

2005 年暗号と情報セキュリティシンポジウムプログラム

1A1	招待講演	1月25日 13:00 ~ 14:00	
1A1-1	情報セキュリティ・アーキテクチャ 大塚寿昭氏 (総務省)		招待講演
1A2	秘密分散	1月25日 14:40 ~ 16:20	
1A2-1	PC共有による安全で低コストなP2Pファイル分散システム 鹿島隆行 (東京工科大学) 宇田隆哉 (東京工科大学) 伊藤雅仁 (東京工科大学) 市村哲 (東京工科大学) 田胡和哉 (東京工科大学) 松下温 (東京工科大学)		1
1A2-2	フレキシブルな料金形態を可能とする視聴率調査方式 阿部正己 (東京工業大学) 荒木俊則 (東京工業大学) 尾形わかは (東京工業大学)		7
1A2-3	アクセス制御機構を持つP2Pファイル共有システム 大津 一樹 (東京工科大学) 宇田 隆哉 (東京工科大学) 伊藤 雅仁 (東京工科大学) 市村 哲 (東京工科大学) 田胡 和哉 (東京工科大学) 松下 温 (東京工科大学)		13
1A2-4	最少トランザクションによる電子権利譲渡方式の提案 廣田啓一 (NTTサイバースペース研究所) 萬本正信 (NTTサイバースペース研究所) 山本隆二 (NTTサイバースペース研究所)		19
1A2-5	移動エージェントを用いた鍵預託の提案 猪俣敦夫 (独立行政法人科学技術振興機構) 中川沙絵 (筑波大学) 岡本栄司 (筑波大学)		25
1B2	ステガノグラフィー	1月25日 14:40 ~ 16:20	
1B2-1	埋め込み位置を記憶不要なJPEG 2000符号化画像のステガノグラフィ 金弘林 (東京都立大学) 関裕介 (東京都立大学) 藤吉正明 (東京都立大学) 貴家仁志 (東京都立大学)		31
1B2-2	DCTブロック毎の複雑さを考慮したJPEG圧縮画像に対するステガノグラフィ 古賀 友久 (大阪府立大学) 岩田 基 (大阪府立大学) 荻原 昭夫 (大阪府立大学) 汐崎 陽 (大阪府立大学)		37
1B2-3	ステガノグラフィの新しい利用法について 石塚裕一 (三菱電機(株)) 西岡毅 (三菱電機(株)) 長谷川俊夫 (三菱電機(株)) 鶴丸豊広 (三菱電機(株))		43
1B2-4	複数画像が復元可能な視覚復号型秘密分散法 清田耕一朗 (電気通信大学) 王磊 (電気通信大学) 岩本貢 (電気通信大学) 米山一樹 (電気通信大学) 國廣昇 (電気通信大学) 太田和夫 (電気通信大学)		49
1B2-5	編集ソフトウェアの特徴を利用する攻撃への耐性を有するSMFステガノグラフィ方式の評価 遠山毅 (横浜国立大学) 鈴木雅貴 (横浜国立大学) 四方順司 (横浜国立大学) 松本勉 (横浜国立大学)		55
1C2	セキュアOS	1月25日 14:40 ~ 16:20	
1C2-1	同一計算機内プロセス間通信に対する保護のための一手法 稲村雄 (株式会社NTTドコモ) 竹下敦 (株式会社NTTドコモ)		61
1C2-2	Construction of RBAC-Enforceable Security Automata Hyung Chan Kim (Gwangju Institute of Science and Technology) Wook Shin (Gwangju Institute of Science and Technology) R. S. Ramakrishna (Gwangju Institute of Science and Technology) Kouichi Sakurai (Kyushu University)		67
1C2-3	XExt3: The design and Implementation of a Security Enhanced Ext3 File system Jiho Cho (GIST) Dong-Hoon Yoo (GIST) Hyung-Chan Kim (GIST) R.S.Ramakrishna (GIST) Kouichi Sakurai (Kyusyu Univ.)		73
1C2-4	ファイルアクセスパーミッションの統合手法とそのトレードオフに関する考察 田端 利宏 (九州大学) 櫻井 幸一 (九州大学)		79
1C2-5	組み込み・モバイル機器のセキュリティリスクとその対策の検討 三品拓也 (日本アイ・ピー・エム(株) 東京基礎研究所) 吉濱佐知子 (日本アイ・ピー・エム(株) 東京基礎研究所) 宗藤誠治 (日本アイ・ピー・エム(株) 東京基礎研究所)		85
1D2	認証	1月25日 14:40 ~ 16:20	
1D2-1	タイムスタンププロトコルのUC安全性について 松尾俊彦 ((株)NTTデータ) 松尾真一郎 ((株)NTTデータ)		91

1D2-2	パスファンクションを用いたユーザ認証法の安全性について	97
	手嶋牧子 (奈良先端科学技術大学院大学) 野島良 (奈良先端科学技術大学院大学) 楢勇一 (奈良先端科学技術大学院大学)	
1D2-3	制限付ブラインド認証と署名	103
	古川 潤 (日本電気) 今井秀樹 (東京大学)	
1D2-4	Bilinear Map を利用した Refreshable Tokens Scheme	109
	繁富利恵 (東京大学) 大塚玲 (情報処理推進機構) 今井秀樹 (東京大学)	
1D2-5	分割して署名されたデータの認証のための符号系列について	115
	萩田真理子 (お茶の水女子大学) 松本真 (広島大学)	
1E2	暗号実装と安全性	1月25日 14:40 ~ 16:20
1E2-1	Fast On-The-Fly Exponent Recording	121
	Erik Dahmen (Technische Universitaet Darmstadt) Katsuyuki Okeya (Systems Development Laboratory, Hitachi, Ltd.) Katja Schmidt-Samoa (Technische Universitaet Darmstadt) Tsuyoshi Takagi (Technische Universitaet Darmstadt, Fachbereich Informatik, Hochschulstr. 10, D-64283 Darmstadt, Germany)	
1E2-2	量子加算に基づく Shor のアルゴリズムの評価	127
	鈴木博一 (電気通信大学) 國廣昇 (電気通信大学) 太田和夫 (電気通信大学)	
1E2-3	テーブルネットワーク型暗号実装ソフトウェアのデータサイズ削減法	133
	佐藤卓也 (横浜国立大学) 松本勉 (横浜国立大学)	
1E2-4	テーブルネットワーク型暗号実装ソフトウェアの耐タンパー性評価法	139
	松永明 (横浜国立大学) 四方順司 (横浜国立大学) 松本勉 (横浜国立大学)	
1E2-5	White-box 攻撃に対する耐性を向上させた多倍長演算の実装	145
	小黑 博昭 (NTT データ) 飯野 徹 (NTT データ) 平井 康雅 (NTT データ) 箱守 聰 (NTT データ)	
1F2	暗号理論 -1	1月25日 14:40 ~ 16:20
1F2-1	ランダムオラクルモデルを用いたプロトコルの指標と方式	151
	鈴木学 (東京工業大学) 田中圭介 (東京工業大学)	
1F2-2	準同型暗号関数を用いた紛失通信と秘匿情報検索	157
	山村明弘 (情報通信研究機構) Tatiana Jajcayova (Comenius University, Slovakia) 黒川貴司 (情報通信研究機構)	
1F2-3	A Universally Composable Secure Channel Based on the KEM-DEM Framework	163
	Waka Nagao (Kyoto university) yoshifumi manabe (NTT/Kyoto University) Tatsuaki Okamoto (NTT/Kyoto University)	
1F2-4	情報理論的に安全なステガノグラフィの再考察	169
	四方順司 (横浜国立大学) 鷹嘴成寿 (横浜国立大学) 松本勉 (横浜国立大学)	
1F2-5	Bounded Storage Model において情報理論的に安全なステガノグラフィ (その2)	175
	鷹嘴成寿 (横浜国立大学) 四方順司 (横浜国立大学) 松本勉 (横浜国立大学)	
1A3	電子メールセキュリティ	1月25日 16:35 ~ 18:15
1A3-1	平均計算量の下界が保証されたスパム対策用プライミング関数の考察	181
	砂見 渉 (奈良先端科学技術大学院大学) 野島 良 (奈良先端科学技術大学院大学) 楢 勇一 (奈良先端科学技術大学院大学)	
1A3-2	迷惑メール内の Word Salad による統計的フィルタリングの学習データへの影響	187
	岩永 学 (九州大学) 田端 利宏 (九州大学) 櫻井 幸一 (九州大学)	
1A3-3	フィッシングメール防御のためのメールフィルタリング手法の提案	193
	猪俣敦夫 (独立行政法人科学技術振興機構) ラーマンミザヌール (筑波大学) 岡本健 (筑波大学) 岡本栄司 (筑波大学)	
1A3-4	ベイジアンフィルタを用いた迷惑メールフィルタリングの最適化	199
	大福 泰樹 (東京大学) 松浦 幹太 (東京大学)	
1A3-5	情報の二次利用ポリシーを記述可能なメールシステムの提案と実装	205

中村真也 (奈良先端科学技術大学院大学) 衛藤将史 (奈良先端科学技術大学院大学) 門林雄基 (奈良先端科学技術大学院大学)

