暗号モジュールのハードウェア実装について

電気通信大学 情報通信工学科

崎山　一男

暗号とハードウェア実装

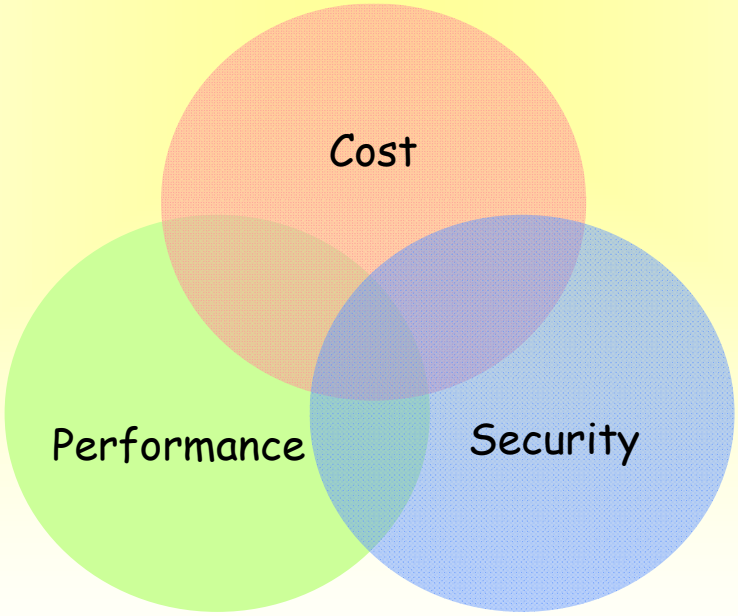
- 情報セキュリティ機器における暗号技術

- 暗号≠セキュリティ
  - きわめて重要な要素

- 広がるアプリケーション
  - ネットワーク
  - スマートカード
  - 携帯電話
  - ゲーム機
  - RFIDタグ
  - VoIP, etc…

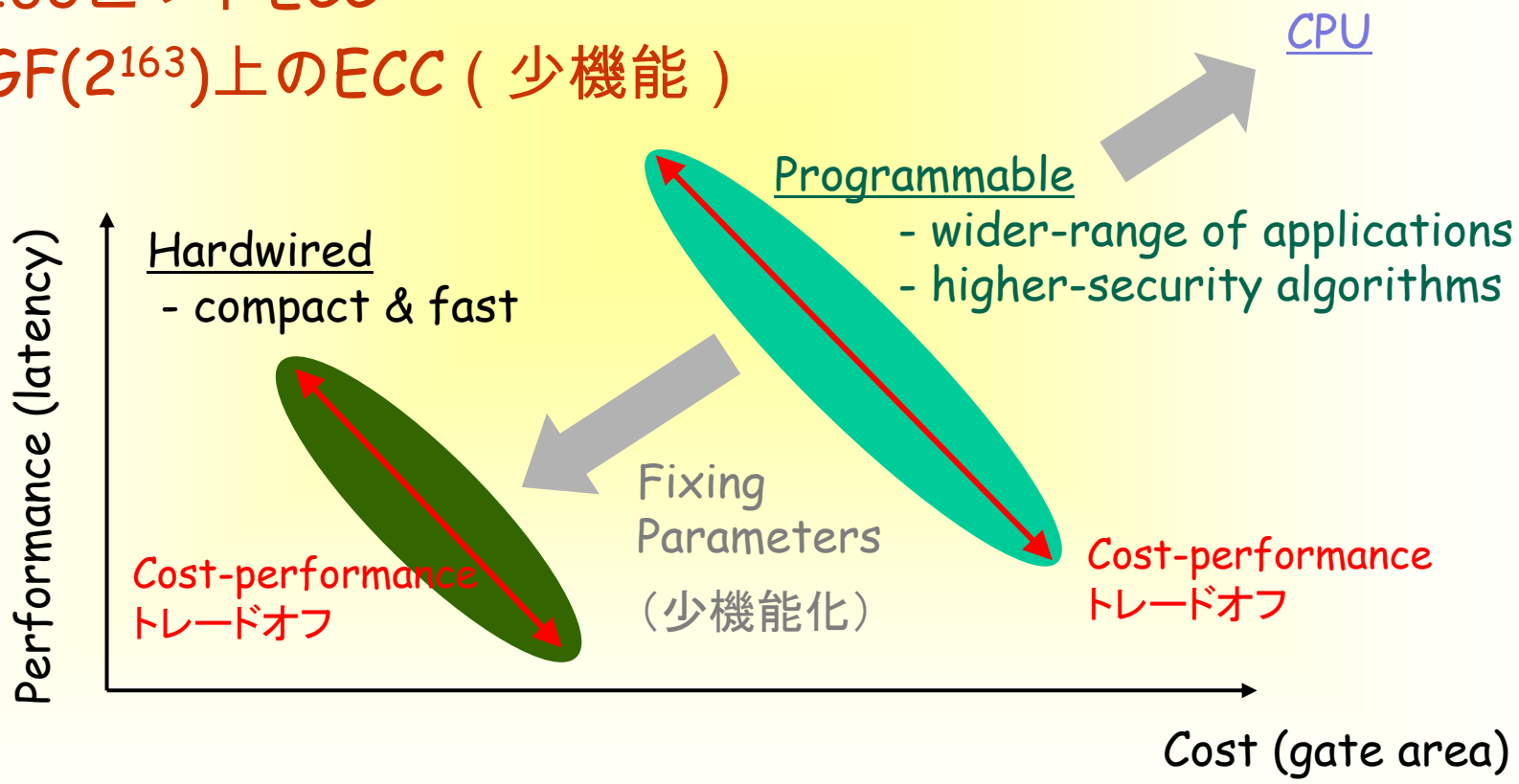
Cost, Performance and Security Trade-offs

