様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ３ 日現在

機関番号：１３３０２
研究種目：基盤研究(A)
研究期間：2009～2014
課題番号：２１２４０００１

研究課題名（和文）センサネットワークの安全・安心を保証する情報セキュリティ技術の研究

研究課題名（英文）Study on secure and safety technology for sensor networks

研究代表者
宮地　充子（Miyaji, Atsuko）

北陸先端科学技術大学院大学・情報科学研究科・教授

研究者番号：１０３１３７０１

交付決定額（研究期間全体）：（直接経費）　　35,700,000円

研究成果の概要（和文）：近年，機器の小型化や省電力化に伴い，各機器をセンサネットワークで認証・接続し，情報の共有や処理を行うアプリケーションが期待されている．その際，共有情報のグループ外での秘匿化，完全性保証が信頼性確保のためには必須である．本研究では，①非均質型端末間のグループ鍵共有プロトコル②鍵共有におけるハッシュ関数の応用③形式言語による安全性証明④安全なグループ鍵共有方式のシミュレーション を行い，特に端末の能力に応じたフレキシブルなネットワークで，受動攻撃モデルで安全なグループ鍵共有方式を構築した．さらにT(<n)端末の故障に対しても安全な鍵共有方式も提案した．

研究成果の概要（英文）：Wireless Sensor Networks (WSNs) consist of battery-operated, limited memory and computational power sensor nodes. It is important to achieve secure communication among WSN. In this research, we have studied a group key exchange (GKE), application of hash functions to GKE, formal security proof, and simulation of GKE. The following are our results. 1.We have proposed T-robust scalable GKE with communicational and computational complexity O(log n) for n parties. Our GKE not only has a resistance to party failures resulting from party crashes, run-down batteries, and network failures, but also satisfies scalability to parties' environment such as computational resources, batteries, etc. 2.We have redesigned GKE using bilinear pairings to reduce the computational and communicational complexity among a small group of parties. We have also redesigned GKE among a large number of parties, where each party is in a different environment.

研究分野：情報セキュリティ

キーワード：暗号・認証等　センサーネットワーク

１．研究開始当初の背景

近年，機器の小型化や省電力化に伴い，各機器をセンサネットワークで認証・接続し，無線通信で各種データを収受するアプリケーションの活用が動き出しつつある．特に，複数端末がセンサネットワークを通して情報の共有や処理を行う健康機器センサの統合管理システムのようなアプリケーションへの期待は大きい．その際，共有情報のグループ外での秘匿化，共有情報の完全性の保証がアプリケーションの信頼性確保のためには必須といえる（図 1）．またセンサネットワークの端末認証では，各端末はアドホックなネットワークを構成するため情報共有のグループがダイナミックに変更する，各端末の計算能力が一定でない，通信チャネルが不安定なため送受信パケット数を抑える必要があるなど，独自の問題も多い．

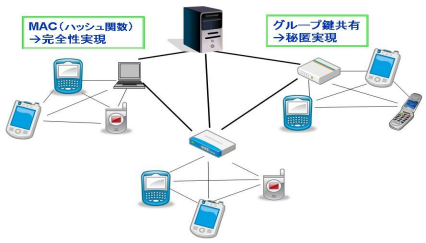

図 1　研究目的の概念

２．研究の目的

本研究開発において以下の研究を行う．

①非均質型端末間のグループ鍵共有プロトコルの構築と可能性

②鍵共有におけるハッシュ関数の応用

③形式言語による安全性証明

④センサネットワークでの安全なグループ鍵共有方式のシミュレーション

３．研究の方法

4 つの研究目的に対して，以下の手法で研究を進めた．

①では非均質型端末間のグループ鍵共有プロトコルを構築する．また本研究開発においては，『任意のネットワークトポロジーのグループが鍵を共有できるか？』という未解決問題についても取り組み，グループ鍵共有が実現できるネットワークトポロジーについて明らかにする．

