乱数転送性能 1Gbps を実現した。

2－2．秘密分散ソフトとの結合評価・総合評価

秘密分散ソフト用 API を開発し、秘密分散ソフトとの結合評価を実施した。秘密分散システム総合評価としては、社内業務（出張先へ秘密情報携帯）への利用にトライし、利用者の意見等により、秘密分散ソフトのマンマシンインタフェース改良に着手した。

2－3．製造要領・評価法の構築

適用する品質マネジメントシステムを検討し、品質保証体系図/QC 工程表へのマッピングを実施した。セキュアな工程については適用するサイバーセキュリティ規格を検討し、方針を決定した。乱数性の評価には NIST 検定や安全性パラメータを適用し、評価を実施した。

研究開発項目３：高速乱数生成装置の開発

３－1．製品プロトタイプの設計・試作・評価

量子乱数発生回路を装置内部に搭載し、19 インチラック 2U 構造を実現した。乱数抽出回路には Toeplitz 行列による高速化を実現し、乱数生成性能 1.244Gbps 以上で LVDS リアルタイム出力が可能となった。また、外部ノイズによるエラー対策としてリアルタイム検定機能を搭載した。

３－2．秘密分散ソフトとの結合評価・総合評価

秘密分散ソフト用 API を開発し、秘密分散ソフトとの結合評価を実施した。機構において、潜在ユーザの量子鍵配送装置に高速物理乱数生成装置を LVDS 接続し、リアルタイム乱数生成の出力確認を実施した。動作に問題ないことを確認した。

３－3．製造要領・評価法の構築

適用する品質マネジメントシステムを検討し、品質保証体系図/QC 工程表へのマッピングを実施した。セキュアな工程については適用するサイバーセキュリティ規格を検討し、方針を決定した。乱数性の評価には NIST 検定や安全性パラメータを適用し、評価を実施した。

（8）研究開発成果の展開・普及等に向けた計画・展望

機構指導の下、研究開発の成果展開として大きく一つの計画がスタートしている。該当機種は高速物理乱数生成装置となり、本研究成果を活用して乱数生成性能5Gbps版の製品化に向け取り組みである。潜在ユーザとして実証評価を実施した QKD 向けとなる。

現在、具体的な物理乱数源事業計画案（研究開発、量産開発）を検討しているところである。

〇研究開発：10Gbps の乱数生成性能実現に向け、来年度量子雑音部、高速 A/D 部、統計処理部等を中心に研究開発を継続

〇製品開発：10Gbps 版の高速物理乱数生成装置量産開発、1Gbps 小型・廉価版の：高速物理乱数生成装置量産開発

標準化に向けては、安全保障等に関わる規格・標準（JIS Q 9100/NIST SP800-171/CMVP ESV）への適用と、これらを反映した作業標準・ガイドラインの作成を継続していく計画である。