

## 教員の総合業績(基礎資料)調査 氏名(高木 剛)

### 1 研究業績

1) 著書・論文・学会発表・作品など(平成17-18年度に限る)

例:(欧文の場合は、原文 alphabet で記入してください)

#全著者あるいは作者名(自己にアンダーライン、単著の場合はアンダーライン不要)

&著書、学術論文又は作品の名称

\$発行所(総頁数)、発表雑誌又は発表学会(号・巻・pp・年月)、展覧会(場所・期間)などの名称

さらに、特別講演・シンポジウム(招待講演)・一般講演など(地方支部会・全国大会・国際会議)の別

註:学会・展覧会など、専門分野以外の人に分りにくい場合は、できるだけその社会的位置づけ、歴史、規模などの簡潔な説明を付してください

#### 査読付き論文

- [1] Izuru Kitamura, Masanobu Katagi, Tsuyoshi Takagi, "A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two", 10th Australasian Conference on Information Security and Privacy, ACISP 2005, LNCS 3574, pp.146-157, 2005, Springer-Verlag.
- [2] Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume, "Efficient Representations on Koblitz Curves with Resistance to Side Channel Attacks", 10th Australasian Conference on Information Security and Privacy, ACISP 2005, LNCS 3574, pp.218-229, 2005, © Springer-Verlag.
- [3] Raylin Tso, Takeshi Okamoto, Tsuyoshi Takagi, Eiji Okamoto, "k-Resilient ID-Based Key Distribution Schemes from Pairing", International Workshop on Coding and Cryptography, WCC 2005, Bergen, Norway, pp.402-412, 2005.
- [4] Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume, "Short-Memory Scalar Multiplication on Koblitz Curves", Workshop on Cryptographic Hardware and Embedded Systems, CHES 2005, LNCS 3659, pp.91-105, 2005, © Springer-Verlag.
- [5] Katja Schmidt-Samoa, Tsuyoshi Takagi, "Paillier's Cryptosystem Modulo  $p^2q$  and its Applications to Trapdoor Commitment Scheme", International Conference on Cryptology in Malaysia, Mycrypt 2005, LNCS 3715, pp.296-313, 2005, © Springer-Verlag.
- [6] Erik Dahmen, Katsuyuki Okeya, Tsuyoshi Takagi, "An Advanced Method for Joint Scalar Multiplications on Memory Constraint Devices", 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, ESAS 2005, LNCS 3813, pp.189-204, 2005, © Springer-Verlag.
- [7] Dong-Guk Han, Tsuyoshi Takagi, Tae Hyun Kim, Ho Won Kim, Kyo Il Chung, "Collision Attack on XTR and a Countermeasure with Fixed Pattern", The First International Workshop on Security in Ubiquitous Computing Systems, SecUbiq-05, LNCS 3823, pp. 864-873, 2005, Springer-Verlag.
- [8] Lihua Wang, Takeshi Okamoto, Tsuyoshi Takagi, and Eiji Okamoto, "Insider Impersonation-MIM Attack to Tripartite Key Agreement Scheme and An Efficient Protocol for Multiple Keys", 2005 International Conference on Computational Intelligence and Security, CIS 2005, Part II, LNAI 3802, pp.198-203, 2005, Springer-Verlag.
- [9] Katja Schmidt-Samoa, Olivier Semay, Tsuyoshi Takagi, "Analysis of Fractional Window Recoding Methods and Their Application to Elliptic Curve Cryptosystems", IEEE Transactions on Computers, Vol.55, No.1, pp.48-57, January, 2006, IEEE Computer Society.

