令和4年度研究開発成果概要図 （目標・成果と今後の成果展開）

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
◆受託者　　：株式会社ワイ・デー・ケー
◆研究開発期間　：平成30年度～令和4年度（5年間）
◆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）

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

研究開発目標

研究開発項目１　物理乱数チップの開発

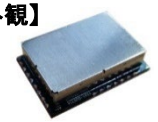
●製品プロトタイプの開発完了
・複数のエントロピー源を搭載可能なマルチ化構造の実現
・低容量な圧縮・自己鍛錬型ランダム行列構造の実現
・高速化により乱数生成性能10Mbps以上の実現
●製造要領・評価法の構築
・製品量産サイクルに対応する作業標準書作成
・製品単体の乱数性評価法確立とドキュメント作成

研究開発成果

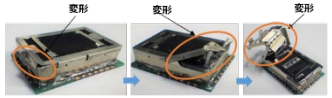
●設計・試作・機能確認・環境試験実施
○マルチ化/ミックス化構造を実現
・メイン基板とサブ基板構造を実現
・2種類の市販エントロピー源の搭載
○Toeplitz行列による低容量化を実現
・圧縮性能は同等のまま低容量化を実現
・廉価デバイス採用（FPGA汎用シリーズ）
○セキュリティ機構の検討と改良
・接着剤封入/金属ケース構造、認証デバイス実装
・階層構造によるセキュリティ強化を実現
○乱数生成性能の高速化を実現
・デュアル出力により、23.8Mbpsを実現
○環境ノイズ対策
・乱数性リアルタイム検定実装

●製造要領・評価法の構築
○製品量産サイクルの安定した品質
・適用する品質マネジメントシステム検討
・品質保証体系図/QC工程表へのマッピング実施
○製品量産サイクルのセキュアな工程
・適用するサイバーセキュリティ規格検討
○乱数評価法
・乱数性の評価：NSIT SP800-90B、安全性パラメータ
・乱数評価用ツールの提供：NIST検定等を実装

【外観】



【開封攻撃への耐性実験】



研究開発項目２　物理乱数ドングルの開発

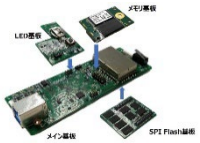
●製品プロトタイプの開発完了
・可搬型として樹脂筐体120m×70 mm×21 mmの小型化実現
・USB3.0によるデータ入出力性能1Gbps以上、給電900mW以下の消費電力を実現
・乱数/分散データを各々10Gbit以上格納
●超長期セキュア秘密分散システムの組み込みと総合評価実施
・課題B分散ソフトウェアとの接続インタフェース実現
・ネットワークサーバ、携帯端末等を用いた秘密分散システムの総合評価実現
●製造要領・評価法の構築
・製品量産サイクルに対応する作業標準書作成
・製品単体の乱数性評価法確立とドキュメント作成
・セキュリティ要件の検討とまとめ

●設計・試作・機能確認・環境試験実施
○小型・可搬型物理乱数源を実現
・樹脂筐体120mm×45 mm×21 mmを実現
○USB3.0インタフェースによる高速転送を実現
・乱数転送性能1Gbpsを実現
○不揮発性メモリの搭載
・乱数保存2GB、分散データ16GBを実現
○セキュリティ機能の検討
・解体検知機構、認証プロトコル実装
○環境ノイズ対策
・USB通信路のエラー検知とエラーデータの廃棄処理
●秘密分散システム結合と総合評価実施
・秘密分散ソフトウェア用APIの開発と結合確認実施
・社内業務としての利用にトライし、改良設計実施

●製造要領・評価法の構築
○製品量産サイクルの安定した品質
・適用する品質マネジメントシステム検討
・品質保証体系図/QC工程表へのマッピング実施
○製品量産サイクルのセキュアな工程
・適用するサイバーセキュリティ規格検討
○乱数評価法
・乱数性の評価：NSIT SP800-90B、安全性パラメータ
・乱数評価用ツールの提供：NIST検定等を実装

【外観】

【内部】



研究開発項目３　高速物理乱数生成装置の開発

●製品プロトタイプの開発完了
・量子乱数発生回路を搭載し、19インチラック2U構造で実現
・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を実現
●超長期セキュア秘密分散システムの組み込みと総合評価実施
・課題B分散ソフトウェアとの接続インタフェース実現
・機構の総合テストベッドを利用し、潜在ユーザとの共同総合評価実現
●製造要領・評価法の構築
・製品量産サイクルに対応する作業標準書作成
・製品単体の乱数性評価法確立とドキュメント作成
・セキュリティ要件の検討とまとめ

●設計・試作・機能確認完了、環境試験実施
○量子乱数発生回路を装置内部に搭載
・19インチラック2U構造を実現
・量子乱数発生回路EOL対応実施
○Toeplitz行列による高速化を実現
・乱数圧縮性能は同等で、回路規模を縮小
・LVDS　1.244Gbpsの速度を実現
○USB3.0インタフェースによる高速転送を実現
・乱数転送性能1Gbpsを実現
○セキュリティ機能の検討
・解体検知機構、認証デバイス、認証プロトコル実装
○環境ノイズ対策
・乱数性リアルタイム検定実装
●秘密分散システム結合と総合評価実施
・秘密分散ソフトウェア用APIの開発と結合確認実施
・潜在ユーザとの共同総合評価実施

●製造要領・評価法の構築
○製品量産サイクルの安定した品質
・適用する品質マネジメントシステム検討
・品質保証体系図/QC工程表へのマッピング実施
○製品量産サイクルのセキュアな工程
・適用するサイバーセキュリティ規格検討
○乱数評価法
・乱数性の評価：NSIT SP800-90B、安全性パラメータ
・乱数評価用ツールの提供：NIST検定等を実装

外観

内部

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	標準化提案	プレスリリース報道	展示会	受賞・表彰
2 (2)	0 (0)	0 (0)	1 (0)	0 (0)	1 (0)	3 (2)	0 (0)

※成果数は累計件数、(　)内は当該年度の件数です。

5. 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版の製品化に向けた取り組みである。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。

○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
○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。