様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　５ 月 ２４ 日現在

機関番号：１５３０１
研究種目：基盤研究(A)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０１７２３

研究課題名（和文）IoT時代の遠隔操作型・自律型移動システムにおける安全かつ高信頼な通信の実現

研究課題名（英文）Realization of secure and reliable communication in a remote control type / autonomous mobile system in the IoT era

研究代表者
野上　保之（Nogami, Yasuyuki）

岡山大学・自然科学研究科・教授

研究者番号：６０３１４６５５

交付決定額（研究期間全体）：（直接経費）　　30,300,000円

研究成果の概要（和文）：本研究では、自律走行・自動運転可能な電気自動車や遠隔操作・駆動系ロボットなど具体的な駆動システムを用い、その制御ネットワークに最先端および先駆的なセキュリティ技術（データ認証、機器認証、鍵更新機能）を施した場合に、どの程度リアルタイム性に影響を与えるか検証することで、問題なく実現できるセキュリティレベルを明確にした。具体的には、CANシステムに対し、AES・乱数・軽量暗号を用いたデータ認証機能を搭載し、リアルタイム処理が実現できることを示した。また、サイドチャネル攻撃の脅威も実証実験し、その対策としての鍵更新機能を、楕円ペアリング暗号を用いて現実的な処理時間で実現できることを示した。

研究成果の学術的意義や社会的意義
自律走行・自動運転可能な電気自動車や遠隔操作・駆動系ロボットなど具体的な駆動システムを用い、その制御ネットワークに最先端および先駆的なセキュリティ技術（データ認証、機器認証、鍵更新機能）を施した場合に、どの程度リアルタイム性に影響を与えるか検証することで、問題なく実現できるセキュリティレベルを明確にしようとする点に意義がある。計算リソース・セキュリティ強度・誤り訂正強度と駆動リアルタイム性の間のトレードオフが明確になり、また昨今とくに脅威となっているサイドチャネル攻撃など電磁物理攻撃への対策実装について、今後の駆動システム内の制御ネットワーク設計に有益な情報となる。

研究成果の概要（英文）：In this research, using a specific drive system such as an electric vehicle and robot capable of autonomous driving and remote control, the advanced security technology (data authentication, device authentication, secure key update) we have clarified the security level that is realized without any problems by verifying how much the real-time performance is affected. Specifically, for the CAN system, data authentication with message authentication code that is generated by AES, random number generator, and lightweight encryption has been implemented. Then, side-channel attack has been demonstrated experimentally, key update function as the countermeasure using elliptic pairing-based cryptography has been also implemented. Their real-time processing could be realized.

研究分野：情報セキュリティ

キーワード：IoTセキュリティ　自律駆動・遠隔操作　リアルタイム処理　暗号セキュリティ　データ認証　鍵更新

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

IoT（Internet of Things）時代への突入は、インターネット創成期にも似て、セキュリティという言葉で括られる「決して忘れてはならない大前提」を置き去りにして、その無限大とも思える利便性を、いままさに大きく、急速に展開しようとしている。その現場を制御しているのは、小型かつ計算リソースの限られた貧弱な端末機器であり、人的な操作を介すことなく、それらが互いに自律してデータをやり取りする。「お金」に代表される大切なデータは、古くは銀行の専用線のような形態から、イーサネット技術、あるいは近年の制御システムにおけるゾーニングのように、その態様を進化させながら守られてきた。ICT 社会の発展は、有線・無線・専用線、オンライン・オフラインを問わず、そのような貧弱な機器に対して大切なデータのやり取りを要求する。そのような状況の中で、複雑化してその隙間が見え隠れする現代 ICT セキュリティ対策はもとより、昨今の「サイドチャネル攻撃」に代表される物理的な解読攻撃の脅威が、ICT 社会における情報の守り手と不正に解読しよう企む攻め手の間の「イタチごっこ」に対し、「圧倒的に攻め手が優位な状況」を生み出しつつある。一方で時代の流れは、ロボットによる遠隔手術や自動車の自動運転に代表される「極めて高度な遠隔操作型・自律型移動システム」の実現を視野に捉えた。自動運転では、これまでのように衝突の危険性を感知して自動的に止まる機能のみならず、GPS や画像処理などを駆使して自律的に自動車が運転されるようになる。それら信号の制御は、車載ネットワーク CAN（Controller Area Network）のように ECU（Electronic Control Unit）と呼ばれる小型機器を数多く連結させて行うこととなり、これらが自律的に動作する環境において、「万一の瞬間」に人的な操作は及ばず、ときに人の生死にもかかわる操作を ECU に委ねることとなる。そのようなネットワーク内を流れるセンサ・制御データなどが「ありのまま」造作なく取得できてしまえば、メーカーが多くの時間と費用をかけて蓄積してきたノウハウが流出し得るだけでなく、システムのクラックを企む悪意ある攻撃者に対して「極めて危険なヒント」を与えてしまうこととなる。本研究は、そのような遠隔操作型・自律型移動システムに対し、センサ・制御データのセキュアかつ高信頼な通信処理と、自律駆動も視野に入れたリアルタイム性を損なわない制御処理の両立を、(1)暗号技術の最適化、(2)セキュア通信プロトコルの開発、(3)高信頼なデータ通信の開発の実装、そして(4)実際に駆動系を用いた実証実験により、具体的に検討するものである。

