社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30 (67)
2005／7／22

第4回PKI R&D ワークショップ参加報告

今本 健二† 櫻井 幸一††

† 九州大学システム情報科学府 〒812-8581 福岡県福岡市東区箱崎 6-10-1
†† 九州大学システム情報科学研究院 〒812-8581 福岡県福岡市東区箱崎 6-10-1
E-mail: †imamoto@itslab.csce.kyushu-u.ac.jp, ††sakurai@csce.kyushu-u.ac.jp

あらまし 2005年4月19日-4月21日に，アメリカのNISTで開催された第4回PKI R&D ワークショップの開催概要について報告する（http://middleware.internet2.edu/pki05/）．また，2005年4月18日にNISTで開催されたIEEE 1363 Study Group Meeting on Pairing based Cryptography and Identity based Encryptionについて報告する．
キーワード 公開鍵認証基盤，相互運用性，標準化活動

A Report on the 4th Annual PKI R&D Workshop

Kenji IMAMOTO† and Kouichi SAKURAI††

† Graduate School of Information Science and Electrical Engineering, Kyushu University Hakozaki 6-10-1, Higashi-ku, Fukuoka 812-8581, Japan
†† Faculty of Information Science and Electrical Engineering, Kyushu University Hakozaki 6-10-1, Higashi-ku, Fukuoka 812-8581, Japan
E-mail: †imamoto@itslab.csce.kyushu-u.ac.jp, ††sakurai@csce.kyushu-u.ac.jp

Abstract This paper reports the 4th Annual PKI Research Workshop held on Aplil 19-21st, 2005 (http://middleware.internet2.edu/pki05/), and IEEE 1363 Study Group Meeting on Pairing based Cryptography and Identity based Encryption held on Aplil 18th, 2005 in NIST.
Key words Public key infrastructure (PKI), Interoperability, Standards activation

1. はじめに

本稿では，今年4月19日から21日にアメリカ合衆国のNIST(National Institute of Standards and Technology)で開催された第4回PKI R&D ワークショップ（4th Annual PKI R&D Workshop）について，その概要を報告する．本ワークショップは，2002年に第1回ワークショップ[1]が開催されて以来，公開鍵認証基盤(Public Key Infrastructure, PKI)に関する研究ワークショップとして毎年NISTにて開催されている．各会議の詳細については，会議ホームページにて論文および発表資料が掲載されている[1]～[4]．第2回PKI研究ワークショップ，第3回PKI R&D ワークショップの概要については，それぞれ文献[5],[6]を参照のこと．

今年のワークショップへの参加者は121名であり，アメリカ以外の各国の参加人数は，ブラジル(3)，カナダ(2)，オランダ(2)，オーストラリア(2)，ノルウェイ(2)，アイルランド(1)，イングランド(1)，韓国(1)であり，日本からは著者の1人である今本が参加した．第2回，第3回ワークショップの参加者総数はそれぞれ120名程度，100名程度であるので，今年のワークショップはそれらとほぼ同様の規模となった．アメリカ以外の参加者数に関しては，第2回では11人，第3回では7人となっており，参加国数，参加者数に関しては過去のワークショップよりも増加が見られた．

参加者のうち，大学関係者は35名ほどであり，政府関係者は20名ほど，その他はセキュリティ企業からの参加者が占めた．今回のワークショップでは17件の論文発表に加え，招待講演，パネル講演が行われた．内容としては，PKIの相互運用性やPKIによるサービス，政府によるPKI，ユーザビリティ，標準化動向など，特に実用的な話題を中心とした幅広い分野に関する議論が行われた．また，本会議への全投稿数は33編であり，採択率は51.5%となっている．

さらに，本ワークショップ開催前日の4月18日にNIST Northにて開催されたIEEE 1363 Study Group Meeting on Pairing based Cryptography and Identity based Encryptionへも参加したので，その参加報告を行う．

本論文では，2章で第4回PKI R&D ワークショップのプログラム委員を紹介し，3章で本ワークショップのプログラムを紹介する．4章では第4回PKI R&D ワークショップで発表された

論文，パネル講演，招待講演の概要を報告する．5章ではIEEE 1363 Study Group Meeting on Pairing based Cryptography and Identity based Encryptionにて発表された講演概要を報告する．6章で本論文のまとめを示す．

2. プログラム委員

General chair: Ken Klingenstein (Internet2)
Program chair: Clifford Neuman (University of Southern)
Steering committee chair: Neal McBurnett (Internet2)
Local arrangements chair: Nelson Hastings (NIST)