②では，ハッシュ関数を利用して，従来方式よりも高効率でかつ安全性が証明により保証される MAC 関数，鍵導出関数，擬似乱数生成器を構成する．

③では，プルーフチェッカ Mizar を用いてグループ鍵共有プロトコル安全性証明を行うための数学ライブラリの開発と上記①，②の成果の計算機援用による証明を行う．

④では，ネットワークシミュレータ NS-2 [5] を利用して，本研究で提案するプロトコルの実装およびシミュレーションを行う．

４．研究成果

①では，端末の能力に応じた任意の(n1，n2)型ネットワーク（低能力端末数 n1，高能力端末数 n2）のグループ鍵共有を行うペアリングベースの方式を構築し，受動攻撃モデルで安全性を証明．次に任意の T(<n)端末が故障した際に O(Logn+T) の性能で鍵共有が可能な T 耐故障-鍵共有方式を提案し，受動攻撃モデルで安全性を証明．耐故障数 T に対しシステマティックに端末配置を行う方法も構築．両方式は KY 変換により，能動攻撃に安全な方式に変換することも可能である．

②では，センサネットワークでのハッシュ関数の利用においては計算資源に制約のある環境でも効率よく処理可能であること（軽量性）が重要である．本課題では，ハードウェア資源の節約の観点からブロック暗号を用いたハッシュ関数の構成に着目し，ブロック暗号として AES と PRESENT を利用した倍ブロックハッシュ関数の衝突計算困難性を攻撃の観点から明らかにした．

③では，グループ鍵共有方式におけるシミュレーション:センサネットワークのグループ鍵共有・鍵配送の提案方式を安全性や効率の観点から，シミュレーションによる評価を実施．新たにグループ鍵配送方式を提案し，さらにハッシュ連鎖を柔軟に構成することで，VANET (Vehicular Adhoc Networks) における効率のよいグループ認証方式を研究開発した．

④では，本研究課題で提案する鍵共有プロトコルの形式検証に利用可能な、暗号理論のための様々な数学的諸定理，ガウス整数環に関する諸定理，有限離散標本空間上の条件付き確率および確率分布, Z-加群, 共通鍵暗号 AES 暗号の形式記述，数論アルゴリズムに関する諸定理について自動証明検証システムを利用した形式定義ライブラリを作成した．

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 74 件）

1. A. Miyaji and K. Omote, Self-healing Wireless Sensor Networks, Concurrency and Computation: Practice and Experience, 査読有, 2015, DOI: 10.1002/cpe.3434.
2. Jiageng Chen, K. Emura, and A. Miyaji, SKENO: Secret Key Encryption with Non-interactive Opening, Journal of Mathematical Cryptology, 査読有, 2014, DOI: 10.1515/jmc-2014-0010.
3. K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, Generic Constructions of Secure-Channel Free Searchable Encryption with Adaptive Security, Wiley Security and Communication Networks, 査読有, 2014, DOI: 10.1002/sec.1103.

