自動車システムへの軽量暗号技術適用に関する現状と課題

渡辺 優平[1]　吉田 博隆[1]　山本 秀樹[1,2]

概要：近年，自動車システムにおいて，コネクテッド化が進展中である．高度な情報通信技術の利用は車載制御機器の低コスト化，利用者への利便性の向上等を促す一方で，情報システムに対する脅威が自動車システムにおいても深刻な影響を及ぼすことが明らかになってきた．このため，業界において，AES 等の標準化済みの情報技術の適用が検討されつつある．本論文では，自動車システムのセキュリティ対策について，暗号技術の観点から検討した結果を報告する．軽量暗号プリミティブとその適用について網羅的に調査検討を行い，現状の把握と整理を行った．さらに，今後，暗号技術をコアとしたセキュリティ対策を策定するための課題を抽出した．

キーワード：自動車システム，セキュリティ対策，軽量暗号プリミティブ，鍵管理，プロトコル

1. はじめに

従来，車両システム内部では，走る・曲がる・止まるを制御するために，いくつかの ECU(Electrircal Control Unit) が通信により，連携して動作していた．現在は，ドライバーの快適性向上を目的とし，自動ブレーキ等の先進運転支援（ADAS : Advanced Driver Assistant Systems）が，搭載が開始されている状況である．さらに，将来に向けて，自動運転を実現するために，セキュリティシステム設計やセキュリティ対策の実装など様々な取り組みが行われている．近年，自動車システムは，車両に関する情報や状態をヘッドユニット，TCU(Telematic Control Unit)，CGW(Central Gateway) 等の情報機器を通じて，インターネットを介し，センタサーバーに情報を吸い上げ，車両に関する情報を中央で監視することにより状況を把握し，遠隔監視や，遠隔ソフトウェア更新等のサービスを提供する，また，自動車同士（V2V），自動車とインフラ（V2I）等の通信により，自動車の制御が実現される，いわゆる，コネックティッドカーの動きが急速に展開されている状況である．

一方で，2010 年の CAN(Controller Area Network) ネットワークへの機器接続による不正ドアロック操作，スマートキー (PKES: Passive Keyless Entry and Start) への攻撃による不正エンジン始動，2015 年の Jeep における ECU ファームウェア書き換え攻撃による自動車の不正遠隔操舵などにおいて見られるように [30]，自動車システムは，セキュリティ脅威が深刻な問題となりつつある．

一般的な情報システムにおいては，セキュリティ設計が ISO/IEC15408[1] 規格として整備され，対応する国際認証スキームもコモンクライテリアとして確立しているが，自動車システムにおいては，ISO26262 [2] 規格の策定において，機能安全に関する規格が整備され，また，SAE J3061 [3] において，サイバーセキュリティと機能安全の関係性も含めて整理が行われ，セキュリティガイドラインやセキュリティ対策が整備されている状況である．

本論文では，自動車システムのサイバーセキュリティ対策の主要コンポーネントの一つである軽量暗号技術を調査検討する．自動車システムにおいては，厳格なリアルタイム性要求や，完全性と可用性等のセキュリティ保護観点の重要性があるため，従来の IT システム向けの暗号技術では完全な対応は困難な状況とされている．

このため，自動車システムを含むデバイス要件・システム要件が厳しい適用先に向けた技術として，軽量暗号技術が 2005 年頃から検討されてきた．自動車に関するサイバーセキュリティ課題として，すでに大きく取り上げられているものとして，CAN，PKES，TCU，TPMS(Tire Pressure Monitoring System) の機器自身や関連する対抗装置との通信プロトコルを対象とし，現状のセキュリティ課題を整理し，対策方針に関して考察する．一方で，セキュリティ対策の要素として期待される軽量暗号技術に関し，学術標準化動向について，現状を調査し，今後検討すべき研究の方向性を明らかにする．

本検討の結果として，軽量暗号プリミティブとその適用について網羅的に調査検討を行い，現状の把握と整理

[1] 国立研究開発法人産業技術総合研究所　情報技術研究部門
住友電工－産総研サイバーセキュリティ連携研究室
[2] 住友電気工業株式会社

を行った．さらに，今後，暗号技術をコアとしたセキュリティ対策を策定するための課題を抽出した．

本論文の構成は以下である．2 章において，本論文の理解に必要な技術説明を行い，3 章において，軽量暗号技術において，プロトコル，モード，プリミティブレイヤに関し，現状を調査した上で，今後の適用に向けた考察と検討を行う．4 章において，安全性と実装面からの暗号技術の自動車システムへの適用に向けた課題について整理し，5 章で結論を述べる．

2. 自動車のセキュリティ対策の動向

2.1 標準化団体の対応状況

2011 年以降，欧州のプロジェクト EVITA では，ECU のアプリケーション CPU が暗号プロセッサないしは HSM(Hardware Security Module) を同伴するアーキテクチャが開発された [10]．EVITA の HSM は，AES 暗号等の共通鍵暗号技術を用いた暗号化機能や改ざん検知機能または楕円暗号等の公開鍵暗号技術を用いた暗号化機能やデジタル署名等を含む全暗号処理を担う．ECU の保護のために，3 つのセキュリティレベル (light，medium，full) を規定し，開発者に脅威とコストを踏まえた選択肢を提供することを薦めている．

