軽量暗号に対するサイドチャネル攻撃

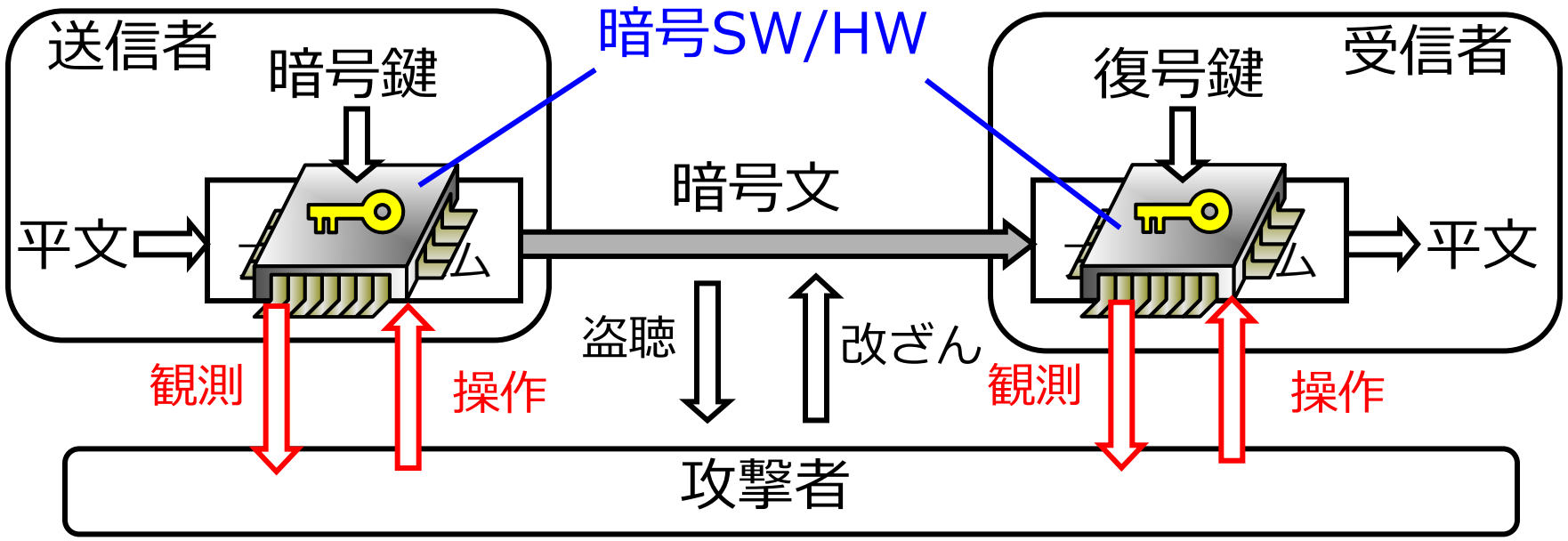
東北大学　電気通信研究所　本間尚文

本日の内容

- サイドチャネル攻撃
- 軽量暗号に対するサイドチャネル攻撃
  - ASCONへの攻撃
  - 典型的な対策
  - 注意すべき攻撃
- まとめ・今後の課題

暗号ソフトウェア・ハードウェアへの物理攻撃

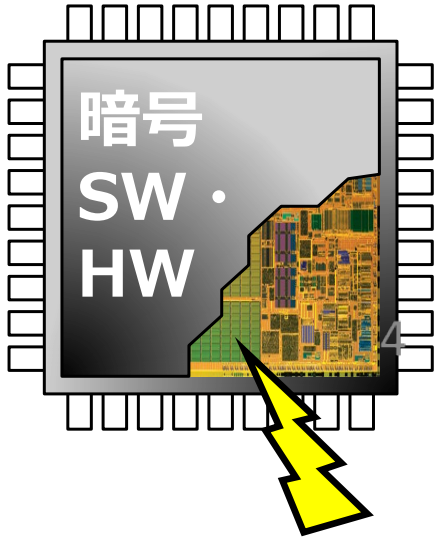
- 暗号SW/HWへの物理的な観測・操作に基づく攻撃
- 暗号アルゴリズム設計段階で考慮できない攻撃：
  認証を得たアルゴリズムでも解読される可能性



さまざまな物理攻撃

■ 破壊攻撃と非破壊攻撃

平文
暗号文



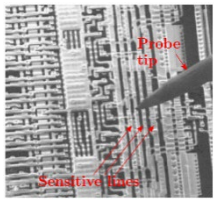
非正規入力
(フォールト攻撃)