4. 宮地充子, ユビキタスネットワークにおけるセキュリティ技術－ 積極的利用を促すセキュリティ技術－, 「電気評論」, 査読有, 夏季増刊号特集, 2014, pp.12-15.
5. Ryoma Ito, and A. Miyaji, How TKIP downgrades security of generic RC4, The 20th ACISP 2015, LNCS, Springer-Verlag, 査読有, 2015, 印刷中.
6. Ryoma Ito, and A. Miyaji, New Linear Correlations related to State Information of RC4 PRGA using Ⅳ in WPA, The 22nd FSE 2015, LNCS, Springer-Verlag, 査読有, 2015, 印刷中.
7. A. Miyaji and Mazumder Rashed, A new (n, 2n) Double Block Length Hash Function based on Single Key Scheduling, The 29th AINA2015, IEEE, 査読有, 2015, pp.546-570.
8. Jiageng Chen, Shoichi Hirose, Hidenori Kuwakado, and A. Miyaji, A Collision Attack on a Double-Block-Length Compression Function Instantiated with Round-Reduced AES-256, The 17th ICISC 2014, LNCS, Springer-Verlag, 査読有, 8949, 2015, pp.271-285.
9. A. Miyaji and Mazumder Rashed, A new (n; n) blockcipher hash function using Feistel Network: Apposite for RFID Security, ICCIDM 2014, LNCS, Springer-Verlag, 査読有, Volume 33, 2015, pp.519-528.
10. A. Miyaji, Mazumder Rashed and Tsuyoshi Sawada, A new (n; n) Blockcipher based Hash Function for Short Messages, ASIA JCIS, IEEE,査読有, 2014, pp.56-63.
11. Ryoma Ito, and A. Miyaji, New Integrated Long-Term Glimpse of RC4, The 15th WISA 2014, LNCS, Springer-Verlag, 査読有, 8909, 2015, pp.137-149.
12. Jiageng Chen, A. Miyaji, and Chunhua Su, A Provable Secure Batch Authentication Scheme for EPCGen2 Tags, The 8th Provsec 2014, LNCS, Springer-Verlag, 査読有, 8782, 2014, pp.103-116.
13. Jiageng Chen, Y. Futa, A. Miyaji, and Chunhua Su, Improving impossible differential cryptanalysiswith concrete investigation of key schedulingalgorithm and its application to LBlock, The 8th NSS 2014, LNCS, Springer-Verlag, 査読有, 8792, 2014, pp.184-197.
14. Mohammad Saiful Islam Mamun and A. Miyaji, Secure VANET Applications with a rened Group Signature, 2014 Twelfth PST, 査読有, 2014, pp.199-206.
15. Mohammad Saiful Islam Mamun, A. Miyaji, and Hiroaki Takada, A multi-purpose Group Signature for Vehicular Network Security, 17th NBiS, 査読有, 2014, pp.511-516.
16. Cheng-Qiang Huangy, A. Miyaji, Long-Hai Li, and Shang-Mei Xu, POND: A Novel Protocol for Network Coding based on Hybrid Cryptographic Scheme, 2014 IEEE International Conference CIT, 査読有, 2014, pp.373-380.
17. Jiageng Chen, A. Miyaji, and Chunhua Su, Distributed Pseudo-Random Number Generation and its application to Cloud Database, The 10th ISPEC 2014, LNCS, Springer-Verlag, 査読有, 8434、2014, pp.373-387.
18. Mohammad Saiful Islam Mamun and A. Miyaji, A Scalable and Secure RFID Ownership Transfer Protocol, The 28th IEEE International Conference AINA 2014, IEEE, 査読有, 2014, pp.343-350.
19. Mohammad Saiful Islam Mamun and A. Miyaji, RFID Path Authentication, Revisited, The 28th IEEE International Conference AINA2014, IEEE, 査読有, 2014, pp.245-252.
20. 小林哲也, 廣瀬勝一, 段数を削減したPRESENTを用いた倍ブロック長圧縮関数に対する衝突攻撃, 電子情報通信学会論文誌 A, 査読有, J96-A, 2013, pp. 541-550.
21. Y. Futa, H. Okaszaki, Yasunari Shidama, Submodule of free Z-module, Formalized Mathematics, 査読有, 21(4), 2014, pp. 275-284, DOI: 10.2478/forma-2013-0029.
22. Kenichi Arai, H. Okaszaki, Formalization of the Advanced Encryption Standard. Part I, Formalized Mathematics, 査読有, 21(3), 2013, pp. 171-184, DOI: 10.2478/forma-2013-0019.
23. Y. Futa, H. Okaszaki, Daich Mizushima, Yasunari Shidama, Formal Definition of Probability on Finite and Discrete Sample Space for Proving Security of Cryptographic Systems Using Mizar, Artificial Intelligence Research, 査読有, 2(４), 2013, pp. 37-48, DOI: 10.5430/air.v2n4p37.
24. Jiageng Chen and A. Miyaji, Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock, CD-ARES 2013 Workshops, LNCS, Springer-Verlag, 査読有, 8123, 2013, pp.1-5.
25. Mohammad Saiful Islam Mamun and