1B3 画像認証	1月25日 16:35 ~ 18:15
1B3-1 印鑑画像を用いた認証システムの提案	211
小林 克樹 (長野工業高等専門学校) 藤澤 義範 (長野工業高等専門学校)	
1B3-2 画像認証システム「あわせ絵」の有効性実証のための評価実験	217
大貫岳人 (電気通信大学) 高田哲司 (ソニーコンピュータサイエンス研究所) 小池英樹 (電気通信大学)	
1B3-3 写真を使った個人認証の脆弱性に対する改善策の提案	223
大貫岳人 (電気通信大学) 高田哲司 (ソニーコンピュータサイエンス研究所) 小池英樹 (電気通信大学)	
1B3-4 画像認証方式の一評価実験	229
小野束 (筑波技術短期大学)	
1B3-5 画像記憶のスキーマを利用したユーザ認証の有効性に関する一検討	235
原田 篤史 (静岡大学) 漁田 武雄 (静岡大学) 西垣 正勝 (静岡大学)	
1C3 無線ネットワークセキュリティ	1月25日 16:35 ~ 18:15
1C3-1 Formal Verification of the Security Properties of EAP-TLS,EAP-MD5 Protocols in Wireless Network: CSP/FDR Model checking	241
タベトアブデイラフ (東京大学) 古原和那 (東京大学) 今井秀樹 (東京大学)	
1C3-2 無線LANにおけるMISプロトコルに対するセキュリティ評価	247
堀良彰 (九州システム情報技術研究所 / 九州大学) 森岡仁志 (ルート株式会社) 真野浩 (ルート株式会社) 櫻井幸一 (九州システム情報技術研究所 / 九州大学)	
1C3-3 WEPの鍵回復攻撃をかわすための鍵更新タイミングに関する考察	253
吉田雅徳 (東京大学) 古原和那 (東京大学) 今井秀樹 (東京大学)	
1C3-4 Impact of security on latency in WLAN 802.11	259
Hanane Fathi (Aalborg University) Kazukuni Kobara (the University of Tokyo) Shyam Chakraborty (Helsinki University) Ramjee Prasad (Aalborg University) Hideki Imai (the University of Tokyo)	
1C3-5 無線環境における位置情報プライバシーのモデルに関する提案	265
黄楽平 (東京大学) 松浦 幹太 (東京大学) 山根弘 (東京大学) 瀬崎 薫 (東京大学)	
1D3 鍵管理	1月25日 16:35 ~ 18:15
1D3-1 コンテンツ配信のためのグループ化による効率的な鍵管理方式	271
福島 和英 (株式会社KDDI研究所) 清本 晋作 (株式会社KDDI研究所) 田中 俊昭 (株式会社KDDI研究所)	
1D3-2 ヘッドサイズを削減したより強力な不正者に対するブラックボックス追跡	277
松下 達之 (東芝) 今井 秀樹 (東京大学)	
1D3-3 散布型セキュアセンサネットワークにおける散布の確率分布を利用した鍵格納方式	283
伊藤 隆 (三菱電機) 太田 英憲 (三菱電機) 松田 規 (三菱電機) 米田 健 (三菱電機)	
1D3-4 時間限定サービスを実現するための時系列鍵管理方式	289
楯 勇一 (奈良先端科学技術大学院大学) 野島 良 (奈良先端科学技術大学院大学)	
1D3-5 可変指向性アンテナを利用した無線秘密鍵共有システム	295
青野智之 (ATR) 樋口啓介 (ATR) 大平孝 (ATR) 小宮山牧兒 (ATR) 笹岡秀一 (同志社大学)	
1E3 ハードウェア実装	1月25日 16:35 ~ 18:15
1E3-1 高性能GF(p)演算器を搭載した楕円曲線暗号LSI	301
小林伸行 (早稲田大学) 久門亨 (早稲田大学) 後藤敏 (早稲田大学) 池永剛 (早稲田大学) 内田純平 (早稲田大学) 角尾幸保 (NECインターネットシステム研究所)	
1E3-2 高基数SRT除算に基づくスケラブル剰余乗算回路	307
葛毅 (東京大学) ルオンディンフォン (東京大学) 阿部公輝 (電気通信大学) 坂井修一 (東京大学)	
1E3-3 素因数分解ハードウェアTWIRLの実現可能性に関する検討報告(III)	313
伊藤孝一 (富士通研究所) 伊豆哲也 (富士通研究所)	
1E3-4 リコンフィギュラブルデバイスを用いたブロック暗号のハードウェア実装評価	319

	反町亨 (三菱電機株式会社情報技術総合研究所) 市川哲也 (三菱電機エンジニアリング)	
1E3-5	MUGI のハードウェア実装及び評価	325
	大和田徹 (日立製作所システム開発研究所) 平重喜 (日立製作所システム開発研究所) 五十嵐 悠一 (日立製作所システム開発研究所) 北原潤 (日立製作所システム開発研究所)	
1F3	暗号理論 -2	1月25日 16:35 ~ 18:15
1F3-1	On The Necessary Assumptions For A Class Of Asymmetric Encryption Schemes	331
	張銳 (東京大学) 花岡悟一郎 (東京大学) 今井秀樹 (東京大学)	
1F3-2	Random Oracle Methodology and Secure Instantiation	337
	小林良成 (中央大学) 高橋淳也 (中央大学) 辻井重男 (情報セキュリティ大学院大学)	
1F3-3	A Scheme for PECK Search Based on the Computational Bilinear Diffie-Hellman Problem	343
	金内志津 (東京工業大学) 田中圭介 (東京工業大学)	
1F3-4	ギャップ問題に基づく公開鍵暗号方式の安全性証明におけるギャップ	349
	藤崎英一郎 (日本電信電話株式会社) 内山成憲 (日本電信電話株式会社)	
1F3-5	汎用的結合可能なグループ署名について	355
	牧田 俊明 (京都大学) 真鍋 義文 (NTT サイバースペース研究所) 岡本 龍明 (NTT 情報流通プラットフォーム研究所)	
2A1	バイOMETRICS -1	1月26日 9:00 ~ 10:40
2A1-1	ペンの移動角度に基づく DWT 領域オンライン署名照合	361
	坂本大征 (鳥取大学) 原秀樹 (鳥取大学) 中西功 (鳥取大学) 伊藤良生 (鳥取大学) 副井裕 (鳥取大学)	
2A1-2	任意筆記における筆者照合時のペンの傾き補正の効果について	367
	川添太郎 (東京理科大学) 吉田孝博 (東京理科大学) 半谷精一郎 (東京理科大学)	
2A1-3	テキストへの埋め込みを目指したオンライン手書き署名の圧縮について	373
	粕川正充 (お茶の水女子大学)	
2A1-4	手による数字表現と本人確認	379
	小林哲二 (日本工業大学) 町田則文 (日本工業大学)	
2A1-5	耳介軟骨の輪郭抽出法	385
	山元 正裕 (工学院大学) 篠原 克幸 (工学院大学) 和田 敏弘 (工学院大学)	
2B1	ストリーム暗号	1月26日 9:00 ~ 10:40
2B1-1	MAC 生成機能を持つストリーム暗号の安全性評価	391
	安藤俊介 (中央大学) 下山武司 (株式会社富士通研究所) 趙晋輝 (中央大学)	
2B1-2	Complexity of Distinguishing Attacks on Clock Controlled Stream Ciphers	397
	清本晋作 (KDDI 研究所) 田中俊昭 (KDDI 研究所) 櫻井幸一 (九州大学)	
2B1-3	内部状態遷移型ストリーム暗号 SSSM の提案 (第 2 報)	403
	鷗川三蔵 (徳島大学) 大東俊博 (徳島大学) 元家宏美 (徳島大学) 白石善明 (近畿大学) 森井昌克 (徳島大学)	
2B1-4	パリティ検査式を用いた事後確率復号に基づく高速相関攻撃の復号誤り確率の低減について	409
	福田 洋治 (徳島大学) 白石 善明 (近畿大学) 森井 昌克 (徳島大学)	
2B1-5	非線形コンバイナ型擬似乱数生成器に対する線形化攻撃に関する一考察	415
	田中秀磨 (独立行政法人情報通信研究機構)	
2C1	コンテンツセキュリティ -1	1月26日 9:00 ~ 10:40
2C1-1	電子文書の訂正・流通を考慮した部分完全性保証方式の改良	421
	吉岡孝司 ((株) 富士通研究所) 武仲正彦 ((株) 富士通研究所)	
2C1-2	Rabin Tree に基づく Broadcast Encryption 再考	427
	浅野 智之 (ソニー (株)) 神尾 一也 (ソニー (株))	
2C1-3	MPEG 圧縮標準向け高セキュリティ及び低オーバーヘッドの部分的ビデオ暗号化手法	433
	劉剛 (早稲田大学) 後藤敏 (早稲田大学) 馬場孝明 (早稲田大学) 池永剛 (早稲田大学)	
2C1-4	不正使用を防止した放送コンテンツ保存方式	439