Program Comittee
Clifford Neuman, USC-ISI (Chair)
Peter Alterman, National Institutes of Health
Bill Burr, NIST
Yassir Elley, Sun Microsystems
Carl Ellison, Microsoft
Stephen Farrell, Trinity College Dublin
Richard Guida, Johnson & Johnson
Steve Hanna, Funk Software
Peter Honeyman, University of Michigan
Russ Housley, Vigil Security LLC
Ken Klingenstein, Internet2
Olga Kornievskaia, University of Michigan
Neal McBurnett, Internet2
John Mitchell, Stanford University
Eric Norman, University of Wisconsin
Tim Polk, NIST
Ravi Sandhu, GMU; NSD Security
Krishna Sankar, Cisco Systems
Jeff Schiller, MIT
Kent Seamons, Brigham Young University
Frank Siebenlist, Argonne National Lab
Sean Smith, Dartmouth College
Michael Wiener, Cryptographic Clarity
Von Welch, NCSA
Will Winsborough, George Mason University

3. プログラム

Session 1: Papers - Shibboleth and more

- "Adding Distributed Trust Management to Shibboleth", David Chadwick, Sassa Otenko, Wensheng Xu, and Zhi Qing Wu University of Kent, England
- "Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration", Von Welch, National Center for Supercomputing Applications, University of Illinois, Tom Barton, Networking Services & Information Technologies, University of Chicago, Kate Keahey, Argonne National Laboratory, and Frank Siebenlist, Argonne National Laboratory
- "XPOLA - An Extensible Capability-based Authorization Infrastructure for Grids", Liang Fang, Indiana University, Dennis Gannon, Indiana University, and Frank Siebenlist, Argonne National Laboratory

Session 2 - Panel - PKI Interoperability and Federations

- "Interfederation Interoperability, E-Authentication and Shibboleth", Ken Klingenstein, University of Colorado; Internet2
- "International and Bridge-to-Bridge Interoperability", Peter Alterman, National Institutes of Health
- "HEBCA and Phase 4 of the PKI Interoperability Project", Scott Rea Dartmouth College

Session 3 Papers: Services in Support of PKI

- "The Design and Implementation of LDAP Component Matching for Flexible and Secure Certificate Access in PKI", Sang Seok Lim, IBM T.J. Watson Research Center, Jong Hyuk Choi, IBM T.J. Watson Research Center, and Kurt D. Zeilenga, IBM Linux Technology Center
- "PKI without Revocation Checking", Karl Scheibelhofer, Institute for Applied Information Processing and Communications, Graz University of Technology
- "Delegation Issuing Service for X.509", David W. Chadwick, IS Institute, University of Salford, Salford, England

Session 4: Papers - PKI In government

- "Meeting the Challenges of Canada's Secure Delivery of E-Government Services", Mike Just and Danielle Rosmarin, Public Works and Government Services Canada
- "The Use of PKCS-12 in the Federal Government", Tice F. DeYoung, National Aeronautics Space Administration
- "Secure Access Control with Government Contactless Cards", David Engberg, CoreStreet, Ltd.

Session 5: Papers - Improving the Usability of PKI

- "Identity-Based Encryption with Conventional Public-Key Infrastructure", Jon Callas, PGP Corporation
- "A Proxy-Based Approach to Take Cryptography Out of the Browsers for Better Security and Usability", Marco Carnut, Tempest Security Technologies and Evandro Curvelo Hora, Universidade Federal de Sergipe - DCCE/CCET

Session 6: Standards Activities

- "Internet Engineering Task Force update", Russ Housley Vigil Security LLC and Tim Polk NIST
- "Pairing standards for Identity Based Encryption", Terence Spiess Voltage Security

Session 7: Papers - Scale and performance

- "Side-Effects of Cross-Certification", James Fisher, Mitretek Systems
- "Evaluating the Performance Impact of PKI on BGP

Security", Meiyuan Zhao, Dartmouth College, Sean Smith, Dartmouth College, and David Nicol, University of Illinois at Urbana-Champaign

- "Observations from the Deployment of a Large Scale PKI", Rebecca Nielsen, Booz Allen Hamilton

Session 8: Work-in-Progress talks

- "Ceremony Analysis", Carl Ellison, Microsoft
- "An idea for Instantaneous Secure Enrollment", Marco Carnut, Tempest Security Technologies
- "Modeling Strength of Security & Its application in PKI", Ho Chung, University of Southern California and Clifford Neuman, USC-ISI
- "PKI Projects in Brazil Jeroen Van de Graaf", Universidade Federal de Minas Gerais

