PQC時代に向けたHSMの研究

TTC・量子ICTフォーラム合同セミナー

2020年1月19日（火）
株式会社村田製作所
石井　宏一良

アジェンダ

- ムラタについて
- ムラタの量子暗号の現状
- 製品コンセプトのご紹介
- PQC実装研究の共有（NewHopeアルゴリズムについて）

ムラタについて　－概要－

村田製作所は、最先端の技術、部品を創出する総合電子部品メーカーです。Innovator in Electronicsをスローガンに掲げ、豊かな社会の実現をめざします。

ムラタの強み

- 最先端の材料を研究開発
- 広範囲な製品ラインナップ
- グローバルな生産、販売ネットワーク

ムラタのプロフィール

- 創業：　1944年
- 売上高：　1兆5千340億4千5百万円
- 企業数：　90社（国内28社、海外62社）
- 従業員数：74,109名（国内31,258名、海外42,851名）

※売上高は、2020年3月期決算。
※従業員数は2020年3月31日時点のものです。
※グループ企業数は2020年3月31日時点のものです。
※村田製作所はグループ企業数に含まれておりません。

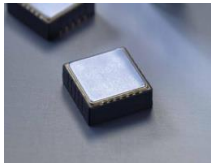
ムラタについて　－部品紹介－

ムラタセイコちゃん®

センサ技術

ジャイロセンサ

不倒停止や超低速走行を可能に



超音波センサ

障害物を検知して衝突を回避

エネルギー技術

リチウムイオン二次電池

ハイパワーと急速充電を実現した新型バッテリ

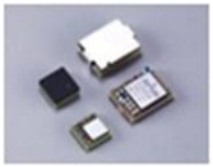
DC-DCコンバータ

体中に安定した電気を供給

通信技術

Bluetooth®モジュール

操作信号や音楽データを送受



アンテナ

PCやケータイと電波でつなぐ

その他回路部品

セラミックコンデンサ

電気を蓄え、電源を安定化

インダクタ（コイル）

信号や電流を安定化

サーミスタ

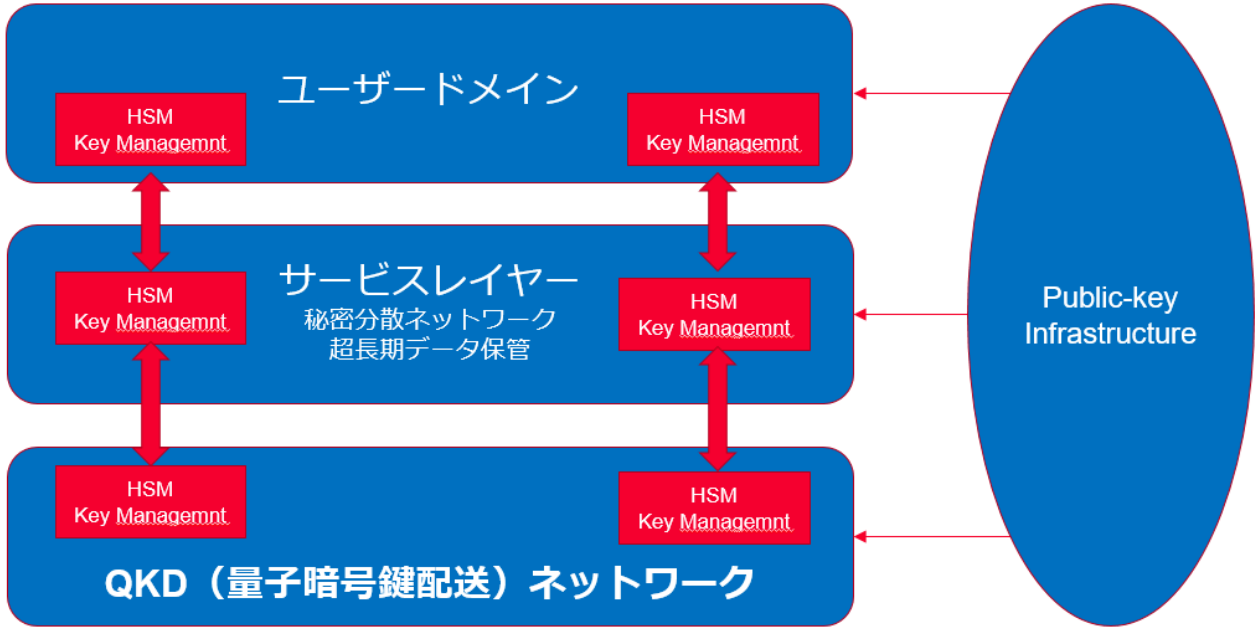
回路の過熱や充電を監視

EMI除去フィルタ

電磁ノイズを除去して誤動作を防ぐ

ムラタの量子暗号の現状

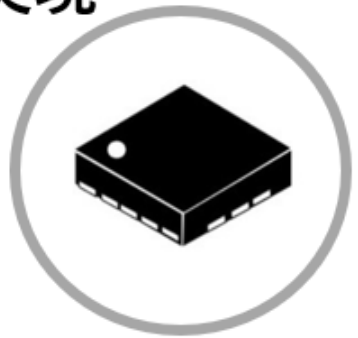
- 量子乱数を用いた高セキュリティモジュールを、量子暗号通信と、それに関係するプロジェクトで活用できないか模索中



