〈一般研究課題〉　携帯端末における認証暗号の実装性能評価

助 成 研 究 者　名古屋大学　　岩田　哲

携帯端末における認証暗号の実装性能評価

岩田　哲
(名古屋大学)

Evaluation of Implementation Characteristics of Authenticated Encryption on Mobile Devices

Tetsu Iwata
(Nagoya University)

Abstract：

An authenticated encryption scheme is a symmetric key cryptographic primitive that simultaneously provides confidentiality and integrity of input data. The scheme has wide applications, and some of them are heavily used in our daily lives. CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness), initiated in 2014, categorizes the use case of authenticated encryption schemes into Use Case 1 (lightweight applications, resource constrained environments), Use Case 2 (high-performance applications), and Use Case 3 (defense in depth). The project was completed with the announcement of the final portfolio in February, 2019. In this study, we focus on the six CAESAR 3rd round candidates in Use Case 1. These are CLOC, SILC, Jambu, Ketje, Ascon, and ACORN. We evaluate the implementation characteristic of these schemes on real mobile devices. Given that mobile devices are equipped with a battery, we focus on the energy consumption of these schemes. We use five Android mobile devices to see their energy consumption. We implement six authenticated encryption schemes based on the reference code provided by the designers on five mobile devises, and we use both hardware and software tools to obtain the figures. As a result, our implementation figures show that CLOC, SILC, Jambu, and Ascon perform better with this order, followed by Ketje or ACORN depending on the input length.

1. はじめに

認証暗号技術は，コンピュータやネットワーク上のデータの秘匿と認証を同時に行うための共通鍵暗号技術であり，これまでに数多くの方式が設計され，そのいくつは実際に身の回りの様々な場面で活用されている．ネットワークとコンピュータの応用範囲の拡大やIoTデバイスの普及に従い，その活用範囲はますます拡大しており，安全であり，なおかつ優れた実装性能を有する認証暗号技術の開発が望まれている．

現在広く利用されているGCM(Galois/Counter Mode)[1]やCCM(Counter with CBC-MAC)[2]といった方式には安全性と効率の面で改善可能であることが知られている．2014年に始められたCAESAR(Competition for Authenticated Encryption: Security, Applicability, and Robustness)[3]は，GCMに代わる優れた認証暗号技術を選定するための国際的な公募プロジェクトであり，認証暗号技術の研究，開発は活発に進められている．CAESARでは認証暗号の利用環境に応じて，Use Case 1(軽量アプリケーション)，Use Case 2(高性能アプリケーション)，Use Case 3(高安全性を必要とするアプリケーション)の3つのカテゴリを設け，それぞれについて推奨方式を選定した．2019年2月に最終結果がアナウンスされ，Use Case 1ではAsconとACORNが，Use Case 2ではAEGIS-128とOCBが，Use Case 3ではDeoxys-IIとCOLMが選定されている．CAESARに続き，米国商務省標準技術局NISTは2019年2月より次世代軽量認証暗号技術の公募を実施しており[4]，今後4年から5年をかけて米国政府標準方式が選定される予定である．CAESARのUse Case 1に相当する軽量認証暗号を対象としており，これは計算資源の乏しい環境での使用に適した方式であり，IoTデバイスをはじめとした環境で使用されることを想定している．

本研究では，CAESARに応募された認証暗号技術を取り上げ，それらを携帯端末上に実装し，性能評価を実機により行う．IoT時代の到来を見据え，軽量認証暗号技術は安心・安全な情報環境を構築するための有効な解決策であることが期待されている．一方で，計算資源やメモリの乏しいデバイスにおける性能評価は重要な課題であり，実際にこれまでにマイコン上でのCAESAR候補方式の性能評価[5]や軽量ブロック暗号の評価[6]，実装に必要なハードウェアゲート数とった指標[7]において評価が行われてきた．また，ソフトウェア速度を計測するベンチマーク環境eBACS(ECRYPT Benchmarking of Cryptographic Systems)[8]や，ハードウェア性能を評価するプラットフォームATHENa(Automated Tools for Hardware EvaluatioN)[9]が整備されている．

