平成１１年度

アジア地域における暗号技術動向と普及に関する調査

平成１２年２月

情報処理振興事業協会

アジア地域における暗号技術動向と普及に関する調査
まとめ

１章の調査概要で示したように、本調査は平成１１年度８月から平成１２年２月の間、中国、香港、インド、韓国、シンガポール、台湾の６ケ国について、暗号技術研究の動向と普及に関する調査を行ったものである。

調査の方法は、まず日本国内の暗号研究専門家に聞き取り調査を行い、その結果を元にアンケートの内容を作成し、調査対象各国の暗号研究専門家に回答を依頼した。アンケートの送付・回収とその後の補充調査は電子メールにて、または１９９９年１１月にシンガポールで開催された「Asiacrypt99」での直接聞き取り調査にて行った。アンケートを送付した人数は２１名で、そのうち１９名から回答が得られた。

調査の結果、暗号技術の実用化や普及度、暗号に関する政府や国民の意識、そして暗号研究機関の規模や数などは、地域によってかなりの差があることが分かった。また、電子署名法や電子商取引法などの法整備が進んでいる国（地域）では、政府と産業界がともに積極的な研究・普及活動を行っており、それに伴うビジネスも急速に発展していくことが予想される。このようなアジア諸地域の事情から、日本における今後の研究課題や暗号の実用化について参考となる点も多いだろう。

また、今回の調査対象に日本は含まれていないが、アンケートの回答の中には日本も含めた調査を望む声が多く聞かれた。

以下に、各地域の概要を記載する。

（１）中国

暗号の研究活動は主にChinese Academy of Sciences　（中国科学院）や大学などの学術機関で行われている。理論的な研究は盛んだが、実用面ではまだ初期段階といえる。電子署名法案はまだ作成されていない。

（２）香港

電子商取引法が２０００年初めに成立する予定。政府主導型のPKI/CAプロジェクトのもとで、確定申告や自動車登録、投票などの公共サービスがオンライン化されており、PKI構築が実用面でかなり進んでいる。暗号学会や協会はなく、大学が個々に研究を行っている。大規模な国際暗号学会もまだ開かれていない。

（３）インド
国内にある暗号研究機関と研究者の数は少なく、むしろ海外に出て研究を行う専門家が多い。今のところPKIシステムは構築されておらず、電子署名法などの法整備も進んでいない。学会については今のところ暗号より数学の研究発表が盛んだが、Asiacrypt2002の開催地に立候補するなど、今後は国内外の学会を定期的に開催して暗号の技術と知識を広めたいと望んでいる。

（４）韓国
暗号機関と研究者数ともに充実している。政府・企業・大学各レベルで暗号学会・研究会の開催や国際間プロジェクトが盛んに行われている。電子署名法は１９９９年７月に成立し、CAの運営や下部認証局の整備に政府が積極的に関わっている。暗号研究者たちのウェブページへのリンクサイトが暗号研究の啓蒙活動のために作成されており、国内はもとより他国の研究家たちにも好評。

（５）シンガポール
電子商取引法が１９９８年に成立しており、PKIとCAシステムの整備・実用化・運営と市民のオンラインシステム利用度は、今回調査対象となった６地域の中で最も進んでいるという印象を受けた。暗号技術の研究とシステム開発が最も盛んなのはNational University of Singapore。国内のワークショップや国際的な学会の開催数も多い。

（６）台湾
電子署名法は現在国会審議中で、近く成立する予定。研究機関ではCCISA (Chinese Cryptology and Information Security Association)、企業では Chunghwa Telecom Co., Ltd.（中華電信）の研究開発活動が盛ん。PKI、CAシステムの構築も進められており、現在政府や民間レベルで様々なCA機関が設立されている。法制度やシステム構築が進むにつれ、電子商取引もますます盛んになることが予想される。

以上、諸地域の調査結果を記載した。近年、アジアにおける暗号認証技術の普及は目覚ましいものがあり、諸作業の電子化やオンライン化に伴い、今後も引き続きかなりの速度で普及が進むものと思われる。日本では学術的な研究は盛んだが、実用化の面で遅れをとることが懸念されている。今後も、暗号技術の安全性についての啓蒙活動や、諸外国との技術交流を積極的に行い、日本だけでなくアジア全体が互いに発展していけるような関係を築くことが望まれる。

目次

1.　調査概要

1.1　調査の背景

近年、アジアにおける暗号技術の普及は目を見張るものがある。特にシンガポールなどでは電子商取引を国家プロジェクトとして行うのみならず、日本などとの連携による国際プロジェクトとして展開している。これに伴って、その安全性を支える暗号認証技術（以下暗号技術）の普及も進んでいる。

この動向に呼応するように、暗号国際会議のひとつAsiacrypt でも開催を望む国がたくさん出てきている。１９９９年はシンガポールで行われ、２０００年は日本で行われる。更にオーストラリア、台湾、インド、香港、ニュージーランドが開催を希望している。既に、日本、韓国、中

国、オーストラリアは開催している。この事実は、ビジネスにつながるプロジェクトのほかに、研究の上でも暗号が盛んに行われつつあることを示しており、基礎研究の醸成が見られる。この分野では現在日本に一日の長があるのは事実であるが、追いつき追い越される可能性も否定できない。特に、実施、普及の面で遅れをとることが懸念される。

1.2　調査目的

これからのアジアにおける暗号研究のあり方を見ると、今後日本の取るべき道は競争していくことではなく、お互いの独自性を尊重しつつ協調できるところは協調しながら、暗号技術の発展を目指すことにあると考えられる。このためには、まずアジアにおける暗号技術の研究、開発、普及の度合いを調査しその実態を把握することが必須である。

本調査では、アジアにおける暗号研究の有力国・地域（以下地域と呼ぶ）に焦点を絞り、各地域での研究組織・研究分野・代表的プロジェクト等を調査した。

1.3　調査指針

調査研究の方法は、調査対象地域を絞って暗号技術の研究と普及に関する事前聞き取り調査、アンケート調査、補充調査、および文献調査により行う。

1.4　調査対象地域

調査対象地域は、下記の６地域とする。

韓国
中国
台湾
香港
シンガポール
インド

1.5　事前聞き取り調査

国内の暗号研究専門家にあらかじめ聞き取り調査を行い、各地域の現状を把握した。また、各調査対象地域においてアンケート記入を依頼する対象者（各地域２名以上）を決定した。更に、アンケートの情報の確認を行った。

1.6　アンケート調査

事前聞き取り調査の結果をもとにアンケートを作成し、各調査対象地域のアンケート記入依頼者にあらかじめ用意したアンケートを配布することにより調査を行った。なお、調査情報は第４条に列挙された情報を含んでいる。

1.7　補充調査

アンケート調査によって得られた回答の内容確認、または追加調査が必要と認められたときには適宜補充調査を行った。

1.8　文献調査

１９９９年Asiacrypt でのすぐれた研究を選び、それぞれの解説を作成した。

1.9　調査内容

1.9.1　各地域の研究状況

各地域における研究体制を把握するため、下記の情報を調査する。

- 主要研究機関一覧
  - 大学
  - 企業
  - 政府（または行政機関）
  - 団体
- 代表研究者一覧
- プロジェクト一覧
  - 政府（または行政機関）
  - 企業

1.9.2　研究内容

各地域で行われている研究の内容とその進捗状況を把握するため、下記の情報を調査した。

- 研究機関の特長
- 研究者と専門分野
- 研究・プロジェクトの概要
- 今後行う予定の研究・プロジェクト

1.9.3　普及状況

各地域におけるＰＫＩおよび電子商取引の普及度を把握するため、下記の情報を調査した。

- ＰＫＩの導入実績および予定
- 電子商取引の現状および将来の方向性

2.　調査結果

2.1　中国の主要暗号研究機関と研究内容

2.1.1　中国(1)　Chinese Academy of Sciences

暗号研究機関に関する一般情報	
暗号研究機関名	Engineering Research Center for Information Security Technology, Chinese Academy of Sciences　（中国科学院）
組織の種類	研究機関 教育機関
所在地	52 Sanlihe Rd. Beijing , China Postcode:100864 Tel:68597289 Fax:68512458 <http://www.cas.ac.cn/cas.html>
代表研究者名	Sihan Qing China Computer Federation <http://www.ccf.org.cn/>
代表研究者肩書	Director of Engineering Research Center for Information Security Technology Chinese Academy of Sciences
代表研究者専門分野	ネットワークセキュリティ、暗号
組織の概要	The Chinese Academy of Sciencesは1949年11月1日に設立された、中国内で最大規模の科学技術研究・開発・教育機関。５つの部門（Division of Mathematics and Physics,Division of Chemistry, Division of Biological Science, Division of Earth Science, Division of Technological Sciences）があり、123機関、500以上の事業所、20以上の賛助機関（非営利団体）から成る。 支部は13都市（上海、南京、合肥、長春、藩陽、武漢、広州、成都、昆明、西安、蘭州、新疆、淮南）にある。 大学、大学院、研究所などの教育機関も多数設立、運営している。 参考URL：<http://wmcgroup.com/cas.htm>
暗号研究グループに関する情報	
研究機関名	Engineering Research Center for Information Security Technology Chinese Academy of Sciences
業種	研究機関
研究グループの人数	５０人～９９人

暗号研究・開発プロジェクトリーダー	Wenling Wu,　Associate Professor 専門：暗号設計, 暗号解読
研究グループ主要メンバー	Bao Li, Associate Professor
研究トピック	暗号設計、暗号解読、電子署名、プロトコル
研究グループの特徴	
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	AES アルゴリズムの暗号解読
プロジェクトの規模	プロジェクトグループ内のみ
プロジェクトリーダー	Wenling Wu, Associate Professor China Computer Federation <http://www.ccf.org.cn/>
プロジェクト主要メンバー	Bao Li, Associate Professor China Computer Federation <http://www.ccf.org.cn/>
プロジェクトグループの人数	１０人～ ２９人
研究・プロジェクトの概要	研究結果のいくつかは下記で発表されている。 (1)"Cryptanalysis of some AES candidate algorithms", Information and Communication Security (ICICS'99),LNCS No.1726, Springer-Verlag (1999), p13-21. (2)"Comments on the 15 AES Candidate Algorithms" Journal of Software, NIST of USA, 1999-10-3-225-230.（中国語）
実施段階	研究段階
プロジェクトのスポンサー	Chinese Academy of Sciences　（中国科学院）
今後行う予定の研究・プロジェクト	新しい暗号の設計と解読