	稲村 勝樹 (KDDI 研究所 / NHK 放送技術研究所) 小川 一人 (NHK 放送技術研究所) 田中 俊昭 (KDDI 研究所)	
2C1-5	JPEG 2000 の階層性を考慮したアクセス制限型暗号化法	445
	今泉祥子 (東京都立大学) 渡邊修 (拓殖大学) 藤吉正明 (東京都立大学) 貴家仁志 (東京都立大学)	
2D1	サイドチャネル攻撃 -1	1月26日 9:00 ~ 10:40
2D1-1	ランダム化初期点を用いた電力解析対策法について (その3)	451
	伊藤 孝一 ((株) 富士通研究所) 伊豆哲也 ((株) 富士通研究所) 武仲 正彦 ((株) 富士通研究所)	
2D1-2	Security Analysis of OT Scheme	457
	Camille Vuillaume (Hitachi, Ltd., Systems Development Laboratory) Katsuyuki Okeya (Hitachi, Ltd., Systems Development Laboratory) Tsuyoshi Takagi (Technische Universitaet Darmstadt)	
2D1-3	格子基底縮小アルゴリズムを用いた (EC)DSA へのサイドチャネル解析について	463
	高島克幸 (三菱電機株式会社)	
2D1-4	Gauss のアルゴリズムを利用する RNS モンゴメリ乗算に対する電力解析	469
	小池正修 (横浜国立大学) 松本勉 (横浜国立大学)	
2E1	公開鍵暗号 -1	1月26日 9:00 ~ 10:40
2E1-1	キメラ暗号	475
	花岡 悟一郎 (東京大学) 張 銳 (東京大学) Nuttapon Attrapadung (東京大学) 今井 秀樹 (東京大学)	
2E1-2	Cramer-Shoup の構成法による平方剰余問題と関連する暗号方式	481
	樋渡玄良 (東京工業大学) 田中圭介 (東京工業大学)	
2E1-3	Piece In Hand Concept for Enhancing the Security of Multivariate Type Public Key Cryptosystems: Public Key Without Containing All the Information of Secret Key	487
	Shigeo Tsujii (Institute of Information Security) Kohtaro Tadaki (Chuo University) Ryou Fujita (Tokyo University of Science)	
2E1-4	A Construction of Public-Key Cryptosystem Using Algebraic Coding on the Basis of Superimposition and Randomness	493
	Masao Kasahara (Osaka Gakuin University)	
2E1-5	A New Principle for Construction of Public-Key Cryptosystems and the Several New Classes of Public-Key Cryptosystems	499
	笠原正雄 (大阪学院大学)	
2F1	量子セキュリティ -1	1月26日 9:00 ~ 10:40
2F1-1	量子論的に実装されたノイズィチャンネルへの簡単な能動的攻撃についての考察	505
	今福健太郎 (東大生研) 今井秀樹 (東大生研)	
2F1-2	大規模ネットワーク向け量子暗号網の考察	511
	西岡 毅 (三菱電機株式会社) 長谷川 俊夫 (三菱電機株式会社) 鶴丸 豊広 (三菱電機株式会社) 石塚 裕一 (三菱電機株式会社)	
2F1-3	既設光ファイバ 96km での量子暗号通信システム実験	517
	長谷川俊夫 (三菱電機株式会社情報技術総合研究所) 西岡毅 (三菱電機株式会社情報技術総合研究所) 石塚裕一 (三菱電機株式会社情報技術総合研究所) 安部淳一 (三菱電機株式会社情報技術総合研究所) 清水克弘 (三菱電機株式会社情報技術総合研究所) 松井充 (三菱電機株式会社情報技術総合研究所)	
2F1-4	量子鍵配送方式の安全性について	523
	渡辺 曜大 (国立情報学研究所)	
2F1-5	量子暗号伝送の長距離 / 高速化	529
	富田章久 (日本電気 (株)) 南部芳弘 (日本電気 (株)) 田島章雄 (日本電気 (株))	
2A2	バイオメトリクス -2	1月26日 10:55 ~ 12:35
2A2-1	バイオメトリクス個人認証テンプレート保護技術の考察	535
	鷲見和彦 (京都大学) 松山隆司 (京都大学) 中島晴久 (社団法人日本自動認識システム協会)	
2A2-2	個別安全性を保障できる指紋の精度評価	541

	門田啓 (NEC メディア情報研究所) 黄磊 (NEC メディア情報研究所) 吉本誠司 (NEC メディア情報研究所)	
2A2-3	Fuzzy Biometric Vault Scheme によるテンプレートの安全性に関する一考察	547
	大木哲史 (早稲田大学) 田島賢 (早稲田大学) 赤塚志郎 (早稲田大学) 小松尚久 (早稲田大学) 笠原正雄 (大阪学院大学)	
2A2-4	携帯機器に搭載された指紋照合装置は人工指を受け入れるか	553
	田辺壮宏 (横浜国立大学) 森下朋樹 (横浜国立大学) 松本勉 (横浜国立大学)	
2B2	ハッシュ関数	1月26日 10:55 ~ 12:35
2B2-1	A Note on Security of Double-Block-Length Hash Functions	559
	Shoichi Hirose (Kyoto University) Mitsuhiro Hattori (Kyoto University)	
2B2-2	A 2/3-rate double length compression function	565
	Mridul NANDI (ISI, INDIA) Wonil LEE (Kyushu University, JAPAN) Kouichi SAKURAI (Kyushu University, JAPAN) Sangjin LEE (CIST, Korea University, KOREA)	
2B2-3	An Implementation of the Biham-Chen Attack on SHA-0	571
	服部 充洋 (京都大学) 廣瀬 勝一 (京都大学) 吉田 進 (京都大学)	
2C2	コンテンツセキュリティ -2	1月26日 10:55 ~ 12:35
2C2-1	電子文書墨塗り技術の画像ファイルへの適用に関する一考察	577
	秦野康生 ((株) 日立製作所 システム開発研究所) 宮崎邦彦 ((株) 日立製作所 システム開発研究所)	
2C2-2	落し戸付き一方向性置換を用いたSD法の一考察	583
	奥秋清次 (職業能力開発総合大学校東京校) 太田和夫 (電気通信大学) 國廣昇 (電気通信大学)	
2C2-3	Tokenを用いた放送サービスの拡張	589
	小川一人 (日本放送協会) 花岡悟一郎 (東京大学) 今井秀樹 (東京大学)	
2C2-4	DAGにおける鍵派生方式の枝切り改良方式	595
	須賀祐治 (キヤノン株式会社) 岩村 恵市 (キヤノン株式会社)	
2D2	サイドチャネル攻撃 -2	1月26日 10:55 ~ 12:35
2D2-1	DPA on Hybrid XTR Single Exponentiation	601
	Dong-Guk Han (Center for Information Security Technologies) Dongjin Yang (Center for Information Security Technologies) Jongin Lim (Center for Information Security Technologies) Kouichi Sakurai (Kyushu University)	
2D2-2	A5/1 に対するサイドチャネル攻撃	607
	一色 寿幸 (NEC) 辻原 悦子 (株式会社ワイ・デー・ケー) 峯松 一彦 (NEC) 角尾 幸保 (NEC)	
2D2-3	暗号回路の耐タンパー性評価手法の構築	613
	佐々木明彦 (電気通信大学) 阿部公輝 (電気通信大学) 太田和夫 (電気通信大学)	
2D2-4	TOYOCRYPT への故障利用攻撃	619
	内藤祐介 (電気通信大学) 指田 岳彦 (電気通信大学) 根岸 大宙 (電気通信大学) 太田和夫 (電気通信大学) 國廣昇 (電気通信大学)	
2E2	署名の安全性	1月26日 10:55 ~ 12:35
2E2-1	Chaum の Undeniable signature の安全性評価	625
	尾形わかは (東京工業大学) 黒澤馨 (茨城大学) ヘン スィー フィー (マルチメディア大学)	
2E2-2	共通法を用いた RSA 型多重署名方式の安全性に関する再考察	631
	河内恵 (千葉大学) 多田充 (千葉大学)	
2E2-3	Concrete Argument on the Optimal Security Proof for PFDH	637
	SANTOSO BAGUS (電気通信大学) 太田和夫 (電気通信大学)	
2E2-4	Universally Composable 1-out-of-n 署名に関する一考察	643
	花谷 嘉一 (電気通信大学) 米山一樹 (電気通信大学) サントソ バグス (電気通信大学) 太田 和夫 (電気通信大学)	
2E2-5	An Extension of UC Digital Signature to sUF-ACMA	649
	米山 一樹 (電気通信大学) サントソ バグス (電気通信大学) 太田 和夫 (電気通信大学)	