グローバル開発パートナーシップ AUTOSAR (AUTomotive Open System ARchitecture) [5] は，Release 4.3 における SecOC(Secure Onboard Communication) において，MAC アルゴリズムによるメッセージ認証が明記する等，セキュリティ機能の定義を進めている．TCG (Trusted Computing Group) は，暗号鍵のセキュアな保管を目的として PC 等に採用実績を有する TPM(Trusted Platform Module) に自動車に適用するための活動を行なっており，自動車向け TPM のプロファイル [9] を定義している．

国内では，自動車メーカや電装品メーカ等から成る JasPar（Japan Automotive Software Platform and Architecture）において，AUTOSAR 標準化 WG や情報セキュリティ WG が設置され，海外標準化動向を見据えたセキュリティ対策が検討されている．

2.2 暗号適用におけるレイヤーの全体像

自動車分野において，システムとしてセキュリティを考える上では，セキュリティ対策を実現する要素である暗号技術についても，仕様策定，実装，運用と広範囲の視点が必要である．仕様策定に関しては，以下の図に見られるように，複数レイヤーから成る暗号技術を組み立てて実現される場合も多いと考えられる．

3. 自動車システム向けプロトコル

自動車システムのコネクテッド化に伴って，様々な通信プロトコルがそのシステム上で運用されている．通信プロトコルの中には電波を用いて車両外部と通信を行うものもあり，盗聴による脅威が考えられる．本章では，CAN，TCU，PKES，TPMS の各プロトコルについて確認されている脅威とその対策方針について述べる．

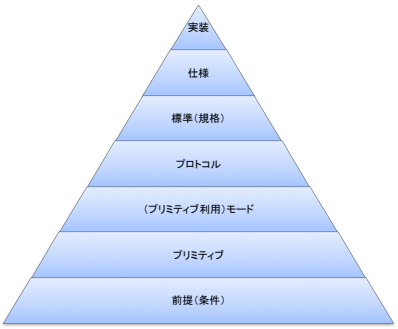

図 1 暗号技術のレイヤー

3.1 CAN

3.1.1 既存技術に対する脅威

CAN メッセージのなりすまし攻撃は，OBD-II ポートを介した不正パケットの入力等により実施されることが知られている．

3.1.2 対策方針

CAN メッセージのなりすまし対策として，多数提案されているが，不正パケットを拒絶するために，CAN のパケットに MAC タグを付与する方法は　文献 [8] において提案されている．さらに処理を効率化することを目指し，監視ノードを設置して，メッセージの MAC を検証して，なりすましメッセージを拒絶する方式 [11] も提案されている．

3.1.3 考察

CAN への暗号適用は，ECU のリソース不足やシステムのリアルタイム性対応の点で，実装する暗号の軽量化が課題であると考える．

3.2 TCU

TCU は移動体通信の技術を用いて，車両外部との通信を行い，周囲の道路状況などの情報を収集，提供する機器である．外部との通信プロトコルとして Wi-Fi や LTE が利用される．TCU の概念図を図 2 に示す．

3.2.1 既存技術に対する脅威

2015 年に Miller と Valasek が Jeep における TCU に対するハッキングを提案し，マルチメディアシステムを外部から操作可能であることを示した [30]．攻撃対象の Jeep では車外通信に WPA2 を用いているが，パスワードの生成方式に起因する脆弱性によりパスワードをクラックすることで，Jeep のヘッドユニットに接続が可能となる．図 3 に，攻撃者による接続の概念図を示す．さらにヘッドユ

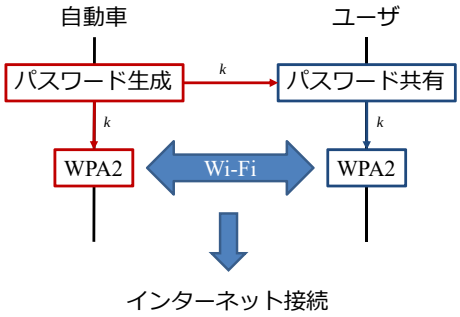

図 2　TCU の概念図

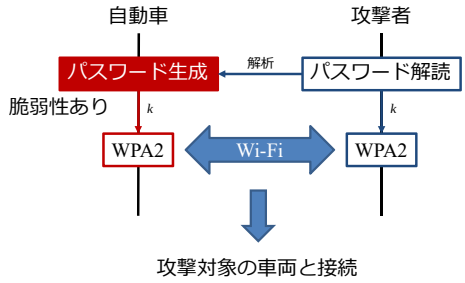

図 3　TCU に対する攻撃

ニットにおけるソフトウェア上の脆弱性を利用して，ヘッドユニットシステムの制御を乗っ取る．

本攻撃は，携帯電話網を通じて ECU のファームウェアを不正に書き換えた上で，自動車の操舵をリモート操作することを実行する．一方で，標準団体においても，車載機器の安全なソフトウェア更新は課題とされており，2017 年に ITU-T から X.1373 勧告 [6] として，車載機器のリモートソフトウェア更新を安全に行うためのプロトコルが策定された．本プロトコルにおいて，暗号技術として，MAC アルゴリズムを用いる方法やデジタル署名を用いる方法が薦められている．