Session 9: Papers - Miscellaneous

- "Language Based Policy Analysis in a SPKI Trust Management System", Arun K. Eamani and A. Prasad Sistla, University of Illinois at Chicago
- "Enhancing Security of Security-Mediated PKI by One-time ID", Satoshi Koga, Kenji Imamoto, and Kouichi Sakurai, Kyushu University

Session 10 Paper and Panel - PKI In Healthcare

- "On Securing the Public Health Information Network Messaging System", M. Barry Rhodes, Centers for Disease Control and Prevention and Rajashekar Kailar, Business Networks International Inc.
- PANEL: "PKI In Healthcare", Richard Guida, Johnson & Johnson

Invited Talk

- "Progress in Hashing Cryptanalysis", Arjen Lenstra Bell Labs (Lucent Technologies)

Birds of a Feather session

- "Usability and Human Factors", Eric Norman, University of Wisconsin

4. 発表内容

本章では，第4回 PKI R&D ワークショップにおいて発表された論文，パネル講演，招待講演の概要をいくつか紹介する．

"Adding Distributed Trust Management to Shibboleth", David Chadwick, Sassa Otenko, Wensheng Xu, and Zhi Qing Wu University of Kent, England

Shibboleth とは，シングル・サイン・オンを可能とする，ウェブベースの認証や認可システムの1つである．本論文では，ターゲットサイトとオリジンサイトは相互に信頼している前提が必要ということから，Shibboleth のトラストモデルに制限がある点を指摘し，その問題が X.509 証明書を用いることで解決可能であることを示している．強化したトラストモデルでは，複数の属性認証局が属性を発行できるべきであり，ターゲットはどれを信頼するか選択できるべき，としている．

"XPOLA - An Extensible Capability-based Authorization Infrastructure for Grids", Liang Fang, Indiana University, Dennis Gannon, Indiana University, and Frank Siebenlist, Argonne National Laboratory

グリッド・セキュリティ・インフラストラクチャ（GSI）では，公開鍵システムが安全性の基礎として適用されている．グリッドサービスを用いるためには，多くの手続き（証明書発行，グリッドマップ更新など）が必要となる．これにより，実際のグリッドアプリケーションにおける認可問題として，管理の拡張性が乏しい，認可されたユーザがサービスに接続する以上のことができる，などが存在している．既存の Fine-grained authorizaiton 方式としては，ACL モデル（Akenti, Shibboleth, PERMIS など），Capability モデル（CAS, VOMS, PRIMA）などがあるが，既存の方式では一般的な Web/Grid サービスやダイナミックなサービスを考慮していない．本論文では，一般的な Web/Grid サービスに対し，細かな認可インフラを提供可能な XPOLA が提案されている．本方式は、ユーザレベルでの peer-to-peer 信頼関係に基づいており、細かな認可ポリシーによる Web/Grid サービスが実現している．

"PKI without Revocation Checking", Karl Scheibelhofer, Institute for Applied Information Processing and Communications, Graz University of Technology

現在の X.509 証明書を用いた PKI システムは，証明書の有効性確認（revocation check）が行われるため，構成が複雑になっている．この処理を行う場合，CA にとっては無効化情報を提供するために高いコストが掛かり，クライアントにとってはそれら全ての情報を収集するために高いコストが掛かる．本論文では，このような有効性確認の手続きを取り除くため，CA に対してオンラインでアクセスすることにより証明書を生成するシステムが提案されている．シミュレーションにより，本システムが従来の有効性確認手法である CRL，差分 CRL，OCSP 以上に通信・計算の効率性が良いことが示されている．欠点は，OCSP 同様，クライアントが有効性確認のたびに検証サーバへアクセスする必要がある点である．

"Meeting the Challenges of Canada's Secure Delivery of E-Government Services", Mike Just and Danielle Rosmarin, Public Works and Government Services Canada

本論文では，個人やビジネスでの PKI による認証の開発・発展に関する多くの技術的，法的問題，およびビジネスに関わる問題として，カナダにおける状況が紹介されている．カナダでは，電子政府サービスをサポートする技術として Secure Channel (SC) と呼ばれる認証サービスを含んだネットワーク基盤が市民へ提供されている．市民は SC を利用する際，*epass* と呼ばれるカナダ政府発行の公開鍵証明書を利用できる．問題として，カナダは多くの地域に分けられるため，各地域間でのポリシーやビジネスへの要求の違いによる相互運用性，法律の制定などの問題がある．その他，電子情報の証拠性を保証する