- [10] Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume, "Security Analysis of the SPA-Resistant Fractional Width Method", IEICE Transactions, Vol.E89-A, No.1, pp.161-168, IEICE, 2006.
- [11] Masanobu Katagi, Toru Akishita, Izuru Kitamura, Tsuyoshi Takagi, "Efficient Hyperelliptic Curve Cryptosystems using Theta Divisors", IEICE Transactions, Vol.E89-A, No.1, pp.151-160, IEICE, 2006.
- [12] Tsuyoshi Takagi, David Reis, Jr., Sung-Ming Yen, Bo-Ching Wu, "Radix-r Non-Adjacent Form and Its Application to Pairing-Based Cryptosystem", IEICE Transactions, Vol.E89-A, No.1, pp.115-123, IEICE, 2006.
- [13] Hisayoshi Sato, Tsuyoshi Takagi, Satoru Tezuka, Kazuo Takaragi, "Generalized Powering Functions and Their Application to Digital Signatures", IEICE Transactions, Vol.E89-A, No.1, pp.81-89, IEICE, 2006.
- [14] Dong-Guk Han, Tsuyoshi Takagi, Jongin Lim, "Further Security Analysis of XTR", The 2nd Information Security Practice and Experience Conference, ISPEC 2006, LNCS 3903, pp.33-44, 2006, Springer-Verlag.
- [15] Toru Akishita, Tsuyoshi Takagi, "Power Analysis to ECC Using Differential Power between Multiplication and Squaring", Seventh Smart Card Research and Advanced Application, CARDIS 2006, LNCS 3928, pp.151-164, 2006, © Springer-Verlag.
- [16] Camille Vuillaume, Katsuyuki Okeya, Tsuyoshi Takagi, "Defeating Simple Power Analysis on Koblitz Curves", IEICE Transactions, Vol.E89-A No.5 pp.1362-1369, IEICE, 2006.
- [17] Katsuyuki Okeya, Tsuyoshi Takagi, "Security Analysis of CRT-Based Cryptosystems", International Journal of Information Security, IJIS, Vol.5, No.3, pp.177-185, 2006, Springer-Verlag.
- [18] Dong-Guk Han, Tsuyoshi Takagi, Ho Won Kim, Kyo Il Chung, "New Security Problem in RFID Systems "Tag Killing"", Applied Cryptography and Information Security, ACIS 2006, LNCS 3982, pp.375-384, 2006, Springer-Verlag.
- [19] Kyosuke Osaka, Tsuyoshi Takagi, Kenichi Yamazaki, Osamu Takahashi, "An Efficient and Secure RFID Security Method with Ownership Transfer", CIS 2006, pp.1090-1095, © IEEE Press, 2006. (A revised version to appear in LNAI, Springer-Verlag)
- [20] Yuto Kawahara, Tsuyoshi Takagi, Eiji Okamoto, "Efficient Implementation of Tate Pairing on a Mobile Phone using Java", International Conference on Computational Intelligence and Security, CIS 2006, pp.1247-1252, © IEEE Press, 2006. (A revised version to appear in LNAI, Springer-Verlag)
- [21] Tae Hyun Kim, Tsuyoshi Takagi, Dong-Guk Han, Ho Won Kim, Jongin Lim, "Side Channel Attacks and Countermeasures on Pairing Based Cryptosystems over Binary Fields", 5th International Conference on Cryptology and Network Security, CANS 2006, LNCS 4301, pp.168-181, 2006, © Springer-Verlag.
- [22] Kaoru Kurosawa, Tsuyoshi Takagi, "Efficient Selectively Convertible Undeniable Signature Without Random Oracle", Asiacypt 2006, LNCS 4284, pp.428-443, 2006, © Springer-Verlag.
- [23] Chunhua Su, Jianying Zhou, Feng Bao, Tsuyoshi Takagi, Kouichi Sakurai, "Two Party Privacy-Preserving Agglomerative Document Clustering", 3rd Information Security Practice and Experience Conference, ISPEC 2007, LNCS 4464, pp.193-208, Springer-Verlag, 2007.
- [24] Masaaki Shirase, Tsuyoshi Takagi, Eiji Okamoto, "Some Efficient Algorithms for the Final Exponentiation of  $\eta_T$  Pairing", 3rd Information Security Practice and Experience Conference, ISPEC 2007, LNCS 4464, pp.254-268, Springer-Verlag, 2007.
- [25] Erik Dahmen, Katsuyuki Okeya, Tsuyoshi Takagi, "A New Upper Bound for the Minimal Density of Joint Representations in Elliptic Curve Cryptosystems", IEICE Transactions, Volume E90-A No.5, pp.952-959, 2007.
- [26] Eun-Kyung Ryu, Tsuyoshi Takagi, "Efficient Conjunctive Keyword-Searchable Encryption", 3rd IEEE International Symposium on Security in Networks and Distributed Systems, SSNDS-07, pp.409-414, © IEEE Computer Society, 2007.
- [27] Chunhua Su, Feng Bao, Jianying Zhou, Tsuyoshi Takagi, Kouichi Sakurai, "Privacy-Preserving Two-Party K-Means Clustering Via Secure Approximation", The 2007 IEEE International Symposium on Data Mining and Information Retrieval, DMIR 2007, pp.385-391, 2007 © IEEE Computer Society.

