令和3年度研究開発成果概要図 （目標・成果と今後の研究計画）

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年度から令和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3年度15百万円）

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

①物理乱数チップ

複数のエントロピー源の多重化構造等による高速化、環境・乱数性評価等で抽出した課題の改良
・乱数生成性能の高速化
・原価低減の検討
・物理的セキュリティの改良
・環境ノイズ対策

研究開発成果

●高速化、改良設計の実施
○乱数生成性能の高速化を実現
・デュアル出力による高速化を実現
○原価低減の検討を実施
・電源系統見直し実施、消費電力削減も可能
○物理的セキュリティの改良
・階層構造によるセキュリティ強化を実現
○環境ノイズ対策
・乱数性リアルタイム検定実装

インナーカバー　ポッティング　アウターカバー

②物理乱数ドングル

環境評価、乱数性評価、結合評価等で抽出した課題の改良と秘密分散システムの総合評価
・消費電力・発熱の低減
・物理乱数生成データの不揮発メモリ格納性能高速化
・物理乱数ドングルAPI動作の改良
・環境ノイズ対策
・秘密分散システムの総合評価

●改良設計の実施
○消費電力・発熱の低減を検討
・構成部品、動作スペックによる検討を実施
○不揮発メモリ格納性能の高速化を実現
・最終目標10Mbps以上の性能を達成
○物理乱数ドングルAPI動作の改良を実施
・USB転送と乱数生成同時処理時の消費電力を測定
○環境ノイズ対策
・USB通信路のエラー検知とメッセージ表示対応

◇秘密分散システム総合評価
・社内業務としての利用にトライ
・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

認証/分散/格納フェーズ　収集/復元フェーズ

③高速物理乱数生成装置

環境評価、乱数性評価、結合評価等で抽出した課題の改良と潜在ユーザとの共同総合評価
・環境動作温度範囲の改良
・環境ノイズ対策
・潜在ユーザとの共同総合評価

●改良設計の実施
○環境動作温度範囲の改良検討
・量子乱数発生回路の構成部品見直中
○環境ノイズ対策
・USB通信路のエラー検知とメッセージ表示対応
・乱数性リアルタイム検定実装

◇潜在ユーザとの共同総合評価
・機構内QKDとの結合確認実施
LVDSリアルタイム乱数出力

QKD：LVDS接続

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・採択	プレスリリース 報道	展示会	受賞・表彰
0 （0）	0 （0）	0 （0）	1 （0）	0 （0）	1 （0）	1 （0）	0 （0）

※成果数は累計件数、（ ）内は当該年度の件数です。

５．今後の研究開発計画

（1）製品化に向けた取り組み

①物理乱数チップ

・製造要領（製品量産サイクル作業標準書）、乱数性評価法（評価法ドキュメント）を構築する。

②物理乱数ドングル

・製造要領（製品量産サイクル作業標準書）、乱数性評価法（評価法ドキュメント）を構築する。セキュリティ要件（ガイドライン）をまとめる。

③高速物理乱数生成装置

・製造要領（製品量産サイクル作業標準書）、乱数性評価法（評価法ドキュメント）を構築する。セキュリティ要件（ガイドライン）をまとめる。

（2）製品利用に向けた取り組み

①秘密分散システム

・自社業務でのトライを重ねながらシステムの改良を推進し、展示会等を活用した潜在ユーザへのアプローチを実施する。
貸出品として新規製作の検討を進める。

②量子暗号通信システム

・QKDインタフェースの改良を検討する。機構と連携し潜在ユーザへのアプローチを実施する。
貸出品として新規製作の検討を進める。

（3）成果展開等

①特許出願（出願原稿作成中：2件、出願検討中：1件）

②展示会（量子コンピュータEXPO（春）、CEATEC2022、情報セキュリティEXPO（秋）への出展

③その他研究発表（電子通信学会など）