【ＨＰ公表資料】

平成26年度　日中韓フォーサイト事業
終了時評価資料(進捗状況報告書)

１．概要

研究交流課題名（和文）	次世代のインターネットとネットワークセキュリティに関する研究		
日本側拠点機関名	東北大学大学院情報科学研究科		
研究代表者 所属・職・氏名	大学院情報科学研究科・教授・加藤寧		
相手国（地域）側	**国　名**	**拠点機関名**	**研究代表者　所属・職・氏名**
	中国	上海交通大学	コンピュータ理工学科・教授・Zhenfu CAO
	韓国	韓国科学技術院	電気工学科・教授・Dan Keun SUNG

２．研究交流目標

申請時に計画した目標とその達成度について記入してください。

○申請時の研究交流目標

本事業による研究交流を通じ、日中韓の 3 カ国のそれぞれにおいて次世代ネットワーク並びにネットワークセキュリティの分野で先端的な研究を行っている研究者間の人的ネットワークを構築し、情報通信分野において世界的水準の研究拠点を形成することを目標とする。

技術的な課題としては、(1)次世代のインターネット技術、(2)ネットワークのエネルギー消費やリソース利用の効率化を実現する技術、(3)ネットワークの安全性を向上させる技術の 3 つを 3 カ国で共有する。情報通信分野で最重要課題として位置づけられるこれら 3 つの研究項目について世界最先端の研究を実施することにより、今後の世界の情報通信技術の発展に寄与する学術的価値の高い成果を本研究拠点から発信する。

世界的水準の研究拠点の形成を目指し、本事業中はもちろん事業終了後も将来的に持続・発展可能な研究者間の人的ネットワークを構築することを目標とする。お互いの強みを生かした共同研究の実施、共同での研究成果の発表、研究者間の交換交流などを軸とした研究交流を展開するとともに、研究課題を共有する複数グループ交流や研究者(研究室)単位での 2 者間交流などの様々なレベルでの研究交流体制を構築することにより、強固で緊密に連携した国際研究拠点を形成する。また、日本側研究者には女性 2 名が含まれており、女性の視点に立った研究交流を進めていけることも本研究チームの特徴である。一方、女性研究者を含む若手研究者の育成にも力を入れる。専門技術に精通するだけでなく、学術の幅広い分野に対する理解力や国際舞台でリーダシップを発揮できる能力を備えた若手研究者育成を目標として、若手研究者(特に大学院生)が主導して企画・運営するジョイントセミナーなどを開催する。

以上のような取り組みを通じ、日中韓を中心とした情報通信技術の世界トップレベルの研究拠点を形成する。さらには、その存在を世界に広くアピールすることにより、アジアはもちろん世界中からの人材流入による研究拠点体制の強化を図る。

○目標に対する達成度

☑研究交流目標は十分に達成された。
☐研究交流目標は概ね達成された。
☐研究交流目標はある程度達成された。
☐研究交流目標はほとんど達成されなかった。

【理由】

本事業の初年度に当たる平成 23 年度は、研究交流課題である「次世代のインターネットとネットワークセキュリティに関する研究」において、まずは 3 カ国の研究者がそれぞれどのような問題意識を持っているかについて相互理解を深めるための研究交流活動を行った。各研究者が取り組んでいる個別の研究内容についての議論などを通じて新たな知見や研究の方向性が得られただけでなく、研究者間の相互理解の深まりによって連携に向けた動きが活発化するなど、研究者間の人的ネットワークを拡大することができた。また、韓国にて 3 カ国の主要メンバによるワークショップを開催した。

本事業の 2 年度目に当たる平成 24 年度は、より緊密な連携による研究拠点の形成を最大の目標として、初年度より活発な研究交流活動を実施した。実際、連携の成果として年 2 回におよぶワークショップ形式のセミナーの開催や、共同研究の成果を国際的に著名な学術論文誌や国際会議にて発表するなど、研究拠点形成は着実に進んでいると考えられる。中国および韓国で開催したセミナーでは、修士課程学生を含む大学院生が多数参加して熱心に議論を行うなど、学術の幅広い分野に対する理解力や国際舞台でリーダシップを発揮できる能力を備えた若手研究者育成という点において非常に有意義であった。