A. Miyaji, A fully-secure RFID authentication protocol from exact LPN assumption, The 12th IEEE TrustCom'13, IEEE, 査読有, 2013, pp.102-109.
26. K. Emura, A. Miyaji and M. S. Rahman, Private Multiparty Set Intersection Protocol in Rational Model, The 12th IEEE TrustCom'13, IEEE, 査読有, 2013, pp.431-438.
27. Y. Futa, H. Okaszaki, Yasunari Shidama, Formalization of Definitions and Theorems Related to an Elliptic Curve Over a Finite Prime Field by Using Mizar, Journal of Automated Reasoning, 査読有, 50(2), 2013, pp.161-172, DOI: 10.1007/s10817-012-9265-2.
28. Y. Futa, H. Okaszaki, Yasunari Shidama, Free Z-module, Formalized Mathematics, 査読有, 20(4), 2013, pp. 275-280, DOI: 10.2478/v10037-012-0030-0.
29. Y. Futa, H. Okaszaki, Yasunari Shidama, Quotient Module of Z-module, Formalized Mathematics, 査読有, 20(3), 2013, pp. 205-214, DOI: 10.2478/v10037-012-0024-y.
30. H. Okaszaki, Yoshiki Aoki,Yasunari Shidama, Extended Euclidean Algorithm and CRT Algorithm, Formalized Mathematics, 査読有, 20(2), 2013, pp. 175-179, DOI: 10.2478/v10037-012-0020-2.
31. Atsushi Waseda and M. Soshi, Consideration for multi-threshold multi-secret sharing schemes, ISITA 2012, 査読有, 96-A, 2012, pp. 265-269.
32. Kazuya Izawa, A. Miyaji and K. Omote, Lightweight Integrity for XOR Network Coding in Wireless Sensor Networks, The 8th ISPEC 2012, 査読有, 2012, pp. 245-258.
33. Mohammad Saiful Islam Mamun and A. Miyaji, An Optimized Signature Verication System for Vehicle Ad hoc NETwork, The 8th WiCOM, 査読有, 2012, pp.1-8.
34. Mohammad Saiful Islam Mamun, A. Miyaji, and M. S. Rahman, A Secure and private RFID authentication protocol under SLPN problem, The 6th NSS 2012, LNCS, 査読有, 7645, 2012, pp.476-489.
35. A. Miyaji and Yiren Mo, How to Enhance the Security on the Least Signi_cant Bit, *The 11th CANS 2012*, LNCS, 査読有, 7712, 2012, pp.263-279.
36. A. Miyaji and Phuong Viet Xuan TRAN, Constant-Ciphertext-Size Dual Policy Attribute Based Encryption, *The 4th CSS 2012*, LNCS, 査読有, 7672, 2012, pp.400-413.
37. Tomoyuki Karasawa, M. Soshi and A. Miyaji, A Novel Hybrid IP Traceback Scheme with Packet Counters, *The 5th IDCS 2012*, LNCS, 査読有, 7646, 2012, pp.71-84.
38. Tatsuro Iida, K. Emura, A. Miyaji and K. Omote, An Intrusion and Random-Number-Leakage Resilient Scheme in Mobile Unattended WSNs, The 8th AINA 2012 Workshops, HWISE 2012, 査読有, 2012, pp.552-557.
39. A. Miyaji and M. S. Rahman, Privacy-preserving Set Operations in the Presence of Rational Parties, *The 5th AINA 2012 Workshops*, MAW 2012, 査読有, pp.869-874.
40. K. Emura, A. Miyaji, and K. Omote, A Revocable Group Signature Scheme with the Property of Hiding the Number of Revoked Users, *The 14th ICISC 2011*, LNCS, 査読有, 7259, 2012, pp.186-203.
41. K. Emura, A. Miyaji, Akito Nomura, M. S. Rahman, and M. Soshi, Ideal Secret Sharing Schemes with Share Selectability, The 13th ICICS 2011, LNCS, 査読有, 7043, 2011, pp.143-157.
42. Kai-Yuen Cheong and A. Miyaji, Unconditionally Secure Oblivious Transfer Based on Channel Delays, The 13th ICICS 2011, LNCS, 査読有, 7043, 2011, pp.112-120.
43. Tatsuro Iida, A. Miyaji, and K. Omote, POLISH: Proactive co-Operative LInk Self-Healing for Wireless Sensor Networks, *The 13th SSS 2011*, LNCS, 査読有, 6976, 2011, pp.253-267.
44. K. Emura, A. Miyaji, and K. Omote, Adaptive Secure-Channel Free Public-Key Encryption with Keyword Search Implies Timed Release Encryption, The 14th ISC 2011, LNCS, 査読有, 7001, 2011, pp.102-118.
45. Jiageng Chen and A. Miyaji, How to Find Short RC4 Colliding Key Pairs, *The 14th ISC 2011*, LNCS, 査読有, 7001, 2011, pp.32-46.
46. A. Miyaji and M. S. Rahman, Privacy-Preserving Data Mining: A Game-theoretic Approach, The 25th IFIP WG 11.3 DBSEC 2011, LNCS, 査読有, 6818, 2011, pp.186-200.
47. K. Emura, A. Miyaji, and M. S. Rahman, Toward Dynamic Attribute-Based Signcryption (Poster), The 16th ACISP 2011, LNCS, 査読有,

6812, 2011, pp.439-443.