3.2.2　対策方針

車両への TCP/IP のパケットを入力を受け付けないという対策が行われた．

3.2.3　考察

暗号技術に基づく対策として，WPA2 パスワード生成の複雑化，容易に推測できないように高品質な擬似乱数生成器を利用することが考えられる．

3.3　キーレスエントリーシステム

キーレスエントリーシステムとして PKES や RKES(Remote Keyless Entry System) が存在する．これらは一般的に RF(Radio Frequency) を用いて通信が行われる．RKES では Key Fob 側が 433/315MHz，イモビライザー側が 125kHz という異なる RF 波を用いて通信を行っている．

3.3.1　既存技術に対する脅威

PKES や RKES の多くはアルゴリズムやその安全性が明らかでない暗号プリミティブおよびプロトコルを利用している．脆弱な暗号プリミティブを利用していた例として，Hitag2 を用いた PKES および RKES に対する攻撃がある

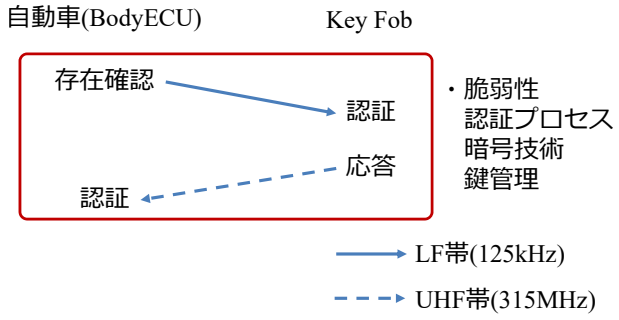

図 4　キーレスエントリーシステムに対する攻撃

表 1　PKES プロトコルに対する攻撃シナリオと対策方針

攻撃シナリオ	対策方針	コスト
正規の Key Fob によるリレー攻撃	通信相手の距離を確認するプロセスを導入	通信：増加，計算：増減なし
Key Fob の追跡	Nonce を利用するセキュリティ機構のにより，ID の値を相互に認証	通信：増加，計算：増加
サービス妨害攻撃	リーダが鍵とその MAC を送信し，Key Fob がそれらを検証するプロセスにより鍵を更新	通信：増加，計算：増加
認証におけるリプレイ攻撃	Key Fob 側からもチャレンジを送信	通信：増加，計算：増加
メモリアクセス保護コマンドのなりすまし攻撃	コマンドに対する事前認証の導入	通信：増加，計算：増加
セッションの乗っ取り	セッション鍵を用いて，各コマンドに MAC を付与することにより導入し，認証を強化	通信：増加，計算：増加

[32], [55]．リバースエンジニアリングによって Hitag2 の暗号化アルゴリズムやプロトコルが明らかにされた結果，脆弱なプリミティブであることがわかり，攻撃が提案された．図 4 にキーレスエントリーシステムに対する攻撃の概念図を示す．

暗号プリミティブの運用において鍵管理が不適切であるために攻撃が成立する場合がある [32]．USENIX 2016 で VW の様々な年式の RKES を解析した結果，RKES のモデルごとに単一の鍵が用いられていることが確認された．さらに，これを用いた攻撃が提案されている．

Atmel がイモビライザー用のプロトコルを公開している [33]．このプロトコルでは暗号プリミティブに AES が用いられている．AES のような標準的で実績のある暗号プリミティブを利用している場合でも，その運用方法やプロトコルによっては安全性が保証されないため，さまざまな攻撃が提案されている [54]．攻撃シナリオの内容を表 1 に示す．以上から，プリミティブだけでなくプロトコルについても安全性の検討が必要であることがわかる．

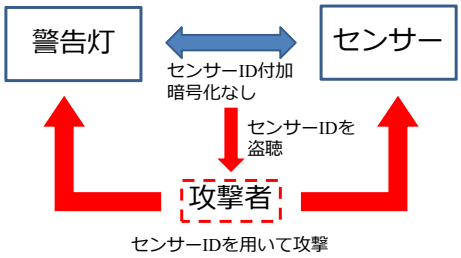

図 5　TPMS に対する攻撃

3.3.2　対策方針

暗号プリミティブについては，一般的にアルゴリズムを公開した上で，研究者による安全性の議論がオープンに行われる．自動車システムにおいても，安全性が十分に検証された暗号プリミティブの利用が広がっている．

Atmel が公開しているプロトコルに対しては，攻撃の提案者が同時に対策についても言及している．表 1 にその対策を記載する．

3.3.3　考察

一般的な暗号プリミティブと同様に，自動車システムにおける暗号プリミティブやプロトコルの安全性について，有識者がオープンに議論し，評価を行うことが，今後，必要となると考えられる．自動車システムにおいて暗号技術を適切に利用するために必要なコストについて検討し，安全性とコストのトレードオフを考慮したシステムが考えられる．

3.4　TPMS

TPMS はタイヤ圧および温度を監視する機器である．タイヤ圧低下が原因の事故から，米国や EU 諸国などにおいて段階的に搭載が義務付けられていった．日本では義務化が遅れている．タイヤに設置されたセンサと車体側のアンテナとの間で無線通信が行われ，受信した情報が ECU で処理される．

3.4.1　既存技術に対する脅威

TPMS のリバースエンジニアリングとその結果を用いた攻撃が提案されている [50]．自動車側の Body ECU がセンサを認識するための情報としてセンサの位置と ID の情報を持っている．データフォーマットに ID がそのまま入力され，通信が行われるので，その ID 情報を盗聴することで様々な攻撃が可能となる．図 5 に攻撃の概念図を示す．具体的には，センサの起動信号を盗聴することで，車両の追跡が可能となる．さらに起動信号のなりすまし攻撃を行うことで，TPMS のバッテリーを減少させることができる．また，センサからのパケットを偽造することで，タイヤ圧に関する警告灯の誤作動を引き起こすことが可能である．以上のように，盗聴に基づいて様々な攻撃が成立する．