本事業の最終年度に当たる平成 25 年度は、これまでの研究交流活動の幅を更に広げ、日中韓を中心とした情報通信技術の世界トップレベルの研究拠点を形成すべく、より積極的に活動を行った。本年度は日本においてワークショップを行い、各国の研究者間の交流をより一層深めるとともに、次世代ネットワークに関して様々な新しい学術的知見を得た。また、ワークショップの開催に際しては大学院生が中心となり企画から運営までに携わり、国際舞台でリーダシップを発揮できる能力を備えた若手研究者育成にも大きく貢献した。

以上のように、本事業で掲げた研究交流目標を大きく上回る成果を達成することができた。

３．研究交流活動の成果

これまでの交流を通じての成果を「学術的側面」「若手研究者の育成」及び「日中韓における継続的な研究教育拠点の構築」の観点から記入してください。また、活動成果から発生した波及効果がある場合には記入してください。

○学術的側面

本事業では「次世代のインターネットとネットワークセキュリティ」を研究交流課題として掲げているが、これまでの研究交流活動により、学術面において次のような成果が得られた。

次世代のインターネットの研究について、各国の研究者との共著論文が情報通信分野において世界最大規模かつ最も権威のある米国電気電子学会（IEEE）の学術論文誌である IEEE Transactions on Parallel and Distributed Systems や IEEE Journal on Selected Areas in Communications に採録が決定している。同論文誌は無線通信分野において、Impact Factor が世界で最高クラスとなっている。また、IEEE が主催する国際会議においても多数の研究発表を行っており、INFOCOM、 Globecom 等の採択率の低い難関国際会議においても論文を発表している。

また、ネットワークのセキュリティに関する研究について、日中間の共著論文がインパクトファクタが 3.6 以上である論文誌 Information Sciences に採録されている。その他にも、情報処理学会(IPSJ)への推薦論文としての採録、国際会議 AsiaJCIS 発表論文の最優秀論文賞受賞、暗号研究に関して高いレベルの国際学会の一つである ISC への論文採録など、数多くの成果を挙げている。これらは、本事業による研究成果が世界的に非常に高い影響力を持つことを意味している。

このように、本拠点では、日中韓が連携して次世代ネットワークに関して総合的な学術交流を行う体制ができ、物理層からアプリケーション層に至る幅広い分野で学術交流を活発に行い、次世代ネットワークに関して様々な新しい学術的知見を得た。

○若手研究者の育成

本事業では、若手研究者育成のための活動の一つとして、平成 24 年 1 月 4 日から 13 日まで、日本側 NICT・筑波大学・金沢大学、中国側北京郵電大学・上海交通大学のメンバ、特に若手研究員と在学中の学生メンバが中心となって連携企画した共同研究活動を行った。総勢 25 人が参加し、ペアリング暗号(暗号の設計から、応用、分析、実装まで豊富な研究課題に関連)、非可換暗号（理論研究、魔方群ベース暗号、耐量子攻撃プロトコル設計と安全性証明）について研究交流をし、参加者達は互いに相手の研究に深く興味を示し、活発な議論を行った。また、これまで各国で開催を行ったワークショップでは、物理層からアプリケーション層に至る幅広い分野の研究発表と討論を通じて総合的観点から次世代ネットワークについて学術研究できる能力と国際的視野を向上できた。これにより、狭い分野に閉じこもらず、本拠点のように物理層からアプリケーション層に至る幅広い分野を理解したうえで、それぞれの分野の学術研究を行う若手研究者を育成できる体制が整った。また、平成 24 年 3 月 20 日から 27 日まで、NICT 王主任研究員と金沢大学満保教授が北京郵電大学を訪問し、学生の研究教育に有益なプログラムの立ち上げや、共著論文の修正、研究と計画の打ち合わせ、講演会を行い、若手研究者との活発な交流を行った。

これらの若手研究者育成のための活動の成果として、初年度に JSPS 特別研究員であった若手研究者の内、太田香が国立大学のテニュアトラック助教として採用､董冕雄が独立行政法人の研究所に就職している｡また、NICT 王主任研究員が協力指導してきた北京郵電大学の博士 Ping Pan と Yuanju Gan が 2013 年 3 月と 6 月にそれぞれ卒業し、博士学位を獲得した。さらに、王研究員はこれまでの若手研究者の教育への貢献を認められ、2013 年 7 月から 3 年間北京郵電大学の客員教授となった。その他にも、筑波大学博士学生である矢内直人は暗号セキュリティ研究に関する賞である、SCIS 論文賞と CSS 学生論文賞を受賞し、暗号セキュリティの国際会議である IWSEC での招待講演と、筑波大学システム情報工学研究科研究科長賞を受賞している。また、金沢大学博士前期課程学生である高橋寛弥が、国際会議 AsiaJCIS で論文発表を行い、最優秀論文賞を受賞するなど、本事業のメンバである若手研究者の多くが非常に優れた研究成果を挙げることができた。