周波数・電圧変動
クロックグリッチ
電磁波干渉

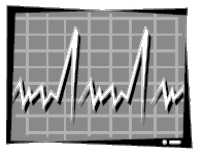
**能動的サイド
チャネル攻撃**

破壊攻撃

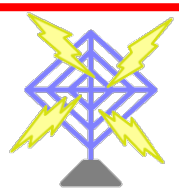
回路パターン解析
配線プロービング
レーザー照射・FIB



非破壊攻撃



消費電力



放射電磁波

演算時間

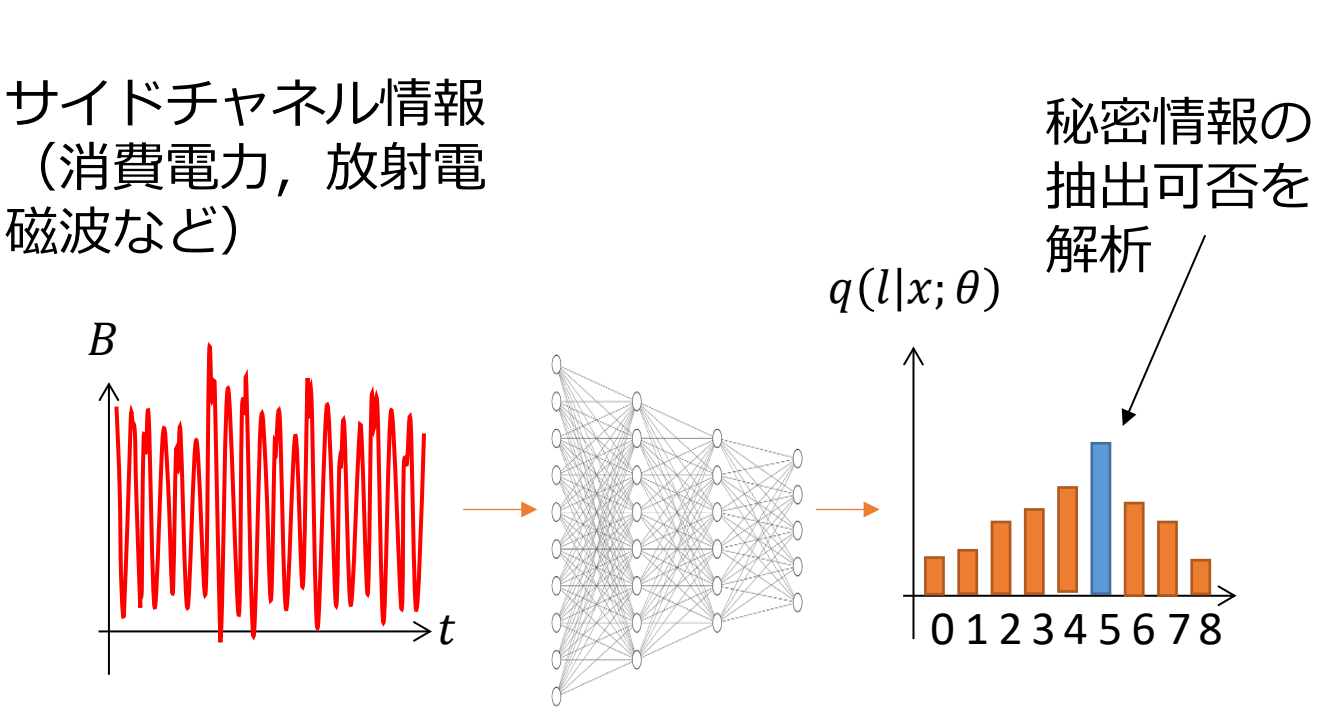
受動的サイドチャネル攻撃

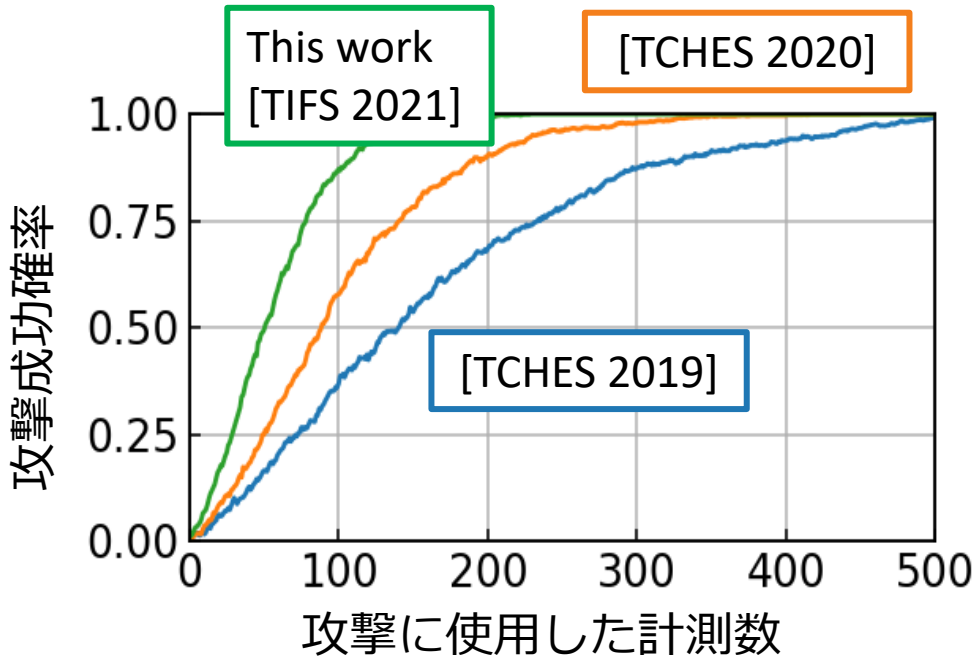
代表的なサイドチャネル攻撃

- タイミング攻撃：実行時間のデータ依存性を利用
  - 物理的計測不要な遠隔からの攻撃の可能性
- 電力・電磁波解析攻撃：電力（放射電磁波）のデータ依存性を利用
  - 単純解析（SPA, SEMA），差分解析（DPA, DEMA）
- プロファイリング攻撃：SC情報の傾向を事前にプロファイリング
  - DL-SCA (Deep-Learning Side-Channel Analysis)
- フォールト攻撃：一時的な故障を生じさせてその挙動を利用

機械学習によるサイドチャネル攻撃

- 機械学習を用いたサイドチャネル攻撃の脅威が顕在化
  - 従来対策により抑制された情報漏えいへの適用可能性
  - 深層学習に基づくサイドチャネル攻撃（DL-SCA）



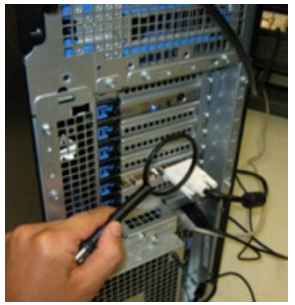


対策済みAESソフトウェアへの適用

サイドチャネル攻撃の事例

- ニューヨークやロンドンなどの地下鉄，オランダで使用されていたICカードの鍵をサイドチャネル攻撃で取得
  - Breaking Mifare DESFire MF3ICD40（CHES 2011）