2.1.2　中国(2)　Chinese Academy of Sciences (SKLOIS)

暗号研究機関に関する一般情報	
暗号研究機関名	State Key Laboratory of Information Security (SKLOIS) Chinese Academy of Sciences

組織の種類	教育機関 研究機関
所在地	SKLOIS Graduate School of USTC (University of Science and Technology of China) #19A Yu-Quan road Beijing , 100039 , PRC Tel:+86-10-6821-3046 Fax:+86-10-6821-0501 <http://www.ustc.edu.cn/> (USTC)
代表研究者名	Dingyi Pei
代表研究者肩書	Chairman, Academic committee of SKLOIS
代表研究者専門分野	認証コード、公開鍵暗号システム
組織の概要	Chinese Academy of Sciencesの下部組織。暗号とインフォメーションセキュリティに関する理論的・実際的なリサーチ研究を行う。
暗号研究グループに関する情報	
研究機関名	State Key Laboratory of Information Security
業種	教育機関 研究機関
研究グループの人数	21人
暗号研究・開発プロジェクトリーダー	Dengguo Feng 専門分野：ロジック関数スペクトラムと電子支払システム
研究グループ主要メンバー	Zongduo Dai Keqin Feng Shuwang Lu Dingyi Pei Sihan Qing
研究トピック	暗号アルゴリズムとセキュリティプロトコル
研究グループの特徴	数学とコンピュータサイエンスの組み合わせ
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	ネットワークにおける情報セキュリティ
プロジェクトの規模	国内の他の２機関との共同プロジェクト (1) Institute of software、Chinese Academy of Sciences <http://www.ios.ac.cn/English/index.htm> (2) Xidian University <http://www.xidian.edu.cn/english/index.htm>

プロジェクトリーダー	Dengguo Feng, SKLOIS
プロジェクト主要メンバー	Zongduo Dai Keqin Feng Shuwang Lu Dingyi Pei Sihan Qing Yuming Wang (Xidian University)
プロジェクトグループの人数	9 人
研究・プロジェクトの概要	(1) ネットワークセキュリティシステムの理論モデル (2) セキュリティプロトコル (3) 暗号アルゴリズム
実施段階	研究段階
プロジェクトのスポンサー	Chinese Academy of Sciences
今後行う予定の研究・プロジェクト	

2.1.3　中国(3)　Xidian University

暗号研究機関に関する一般情報	
暗号研究機関名	Xidian University　（西安電子科技大学）
組織の種類	大学
所在地	Xidian University, Xi'an,　（西安） Shaanxi Province, 710071, P.R. China <http://www.xidian.edu.cn/english/index.htm>（英語） <http://www.xidian.edu.cn/>（中国語）
代表研究者名	Guozhen Xiao < http://www.xidian.edu.cn/english/HTTP/WHO/gzxiao/gzhxiao.htm>
代表研究者肩書	(1) Chairman of Institute of Information Security and Privacy　（情報安全機密研究所　所長） (2) Vice Chairman of Chinese Cryptologic Society　（中国暗号学会　副理事長） (3) Asiacrypt Steering Committee Member　（Asiacrypt運営委員）
代表研究者専門分野	情報理論, 暗号, コーディング

組織の概要	Xidian Universityは６学部（Communication Engineering、Electronic Engineering、Computer Science、Electronics Mechanics、Economical Management、Adult Education）１７学科、６０以上のコースがある。スタッフ３４００名、生徒数約１２，４００名　（うち大学院生７６０名）。国家レベルの研究所が３つ、特別研究のための研究施設が３０以上ある。これまでに2200件以上の国家プロジェクトを請け負った。 参考URL<http://www.xidian.edu.cn/English/index.htm>
暗号研究グループに関する情報	
研究機関名	Research Institute of Information Security and Privacy College of Communications Engineering Xidian University
業種	教育機関
研究グループの人数	約５０名
暗号研究・開発プロジェクトリーダー	Guozhen Xiao 専門：情報理論、暗号、コーディング
研究グループ主要メンバー	Guozhen Xiao, Professor Yuming Wang, Professor Xinmei Wang, Professor
研究トピック	(1)ストリーム/ブロック暗号 (2)暗号アルゴリズム (3)電子署名と公開鍵暗号システム 他に、通信システム、ネットワークシステム、モバイル通信の研究を行っているリサーチグループもある。
研究グループの特徴	グループメンバーの人数が多く、生徒の専門分野が多様　（コンピュータサイエンス、コミュニケーション、数学など）。
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	鍵の配送と鍵管理を含むブロック暗号を、企業数社のために設計する。
プロジェクトの規模	プロジェクトグループ内のみ
プロジェクトリーダー	Guozhen Xiao
プロジェクト主要メンバー	Guozhen Xiao, Professor Yuming Wang, Professor Xinmei Wang, Professor

プロジェクトグループの人数	約５０名
研究・プロジェクトの概要	中国では現在、マルチレベルセキュリティのための暗号アルゴリズムを決定する検討作業が行われている。政府や軍部用のセキュリティは企業用よりも高くなければならないので、マルチレベルなアルゴリズムが必要である。現在、当プロジェクトメンバーは企業用のブロック暗号の開発作業に取り組んでいる。
実施段階	研究段階
プロジェクトのスポンサー	政府、教育基金、企業、銀行、Xidian University
今後行う予定の研究・プロジェクト	ストリーム暗号、ブロック暗号

2.1.4　中国のPKI (Public Key Infrastructure)と電子商取引（EC）の現状および将来の方向性

PKI、CAシステムの現状	Xidian University が、銀行で使用する鍵配布のためのブロック暗号とストリーム暗号を設計し、１９９８年に実用化された。中国では暗号の理論的な研究は盛んに行われているが、実用レベルではまだ初期段階といえる。PKIの整備と電子商取引の実用化に向けて、今後も盛んに研究が行われることが予想される。
PKI,CAシステムの将来と傾向	中国人民銀行（The People's Bank of China）がPKI/CAに関するプロジェクトを行っている。
電子商取引の現状	初期の段階
電子商取引の将来と傾向	The Ministry of Foreign Trade and Economic Cooperation, PRC（対外貿易経済合作部<http://www.moftec.gov.cn/>）や国内の銀行数行で電子商取引に関するプロジェクトが進行中。
PKI/CAに関する法律の現状	将来法案が提出される予定（時期は不明）

2.1.5　中国の暗号学会および論文誌

国内の暗号学会、協会名	Chinese Cryptologic Society
	Chinese Institute of Computer Science (CICS)
暗号学会誌の発行	各学会のProceedingsが出版されている。暗号に関する定期刊行物はない。

国内で開催されている学会	ChinaCrypt １９９４年に正式な暗号のカンファレンス「ChinaCrypt」第一回目がUniversity of Peking （北京大学）で開催された。以降、隔年開催。2000年は湖北省武漢で開催。
	第一回 Chinese Conference on Information and Communications Security (CCICS'99) 主催：　Engineering Research Center for Information Security Technology, Chinese Academy of Sciences. Proceeding：中国 Science Press より発行
国際的な学会	Asiacrypt'98 （北京）<http://www.bta.net.cn/csp/isdata/index.htm> 主催：Asiacrypt Steering Committee (ASC) スポンサー：State Key Laboratory of Information Security (SKLOIS) 協賛：International Association for Cryptology Research (IACR) <http://www.iacr.org/> 日時：1998年10月18日～22日 場所：北京 予稿集：Advances in Cryptology - ASIACRYPT '98, LNCS no.1514, Springer-Verlag (1998)
	第16回 IFIP (International Federation for Information Processing ：国際情報処理学会) World Computer Congress　<http://www.wcc2000.org/> 主催：The Chinese Institute of Electronics　<http://www.cie-china.org/> China Computer Federation　<http://www.ccf.org.cn/> Chinese Institute of Communication 日時：2000年8月21日～25日 場所：北京
	International Conference on Information and Communications Security (ICICS'97) 主催：　Engineering Research Center for Information Security Technology, Chinese Academy of Sciences 予稿集：Information and Communication Security (ICICS'97), LNCS No.1334, Springer-Verlag (1997)

2.2　香港の主要暗号研究機関と研究内容

2.2.1　香港(1)　City University of Hong Kong

暗号研究機関に関する一般情報	
暗号研究機関名	City University of Hong Kong　（香港城市大学）
組織の種類	教育機関
所在地	City University of Hong Kong Tat Chee Avenue, Kowloon Hong Kong TEL:(852) 2788 7654（代表） FAX:(852) 2788 1167 （代表） Email:puo@cityu.edu.hk < http://www.cityu.edu.hk/>
代表研究者名	Chan H. Lee
代表研究者肩書	Associate Professor
代表研究者専門分野	ネットワーク・情報セキュリティ
組織の概要	1984年1月に設立。規模：生徒数約13,500人。プログラム数90。スタッフ数約800人。 参考URL：<http://www.cityu.edu.hk/cityu/introd.htm>
暗号研究グループに関する情報	
研究機関名	Department of Computer Science City University of Hong Kong
業種	大学
研究グループの人数	１０人以下
暗号研究・開発プロジェクトリーダー	
研究グループ主要メンバー	Chan H. Lee Xiaotie Deng Zhonping Qin Haufei Zhu
研究トピック	否認不可暗号、公開鍵方式、セキュリティプロトコル
研究グループの特徴	主に実用化のための暗号研究を中心に行っている。
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	(1) 効率的な否認不可認証方式 (2) ダイナミックパスワード方式 (3) 匿名デジタルキャッシュ方式 (4) イントラネットのPKI

プロジェクトの規模	プロジェクトグループ内のみ
プロジェクトリーダー	Chan H. Lee（City University of Hong Kong） Xiaotie Deng　（City University of Hong Kong）
プロジェクト主要メンバー	Huafei Zhu　(Zhejiang University)
プロジェクトグループの人数	
研究・プロジェクトの概要	不認不可能な認証プロトコルの有効な方式を考案し、パスワード方式の基礎を構築した。これから完成に向けて実験とセキュリティ評価を行う予定。
実施段階	研究段階
プロジェクトのスポンサー	City University of Hong Kong
今後行う予定の研究・プロジェクト	電子入札制度と電子投票システムの考案