- 暗号モジュールの3要素
  - Cost: ゲート数, データメモリ容量, テスト性, etc.
  - Performance: 処理速度, 消費電力, etc.
  - Security: 物理攻撃耐性, サイドチャネル攻撃耐性



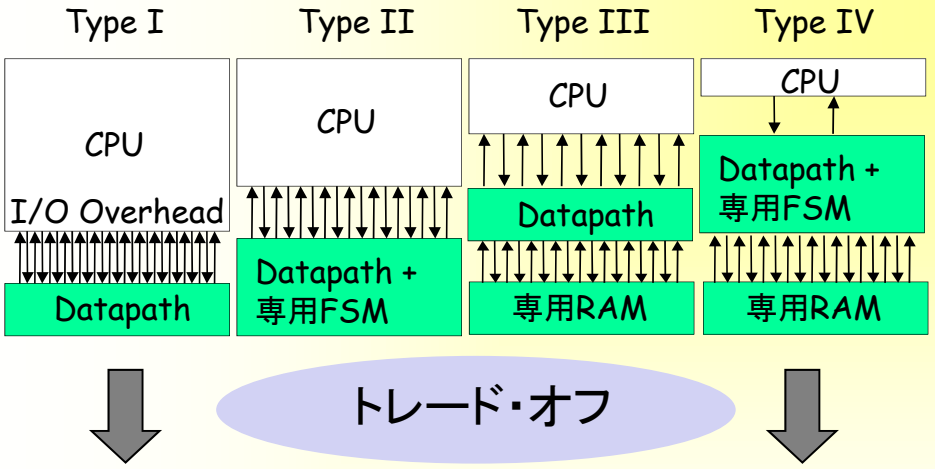
ハードウェア実装と柔軟性

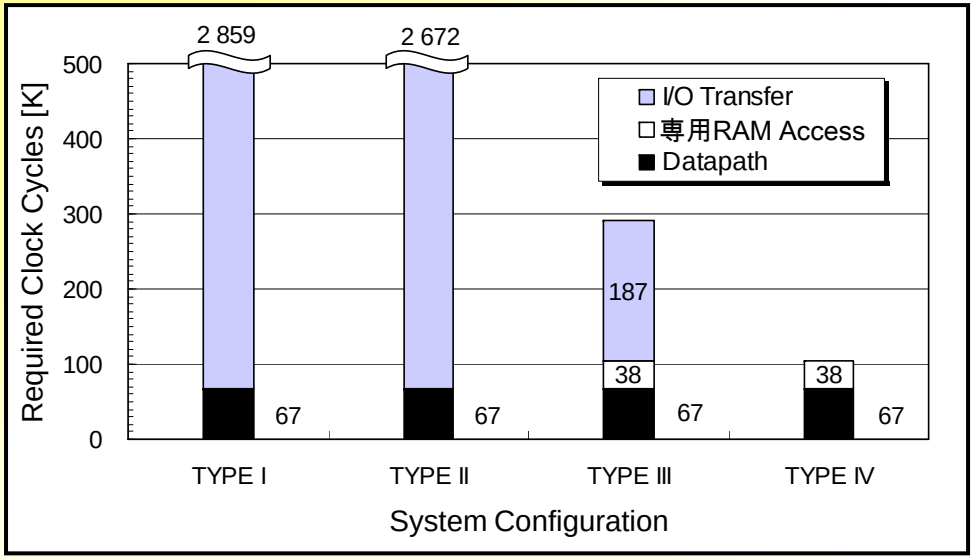
- 多機能 vs 少機能
  - 例えばRSAとECCをサポート（多機能）
  - 163ビットECC
  - GF(2^{163})上のECC（少機能）