○日中韓における継続的な研究教育拠点の構築

次世代ネットワークは国際協調なしには構築できない｡アジアで先進的ネットワークの研究を進めている日中韓が協調して､物理層からアプリケーション層に至る幅広い分野での学術交流を行うことが次世代ネットワークの構築に欠かせない｡例えば､上海交通大学の研究者とは､年２回程度の相手国での研究打ち合わせの他､日常的に電話会議を実施するなどし、緊密な連携関係を築いている。また、各研究機関の間で頻繁に研究打ち合わせを行うなどし、多くの共同研究成果を挙げてきた。これらの協力関係は今後も継続させていく予定である。このように、本拠点では日中韓で次世代ネットワークに関する拠点を早期に立ち上げ、当初の目標を上回る学術交流成果を上げ、継続的な研究教育拠点の構築を実現した。

○成果の波及効果

NICT の王主任研究員(Lihua Wang)が主要参画者として、北京郵電大学 Licheng Wang 准教授が研究代表者として申請した中国国家自然科学基金プロジェクト“Research on Two Key Problems of Non-Commutative Cryptography”に参加することになった（期間 2014 年 1 月～2017 年 12 月)。この成果は本事業における研究交流活動の成果の一つであり、今後も大きな波及効果が期待できる。

４．研究交流活動の実施状況

（1）これまでの研究交流活動について、「共同研究」、「セミナー」及び「研究者交流」の交流の形態ごとに、派遣及び受入の概要を記入してください。※各年度における派遣及び受入実績については、「終了時評価資料（経費関係調書）」に記入してください。

○共同研究

【概要】

お互いのアイディアやアプローチなどについてメールや電話会議などを通じて頻繁に研究者間で意見交換および議論・検討を行う一方、必要に応じて研究者を数日間程度の短期で派遣または受け入れるなどして集中的な議論や直接指導・交流を定期的に行った。また、大学院博士課程（前期及び後期）の学生の派遣や受け入れも行うことにより、若手人材の育成も図った。さらに、お互いの強みを生かした共同研究の実施と密な連携により、共同での研究成果の発表や、研究者の派遣や受け入れを行い、長期的な世界的水準の研究拠点の形成や、その拠点の核として活躍することになるであろう若手人材の育成を実現する多くの成果を得た。

○セミナー

	平成23年度	平成24年度	平成25年度
国内開催	0 回	0 回	1 回
海外開催	1 回	2 回	0 回
合計	1 回	2 回	1 回

【概要】

本事業によって得られた研究成果について 3 カ国の各研究者が一堂に会して発表を行うワークショップ形式のセミナーを開催した。研究者間での情報交換、問題意識の共有、研究方法・結果について議論する場を設けることにより、より緊密な関係の構築を実現し、新たな研究者間連携について模索した。また、各研究者が取り組んでいる課題について議論することにより、新たな知見や研究の方向性が得られ、研究者間の人的ネットワークを拡大することができた。さらに、3 カ国の PI を中心とした研究者・事務者打ち合わせ、それまでの活動の総括及び以後の研究交流計画について意見交換などを行い、研究交流活動の活発化と円滑な実施を図った。また、韓国及び日本の PI による基調講演を行い、各国の研究の全体像を明確化し、次世代ネットワーク及びセキュリティに関する重要課題について、参加者間での問題意識などの共有を強化した。

○研究者交流

【概要】

該当なし（本事業では全てのメンバが同一の参加形態に参加し活動を行っており、その活動は全て共同研究に分類されているため研究者交流に該当する活動は無い）

（２） 本事業における、「日本側拠点機関の実施体制」、「中国・韓国の拠点機関との協力体制」、「日本側拠点機関の事務支援体制」について記入してください。

○日本側拠点機関の実施体制 （拠点機関としての役割・国内の協力機関との協力体制等）

日本の研究チームは、ネットワーク技術とセキュリティ技術のそれぞれを担当する 2 グループによって編成された。ネットワークグループは東北大学と会津大学の研究者から構成され、セキュリティグループは筑波大学と情報通信研究機構（NICT）の研究者から構成された。