2.2.2　香港(2)　The Open University of Hong Kong

暗号研究機関に関する一般情報	
暗号研究機関名	The Open University of Hong Kong　（香港公開大学）
組織の種類	大学
所在地	The Open University of Hong Kong 30 Good Shepherd StreetHomantin, Kowloon Hong Kong < http://www.oli.hk/>
代表研究者名	Siu Leung Chung < http://balinux.ouhk.edu.hk/~school/staff/slchung.htm>
代表研究者肩書	Associate Professor School of Business and Administration
代表研究者専門分野	インターネットセキュリティ、侵入検出、ECセキュリティ
組織の概要	規模：現在約1,500名（そのうちフルタイム400名）のスタッフと約24,000名以上の生徒を持つ。４つの学部がある （School of Arts and Social Sciences, School of Business and Administration, School of Education and Languages, and School of Science and Technology）

	参考URL： <http://www.ouhk.edu.hk/~powww/figures1.htm#program>
暗号研究グループに関する情報	
研究機関名	The Open University of Hong Kong
業種	大学
研究グループの人数	１０人以下
暗号研究・開発プロジェクトリーダー	Siu Leung Chung 専門：コンピュータサイエンス
研究グループ主要メンバー	
研究トピック	侵入検出
研究グループの特徴	
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	侵入検出方法に関する調査
プロジェクトの規模	プロジェクトグループ内のみ
プロジェクトリーダー	Dr. Siu Leung Chung Associate Professor The Open University of Hong Kong
プロジェクト主要メンバー	
プロジェクトグループの人数	
研究・プロジェクトの概要	現在知られている侵入検出方法に関する調査
実施段階	実験段階
プロジェクトのスポンサー	The Open University of Hong Kong
今後行う予定の研究・プロジェクト	

2.2.3　香港のPKI (Public Key Infrastructure)と電子商取引（EC）の現状および将来の方向性

PKI、CAシステムの現状	2000年から、政府主導型のPKI/CAプロジェクト「Digital 21」構想が実施される予定。香港の郵政省であるHong Kong Post <http://www.hongkongpost.com/>が開発運営を任され、CA運営の責任を担う。「Digital 21」とは公共サービスをインターネット上で行えるようなシステムで、Information Technology and Broadcasting Bureau <http://www.info.gov.hk/itbb/content/index.htm>が1998年11月に発表した。その一貫として「Electronic Services Delivery (ESD：公共服務電子化)」プロジェクトが進行中。ESDの第一段階は2000年10月より開始され、確定申告や自動車の登録、投票などがオンライン上で行えるようになる予定。参考URL：<http://www.info.gov.hk/itbb/new/presentation-hku.ppt> 企業側も独自のPKI/CAシステムの構築を計画・準備中で、例として香港の49銀行をメンバーに持つJETCO(Joint Electronic Teller Services Ltd)がある。参考URL：<http://www.tdc.org.hk/prodmag/electron/ele199905in.htm#1>
PKI,CAシステムの将来と傾向	PKI/CAに基づく安全なトランザクションは、最初は政府レベルの事業として行われ、その後、民間によるCA構想が描かれるだろう。民間の各企業や組織レベルでの作業のオンライン化、PKI/CAインフラ整備は既に始まっており、２，３年のうちには一般的になると予想される。
電子商取引の現状	企業組織間（B to B）ECは盛んになりつつあるが、一般消費者と販売業者間(B to C)ECはあまり普及していない。その理由は、PKIシステムと法的整備がまだ完全ではないため、あまり安全ではないという認識が一般消費者の間にあるためと考えられる。だがこの状況は変化しつつあるので、２０００年にはECの実施はもっと盛んに行われるようになると予想される。
電子商取引の将来と傾向	政府や民間企業が主導のプロジェクトの数も増え、電子商取引がますます盛んになるだろう。様々なタイプの電子商取引トランザクションを行うために、政府は市民に対して郵政省のCAを推奨すると思われる。
PKI/CAに関する法律の現状	電子商取引法は１９９９年７月１４日に議会に提出され、現在審議中。2000年初めには成立する予定。 Electronic Transactions Bill：参考URL<http://www.info.gov.hk/itbb/new/index1.htm>

2.2.4　　香港の暗号学会および論文誌

国内の暗号学会、協会名	なし
暗号学会誌の発行	なし
国内で開催されている学会	International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC'99) 日時：1999年7月5日～8日 主催：City University of Hong Kong < http://www.cs.cityu.edu.hk/~cryptec/cryptec.htm>
国際的な学会	なし

2.3　インドの主要暗号研究機関と研究内容

2.3.1　インド(1)　Indian Statistical Institute

暗号研究機関に関する一般情報	
暗号研究機関名	Indian Statistical Institute, Calcutta
組織の種類	教育機関 研究機関
所在地	203, Barrackpore Trunk Road Calcutta 700035 INDIA TEL:91-33-577 2088 FAX:91-33-577 6680 <http://www.isical.ac.in/>
代表研究者名	Bimal Roy
代表研究者肩書	Professor
代表研究者専門分野	暗号作成、組合せ論
組織の概要	Indian Statistical Institute (ISI)は1931年12月17日にインド政府により設立された教育・研究機関。単位取得は４つの学科(Statistics, Mathematics, Computer Science, and Economics)に限られているが、研究グループのテーマは多岐に渡る。規模：教職員100名～299名、大学院生が600名～700名、併せて約1000人。
暗号研究グループに関する情報	
研究機関名	Indian Statistical Institute

業種	研究機関
研究グループの人数	11
暗号研究・開発プロジェクトリーダー	Bimal Roy 専門：暗号学、組合せ論
研究グループ主要メンバー	Rana Barua Pabitra Pal Choudhury Aditya Bagchi Sarbani Palit Mamtaj Modi Arindam De Joydeep Bhanja K. Sikdar Palash Sarkar Subhamoy Maitra
研究トピック	ストリーム暗号、ブール関数, 暗号解読、データベースセキュリティ
研究グループの特徴	メンバーの専門の多様性
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	ストリーム暗号、ブール関数、暗号解読、データベースセキュリティ
プロジェクトの規模	暗号解読とストリーム暗号については、国内の他機関内の研究グループ「Bengal Engineering College （Shibpur, West Bengal, India）」とのジョイントプロジェクト。インターナショナルプロジェクトは現在行っていない。
プロジェクトリーダー	Bimal Roy
プロジェクト主要メンバー	Dr. Alok Datta Dr. P. Pal Choudhury
プロジェクトグループの人数	
研究・プロジェクトの概要	下記のカンファレンスに出席し研究発表を行っている。 (1) Crypt99（1999年8月） 予稿集：Advances in Cryptology - CRYPTO '99, LNCS no.1666, Springer-Verlag (1999) (2) ACISP'99(Australasian Conference on Information Security and Privacy) （1999年4月）

	予稿集：Information Security and Privacy, ACISP'99 (ACISP'99),LNCS no. 1587, Springer-Verlag (1999) (3) Asiacrypt99（1999年１１月） 予稿集："Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining Function", Advances in Cryptology - ASIACRYPT '99, LNCS no.1716, Springer-Verlag (1999), p306-320.
実施段階	研究段階（現在は理論的な研究段階を中心に行っている。国内の企業が実用化に興味を持てば実験段階に移っていくであろう。）
プロジェクトのスポンサー	Indian Statistical Institute
今後行う予定の研究・プロジェクト	未定

2.3.2　インド(2)　Institute of Mathematical Sciences

暗号研究機関に関する一般情報	
暗号研究機関名	Institute of Mathematical Sciences
組織の種類	研究機関
所在地	Institute of Mathematical Sciences C.P.T Complex Taramani, Chennai India 600113 TEL:+91-44-235 1856 FAX: +91-44-235 0586 <http://www.imsc.ernet.in/>
代表研究者名	Ramachandran Balasubramanian
代表研究者肩書	Senior Professor
代表研究者専門分野	Number Theory [Zeta Function, Additive Number Theory （例：Waring's Problem）, Combinatorial Number Theoryを含む]。 楕円曲線、暗号作成法
組織の概要	1962年に設立された国立研究・教育機関。主に３つの分野(Mathematics, Theoretical Physics and Theoretical Computer Science)の研究を行う。 規模：職員約４０名。Master, Ph.Dコースがある。参考URL： <http://www.imsc.ernet.in/Info/>
暗号研究グループに関する情報	
研究機関名	Institute of Mathematical Sciences

業種	教育・研究機関
研究グループの人数	５０名以下
暗号研究・開発プロジェクトリーダー	今のところ、研究所内で暗号研究を行っているのはProf. Balasubramanianのみ。
研究グループ主要メンバー	
研究トピック	
研究グループの特徴	
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	Prof. Balasubramanianは基本的には数論学者だが、暗号との関連性に興味を持ち暗号研究を開始した。現在は理論的な研究のみを行っている。実用性はあまり重視していないため、プロジェクトは現在持っていない。 従って、プロジェクトについての他の質問には回答なし

2.3.3　インドのPKI (Public Key Infrastructure)と電子商取引（EC）の現状および将来の方向性

PKI、CAシステムの現状	現時点では商用も私用もシステムが構築されておらず、一般市民はあまり興味を持っていない。
PKI,CAシステムの将来と傾向	将来的には政府が実施するかもしれないが、今のところは不明。これが今後良いビジネスになると考えれば、企業がもっと興味を示して参入するかもしれないが、現在インドではシステムが整っておらず、まだ研究の段階。
電子商取引の現状	まだ知名度が低い
電子商取引の将来と傾向	CAもPKIも電子商取引も、ビジネスチャンスになると考える人が多く出てくれば将来的に変わっていくだろうが、今のところはほとんどいないので予測できない。
PKI/CAに関する法律の現状	法律はまだ制定されていない。

