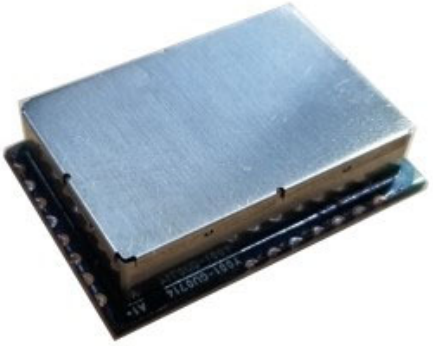
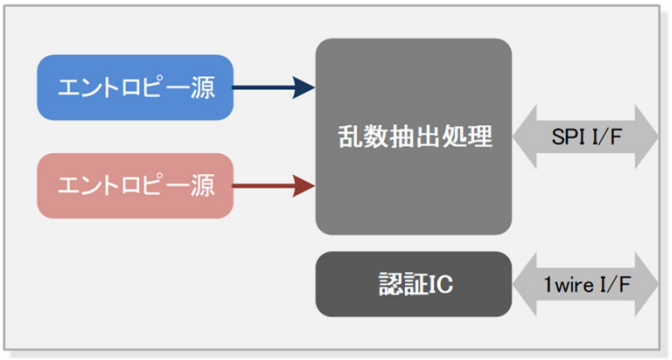
平成30年度 情報通信研究機構「高度通信・放送研究開発委託研究
超長期セキュア秘密分散保管システム技術の研究開発」成果