3.4.2　対策方針

Rouf らは以下のような対策を提案している [50]．パケット偽造攻撃の原因の一つとして，既存の TPMS ではタイヤ圧などのデータ領域と警告フラグの領域の関係性を確認していないことがあげられる．このため，パケットを偽造し，警告灯を誤作動させる攻撃の対策として，Rouf らはパケットの整合性を確認し，不正パケットを排除するために強制的な手法を導入することを主張している．

盗聴やなりすまし攻撃が成立する根本的な原因はパケットが平文で送信されていることである．暗号化を導入することで解決が図られるが，現状のパケット構成ではリプレイ攻撃が成立してしまう．パケットにシーケンス番号を付加し，順序の情報を付加することで，リプレイ攻撃の対策とする．また，メッセージ偽造の対策として CRC チェックサムの代わりに MAC のような暗号論的なチェックサムの導入が考えられる．暗号技術の導入の際には鍵を保管する領域やその導入方法などを検討する必要がある．

起動信号のなりすましの対策として以下が検討されている．起動信号は大きなデータを送信できないため，小さい領域に適した方式を考える．既存の領域をシーケンシング領域として利用する．ハッシュ関数を用いてシーケンス番号を隠し，シーケンス番号の確認で，起動信号の連続性を確認し，なりすましを防ぐ．

3.4.3　考察

パケットに対する暗号化の導入に際して，コストを抑えるために，パケットのへの暗号化と認証の付加を認証暗号により一つの暗号技術によって導入することを考える．

4.　軽量暗号技術

本章では，軽量暗号技術の現在の標準化や学会での評価の動向を踏まえて，代表的な軽量暗号技術を網羅的に調査した結果について述べる．軽量暗号技術は暗号プリミティブ，利用モード，プロトコルの 3 つのレイヤーで議論される．また，軽量暗号技術の一種として，データの暗号化と認証の処理を一つのプリミティブあるいは利用モードで行う認証暗号の研究が進んでいる．

軽量暗号技術の評価プロジェクトとして CRYPTREC，FELICS[13]，CAESAR，NIST などがある．CRYPTREC からは軽量暗号技術の利用や実装性能に関する報告書が公開されている [14]．軽量暗号技術全般について記載されているが，ブロック暗号が主になっている．FELICS はローエンド環境での軽量暗号技術を評価するプロジェクトである．ブロック暗号とストリーム暗号について評価されている．CAESAR は認証暗号のコンペティションであり，現在第 3 ラウンドまで評価が進んでいる．NIST は米国の産業や技術の規格標準化を行っており，特に暗号技術に関しては国際的に牽引する機関である．

軽量暗号の代表的な性能指標としてハードウェア向けのものでは回路規模，消費電力量，レイテンシがソフトウェア向けのものではメモリサイズおよびレイテンシが考えら

れる．調査対象の暗号技術は，ブロック暗号，ストリーム暗号，ハッシュ関数，メッセージ認証コード (MAC)，認証暗号，プロトコルのそれぞれについて特徴や実装性能などについて説明する．

4.1 ブロック暗号

軽量ブロック暗号において，主に ISO/IEC で標準化されているプリミティブとして，PRESENT [27]，CLEFIA [52]，SIMON [21]，SPECK [21] がある．特に PRESENT は自動車関連の団体である AUTOSAR でも標準化が進んでいる．一方，学会等で安全性や性能の検証が進んでいるプリミティブとして，PRINCE [28]，LED [35]，Piccolo [51]，TWINE [53]，Midori [19] がある．表 2 にローエンドな環境での利用が期待できるプリミティブを示す．

ブロック暗号は秘密鍵と平文を入力として暗号文を出力する．

4.2 ストリーム暗号

軽量ストリーム暗号において，ISO/IEC で標準化されているプリミティブとして，Enocoro-128 v2 [62]，Enocoro-80 [62]，Trivium [29] がある．IETF や AUTOSAR で標準化されているプリミティブとして，ChaCha20 [22] がある．一方，学会等で安全性や性能の検証が進んでいるプリミティブとして，Micro-Trivium [61]，Grain v1 [36]，MICKEY 2.0 [18] がある．表 2 にローエンドな環境での利用が期待できるプリミティブを示す．

ストリーム暗号は秘密鍵と初期化ベクトルを入力としてキーストリームを生成する．平文とキーストリームとの排他的論理和により，暗号文を得る．

4.3 ハッシュ関数

軽量ハッシュ関数において，ISO/IEC で標準化されているプリミティブとして，SPONGENT [26]，PHOTON [34]，Lesamnta-LW [37] がある．また，同様に標準化されているプリミティブとして SHA-1 が存在するが，近年多くの脆弱性が指摘されている．一方，学会等で安全性や性能の検証が進んでいるプリミティブとして，Quark [16] や KECCAK-f[200] [25] がある．表 2 にローエンドな環境での利用が期待できるプリミティブを示す．