本研究では，CAESARの第3ラウンド候補のうち，軽量アプリケーション向けに提案されている方式を取り上げ，それらを携帯端末上に実装し，その性能を実機により評価する．本研究で考える方式はCLOC，SILC，JAMBU，Ketje，Ascon，ACORNの6方式であり，携帯端末として5台のAndroid端末を用意する．一般に軽量暗号の要件として，回路規模，消費エネルギー，レイテンシ，メモリサイズの4点が挙げられる．2点目の消費エネルギーは，省エネの観点から重要であると同時に，限られたバッテリで動作する携帯端末において重要だと考えられることから，本研究ではこれら4つの要件のうち消費エネルギーに焦点を絞る．先に挙げた6方式を5台の端末に実装し，ある一定の長さの入力を処理する．このときに入力1バイト当たりの処理にかかる消費エネルギー(J/Byte)を算出し，これら6方式の比較を行う．測定はバッテリがとりはずせる端末ではハードウェアの計測機器によりバッテリからの電流を計測することで，暗号処理にかかる消費エネルギーを算出する．バッテリがとりはずせない端末ではOSの機能や汎用アプリを利用することとし，ソ

フトウェアによる算出を行う．

2. 対象方式，実装端末，および実験方法

2.1 対象方式

対象方式として，CAESARの第3ラウンド候補方式であり，カテゴリUse Case 1(軽量アプリケーション)向けとして提案されている下記の6方式を考える．

- CLOC [10]：ブロック暗号に基づく方式であり，証明可能安全性を有する．ブロック暗号の呼び出し回数を削減するよう設計されており，短い入力長に対して効率的に動作する．
- SILC [10]：CLOCと同様の設計方針であり，ブロック暗号に基づく方式であるが，よりハードウェアでの実装規模が小さくなるよう条件分岐を少なくしている．ブロック暗号呼び出し回数はCLOCよりも多くなる．
- JAMBU [11]：ブロック暗号に基づく方式である．CLOC/SILCよりも軽量環境に適したブロック暗号を採用しており，必要メモリサイズの観点からの最適化を行っている．
- Ketje [12]：暗号学的置換に基づく設計であり，Sponge構造と呼ばれる設計手法を採用している．メモリサイズが小さくて済み，ハードウェアでの実装に適している．
- Ascon [13]：Ketjeと同様に暗号学的置換とSponge構造に基づく設計であり，ハードウェアでの小型実装に適している．
- ACORN [14]：Use Case 1では唯一，ストリーム暗号に基づく設計であり，内部状態以外の関数が簡素であり，ソフトウェアでの高速実装，ハードウェアでの小型実装に適している．初期処理はコストがかかる．

CAESARでは設計者がいくつかのパラメータを設定することが許されており，本研究では設計者が第一優先パラメータとしたパラメータを用いて実装を行う．また，CAESARでは設計者がreference実装を提出することが要求されており，これをもとに計測を行う．

2.2 実装端末

本研究ではAndroidをOSとして使用している機種を用いることとし，端末の選定には主に年代とCPUメーカー違いを考慮した．最近の機種としてHuawei P20とZenFone 5z，古い機種としてXperia E dualとGalaxy S III，中間の機種としてZTE Blade L110の計5機種を用いる．それぞれの発売時期，チップセット，CPU，RAM/ROMサイズをまとめる．

- Huawei P20：2018年3月，Hisilicon Kirin 970，4x2.36 GHz Cortex-A73 + 4x1.8 GHz Cortex-A53，4GB/128GB
- ZenFone 5z：2018年6月，Qualcomm SDM845 Snapdragon 845，4x2.7 GHz Kryo 385 Gold + 4x1.7 GHz Kryo 385 Silver，6GB/128GB
- Xperia E dual：2013年1月，Qualcomm MSM7227A Snapdragon S1，1.0 GHz Cortex-A5，512MB/4GB
- Galaxy S III：2012年6月，Qualcomm MSM8960 Snapdragon S4 Plus，2x1.5 GHz Krait，2GB/32GB
- ZTE Blade L110：2016年7月，Spreadtrum SC7731G，4x1.3 GHz Cortex-A7，512MB/