2.3.4　インドの暗号学会および論文誌

国内の暗号学会、協会名	数学の学会はあるが、暗号に特定された学会はまだ設立されていない。

暗号学会誌の発行	なし
国内で開催されている学会	Indian Statistical Institute の主催で、2000年12月10日～13日に「INDOCRYPT」第１回を開催する。 <http://www.isical.ac.in/~indocrypt/> ２回目以降は、できれば２年に１度は開催したい。国内外の暗号専門家をスピーカーとして招き、国内の政府機関や企業に暗号についての知識・技術をもっと広めたい。
国際的な学会	Asiacrypt 2002の開催地候補に応募している（Indian Statistical Institute がオーガナイザー）。2000年以降は、国際的規模の暗号カンファレンスを年１回は開催したい。 他の国際学会は、暗号がテーマではないが、High Performance ComputingとVLSI (Very Large Scale Integration) の設計をテーマとする"Computer Science Conference"が開催される。

2.4　韓国の主要暗号研究機関と研究内容

2.4.1　韓国(1)　ETRI (Electronics and Telecommunications Research Institute)

暗号研究機関に関する一般情報	
暗号研究機関名	ETRI (Electronics and Telecommunications Research Institute：電子通信研究所)
組織の種類	研究機関
所在地	161 Kajong-Dong, Yusong-Gu Taejon,　305-350, Korea <http://www.etri.re.kr/>
代表研究者名	Choonsik Park
代表研究者肩書	Director
代表研究者専門分野	情報セキュリティ
組織の概要	ETRIは1976年に設立された国家研究機関の１部門。主な業務は、電気通信技術や半導体技術などの研究開発。1998年4月に組織の再編を行い、現在は４つの専門技術研究所（スイッチング＆トランスミッションテクノロジー、ラジオ＆ブロードキャスティングテクノロジー、コンピュータ＆ソフトウェアテクノロジー、マイクロエレクトロニクステクノロジー）を持ち、基礎技術研究や情報セキュリティなど７つの部署がある。

	参考URL<http://www.etri.re.kr/> 規模：従業員約１０００名以上
暗号研究グループに関する情報	
研究機関名	ETRI（Electronics and Telecommunications Research Institute）
業種	研究機関
研究グループの人数	
暗号研究・開発プロジェクトリーダー	Choonsik Park 専門：情報セキュリティ
研究グループ主要メンバー	Choonsik Park
研究トピック	情報セキュリティとECセキュリティ
研究グループの特徴	
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	
プロジェクトの規模	プロジェクトグループ内のみ
プロジェクトリーダー	Choonsik Park, Director, ETRI
プロジェクト主要メンバー	
プロジェクトグループの人数	
研究・プロジェクトの概要	情報セキュリティの応用システムの研究開発
実施段階	研究段階 実験段階 実用段階 （プロジェクトによって異なる）
プロジェクトのスポンサー	政府
今後行う予定の研究・プロジェクト	次世代の情報セキュリティ

2.4.2　韓国(2)　Information and Communications University

暗号研究機関に関する一般情報	
暗号研究機関名	Information and Communications University
組織の種類	教育機関（大学）
所在地	P.O.Box 77. Yusong,Taejon, Korea Zipcode：305-600 Tel: (042)866-6014 <http://www.icu.ac.kr/english/index.html>
代表研究者名	Kwangjo Kim <http://www.icu.ac.kr/cgi-bin/professor_eng/professor_profile_eng.cgi?p_no=30>
代表研究者肩書	Associate Professor, School of Engineering
代表研究者専門分野	暗号、情報セキュリティ：理論と応用
組織の概要	ICUは1997年12月に、Ministry of Information and Communications（郵政省）とETRIその他の電気通信産業界の出資により設立された。教授と生徒の割合は１：６。２学部（School of Engineering、School of Management）８学科（Computer and Information Systems Group、Multimedia Information and Communication、Broadband Network、Optical Communications and Photonics、Wireless Telecommunication、Semiconductor Technology、Industrial Management、IT-MBA）を提供している。 参考URL： <http://www.icu.ac.kr/english/academic/department/engineering.html>
暗号研究グループに関する情報	
研究機関名	Cryptology and Information Security Lab Information and Communications University <http://vega.icu.ac.kr/~cais/>
業種	研究室
研究グループの人数	１１名（Professor１名、Ph. D Student　１名、　M.S. Student ９名）
暗号研究・開発プロジェクトリーダー	Kwangjo Kim

研究グループ主要メンバー	ByoungCheon Lee Weonkeun Huh Moonseog Seo Kyubeom Hwang Heesun Kim Joonsang Baek Kuk-Hwan An Jae-Seung Go Hyun-Cheol Park Bo-Yeun Song
研究トピック	「研究・プロジェクトの概要」を参照
研究グループの特徴	
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	(1) 暗号アプリケーションプログラムインターフェース（Crypto API） (2) 否認防止の標準化 (3) モバイル通信の認証技術
プロジェクトの規模	研究室内だけのものから国内の他機関や国際ジョイントプロジェクトなど、様々な規模のプロジェクトがある。「研究・プロジェクトの概要」を参照。
プロジェクトリーダー	Kwangjo Kim
プロジェクト主要メンバー	
プロジェクトグループの人数	Prof. Kim個人のプロジェクトは学生がメンバー。現在のプロジェクトは５人～８人くらいで活動している。
研究・プロジェクトの概要	<http://vega.icu.ac.kr/~kkj/>　Prof.Kim個人のサイト。ETRIから大学に移ってからの２年間のプロジェクトが掲載されている。 国際間プロジェクト （１）シンガポールとの国際プロジェクトを計画中（National University of Singapore　の　Prof.Lamと共同研究）。これは、韓国とシンガポール間でクロスボーダーPKIを利用した電子商取引を行うもの。まだ実施段階ではないが、成功した場合、シンガポールと韓国はそれぞれ日本とも同様の共同プロジェクトを行いたい意向。 （２）東大の今井教授とともに、韓国・日本間でSETプロトコルの設定を計画中。韓国政府に提案したがまだ採用されていない。試験が終わった段階で政府側に予算が確保できれば再度提案する予定。現在、理論的な検討段階。

	国家プロジェクト ETRIと共同研究中。スマートカード、テレコミュニケーションアプリケーションに関する研究。
実施段階	研究段階
プロジェクトのスポンサー	政府、企業
今後行う予定の研究・プロジェクト	モバイル電子商取引 （携帯電話を使って電子商取引を行う計画。韓国では特に証券会社と通信会社が興味を持っている分野。）

2.4.3 韓国(3) KIISC (Korea Institute of Information Security & Cryptology)

暗号研究機関に関する一般情報	
暗号研究機関名	KIISC (Korea Institute of Information Security & Cryptology：韓国情報保護学会)
組織の種類	政府・教育機関
所在地	<http://www.kiisc.or.kr>
代表研究者名	Kil-Hyun Nam
代表研究者肩書	(1)Professor, Korea National Defense Univerisity Soosack-Dong, Eunpyung-Gu, Seoul, 122-090, Korea (2)Chairman of KIISC
代表研究者専門分野	暗号、情報セキュリティ、アルゴリズム解読
組織の概要	規模：500人～ 999人
暗号研究グループに関する情報	
研究機関名	Korea Institute of Information Security & Cryptology (KIISC)
業種	研究機関 非営利団体
研究グループの人数	１０人以下
暗号研究・開発プロジェクトリーダー	KIISC メンバーの教授陣 専門分野：暗号、情報セキュリティ、コンピュータサイエンス、数学
研究グループ主要メンバー	情報セキュリティ
研究トピック	

研究グループの特徴	KIISCは学術研究機関なので、固定された研究グループはない。
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	政府や企業から特定の研究課題を受け取った時のみ、臨時のリサーチグループを組織する。　よって、プロジェクトについての他の質問には回答なし。
プロジェクトのスポンサー	KISA(Korea Infromation Security Agency), Ministry of Information and Communication
今後行う予定の研究・プロジェクト	

2.4.4　韓国(4)　KISA (Korea Information Security Agency)

暗号研究機関に関する一般情報	
暗号研究機関名	KISA (Korea Information Security Agency：韓国情報保護センター)
組織の種類	政府機関
所在地	5th FL., Dong-A Tower1321-6 Secho-Dong, Secho-Gu Seoul 137-070, KOREA <http://www.kisa.or.kr>
代表研究者名	Sung-Jun Park <http://dosan.skku.ac.kr/~sjpark/>
代表研究者肩書	Project Manager / Senior Member of Technical Staff Information Security Technology Division
代表研究者専門分野	キーリカバリー、暗号システムの設計と解析、電子署名
組織の概要	KISAはMinistry of Information and Communicationの下に１９９６年４月に設立された。 参考URL。民間のセキュリティ企業の窓口。ファイアウォールやCAの基準を策定している。 規模：１００人～２９９人 参考URL：<http://www.kisa.or.kr/index_e.html> また、韓国内の暗号研究者のウェブページへのリンク一覧を作成・管理している。 KRyptoGate：<http://dosan.skku.ac.kr/~sjkim/kryptogate.html>

暗号研究グループに関する情報	
研究機関名	Cryptographic Technology Team Korea Information Security Agency (KISA)
業種	政府機関
研究グループの人数	１０人～２９人
暗号研究・開発プロジェクトリーダー	Sung-Jun Park 専門：暗号
研究グループ主要メンバー	Seungjoo Kim Byungchun Kim Insoo Lee Maenghee Sung Jeeyeon Kim Sungjae Lee
研究トピック	キーリカバリー 暗号システムのデザインと解析 電子署名
研究グループの特徴	Ph.D.：４人（暗号専攻が２人、数学専攻が２人) Ms.D：７人(暗号専攻が３人、数学専攻が４人)
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	(1) ブラインド署名の開発 (2) 多重電子署名法の開発 (3) 可変長出力ハッシュアルゴリズムの設計 (4) 公開鍵暗号システムの開発 (5)　鍵管理インフラのモデルと技術の開発
プロジェクトの規模	プロジェクトグループ内のみ
プロジェクトリーダー	Sung-Jun Park、KISA
プロジェクト主要メンバー	(1)Seungjoo Kim (シニアメンバー)　　担当： 鍵管理インフラのモデルと技術の開発 (2)Byungchun Kim (シニアメンバー)　担当： 多重電子署名法の開発 (3)Insoo Lee (メンバー)　　担当： 可変長出力ハッシュアルゴリズムの設計 (4)Maenghee Sung (メンバー)　　担当：公開鍵暗号システムの開発 (5)Jeeyeon Kim (メンバー)　　担当： ブラインド署名の開発
プロジェクトグループの人数	５名