物理乱数チップ



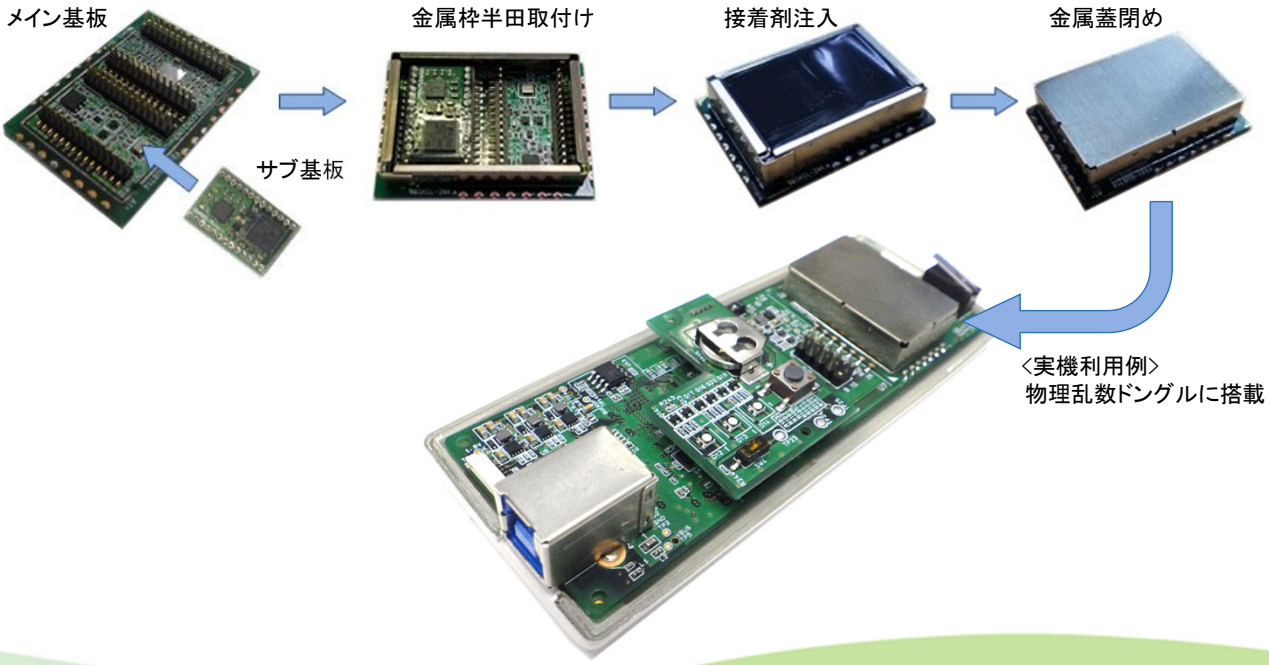
外観



ブロック構成図

○ 特徴

- ランダムな物理現象に基づき、真性乱数を生成
- 熱雑音、量子雑音など複数のエントロピー源を搭載可能（特許出願準備中）
- 搭載可能なエントロピー源は2種類(2021年3月時点)
- 乱数抽出回路には情報通信研究機構（NICT）考案の自己鍛錬型エクストラクタ
  （特開2018-147092）を採用
  （NIST Special Publication 800-22/-90Bをパス）
- 物理乱数生成性能：10Mbps以上
- セキュリティー機能を搭載
  a) ECDSA採用のデバイス認証IC搭載し、個体識別が可能
  b) 金属カバー内部は、熱伝導性接着剤を充填し、容易な分解を防御する構造
- サイズ：24.87(W)×35.3(D)×7.9(H) mm。
- 取り付け：端面スルーホール29ピン　半田付け

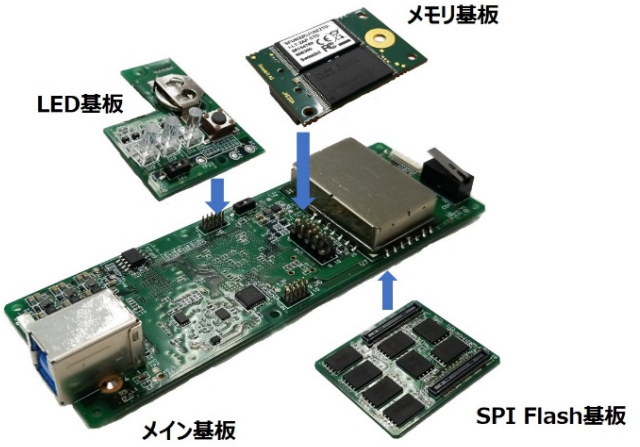


仕様は予告なく変更することがあります

YDK 株式会社 ワイ・デー・ケー
～確かなモノづくりで「世界へ」「未来へ」つなぐ！～
〒206-0811 東京都稲城市押立1288　技術本部ビル
電話：042-378-8511　https://ydkinc.co.jp/

平成30年度 情報通信研究機構「高度通信・放送研究開発委託研究
超長期セキュア秘密分散保管システム技術の研究開発」成果

物理乱数ドングル



○ 特徴

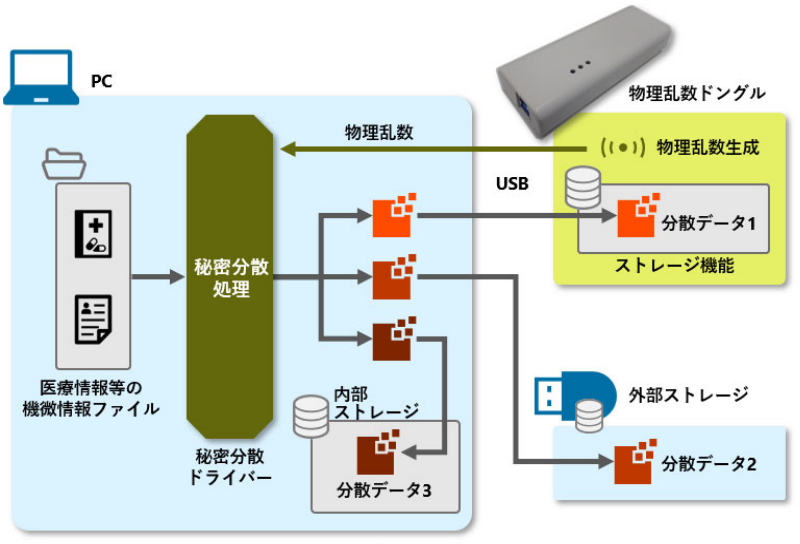
・持ち運び可能な物理乱数源
　120mm × 45mm × 21mm 、重さ 120g
・生成した物理乱数を保存し、利用時にまとめて使用することが可能
　物理乱数保存容量：16Gbit
・秘密分散された1片を格納し、持ち運びするストレージとして使用することが可能
　分散データ保存容量：32GB
・乱数出力(PC接続)インタフェースはUSB3.0により、1Gbps以上の転送が可能
・乱数生成には物理乱数チップを搭載
　生成性能：10Mbps以上、NIST Special Publication 800-22/-90Bをパス
・乱数データ形式：API側で、バイナリー、整数、浮動小数点を選択可能
・セキュリティー機能
　a) ワンタイム組立により容易に解体出来ない仕組み
　b) 解体時には、認証用鍵ペアを消去する
　c) ECDSAによる個体認証