- Intel AES-NI命令セットにサイドチャネル攻撃に対する脆弱性
  - Defend encryption systems against side-channel attacks　(EDN Network 2015)



- マイクロアーキテクチャに存在する機能とサイドチャネル攻撃を組み合わせた攻撃（USENIX Security 2018, S&P 2019）
  - Spectre / Meltdown：Intel製・AMD製のプロセッサに影響

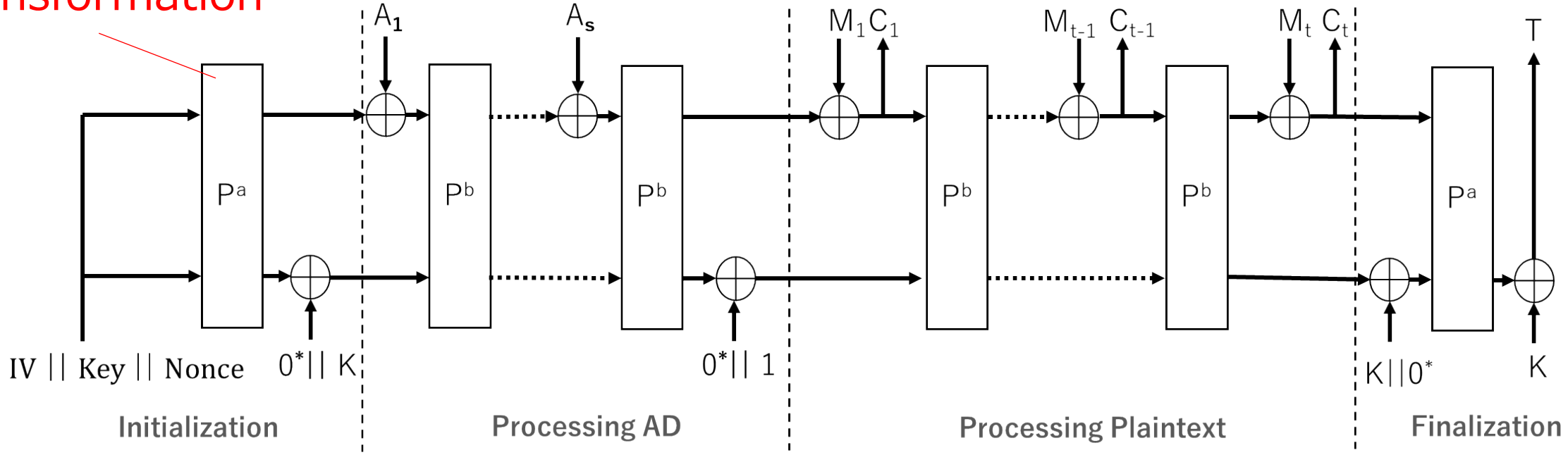
SPECTRE　MELTDOWN

- Google Titan セキュリティキーを機械学習サイドチャネル攻撃で復元 (USENIX Security 2021)

軽量暗号に対するサイドチャネル攻撃

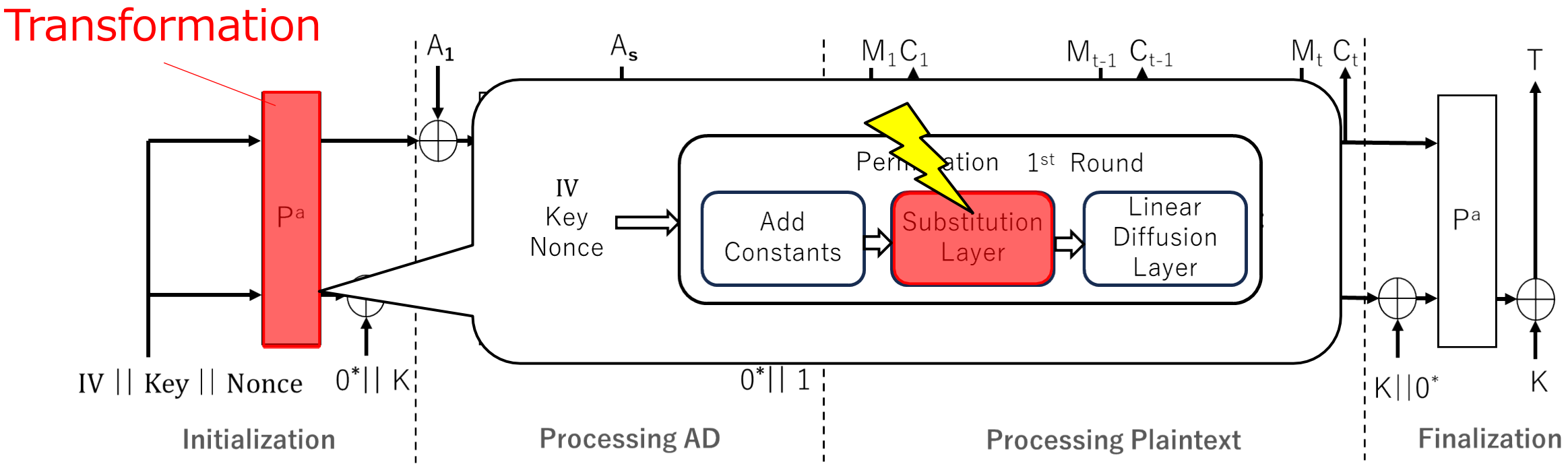
- 軽量暗号にもサイドチャネル攻撃の脅威あり
  - PermutationベースのASCONも攻撃可能
- 典型的な対策
- 軽量暗号でよく利用されるアーキテクチャ特有の漏えい