研究・プロジェクトの概要	
実施段階	研究段階 実施段階
プロジェクトのスポンサー	MIC (Ministry of Information and Communication)
今後行う予定の研究・プロジェクト	キーリカバリー、対称暗号の設計と解読

2.4.5　韓国(5)　Kyungpook National University

暗号研究機関に関する一般情報	
暗号研究機関名	Kyungpook National University
組織の種類	教育機関（大学）
所在地	Kyungpook National University 1370 Sankyuk-dong, Puk-guTeagu 702-701　KOREA <http://www.kyungpook.ac.kr/>
代表研究者名	Sang-Jae Moon <http://crypto.kyungpook.ac.kr/professor.htm>
代表研究者肩書	Professor
代表研究者専門分野	暗号
組織の概要	Kyungpook National University(KNU) は1951年に設立された。教授数約800人、生徒数約23500人。研究活動に力を入れるため、45の研究施設を持ち、13カ国の41大学/組織と提携している。学部：Colleges of Humanities、Colleges of Social Sciences、 Colleges of Natural Science、Colleges of Economics & Commerce、 Colleges of Law、Colleges of Engineering、Colleges of Agriculture、 Colleges of Music & Visual Arts、Teachers College、School of Medicine、School of Dentistry、Colleges of Veterinary Medicine、 Colleges of Human Ecology 参考URL：<http://www.kyungpook.ac.kr/english/eindex.html>
暗号研究グループに関する情報	
研究機関名	Communication and Information Security Lab School of Electrical & Electronic Engineering

	Kyungpook National University <http://crypto.kyungpook.ac.kr/home.htm>
業種	教育機関
研究グループの人数	
暗号研究・開発プロジェクトリーダー	Sang-Jae Moon 専門：情報セキュリティ
研究グループ主要メンバー	Kuck-Heui Lee
研究トピック	セキュリティメカニズムと暗号
研究グループの特徴	主にコミュニケーションエンジニアリングに基づいた暗号の応用
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	安全な電子支払システム
プロジェクトの規模	国内の他組織「KorEC Inc.社」との共同プロジェクト
プロジェクトリーダー	Sang-Jae Moon, Professor Kyungpook National University
プロジェクト主要メンバー	Hyungso Yoo , Graduate student Kyungpook National Univ
プロジェクトグループの人数	１０人～２９人
研究・プロジェクトの概要	簡単に低予算で実現できる、安全かつ効果的な方法で設計された、SSLベースの安全な電子支払プロトコルを開発中
実施段階	研究段階
プロジェクトのスポンサー	Kyungpook National University、企業
今後行う予定の研究・プロジェクト	次世代モバイルコミュニケーションの安全なシステム

2.4.6　韓国のPKI (Public Key Infrastructure)と電子商取引（EC）の現状および将来の方向性

PKI、CAシステムの現状	１９９９年７月１日に電子署名法が成立し、同年７月７日にRoot CA（KISA）が設立された。CAの運営、電子署名法についての文書化、改訂などはKISAの管轄。現在、認証局候補（３機関）の調査が行われるなど、下部認証局の調整・整備作業が進められている。 CAの組織構成 MIC (Min. of Information and Communication) ｜ KISA（Root　CA） TTA(Telecommunication Technology Association)　*TTAはアルゴリズム標準化の窓口 ｜ ｜―――――｜―――――｜―――――｜ 銀行　証券会社　通信業界　企業 電子署名に使用されるアルゴリズムは法律では決められていないが、国の標準化の１つとしてKCDSA (Korean Certificate-based Digital Signature Algorithm) が提案されている。 参考URL：<http://dosan.skku.ac.kr/~sjkim/Kr-Standard.html>
PKI,CAシステムの将来と傾向	PKI/CAシステムは数年のうちに整備や拡張が急激に進むことが予想される。認証局の数も増えるだろう。
電子商取引の現状	初期段階。電子支払システムを使ったインターネットショッピングモールの開発計画が国内で広がりつつある。金融・証券業界ではほとんどの企業がオンライン決済のための安全なシステムを使用している（安全度の高いSSLなど）。
電子商取引の将来と傾向	今後ますます盛んになることが予想される。より安全な電子商取引や決済法が研究・開発され、法的な整備も政府によって進められるだろう。認証局の数も増える見込み。
PKI/CAに関する法律の現状	電子署名法が１９９９年７月１日に成立した。 KCDSA（Korea Certificate-based Digital Signature Agreement）は韓国内の電子署名標準の１つであるが、アルゴリズムの選択は利用者に任せている。 法律の制定・整備に関連する省庁 電子署名法：Ministry of Information and Communication　（日本の郵政省に相当する）<http://www.mic.go.kr/> 電子商取引法（電子マネー取引法）：Ministry of Commerce, Industry and Energy（日本の通産省に相当する） <http://www.mocie.go.kr/work/index.html>

2.4.7　韓国の暗号学会および論文誌

国内の暗号学会、協会名	KIISC (Korea Institute of Information Security & Cryptology) 会長：　Kil-Hyun Nam
暗号学会誌の発行	Journal of KIISC：季刊誌。2000年より２ヶ月毎に発行予定
国内で開催されている学会	CISC (Conference of Information Security on Cryptology) 主催：KIISC 第９回は1999年11月6日にInformation and Communications Universityで開催された。
	Network Security Workshop 主催：KIISC 第2回は1999年12月9,10日にKorea Universityで開催された。
	Symposium on Information Security 主催：KISA
国際的な学会	JWISC(Korea-Japan Joint Workshop on Information Security and Cryptology) 主催：KIISC、ISEC研究会（電子情報通信学会） 2000年1月25,26日に沖縄で開催 <http://www.ee.kagu.sut.ac.jp/www/staff/hangai/JW-ISC2000/>（英語） <http://kiku.csce.kyushu-u.ac.jp/scis2000/index.ja.html>（日本語）
	ICISC　(International Conference on Information Security & Cryptology) 主催：KIISC

2.5　シンガポールの主要暗号研究機関と研究内容

2.5.1　シンガポール(1)　Gemplus Technologies Asia

暗号研究機関に関する一般情報	
暗号研究機関名	Gemplus Technologies Asia
組織の種類	企業（製造業）
所在地	Gemplus Technologies Asia Pte Ltd 89, Science Park Drive # 04-01/05 - The Rutherford

	Singapore Science Park 118 261 SINGAPORE Tel.: +65 776 19 89 Fax: +65 773 06 48 <http://www.gemplus.com/>
代表研究者名	Yongfei Han
代表研究者肩書	Chief Scientist
代表研究者専門分野	公開鍵暗号、DPA、アルゴリズム
組織の概要	１９８８年創立。スマートカードの製造・販売を行う。２７カ国に10工場、5研究開発所、41セールスオフィスを持つ。従業員数４３００人以上 参考URL：<http://www.gemplus.com/>
暗号研究グループに関する情報	
研究機関名	Gemplus
業種	企業
研究グループの人数	１０人～２９人
暗号研究・開発プロジェクトリーダー、研究グループ主要メンバー、研究トピックについては回答なし	
研究グループの特徴	Gemplus の研究チームは、スマートカードの設計、製造、応用すべての過程に関連する研究を行っている。 -製造工程システム -特殊印刷技術 -チップデザイン -暗号 -システムモデリング -チップオペレーションシステム -カードアプリケーションソフトウェア -外部ソフトウェアシステム
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック以下、回答なし	

2.5.2　シンガポール(2) National University of Singapore (Professor Kwok-Yan Lam)

暗号研究機関に関する一般情報	
暗号研究機関名	School of Computing National University of Singapore

組織の種類	教育機関
所在地	Department of Computer Science National University of Singapore Blk S16, Level 5, Science Drive 2 Singapore 117599 <http://www.nus.edu.sg/>
代表研究者名	Kwok-Yan Lam <http://www.comp.nus.edu.sg/~lamky/>
代表研究者肩書	Professor（National University of Singapore） Visiting Professor（Hong Kong University of Science and Technology）
代表研究者専門分野	システムセキュリティ、侵入検出、高速暗号アルゴリズム、認証プロトコル、コンテキスト依存型アクセスコントロール、Distributed Computing
組織の概要	National University of Singaporeは１９９８年７月１日にSchool of Computingを設立。主な学科は３つ： (1)Computer Engineering (joint with the Faculty of Engineering) (2)Computational Finance (joint with the Faculty of Science) (3)Information and Communication Management (joint with the Faculty of Arts and Social Sciences) また、大学院課程にはMaster of Computing, Master of Science, and Doctor of Philosophyがある。 リサーチセンターはCentre for Internet Research、Centre for Information Mining and Extraction, Centre for Systems Security, the Centre for TeleMedia Strategyなどがある。 そのうち、Center for System SecurityはProfessor Lamによって１９９７年に設立された。 参考URL：<http://www.nus.edu.sg/> 規模：１０００人以上
暗号研究グループに関する情報	
研究機関名	National University of Singapore School of Computing
業種	大学機関 教育機関 研究機関
研究グループの人数	１０人～２９人
暗号研究・開発プロジェクトリーダー	Professor Kwok-Yan Lam 専門：セキュリティ、暗号