製品コンセプトのご紹介

Preliminary

Quantum・*HSM
OTA時代、量子コンピューター時代のHSMを実現



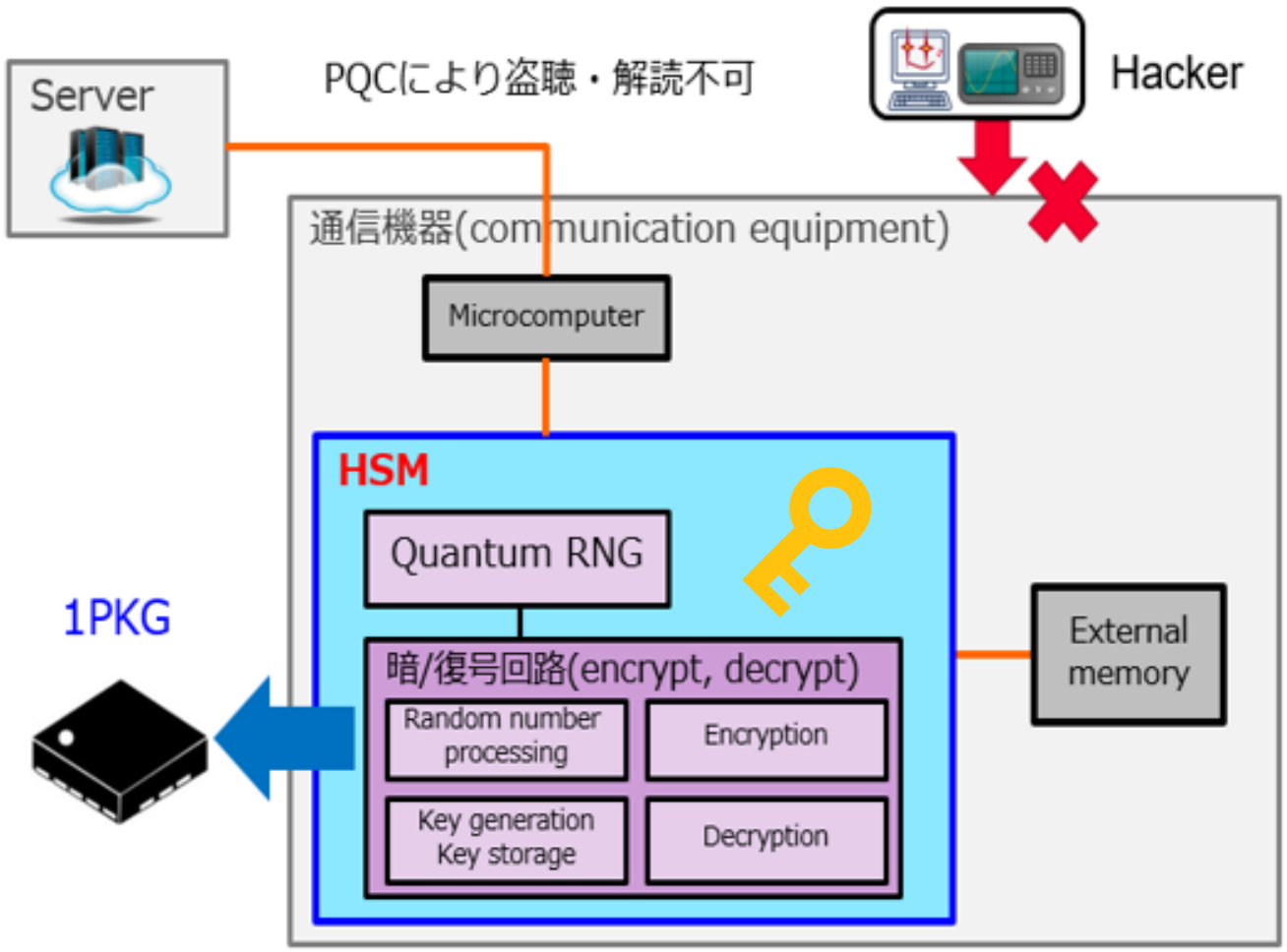
Quantum・HSMが、高速な暗号化を活かして、インターネットにつながるコネクティッドカーやドローンのサイバーセキュリティ対策や、量子コンピューター時代の*PQC(耐量子計算機暗号)へ移行をお手伝いします。