[28]Jean-Luc Beuchat, Nicolas Brisebarre, Masaaki Shirase, Tsuyoshi Takagi, Eiji Okamoto, "A Coprocessor for the Final Exponentiation of the Eta\_T Pairing in Characteristic Three", International Workshop on the Arithmetic of Finite Fields, WAIFI 2007, LNCS 4547, pp.25-39, © Springer-Verlag, 2007.

2) 学会活動(役員・会員)、学会の組織運営、学会誌の編集委員など(平成17年度にる)

例:

#学会などの名称

&編集委員長又は委員などの別

\$任務期間(年月)

註: 専門分野によっては適宜変更(例えば、学会を展覧会などと記す)・追加説明を付してください。できれば展覧会・学会などについても社会的位置付け、歴史、規模などの簡潔な説明を添えてください。

#### 国内学会活動

- [1] 電子情報通信学会情報セキュリティ研究会 専門委員 平成17年9月～
- [2] 情報処理学会コンピュータセキュリティ研究会 運営委員 平成17年9月～
- [3] 国際会議 IWSEC 運営委員 平成17年3月～
- [4] 電子情報通信学会英文論文誌 暗号と情報セキュリティ小特集号 編集委員 平成17年度～
- [5] 電子情報通信学会英文論文誌 離散数学とその応用小特集号編集委員 平成17年度～
- [6] 電子情報通信学会英文論文誌 情報理論とその応用小特集号編集委員 平成18年度～
- [7] 電子情報通信学会和文論文誌 A 編集委員 平成18年度～
- [8] 電子情報通信学会和文論文誌 留学生による日本語技術論文小特集号 編集委員 平成18年度～

#### 国際会議プログラム編集委員

- [1] ACNS 2005, Applied Cryptography and Network Security 2005, June 7-10, 2005, New York, USA.
- [2] CCN 2005, IASTED International Conference on Communications and Computer Networks, October 24-26, Marina Del Rey, USA.
- [3] CHES 2005, Workshop on Cryptographic Hardware and Embedded Systems 2005, August 29 - Sep. 1, Edinburgh, Scotland.
- [4] IWAP 2005, International Workshop for Applied Public Key Infrastructure, September 21-23, Singapore.
- [5] DIM 2005, ACM CCS2005 Workshop on Digital Identity Management, November 11, 2005, George Mason University, Fairfax, VA, USA
- [6] SSI 2005, International Symposium on System and Information Security, November 11, 2005, Sao Jose dos Campos, Brasil
- [7] CNIS 2005, IASTED International Conference on Communication, Network and Internet Security, November 14-16, 2005, Phoenix, USA
- [8] ICISC 2005, International Conference on Information Security and Cryptology, December 1-2, 2005, Seoul, Korea.
- [9] MultiSec 2005, IEEE International Workshop on Security and Pervasive Multimedia

- Environments, December 12-14, 2005, Irvine, California, USA
- [10] AReS 2006, International Conference on Availability, Reliability and Security, April 20-22, 2006, Vienna, Austria.
  - [11] ACIS 2006, Applied Cryptography and Information Security, May 8-11, 2006, Glasgow, UK.
  - [12] ACNS 2006, International Conference on Applied Cryptography and Network Security, June 6-9, 2006, Singapore
  - [13] ETRICS 2006, International Conference on Emerging Trends in Information and Communication Security, June 6-9, 2006, Freiburg, Germany.
  - [14] SecUbiq-06, International Workshop on Security in Ubiquitous Computing Systems, August 1-2, 2006, Seoul, Korea.
  - [15] SECRYPT 2006, International Conference on Security and Cryptography, August 7-10, 2006, Setubal, Portugal.
  - [16] ATC-06, International Conference on Autonomic and Trusted Computing, September 3-6, 2006, Wuhan and Three Gorges, China.
  - [17] TAMC 2006, Workshop on Tools and Applications for Mobile Contents, May 13, 2006, Nara, Japan.
  - [18] VietCrypt 2006, International Conference on Cryptology in Vietnam, September 25-28, 2006, Hanoi, Vietnam.
  - [19] CNIS 2006, IASTED International Conference on Communication, Network and Internet Security, Cambridge, USA from October 9-11, 2006.
  - [20] IWSEC 2006, International Workshop on Security, October 23-24, 2006, Kyoto, Japan.
  - [21] ICISC 2006, International Conference on Information Security and Cryptology, November 1 - December 2, 2006, Busan, Korea.
  - [22] AReS 2007, Second International Conference on Availability, Reliability and Security, April 10-13, Vienna, Austria. [3] ISPEC 2007, Information Security Practice and Experience Conference, 7-10 May 2007, Hong Kong, China.
  - [23] ISPEC 2007, Information Security Practice and Experience Conference, 7-10 May 2007, Hong Kong, China.
  - [24] Pairing 2007, International Conference on Pairing-based Cryptography, July 2-4, 2007, Tokyo, Japan.

