電気通信大学 情報・通信工学科 佐藤研究室

暗号アルゴリズムの実装性能評価

The University of Electro-Communications
SATOH Lab

広がる暗号の民間利用と標準化

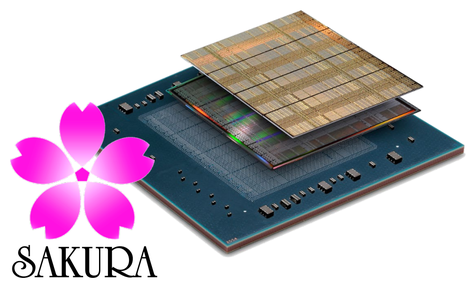
- 暗号の研究は第二次世界大戦で発展したが，現在はデジタル放送，携帯電話，ネットショッピング，電子マネー等様々な電子機器や民間サービスで広く利用されている.
- 従来は数学者による論理的な研究が主であったが，暗号アルゴリズムの標準化では，ソフトウェアやハードウェアへの実装性能が重視されている.
- 暗号は情報の秘匿だけでなく，改ざん防止や，デジタル署名にも用いられ，また用途に応じて様々なアルゴリズムが標準化されている.
- 佐藤研では，標準化活動への貢献として，暗号アルゴリズムを様々なプラットフォームに実装して性能を比較評価している.

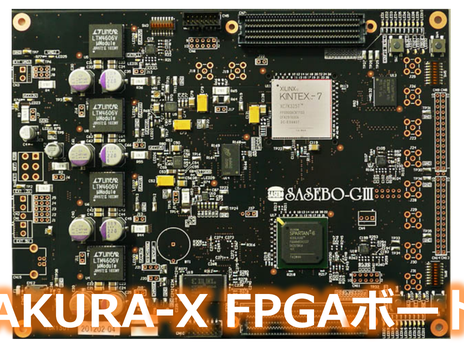
エニグマ暗号機

http://imitationgame.gaga.ne.jp/

FPGAとGPGPUへの実装性能評価

- 従来はPC用汎用プロセッサや組込MPUへのソフトウェア実装と，カスタムICチップへのハードウェア実装がメインであったがFPGAやGPGPU等への実装が今後重要となる.
- FPGA (Field Programmable Gate Array) はユーザーが手元で機能を書き換え可能なハードウェアデバイスで，多くの民生機器で使用されている.
- GPGPU (General Purpose Graphic Processing Unit) は元来グラフィック用のプロセッサを科学技術計算等に活用し発展したもので，2~8コア程度のIntelプロセッサに対してGPUモジュールは数千個のコアを搭載.



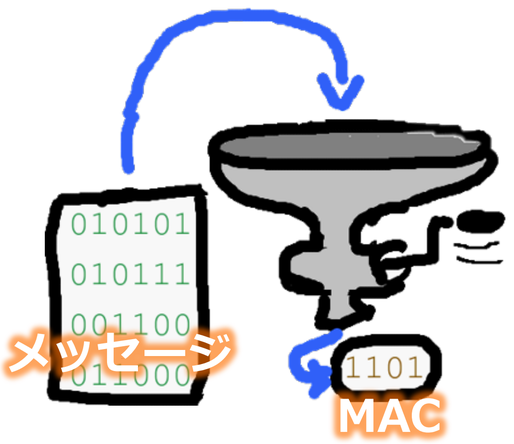


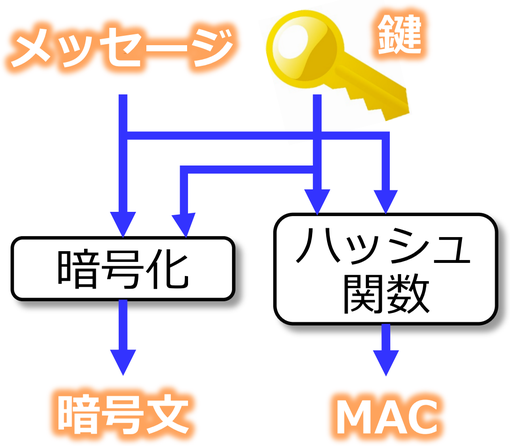
SAKURA-X FPGAボード


NVIDA Tega K1 GPU

ハッシュ関数SHA-3と認証付暗号Minalpher

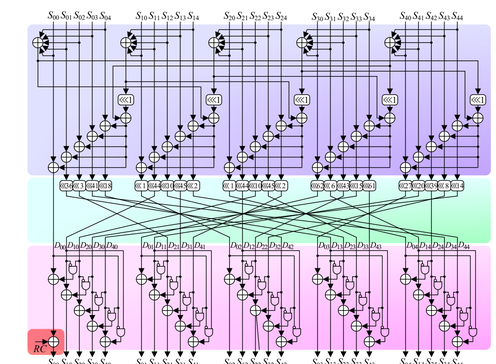
- ハッシュ関数は可変長のメッセージを固定長のMACに圧縮して改ざんを防止するもので，従来の標準SHA-1/-2に弱点が見つかりSHA-3の策定が2007-13年に行われた.
- 認証付き暗号は暗号化とMAC生成を一つのアルゴリズムにまとめたもので，CAESARプロジェクトで2017年の標準化がすすめられている．Minalpherは日本からCAESARプロジェクトに提案されたアルゴリズム.

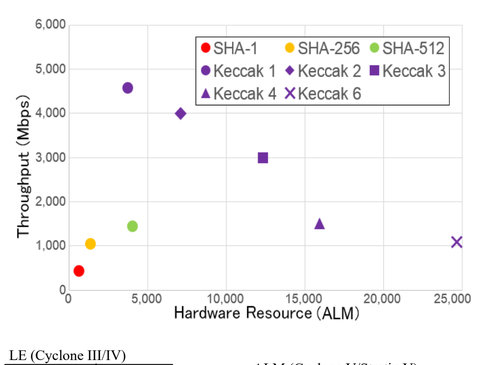


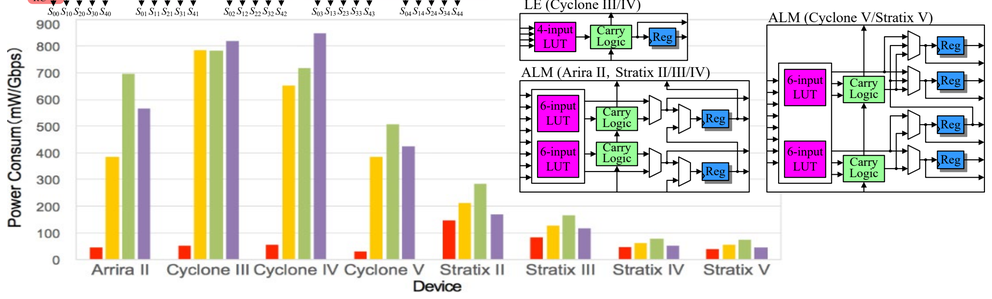


SHA-3とMinalpherの実装性能

- SHA-3とMinalpherの複数のアーキテクチャによる回路を設計し主要な14種類のFPGAを用いて，回路規模，動作速度，消費電力などの実装性能を比較評価.
- SHA-3は高速性に優れているが，小型化や最新のFPGAデバイスへの実装性能に問題があることが明らかに.
- MinaplherはFPGA実装において小型～高速まで高いスケーラビリティを有し，従来の認証付き暗号の標準AES-GCMよりも優れた性能を示した.
- Minalpherの並列処理性を生かし，GPGPUによる高速なソフトウェア実装を予定.







akashi.satoh@uec.ac.jp