HW/SW Co-design

- ハードウェア性能とインタフェース
  - 専用FSM（μコントローラ）
  - 専用RAM
  - コストとスピードのトレード・オフ





超楕円曲線暗号の実装例
[CHES2006]

暗号モジュールの実装性評価

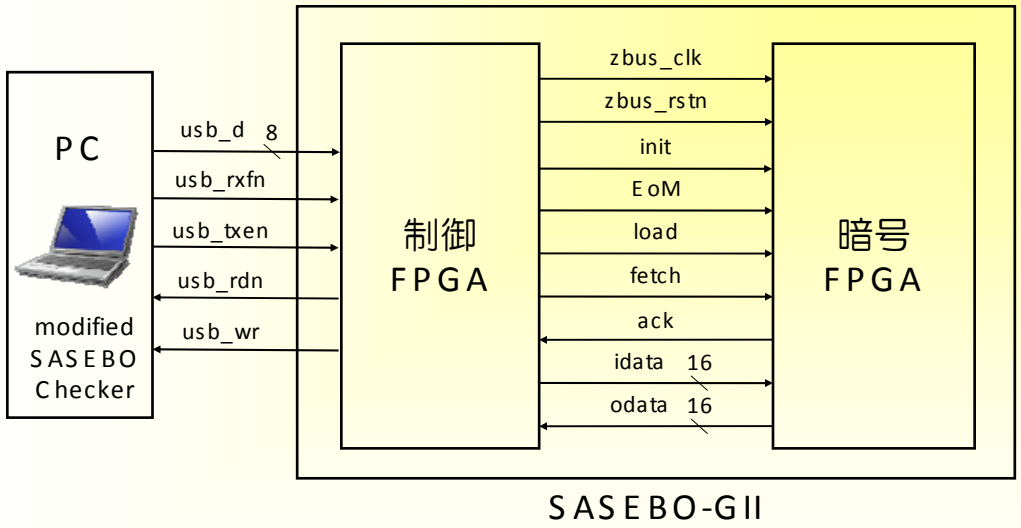
- どう評価するか (HOW?)
  - 評価プラットフォーム
    - ハードウェアでは多種多様 (cf. ソフトウェア評価のIntel)
  - 設計フロー
    - 多くのパラメター (cf. C言語のコンパイルオプション)
    - Verilog or Custom Cell (cf. C言語 or アセンブラ)

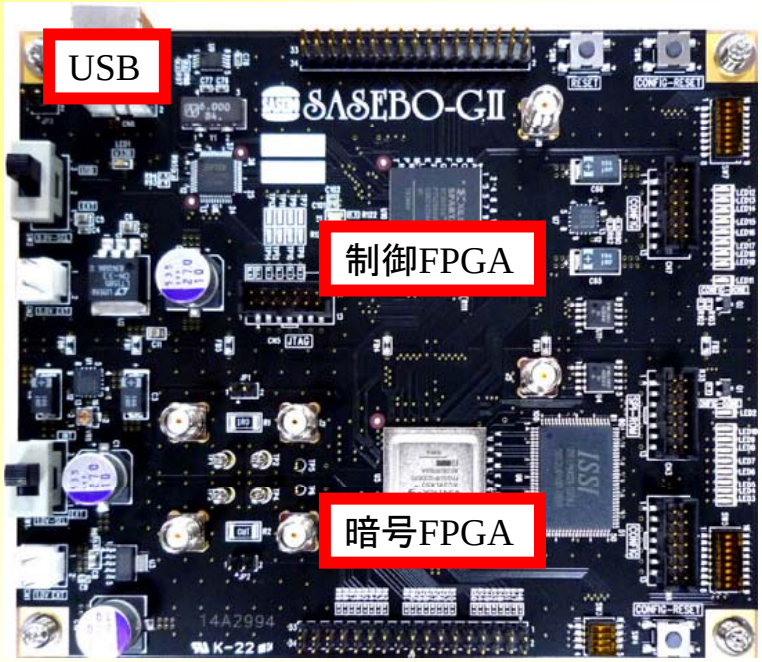
- 何を評価するか (WHAT?)
  - 実装効率
    - Throughput / gate
    - Latency・gate
  - サイドチャネル攻撃耐性

- プラットフォーム
- 設計方針
- 評価基準

最近のとりくみ

- 公平なSHA-3候補のハードウェア評価に向けて
  - SASEBO-GIIを使用
    - 共通インタフェース
    - 共通デザインフロー
    - 公平な結果比較





[SCIS2010, ePrint2010/010]

SHA-3候補の評価基準

ロ 総サイクル数

十分長いメッセージでは無視できる

$$I = \frac{M_{pad}}{B}(I_{din} + I_{core}) + I_{dout} + I_{final}$$

ロ ロングメッセージではスループット

$$Th = \frac{B \cdot f_{max}}{I_{in} + I_{core}}$$

【チーター】最高時速~100km
100m走 6秒13 [Wikipedia]