ハッシュ関数はメッセージを入力して，固定長のハッシュ値を出力する．

4.4 メッセージ認証コード

省リソース環境下においてのメッセージ認証を目的とした軽量 MAC が，プリミティブ，利用モードの両面で提案されている．軽量 MAC の代表的なプリミティブとして Chaskey-12 [46] が，代表的な利用モードとして LightMAC [41] がそれぞれ挙げられる．Chaskey-12 は ISO/IEC で標準化が進んでいる．

MAC は秘密鍵とメッセージを入力して，認証用のタグを出力する．

4.5 認証暗号

代表的な認証暗号としてブロック暗号利用モードである AES-GCM が存在する．AES-GCM に対して優位性を持ち，多くの範囲で利用可能な認証暗号のコンペティションとして CAESAR が行われている．

CAESAR は現在第 3 ラウンドまで進行しており，プリミティブおよび利用モードとして ACORNv3 [56], AEGISv1.1 [59], OTRv3.1 [44], AEZv4.2 [38], Asconv1.2 [31], CLOC and SILC v3 [45], COLMv1 [15], Deoxysv1.41 [39], JAMBUv2.1 [58], Ketjev2 [23], Keyakv2.2 [24], MORUSv2 [57], NORXv3.0 [17], OCBv1.1 [40], Tiaoxinv2.1 [47] が提案されている．表 3 にハードウェア実装のスライス数が少なくかつローエンドのソフトウェア実装の性能が明確に示されている認証暗号を示す．ハードウェア実装が Virtex 6 を用いた FPGA で行われているため，回路規模をスライス数で示す．ローエンドのソフトウェア実装は ARM Cortex-A5 Amlogic S805 1.5GHz での実装結果を，ハイエンドのソフトウェア実装は AMD Ryzen 7 1700 2.99GHz での実装結果をそれぞれ示す．

認証暗号は秘密鍵，平文，Nonce，Associated data を入力として，暗号文とタグを得る．

4.6 プロトコル

車載システムではリアルタイム性が非常に重要である．リアルタイム性に対応した認証・秘匿を行うプロトコルとして，ITU-T によって EAMD が標準化されている [60]．EAMD はパケットの元データに対してマスクをかけ，取り出したデータに対して暗号化や MAC の処理を行う．元データ全体ではなく，一部のデータに対してのみ暗号化および MAC の処理を行うため，非常に軽量となる．

4.7 考察

表 2 および 3 で示した通り，評価プロジェクトや学会において軽量暗号の実装性能の評価が行われている．認証暗号では RAM/ROM の評価が行われておらず，また，CPU の性能の観点からもローエンドの評価が十分であるとは言えない．さらに軽量暗号技術全般で見ても，RAM/ROM の評価が行われているものは少ない．自動車システムを考慮した環境における性能指標を十分に評価する必要があると考えられる．

3 章に示した通り，PKES や TPMS などの自動車システムは Key Fob やセンサと ECU 間で通信が行われる．これらのシステムへ暗号技術を適用する際に，ECU とその通信相手の双方に対し，求められる実装形態（HW/SW）や実

表 2　軽量暗号と実装性能

C*	名称	安全性強度 [bit]	論理規模 [kgate]	スループット	ローエンド (速度 [cpb], RAM[Byte])	ハイエンド 速度 [cpb]	参考文献
B	PRESENT	128	1.9/1.4	200/11 kbps @100kHz	–	4.7 @Xeon E3	[27], [42], [49]
B	CLEFIA	128	6.2	83.5 Mbps @114MHz	(6208, 86) @RL78	–	[14], [43]
B	PRINCE	128	3.0/3.4	533.3 kbps @100kHz	(2225.4, 220) @ATtiny85	–	[20], [28], [48]
S	ChaCha20	256	–	–	(54.3, –) @ Cortex-M3	1.2 @Core i5	[12], [13]
S	Enocoro-128 v2	128	4.1	3.52 Mbps @440MHz	–	27 @Core2 Duo	[63]
H	SPONGENT	128	2.0/3.3	0.17/11.4 kbps @100kHz	–	–	[26]
H	Lesamnta-LW	128	8.2	125 Mbps @188MHz	(3301, 50) @H8	43 @Core i5	[37]

*暗号技術のカテゴリ，B：ブロック暗号，S：ストリーム暗号，H：ハッシュ関数，M：MAC を表す

表 3　認証暗号と実装性能

カテゴリ*	名称	安全性強度 [bit]	スライス数	スループット [Mbps]	ローエンド 速度 [cpb]	ハイエンド 速度 [cpb]	参考文献
S	ACORN	128	161	3,419 @427.4MHzMHz	76.44	5.30	[64], [65]
B	ASCON	128	451	3,118 @341.1MHz	169.93	5.77	[64], [65]
B	Deoxys	128	956	2,870 @336.4MHz	94.30	0.75	[64], [65]
B	MORUS	128	1025	49,421 @193.1MHz	23.75	0.84	[64], [65]
SP	Keyak	128	1751	7,417 @163.6MHz	43.72	8.95	[64], [65]
M	COLC	128	891	1,536 @280.9MHz	125.41	2.55	[64], [65]
M	SILC	128	921	4,040 @315.7MHz	137.42	2.56	[64], [65]
M	OCB	128	1348	3,122 @292.7MHz	46.42	0.48	[64], [65]