48. Tetsuya Hatano, A. Miyaji, and Takashi Sato, T-Robust Scalable Group Key Exchange Protocol with O(log n) complexity, The 16th ACISP 2011, LNCS, **査読有**, 6812, 2011, pp.189-207.
49. Y. Futa, H. Okaszaki, Yasunari Shidama, Set of Points on Elliptic Curve in Projective Coordinates, Formalized Mathematics, **査読有**, 19, 2011.
50. H. Okaszaki, Kenichi Arai, Yasunari Shidama, Normal Subgroup of Product of Groups, Formalized Mathematics, **査読有**, 19, 2011.
51. Jiageng Chen and A. Miyaji, A New Class of RC4 Colliding Key Pairs With Greater Hamming Distance, The 6th ISPEC 2010, LNCS, **査読有**, 6047, 2010, pp.30-44.
52. Raveen Ravinesh Goundar, Marc Joye, and A. Miyaji, Co-Z Addition Formulae and Binary Ladders on Elliptic Curves, The 12th CHES 2010, LNCS, **査読有**, 6225, 2010, pp.65-79.
53. Jiageng Chen and A. Miyaji, Generalized RC4 Key Collisions and Hash Collisions, The 7th SCN 2010, LNCS, **査読有**, 6280, 2010, pp.73-87.
54. K. Emura, A. Miyaji, and K. Omote, An Anonymous Designated Verier Signature Scheme with Revocation: How to Protect a Company's Reputation, The 4th ProvSec 2010, LNCS, **査読有**, 6402, 2010, pp.184-198.
55. K. Emura, A. Miyaji, and K. Omote, A Timed-Release Proxy Re-Encryption Scheme and its Application to Fairly-Opened Multicast Communication, The 4th ProvSec 2010, LNCS, **査読有**, 6402, 2010, pp.200-213.
56. Hisashige Ito, A. Miyaji, and K. Omote, RPoK: A Strongly Resilient Polynomial-based Random Key Pre-distribution Scheme for Multiphase Wireless Sensor Networks, The 8th IEEE GLOBECOM 2010, **査読有**, 2010, pp.1-5.
57. K. Emura, A. Miyaji, and K. Omote, An Identity-based Proxy Re-Encryption Scheme with Source Hiding Property, and its Application to a Mailing-list System, The 7th EuroPKI 2010, LNCS, **査読有**, 6711, 2011, pp.77-92.
58. A. Miyaji, M. S. Rahman, and M. Soshi, Hidden Credential Retrieval Without Random Oracles, The 11th WISA 2010, LNCS, **査読有**, 6513, 2010, pp.160-174.
59. A. Miyaji and K. Omote, Efficient and Optimally Secure In-Network Aggregation in Wireless Sensor Networks, The 11th WISA 2010, LNCS, **査読有**, 6513, 2010, pp.135-149.
60. A. Miyaji and M. S. Rahman, APRAP: Another Privacy Preserving RFID Authentication Protocol, The 6th NPSec 2010, IEEE, **査読有**, 2010, pp.13-18.
61. A. Miyaji and M. S. Rahman, Privacy-Preserving Data Mining in Presence of Covert Adversaries, The 6th ADMA 2010, LNCS, **査読有**, 6440, 2010, pp.429-440.
62. K. Emura, A. Miyaji, and M. S. Rahman, Efficient Privacy-Preserving Data Mining in Malicious Model, The 6th ADMA 2010, LNCS, **査読有**, 6440, 2010, pp.370-382.
63. Jiageng Chen and A. Miyaji, A New Practical Key Recovery Attack on the Stream Cipher RC4 under Related-Key Model, The 6th Inscrypt 2010, LNCS, **査読有**, 6584, 2011, pp.62-76.
64. Yvo Desmedt and A. Miyaji, Redesigning Group Key Exchange Protocol based on Bilinear Pairing Suitable for Various Environments, The 6th Inscrypt 2010, LNCS, **査読有**, 6584, 2011, pp.236-254.
65. K. Emura, A. Miyaji and K. Omote, A Selectable k-Times Relaxed Anonymous Authentication Scheme, The 10th WISA 2009, LNCS, **査読有**, 5932, 2009, pp.281-295.
66. K. Emura, A. Miyaji and K. Omote, A Ciphertext-Policy Attribute-Based Encryption Scheme with Strong Recipient Anonymity, IWSEC 2009, **査読有**, 2009, pp.49-63.
67. A. Miyaji and Masahiro Sukegawa, New Correlations of RC4 PRGA Using Nonzero-Bit Differences, The 14th ACISP 2009, LNCS, **査読有**, 5594, 2009, pp.134-152.
68. Shoujirou Hirasawa and A. Miyaji, Elliptic Curves with a Pre-determined Embedding Degree, The 2009 IEEE ISIT 2009, **査読有**, 2009, pp. 2391-2395.
69. K. Emura, A. Miyaji, Akito Nomura, K. Omote, and M. Soshi, A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length, The 5th ISPEC 2009, LNCS, **査読有**, 5451, 2009, pp.13-23.
70. K. Emura, A. Miyaji and K. Omote, A Dynamic Attribute-Based Group Signature Scheme and Its Application in an Anonymous Survey for the