ためのサポートに関する問題も存在する．著者らは，サービス提供に関わる各問題に対するこれまでの取り組み，および現在までに解決されていない問題を紹介している．

"Identity-Based Encryption with Conventional Public-Key Infrastructure", Jon Callas, PGP Corporation

IBE システムの興味深い点は，オフラインでの鍵生成が可能であるという点が挙げられる．しかし，オフラインでの鍵生成は安全性の問題が起こる．例えば，不正ユーザが鍵を生成し，その鍵を利用したスパム送信，サイドチャネル攻撃がある．また，鍵廃棄が困難であるという問題がある．そこで本論文では，このような問題を解決するためにオンラインで鍵生成する IBE システムを提案している．提案するオンライン鍵生成 IBE システムを用いることにより，既存システムとの相互運用，IBE と non-IBE システム要素をミックス可能，既存のあらゆる公開鍵システムを利用可能（RSA, DSS など）といった効果が得られる．

パネル講演: "Internet Engineering Task Force update", Russ Housley Vigil Security LLC and Tim Polk NIST

本講演では，前回のワークショップからの IETF による作業の進展状況，および未解決の問題が報告された．進展として，Public key infrastructure using X.509 では，ドキュメントの公開，RFC3779（現在は 3280bis，SCVP の作成），および 3280bis の新しいコンセプトとして，国際的な名前付けのためのサポートを拡張した（IDN，IRI，メールアドレス）．また PKI for IPsec（PKI4IPsec）においては IKE のための証明書プロファイルを作成している．未解決問題として，PKI4IPsec における VPN デバイスの登録がある．現時点では要求に関するドキュメントはほぼ終了したが，プロトコル に関するドラフトはまだ未完成である．WG の目標は，登録手続きを記述するためのモデル作成，登録のためのフレームワーク作成，および各 credential type のためのプロファイル作成が挙げられる．

パネル講演: "Pairing standards for Identity Based Encryption", Terence Spiess, Voltage Security

本講演は，次章で説明する 2005 年 4 月 18 日に開催された IEEE P1363 Working Group の標準化ミーティング参加者の 1 人による発表であり，ペアリングを用いた暗号システムの標準化活動の報告が行われた．最初にペアリングによって実現できるシステムとして，IBE システム，ID ベースの鍵交換，署名（160bit 署名），探索可能な暗号化などを紹介した．本標準化活動の目的は PAR（Project Authorization Request）のドラフト投稿である．PAR には，標準規格の目的と適用範囲，IEEE-SA の標準化プロセスに準拠していることを示す管理情報も明記する．支援組織は，この PAR を IEEE-SA の新標準委員会（NESCOM）に提出する．現在の議論のポイントは安全性を 128/256 ビットへ拡大，およびペアリングと暗号のレイヤ分けなどが考えられている．

"Observations from the Deployment of a Large Scale PKI", Rebecca Nielsen, Booz Allen Hamilton

アメリカ合衆国国防統合軍（DoD: United States Department of Defense）が 2000 年に PKI を運用開始して以来，その公開鍵証明書ユーザ 350 万人の内，85% 以上の証明書を Common Access Cards (CAC) を用いて発行している．本論文では，世界最大規模の PKI の発展から学んだ技術的，組織的教訓が示されている．DoD PKI を運用する際に考慮すべき点として PKI の構成，CA の拡張性，システムを構成するハードウェア・ソフトウェアの管理などが挙げられる．また技術的に最も解決困難な問題として証明書の有効性確認が挙げられ，利用者が最も必要とする機能として鍵復元が存在し，組織的課題としてはポリシーの設定，ユーザやアプリケーション開発者に対する教育などが存在する．さらに，これらの問題に対する DoD のこれまでの取り組みや今後の動向が説明されている．

"On Securing the Public Health Information Network Messaging System", M. Barry Rhodes, Centers for Disease Control and Prevention, and Rajashekar Kailar, Business Networks International Inc.