2F2	量子セキュリティ-2	1月26日 10:55 ~ 12:35	
2F2-1	4状態を用いた量子鍵配送プロトコルの光子数分割攻撃に対する安全性について	655	
	江口誠(東京大学) 萩原学(東京大学) 今井秀樹(東京大学)		
2F2-2	B B 8 4 プロトコルの量子通信路雑音に対するC S S型の原始 BCH 符号構成	661	
	萩原学(東京大学) 今井秀樹(東京大学)		
2F2-3	量子暗号通信のための単一光子発生器開発	667	
	臼杵 達哉((株)富士通研究所) 佐久間 芳樹(独)物質・材料研究機構) 廣瀬 真一((株)富士通研究所)		
	竹本 一矢((株)富士通研究所) 横山 直樹((株)富士通研究所) 宮澤 俊之(東京大学) 高津 求(東京大学)		
	荒川 泰彦(東京大学)		
2F2-4	Threshold quantum cryptography	673	
	Yuuki Tokunaga (NTT Information Sharing Platform Laboratories) Tatsuaki Okamoto (NTT Information Sharing Platform Laboratories) Nobuyuki Imoto (Osaka University)		
2F2-5	Computational Indistinguishability between Quantaum States and Its Applications	679	
	河内 亮周(東京工業大学) 小柴 健史(富士通研究所) 西村 治道(今井量子計算機構プロジェクト) 山上 智幸(Trent University)		
2A3	バイオメトリクス招待講演	1月26日 14:20 ~ 17:10	
2A3-1	Palmprint Authentication		招待講演
	David Zang 氏(The Hongkong Polytechnic University)		
2A3-2	Recent Progress in Fingerprint Authentication		招待講演
	Nalini K. Ratha 氏(IBM Thomas J. Watson Research Center)		
2A3-3	Biometrics and Privacy		招待講演
	Marek-Rejman Greene 氏(BT Exact, Security Technologies)		
2B3	ネットワークセキュリティ	1月26日 14:10 ~ 15:50	
2B3-1	アドホックネットワークにおけるトラフィック解析を利用した利己的なノードの検出法	685	
	太田 英憲(三菱電機) 伊藤 隆(三菱電機) 米田 健(三菱電機)		
2B3-2	セキュアオーバーレイネットワーク構築のための段階的アプローチ	691	
	門林 雄基(情報通信研究機構 / 奈良先端大) 中尾 康二(情報通信研究機構 / KDI) 滝澤 修(情報通信研究機構)		
2B3-3	Proposal of Secure Routing Protocol for Distributed Sensor Networks	697	
	So Young Park (Gwangju Institute of Science and Technology) Hyung Chan Kim (Gwangju Institute of Science and Technology) R. S. Ramakrishna (Gwangju Institute of Science and Technology) Kouichi Sakurai (Kyushu University)		
2B3-4	IPv6 ネットワークにおけるセキュリティの一検討	703	
	村瀬 一郎(株式会社三菱総合研究所) 牧野京子(株式会社三菱総合研究所) 村野正泰(株式会社三菱総合研究所) 三宅 喬(倉敷芸術科学大学) 小林和真(倉敷芸術科学大学)		
2B3-5	CCS2004 併設ワークショップの参加報告	709	
	鐘講平(九州大学) 堀良彰(九州大学) 櫻井幸一(九州大学)		
2C3	電子透かし-1	1月26日 14:10 ~ 15:50	
2C3-1	印刷画像に対する電子透かし方式	715	
	江島將高(松下電器産業株式会社) 井上尚(松下電器産業株式会社) 乗富賢一(松下電器産業株式会社)		
	吉田裕之(松下電器産業株式会社)		
2C3-2	代数幾何符号の画像への組み込みと電子透かしへの応用	721	
	古藤 かおり(お茶の水女子大学) 金子 晃(お茶の水女子大学) 清水 英子(お茶の水女子大学)		
2C3-3	電子透かしの最良安全度について	727	
	伴野 幸造(東北大学) 折原 慎吾(NTT 情報流通プラットフォーム研究所) 水木 敬明(東北大学) 西関 隆夫(東北大学)		
2C3-4	GPS を用いた電子透かしシステムの改良について	733	
	国狭亜輝臣(三洋電機) ファングウィルソン(三洋電機)		
2C3-5	多重解像度表現を用いたフラクタル符号化に基づく電子透かし	739	
	米倉和也(北九州市立大学) 佐藤敬(北九州市立大学)		

2D3	PKI	1月26日 14:10 ~ 15:50	
2D3-1	プライバシーを考慮したオンライン証明書状態プロトコルの事前応答生成方式	745	
	古賀 聡 (九州大学) 櫻井 幸一 (九州大学)		
2D3-2	署名時刻偽装を不可能とする署名方式の提案	751	
	穂積俊充 (筑波大学) 猪俣敦夫 (独立行政法人科学技術振興機構) 岡本栄司 (筑波大学)		
2D3-3	証明書利用情報を用いたユーザ証明書自動選択方式の提案	757	
	米田 健 (三菱電機) 松田 規 (三菱電機)		
2D3-4	端末環境に応じて利用者権限を制限するアクセス制御法の提案	763	
	半田富己男 (大日本印刷 (株) ビジネスフォーム事業部)		
2E3	楕円曲線暗号-1	1月26日 14:10 ~ 15:50	
2E3-1	CM法と3乗剰余, 非剰余の関係	769	
	野上保之 (岡山大学) 森川良孝 (岡山大学)		
2E3-2	On Security of Superelliptic Curves Based Cryptosystems against GHS Weil Descent Attacks	775	
	小田崇博 (中央大学) 飯島努 (中央大学) 志村真帆呂 (中央大学) 趙晋輝 (中央大学) 辻井重男 (中央大学)		
2E3-3	楕円曲線暗号に対する quadratic twist 攻撃	781	
	川添充 (大阪府立大学) 森達哉 (大阪府立大学) 高橋哲也 (大阪府立大学)		
2E3-4	有限体上の楕円曲線の次数2の Weil restrictions	787	
	百瀬文之 (中央大学) 趙晋輝 (中央大学) 志村真帆呂 (中央大学)		
2E3-5	Pairing に適した楕円曲線のパラメータ生成	793	
	山本暖 (東京工業大学) 小林鉄太郎 (NTT 情報流通プラットフォーム研究所) 内山成憲 (NTT 情報流通プラットフォーム研究所)		
2F3	暗号基礎理論・対話証明	1月26日 14:10 ~ 15:50	
2F3-1	A Model and Methods for Moderately-Hard Functions (Extended Abstract)	799	
	小野寺貴男 (東京工業大学) 田中圭介 (東京工業大学)		
2F3-2	A Note on the Complexity of Arthur-Merlin Games	805	
	羽田知史 (日本アイビーエム)		
2F3-3	限定コンカレントゼロ知識のラウンド数の改良	811	
	村谷博文 (東芝)		
2F3-4	量子弱一方向性置換の万能検査	817	
	河内亮周 (東京工業大学) 小林弘忠 (科学技術振興機構) 小柴健史 (富士通研究所) Rudy Raymond Harry Putra (京都大学)		
2F3-5	超選択則による弱いコイン投げについての考察	823	
	鶴丸豊広 (三菱電機 (株) 情報技術総合研究所) 今福健太郎 (東京大学) 今井秀樹 (東京大学)		
2B4	セキュリティポリシ・ユビキタス	1月26日 16:05 ~ 17:45	
2B4-1	わが国における暗号モジュール評価制度について	829	
	山岸篤弘 (独立行政法人情報処理推進機構セキュリティセンター暗号グループ) 網島和博 (独立行政法人情報処理推進機構セキュリティセンター暗号グループ) 近藤潤一 (独立行政法人情報処理推進機構セキュリティセンター暗号グループ) 大熊健司 (独立行政法人情報処理推進機構セキュリティセンター暗号グループ) 西原正人 (独立行政法人情報処理推進機構セキュリティセンター暗号グループ)		
2B4-2	トレーサビリティにおけるポリシー運用フレームワーク	835	
	渡邊 裕治 (日本 IBM) 吉澤 武朗 (日本 IBM) 百合山 まどか (日本 IBM) 小金山 美賀 (日本 IBM) 伊藤 貴之 (日本 IBM) 沼尾 雅之 (日本 IBM) ロブソン クリスティーン (日本 IBM)		
2B4-3	位置検証(1): 中継攻撃に耐性を有する位置検証方式	841	
	安齋 潤 (横浜国立大学/パナソニック MSE(株)) 松本勉 (横浜国立大学)		
2B4-4	位置検証(2): 複数証明者を検証可能な位置検証方式	847	
	安齋 潤 (横浜国立大学/パナソニック MSE(株)) 松本勉 (横浜国立大学)		
2C4	電子透かし-2	1月26日 16:05 ~ 17:45	

