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

平成　３０　年　　９　月　　７　日現在

機関番号：　２１６０２
研究種目：　若手研究(B)
研究期間：　2015～2017
課題番号：　１５Ｋ１６００５

研究課題名（和文）IoT環境向けの認証及びプライバシー保護手法

研究課題名（英文）Authentication and Privacy-preserving Technologies for IoT Environment

研究代表者
ＳＵ　Ｃｈｕｎｈｕａ（Su, Chunhua）

会津大学・コンピュータ理工学部・准教授

研究者番号：４０７１６９６６

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：IoT環境に使用されるデバイスの多くは計算能力に限りがあるため，既存のセキュリティ技術を使用して効率的に認証を行うことは困難である．また，従来の情報システムと異なりIoT環境のモビリティとソーシャルという特徴があり，接続デバイスから収集されるデータの活用時の発生したプラバイシ問題が複雑化となりつつある．本研究ではこれらの問題を解決するために，新しい技術を研究開発した．具体的に安全性と認証効率を取れたIoT機器のバッチ認証と生体認証方式を提案した．さらに、 IoT環境におけるプライバシを保護したIoTデータ収集・管理するフレームワークや侵入・異常検知システムを提案し，実装検証で有効性を示した．

研究成果の概要（英文）：Many of inter-connected devices used for IoT environments have restricted computing power and memory, so it is difficult to efficiently to execute secure authentication using conventional security techniques. Also, different from conventional information systems, the features of mobility and socialization in IoT environments, and security and privacy problems that occurred when utilizing data gathered from connected devices are getting more and more complicated. In this research, in order to solve these problems mentioned above, we have researched and developed new technologies for IoT authentication and privacy protection. Specifically, we proposed some batch authentication schemes and biometric authentication method for IoT devices achieving both security and efficiency. Furthermore, we proposed a framework to integrate intrusion and anomaly detection systems to collect and manage data privacy in IoT environment, and demonstrated its effectiveness in implementation verification.

研究分野：　情報セキュリティ

キーワード：　IoTセキュリティ　プライバシ保護　IoT機器認証

１．研究開始当初の背景

IoT アプリケーションの多様性から様々なセキュリティ上の研究課題が生まれている．本研究では、以下の二つの課題を注目する．

1. IoT 環境に向けたデバイス認証： RFID 技術は IoT 実現の中核技術の一つであり， IoT 環境の認証技術の代表例として挙げらる RFID 認証技術はすで長年に渡って研究されている．しかし，従来の計算機端末のセキュリティプロトコルと違い，IoT 環境では接続するデバイスが一括処理をする場合がことが多い．特に，物流業界で使われる RFID 管理システムやデータ観測機器のセンサーなどのデータ処理をする際に，同時に数多くのデバイスのから情報を読み取る場合がほとんどである．そのため，一括処理でデバイスの認証とその完全性を検証するプロトコルが必要になる．既存の提案手法では計算時間もかかりすぎで，実用ではないと指摘されている．セキュリティ・プライバシーの面を確保しながら，認証の効率を向上する認証方式に関する研究は必要になる．

2. IoT における集計データのプライバシ保護：IoT の世界では集めてきたデータを処理する際，プライバシーを保護する手法が必要である．しかし，守秘性の強度の立場からは優れているものの，計算量・通信量が多いため，未だ実用化されていない．特に大量のデータの処理に対するスケーラビリティがないと見なされる．実用化はまだ至ってないのは現状である．既存提案は単一のデータベースに対する提案であり，IoT 環境では多様なデータ（各種センサーからのデータ等，非構造なものも含む多種多様なデータ）と異種データベース（医療データベース，空間データベース，ウェブデータなど）間の連携処理が普通である．入力するデータ情報の提供時に利用者の匿名化処理が行われていたとしても，集まってきたデータの連携によって個人を特定したり，行動を推測したりできうるという特徴がある．

２．研究の目的

本研究の目的は Internet of Things（IoT）環境におけるモバイル・ウェアラブルデバイスを中心とした情報システムの認証およびプライバシー問題を研究し，軽量・高速化した新しい認証技術とデバイスが生成するデータの集計処理やモニターリングする際のプライバシー保護手法を提案することである．IoT 環境に使用されるデバイスの多くは計算能力に限りがあるため，既存のセキュリティ技術を使用して効率的に認証を行うことは困難である．また，従来の情報システムと異なり IoT 環境のモビリティとソーシャルという特徴があり，接続デバイスから収集されるデータの活用時の発生したプライバシーの問題が複雑化となりつつある．これらの問題の解決方式を提案する研究である．