ネットワークグループを統括する研究代表者の東北大学の加藤教授は、地上系のみならず、衛星、モバイル、センサ・アドホックなど次世代ネットワークを構成する様々なネットワーク技術に精通する国内有数の研究者であり、本研究分野で世界最高峰の学会である IEEE を中心に活動し、IEEE 衛星宇宙通信委員会委員長を務めるなど、世界を舞台に活躍している。また、数多くの学術賞や活動貢献賞も受賞している。国内では、総務省 ITU-R SG4 の主査を務めており、我が国の標準化活動に貢献している。一方、無線通信技術を担当する東北大学の安達教授は、トムソン・ロイターによって論文被引用数が多い科学者として選ばれるなど（2011 年 1 月 1 日現在 21 分野で 266 人の日本人が登録されている）、無線通信分野で世界に名立たる研究者の一人である。

セキュリティグループは筑波大学の岡本教授と金沢大学の満保教授が中心となり、筑波大学メンバと NICT メンバで共に研究を遂行した。岡本教授は、日本を代表する暗号研究者であり、暗号と情報セキュリティに係わる日本を代表する学会の研究会である ISEC と CSEC の委員長と主査をそれぞれ務めた経験を有し、長年、国際会議 Asiacrypt 組織委員会に日本代表として参加しており、中国や韓国を含むアジアの関係者からの信頼も厚い。満保教授は暗号応用の分野において、研究の一分野を形成する論文を執筆するなど、世界的な認知度も高い。NICT メンバの王は、中国側の研究代表者である Cao 教授のグループと岡本グループで学んだ経験を有し継続的にグループ間の共同研究の遂行に貢献した。

○中国・韓国の拠点機関との協力体制 （各国の役割分担・ネットワーク構築状況等）

本事業では、中国の拠点機関である上海交通大学、韓国の拠点機関である韓国科学技術院が各国の中心として様々な研究交流活動を行ってきた。各国において開催したワークショップやジョイントセミナーを通じて研究者間での情報交換、問題意識の共有、研究方法・結果について議論を行い、より緊密な研究者間の関係の構築を実現し、新たな研究者間連携の形を見出した。また、研究者単位での2者間交流といった研究交流活動を通じ、各研究者が取り組んでいる課題について議論等を行い、新たな知見や研究の方向性を得ながら、研究者間の人的ネットワークを拡大した。さらに、各国が有する研究課題を共有することで国際的な連携グループを形成することができた。

○日本側拠点機関の事務支援体制 （拠点機関全体としての事務運営・支援体制等）

本事業にかかる事務処理は、情報科学研究科事務室にて担当した。研究代表者所属の事務室が窓口となることで、他大学との連携をスムーズかつ継続的に行った。なお、必要に応じて本部事務局国際交流課がサポートすることにより、効率よく業務を実施した。

５．この課題に関連した主な発表論文名・著者名

研究代表者あるいは参加研究者が実施期間中に発表した論文等で、この交流の成果であり、**本事業名が明記されているもの**を記載してください。研究代表者・参加研究者の氏名にはアンダーラインを付してください。また、相手国の参加研究者との共著論文には、文頭の番号に〇印を付し、その場合、中国・韓国いずれの研究者との共著論文かが分かるように備考欄に国名を記入してください。