２．研究の目的

車の自動運転や、医用ロボットによる遠隔手術など、GPS による位置情報、小型カメラによる画像情報、そして様々なセンサ情報を連携させ、極めて高度な「遠隔操作型・自律型移動システム」が実現されつつある。一方で、それらを制御するためのデータ通信は、何よりも動作のリアルタイム性を最優先とするため、その信頼性と安全性は二の次であった。しかし、IoT 時代への突入と、サイドチャネル攻撃など新手のセキュリティ脅威はこれを許さず、そのような制御・データ通信に対し、高い信頼性と高度な安全性の確保を要求する。これに対して本研究では、具体的にロボットなどを用いながら、種々のセキュリティ・高信頼化・攻撃手法を投入し、これらがどの程度リアルタイム性に影響するのか実証実験し、そのトレードオフを見極めた最適な実現を検討する。

３．研究の方法

4 つの項目：(1)システムに適応した暗号化手法の開発、(2)セキュア通信プロトコルの開発、(3)高信頼なデータ通信の開発と実装、(4)遠隔操作型・自律型移動ロボットによる実証実験に分ける。(1)と(2)では、主として遠隔操作型・自律型移動ロボット向けの暗号化手法とプロトコルを設計し、(3)と(4)では、主として(1)と(2)で開発したプロトコルを高信頼・リアルタイム性に注目して実装し、実験評価する。そのような過程を繰り返し、改良や拡張を重ね、セキュリティ強度と動作のリアルタイム性のトレードオフを厳密に評価できるように連携して研究開発を進めた。それぞれの、より詳細な研究項目は下記の通りである。

(1) システムに適応した暗号化手法の開発

(1-1) AES 暗号の効率的な実装と暗号用擬似乱数の設計：データ暗号化やデータ認証のためのハッシュ値の計算のためである。(1-2) 適応的な楕円曲線暗号の設計：機器認証や鍵更新のためのペアリング暗号実装のためである。(1-3) 暗号状態制御法のためのペアリング暗号の開発：これは鍵更新実装の実現のためである。

(2) セキュア通信プロトコルの開発

(2-1) データ暗号化とメッセージ認証のプロトコル設計：CAN 通信におけるデータ認証のためのプロトコルを設計する。(2-2) 機器認証プロトコル設計：機器認証を実現するためのプロトコルを設計する。(2-3) 暗号状態で制御するためのプロトコル設計：より高度なセキュリティ応用プロトコルを実現するためである。

(3) 高信頼なデータ通信の開発と実装

(3-1) 誤り訂正による通信エラーおよび物理的なデータ改ざん対策：データ通信の信頼を上げるためのものであり、サイドチャネル攻撃への対策のベースにもなる。(3-2) マイコンなどに

よるコントローラ実装：CAN 通信におけるコントローラを設計し、暗号技術・プロトコルを実装する。(3-3) ノイズおよびサイドチャネル攻撃対策：攻撃実証し、対策としてのデータ認証機能が正しく動くことを検証する。

(4) 遠隔操作型・自律型移動ロボットによる実証実験
(4-1) 実験ロボットの通常動作確認および乗っ取りテスト：データ認証などセキュリティ機能を搭載しない状況においてサイドチャネル攻撃が行えてしまうことを実証する。(4-2) 提案システムの実験ロボットへ移植および安全性とリアルタイム性の検証：データ認証機能を経由した場合の駆動系のリアルタイム処理性能に対するオーバヘッドの大小を検討する。(4-3) 自律駆動システムの設計と総合的な検証試験：乗っ取りの有無、セキュア制御対策の有無、および乗っ取られた際の安全設計（Safety 機能）の実験による検証を行う。