３．研究の方法

本研究では，従来方式の問題点の解析，実用性と理論解析の両方を意識した IoT デバイスのバッチ認証プロトコル及びそのデータプライバシー保護手法の設計と安全性評価，計算機実験による性能評価および実験結果に基づくの再検討が主である．バッチ認証は各デバイスのデータの秘匿・暗号化（Encryption）とそのデータ整合性の検証(Verification)機能が必要とされている．応募者はこの問題を取り上げ，これまで従事してきた RFID システムの認証と共通鍵暗号の研究経験を生かし，認証暗号というデータ内容の秘匿と整合性の両方を同時に確保する共通鍵暗号アルゴリズム[5]の構成方法とその安全性分析を導入し，IoT デバイスのバッチ認証に応用できるように改善したいと考える.従来の認証方式では, 各デバイスはそれぞれに異なる秘密鍵を持つので，バッチ認証の検証を行う場合効率が悪い，しかし同じ鍵を持つと攻撃者が一つのデバイスの内部状態を取得すると全体の認証のセキュリティが破れる．応募者はセキュリティと検証効率を取れたバッチ認証方式を提案する．提案された方式をランダム関数あるいはランダム置換との識別不能性という仮定で安全性証明手法を取り入れ，バッチ内部の出力の衝突困難性と集計された認証子の適応的選択文書攻撃に対する攻撃者の偽造不能性を議論する．

４．研究成果

IoT 環境の認証技術の代表例として挙げらる RFID 認証技術はすで長年に渡って研究されている.従来の認証ロ トコルと違い，IoT 環境では接続するデバイスが一括処理をする場合がことが多い.そのため, 一括処理でデバイスの認証とその完全性を検証するプロトコルが必要になる.本年度の研究は RFID バッチ認証を行う際に汎用的結合可能性(Universal Composability)のモ デルで安全な相互認証プロトコルを提案した.我々の提案でバッチ処理に結合してもバッチ認証における全体として安全であることも 証明した.

次に IoT 機器から情報収集する際のプライバシー保護:信頼できないサーバから IoT 機器などのアクセスパターンを隠蔽するための Oblivious RAM(ORAM)を研究した.既存手法の問題点はモデルと実際のコンピュータに違いがあること，また実際の性能評価が行われていな いこと，そして，記憶領域などが一部理想化され，現在の ORAM アルゴリズムは依然として莫大な計算コストがか

かる．本研究は従来の パス型 ORAM の構築手法とアルゴリズムに焦点を当て，効率的なパス ORAM 実装手法を提案し，また存在する問題点を考察した.具体的に は，我々はサーバ上のブロックの重複を避けるためにAES を使用し, 暗号化モードの選択による違う効果を分析した.また，我々は通 信のオーバーヘッドを減らすためにクライアント上のローカルキャッシュを使用し, パス ORAM の改良案を提案した．また IoT 向けの共通鍵暗号技術の安全性解析:最近注目されている IoT 機器向けの共通鍵暗号とアプリケーションに対して，より厳密的な暗号解析を行うことにより，既存の安全性評価の精確性を向上さた.本研究では統計学の手法を導入して IoT 軽量化暗号安全性解析に関する差分パス探索のアルゴリズムの効率の改善案を提案した．IoT 機器などの計算能力とストレージ容量の少ないクライアント端末向けの(Recursive Matrix ORAM) RM- ORAM を提案した.我らの提案ではサーバー側の暗号化したポジションマップの再帰構造を構築し，クライアント側のデータ構造(スタッシュ)の最適化を行う .提案では従来の M-ORAM よりクライアントのストレージ・スペースは従来の ORAM O(N)から O(logN)に減らすことができた.そのほかに IoT データのプライバシ保護手法も提案した.

大量 IoT デバイス間のリアルタイムデータ通信と計算を円滑に行うために，まず高速化かつ軽量化した共通鍵暗号アルゴリズムを研究し, 高速化を確保する上に H28 年度の後半は CPU パワーやメモリなどが制限される IoT デバイスにおいても，高度なセキュリティを 実現できる軽量化認証暗号を提案した．また，開発した IoT デバイス向けに共通鍵暗号方式の実装検証とそれに基づいた IoT 機器の認証 方式も行った.具体的に IoT デバイスまたはインテリジェントモバイルデバイス用の軽量暗号の効率的で安全な実装検証を行い，既存 軽量ブロック暗号の差分攻撃、線形攻撃の視点から研究を展開し，IoT 認証へ応用も行った.既存の軽量化暗号を差分解読法，線形解 読法などの手法を使って攻撃分析を行い，そのセキュリティ上の弱点を探る.それらの提案の弱点を避けて, それを基いてプログラムや回路規模をさらに，小型センサなどより低コストデバイスへの実装性を向上でき，医療用の認証システムや RFID に利用して，より実 用性のある共通鍵暗号基づいた IoT 機器を認証方式を提案した．さらに IoT デバイスなどで生成したデータを複数の機関の間に利活用するためのプライバシ保護手法も提案した.