ASCON(-AEAD)の構成



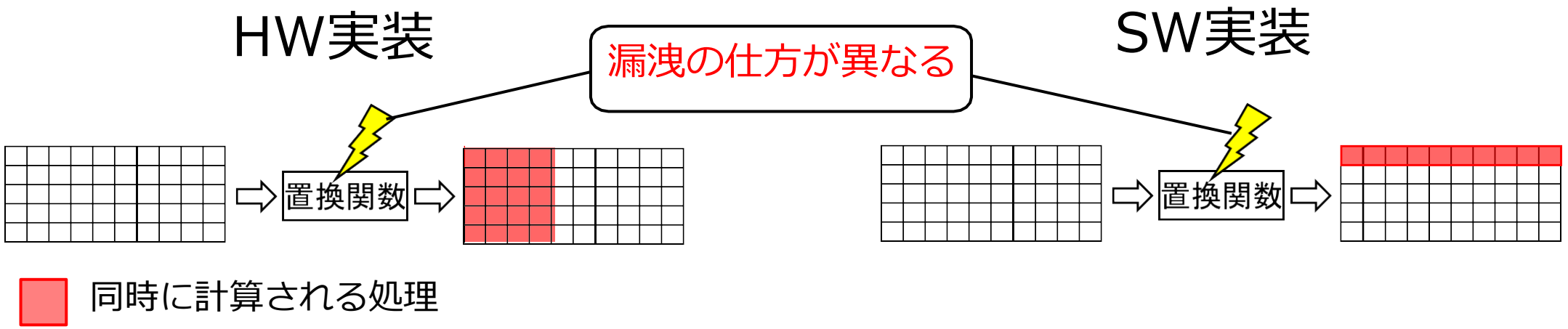
- 暗号学的置換に基づく軽量認証暗号
  - Transformation処理は大きく3つの処理から構成
- 320bitの内部状態をもつ
  - IV 64ビット, Key 128ビット, Nonce 128ビット

ASCONに対するサイドチャネル攻撃



- ASCONに対する相関電力解析攻撃
  - ハードウェア実装への攻撃 [Samwel, et. al., 2017]
  - ソフトウェア実装への攻撃 [Batina, et. al., 2022]