4GB

以降それぞれ端末1から端末5と呼ぶこととする．

2.3 実験方法

測定対象の各方式は認証暗号技術であり，秘密鍵，付加データ，平文を入力とし，暗号文とタグを出力する．秘密鍵は固定長のデータである．付加データは暗号化はせず，認証のみを行うデータであり，可変長である．これはヘッダとして利用されることを想定している．平文は暗号化も認証も行うデータであり，これも可変長である．出力の暗号文は一般に平文と同じバイト数の可変長データであり，タグは認証のための固定長データである．バイト当たりの消費エネルギーを計測する際，バイト長の短い付加データ，平文に対しては初期処理にかかる影響が無視できず，バイト長の長い付加データ，平文に対しては初期処理にかかるコストを無視できる漸近的な性能が評価できると期待される．実際，CAESARでは各提案方式のソフトウェア実行速度を計測するためのベンチマーク環境であるeBACSが利用されており，様々な入力長の速度を計測できる環境が整備されている．eBACSにおける暗号化時の付加データ，平文のバイト長(あるいは復号時の付加データ，暗号文のバイト長)は0バイトから2048バイトまで計9通りの組み合わせを考えている．本研究ではこれを参考にし，暗号化時の付加データ，平文のバイト長(あるいは復号時の付加データ，暗号文のバイト長)をZero，Short，Medium，Longの4通りを計測することとした．付加データ，平文，暗号文は同じバイト数であるとし，Zeroは0バイト，Shortは64バイト，Mediumは1536バイトである．Longは65536バイトの際の計測値と64バイトの計測値との差を算出する．これは，eBACSと同様に，初期処理の影響が無視できることを疑似的に再現するものである．

認証暗号6方式，端末5台，入力サイズ4通りそれぞれについて暗号化，復号に要するバイト当たりの消費エネルギーを計測する．計240通りの組み合わせがあり，これらに加えて，各端末でスリープ状態を計測する．各組合せに対して一定回数の入力を与え消費エネルギーを算出し，それらの平均値を計算する．

計測方法は2通りあり，バッテリが取り外せる端末3,4,5ではトライグル社のモバイル電力測定器であるTRYGLE POWER BENCH [15]を用いる．これは，バッテリと端末本体の間に挿入する機器であり，バッテリから流れる電流をリアルタイムに計測する．このツールによる測定の画面の例を図1に示す．SILC-ENC-0は0バイト入力時のSILCの暗号化を指しており，図1はこの電流波形を示している．同時に，SILCの実行をスリープ関数に置き換えた電流を示しており，これらの差から暗号化処理に必要な消費エ

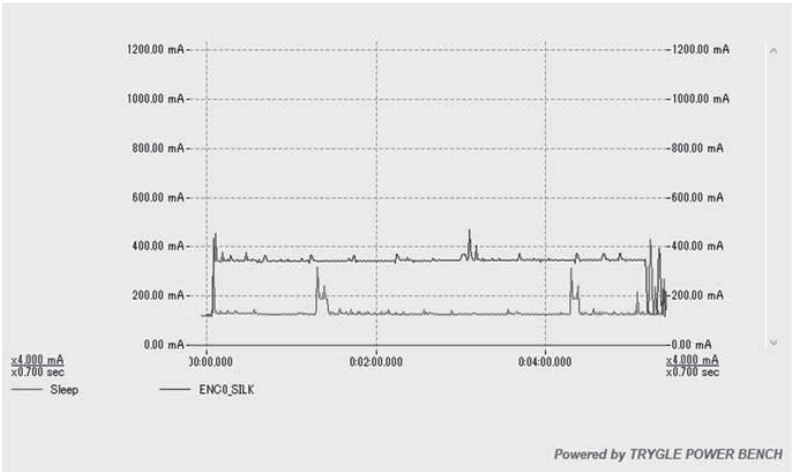

図1. 端末4によるSILC-ENC-0とSLEEPのベンチマークアプリ実行時の電流波形の例

ネルギーを算出する．

端末1,2ではバッテリの取り外しができず，ソフトウェアによる計測を行う．Android 8.0からはOSで消費エネルギーを観測できるようになっている．また一般に電力測定用にアプリがあり，端末1ではAccuBattery [16]というアプリを利用し，端末2ではOSの設定から直接読み取る．AccuBatteryではハードウェア，ソフトウェアの区別なく合算されて表示され，アプリの消費電力には画面のバックライトなどの定常的な消費電力が含まれている．このため，暗号化処理を行わない場合の定常的な消費電力を測定し，暗号処理を実装したアプリとの差を取ることで，暗号処理の消費エネルギーを算出する．OSから直接読み取る場合は，CPUやGPUによる電池消費量を読み取ることができ，これを用いる．それぞれ，得られたデータから1バイト当たりの処理に必要な消費エネルギー(J/Byte)を算出する．