最後にデータ内容の秘匿と整合性の両方を同時に確保する軽量化共通鍵暗号アルゴリズムを提案した.その上に IoT 機器の安全認証システムを提案し，プロタイプを 実現した.さらに，IoT データの安全収集と保存の並列暗号処理やプライバシ保護技術のを提案し，実装検証を行った.主に以下の 3 つの成果が得られた．1 つ目は我々はより効率的で大規模な IoT データ暗号化と認証処理に適するノンス依存方式と確率的暗号方式について考察し，二つの新しい方式を提案した．並 列処理モードで動作し，セキュリティはランダム生成したノンスに基づいており，関連データをサポートする.さらに，セキュリティモデルの構築が弱いが，高 速で軽量化した解決策を提案した.2 つ目はウェアラブルヘルスケアに関連するスマートオブジェクトを所有するユーザーとの IoT ベース環境の継続的な認証方式を提案した.新しいバイオメトリ クスの特性を導入し，市販の圧力センサーと Raspberry PI プラットフォームを介して構築された着用可能な足底の生体特徴抽出器を構築してプロタイプを作っ た．さらに IoT ベースのネットワークの侵入・異常検知システムが提案した．3 つ目は我々は PrivacyBat という BLE ベースのアプリケーションのプライバシ管理するフレームワークを提案した.このフレームワークは、ユーザーが近くの BLE デバイスとのプライバシに関する合意を達成するための仕様を定義してい，さらに、IoT デバイスが契約に従ってユーザーの要求を処理するためのガイドライン を提供した.フレームワークがどのように動作するかを実証するために，実装実証をさらに行った.我々が提案されたフレームワークは IoT アプリケーションに おけるプライバシーポリシ合意プロセスを改善することができるので，IoT アプリケーションに対するユーザーの信頼性向上に貢献した．IoT 環境では，高精度かつ高頻度にデバイスの位置を測位やデバイスデータをデータマイニングをする際にデバイスを所有する個人のプラバイシが侵害される可能性がある．既存の方式は一つのプロトコルにおけるプラバイシ問題のみを考え，そのプロトコルと同じデータソースを利用するほか複数のプロトコルの関連情報からのプラバイシー漏えい問題は考えていない．IoT 環境が生成する大量のデータを処理（データマイニングなど）際，攻撃者が複数の IoT データ処理プロトコルを参加しても，プラバイシー情報の相関性を最小限にすることで，十分な匿名性や個人情報保障することができるデータプラバイシー保護技術の提案する.

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　16　件）

1. Kuo-Hui Yeh, Chunhua Su, Wayne Chiu, Lu Zhou. “I Walk, Therefore I Am: Continuous User Authentication with Plantar Biometrics”, IEEE Communication Magazine, vol.56 (2). Pp.150-157, 2018.
2. Lu Zhou, Chunhua Su, Kuo-Hui Yeh and Wayne Chiu. “You Think, Therefore You