研究グループ主要メンバー	Kwok-Yan Lam Chaoping Xing
研究トピック	(1)スマートカード (2)モバイルプロトコルセキュリティ (3)楕円曲線 (4)ビット系列
研究グループの特徴	メンバーの専門分野が幅広い（数学、コンピュータサイエンスなど）。研究タイプは３つに分かれており、それぞれ理論的な研究、実用的研究、産業界との共同研究を専門に行う。 Prof. Lamは、シンガポールの各産業間のオープンシステムトランザクションを安全に行うためのセキュリティインフラストラクチャを開発するプロジェクト「Singapore Enterprise Security Architecture Project」のリーダーを務めた。
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	モバイル電子商取引、スマートカードの暗号、ビット系列
プロジェクトの規模	研究のタイプによって規模も異なる。 (1)理論的な研究は大学の研究グループ内 (2)応用は産業界（銀行、通信業界など）との共同研究 (3)国際プロジェクトはは現在、香港と韓国との間で進行中。 香港：モバイル電子商取引プロジェクト。 韓国：シンガポールと韓国の両政府レベルとNational University of Singaporeの３者間で、Smart Card に関するプロジェクトディスカッションを開始した。
プロジェクトリーダー	Kwok-Yan Lam
プロジェクト主要メンバー	Huan-Hui Zhao, リサーチフェロー National University of Singapore (モバイル電子商取引プロジェクト)
プロジェクトグループの人数	
研究・プロジェクトの概要	ワイヤレスプラットフォームでの電子商取引トランザクション
実施段階	研究段階 実験段階
プロジェクトのスポンサー	政府、銀行
今後行う予定の研究・プロジェクト	未定

2.5.3　シンガポール(3) National University of Singapore (Professor Cunsheng Ding)

暗号研究機関に関する一般情報	
暗号研究機関名	Department of Computer Science National University of Singapore
組織の種類	大学
所在地	Department of Computer Science National University of Singapore Blk S16, Level 5, Science Drive 2 Singapore 117599 <http://www.nus.edu.sg/>
代表研究者名	Cunsheng Ding < http://www.comp.nus.edu.sg/~dingcs/>
代表研究者肩書	Assistant Professor
代表研究者専門分野	暗号、情報とシステムセキュリティ、コーディング理論
組織の概要	シンガポール(2) National University of Singapore (Professor Kwok-Yan Lam)の「組織の概要」を参照
暗号研究グループに関する情報	
研究機関名	Department of Computer Science National University of Singapore
業種	大学機関 教育機関
研究グループの人数	１０人以下
暗号研究・開発プロジェクトリーダー	Cunsheng Ding 専門：暗号
研究グループ主要メンバー	Cunsheng Ding San Ling Chaoping Xing
研究トピック	数論、有限体、組合せ論、代数幾何学および代数関数体へのストリーム暗号、秘密分散、認証符号、完全ハッシュ族や楕円関数公開鍵暗号への応用
研究グループの特徴	グループメンバーは、深く幅広い数学知識を応用し、暗号システム設計と解析のために確立された様々な数学的方法を用いる。メンバーの何人かは１９

	８５年頃から既に暗号の研究に携わっており、アジア地域の暗号研究の先駆者である。
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	暗号の数学的構造
プロジェクトの規模	大学内の他のリサーチグループ「Applied Math Group」との共同研究
プロジェクトリーダー	Cunsheng Ding, Assistant Professor National University of Singapore
プロジェクト主要メンバー	San Ling, Associate Professor, National University of Singapore Chaoping Xing, Associate Professor, National University of Singapore
プロジェクトグループの人数	
研究・プロジェクトの概要	このプロジェクトは強力な数学的手法を用いて暗号システムの開発と解読を行うことを目的とする。研究トピックは、ストリーム暗号、秘密分散、楕円曲線公開鍵暗号、認証コード、完全ハッシュ族など。数学的手法には、数論、代数関数体、代数幾何学、組合せ論を含む。
実施段階	研究段階
プロジェクトのスポンサー	National University of Singapore National Science and Technology Board of Singapore
今後行う予定の研究・プロジェクト	暗号とコード理論間の暗号プロトコルと相互作用

2.5.4　シンガポールのPKI (Public Key Infrastructure)と電子商取引（EC）の現状および将来の方向性

PKI、CAシステムの現状	現在ある認証機関は「Netrust Pte.Ltd. <http://www.netrust.com.sg/>」。Netrustは　Singapore National Computer Board (NCB) <http://www.ncb.gov.sg/>　と Network for Electronic Transfers (Singapore) Pte Ltd (NETS) <http://www.nets.com.sg/>とのジョイントベンチャー企業。 最近「ID. Safe Pte Ltd.」が新たに加わった。最上位レベルのCAは今のところ民間企業。政府は法整備を行い、PKIとCAシステムの確立・普及を目指している。
PKI,CAシステムの将来と傾向	より多くの民間の認証機関がCAオペレーターとして認可されるようになり、CAシステムの整備が進むだろう。そして、PKIとCAに伴う法的問題につい

	て、より多くの研究が行われる予定。
電子商取引の現状	シンガポールは１９９６年から電子商取引を開始した。Prof. Lamをリーダーとする National University of Singapore　のプロジェクトチームがセキュリティインフラを構築した。スポンサーは、政府機関、６銀行、テレコム、ケーブルTV、DDIオペレーター、ISPなど併せて１３社。プロジェクト開始から実用化まで１年をかけた。 現在も多くのプロジェクトや実験が進行中で、実用化されているものも多い。オンラインショッピングモールは既に多数存在する。各種チケットの売買やスーパーでの買い物はオンラインでも一般的に行われている。 確定申告のオンライン版も１９９８年４月から開始された。二回目の１９９９年４月にはおよそ２７万件のファイルが電子フォームを利用したと新聞で報道された。確定申告のセキュリティシステムは Prof. Lam の設計による。 また、政府は電子商取引のプロモーションのためにセミナーや講演会を多数開催している。政府は、シンガポールがアジアの経済センターとなるために電子商取引を成功させることが必要不可欠であると考え、積極的に政策を推進している。一部の銀行ではオンラインサービスが開始されている。
電子商取引の将来と傾向	引き続き、政府によるEC促進計画が盛んに実施されるだろう。
PKI/CAに関する法律の現状	Electronic Transactions Act　が１９９８年６月に国会を通過し、同年７月１０日に施行された。 参考URL<http://www.cca.gov.sg/index.html>

2.5.5　　シンガポールの暗号学会および論文誌

国内の暗号学会、協会名	暗号の学会はないが、暗号の研究・開発が国内でもっとも活発に行われているのはNational University of Singapore。
暗号学会誌の発行	なし
国内で開催されている学会	Cryptography and Computational Number Theory Workshop(1999年11月22日) 主催：National University of Singapore
	Sequence conference　（1998） 主催：National University of Singapore
	System Security Curriculum （National University of Singaporeが産業界のために毎年開催するセキュリティワークショップ） 主催：National University of Singapore

国際的な学会	ACM Conference on Communications and Computer Security 99 1999年11月1日～4日 <http://www.isi.edu/ccs99/> スポンサー：ACM SIGSAC
	Asiacrypt99 1999年11月14日～18日 <http://www.comp.nus.edu.sg/~asia99/> 主催：ASC（Asiacrypt Steering Committee） 予稿集：Advances in Cryptology - ASIACRYPT '99, LNCS no.1716, Springer-Verlag (1999)
	SETA' 98　（INTERNATIONAL CONFERENCE ON SEQUENCES AND THEIR APPLICATIONS） 1998年12月14日～17日 <http://www.comp.nus.edu.sg/%7Edingcs/seta98.html> 主催：National University of Singapore
	JWIS' 98 <http://www.comp.nus.edu.sg/~jwis98/paper.htm> 1998年12月10日～12日 共催：Centre For Systems Security, The National University of Singapore、 ISEC (Information Security Technical) Group of IEICE of Japan

---

2.6　台湾の主要暗号研究機関と研究内容

2.6.1　台湾(1)　Chinese Cryptology and Information Security Association

暗号研究機関に関する一般情報	
暗号研究機関名	Chinese Cryptology and Information Security Association (CCISA)
組織の種類	研究機関 非営利団体
所在地	事務局はCCISA理事長の所属する組織に置かれる。1997年～2000年までは、会長であるProfessor Chi Sung Laih が所属する　National Cheng Kung Universityに置かれる。 <http://crypto.ee.ncku.edu.tw/~ccisa> Professor Chi-Sung Laih Cryptology & Network Security Lab

	Dept. of Electrical Engineering National Cheng Kung University #1University Road. Tainan, Taiwan, ROC Tel: 886-6-2757575
代表研究者名	Chi-Sung Laih <http://crypto.ee.ncku.edu.tw/laih_eng.html> Cryptology & Network Security Lab <http://crypto.ee.ncku.edu.tw/eng.html>
代表研究者肩書	(1)Professor, Department of Electrical Engineering of National Cheng Kung University (2)Chairman, Computer Center of National Cheng Kung University (3)Chairman, Chinese Cryptology and Information Security Association
代表研究者専門分野	情報セキュリティ、誤り制御符号、コミュニケーションシステム
組織の概要	台湾国内の暗号の教育・研究・開発の促進および情報セキュリティの啓蒙活動を目的に、１９９４年に設立された。国のセキュリティ基準の策定に協力し、国際学会に積極的に参加し活動する。規模：個人会員250人以上、法人会員３２団体。参考URL<http://crypto.ee.ncku.edu.tw/~ccisa>
暗号研究グループに関する情報	
研究機関名	Chinese Cryptology and Information Security Association (CCISA)
業種	研究機関
研究グループの人数	２８０人
暗号研究・開発プロジェクトリーダー	Professor Chi Sung Laih 専門：暗号
研究グループ主要メンバー	
研究トピック	
研究グループの特徴	
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	FIPS 140-1の調査
プロジェクトの規模	FIPS140-1の調査については５つのサブプロジェクトがあり、４つの大学に分けて行われている（National Cheng Kung University、TungHai

	University、National Chiao-Tung University、National Taiwan University of Science Technology)。
プロジェクトリーダー	Chi-Sung Laih
プロジェクト主要メンバー	４大学の教授５名 各大学につき教授１名が責任者。National Chiao-Tung University のみ２名（Prof. Shiuh Pyng Shieh　と Prof. Jing-Jang Hwang）
プロジェクトグループの人数	１９人（National Cheng Kung University内のプロジェクトチームの人数。教授と生徒を併せた数）
研究・プロジェクトの概要	FIPS 140-1（U.S.Federal Information Processing Standard) の調査。 FIPS140-1とは、暗号モジュール用セキュリティ要件を規定するもので、NIST（米国標準技術研究所）が1995年に策定した。改訂版140-2がもうすぐ発行される予定。 FIPS 140-1<http://csrc.nist.gov/cryptval/140-1/1401val.htm> 暗号アルゴリズムDESの暗号の質、中身を査定するという意味で、政府が深い興味を示している(暗号を悪用されないため)。台湾にならってシンガポールもFIPSの調査を行う予定。プロジェクトの期間は１９９８年９月から２年間。このプロジェクト開始にあたり、９カ国のセキュリティポリシーについて調査した。
実施段階	研究段階
プロジェクトのスポンサー	政府。CCISAが研究母体。
今後行う予定の研究・プロジェクト	

2.6.2　台湾(2)　Chunghwa Telecom Co., Ltd.