3. 実験結果

3.1 実験結果

図2～図6に得られた消費エネルギーのデータを示す．それぞれの図は端末1から5に対応し，各図は縦軸が消費エネルギー(nJ/Byte)を対数で示しており，左側に復号時，右側に暗号化時のデータが示されている．各グラフは左から入力長Short，Medium，Longの順で並んでおり，各入力長に対して左からCLOC，SILC，Jambu，Ketje，Ascon，ACORNの順で並んでいる．入力長0の場合はバイト当たりの消費エネルギーは算出できず，示していない．

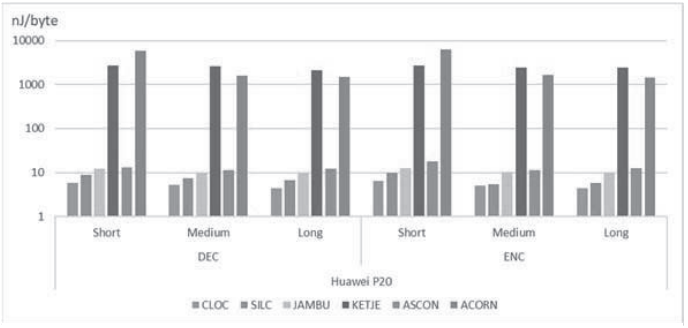

図2. 端末1による測定結果

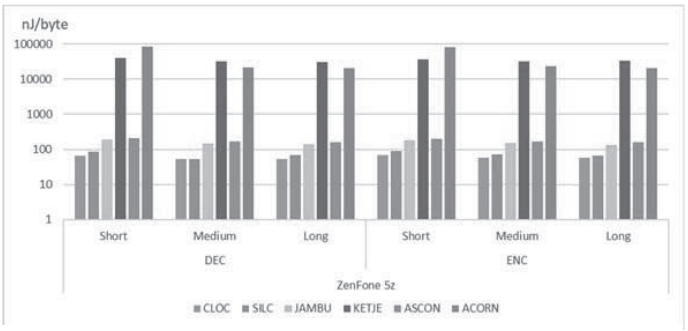

図3. 端末2による測定結果

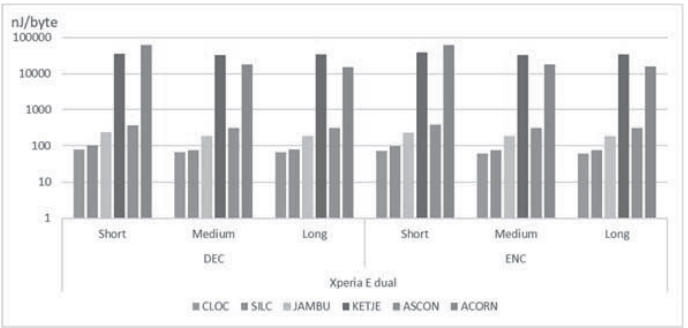

図4. 端末3による測定結果

3.2 考察

図2～6のいずれのグラフからもブロック暗号に基づくCLOC，SILC，Jambuの消費エネルギーが小さく，それに次いでASCONが続く．KetjeとACORNはこれらのグラフからは，CLOC，SILC，Jambu，ASCONに比べて消費エネルギーが大きい結果となった．

消費エネルギーの小さい順にCLOC，SILC，Jambu，Asconとなっており，KetjeとACORNはShort

とMedium/Longで順位が入れ替わる．これはACORNの初期処理のコストが大きく，入力長が長くなるにしたがってその影響が小さくなるためだと考えられる．ブロック暗号に基づく方式の結果が総じて良いのはreference実装の時点である程度の性能が出る実装になっているのに対して，暗号学的置換，ストリーム暗号に基づく方式では実行環境に応じた最適化の余地が大きいためだと考えられる．より精度の高い比較を行うには，使用するCPUに特化した最適実装においての比較が重要であると考えられる．