Are: Transparent Authentication System with Brainwave-oriented Bio-features for IoT Networks". IEEE Transactions on Emerging Topics in Computing, In Press 2018.
3. Shi-Cho Cha, Jyun-Fu Chen, Chunhua Su, Kuo-Hui Yeh. "A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things." IEEE Access Vol.6, pp.24639-24649, 2018.
4. Shi-Cho Cha, Ming-Shiung Chuang, Kuo-Hui Yeh, Zijia Huang, Chunhua Su. "A User-Friendly Privacy Framework for Users to Achieve Consents With Nearby BLE Devices". IEEE Access Vol.6, pp.20779-20787, 2018.
5. Wenjuan Li, Weizhi Meng, Chunhua Su, Lam For Kwok. "Towards False Alarm Reduction Using Fuzzy If-Then Rules for Medical Cyber Physical Systems". IEEE Access 6, pp.6530-6539, 2018
6. Weizhi Meng, Wenjuan Li, Chunhua Su, Jianying Zhou, and Rongxing Lu "Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data", IEEE Access Vol.6, pp.7234-7243, 2018.
7. Rashed Mazumder, Atsuko Miyaji, Chunhua Su. "Probably Secure Keyed-Function based Authenticated Encryption Schemes for Big Data", International Journal of Foundations of Computer Science, In press, September Issue, 2017.
8. Steven Gordon, Xinyi Huang, Atsuko Miyaji, Chunhua Su, Karin Sumongkayothin, Komwut Wipusitwarakun. "Recursive Matrix Oblivious RAM: An ORAM Construction for Constrained Storage Devices". IEEE Transaction of Information Forensics and Security 12(12), pp.3024-3038, Dec, 2017.
9. Jiageng Chen, Jesen Teh, Zhe Liu, Chunhua Su, Azman Samsudin, Yang Xiang. "Towards Accurate Statistical Analysis of Security Margins: New Searching Strategies for Differential Attacks", IEEE Transactions on Computers, Volume: 66, Issue: 10, pp.1763 – 1777, 2017
10. Rashed Mazumder, Atsuko Miyaji, Chunhua Su, "A simple authentication encryption scheme", Concurrency and Computation: Practice and Experience, Volume 29, Issue 16, August 2017.
11. Kuo-Hui Yeh, Nai-Wei Lo, Ren-Zong Kuo*, Chunhua SU, Hsuan-Yu Chen, "Formal Analysis on RFID Authentication Protocols against De-synchronization Attack," Journal of Internet Technology, In press, Vol.18 No.4, July 2017.
12. Kuo-Hui Yeh, Chunhua Su, Kim-Kwang Raymond Choo, Wayne Chiu, "A Novel Certificateless Signature Scheme for Smart Objects in the Internet- of-Things", Sensors. 2017; Vol.17, No.5, 1001, 2017.
13. Jiageng Chen, Rashed Mazumder, Atsuko Miyaji, Chunhua Su. "Variable Message Encryption through Blockcipher Compression Function", Concurrency and Computation: Practice and Experience, Vol 29. No.7, 2017.
14. Chunhua Su, Bagus Santoso, Yingjiu Li, Robert H. Deng, Xinyi Huang. "Universally Composable RFID Mutual Authentication". IEEE Transactions on Dependable and Secure Computing, Vol. 14, Issue 1, pp. 83-94, 2017.
15. Steven Gordon, Atsuko Miyaji, Chunhua Su, Karin Sumongkayyothin, "A Matrix based ORAM: Design, Implementation and Experimental Analysis". Vol.E99-D, No.8,pp.2044-2055, Aug. 2016.
16. Xu Yang, Xinyi Huang, Jinguang Han and Chunhua Su. "Improved Handover Authentication and Key Pre-distribution for Wireless Mesh Networks". Concurrency and Computation: Practice and Experience. pp. 2978–2990, Vol. 28, Issue 10, July 2016.

〔学会発表〕（計 21 件）

1. Yidan Zhang, James Silver, Jiageng Chen, Chunhua Su and Jinguang Han "Smart encryption scheme based on the neural networks: analysis and discussions on various adversarial models". ISPEC 2017, LNCS 10701, 2017.
2. Weizhi Meng, Wang Hao Lee, Zhe Liu, Chunhua Su and Yan Li. "Evaluating the Impact of Juice Filming Charging Attack in Practical Environments", ICICS 2017 Dec 2017.
3. Lijun Jiang, Weizhi Meng, Yu Wang, Chunhua Su, Jin Li. "Exploring Energy Consumption of Juice Filming Charging Attack on Smartphones: A Pilot Study". NSS 2017, LNCS10394 pp.199-213, Finland, 2017.
4. Hiroshi Nomaguchi, Atsuko Miyaji, Chunhua Su. Evaluation and Improvement of Pseudo-Random Number Generator for EPC Gen2. TrustCom 2017, IEEE press pp.721-728, Australia, 2017
5. Ye Li, Kaitai Liang, Chunhua Su and Wei Wu. DABEHR: Decentralized Attribute-Based Electronic Health Record System with Constant-Size Storage