2C4-1	Rotation, Scaling, and Translation-Invariant Multi-bit Watermarking Based on Log-Polar Mapping and Discrete Fourier Transform	853
	ファングウィルソン (三洋電機 (株)) 国狭亜輝臣 (三洋電機 (株))	
2C4-2	A scale-space Reeb-graph of topological invariants of images and its applications to copyright protection	859
	鈴木 慎太郎 (中央大学) 工藤健太郎 (中央大学) 趙晋輝 (中央大学)	
2C4-3	フレーム間の類似性を利用した動画像用相関型電子透かしの時系列攻撃への対処法	865
	山本基夫 (大阪府立大学) 岩田基 (大阪府立大学) 荻原昭夫 (大阪府立大学) 汐崎陽 (大阪府立大学)	
2C4-4	時間軸方向の周波数成分を用いた動画像用電子透かし	871
	小林洋士 (大阪府立大学) 岩田基 (大阪府立大学) 荻原昭夫 (大阪府立大学) 汐崎陽 (大阪府立大学)	
2C4-5	独立成分分析を利用した多値ロゴマーク用の電子透かし	877
	中野 達也 (大阪府立大学) 岩田 基 (大阪府立大学) 荻原 昭夫 (大阪府立大学) 汐崎 陽 (大阪府立大学)	
2D4	電子投票	1月26日 16:05 ~ 17:45
2D4-1	汎用的結合可能な電子投票方式について	883
	土居誠司 (京都大学) 真鍋義文 (NTT サイバースペース研究所 / 京都大学) 岡本龍明 (NTT 情報通信プラットフォーム研究所 / 京都大学)	
2D4-2	携帯電話による投票所電子入場券とセキュリティ	889
	金宰郁 (日本工業大学) 小林哲二 (日本工業大学) 町田則文 (日本工業大学)	
2D4-3	準同型性と MIX-net に基づいた電子投票方式の評価	895
	小山拓郎 (東京工業大学) 石田夏樹 (日立ソフトウェアエンジニアリング株式会社) 尾形わかは (東京工業大学)	
2D4-4	カメラ付き携帯電話を利用した電子投票システムの実装	901
	桂川 健一 (東京電機大学) 本杉 洋 (東京電機大学) 佐々木 良一 (東京電機大学)	
2D4-5	Security and Privacy in E-voting and RFID System Based on Universal Re-encryption Mix-net	907
	許容碩 (九州大学) 齊藤純一郎 (九州大学) 今本健二 (九州大学) 櫻井幸一 (九州大学)	
2E4	超楕円曲線暗号	1月26日 16:05 ~ 17:45
2E4-1	Improvement of Thériault Algorithm of Index Calculus for Jacobian of Hyperelliptic Curves of Small Genus	913
	長尾孝一 (関東学院大学)	
2E4-2	Tate Pairing の効率的な計算について	919
	高橋昌史 ((株) 日立製作所 システム開発研究所)	
2E4-3	A Construction of an Algebraic Surface Public-key Cryptosystem	925
	Koichiro AKIYAMA (TOSHIBA Corp. Corporate R&D Center Computer & Network Laboratory) Yasuhiro GOTO (Department of Mathematics, Hokkaido University of Education at Hakodate)	
2E4-4	Tate Pairing on $y^2 = x^5 - x$ in Characteristic Five	931
	Ryuichi Harasawa (Nagasaki University) Yutaka Sueyoshi (Nagasaki University) Aichi Kudo (Nagasaki University)	
2E4-5	三浦予想について	937
	鈴木讓 (大阪大学)	
2F4	格子問題	1月26日 16:05 ~ 17:45
2F4-1	転写攻撃に対する NTRUSign の改良について	943
	長谷川 真吾 (東北大学) 磯辺 秀司 (東北大学) 満保 雅浩 (筑波大学) 静谷 啓樹 (東北大学) 布田 裕一 (松下電器産業) 大森 基司 (松下電器産業)	
2F4-2	プリコーディングを用いた高密度 MH 型ナップザック暗号の提案	949
	名迫 健 (大阪電気通信大学) 横山 晃子 (大阪電気通信大学) 村上 恭通 (大阪電気通信大学)	
2F4-3	ガウス整数環上のナップザック暗号の鍵生成法について	955
	坂本寿 (金沢工業大学) 林彬 (金沢工業大学)	
2F4-4	A New NP-Complete Problem Associated with Lattice	961

	Shunichi HAYASHI (Graduate School of Science and Technology, Chiba University) Mitsuru TADA (Institute of Media and Information Technology, Chiba University)	
2F4-5	最小ベクトルの係数の存在範囲に関する考察	967
	金山 直樹 (電気通信大学) 木田 雅成 (電気通信大学) 太田 和夫 (電気通信大学) 國廣 昇 (電気通信大学)	
3A1	バイオメトリクス-3	1月27日 9:00 ~ 10:40
3A1-1	テキスト提示型話者認識のための唇動作個人認証方式	973
	市野将嗣 (早稲田大学) 坂野鋭 ((株)NTT データ) 小松尚久 (早稲田大学)	
3A1-2	生体反射型認証: 盲点位置とサッカーボール反応時間を利用した認証方式	979
	荒井 大輔 (静岡大学) 西垣 正勝 (静岡大学)	
3A1-3	特徴点の3次元情報を利用した顔認証システムの研究	985
	佐藤康之 (成蹊大学) 井辺昭人 (早稲田大学) 前島謙宣 (早稲田大学) 森島繁生 (早稲田大学)	
3A1-4	リアルタイムビデオセキュリティ	991
	黄興華 (東京大学) 松浦幹太 (東京大学)	
3A1-5	ユビキタスネットワーク社会における顔認証	997
	井尻善久 (オムロン株式会社 センシング研究所) 櫻木美春 (オムロン株式会社 センシング研究所) 細井 聖 (オムロン株式会社 センシング研究所) 川出雅人 (オムロン株式会社 センシング研究所)	
3B1	Web セキュリティ-1	1月27日 9:00 ~ 10:40
3B1-1	木構造を用いたXMLアクセス制御モデル	1003
	工藤道治 (日本アイ・ピー・エム東京基礎研究所) 戚 乃箴 (日本アイ・ピー・エム東京基礎研究所)	
3B1-2	制御効果値を用いたXMLアクセス判定方法	1009
	戚乃箴 (日本IBM東京基礎研究所)	
3B1-3	OSGi上のセキュアなWebサービスの構築	1015
	寺口 正義 (日本アイ・ピー・エム(株)東京基礎研究所) 山口 裕美 (日本アイ・ピー・エム(株)東京基礎研究所) 伊藤 貴之 (日本アイ・ピー・エム(株)東京基礎研究所)	
3B1-4	セマンティックWebシステムに於ける"Community Based Access Control Model"の適用に関する一考察	1021
	森住哲也 (東洋通信機株式会社) 牛頭靖幸 (神奈川大学) 酒井剛典 (神奈川大学) 畔上昭司 (神奈川大学) 稲積泰宏 (神奈川大学) 木下宏揚 (神奈川大学)	
3B1-5	Webアプリケーションシステムに適したセキュリティモデル"Community Based Access Control Model"の提案	1027
	酒井剛典 (神奈川大学) 森住哲也 (東洋通信機株式会社) 牛頭靖幸 (神奈川大学) 畔上昭司 (神奈川大学) 稲積泰宏 (神奈川大学) 木下宏揚 (神奈川大学)	
3C1	電子透かし-3	1月27日 9:00 ~ 10:40
3C1-1	動画像用相関型電子透かしの誤検出確率を保証可能とするフレーム間類似度の評価	1033
	藤田 高彬 (大阪大学) 岡本 邦宏 (大阪大学) 吉田 真紀 (大阪大学) 藤原 融 (大阪大学)	
3C1-2	不完全暗号系による電子透かし	1039
	岩切 宗利 (防衛大学) タミン タイン (防衛大学)	
3C1-3	電子透かし技術の研究動向	1045
	上繁義史 ((財)九州システム情報技術研究所) 櫻井幸一 ((財)九州システム情報技術研究所)	
3C1-4	H.323 ネットミーティング画像を利用する透かし	1051
	角田貢 (東京工業大学) 森田栄治 (東京工業大学)	
3C1-5	スペクトル拡散技術を用いた電子透かし	1057
	實松豊 (九州大学) 香田徹 (九州大学)	
3D1	鍵共有-1	1月27日 9:00 ~ 10:40
3D1-1	Efficient RSA-based Authenticated Key Exchange with Leakage-Resilience and Perfect Forward Secrecy	1063
	SeongHan SHIN (The University of Tokyo) Kazukuni KOBARA (The University of Tokyo) Hideki IMAI (The University of Tokyo)	

3D1-2	安全な P2P グルーピング方式の提案とその実装	1069
	古志智也 (東京工科大学) 齋藤孝道 (東京工科大学)	
3D1-3	Diffie-Hellman の依頼計算プロトコル	1075
	大石和臣 (キヤノン株式会社)	
3D1-4	An ID-based Non-Interactive Tripartite Key Agreement Protocol with k-Resilience	1081
	Raylin TSO (University of Tsukuba) Takesi OKAMOTO (University of Tsukuba) Tsuyoshi TAKAGI (Darmstadt University of Technology (Germany)) Eiji OKAMOTO (University of Tsukuba)	
3D1-5	認証付き鍵交換プロトコルにおける non-malleability に基づく安全性	1087
	羽田大樹 (東京工業大学) 田中圭介 (東京工業大学)	
3E1	公開鍵暗号計算手法	1月27日 9:00 ~ 10:40
3E1-1	Some Improved Algorithms for Hyperelliptic Curve Cryptosystems using Degenerate Divisors	1093
	Masanobu Katagi (Sony Corporation) Toru Akishita (Sony Corporation) Izuru Kitamura (Sony Corporation) Tsuyoshi Takagi (Technische Universitaet Darmstadt)	
3E1-2	楕円曲線上の離散対数アルゴリズム	1099
	米川智 (山形大学) 小林邦勝 (山形大学)	
3E1-3	A Complete Point Halving Algorithm for Hyperelliptic Curve Cryptosystems	1105
	北村出 (ソニー (株)) 堅木雅宣 (ソニー (株)) 高木剛 (ダルムシュタット工科大)	
3E1-4	Aryabhata Remainder Theorem: Relevance to public-key crypto-algorithms	1111
	T.R.N. Rao (University of Louisiana at Lafayette) 楊中皇 (国立高雄師範大学)	
3E1-5	モンゴメリのトリックに基づく 2^k 倍点の改良計算法	1117
	安達大亮 (名古屋大学) 平田富夫 (名古屋大学)	
3F1	放送用暗号・グループ署名	1月27日 9:00 ~ 10:40
3F1-1	Hwang-Kim-Lee のブロードキャスト暗号の改良	1123
	金沢史明 (北陸先端科学技術大学院大学) 宮地充子 (北陸先端科学技術大学院大学)	
3F1-2	Short Encrypted Broadcast with Short Key	1129
	アツラパドゥンナッタボン (東京大学) 今井 秀樹 (東京大学)	
3F1-3	Key generation scheme for broadcast encryption exploiting chaotic sequences	1135
	栗林 稔 (神戸大学) 田中 初一 (神戸大学)	
3F1-4	A Verifier-Local Revocation Group Signature Scheme with Backward Unlinkability from Bi-linear Maps	1141
	中西 透 (岡山大学) 船曳 信生 (岡山大学)	
3F1-5	計算能力の低いデバイスに適したグループ署名方式	1147
	岡田 光司 (東芝ソリューション (株)) 吉田 琢也 (東芝ソリューション (株)) 加藤 岳久 (東芝ソリューション (株))	
3A2	バイオメトリクス-4	1月27日 10:55 ~ 12:35
3A2-1	手形状の抽出と面積時系列を用いた本人認証	1153
	松村 博之 (大阪府立大学) 荻原 昭夫 (大阪府立大学) 汐崎 陽 (大阪府立大学)	
3A2-2	DNA の情報構造に基づく個人情報階層的分類	1159
	田中裕 (情報セキュリティ大学院大学) 板倉征男 (情報セキュリティ大学院大学)	
3A2-3	テンプレート証明書を用いたバイオメトリクス認証プロトコルの提案とメッセージ漏洩に対する安全性	1165
	上繁義史 ((財)九州システム情報技術研究所) 櫻井幸一 ((財)九州システム情報技術研究所, 九州大学)	
3A2-4	Maximizing Election Security through the Efficient Use of Technology	1171
	ホセ・ルイス・ラクソン (東京大学) 松浦幹太 (東京大学)	
3A2-5	モバイルエージェントの安全性向上のためのバイオメトリクス認証の適用	1177
	明石正則 (日本テレコム株式会社) 岡宅泰邦 (日本テレコム株式会社) 吉岡信和 (国立情報学研究所) 大岸伸之 (東芝情報システム株式会社) 本位田真一 (国立情報学研究所)	