暗号研究機関に関する一般情報	
暗号研究機関名	Chunghwa Telecom Co., Ltd.（中華電信）
組織の種類	通信業
所在地	12, Lane 551 LineMin-Tsu Road Sec. 5 Yang-Mei Taoyuan 326R.O.C <http://www.chttl.com.tw/>
代表研究者名	Kuang-Yao Chang
代表研究者肩書	Managing Director
代表研究者専門分野	情報セキュリティ、暗号

組織の概要	http://www.cht.com.tw/english/index.htm 規模：従業員約１０００名以上
暗号研究グループに関する情報	
研究機関名	Telecommunication Laboratories Applied Research Lab Chunghwa Telecom Co., Ltd.
業種	研究機関
研究グループの人数	ラボ内には約３０人の研究メンバーが所属している。
暗号研究・開発プロジェクトリーダー	Ph. D. Kuang-Yao Chang 専門：コンピュータサイエンス、情報技術
研究グループ主要メンバー	Ph. D. Gan-How Chang Ph. D. Dung-Ming Shieh Ph. D. Ren-Han Tsou Ph. D. Tsann-Shyong Liu
研究トピック	情報セキュリティに関する研究
研究グループの特徴	グループの研究内容は主に４つに分類される 1. CA構成要素の開発 2. PKIの構築 3. 暗号の研究 4. 検査技術の改良
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	現在は政府PKIの構築プロジェクトに携わっている。このプロジェクトは「National Information Infrastructure Plan」のサブプロジェクト。
プロジェクトの規模	他の５つ以上の組織（Chunghwa Telecom, Ministry of Transportation and Communicationその他）との共同研究
プロジェクトリーダー	Ms Cher-Jean Lee Section Chief of Research Development and Evaluation Commission The Executive Yuan
プロジェクト主要メンバー	(1)Mr. Chouan-Te Ho (Computer Analyst of Development and Evaluation Commission) (2)Ph. D. Lang-Chee Chang (Vice President of Data Communication Business Group of Chunghwa Telecom) (3)Ph. D. Bor-Shenn Jeng (Vice President of Chunghwa Telecom Laboratories) (4)Ph. D. Kuang-Yao Chang (Managing Director of Applied Research Lab of Chunghwa Telecom Laboratories)

プロジェクトグループの人数	３０人～５０人
研究・プロジェクトの概要	「National Information Infrastructure Plan」のサブプロジェクトとして、政府PKIの構築を行っている。
実施段階	実用段階 Chunghwa Telecom が開発した政府のPKI・CAシステムは、確定申告システムや、自動車・バイクの運転免許証システム、国家プロジェクト入札システムその他に応用されている。
プロジェクトのスポンサー	Research, Development and Evaluation Commission The Executive Yuan
今後行う予定の研究・プロジェクト	1. 現行のシステムをDESからAESに変更する 2. 他のCAとの相互認証を可能にする

2.6.3　台湾(3)　National Cheng Kung University

暗号研究機関に関する一般情報	
暗号研究機関名	National Cheng Kung University　（国立成功大学）
組織の種類	教育機関
所在地	National Cheng Kung University #1, University Road. Tainan Taiwan ROC <http://www.ncku.edu.tw/>
代表研究者名	Tzonelih Hwang
代表研究者肩書	Professor
代表研究者専門分野	CA-PKIの開発、ネットワークセキュリティ、インターネットセキュリティ開発ツール、鍵管理
組織の概要	College of Liberal Arts、College of Sciences、College of Engineering、College of Management Science、College of Medicine、College of Social Sciencesの６つのコースを提供している。 参考URL<http://www.ncku.edu.tw/english/>
暗号研究グループに関する情報	
研究機関名	Information Security Lab Computer Science &　Information Engineer National Cheng Kung University

業種	教育機関 研究機関 非営利団体
研究グループの人数	１０人～２９人
暗号研究・開発プロジェクトリーダー	Tzonelih Hwang 専門： CA-PKIの開発、ネットワークセキュリティ、インターネットセキュリティ開発ツール、鍵管理
研究グループ主要メンバー	Tzonelih Hwang
研究トピック	CA-PKI、鍵管理
研究グループの特徴	
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	
プロジェクトの規模	
プロジェクトリーダー	Tzonelih Hwang
プロジェクト主要メンバー	
プロジェクトグループの人数	
研究・プロジェクトの概要	
実施段階	研究段階 実験段階
プロジェクトのスポンサー	National Science Council,　Republic of China <http://www.nsc.gov.tw/english/index.html>
今後行う予定の研究・プロジェクト	

2.6.4　台湾(4)　National Chung Cheng University

暗号研究機関に関する一般情報	
暗号研究機関名	Institute of Computer Science and Information Engineering, National Chung Cheng University
組織の種類	教育機関
所在地	Institute of Computer Science and Information Engineering National Chung Cheng University Chiayi, Taiwan 62107, R.O.C. <http://www.ccu.edu.tw/ccu/introduction/english/index.html>
代表研究者名	Chin-Chen Chang
代表研究者肩書	Professor
代表研究者専門分野	暗号、情報セキュリティ、画像処理、データ技術、データベース設計
組織の概要	規模：１０００人以上 １９８９年７月１日に設立された。 参考URL： <http://www.ccu.edu.tw/ccu/introduction/english/page.01.html>
暗号研究グループに関する情報	
研究機関名	National Chung Cheng University
業種	教育機関
研究グループの人数	１０人～２９人
暗号研究・開発プロジェクトリーダー	Profesor Chin-Chen Chang 専門：暗号、情報セキュリティ、画像処理、データ技術、データベース設計
研究グループ主要メンバー	(1) Tung-Shou Chen,　Professor (2) Wei-Bin Lee,　Associate Professor (3) J. H. Jiang (Ph.D. Candidates) (4) Y.C. Hu (Ph.D. Candidates) (5) C.T. Wang (Ph.D. Candidates) (6) Y.K. Chan (Ph.D. Candidates)
研究トピック	画像処理、情報セキュリティ、データ技術
研究グループの特徴	メンバーの専門性が多様
現在行っている研究プロジェクトに関する情報	
現在行っているプロジェクトの名前またはトピック	ルーカス関数計算のスピードアップ法と楕円曲線暗号システム

プロジェクトの規模	プロジェクトグループ内のみ
プロジェクトリーダー	Chin-Chen Chang
プロジェクト主要メンバー	Professor Tung-shou Chen (Providence University) Associate Professor Wei-Bin Lee (Feng Chia University)
プロジェクトグループの人数	
研究・プロジェクトの概要	電子商取引暗号システム計算のスピードアップ法
実施段階	研究段階
プロジェクトのスポンサー	National Science Council, Republic of China <http://www.nsc.gov.tw/english/index.html>
今後行う予定の研究・プロジェクト	データ・ハイディング、電子透かし

2.6.5　台湾のPKI (Public Key Infrastructure)と電子商取引（EC）の現状および将来の方向性

PKI、CAシステムの現状	現在台湾には４種類のCAがある。 (1)「GCA」(Government Certification Authority)：政府レベルのCA。Government Service Network に所属する機関の認証や、確定申告など政府関連の諸手続に使われる。第一回目のオンライン確定申告は１９９８年２月に実施された。申告書約５万件が配布され、実際に使用された申告書は約２万件だった。 (2)FISC (Financial Information Service Center)：金融情報サービスセンター。SET（Secure Electronic Transaction protocol、安全な電子商取引プロトコル）を利用するシステムと、NON-SET（SETを利用しないもの）の２種類がある。NON-SETには「NBCA」（Network Banking Certification Authority）があり、オンラインバンキングに利用される。 (3)民間企業のジョイントベンチャーで設立されたCA。VeriSignやHiTrust社<http://www.hitrust.com.tw/>などが含まれる。 (4)TAS (Taiwan Authentication Service)：安全なオンライン証券取引サービスの提供を目的とする。Ministry of Finance<http://www.mof.gov.tw/eindex1.html> が多額の出資や積極的な促進活動を行っており、国内には約２００以上の証券会社や約６百万人も

	の顧客がいることから、将来的には台湾で最大規模のCAになると予想される。現在はまだシステム構築中の段階だが、2000年前半までには運営が開始される予定。 (1),(2),(3)はいずれも１９９８年頃から運営を開始している。現時点では、それぞれの目的別のCAが設立され充分な機能を果たしているので、相互認証の必要性もそれほど高くはないが、将来的には必要になるだろう。
PKI,CAシステムの将来と傾向	GCAと民間の認証機関の整備が進み、国家全体のCAインフラが確立されるだろう。また、相互認証を行ったり、CAの階層を増やしたりすることで、提供できるサービスの範囲が広がる見込み。確定申告のオンライン化については、若い世代の人々は好んで新しい様式を使う傾向にあるが、年長者にはまだまだ普及率が低い。電子署名法が成立し、政府がもっと促進活動を行えば今後いっそう普及すると思われる。
電子商取引の現状	Ministry of Economic Affairs (MOEA) <http://www.moea.gov.tw/~meco/Intro_e/xmoe0.htm> の Department of Commerce　の出資による「Commerce Automation Project」が１０年計画（1992-2001）で進行中。オンラインショッピングサービスに関する消費者のニーズに答えるため、インターネットベースの Quick Response System (QRS) と Efficient Consumer Response System (ECR) を開発する目的で、商業地区１０カ所を選んだ。 プロジェクトは下記のサブプロジェクトを含む。 1. EDI Electronic Business （企業間情報交換） 2. 企業間 (B to B) クイックレスポンス 3. 企業・消費者間 (B to C) クイックレスポンス 4. 電子商取引のプロモーション 電子入札、オンラインショッピングモール、オンライン株式市場など、実際に実験段階に入っているものが多い。Chunghwa Telecomは政府の電子入札システムや、Kaohsiung(高雄)の電子港(Electronic Port)計画などのプロジェクトを持っている。参考URL：高雄港<http://www.khb.gov.tw/> 高雄港情報システム <http://www.khb.gov.tw/english/e0110.htm#E011007>
電子商取引の将来と傾向	政府は現在、銀行に関連する２２の法律の改定を行っている。電子バンキングの運営法や、他の金融・証券機関のオンライン化などに関する法律の策定・改訂作業も近々完了する予定。その後、企業や一般の人々の間で電子バンキングが普及するだろう。Ministry of Finance (MOF)のThe Monetary Information Center は、インターネットベースの取引・トランザクションを一般の市民のレベルで普及させる促進計画を立てている。
PKI/CAに関する法律の現状	電子署名法は国会に提出済み（１９９９年５月頃）で、現在審議中。1～2年のうちに成立する見込み。