Public Health Information Network Messaging System (PHINMS) とは，Centers for Disease Control（CDC）により開発された，インターネットを介した安全で信頼性の高いメッセージ送受信システムである．本論文では，PHINMS に対して様々なセキュリティの観点からシステムを検討した結果が報告された．具体的には，認証・認可・秘匿性・非拒否性・完全性，および本システムにおける PKI やファイアウォール，認証の相互運用性について検討した結果が報告されている．

パネル講演: "PKI, Security, and Health Care", モデレータ : Richard Guida, Johnson and Johnson パネラー : Terry Zagar Biopharma SAFE initiative, John Landwehr Adobe

モデレータである Richard Guida からは，病院での医療情報に関するセキュリティの現状が紹介された．ヘルスケアに関わる人・機関としては医者，病院，患者，医療機器会社，政府，研究者が存在している．これらを個人の健康に関する情報（PHI: Personal Health Information）の取り扱いの観点から見ると，患者の情報を扱うパーティとして医者・病院・患者・研究者，通常は扱わないパーティとして医療機器会社・政府に分類される．PHI の取り扱いについては，いくつかの法律によって規定されており，高いセキュリティの実現が必要となる．PHI に関する重要なプロセス例としては，新薬の実験，保険記録の管理，製品配布，支払いが挙げられ，それぞれに対して完全性/認証/秘匿性が必要となる．現在のヘルスケアに関するセキュリティは，ほとんどが ID/PassWD ベースの認証に基づいているが，現在は広範囲にわたって公開鍵を用いた証明書ベースの方式への動きが広まっている．証明書を用いることによって得られる利点として，情報管理がシンプルになる，署名や公開鍵暗号な

どのより強い安全性が得られる点がある.

John Landwehr は "Digital Signature Update Acrobat/Reader7.0" というタイトルで, Acrobat/Reader7.0 における電子署名への取り組みについて説明された. 電子署名はフィッシングや情報漏えいを防ぐ (そのドキュメントを誰がいつ生成したのか, 偽造されていないかを確認) ことを目的とし, 1999 年の Acrobat4.0 から利用可能になった. Acrobat/Reader7.0 で新しくなった点として, OCSP, RFC3161 のタイムスタンプ, ブリッジ CA からの証明書, XML 署名, SHA-256 検証, PKCS#11 のサポートなどへの対応がある. 本製品は第三者機関によるテストとして NIST PKI Test Suite (250 以上のテストをクリア), DoD JITC Certified (全テストをクリア), FIPS 201 cards (評価中) などを受けている. また, 本製品では PDF ではないコンテンツに対しても署名が可能であり, 他フォーマットのファイルを PDF フォームへ添付し, 署名処理に含むことができる.

招待講演: "Progress in Hashing Cryptanalysis", Arjen Lenstra, Bell Labs (Lucent Technologies)

本講演では, ハッシュ関数がどのような性質を持った関数であるかを説明した後, MD4 や MD5, SHA family などのハッシュ関数に対する暗号解析の歴史を紹介した. その際, 2005 年 2 月に発表された Wang らによる研究の結果 (SHA-1 に対するランダム・コリジョンに関する攻撃) を紹介し, SHA-1 が 2010 年まで持つのは難しそうであるという見解を述べた. これまでに発見された衝突は全てランダム・コリジョンであり, 実際に意味のある攻撃にはつながらないと考えられてきたが, 無作為の衝突を重要なデータに変換することが可能となることを, X.509 証明書に対する攻撃を例として紹介した (講演者のサイト [7] にて, MD5 に基づいた有効な X.509 証明書の組が示されている). このような問題を防ぐため, Twin RSA と呼ばれる新たな RSA 公開鍵システムの構成を示した.

5. IEEE 1363 Study Group Meeting on Pairing based Cryptography and Identity based Encryption

本章では, 第 4 回 PKI R%D ワークショップの前日 (2005 年 4 月 18 日) に開催された IEEE 1363 Study Group Meeting on Pairing based Cryptography and Identity based Encryption の参加報告を行う. 本会議は IEEE P1363 ワーキンググループによる会議であり, ペアリングに基づいた IBE システムの標準化を目指している. 今回の参加者は 24 名であった. 本会議では質疑応答が活発に行われ, 発表の途中でも参加者間での議論が頻繁に起こっていた. 論文発表などの会議とは違い, 標準化に向けての指針や現在の活動状況を報告した上で, 今後どのように活動するか検討するための議論が行われた. 本会議にて使用された発表資料は, IEEE P1363 WG の活動を知らせる HP 内 [8] にて公開されている.