#### 国内シンポジウムプログラム委員

- [1] 情報処理学会コンピュータセキュリティシンポジウム CSS2006, プログラム委員
- [2] 第29回情報理論とその応用シンポジウム SITA 2006, プログラム委員

### 3) 研究費獲得状況(未来大学外からの財源)(科学研究費、財団助成金、委任経理金(平成17-18年度))

例:

#平成17年度

&財源、たとえば科学研究費補助金

\$研究課題名

%代表者、分担者の別、研究課題参加者数、あるいは〇〇研究所との共同研究(相手機関の協同研究者数など)

¥研究経費(例:平成12年度;800千円、平成13年度;500千円)

- [1] 平成 16-19 年度、科研費、特定領域、新世代の計算限界 -その解明と打破- B06: 暗号システムに対する実装攻撃の適用と限界に関する計算論的研究、分担者
- [2] 平成 17-19 年度、韓国情報通信研究院 (ETRI)、“Secure and Efficient Digital Signatures for Ubiquitous era”、代表者、10,000 千円。
- [3] 平成 17-19 年度、新エネルギー・産業技術総合開発機構 (NEDO)、“Pairing Lite の研究開発”、分担者、23,000 千円。
- [4] 平成 18-19 年度、科研費、基盤研究(C)、公開鍵暗号用の算術技法における安全性を考慮した効率解析と応用、4,000 千円
- [5] 平成 18-20 年度、科研費、基盤研究(B)、利己的ノードを考慮した安全なモバイルアドホックネットワーク構成法の研究、分担者
- [6] 平成 18 年度、科研費、特定領域、情報爆発時代に向けた新しいIT基盤技術の研究、A01-01: 情報ネットワークにおける大規模知識処理のための超高速アルゴリズムの研究、分担者
- [7] その他、民間企業との受託/共同研究・奨学寄付など

- 4) その他 (特許、内地研究 (学内共同研究は除外) および在外研究歴と成果など特記すべきこと。平成 17-18 年度)

**招待講演:**

- [1] 平成 17 年 9 月、北陸先端科学技術大学院大学情報科学研究科セミナー (第 7 回)
- [2] 平成 17 年 10 月、Korea-Japan Joint Workshop on Ubiquitous Network Security, Tokyo.
- [3] 平成 19 年 2 月、韓国 Information Communication University 情報通信学部、Taejon
- [4] 平成 19 年 3 月、韓国梨花女子大学数学部、ソウル
- [5] 平成 19 年 4 月、IPA 組込みセキュリティワークショップ、東京

**客員研究員:**

- [1] 平成 18 年 11 月～、筑波大学産学リエゾン共同センター客員研究員

**博士論文審査委員:**

- [1] 平成 18 年 1 月、Andreas Meyer, Katja Schmidt-Samoa, Department of Computer Science, Darmstadt University of Technology, Germany.
- [2] 平成 18 年 2 月、白勢政明、北陸先端科学技術大学院大学情報科学研究科。

**海外研究プロジェクト審査委員:**

- [1] 平成 17 年 12 月、Austrian Science Fund FWF, Austria
- [2] 平成 18 年 11 月、British Council Science, UK
- [3] 平成 19 年 1 月、Natural Sciences and Engineering Research Council, Canada
- [4] 平成 19 年 3 月、Research Grants Council, Hong Kong, China