*B：ブロック暗号，S：ストリーム暗号，SP：スポンジ構造，M：利用モードを表す．

装リソース（必要ゲート数・スライス数/RAM・ROM 使用量，CPU 能力等）を踏まえた，暗号仕様の選択と最適化実装を提供する必要がある．

本章の各暗号技術の項で示したとおり，暗号技術の運用には様々な入力が必要となる．暗号技術を安全に利用するためには秘密鍵や Nonce，マスクなどの安全性に直結する入力値を適切に管理する必要がある．適用先のシステムの安全性要件と暗号技術の運用コストを十分に検討して，適用する技術を選定するべきである．

5. 課題整理

5.1 システムセキュリティの課題

安全な通信を考える上で暗号化は必要であることは単純な通信モデルではよく知られているが，自動車分野において，システムとしてセキュリティを考える上では，セキュリティ対策の仕様策定，実装，運用と広範囲の視点が必要である．仕様策定に関しては，セキュリティ対策は，複数レイヤーから成る暗号技術を組み立てて実現される場合も多いと考えられる．弱い暗号プリミティブを利用した場合も脆弱なシステムになり得るだけでなく，高い安全性を有すると知られる AES を用いたとしてもプロトコルの構成によっては脆弱なシステムになる．

運用に関しては，暗号化を用いても鍵管理が適切に行われない場合，攻撃可能となる．鍵管理やプロトコルのチャレンジの生成の都合上，コスト制約下で適切な安全性を提供する乱数生成器をシステムに搭載する必要がある．例えば，リアルタイム対応の IoT 向け ITU-T 勧告プロトコル EAMD についても，鍵管理や鍵や同伴データの共有スキームの具体的な方式についても未策定な状況である．

5.2 実装の課題

CRYPTREC，FELICS，CESAR などのように，軽量暗号技術の評価プロジェクトは存在し，多くの貢献を行っているが，複雑な自動車システムにおいて，最適な対策を提供するために必要な，暗号技術の評価ベンチマークは未だ完成していない状況にあると考えられる．実装比較評価環境についても，軽量暗号の研究開発は 2005 年頃から開始されているために，一部の軽量標準暗号については，実装環境が古いものもあり，将来的な利用に備えた，想定される実装環境における再評価が望まれる．

レイヤ毎に見ていても，プリミティブについては，ストリーム暗号やハッシュ関数等の主要なカテゴリーの技術に関して，評価数値は充実しているとは言えない．プロトコルレイヤ～プリミティブレイヤと言う複数レイヤを縦断するような性能評価も今後の課題である．前節において，適切な安全性要件が明確になったとしても，自動車システムは，PKES や TPMS 等の無線通信においては，車両側と対抗装置（key fob，センサ) 等のデバイス実装要件や，リアルタイム性能要件等のシステム要件（1ms 処理等の短周期処理）は，別途，検討する必要がある．

どのレイヤがボトルネックになるかを明確化した上で，方式策定，実装，運用等のどの観点での検討にフォーカスするかを決めることが必要になると思われる．例えば，AES を固定して，その上のモード，プロトコルレイヤで軽

量な技術を利用すべきなのか，あるいは，モード・プロトコルレイヤはビジネス上の利用でクローズで固定されている場合があり，その場合は，それらを固定し，プリミティブレイヤを軽量暗号から選択することも考えられる．

暗号技術は，その性能が実装に大きく依存することが多く，一台の車内においても多数多様な ECU 上で実装を踏まえると，ハードウェアや暗号コプロセッサによる実装が真に必要な ECU 群，ハードウェアによる暗号機能が非提供であるがため，ソフトウェア実装が必要な ECU 群等，様々なセキュリティユースケースが考えられる．

例えば，ハードウェア志向で設計された軽量暗号が，ハードウェアでもソフトウェアでも双方の実装が必要になる場合も想定されるが，こうした場合にどの暗号技術を選択することが最適か判断するために必要な評価数値情報は不足している状況にあると言える．

6. おわりに

本論文では，自動車システムのセキュリティ対策について，暗号技術の観点から調査検討した．暗号適用対象となる車載機器とその利用ユースケース（PKES，TCU，TPMS 等）を明確化し，現状想定されている脅威，対策方針，暗号適用先等を整理した．その上で，対策方針を実現するために，今後利用が期待される軽量暗号技術に関して，プリミティブ，利用モード，プロトコルの各レイヤの観点や SW/HW の実装観点から，ISO/IEC 等の標準化や CAESER 等学会の暗号技術への取り組み状況を調査検討した．その結果，現状は対策実現に向けた検討が十分とは言い切れない状況が明らかになり，今後，セキュリティをシステムとして実現するために，組込みローエンド環境の RAM/ROM 評価の充実，送信機と受信機で HW/SW のそれぞれの性能が重要になる場合の方式選定と最適化実装，複数の暗号技術をリソース制約下で安全に組み立てるための手法論と実装評価等, 解決すべき課題を抽出した．

参考文献

[1] ISO/IEC 15408-1:2009 Information technology Security techniques Evaluation criteria for IT security Part 1: Introduction and general model.

[2] ISO 26262 Road vehicles – Functional safety.

[3] SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, SAE International, January, (2016).

[4] C. Valasek, and C. Miller, “Adventures in Automotive Networks and Control Units”, DEFCON 21, (2013).

[5] AUTOSAR, Release 4.3 https://www.autosar.org/standards/classic-platform/release-43/.

[6] ITU-T X.1373: Secure applications and services - Intelligent transportation system (ITS) security, Secure software update capability for intelligent transportation system communication devices.