＊HSMは、盗聴、改ざん、成りすましなどのサイバー攻撃を防ぐため、データの暗号化やデジタル署名のための暗号鍵を安全に保管するセキュリティハードウエアです。

＊PQCとは、量子計算機で解読が困難な耐量子計算機暗号のこと。米国国立標準技術研究所（NIST）が2024年までに標準化を予定する。

製品コンセプトのご紹介

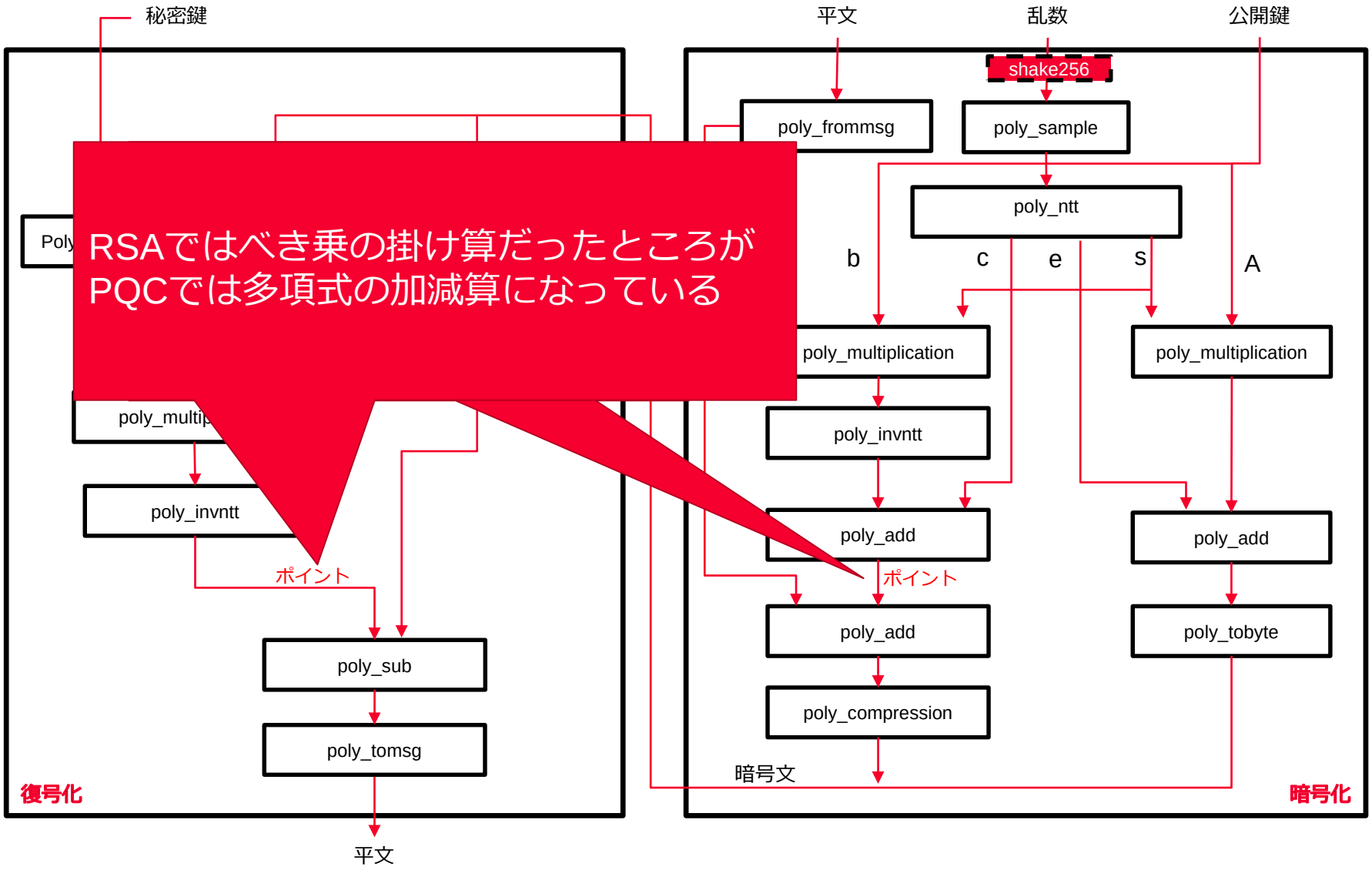
構成図 Block Diagram



製品コンセプトのご紹介

- 特長
  - ①暗号化が高速
  - ②耐量子計算機暗号で量子コンピューター時代に対応
  - ③後付けで Key-management を提供

PQC実装研究の共有（NewHopeアルゴリズムについて）



RSAではべき乗の掛け算だったところが
PQCでは多項式の加減算になっている