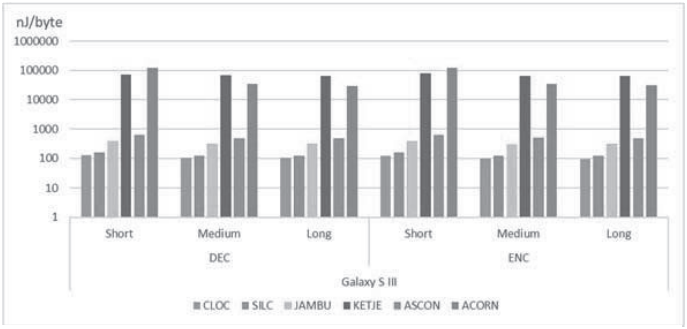

図5．端末4による測定結果

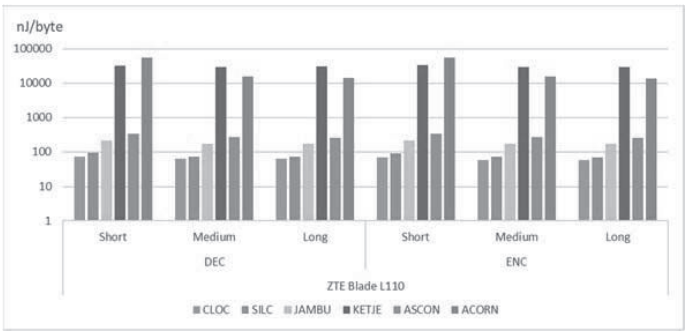

図6．端末5による測定結果

4. まとめと今後の課題

本研究では，CAESARの第3ラウンド候補方式のうち，Use Case 1(軽量アプリケーション)向けの6方式を対象とし，5台の携帯端末を用意し，実装した　各端末における各方式の1バイト当たりの消費エネルギーを算出し，6方式の順位付けを行った．Ketje，ACORNはいずれも小型ハードウェア実装においては優れた性能を示しているが，本研究の測定環境では他の方式に比べて消費エネルギーが大きいという結果になった．また，CLOC，SILC，Jambu，Asconはいずれも高い性能を示した．

今後の課題として，reference実装ではなく，実装環境に特化したコードを用いることでより精度の高い比較ができると考えられる　また，本研究ではAndroid端末を使用したが，iOSなどの他のOSでの比較が望まれる　2019年2月に公募締め切りを迎えたNIST による次世代軽量認証暗号技術の公募であるLightweight Cryptographyプロジェクトでは多数の軽量アプリケーション向け認証暗号方式が提案されており，それらの比較は重要な課題であると考えられる．

謝辞

本研究の推進にあたり，野村太志君(名古屋大学工学部)の多大な協力をいただきました．ここに記して感謝いたします．

参考文献

[1] Morris Dworkin. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007.

[2] Morris Dworkin. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST Special Publication 800-38C, 2004.
[3] Cryptographic competitions, https://competitions.cr.yp.to/caesar.html（2019年5月31日参照）
[4] NIST Lightweight Cryptography Project, https://www.nist.gov/programs-projects/lightweight-cryptography（2019年5月31日参照）
[5] 松井充，村上ユミコ．組み込みマイコンRL78での軽量共通鍵暗号のソフトウエア実装評価．SCIS 2016，3C3-6，2016.
[6] 菅原健，鈴木大輔，松井充．Bluetooth Low Energyを題材とした軽量暗号の性能評価．SCIS 2016，2C4-4，2016.
[7] Subhadeep Banik, Andrey Bogdanov, Kazuhiko Minematsu. Low-area hardware implementations of CLOC, SILC and AES-OTR. HOST 2016: 71-74.
[8] eBACS: ECRYPT Benchmarking of Cryptographic Systems, https://bench.cr.yp.to/（2019年5月31日参照）
[9] ATHENa: Automated Tools for Hardware EvaluatioN, https://cryptography.gmu.edu/athena/（2019年5月31日参照）
[10] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, Eita Kobayashi. CLOC and SILC v3. Submission to CAESAR, 2016.
[11] Hongjun Wu, Tao Huang. The JAMBU Lightweight Authentication Encryption Mode (v2.1). Submission to CAESAR, 2016.
[12] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, Ronny Van Keer. CAESAR submission: Ketje v2. Submission to CAESAR, 2016.
[13] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer. Ascon v1.2, Submission to the CAESAR Competition. Submission to CAESAR, 2016.
[14] Hongjun Wu. ACORN: A Lightweight Authenticated Cipher (v 3). Submission to CAESAR, 2016.
[15] TRYGLE POWER BENCH，スマートフォン向け電力測定ツール．http://trygle.com/product-trygle-power-bench.php（2019年5月31日参照）
[16] AccuBattery, https://www.accubatteryapp.com/（2019年5月31日参照）