[7] JasPar https://www.jaspar.jp/.

[8] Nilsson, D. K., Larson, U. E., and Jonsson, E., :Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes, Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th.

[9] TCG, TPM 2.0 Library Profile for Automotive Thin Specification, Version 1.0 https://trustedcomputinggroup.org/tcg-tpm-2-0-library-profile-automotive-thin/

[10] EVITA, Deliverable: D3.2 Secure on-board architecture specification.

[11] 倉地 亮 松原 豊 高田 広章 上田 浩史 堀端 啓史 、: メッセージ認証を用いた CAN の集中監視システム”, 特集論文 (組込みシステムセキュリティ論文小特集)、電子情報通信学会論文誌 A Vol.J99-A No.2 pp.118-130, (2016).

[12] ebacs: Ecrypt benchmarking of cryptographic systems, `http://bench.cr.yp.to/results-stream`.

[13] FELICS - Fair Evaluation of Lightweight Cryptographic Systems, `https://www.cryptolux.org/index.php/FELICS`.

[14] 暗号技術ガイドライン（軽量暗号）, `http://www.cryptrec.go.jp/report/cryptrec-gl-0001-2016-j.pdf` (2017).

[15] Andreeva, E., Bogdanov, A., Datta, N., Luykx, A., Mennink, B., Nandi, M., Tischhauser, E. and Yasuda, K.: COLM v1, *Submission to the CAESAR competition* (2016).

[16] Aumasson, J., Henzen, L., Meier, W. and Naya-Plasencia, M.: Quark: A Lightweight Hash, CHES 2010, LNCS, Vol. 6225, Springer, pp. 1–15 (2010).

[17] Aumasson, J.-P., Jovanovic, P. and Neves, S.: NORX v3. 0. Submission to CAESAR (2016).

[18] Babbage, S. and Dodd, M.: The stream cipher MICKEY 2.0, *ECRYPT Stream Cipher, Available at* *`http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickeyp3.pdf`* (2006).

[19] Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T. and Regazzoni, F.: Midori: A Block Cipher for Low Energy, ASIACRYPT 2015, LNCS, Vol. 9453, Springer, pp. 411–436 (2015).

[20] Batina, L., Das, A., Ege, B., Kavun, E. B., Mentens, N., Paar, C., Verbauwhede, I. and Yalçin, T.: Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures, RFIDsec 2013, LNCS, Vol. 8262, Springer, pp. 103–112 (2013).

[21] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L.: SIMON and SPECK: Block Ciphers for the Internet of Things, *IACR Cryptology ePrint Archive*, Vol. 2015, p. 585 (2015).

[22] Bernstein, D. J.: ChaCha, a variant of Salsa20, *In The State of the Art of Stream Ciphers, SASC 2008*, ECRYPT (2008).

[23] Bertoni, G., Daemen, J., Peeters, M. and Assche, G.: CAESAR submission: Ketje v2 (2016).

[24] Bertoni, G., Daemen, J., Peeters, M. and Assche, G.: CAESAR submission: Keyak v2 (2016).

[25] Bertoni, G., Daemen, J., Peeters, M. and Van Assche, G.: The Keccak sponge function family, `http://keccak.noekeon.org/`.

[26] Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K. and Verbauwhede, I.: spongent: A Lightweight Hash Function, CHES 2011, LNCS, Vol. 6917, Springer, pp. 312–325 (2011).