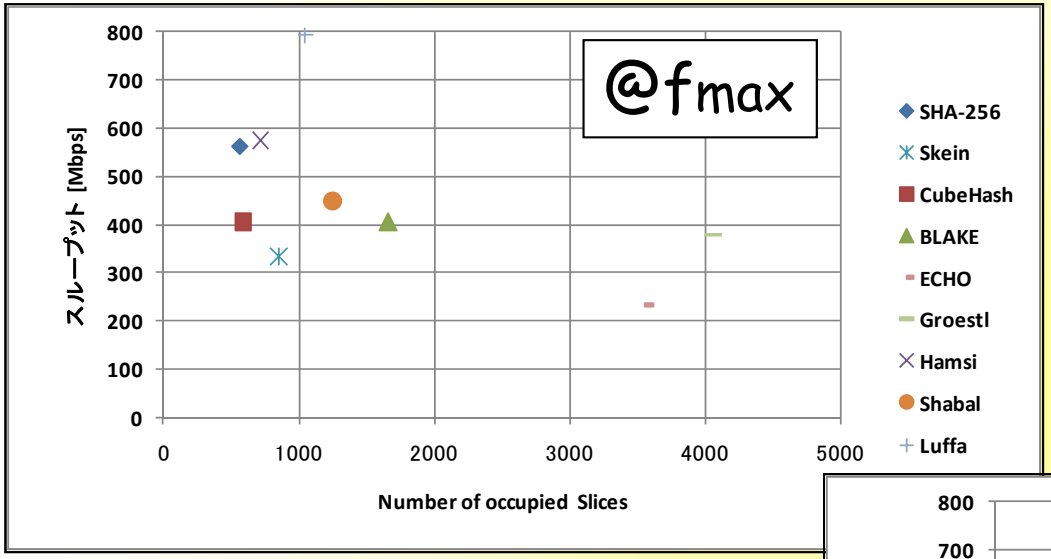
ロ ショートメッセージではレイテンシィ

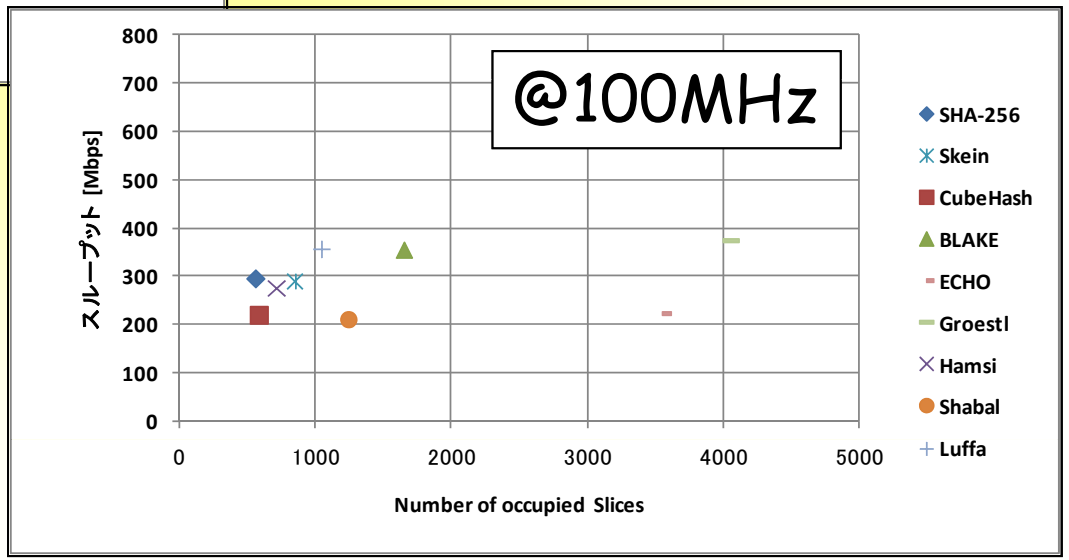
$$L = \frac{I}{f_{max}}$$

【ｸﾞﾚｲﾊｳﾝﾄﾞ】100m走 4~5秒

SHA-3候補評価結果(一部)

ロ コスト vs スループット





Open Questions

- プラットフォーム
  - FPGAの評価結果 ⇒ ASICの実装性見積もり?
  - インタフェースの違い
  - 消費電力評価
    - RFID応用
    - バッテリー駆動システム (低エネルギー)
- 評価基準
  - f_{max} での評価は重要?
  - Throughput/gate が全て？
    - 多少コストが高くても高スループット優先
    - 多少スループットが悪くても低コスト優先