（1）学術雑誌等（紀要・論文集等も含む）に発表した論文又は著書

・査読がある場合、印刷済み及び採録決定済のものに限り、査読中・投稿中のものは除く。また「査読」欄に〇印を付すこと。

整理番号	著者名、発表論文名、学会誌名、発表年月巻号等	査読	相手国名（共著の場合）
1	N. Yanai, E. Chida, M. Mambo, and E. Okamoto, “A CDH-based Ordered Multisignature Scheme Provably Secure without Random Oracles,” *Journal of Information Processing*, vol. 22, no. 2, Apr. 2014. (recommended paper, to appear)	〇	
②	H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, “A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks,” *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, vol. 25, no. 1, pp. 22-32, Jan. 2014.	〇	中国
3	N. Yanai, M. Mambo, and E. Okamoto, “Ordered Multisignature Schemes under the CDH Assumption without Random Oracles,” *Proc. of Information Security Conference*. Proceedings will be published in January 2014 as a book in LNCS.	〇	
④	J. Yan, L. Wang, L. Wang, Y. Yang, and W. Yao, “Efficient Lattice-Based Signcryption in Standard Model,” *Mathematical Problems in Engineering*. (accepted)	〇	中国
⑤	Y. Gan, L. Wang, L. Wang, P. Pan, and Y. Yang, “A Publicly Verifiable Secret Sharing Scheme with Provable Security Against Chosen Secret Attacks,” *International Journal of Distributed Sensor Networks*, vol. 2013.	〇	中国
⑥	J. Yang, L. Yuan, C. Dong, G. Cheng, N. Ansari, and N. Kato, “On Characterizing Peer-to-Peer Streaming Traffic,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 175-188, Sep. 2013.	〇	中国
⑦	M. Dong, K. Ota, H. Li, S. Du, H. Zhu, and S. Guo, “RENDEZVOUS: Towards Fast Event Detecting in Wireless Sensor and Actor Networks,” *In Press, Springer Computing*, Oct. 2013.	〇	中国
⑧	M. Dong, K. Ota, Z. Tang, M. Lin, S. Du and H. Zhu, “UAV Assisted Data Gathering in Wireless Sensor Networks,” *Springer Journal of Supercomputing*. (accepted)	〇	中国
⑨	S. Du, H. Zhu, X. Li, K. Ota, and M. Dong, “MixZone in Motion: Achieving Dynamically Cooperative Location Privacy Protection in Delay-tolerant Networks,” *IEEE Transactions on Vehicular Technology (TVT)*, vol. 62, no. 9, pp. 4565-4575, 2013.	〇	中国
10	Y. Cai, Y. Mo, K. Ota, C. Luo, M. Dong, and L. T. Yang, “Optimal Data Fusion of Collaborative Spectrum Sensing under Attack in Cognitive Radio Networks,” *In Press, IEEE Network*, 2013.	〇	
11	J. Wu, M. Dong, K. Ota, and Z. Zhou, “Regenerating Code based Secure Distributed Storage for Wireless Sensor Networks,” *Elsevier Procedia Computer Science*, vol. 21, pp. 183-190, 2013.	〇	
12	J. Wu, M. Dong, K. Ota, and B. Duan, “Towards Fault-Tolerant Fine-Grained Data Access Control for Smart Grid,” *In Press, Springer Wireless Personal Communications*, Jun. 2013.	〇	
⑬	L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao, and Y. Yang, “New Public Key Cryptosystems based on Non-Abelian Factorization Problems,” *Wiley Security and Communication Networks*, vol. 6, no. 7, pp. 912-922. Jul. 2013.	〇	中国
⑭	S. Du, P. Tian, K. Ota, and H. Zhu, “A Secure and Efficient Data Aggregation Framework in	〇	中国

	Vehicular Sensing Networks," *International Journal of Distributed Sensor Networks (Hindawi)*, vol. 2013, 2013.		
⑮	L. Gu, Y. Pan, M. Dong, and K. Ota, "Non-Commutative Lightweight Signcryption for Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.	○	中国
⑯	L. Wang, J. Shao, Z. Cao, M. Mambo, A. Yamamura, and L. Wang, "Certificate-based proxy decryption systems with revocability in the standard model," *Information Sciences*, vol. 247, pp. 188-201, 2013.	○	中国
⑰	Y. Gan, L. Wang, L. Wang, P. Pan, and Y. Yang, "Efficient Construction of CCA-Secure Threshold PKE Based on Hashed Diffie-Hellman Assumption," *The Computer Journal*, vol. 56, no.10, pp. 1249-1257, 2013.	○	中国
⑱	P. Pan, L. Wang, Y. Gan, Y. Yang, and L. Wang, "Chameleon Hash Functions and One-Time Signature Schemes from Inner Automorphism Groups," *Fundamenta Informaticae*, vol. 126, pp. 103-119, 2013.	○	中国
⑲	W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato, "Cluster- based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks," *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, vol. 24, no. 2, pp. 239-249, Feb. 2013.	○	中国
20	H. Kokubo, A. Kanaoka, M. Mambo, and E. Okamoto, "A Combined Machine Learning Method for the Detection of Attacks," *IPSJ Journal*, vol. 53, no. 9, pp. 2086-2093, Sep. 2012.	○	
㉑	P. Pan, L. Wang, L. Wang, L. Li, and Y. Yang, "CSP-DHIES: A New Public-Key Encryption Scheme From Matrix Conjugation," *Security and Communication Networks*, vol. 5, no.7, pp. 809-822, Jul. 2012.	○	中国
㉒	A. Abdulla, H. Nishiyama, J. Yang, N. Ansari, and N. Kato, "HYMN: A Novel Hybrid Multi-Hop Routing Algorithm to Improve the Longevity of WSNs," *IEEE Transaction on Wireless Communications*, vol. 11, no. 99, pp. 1-11, 2012.	○	中国