2.6.6　台湾の暗号会および論文誌

国内の暗号学会、協会名	Chinese Cryptology and Information Security Association (CCISA)
	Institute of Information Science, Academia Sinica <http://www.iis.sinica.edu.tw/>
暗号学会誌の発行	Information Security Newsletter (発行：CCISA) 現在は年４回の発行だが、将来的には月刊にしたい。
	Journal of Information Science and Engineering　(発行：Institute of Information Science, Academia Sinica) 隔月刊行。<http://www.iis.sinica.edu.tw/JISE/>
国内で開催されている学会	Information Security Conference 主催：CCISA
	National Computer Symposium 主催：CCISA
国際的な学会	International Computer Symposium 主催：CCISA（２０００年）
	Asiacrypt (２００３年) 主催：International Association for Cryptologic Research (IACR) オーガナイザー：CCISA（予定）

4.　資料編

4.1　　調査依頼書

Japan Computer Security Research center
1-1 Midorigaoka-cho, Shizuoka-shi,
Shizuoka-ken, 422-8052 Japan
TEL: +81-54-283-5327 FAX: +81-54-283-5328

November 5, 1999

To whom it may concern:

My name is Seiji Murakami, president of Japan Computer Security Research center. We

are conducting a survey on the status of theoretical and practical research and development on cryptography in Asia for IPA (Information-technology Promotion Agency of Japan), with help and support of Professor Eiji Okamoto (University of Wisconsin-Milwaukee), Professor Hideki Imai (University of Tokyo), Professor Tsutomu Matsumoto (Yokohama National University), Doctor Mitsuru Matsui (Mitsubishi Electric Company), and Doctor Tatsuaki Okamoto (Nippon Telegraph and Telephone Corporation).

The objective of this survey is to find out the current trend of research on cryptography in Asia, and to understand the level of its experimentation and implementation in each region.

Recently, Asia has been very active in the area of research on cryptography. For example, "Asiacrypt" is given high profile and became internationally well- known conference; it will be sponsored by International Association for Cryptology Research (IACR) from the year 2000. This means Asiacrypt is considered as same level as Crypto and Eurocrypt.

The other fact is that Public Key Infrastructure (PKI) and Certificate Authorities (CA) have already been established and are used in electronic commerce systems such as Electric Toll System (ETC) or tax refund.

Considering these facts, we believe that now is good time to conduct survey to find out the status of research and development of cryptography to promote further development and activity in Asia. The result of this survey will be posted to IPA website <http://www.ipa.go.jp/>. We hope this will be useful information among people including us engaged in cryptography.

The scope of the survey includes:
- Organizations in Asian regions listed below.
- PUBLIC INFORMATION ONLY (that means information you can share with others. Please DO NOT write confidential information.)

We would highly appreciate if you could take your time filling out the attached questionnaires and return to us at your earliest convenience.

Thank you very much in advance for your cooperation.

Yours sincerely,
Seiji Murakami
President

4.2　調査票　（原文）

Questionnaire for Research and Development of
Cryptography in Asia

Respondents to this survey (in alphabetical order)

CHINA
HONG KONG
INDIA
KOREA
SINGAPORE
TAIWAN

Due Date

November 30, 1999

Return Address
---

*Please send your reply by e-mail, airmail or fax to:
Harumi Sugimura (Ms)
Administrative Assistant
Japan Computer Security Research Center
1-1 Midorigaoka-cho, Shizuoka-shi
Shizuoka-ken 422-8052 Japan
Email: haru@jcsa.or.jp
Tel: +81-54-283-5327
Fax: +81-54-283-5328

General Questions

Your Name:
Affiliation:
Position/Title:
Address:

E-mail Address:
Phone Number:
Fax Number:
URL:

Your organization's primary line of business:
(please put X inside [ ] where applicable)
For example:
[X] Research Institute

[ ]Communication
[ ]Education
[ ]Research Institute
[ ]Engineering
[ ]Medical
[ ]Government/Agency
[ ]Legal
[ ]Manufacturing
[ ]Non-profit
[ ]Transportation
[ ]Others (please specify industry)

Your Job description:
Your Research Area:

Questionnaires on Cryptography

Please fill out the following question about your organization as well as other organizations in your country/region ONLY IF you have such information AND such information is opened to public.)

NOTE:
1. Do not write confidential information.
2. If your answer is for two or more organizations, please cut and paste the following questions, and attach them at the end of this questionnaire.
3. Please contact Ms. Harumi Sugimura at haru@jcsa.or.jp if you have any questions.

********** Questionnaire begins **********

Q1 - Q9
General questions on your organization and/or

research groups in your country/region.

Q1: Name of Organization:

Q2: Type of Organization:
(please put X inside [ ] where applicable.)
[ ]University
[ ]Company
[ ]Research
[ ]Others (please specify)

Q3: How many people are there in the organization?
(please put exact number if you know, otherwise, put X beside the number.)
Exact number:
[ ]Less than 50 [ ]50 to 99 [ ]100 to 299
[ ]300 to 499 [ ]500 to 999 [ ]More than 1000

Q4: What is the organization's primary line of business?
(please put X inside [ ] where applicable.)
[ ]Education
[ ]Research
[ ]Government/Agency
[ ]Manufacturing
[ ]Non-profit
[ ]Others (please specify)

Q5: What is the name of the project leader on research/development of cryptography?

Q5-1: What is his/her major field of study?

Q6: Who is (are) the main member(s) of the group?
(please list the member(s) in full name)

Q7: How many members are there in the group?
(please put exact number if you know, otherwise, put X beside the number.)
Exact number:
[ ]Less than 10 [ ]10 to 29 [ ]30 to 50
[ ]More than 50:

Q8: What is the main topic or theme of the group?

Q9: What are the characteristics of the group?

(unique research methods, diversity in expertise of group members etc.)

Q10 - Q17
Questions on current project(s) of your organization and/or
research groups in your country/region.

Q10: What is the name of current project?

Q11: What is the size of the project?
(please put X or number inside [ ] where applicable.)
[ ]A. Only within one project group
[ ]B. Joint research project
[ ]B1: within its organization:
with how many groups? [ ]
with which groups? [ ]
[ ]B2: Inter-organization:
with how many organizations?[ ]
with which organizations? [ ]
[ ]B3: International:
with which countries/regions?[ ]

Q12: What is the name, title and affiliation of the project leader?

Q13: What is (are) the name, title and affiliation of the main member(s)?

Q14: Please describe briefly about the project.

Q15: What is the current stage of the project?
(please put X inside [ ] where applicable.)
[ ]Research
[ ]Field Experiment
[ ]Actual Use: if this applies, please describe in what area and how it is used.

16: Who is (are) the sponsor(s)of the project?

Q17: What will be the next (future) theme of research or project on cryptography?

Q18 - Q21
General questions on PKI/CA and Electronic Commerce
in your country/region

Q18: What is the present status of Public Key Infrastructure (PKI) and Certificate Authority system in your country/region? Please give examples of how it is introduced and used.

Q18-1: What is the future plan and tendency of PKI/CA?

Q19: What is the present status of Electronic Commerce (EC) in your country/region? Please give examples of how it is introduced and used.

Q19-1: What is the future plan and tendency of EC?

Q20: What is the present status of law concerning PKI/CA?

Q20-1: What is the status of law on electronic signature?
(please put X inside [ ] where applicable)
[ ]A. Bill was enacted as of [/ /](please put year/month/date)
[ ]B. Bill is under deliberation:
it will be enacted on [/ /](please put year/month/date)
[ ]C. Bill will be submitted in the future:
[ ]D. Others:

Q21: What kind of Society/Association of Cryptography do you have in your country? (Please list the name of organization.)

Q21-1:What journals do they publish? How often?

Q21-2:What kind of conference or symposium on cryptography is held in your region/country?

Q21-3:Please enter the name of the host(s) of the conferences stated in Q21-2.
A. Domestic conference:
B. International conference:

Thank you very much for taking time to fill out this questionnaire.

********** End of the questionnaire **********

4.3　調査票　（日本語訳）

回答者属性

氏名
所属組織
肩書
所在地
Emailアドレス
電話番号
FAX番号
URL
主たる業種
職務
専門分野

所属地域における暗号研究組織に関する質問

組織名
組織の種類
組織の人数
主たる業種
暗号研究・開発のプロジェクトリーダー
プロジェクトリーダーの専門分野
プロジェクトチームの主要メンバー
プロジェクトチームの人数
プロジェクトチームの研究テーマ
プロジェクトチームの特徴

所属組織で現在行っている研究プロジェクトに関する質問

プロジェクト名
プロジェクトの規模
プロジェクトリーダーの氏名、肩書、所属組織名
プロジェクト主要メンバーの氏名、肩書、所属組織名
プロジェクトの概要
プロジェクトの実施段階
プロジェクトのスポンサー
次のプロジェクトテーマ

PKI（Public Key Infrastructure：公開鍵方式）, CA(Certificate Authority：認証局), そしてElectronic Commerce：電子商取引）に関する質問

PKIとCAシステムの現状
PKIとCAシステムの将来と傾向
電子商取引の現状
電子商取引の将来と傾向
PKIとCAに関する法整備律の現状
電子署名法の現状
暗号に関する学会や団体
学会が発行する論文誌や定期刊行物とその発行期間
地域で開催される暗号学会
学会の主催者