"IEEE Standards Process", William Whyte (NTRU, IEEE 1363)

IEEE の WG で標準化される際に必要な手続きについて説明された. 最初にスポンサーを見つけ, Study group を設立して PAR を投稿する. その後 WG を組み, ドキュメントを書いてスポンサー投票を行う. WG ミーティングでの投票では投票者の 75% 以上の賛成が必要となる. 投票が失敗した場合は再投票が必要となり, 投票が成功した場合, RevCom (review committee) により審査される. その際には全投票のコメントがアドレスされたこと, およびその標準化が IEEE ガイドラインを満たしていることが確認され, その後その内容が発布される. これらの工程は全部でおよそ 3 年掛かる.

"Pairing Standards", Hovav Shacham

ペアリングの標準化に向け, ペアリングに関する研究の現状や実装の際のパラメータ設定について発表した. ペアリングを実装する際のオプションとして, 使用する体・カーブ・ペアリングのタイプなどがある. しかし, すべての組み合わせを記述すると, 標準化を書く・実装・採用が難しくなるので, 原則として標準化のスコープを最小化, より一般的なカーブ族の利用, 速度が最重要でサイズはその次, といったことを考える必要がある. 発表者が推薦するパラメータとしては, カーブは Supersingular および ordinary, 埋め込み次数には $k = 2$ のみ, Tate ペアリングのみを使用するといったことが挙げられている.

また, Mike Scott (Noretech Ltd.) からもペアリングの標準化についての話があり, 標準化では, 記述ができるだけ実装する人に対してフレンドリーであること (数学的過ぎないこと) が大事であると述べた. 現在のペアリングの研究動向を紹介し, 恐らく "reasonable" なセキュリティレベルにおいては Tate ペアリングの方が Weil ペアリングより優ることを主張した. 問題として, 安全性証明が正しく行われるように設計すること, および今発表者が行っていることと Hovav の結果との間の境界線が不明確であることを挙げた.

"D20.1 Draft Standard Specification for Password-based Public Key Cryptographic Techniques"

2005 年 3 月 31 日の電話会議にて PKRS-1 に対する攻撃が指摘されたので, それに基づいてドラフト D20 を更新したことが報告された. 具体的には, PKRS-1 における攻撃者のパスワード推測の制限について追加, およびグループパスワードについての記述を修正した. 発表後の議論では, 頻繁なパスワードの変更が必要となった場合, ユーザによるパスワード選択が単調になる危険性が指摘された.

また, ペアリングによる IBE 標準化のドラフト投稿に関するディスカッションが行われ, 現在作成中の投稿内容に問題がないか話し合われた. 議論の中では, IBE は認証を含むのか, 投稿タイトルが内容を制限しすぎているので修正すべきではないか, 概要の中で使われている「アルゴリズム」とはどのような意味で使っているのか, 他に類似のプロジェクトが存在するのか (2 つの IBE ベースの署名を含んだ, 署名に関するプロジェ

クトが存在することを確認），といった様々な検討がされ，内容の修正が確認された．

6. まとめ

本論文では，第4回 PKI R&D ワークショップの開催概要について報告した．ワークショップ参加者には論文を掲載した予稿集が配布されたが，論文及び発表資料はワークショップのホームページ[4]上に公開されている．また，IEEE 1363 Study Group Meeting on Pairing based Cryptography and Identity based Encryption についても報告した．

謝　辞

本研究の一部は，21世紀 COE プログラム「システム情報科学での社会基盤システム形成」の支援，および財団法人 セコム科学技術振興財団からの支援を受けている．また，第一著者は日本学術振興会科学研究費補助金（特別研究員奨励費 課題番号：06737）からの支援を受けている．

文　献

[1] 1st Annual PKI Research Workshop
http://www.cs.dartmouth.edu/ pki02/
[2] 2nd Annual PKI Research Workshop
http://middleware.internet2.edu/pki03/
[3] 3rd Annual PKI R&D Workshop
http://middleware.internet2.edu/pki04/
[4] 4th Annual PKI R&D Workshop
http://middleware.internet2.edu/pki05/
[5] 古賀, 櫻井, “第2回 PKI 研究ワークショップ参加報告”, 情報セキュリティ研究会 (ISEC), 信学技報 Vol.103 No.196, Jul. 2003.
[6] 古賀, 菊池, “第3回 PKI R&D ワークショップ参加報告”, 情報セキュリティ研究会 (ISEC), 信学技報 Vol.104 No.199, Jul. 2004.
[7] A. Lenstra, “Colliding X.509 Certificates based on MD5-collisions”,
http://www.win.tue.nl/ bdeweger/CollidingCertificates/
[8] The IEEE P1363 Working Group
http://grouper.ieee.org/groups/1363/WorkingGroup/