(2)国際会議における発表

・著者名(参加研究者を含む全員の氏名を、論文等と同一の順番で記載すること)、発表題目名、発表した学会名、開催場所、口頭・ポスター等の形式、論文等の番号、発表年月日等を記載すること。発表者に○印を付すこと。

・査読がある場合、「査読」欄に○印を付すこと。

整理番号	著者名、発表題目名、学会名、開催場所、口頭・ポスター等の形式、論文等の番号、発表年月日等	査読	相手国名(共同発表の場合)
1	○ M. Dong, K. Ota, and M. Sakai, " A Novel Information Dissemination System for Vehicle-to-RSU Communication Networks," *in Prof. of IEEE International Conference on Connected Vehicles & Expo (IEEE ICCVE 2013)*, Las Vegas, Nevada, USA, Dec. 2-6, 2013.	○	
②	○M. Dong, K. Ota, S. Du, H. Zhu, and S. Guo, "ANTS: Pushing the Rapid Event Notification in Wireless Sensor and Actor Networks," *in Proc. of Joint International Conference on Awareness Science and Technology & Ubi-Media Computing (iCAST2013 & UMEDIA 2013)*, Aizu Wakamatsu, Japan, Nov. 2-4, 2013.	○	中国
3	○K. Ota, M. Dong, X. Chen, A. Liu and Z. Chen, "Cross Layer Optimal Design for Wireless Sensor Networks under Rayleigh Fast Fading Channels," *in Proc. of IEEE International Conference on High Performance Computing and Communications (IEEE HPCC 2013)*, Zhangjiajie, China, Nov. 13-15, 2013.	○	
4	○H. Zhu, M. Dong, S. Chang, Y. Zhu, M. Li, and X. Shen, "ZOOM: Scaling the Mobility for Fast Opportunistic Forwarding in Vehicular Networks," *in Proc. of the 32nd IEEE International*	○	

	Conference on Computer Communications (IEEE INFOCOM 2013), Turin, Italy, Apr. 14–19, 2013.		
5	○N. Yanai, M. Mambo, and E. Okamoto, "Ordered Multisignature Schemes under the CDH Assumption without Random Oracles," *in Proc. of Information Security Conference (ISC)*, Texas, America, in session of Cryptography, Nov. 13–15, 2013.	○	
⑥	○H. Takahashi, K. Yasunaga, M. Mambo, K. Kim, and H. Y. Youm, "Preventing Abuse of Cookies Stolen by XSS," *in Proc. of the 2013 Eight Asia Joint Conference on Information Security (AsiaJCIS)*, pp.85–89, Seoul, Jul. 25, 2013.	○	韓国
⑦	○A. Yoshinari, H. Nishiyama, N. Kato, and D. K. Sung, "Dynamic Topology Update Mechanism in Local Tree-based Reliable Topology (LTRT) based MANETs," *in Proc. of IEEE International Conference on Communications (ICC 2012)*, Ottawa, Canada, Jun. 10–15, 2012.	○	韓国
8	○Y. Kawamoto, H. Nishiyama, N. Kato, N. Yoshimura, and N. Kadowaki, "A Delay-Based Traffic Distribution Technique for Multi-Layered Satellite Networks," *in Proc. of IEEE Wireless Communications and Networking Conference (WCNC 2012)*, Paris, France, pp. 2401–2405, Apr. 1–4, 2012.	○	
9	○J. Liu, X. Jiang, H. Nishiyama, N. Kato, and X. (S.) Shen, "End-to-End Delay in Mobile Ad Hoc Networks with Generalized Transmission Range and Limited Packet Redundancy," *in Proc. of IEEE Wireless Communications and Networking Conference (WCNC 2012)*, Paris, France, pp. 1731–1736, Apr. 1–4, 2012.	○	
⑩	○S. H. Kim, S. J. Lee, D. K. Sung, H. Nishiyama, and N. Kato, "Optimal Rate Selection Scheme in a Two-hop Relay Network Adopting Chase Combining HARQ in Rayleigh Block-fading Channels," *in Proc. of IEEE Wireless Communications and Networking Conference (WCNC 2012)*, Paris, France, pp. 1731–1736, Apr. 1–4, 2012.	○	韓国
⑪	○M. Li, Z. Gao, S. Du, H. Zhu, M. Dong, and K. Ota, "PriMatch: Fairness-aware Secure Friend Discovery Protocol in Mobile Social Network," *in Proc. of IEEE Global Communications Conference (IEEE GLOBECOM 2012),* pp.738–743, Dec. 3–7, 2012.	○	中国
12	○J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Exact Throughput Capacity under Power Control in Mobile Ad Hoc Networks," *in Proc. of 31st IEEE International Conference on Computer Communications (INFOCOM 2012)*, Orlando, Florida, USA, Mar. 25–30, 2012.	○	
13	○J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Multicast Capacity, Delay and Delay Jitter in Intermittently Connected Mobile Networks," *in Proc. of 31st IEEE International Conference on Computer Communications (INFOCOM 2012)*, Orlando, Florida, USA, pp. 253–261, Mar. 25–30, 2012.	○	

