様式 1-4-2 (2021-2)

令和３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３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）
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	0	0
	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	2	0
	受賞・表彰	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

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。

環境評価、乱数性評価等で抽出した課題については、改良検討・設計を実施し、以下の成果を得た。

乱数信頼性に付随するリアルタイム検定（ヘルスチェック）や乱数生成速度の一定化機構も搭載し、良好な結果を得た。セキュリティ面では物理セキュリティ機構を改良し、金属筐体をアウターカバーとインナーカバーに分割し、階層構造とすることで、開封攻撃への耐性を向上させることに成功した。原価低減の取り組みとしては、電源系回路の見直しを実施し、消費電力低減にも繋ながる見込みを得た。

研究開発項目２：物理乱数ドングルの開発

環境評価、乱数性評価等で抽出した課題については、改良検討・設計を実施し、以下の成果を得た。

消費電力・発熱を低減するため、搭載する物理乱数チップの電源系統を見直し、消費電力低減に繋げる方針とした。金型による樹脂成型を前提とした発熱対策については対策方針をリストアップした。物理乱数生成データの不揮発メモリ格納性能は最終目標 10Mbps 以上の性能を達成した。秘密分散ソフトからの乱数取得に際して、乱数生成停止せず連続生成動作に変更した。ノイズ等により外部信号ライン（USB3.0）にエラーが発生した場合には秘密分散ソフト用 API で検知し、エラー処理を実行するように対応した。

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。

研究開発項目３：高速乱数生成装置の開発

環境評価、乱数性評価等で抽出した課題については、改良検討・設計を実施し、以下の成果を得た。

機構と提供を受けている量子乱数発生回路構成部品の見直を開始した。環境動作温度範囲の精査や原価低減に繋げる。ノイズ等による外部信号ライン（USB3.0）への影響については物理乱数ドングルと同様である。また、ノイズ等による乱数生成中の影響については、物理乱数チップと同様にリアルタイム検定（ヘルスチェック）を搭載することで良好な結果を得た。

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。

（8）今後の研究開発計画

研究開発項目１：物理乱数チップの開発

製品化に向け製造要領として、製品の安定した品質/セキュアな工程を保証できるような製品量産サイクルに対応する作業標準書の整備を行う。製品の乱数性評価法確立とドキュメント作成を実施する。

研究開発項目２：物理乱数ドングルの開発

製品化に向け製造要領として、製品の安定した品質/セキュアな工程を保証できるような製品量産サイクルに対応する作業標準書の整備を行う。製品の乱数性評価法確立とドキュメント作成を実施する。

また、セキュリティ要件の検討を実施し、ガイドラインとしてまとめる。

研究開発項目３：高速乱数生成装置の開発

製品化に向け製造要領として、製品の安定した品質/セキュアな工程を保証できるような製品量産サイクルに対応する作業標準書の整備を行う。製品の乱数性評価法確立とドキュメント作成を実施する。

また、セキュリティ要件の検討を実施し、ガイドラインとしてまとめる。