## 2 教育業績

- 1) 教育負担の実態 (複数教員で担当する科目の場合は、貴方の分担分のみ) 本項目は時間割に含まれた教科 (補講・補習など教室で行なったものは含む) を調査の対象としております。従って、〇〇研究会、〇〇同好会など、各教員室他で行なったものは、対象外とします。試験

やレポートなどの採点時間も除外します。

例：

#科目名（講義・演習・実習・補講の別）、単位数・必修/選択の別、担当教員数（単独の場合は不要）

&実施期間（平成12年度前期、あるいは平成13年10-11月）、実施コマ数（休講しても補講で補えば算定する）、補講をしなかった休講回数（例：実施13コマ、休講2コマ）

\$実働時間数（全て、実時間合計(推定)値をお願いします）、演習などは一コマ1.5時間を超えていると思われるので、そのような場合は、たとえば一コマ2.2時間などと算定してください（例：実働22.5時間）

%受講登録学生数（例：45名）、平均的出席者数（例：38名；初めは40名、終りは25名など）、単位認定（合格）者数

註：本項目はできるだけ正確にお願いしたいですが、概数でも結構です。記述がない場合は0と判断します

- [1] 数学総合演習 I, II、平成17年度前後期、各2単位、必修、担当教員数2、受講学生90名
- [2] 線形代数学 II、平成17年度後期、2単位、必修、受講学生90名
- [3] 数学総合演習 I, II、平成18年度前後期、各2単位、必修、担当教員数2、受講学生90名
- [4] 線形代数学 I, II、平成18年度前後期、各2単位、必修、受講学生90名
- [5] 情報セキュリティ特論、平成18年度後期、単位、選択、受講学生20名

2) 成績評価方法（その方法を具体的に記載・学生（社会）が納得するような具体的説明。）

また、複数の教員で担当する科目の場合は、取りまとめの方法についても記述してください。

出席率、毎回実施する小テスト、中間テスト、期末テストなどを総合して判断する。

3) 講義方法など改善への努力（FD関連の講演会などの聴講回数、教育内容とそれらの効果について貴方が行われた事柄・目標を具体的に記述して下さい）。

授業評価システムのフィードバックを参考にして講義を改善している。

4) その他（上記以外に特記すべきことがありましたら、簡潔かつ具体的に、箇条書きなどで記述してください。特に、貴方が作られたシラバスと現在教務委員会で検討されている（コース別）講義内容・目標、あるいは JABEE などとの関連、並びに貴方が担当されている科目の位置付けなどについてご意見があれば記して下さい。また、本学は教員の専門分野が多岐にわたっている

ため、相互理解を目的としたコース特有の問題点や、皆さんの教育に対する抱負などを記述して戴いても結構です。)

- [1] 平成 17 年 5 月～平成 18 年 4 月、韓東国博士を、韓国学術振興会 (Korean Research Foundation) のポストドクター (Post Doctor Fellow) として受入れた。
- [2] 平成 18 年 4 月～平成 19 年 9 月、金兌炫氏を、訪問研究員として研究指導した。
- [3] 平成 18 年 6 月～平成 19 年 5 月、柳恩京博士を、韓国学術振興会 (Korean Research Foundation) のポストドクター (Post Doctor Fellow) として受入れた。
- [4] 平成 17 年 4 月～平成 20 年 3 月、白勢政明博士を、NEDO のポスドクとして受入れた。

### 3 大学の管理運営

各種委員会 (委員長・委員、クラス担任、学習指導・生活指導、クラブ活動の顧問等の実績 (具体的に記述してください、できれば実働延べ時間数など))、その他。

- [1] 平成 17 年度、外部評価専門委員会委員
- [2] 平成 17 年度～、セクシャルハラスメント相談委員
- [3] 平成 18 年度～、自己評価専門委員会委員
- [4] 平成 18 年度、システム委員会委員

### 4 その他

資格 (技術士など)、地域への貢献 (地域自治体審議会、委員会等の役員、委員。地域との共同研究・技術相談。公開講座・出前授業・市民向け講演) あるいは提言・御意見など

平成 17 年 8 月、函館市立函館東高校の生徒へ模擬授業を実施した。  
平成 18 年 11-12 月、函館市 IT 企業塾講師として 4 回講演した。