○ 運用例

株式会社ZenmuTechが提供する秘密分散技術と組み合わせて、下記の機能を提供する。

・秘密鍵用の物理乱数

・秘密分散後のデータストレージ機能



※ 分散データ1～3のいずれか２つにより元のデータを復元可能

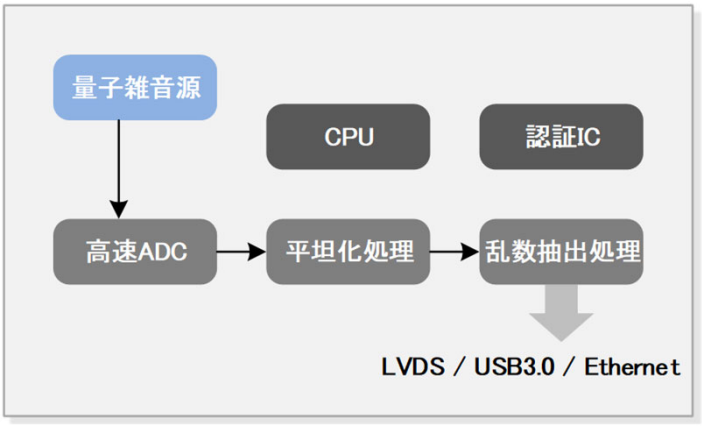
仕様は予告なく変更することがあります

株式会社ワイ・デー・ケー
～確かなモノづくりで「世界へ」「未来へ」つなぐ！～
〒206-0811 東京都稲城市押立1288　技術本部ビル
電話：042-378-8511　https://ydkinc.co.jp/

平成30年度 情報通信研究機構「高度通信・放送研究開発委託研究
超長期セキュア秘密分散保管システム技術の研究開発」成果

高速物理乱数生成装置

外観

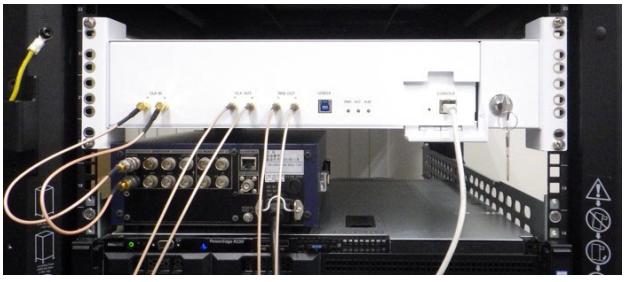


ブロック構成図

○ 特徴

・ランダムな物理現象に基づき、真性乱数を生成
量子乱数発生回路（NICT考案）を小型化し搭載。
・乱数抽出回路には情報通信研究機構（NICT）考案の自己鍛錬型エクストラクタ
（特開2018-147092）を採用
（NIST Special Publication 800-22 /-90Bをパス）
・高速なリアルタイム物理乱数生成を実現
a) 1.244Gbps（SMAコネクタ、LVDS、リアルタイム出力）
b) USB3.0 インタフェースによる乱数高速転送（1Gbps）
・保守用インタフェース
RJ-45(10Base-T/100Base-TX/1000Base-T)、前面鍵付き蓋で保護
・19inchラック搭載可能。高さ2Uに収容
430(W)×370(D)×88(H)mm
・セキュリティー機能
a) One Wrap Around 構造により、解体しにくい仕組み。
b) 解体時には、認証用の鍵情報を無効化
c) ECDSAによる個体認証

○ 接続例



QKD装置との接続（外部クロック同期）

USB3.0によるサーバーとの接続

仕様は予告なく変更することがあります

YDK 株式会社 ワイ・デー・ケー
～確かなモノづくりで「世界へ」「未来へ」つなぐ！～
〒206-0811 東京都稲城市押立1288 技術本部ビル
電話：042-378-8511 https://ydkinc.co.jp/