3B2	不正アクセス解析実験環境	1月27日 10:55 ~ 12:35
3B2-1	不正アクセス等再現実験環境の統合手法に関する研究	1183
	三輪信介 (情報通信研究機構 情報通信部門 セキュアネットワークグループ) 宮地利幸 (北陸先端科学技術大学院大学) 大野浩之 (情報通信研究機構 情報通信部門 セキュアネットワークグループ) 篠田 陽一 (北陸先端科学技術大学院大学)	
3B2-2	ウイルス分析のためのテストベッドの構築	1189
	藤長 昌彦 (KDDI) 中尾 康二 (KDDI) 森井 昌克 (徳島大学)	
3B2-3	ワームエミュレータについて	1195
	東角芳樹 (株式会社富士通研究所) 面和成 (株式会社富士通研究所) 鳥居悟 (富士通研究所)	
3B2-4	仮想ウイルス感染ネットワークの構築とその感染発症機構の開発	1201
	広岡 俊彦 (徳島大学) 妹脊 敦子 (徳島大学) 曾根 直人 (鳴門教育大学) 白石 善明 (近畿大学) 森井 昌克 (NICT, 徳島大学) 星澤 祐二 (株式会社セキュアブレイン) 中尾 康二 (NICT, KDDI株式会社)	
3B2-5	メモリに展開されたコードを使う未知ウイルス解析支援システム	1207
	神園 雅紀 (徳島大学) 市川 幸宏 (徳島大学) 白石 善明 (近畿大学) 森井 昌克 (徳島大学)	
3C2	ネットワークプロトコル	1月27日 10:55 ~ 12:35
3C2-1	属性付き匿名資格証明システムと属性投票システム	1213
	平井康雅 (株式会社 NTT データ) 松尾真一郎 (株式会社 NTT データ)	
3C2-2	A Protocol of Unlinkable Transaction for Preserving Customer Privacy	1219
	Seok-kyu Kang (Informaiton and Communications Univ.) Tomoyuki Asano (Sony Information Technologies Lab. Secure System Group) Kwnagjo Kim (Informaiton and Communications Univ.)	
3C2-3	GNUnet におけるイニシエータの匿名性保護に関する提案	1225
	鐘講平 (九州大学) 堀良彰 (九州大学) 櫻井幸一 (九州大学)	
3C2-4	モバイルエージェントを利用した、柔軟な SET 型電子商取引引きプロトコルの提案	1231
	盛 拓生 (山梨大学) 今井秀樹 (東京大学)	
3C2-5	複数環状経路を用いる匿名通信	1237
	角田勝義 (東洋大学) 伊東克能 (東洋大学)	
3D2	鍵共有 -2	1月27日 10:55 ~ 12:35
3D2-1	鍵更新情報の所要伝送量を低減するための効率的グループ鍵配送方式	1243
	西竜三 ((財)九州システム情報技術研究所) 櫻井幸一 (九州大学)	
3D2-2	内部不正者検知が可能なグループ鍵共有方式とその安全性の検討	1249
	小田 哲 (慶應義塾大学)	
3D2-3	階層化されたパスワードベースの認証つき鍵交換プロトコルの構成	1255
	太田 陽基 ((株)KDDI 研究所) 清本 晋作 ((株)KDDI 研究所) 田中 俊昭 ((株)KDDI 研究所) 太田 和夫 (電気通信大学)	
3D2-4	KEM-DEM における同報通信	1261
	安田 幹 (NTT) 小林 鉄太郎 (NTT) 青木 和麻呂 (NTT) 藤崎 英一郎 (NTT) 藤岡 淳 (NTT)	
3D2-5	Identity-Based Non-Interactive Key Sharing Equivalent to RSA Deciphering	1267
	田中 初一 (神戸大学)	
3E2	素因数分解	1月27日 10:55 ~ 12:35
3E2-1	有理側・代数側の special-Q の併用について	1273
	青木和麻呂 (NTT) 植田広樹 (NTT)	
3E2-2	一般数体篩法実装実験 (7) — 代数的数の平方根	1279
	下山武司 (富士通研究所) 木田祐司 (立教大学) 青木和麻呂 (NTT 情報流通プラットフォーム研究所)	
3E2-3	Coppersmith の方法を用いた P^rQ 型合成数の素因数分解について (2)	1285
	宮永望 (早稲田大学) 金山直樹 (電気通信大学) 小宮山雄木 (早稲田大学) 内山成憲 (NTT)	
3E2-4	床関数を用いる素因数分解アルゴリズム	1291
	藤井進 (山形大学) 小林邦勝 (山形大学)	
3E2-5	Carmichael 数についての簡単な注意	1297
	内山成憲 (NTT)	

3F2	匿名通信	1月27日 10:55 ~ 12:35
3F2-1	Sliced Onion Routing Scheme and its aptitude for Recent Networks Jin Tamura (University of Tokyo) Kazukuni Kobara (University of Tokyo) Hideki Imai (University of Tokyo)	1303
3F2-2	能動攻撃に耐性のある Valkyrie 山中晋爾 (東芝) 古原和邦 (東京大学) 今井秀樹 (東京大学)	1309
3F2-3	ElGamal 暗号と Cramer-Shoup 暗号をもとにした匿名性をもつ暗号方式 林 良太郎 (東京工業大学) 田中 圭介 (東京工業大学)	1315
3F2-4	The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity Ryotaro Hayashi (Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology) Keisuke Tanaka (Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology)	1321
3F2-5	仲裁者を伴うモデルにおける情報理論的に安全な匿名認証 黄瀬和之 (横浜国立大学) 清藤武暢 (横浜国立大学) 四方順司 (横浜国立大学) 松本勉 (横浜国立大学)	1327
3A3	脆弱性評価・監査	1月27日 14:10 ~ 15:50
3A3-1	ポータビリティ、ユーザビリティの高いセキュリティスキャナの開発 吉本道隆 (岩手県立大学) ベッド B ビスタ (岩手県立大学) 高田豊雄 (岩手県立大学)	1333
3A3-2	日本におけるソフトウェア脆弱性関連情報共有体制の構築 村野 正泰 ((株) 三菱総合研究所) 村瀬 一郎 ((株) 三菱総合研究所) 牧野 京子 ((株) 三菱総合研究所)	1339
3A3-3	C プログラムの静的なバッファオーバーフロー検出 中村 豪一 ((株) 三菱総合研究所) 牧野 京子 ((株) 三菱総合研究所) 村瀬 一郎 ((株) 三菱総合研究所)	1345
3A3-4	バッファオーバーフロー回避のためのプログラミングガイドラインの提案 牧野京子 (株式会社三菱総合研究所) 中村豪一 (株式会社三菱総合研究所) 石黒正輝 (株式会社三菱総合研究所) 村野正泰 (株式会社三菱総合研究所) 村瀬一郎 (株式会社三菱総合研究所)	1351
3A3-5	Tamper Resistant Software Through Dynamic Integrity Checking Ping Wang (Information and communications University) Seokkyu Kang (Information and communications University) Kwangjo Kim (Information and communications University)	1357
3B3	広域ネットワークセキュリティ -1	1月27日 14:10 ~ 15:50
3B3-1	動的サンプリングと情報理論的複雑度変動を利用したサービス妨害攻撃検知システムの最適化 古谷隆行 (東京大学) 松浦幹太 (東京大学)	1363
3B3-2	属性指向帰納によるネットワークログ特徴抽出方式の評価 山田明 (株式会社KDDI研究所) 三宅優 (株式会社KDDI研究所) 竹森敬祐 (株式会社KDDI研究所) 田中俊昭 (株式会社KDDI研究所) 山本明仁 (独立行政法人情報通信研究機構) 三田村好矩 (北海道大学)	1369
3B3-3	ISP のためのネットワークセキュリティ分析支援ツールの設計と実装 松本文子 (独立行政法人情報通信研究機構) 馬場俊輔 (横河電気株式会社) 井澤志充 (有限会社インターネット応用技術研究所) 中尾康二 (独立行政法人情報通信研究機構 / KDDI 株式会社)	1375
3B3-4	定点観測システム収集データを利用したインターネット空間補間手法の提案と早期異常検知への適用 田村研輔 (警察庁) 松浦幹太 (東京大学) 今井秀樹 (東京大学)	1381
3B3-5	コンピュータウイルスに対する疫学的接近の提案 佐々木良一 (東京電機大学) 関聡司 (早稲田大学) 高橋正和 (ISS) 石井真之 (東京電機大学)	1387
3C3	RFID セキュリティ -1	1月27日 14:10 ~ 15:50
3C3-1	Security and Privacy on Authentication Protocol for Low-cost RFID Jeongkyu Yang (Information and Communicatin University (ICU)) Kwangjo Kim (Information and Communicatin University (ICU))	1393
3C3-2	How to provide a solution of RFID privacy protection without recordable memory in relatively low cost 劉鼎哲 (東京大学) 古原和邦 (東京大学) 今井秀樹 (東京大学)	1399
3C3-3	R F I D プライバシー保護の一方式 1405	