４．研究成果
上記の項目について、以下のような成果を得ることができた。
(1) システムに適応した暗号化手法の開発
データの改ざん・偽装を防止するため、制御データ・センサデータを対称鍵暗号 AES およびストリーム暗号で暗号化することを検討した。AES 暗号については極めて軽量化した我々の提案手法、擬似乱数を用いたストリーム暗号・メッセージ認証（MAC）を適用することも検討した。また、ECU などによる接続や機器の偽装を防止するため、短い鍵長でも十分な安全性を得られる楕円曲線暗号（ECC）を用いた。さらに先駆的な取組として、暗号化したままでもデータ処理が可能（暗号状態制御法）である準同型暗号の実装も考え、楕円ペアリング暗号を適用した放送鍵暗号を実装し、鍵更新機能を実現した。具体的には、Curve25519 と呼ばれる効率的な楕円曲線（暗号）を Arduino UNO に搭載し、BN 曲線および BLS 曲線と呼ばれるペアリング暗号を RaspberryPi に搭載した。後述する実証実験の通り、それぞれ実時間での有効な処理が行えている。鍵更新については、頻繁な更新を想定せず、1 秒以内での更新実現を達成している。

(2) セキュア通信プロトコルの開発
車載ネットワークを流れる情報は、主にセンサ値などの観測情報と車をコントロールする制御情報からなり、機密性は必須要件ではなく、完全性・可用性が重要であることを確認した。そこで、改ざん検知技術に着目し、ECU を想定した 8 ビットマイコンである Arduino にワード長などを 8 ビットに変更した SHA-1 の実装を行った。最短送信間隔である 10msec 以内にハッシュ値の生成が可能なことを確認した。続いて、CAN のデータフレームは最長 64 ビットである制約のため、SHA-1 ですらハッシュ値の送信に 3 パケットを要する問題を確認した。そこで、すべてのデータフレームの空き領域にハッシュ値の一部分を挿入する手法、複数のデータに対するハッシュ値を複数パケットで送信する手法の 2 段構えの改ざん検知手法を提案した。そして、車載ネットワークにおける改ざん検知手法として、準同型性をもつ MAC が適していると考え、準同型共通鍵暗号 SymPC を利用した手法を提案した。SymPC は平文に対して暗号文の長さが数倍になるという問題があるため、擬似乱数列を共有することにより短い MAC 値で送信できる手法を考えた。検討材料として、AES 暗号、SHA-1 のみならず、軽量暗号である Chaskey や、各種の擬似乱数、また共通鍵暗号ベースの鍵更新プロトコルなど、設計・実験を行った。

(3) 高信頼なデータ通信の開発と実装
とくに、サイドチャネル攻撃など安全性評価の面で検討を進めてきた。まず、FPGA 実装された AES 暗号回路のサイドチャネル情報漏洩特性を解明し、SCA 対策の要点を明らかにした。合成体実装の場合について検討し、中間値を格納するフリップフロップおよび S-Box 内の一部のサブ回路部よりサイドチャネル情報が漏洩することを確認した。続いて、CAN 送受信器の電磁妨害波に対する挙動の検査手法の開発に向けた準備として、電流注入プローブを用いて CAN バスに差動モード注入した妨害波パルスに対して送受信器がそれぞれどのような挙動を示すかを実験により検討した。その結果、注入妨害波パルスのタイミングによるデータビットの同期挙動およびエラーフレームの送出動作を観測できることを確認した。そして、暗号回路のサイドチャネル攻撃対策として、S-Box を LUT 実装した AES 回路に対して乱数によるマスキング対策を実装し、サイドチャネル攻撃耐性を評価した。その結果、最高レベルの安全性である Level 4 をクリアすることを示した。電流注入プローブを用いた妨害波パルスに対する CAN 送受信器の挙動試験系を構築した。構築した試験系により、CAN 送受信器の挙動をノード毎に評価できることを実験により示した。使用した評価用モジュールにおいて、CAN プロトコルに従ってビットフレームの同期、およびエラーフレームの送出が観測された。さらに、一部の条件においてプロトコルと異なる挙動も確認された。とくにこの成果については、その製品の誤動作を示せていることのみならず、悪用すれば送り手に気づかれず受け手に改ざんできるようなことにも繋がり得る大きな問題点の指摘になっている。乱数マスキングの新しい手法についても検討ができており、その成果はマイコンや FPGA における物理的な乱数の生成にも活用できる。