[27] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y. and

Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher, CHES 2007, LNCS, Vol. 4727, Springer, pp. 450–466 (2007).
[28] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S. S. and Yalçin, T.: PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract, ASIACRYPT 2012, LNCS, Vol. 7658, Springer, pp. 208–225 (2012).
[29] Cannière, C. D.: Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles, *ISC 2008*, LNCS, Vol. 4176, pp. 171–186 (2006).
[30] Charlie, M. and Chris, V.: Remote exploitation of an unaltered passenger vehicle, *Black Hat USA*, Vol. 2015 (2015).
[31] Dobraunig, C., Eichlseder, M., Mendel, F. and Schläffer, M.: Ascon v1. 2, *Submission to the CAESAR Competition* (2016).
[32] Garcia, F. D., Oswald, D., Kasper, T. and Pavlidès, P.: Lock It and Still Lose It - on the (In)Security of Automotive Remote Keyless Entry Systems, *Proceedings of the 25th USENIX Security Symposium, 2016*, USENIX Association, pp. 929–944 (2016).
[33] Goings, J., Prescott, T., Hahnen, M. and Milizer, K.: Design and Security Considerations for Passive Immobilizer Systems, *Automotive Compilation vol. 7* (2010).
[34] Guo, J., Peyrin, T. and Poschmann, A.: The PHOTON Family of Lightweight Hash Functions, CRYPTO 2011, LNCS, Vol. 6841, Springer, pp. 222–239 (2011).
[35] Guo, J., Peyrin, T., Poschmann, A. and Robshaw, M. J. B.: The LED Block Cipher, CHES 2011, LNCS, Vol. 6917, Springer, pp. 326–341 (2011).
[36] Hell, M., Johansson, T. and Meier, W.: Grain - A Stream Cipher for Constrained Environments, ECRYPT Stream Cipher Project Report 2005/010, 2005. Available at `http://www.ecrypt.eu.org/stream` (2005).
[37] Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B. and Yoshida, H.: An AES Based 256-bit Hash Function for Lightweight Applications: Lesamnta-LW, *IEICE Transactions*, Vol. 95-A, No. 1, pp. 89–99 (2012).
[38] Hoang, V. T., Krovetz, T. and Rogaway, P.: AEZ v4. 2: Authenticated Encryption by Enciphering (2016).
[39] Jean, J., Nikolic, I., Peyrin, T. and Seurin, Y.: Deoxys v1. 41, *Submission to the CAESAR competition* (2016).
[40] Krovetz, T. and Rogaway, P.: OCB (v1. 1), *Submission to the CAESAR competition* (2016).
[41] Luykx, A., Preneel, B., Tischhauser, E. and Yasuda, K.: A MAC Mode for Lightweight Block Ciphers, FSE 2016, LNCS, Vol. 9783, Springer, pp. 43–59 (2016).
[42] Matsuda, S. and Moriai, S.: Lightweight Cryptography for the Cloud: Exploit the Power of Bitslice Implementation, CHES 2012, LNCS, Vol. 7428, Springer, pp. 408–425 (2012).
[43] Matsui, M. and Murakami, Y.: Minimalism of Software Implementation - Extensive Performance Analysis of Symmetric Primitives on the RL78 Microcontroller, FSE 2013, LNCS, Vol. 8424, Springer, pp. 393–409 (2013).
[44] Minematsu, K.: AES-OTR v3. 1 (2016).
[45] Minematsu, K., Guo, J. and Kobayashi, E.: CLOC and SILC (2016).
[46] Mouha, N.: Chaskey: a MAC Algorithm for Microcontrollers - Status Update and Proposal of Chaskey-12 -, *IACR Cryptology ePrint Archive*, Vol. 2015, p. 1182 (online), available from ⟨http://eprint.iacr.org/2015/1182⟩ (2015).
[47] Nikolic, I.: Tiaoxin-346, *Submission to the CAESAR Competition* (2016).
[48] Papapagiannopoulos, K.: High Throughput in Slices: The Case of PRESENT, PRINCE and KATAN64 Ciphers, RFIDSec 2014, LNCS, Vol. 8651, Springer, pp. 137–155 (2014).
[49] Poschmann, A.: Lightweight Cryptography - Cryptographic Engineering for a Pervasive World, *IACR Cryptology ePrint Archive*, Vol. 2009, p. 516 (2009).
[50] Rouf, I., Miller, R. D., Mustafa, H. A., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W. and Seskar, I.: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, *19th USENIX Security Symposium, 2010, Proceedings*, USENIX Association, pp. 323–338 (2010).
[51] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. and Shirai, T.: Piccolo: An Ultra-Lightweight Blockcipher, CHES 2011, LNCS, Vol. 6917, Springer, pp. 342–357 (2011).
[52] Shirai, T., Shibutani, K., Akishita, T., Moriai, S. and Iwata, T.: The 128-Bit Blockcipher CLEFIA (Extended Abstract), FSE 2007, LNCS, Vol. 4593, Springer, pp. 181–195 (2007).
[53] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E.: $\textnormal{\textsc{TWINE}}$: A Lightweight Block Cipher for Multiple Platforms, SAC 2012, LNCS, Vol. 7707, Springer, pp. 339–354 (2012).
[54] Tillich, S. and Wójcik, M.: Security Analysis of an Open Car Immobilizer Protocol Stack, *In 10th escar Embedded Security in Cars Conference* (2012).
[55] Verdult, R., Garcia, F. D. and Balasch, J.: Gone in 360 Seconds: Hijacking with Hitag2, *Proceedings of the 21th USENIX Security Symposium, 2012*, USENIX Association, pp. 237–252 (2012).
[56] Wu, H.: ACORN: A lighweight authenticated cipher (v3), *Candidate for the CAESAR Competition. See also https://competitions. cr. yp. to/round3/acornv3. pdf* (2016).
[57] Wu, H. and Huang, T.: The Authenticated Cipher MORUS (v2), *Submission to the CAESAR competition* (2016).
[58] Wu, H. and Huang, T.: The JAMBU Lightweight Authentication Encryption Mode (v2. 1), *Submission to the CAESAR competition* (2016).
[59] Wu, H. and Preneel, B.: AEGIS: A Fast Authenticated Encryption Algorithm (v1, 1) (2016).
[60] X.1362, I.-T.: Simple encryption procedure for Internet of things (IoT) environments (2017).
[61] Zhang, S. and Chen, G.: Micro-Trivium: A lightweight algorithm designed for radio frequency identification systems, *IJDSN*, Vol. 13, No. 2 (2017).
[62] 株式会社日立製作所：疑似乱数生成器 Enocoro, *http://www.hitachi.co.jp/rd/yrl/crypto/enocoro/index.html*.
[63] 三上 修吾, 渡辺 大：ストリーム暗号 Enocoro-128v2 のソフトウェアおよびハードウェア実装と評価, コンピュータセキュリティシンポジウム 2012 論文集, Vol. 2012, No. 3, pp. 742–748 (2012).
[64] Cryptographic Engineering Research Group at George Mason University: ATHENa: Automated Tools for Hardware EvaluatioN, https://cryptography.gmu.edu/athena/.
[65] Bernstein, D. J.: eBACS: ECRYPT Benchmarking of Cryptographic Systems, http://bench.cr.yp.to/results-caesar.org/.