	西川弘幸 (北陸日本電気ソフトウェア株式会社) 双紙正和 (北陸先端科学技術大学院大学) 宮地充子 (北陸先端科学技術大学院大学)	
3C3-4	A Prototype System of RFID Authentication Processing Framework	1411
	John Ayode (独立行政法人情報通信研究機構) 滝澤修 (独立行政法人情報通信研究機構) 中尾康二 (独立行政法人情報通信研究機構 / KDDI 株式会社)	
3C3-5	RFID タグにおける所有者変更方式の提案	1417
	齊藤純一郎 (九州大学) 今本 健二 (九州大学) 櫻井幸一 (九州大学)	
3D3	暗号解析・数論応用	1月27日 14:10 ~ 15:50
3D3-1	既知平文攻撃に対して安全な部品を組み込んだハイブリッド暗号	1423
	峯松一彦 (NEC インターネットシステム研究所) 角尾幸保 (NEC インターネットシステム研究所)	
3D3-2	AES 型の秘密鍵暗号に対する XSL の見積もり評価	1429
	樋口敬士 (電気通信大学) 國廣昇 (電気通信大学) 太田和夫 (電気通信大学)	
3D3-3	Signal Matrix Cover Problem に基づいた新たな公開鍵認証	1435
	金谷佳敬 (千葉大学) 多田充 (千葉大学)	
3D3-4	RSA 暗号鍵の Lehman 法による素因数分解の考察	1441
	沖秀一 (大日本印刷 (株) ビジネスフォーム事業部) 半田富己男 (大日本印刷 (株) ビジネスフォーム事業部)	
3E3	署名-1	1月27日 14:10 ~ 15:50
3E3-1	オブリアス署名の設計と解析	1447
	岡本健 (筑波大学) 椎名信行 (筑波大学) 岡本栄司 (筑波大学)	
3E3-2	指定検証者署名への変換が可能な Aggregate Signature	1453
	三原章裕 (東京工業大学) 田中圭介 (東京工業大学)	
3E3-3	署名生成機能の危殆化を自己検出可能なデジタル署名方式	1459
	上山真貴子 (横浜国立大学) 四方順司 (横浜国立大学) 松本勉 (横浜国立大学)	
3E3-4	離散対数問題に tight 安全でかつ計算量の少ない署名方式	1465
	寺西勇 (NEC インターネットシステム研究所)	
3E3-5	双線形写像を用いた電子文書墨塗り技術	1471
	宮崎邦彦 ((株) 日立製作所 / 東京大学) 花岡悟一郎 (東京大学) 今井秀樹 (東京大学)	
3F3	暗号プロトコル	1月27日 14:10 ~ 15:50
3F3-1	任意に譲渡制限可能な匿名電子チケットシステム	1477
	三神京子 (津田塾大学) 繁富利恵 (東京大学) 小川貴英 (津田塾大学) 今井秀樹 (東京大学)	
3F3-2	アイテムの価値が可変な状況を考慮した配達証明付き電子メール	1483
	今本健二 (九州大学) 櫻井幸一 (九州大学)	
3F3-3	検索結果の秘匿と一貫性検証を可能とするデータ検索プロトコルの提案	1489
	中山 敏 (大阪大学) 藤原 晶 (大阪大学) 吉田 真紀 (大阪大学) 藤原 融 (大阪大学)	
3F3-4	攻撃シナリオを用いた認証プロトコルの安全性検証器の実装	1495
	齋藤孝道 (東京工科大学)	
3F3-5	Security Protocols Attacks Detection Based on Bayesian Network	1501
	ALHARBY Abdulrahman (The University of Tokyo) Hideki Imai (The University of Tokyo)	
3A4	リスクマネージメント	1月27日 16:05 ~ 17:45
3A4-1	問題構造化技法による情報セキュリティ課題の把握	1507
	板倉征男 (情報セキュリティ大学院大学)	
3A4-2	多重リスクコミュニケータの開発構想と試適用 (その1)	1513
	石井真之 (東京電機大学) 日高悠 (東京電機大学) 佐々木良一 (東京電機大学)	
3A4-3	多重リスクコミュニケータの開発構想と試適用 (その2)	1519
	日高悠 (東京電機大学) 石井 真之 (東京電機大学) 佐々木 良一 (東京電機大学)	
3A4-4	公開鍵暗号危殆化時のデジタル署名付文書への影響分析	1525
	藤本肇 (東京電機大学) 上田祐輔 (東京電機大学) 佐々木良一 (東京電機大学)	

3A4-5	インターネットリスク分析モデルに関する考察	1531
	中尾 康二 (KDDI 株式会社) 丸山 裕子 (日本電気) 大河内 一弥 (日立製作所) 松本 文子 (情報通信研究機構) 守山 栄松 (情報通信研究機構) 武智 洋 (横河電機)	
3B4	広域ネットワークセキュリティ -2	1月27日 16:05 ~ 17:45
3B4-1	On Distributed Intrusion Detection System (DIDS) and Utilization of Data Fusion in DIDS	1537
	ラーマンモハammadグーラム (情報通信研究機構) 中尾 康二 (情報通信研究機構 / KDDI)	
3B4-2	キャンパスネットワークにおけるポートスキャンの現状およびその自動検出手法	1543
	小原正芳 (九州大学) 堀良彰 (九州大学) 櫻井幸一 (九州大学)	
3B4-3	IP トレースバックシステムの相互接続アーキテクチャの提案	1549
	大江将史 (国立天文台) 樫山寛晃 (奈良先端科学技術大学院大学) 門林雄基 (奈良先端科学技術大学院大学)	
3B4-4	Bloom フィルタを用いたパケットマーキング法による IP トレースバックの擬陽性確率について	1555
	細井琢朗 (東京大学) 松浦幹太 (東京大学) 今井秀樹 (東京大学)	
3B4-5	脆弱性と攻撃ツールに関する傾向と考察	1561
	横地 裕 (横河電機株式会社) 国峰 泰裕 (横河電機株式会社)	
3C4	RFID セキュリティ -2	1月27日 16:05 ~ 17:45
3C4-1	リンク不能性を実現し大規模 RFID システムに適用可能な ID 照合プロトコル	1567
	野原康伸 (九州大学) 井上創造 (九州大学) 馬場謙介 (九州大学) 安浦寛人 (九州大学)	
3C4-2	RFID システムの完全性保証	1573
	中村めぐみ (日本アイ・ピー・エム株式会社) 吉濱佐知子 (日本アイ・ピー・エム株式会社) 宗藤誠治 (日本アイ・ピー・エム株式会社)	
3C4-3	順序履歴検証方式	1579
	大久保美也子 (NTT) 鈴木幸太郎 (NTT) 木下 真吾 (NTT) 森田 光 (NTT) 金井 敦 (NTT)	
3C4-4	RFID トレーサビリティのための所有権移転可能な所有者認証方法	1585
	沼尾雅之 (日本アイ・ピー・エム (株)) 渡邊裕治 (日本アイ・ピー・エム (株))	
3C4-5	ディスプレイからの視覚的情報漏洩防止システムの開発と評価	1591
	竹内啓 (東京電機大学) 佐々木良一 (東京電機大学)	
3D4	楕円曲線暗号 -2	1月27日 16:05 ~ 17:45
3D4-1	放送用暗号の実現法	1597
	境隆一 (大阪電気通信大学) 笠原正雄 (大阪学院大学)	
3D4-2	匿名著作権署名	1603
	岡崎 裕之 (京都工芸繊維大学) 境 隆一 (大阪電気通信大学) 柴山 潔 (京都工芸繊維大学) 笠原 正雄 (大阪学院大学)	
3D4-3	Pairing を用いた Revocable DDH とその応用	1609
	星野 文学 (日本電信電話株式会社) 鈴木 幸太郎 (日本電信電話株式会社) 小林 鉄太郎 (日本電信電話株式会社)	
3D4-4	楕円曲線暗号のための剰余算に対するサイドチャネル解析	1615
	酒井 康行 (三菱電機株式会社) 櫻井 幸一 (九州大学)	
3E4	署名 -2	1月27日 16:05 ~ 17:45
3E4-1	A New Provably Secure Transitive Signature Scheme	1621
	Dang Nguyen Duc (Information and Communications Univ.) Zeen Kim (Information and Communications Univ.) Kwangjo Kim (Information and Communications Univ.)	
3E4-2	Time-Evolving 署名方式の改良法	1627
	ズオングカンベト (情報通信研究機構) 黒澤馨 (茨城大学) 尾形わかは (東京工業大学)	
3E4-3	ドキュメントに対する視覚的検証可能署名の提案	1633
	松本勉 (横浜国立大学) 吉岡克成 (横浜国立大学) 李斌 (横浜国立大学)	
3E4-4	Just t-out-of-n Signature	1639