(3)国内学会・シンポジウム等における発表

・(2)と同様に記載すること。

整理番号	著者名、発表題目名、学会名、開催場所、口頭・ポスター等の形式、論文等の番号、発表年月日等	査読	相手国名（共同発表の場合）
1	○Y. Liu, N. Kanayama, S. Kazutaka, T. Teruya, S. Uchiyama, and E. Okamoto, “Computing fixed argument pairings with elliptic net method,” *SCIS2014*, 鹿児島, 2014年1月21日－24日.		
2	○北島 暢曜, 山川 高志, 西出 隆志, 花岡 悟一郎, 岡本 栄司, “素因数分解仮定に基づく署名長が短いFail-Stop署名,” *SCIS2014*, 鹿児島, 2014年1月21日－24日.		
3	○小岩 敬太, 金岡 晃, 岡本 栄司, “動的かつ並列化された検索可能対称暗号の改良方式”, *SCIS2014*, 鹿児島, 2014年1月21日－24日.		
4	○田中 和磨, 石井 健太, 西出 隆志, 照屋 唯紀, 金山 直樹, 岡本 栄司, “Supersingular な楕円曲線における Weil ペアリングの効率化”, *SCIS2014*, 鹿児島, 2014年1月21日－24日.		
5	○長谷川 佳祐, 西出 隆志, 岡本 栄司, “関数型暗号の実装仕様に関する考察”, *SCIS2014*, 鹿児島, 2014年1月21日－24日.		
6	○中村 裕樹, 満保 雅浩, “証明書不要なIDベース認証付き鍵共有方式”, *SCIS2014*,鹿児島, 2014年1月21日－24日.		
7	○北島 暢曜, 矢内 直人, 西出 隆志, 岸本 渡, 花岡 悟一郎, 岡本 栄司, “多人数の署名者によるFail-Stop署名とその応用”, *SITA2013*, 静岡, 2013年11月26日－29日.		
8	○N. Yanai, E. Chida, M. Mambo, and E. Okamoto, “Efficient CD-based Ordered Multisignature Schemes without Random Oracles,” *第36回情報理論とその応用シンポジウム (SITA 2013)*, 静岡, pp.134-139, 2013年11月26日－29日.		
9	○矢内 直人, 千田 栄幸, 満保 雅浩, 岡本 栄司, “BGP指向アグリゲート署名の構成”, *コンピュータセキュリティシンポジウム (CSS)*, 香川, 2C3-1, pp.510-517, 2013年10月21日－23日.		
10	○矢内 直人, 千田 栄幸, 満保 雅浩, 岡本 栄司, “多者多重署名の構成に関する一考察”, *暗号と情報セキュリティシンポジウム (SCIS)*, 京都, 3A4-3, pp.1-8, 2013年1月22日－25日.		
11	○矢内 直人, 千田 栄幸, 満保 雅浩, 岡本 栄司, “スタンダードモデルにおける順序検証型多重署名方式”, *コンピュータセキュリティシンポジウム (CSS)*, 島根, 2C1-3, pp.293-300, 2012年10月30日－11月2日.		
⑫	Y. Gan, ○L. Wang, P. Pan, L. Wang, and Y. Wang, “A CCA Secure Threshold KEM Scheme,” *Symposium on Cryptography and Information Security (SCIS2012)*, Kanazawa, Japan, Jan. 30-Feb. 2, 2012.		中国