Collection of Attribute Statistics, The Forth AReS 2009, IEEE, 査読有, pp.487-492.
71. K. Emura, A. Miyaji and K. Omote, A Certicate Revocable Anonymous Authentication Scheme with Designated Verier, The First RIBC 2009, IEEE, 査読有, 2009, pp.769-773.
72. M. S. Rahman, M. Soshi and A. Miyaji, A Secure RFID Authentication Protocol with Low Communication Cost, The 3rd IMIS 2009, IEEE, 査読有, 2009, pp.559-564.
73. S. Hirose and H. Kuwakado, Efficient Pseudorandom-Function Modes of a Block-Cipher-Based Hash Function, IEICE Transactions on Fundamentals, 査読有, E92-A, 2009, pp.2447-2453.
74. H. Okazaki, Y. Shidama, Probability Measure on Discrete Spaces and Algebra of Real Valued Random Variables, Formalized Mathematics, 査読有, 18. 2010, pp. 213-217.

〔学会発表〕（計 4 件）

① Y. Futa, Daichi Mizushima, H. Okaszaki, Formalization of Gaussian Integers, Gaussian Rational Numbers, and Their Algebraic Structures with Mizar, ISITA2012, 2012/10/28-31, Honolulu, Hawaii, USA.
② H. Okaszaki, Kenichi Arai, Yasunari Shidama, Formalization Verification of AES Using the Mizar Proof Checker, 2012 FCS'12, 2012/7/16-19, Las Vegas, Nevada, USA.
③ H. Okaszaki, Yasunari Shidama, Y. Futa, Formal Definition of Probability and Probabilistic Function on Finite and Discrete Sample Space for Proving Security of Cryptographic Systems Using Mizar, The 2011 Joint Mathematics Meetings, 2011/1/6-9, New Orleans, USA.
④ K.Arai, N.Kondo, H.Okazaki, Formalization of Probability and Random Sampling on a Finite and Discrete Sample Space Using the Mizar Proof Checker, 2010 FCS'10, 2010/7/12-15, Las Vegas, Nevada, USA.

〔図書〕（計１件）

① 宮地充子，日本評論社，代数学から学ぶ暗号理論，2012,288.

６．研究組織

(1)研究代表者
宮地 充子(MIYAJI, Atsuko)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：１０３１３７０１

(2)研究分担者
廣瀬 勝一（HIROSE, Syouichi）
福井大学・工学(系)研究科(研究院)・教授
研究者番号： ２０２２８８３６

双紙 正和（Soshi, Masakazu）
広島市立大学・情報科学研究科・准教授
研究者番号： ００２９３１４２

岡崎 裕之（OKAZAKI, Hiroyuki）
信州大学・工学部・助教
研究者番号： ５０４３２１６７