(4) 遠隔操作型・自律型移動ロボットによる実証実験
以上のような成果をすべて反映させつつ、具体的な駆動系を用いて実証することが、この研究

項目となる。まずCANの脆弱性によりバスオフ攻撃により移動ロボットの駆動システムに影響を与えることができることを,SH2マイコンならびにCANalyzerを使ったシステムで実証した。続いて、CANの脆弱性をついたバスオフ攻撃がARM Cortex-M3ベースのマイコンにおいても成り立つことを確認した。さらに、セキュリティ対策を実装したCANのコントローラを移動ロボットに組み込んで実験ができるように、Raspberry Pi 3ならびにArduino Unoを使った実験系を構築した。そして、独立二輪駆動タイプの遠隔操作型の移動ロボットに前年度の実験系を組み込んで、セキュリティ対策の有用性を実証するための一連のデモンストレーションを実施した。SHA-1あるいはChaskeyによる認証を実装したCAN通信により、バスオフ攻撃が成立したとしても、その後に攻撃ノードから発行されるコマンドでロボットが乗っ取られることを防ぐことができることを確認した。また、この実験で実装された対策においてはロボットの操作性にほとんど影響を与えずにセキュリティの強化ができることを確認した。さらに、ロボットの遠隔操作性に影響を与える遅延時間について定量的な実験を行い、セキュリティ対策による時間遅延は多くとも400msecに収まるようにすべきであるという指針を得た。これらと合わせて、本研究で開発する頑強で信頼性の高い移動体制御を目的とした通信方式のテスト用実験を開発している。実験用車両が公道を走行できないことを考慮して、敷地内の走行および自動駐車の状況を想定した自律移動システムを開発した。とくに自動駐車について焦点を当て、路面の乾湿に依存しない駐車枠の認識とCAN通信を用いた走行コマンドに基づく駐車制御について研究を進めてきている。

５．主な発表論文等

〔雑誌論文〕（計　８件）

(1) Yuta Kodera, Takeru Miyazaki, Md. Al-Amin Khandaker, Ali Md. Arshad, Takuya Kusaka, Yasuyuki Nogami, and Satoshi Uehara,
“Distribution of Digit Patterns in Multi-value Sequence over the Odd Characteristic Field,”
IEICE Discrete Mathematics and Its Applications, 2017. （査読有）

〔学会発表〕（計　５０件）

(1) Tatsuya Kamiyama, Shoichi Maeyama, Kazuya Okawa, Keigo Watanabe and Yasuyuki Nogami,
“Recognition of parking spaces on dry and wet road surfaces using received light intensity of laser for ultra small EVs,”
Proceedings of the 2019 IEEE/SICE International Symposium on System Integration, pp.494-501, Paris, France, January 14-16, 2019. （査読有）

(2) Ryunosuke Isshiki, Kengo Iokibe, Takuya Kusaka, Tetsushi Kamegawa, Yasuyuki Nogami,
“Investigation of CAN Transceiver and Controller Response to Electromagnetic Disturbance by Using Current Injection Probe,”
EMC Joint Workshop 2018, Daejeon, EMCJ2018-59, pp. 23-28, Daejeon, Korea, Nov. 2018. （査読有）

〔図書〕（計　０件）

〔産業財産権〕
○出願状況（計　０件）

○取得状況（計　０件）

〔その他〕
ホームページ等
isec.ec.okayama-u.ac.jp/kagaku-jp 科研：基盤 a-2016-2018/

６．研究組織

(1)研究分担者
研究分担者氏名：日下 卓也
ローマ字氏名：Kusaka Takuya
所属研究機関名：岡山大学
部局名：自然科学研究科
職名：講師

研究者番号（8 桁）：00336918

研究分担者氏名：五百旗頭 健吾
ローマ字氏名：Iokibe Kengo
所属研究機関名：岡山大学
部局名：自然科学研究科
職名：助教
研究者番号（8 桁）：10420499

研究分担者氏名：荒木 俊輔
ローマ字氏名：Araki Shunsuke
所属研究機関名：九州工業大学
部局名：大学院情報工学研究院
職名：助教
研究者番号（8 桁）：20332851

研究分担者氏名：籠谷 裕人
ローマ字氏名：Kagotani Hiroto
所属研究機関名：岡山大学
部局名：自然科学研究科
職名：講師
研究者番号（8 桁）：50271060

研究分担者氏名：前山 祥一
ローマ字氏名：Maeyama Shoichi
所属研究機関名：香川大学
部局名：創造工学部
職名：教授
研究者番号（8 桁）：50292537

研究分担者氏名：中西 透
ローマ字氏名：Nakanishi Toru
所属研究機関名：広島大学
部局名：工学研究科
職名：教授
研究者番号（8 桁）：50304332

研究分担者氏名：亀川 哲志
ローマ字氏名：Kamegawa Tetsushi
所属研究機関名：岡山大学
部局名：ヘルスシステム統合科学研究科
職名：講師
研究者番号（8 桁）：80432623

研究分担者氏名：上原 聡
ローマ字氏名：Uehara Satoshi
所属研究機関名：北九州市立大学
部局名：国際環境工学部
職名：教授
研究者番号（8 桁）：90213389

(2)研究協力者
なし