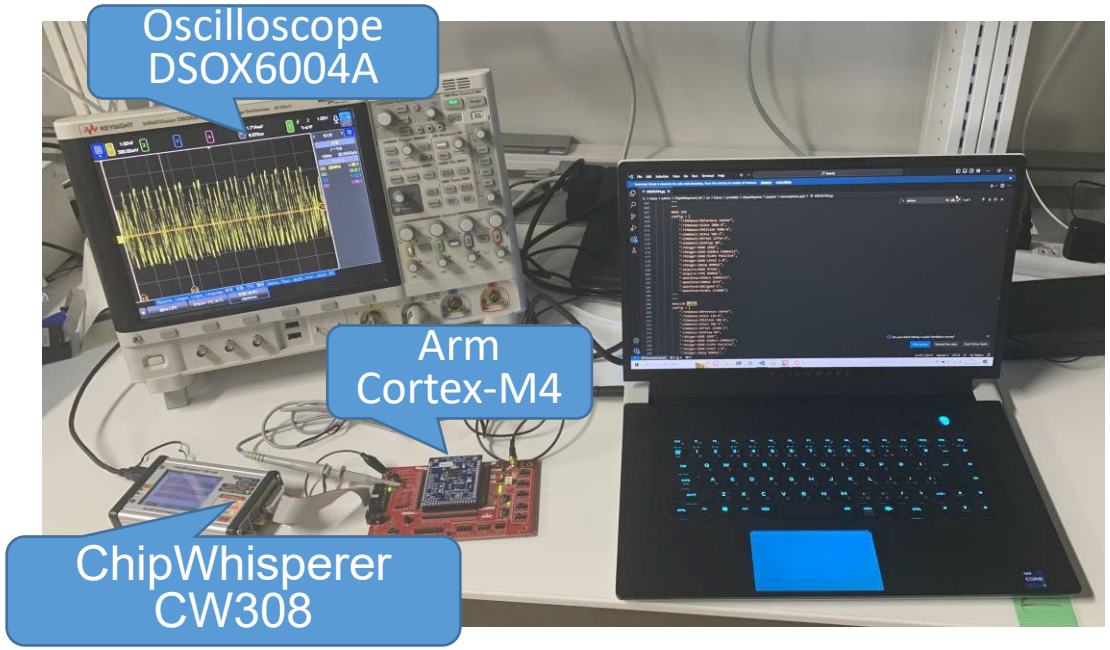
HW実装とSW実装の違い

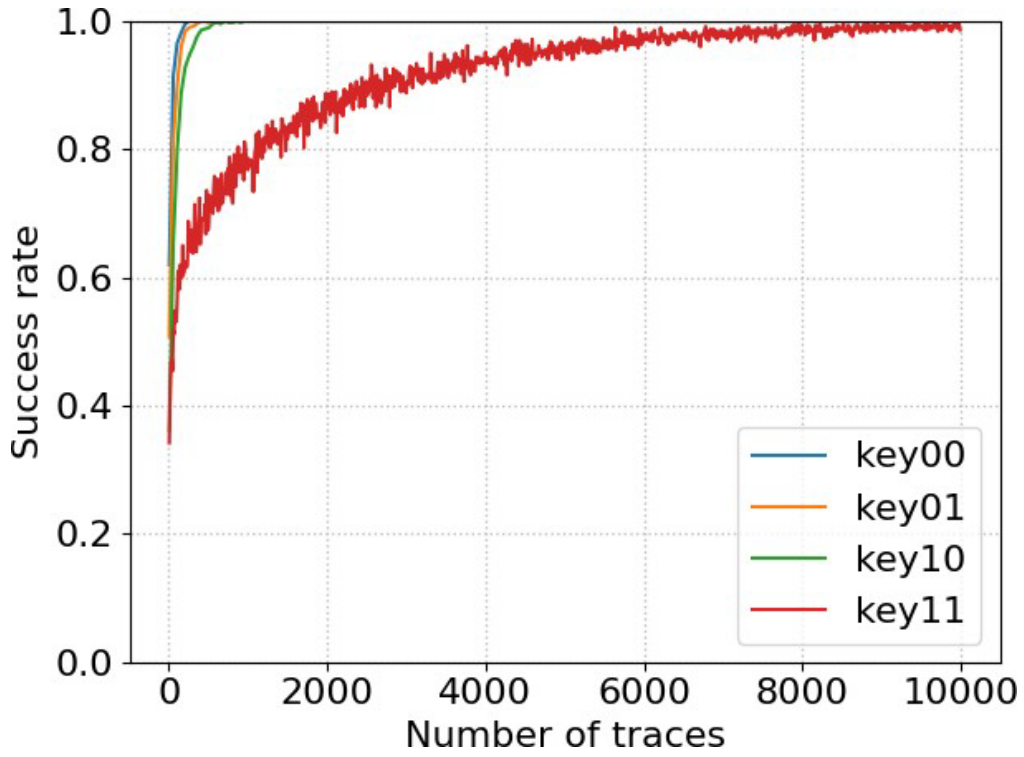


- HW実装：5ビットS-box単位で並列演算
  - アルゴリズムノイズ大：900K計測程度で攻撃成功（FPGA Spartan-6）
- SW実装：プロセッサの語長に合わせて演算
  - アルゴリズムノイズ小：100K計測程度で攻撃成功（Arm Cortex-V6）

攻撃の効率化

- 攻撃時に利用する選択関数を変更 [Iwasa, et. al., 2023]
  - SW実装に対して10K程度でも攻撃成功



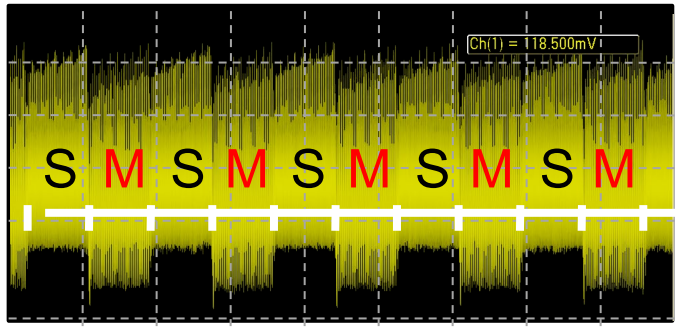


軽量暗号に対するサイドチャネル攻撃

- 軽量暗号にもサイドチャネル攻撃の脅威あり
  - PermutationベースのASCONも攻撃可能
- 典型的な対策
- 軽量暗号でよく利用されるアーキテクチャ特有の漏えい

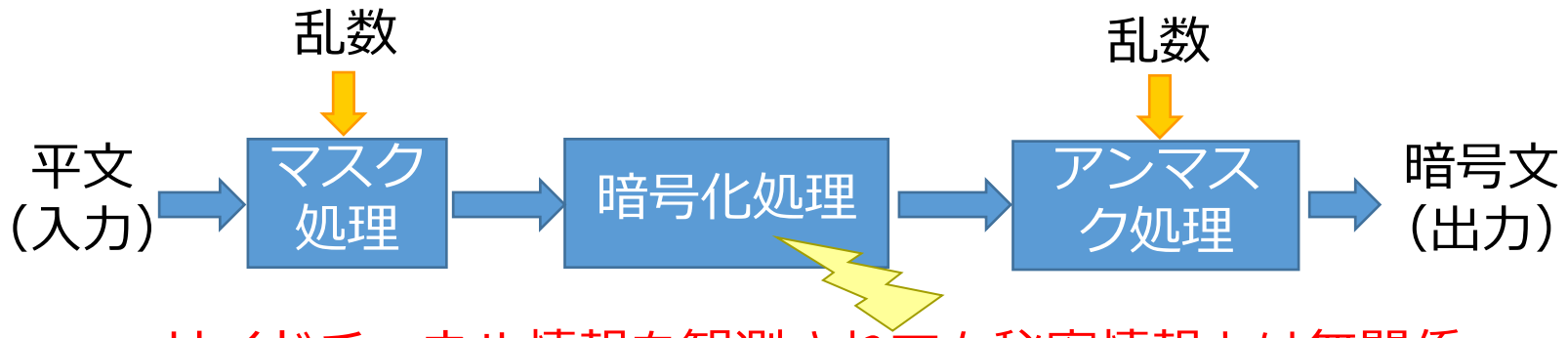
サイドチャネル攻撃対策

- ハイディング：SC情報を処理に依らず一定化（時間・計算量）
  - コンスタントタイム設計が基本
  - 主なタイミング漏えい源
    - 秘密情報に依存した条件分岐
    - メモリアクセス：入力による遅延の変化
    - 秘密情報を入力する演算：入力による演算時間差



