令和2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
◆実施機関　　：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：総額71百万円（令和2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

①物理乱数チップ

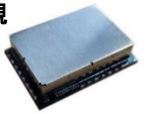
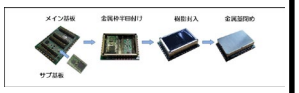
研究開発目標

複数のエントロピー源を搭載可能とするマルチ化構造とし、後段の乱数抽出回路により、真性乱数を安定的に生成できる機能の実現
・複数のエントロピー源を搭載可能なマルチ化構造
・低容量な圧縮・自己鍛錬型ランダム行列
・樹脂封入/金属ケースによる物理セキュリティ機構

研究開発成果

●設計・試作・機能確認完了、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
・乱数圧縮性能は同等で、回路規模を縮小
・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
・接着剤封入/金属ケース構造、認証デバイス実装

◇環境試験評価
外部環境変動における乱数性の確認実施
◇改善検討
課題を抽出し、改善検討実施

外観

内部


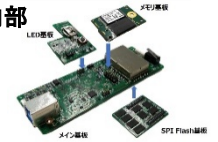
②物理乱数ドングル

物理乱数チップ（①）を実装した可搬型物理乱数源の実現
・可搬型として樹脂筐体120mm×70 mm×21 mm
・乱数/分散データを各々10Gbit以上格納
・USB3.0によるデータ入出力性能1Gbps以上
・消費電力900mW以下
・樹脂封入/金属ケースによる物理セキュリティ機構

●設計・試作・機能確認完了、環境試験実施
○樹脂筐体120mm×45 mm×21 mmを実現
・可搬型物理乱数源を実現
○乱数保存2GB、分散データ16GBを実現
・不揮発性メモリの搭載
○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、認証プロトコル実装

◇環境試験評価
外部環境変動における信頼性・乱数性の確認実施
◇秘密分散ソフト結合評価
物理乱数ドングル/APIと秘密分散ソフトによる実機評価
◇改善検討
課題を抽出し、改善検討実施

外観

内部


③高速物理乱数生成装置

量子乱数発生回路を小型化搭載し、物理乱数生成の高速化実現
・量子乱数発生回路を搭載し、19インチラック2U構造
・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
・USB3.0による乱数データ出力性能1Gbps以上
・金属ケースによる物理セキュリティ機構

●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
○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

◇環境試験評価
外部環境変動における信頼性・乱数性の確認実施
◇秘密分散ソフト結合評価
高速物理乱数生成装置/APIと秘密分散ソフトによる実機評価
◇改善検討
課題を抽出し、改善検討実施

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・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 （1）	0 （0）	1 （1）	1 （1）	0 （0）

※成果数は累計件数、（ ）内は当該年度の件数です。

（1）その他研究発表
「高速量子乱数源の実装と性能評価」2021年電子情報通信学会総合大会、2021/3/9～12オンライン開催
（2）プレスリリース
「100年単位の超長期情報保管にも耐えるストレージシステムを開発 － 物理乱数を用いた秘密分散で高度に安全な保護機能を提供 －」
2020年10月28日、国立研究開発法人除法通信機構、株式会社ZenmuTech、株式会社ワイ・デー・ケー
（3）展示会
第3回 ものづくりAI/IoT展 2021年2月3～5日、幕張メッセ ホール3

5. 今後の研究開発計画

◆物理乱数チップ：高速化改良設計
・抽出した課題の改良検討を基に、製品化に向けた改良設計を施す。乱数生成性能の高速化、物理セキュリティの強化が主となる。
◆物理乱数ドングル：改良設計
・抽出した課題の改良検討を基に、製品化に向けた改良設計を施す。消費電力低減・発熱対策、環境ノイズの耐性・リカバー対策が主となる。
◆高速物理乱数生成装置：改良設計
・抽出した課題の改良検討を基に、製品化に向けた改良設計を施す。動作環境温度の改善、環境ノイズの耐性・リカバー対策が主となる。
◆物理乱数ドングル、高速物理乱数生成装置
・秘密分散システムの総合評価、機構の総合テストベットを利用した総合評価を実施する。
◆物理乱数チップ、物理乱数ドングル、高速物理乱数生成装置
・製造要領・評価法の構築、セキュリティ要件の検討