様式 1-4-2 (2020-2)

令和２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）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 71 百万円（令和２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	1
	標準化提案・採択	0	0
	プレスリリース・報道	1	1
	展示会	1	1
	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

物理乱数ドングルへの搭載において、乱数性評価および製品化を想定した環境評価を実施した結果、以下の成果を得た。

乱数性評価では、搭載エントロピー源２種類に対し、乱数検定（NIST 検定 SP800-22）を実施し、個別および２種類をミックスした結果を得た。搭載エントロピー源の検定合格率を低容量乱数抽出回路により改善できることを確認し、良好な結果を得た。

環境評価については物理乱数ドングルの項目で記載する。

製品ライフサイクルにおける乱数性の保証について、製品量産サイクルを検討しターゲットを設定した。

研究開発項目２：物理乱数ドングルの開発

物理乱数チップの搭載において、乱数性評価および製品化を想定した環境評価を実施した結果、以下の成果を得た。

環境評価については製品の信頼性評価項目（IEC60950/IEC61000 など）の確認と並行して、乱数性への影響も確認を実施した。一部の試験で乱数検定の合格率が低下することなど課題が確認された。課題に関しては改良検討を継続している。

秘密分散ソフトとの結合においては、物理乱数ドングルと秘密分散ソフト用 API 並びに秘密分散ソフトが動作している PC との結合試験を実施し、良好な結果が得られた。

製品ライフサイクルにおける乱数性の保証について、製品量産サイクルを検討しターゲットを設定した。

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の搭載において、乱数性評価および製品化を想定した環境評価を実施した結果、以下の成果を得た。

乱数性評価では、乱数検定（NIST 検定 SP800-22）を実施し、平坦化処理分割比較、乱数抽出処理比較の結果を得た。搭載エントロピー源の検定合格率を低容量乱数抽出回路により改善できることを確認し、良好な結果を得た。

環境評価については製品の信頼性評価項目（IEC60950/IEC61000 など）の確認と並行して、乱数性への影響も確認を実施した。一部の試験で乱数検定の合格率が低下することなど課題が確認された。課題に関しては改良検討を継続している。

秘密分散ソフトとの結合においては、高速物理乱数生成装置と秘密分散ソフト用 API 並びに秘密分散ソフトが動作している PC との結合試験を実施し、良好な結果が得られた。

製品ライフサイクルにおける乱数性の保証について、製品量産サイクルを検討しターゲットを設定した。

（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

2021 年度は、エントロピー源の多重化構造等を実現し、後段の乱数抽出回路は入力データ多重化処理を組み込むことで高速化を図る。また、環境評価、乱数性評価、結合評価等で抽出した改良点の改良設計を実施する。

2022 年度は、製品化に向け製造要領として、製品量産サイクル（部品収集、製造、検査、出荷）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。2021 年度は、エントロピー源の多重化構造等を実現し、後段の乱数抽出回路は入力データ多重化処理を組み込むことで高速化を図る。

研究開発項目２：物理乱数ドングルの開発

2021 年度は環境評価、乱数性評価、結合評価等で抽出した改良点の改良設計を実施する。また、ネットワークサーバ、携帯端末等を用いた秘密分散システムの総合評価実施を実施する。

2022 年度は、製品化に向け製造要領として、製品量産サイクル（部品収集、製造、検査、出荷）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

2021 年度は環境評価、乱数性評価、結合評価等で抽出した改良点の改良設計を実施する。また、ネットワークサーバ、携帯端末等を用いた秘密分散システムの総合評価実施を実施する。

2022 年度は、製品化に向け製造要領として、製品量産サイクル（部品収集、製造、検査、出荷）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。