対策を施した電力波形の例

- マスキング（秘密分散）：乱数による中間値の変換



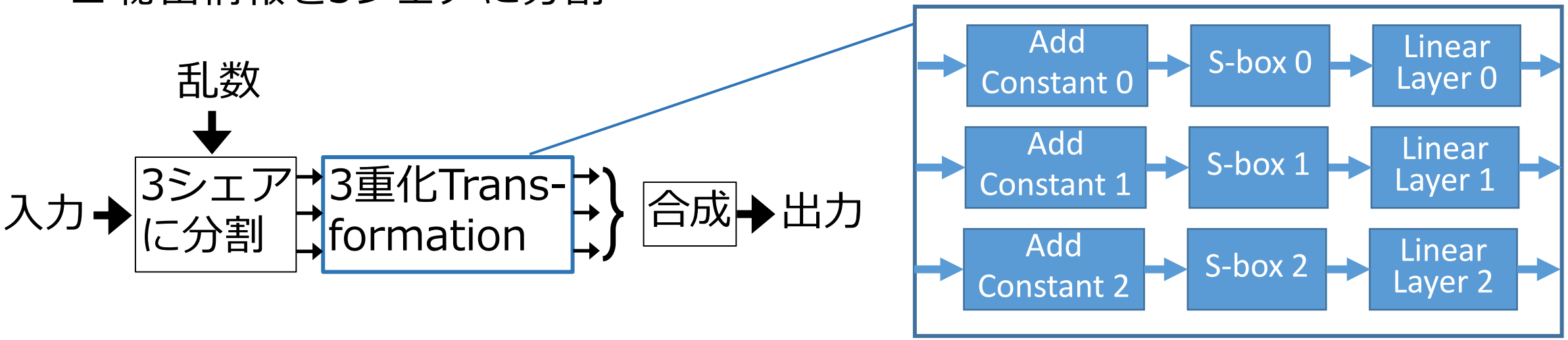
マスキング対策の例

- Threshold Implementation (TI)など
  - 秘密情報を複数の”シェア”に分割

$$a = a_1 + a_2 \cdots + a_i \cdots + a_n$$

a: 秘密情報, a_i: シェア

- TIに基づくASCONの構成 [Kandi et. al., 2023]
  - 秘密情報を3シェアに分割



3シェアによるTransformation関数

対策済みASCONのオーバーヘッド

- 未対策と比べて速度増はわずか（1.1倍程度）
- 面積は4倍程度増加

(a) ASIC (STM 130nm)

Design	Cells	Area (μm^2)	Critical Path (ps)	Power (nW)	
				Leakage	Dynamic
Encryption + Tag generation	5426	73803	8595	0	827861.117
Decryption + Tag verification	5025	71873	8586	0	644860.995
Encryption + Tag generation TI	20364	273857	10001	0	3522435.310
Decryption + Tag verification TI	20191	274688	9981	0	3647338.988

(b) FPGA (Kintex-7)

Design	LUT	F/F	Max. Freq. (MHz)
Encryption + Tag generation	944	734	181
Decryption + Tag verification	1058	735	181
Encryption + Tag generation TI	3977	2174	166
Decryption + Tag verification TI	3795	2179	156

軽量暗号の優位性

回路規模	• 軽量暗号とAESの差(数kgate)は，50μm角クラスの 小さなチップや180nmなど古いプロセスではcriticalで，暗号機能の搭載可否に影響を与えうる
消費電力量	• 回路規模が小さいほど消費電力(量)は小さくなる傾向． 軽量暗号により消費電力(量)に関する設計条件を緩和できる効果が期待できる
レイテンシ	• AESの2倍の応答速度をおよそ1/10の回路規模で実現できる軽量暗号が存在（20kgateで10ns以下での演算が可能）．産業向け I/Oデバイス制御などμsオーダーのリアルタイム性が求められる用途で活用可能
メモリサイズ	• AESのおよそ1/4のROMサイズで実装可能な軽量暗号が存在．軽量暗号なら追加できるケースやチップ単価を下げられるケースあり

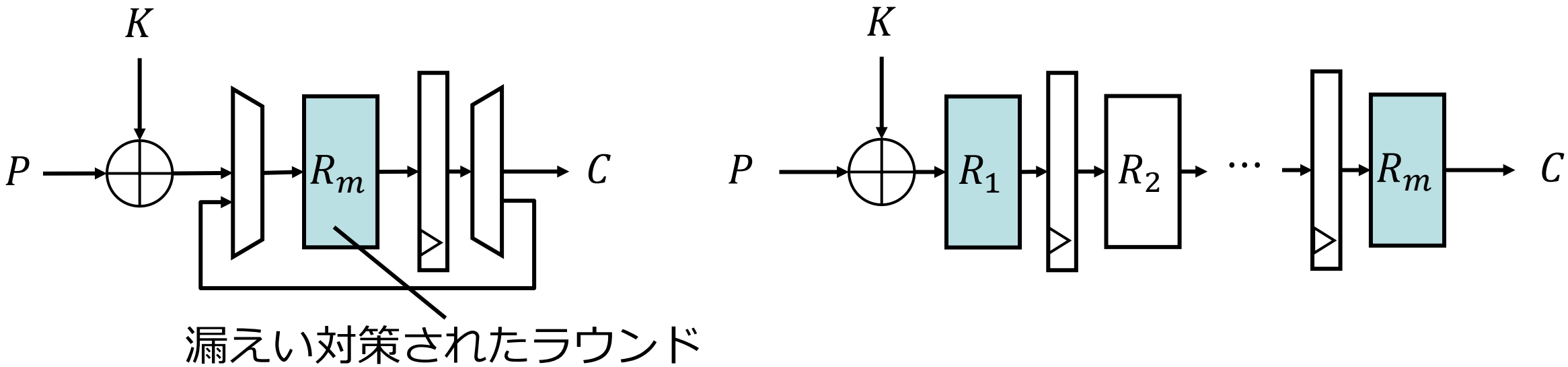
＋サイドチャネル攻撃対策が容易といった軸を足すと優位性が明確に

軽量暗号に対するサイドチャネル攻撃

- 軽量暗号にもサイドチャネル攻撃の脅威あり
  - PermutationベースのASCONも攻撃可能
- 典型的な対策
- 軽量暗号でよく利用されるアーキテクチャ特有の漏えい