Complexity, The 12th International Conference on Green, Pervasive and Cloud Computing. Amalfi Coast, Italy, May, 2017.
6. Rashed Mazumder, Atsuko Miyaji, Chunhua Su. “A Simple Construction of Encryption for a Tiny Domain Message”, The 51st Annual Conference on Information Sciences and Systems, Baltimore, USA, March, 2017.
7. Yaoan Jin, Chunhua Su, Na Ruan, Weijia Jia, “Privacy-preserving Mining of Association Rules for Horizontally Distributed Databases based on FP-tree”, The 12th International Conference on Information Security Practice and Experience (ISPEC 2016), Springer, LNCS, Vol. 10060, pp 300-314, Zhangjiajie, China, November, 2016.
8. Kuo-Hui Yeh, Chunhua Su, Chien-Lung Hsu, Wayne Chiu, Yu-Fan Hsueh. “Transparent Authentication Scheme with Adaptive Biometric Features for IoT Networks”, 2016 IEEE 5th Global Conference on Consumer Electronics.
9. Karin Sumongkayothin, Steven Gordon, Miyaji Atsuko, Chunhua Su and Komwut Wipusitwarakun, “Recursive M-ORAM: A Matrix ORAM for Clients with Constrained Storage Space”. The 2016 International Conference on Applications and Technologies in Information Security (ATIS), Springer, Vol 651 of the series Communications in Computer and Information Science, pp. 130-141, Cairns, Australia.
10. Rashed Mazumder, Atsuko Miyaji and Chunhua Su (30%). “An Efficient Construction of a Compression Function for Cryptographic Hash”, International Cross Domain Conference and Workshop (CD-ARES 2016), Springer, LNCS, Vol. 9817, PP. 124-140, Viena, Australia, August 2016.
11. Rashed Mazumder, Atsuko Miyaji and Chunhua Su (30%). “A Blockcipher based Authentication Encryption”. International Cross Domain Conference and Workshop (CD-ARES 2016), Springer, LNCS, Vol. 9817, PP. 106-123, Viena, Australia, August 2016.
12. Jiageng Chen, Jesen Teh, Chunhua Su (20%), Azman Samsudin, Junbin Fang. “Improved (related-key) Attacks on Round-Reduced KATAN-32/48/64 Based on the Extended Boomerang Framework”. 21st Australasian Conference on Information Security and Privacy (ACISP 2016), pp. 333-346, Melbourne, Australia, July 2016.
13. Kaitai Liang, Atsuko Miyaji, Chunhua Su (50%). “Secure and Traceable Framework for Data Circulation”. 21st Australasian Conference on Information Security and Privacy (ACISP 2016), pp.376-388, Melbourne, Australia.
14. Kaitai Liang, Chunhua Su (30%), Jiageng Chen and Joseph K. Liu, “Efficient Multi-Function Data Sharing and Searching Mechanism for Cloud-Based Encrypted Big Data”, The 11th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2016), pp. 83-94, XiAn, China, May 2016
15. Steven Gordon, Atsuko Miyaji, Chunhua Su and Karin Sumongkayyothin, “Security and Experimental Performance Analysis of a Matrix ORAM", International Conference on Communication (ICC 2016), pp.1-6, 2016.
16. Jiageng Chen, Atsuko Miyaji, Chunhua Su and Je Sen Teh, ``Accurate Estimation of the Full Differential Distribution for General Feistel Structures", The 11th China International Conference on Information Security and Cryptology (Inscrypt 2015), LNCS, Beijing, China, December 2015.
17. Jiageng Chen, Atsuko Miyaji, Chunhua Su, Jesen Teh. "Improved Differential Characteristic Searching Methods," in 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud), pp.500-508, New York, USA, November 2015.
18. Jiageng Chen, Atsuko Miyaji, Chunhua Su and Liang Zhao. " A New Statistical Approach for Integral Attack ". The 9th International Conference on Network and System Security (NSS 2015), LNCS, Volume 9408, pp.345-356, November, New York, USA, 2015.
19. Steven Gordon, Atsuko Miyaji, Chuhua Su, Karin Sumongkayyothin. “Analysis of Path ORAM toward Practical Utilization.” The 18th International Conference on Network-Based Information Systems (NBiS),, pp. 646-651, Taipei, September, 2015.
20. Steven Gordon, Atsuko Miyaji, Chunhua Su and Karin Sumongkayothin, ``M-ORAM: A Matrix ORAM with logN bandwidth cost", The 16th International Workshop on Information Security Applications (WISA 2015), LNCS, Jeju, Korea, August 2015.
21. Jiageng Chen; Atsuko Miyaj, Hiroyuki Sato, Chunhua Su , "Improved Lightweight Pseudo-Random Number Generators for the Low-Cost RFID Tags," in Trustcom 2015 IEEE , vol.1, no., pp.17-24, Helsinki,

Finland, August 2015.

〔図書〕（計　　件）

〔産業財産権〕

○出願状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
Su Chunhua（蘇　春華）
会津大学・コンピュータ理工学部・准教授
研究者番号：
40716966