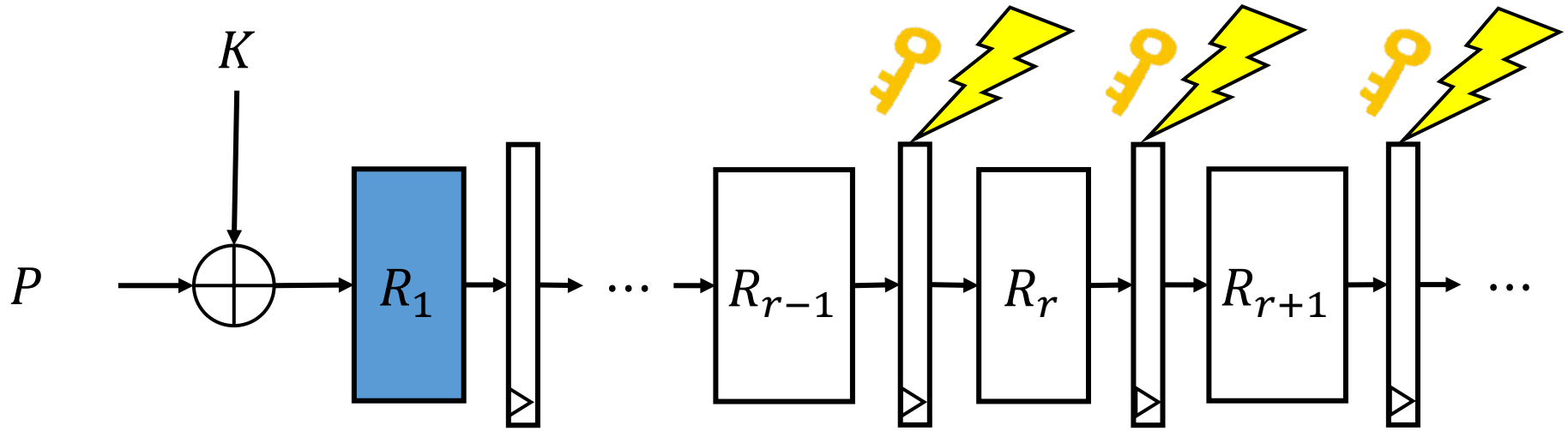
軽量暗号向けアーキテクチャ特有の漏えい

- アンロールドアーキテクチャ
  - 低遅延・高スループットを指向して暗号のラウンドを展開
- サイドチャネル攻撃対策
  - ラウンドアーキテクチャは単一のラウンドのみ対策すればよい
  - アンロールドの場合は第1ラウンド（と最終ラウンド）のみ対策すればよい？



アンロールド実装のSCAの研究動向

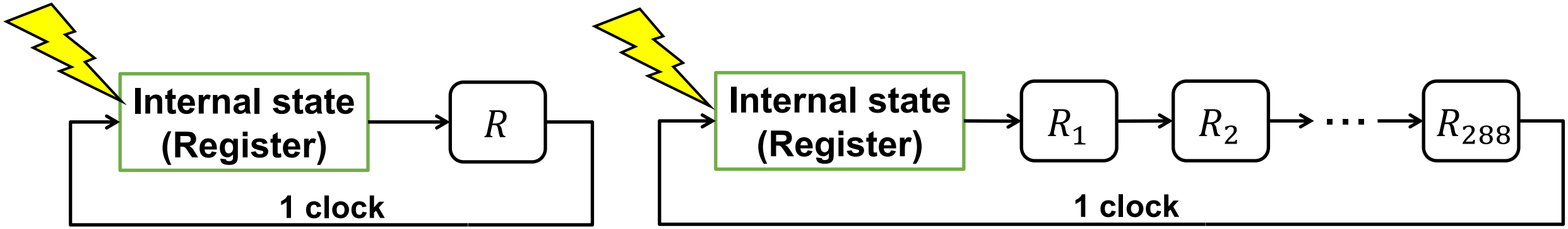
- 中間ラウンドのサイドチャネル情報からも攻撃可能
  - データが完全に攪拌されないため出力に偏りが生じる
  - PRINCEアンロールド実装の第3ラウンドからの漏えいで攻撃成功
    [Yli-Mäyry, et. al., 2020]
  - AESアンロールド実装の第3ラウンドからの漏えいで攻撃成功
    [Higashi, et. al., 2023]



ストリーム暗号のアンロールド実装

- Trivium: ISO/IEC 29192-3標準ストリーム暗号
  - ラウンド関数は少数の論理ゲートで構成
  - CRYPTREC暗号技術ガイドライン（軽量暗号）にも掲載
  - 288ラウンドアンロールド実装が最も高エネルギー効率 [Caforio, et. al., 2021]

- 多ラウンドで攪拌された結果がレジスタに格納されるため従来と比べて攻撃困難とみなされていた



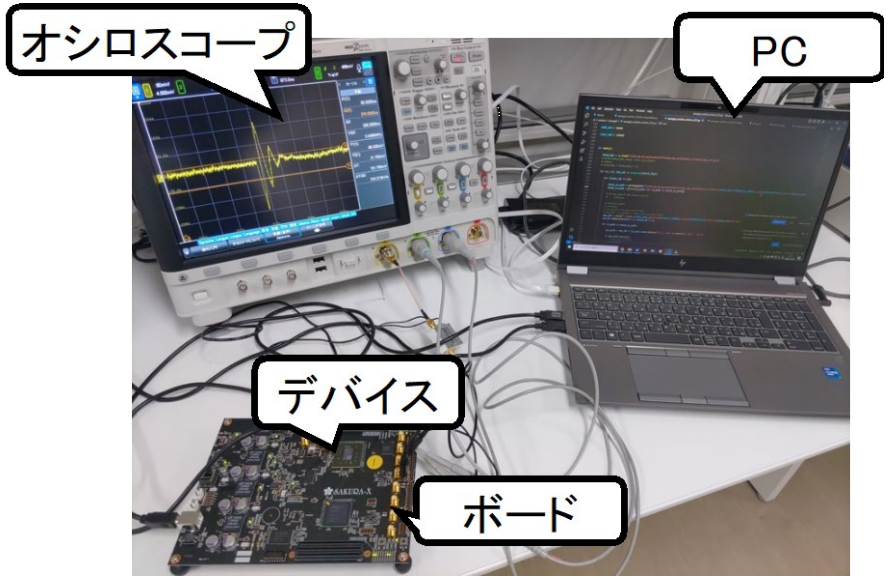
ラウンドベース実装　　288ラウンドアンロールド実装

アンロールド実装されたTriviumへのSCA

- Trivium後段ラウンドへの攻撃 [Kobayashi, et. al., 2023]
  - 変数の分離と鍵の方程式次数の削減手法の適用

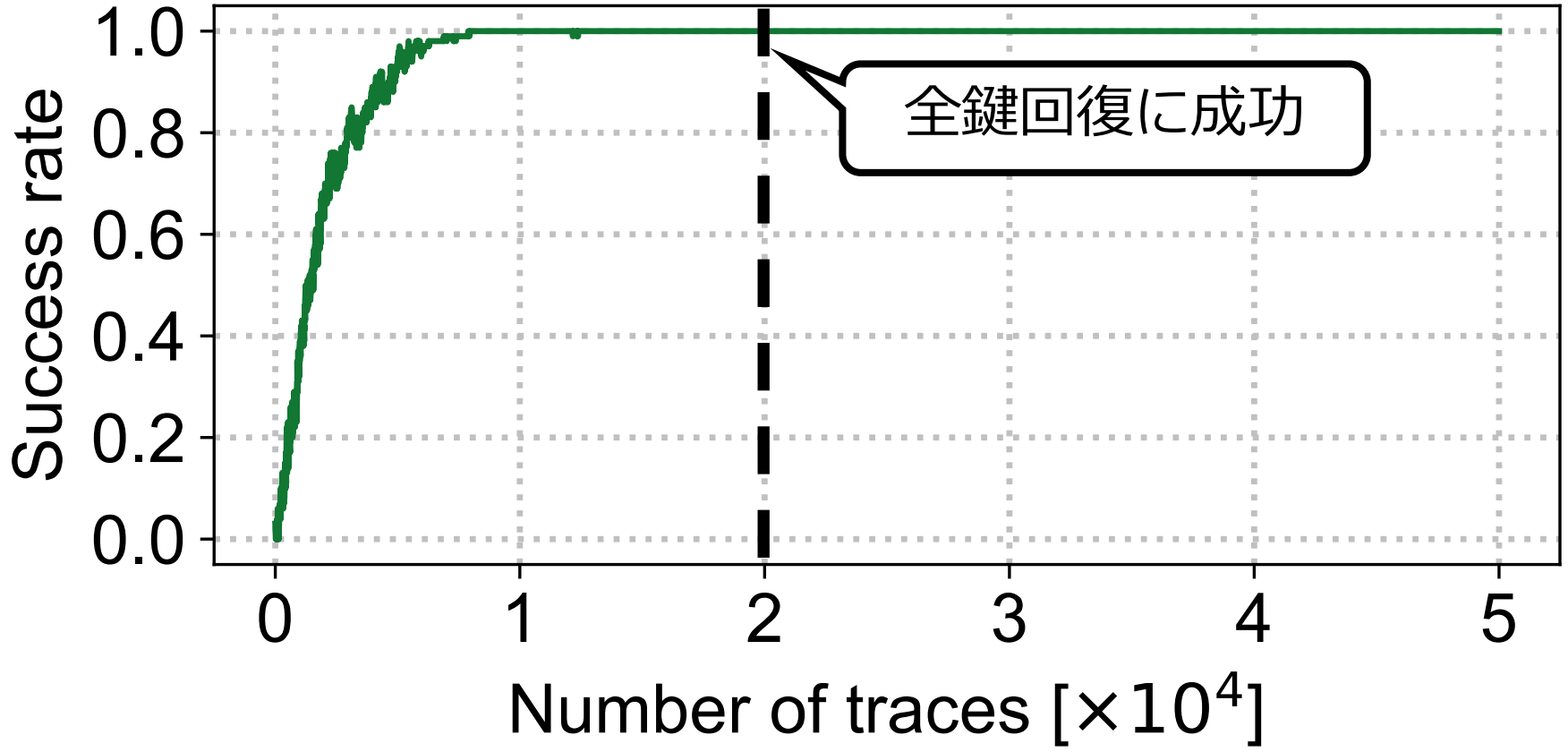
- 288ラウンドアンロールド実装への攻撃の可否を評価
  - FPGA実装が動作中の消費電力情報を攻撃に利用

対象デバイス	Xilinx Kintex-7
ボード	SAKURA-X
オシロスコープ	DSOX 6004A 1G samples/s
取得波形数	700,000



波形取得環境

288ラウンドアンロールド実装へのSCA



288ラウンドアンロールド実装に対しても鍵の高次方程式を一次方程式に変換することで鍵回復に成功

[Kobayashi et. al, 2023]

まとめ・今後の課題

- サイドチャネル攻撃耐性（耐タンパー性）は軽量暗号でも重要
  - ASCON等のPermutationベースでも現実的脅威
- 対策のコストの観点では軽量暗号に優位性
  - 何かの指標＋サイドチャネル攻撃対策容易性で優位性がより明確に
- 軽量暗号向きのアーキテクチャ特有の漏えいあり
  - 適切なラウンド数分の対策が必要
- 今後の課題
  - SCAの高度化への対応
    - 従来有効であった対策であっても破られる可能性
  - サイドチャネル情報漏えいを前提としたレジリエンス性の獲得