	藤崎英一郎 (NTT 情報流通プラットフォーム研究所) 鈴木幸太郎 (NTT 情報流通プラットフォーム研究所)	
3E4-5	木署名	1645
	菊池浩明 (東海大)	
3F4	ソフトウェア実装	1月27日 16:05 ~ 17:45
3F4-1	SIMD 命令を用いた Hessian-form 楕円曲線暗号の効率的な実装	1651
	熊谷 正康 (NTT アドバンステクノロジー株式会社)	
3F4-2	PentiumIII, 4 における共通鍵暗号のソフトウェア実装性能解析 (I)	1657
	福田明香 (三菱電機株式会社) 松井充 (三菱電機株式会社)	
3F4-3	PentiumIII, 4 における共通鍵暗号のソフトウェア実装性能解析 (II)	1663
	松井充 (三菱電機株式会社) 福田明香 (三菱電機株式会社)	
3F4-4	Java 仮想マシン上の高速な多倍長演算の実装手法について	1669
	細島崇 (東京電機大学) 齊藤泰一 (東京電機大学)	
3F4-5	ペアリング高速実装	1675
	小林鉄太郎 (NTT) 青木和麻呂 (NTT) 今井秀樹 (東大)	
4A1	コンテンツ保護	1月28日 9:00 ~ 10:40
4A1-1	電子透かし検出に適した誤り訂正符号の拡張方式	1681
	藤井康広 (日立製作所) 越前功 (日立製作所) 山田隆亮 (日立製作所) 手塚悟 (日立製作所) 吉浦裕 (電気通信大学)	
4A1-2	改行位置の調整によるドキュメントへの情報ハイディングに対する主観評価に関する検討	1687
	滝澤修 (独立行政法人情報通信研究機構) 牧野京子 (株式会社三菱総合研究所) 村野正泰 (株式会社三菱総合研究所) 井上信吾 (株式会社三菱総合研究所) 赤井健一郎 (株式会社三菱総合研究所) 村瀬一郎 (株式会社三菱総合研究所) 鈴木雅貴 (横浜国立大学) 吉岡克成 (横浜国立大学) 松本勉 (横浜国立大学) 中川裕志 (東京大学)	
4A1-3	Tardos 符号の改良	1693
	磯谷 泰知 (東芝) 村谷 博文 (東芝)	
4A1-4	特定のユビキタス環境における共通のコンテキストを用いた暗号化通信	1699
	庄司和宏 (岩手県立大学) 王家宏 (岩手県立大学) 高田豊雄 (岩手県立大学)	
4A1-5	サービスの柔軟な利用と個人情報の保護を実現するエージェントベースフレームワーク	1705
	高橋健一 ((財)九州システム情報技術研究所) 雨宮聡史 (九州大学) 櫻井幸一 ((財)九州システム情報技術研究所) 雨宮真人 (九州大学)	
4B1	エンドポイントセキュリティ -1	1月28日 9:00 ~ 10:40
4B1-1	IPSec を用いたリモートアクセスユーザの動的なネットワークアクセス制御に関する検討	1711
	吉井英樹 (日本テレコム株式会社) 村上誠 (日本テレコム株式会社) 芦萱吉喜 (日本テレコム株式会社)	
4B1-2	モバイルエージェントによるエンドホスト情報収集管理方式の提案	1717
	小手川 祐樹 (九州大学) 田端 利宏 (九州大学) 堀 良彰 (九州大学) 櫻井 幸一 (九州大学)	
4B1-3	ワーム検知隔離と連携したエンドポイントセキュリティシステムの試作	1723
	武仲正彦 (株式会社富士通研究所) 面和成 (株式会社富士通研究所) 東角芳樹 (株式会社富士通研究所) 鳥居悟 (株式会社富士通研究所)	
4B1-4	モバイルエージェントに基づく非共有型広域ログ解析	1729
	葛野弘樹 (岩手県立大学) 川原卓也 (岩手県立大学) 渡邊集 (岩手県立大学) 中井優志 (岩手県立大学) 加藤貴司 (岩手県立大学) Bhed Bahadur Bista (岩手県立大学) 高田豊雄 (岩手県立大学)	
4B1-5	送受信データ間の相関に基づく未知ウイルス検知方法の提案	1735
	杉村 友幸 (静岡大学) 鈴木 功一 (静岡大学) 馬場 達也 (NTT データ) 前田 秀介 (NTT データ) 西垣正勝 (静岡大学)	
4C1	擬似乱数生成	1月28日 9:00 ~ 10:40
4C1-1	k 誤り線形複雑度の計算法と履歴に関する考察	1741
	戒田 高康 (八代工業高等専門学校)	

4C1-2	Multidimensional i.i.d. Binary Random Vectors Generated by Jacobian Elliptic Rational Map	1747
	加藤彩 (九州大学) 小野明香 (九州大学) 香田徹 (九州大学)	
4C1-3	ロジスティック写像による擬似乱数の安全性について	1753
	宮崎武 (北九州市立大学) 荒木俊輔 (九州工業大学) 上原聡 (北九州市立大学) 今村恭己 (九州工業大学)	
4C1-4	耐タンパー機能を有しない携帯電話アプリケーション環境におけるID情報保護方式	1759
	飯野徹 ((株) NTTデータ 技術開発本部) 中村智久 ((株) NTTデータ 技術開発本部) 本城啓史 ((株) NTTデータ 技術開発本部) 箱守聰 ((株) NTTデータ 技術開発本部)	
4C1-5	カオス型関数による擬似乱数の検定と暗号システムへの応用	1765
	川本俊治 (大阪府立大学) 外山淳一郎 (大阪府立大学)	
4D1	リング署名	1月28日 9:00 ~ 10:40
4D1-1	t-ビットドメインで定義されたリング署名方式の安全性評価に関する考察	1771
	星野隼人 (千葉大学) 中村勝洋 (千葉大学)	
4D1-2	指名確認者リング署名	1777
	多田美奈子 (東芝ソリューション (株)) 岡田光司 (東芝ソリューション (株))	
4D1-3	署名者同一性検証可能な 1-out-of-n 署名方式の改良	1783
	高橋 淳也 (中央大学) 土井 洋 (情報セキュリティ大学院大学) 辻井 重男 (情報セキュリティ大学院大学)	
4D1-4	否認機能を持つリング署名方式の再考	1789
	駒野 雄一 ((株) 東芝 研究開発センター) 太田 和夫 (電気通信大学) 新保 淳 ((株) 東芝 研究開発センター) 川村 信一 ((株) 東芝 研究開発センター)	
4E1	サイドチャネル攻撃-3	1月28日 9:00 ~ 10:40
4E1-1	SBOX の特性を利用した DPA 評価手法	1795
	三宅 秀享 (株式会社 東芝) 野崎 華恵 (株式会社 東芝) 清水 秀夫 (株式会社 東芝) 新保 淳 (株式会社 東芝)	
4E1-2	CMOS 論理回路の電力解析モデル	1801
	佐伯 稔 (三菱電機 (株)) 鈴木 大輔 (三菱電機 (株)) 市川 哲也 (三菱電機エンジニアリング (株))	
4E1-3	FPGA を用いた電力解析モデルの検証	1807
	市川 哲也 (三菱電機エンジニアリング (株)) 鈴木 大輔 (三菱電機 (株)) 佐伯 稔 (三菱電機 (株))	
4E1-4	RSL の安全性評価とハイブリット DPA に対する改良	1813
	鈴木 大輔 (三菱電機 (株)) 佐伯 稔 (三菱電機 (株)) 市川 哲也 (三菱電機エンジニアリング (株))	
4E1-5	SEED に対するキャッシュ攻撃	1819
	池田 尚隆 (東京理科大学) 市川 武宜 (東京理科大学) 金子 敏信 (東京理科大学)	
4F1	公開鍵暗号-2	1月28日 9:00 ~ 10:40
4F1-1	E l G a m a l 暗号を用いたマルチパーティーによる秘匿回路計算	1825
	千田浩司 (日本電信電話株式会社) 山本剛 (日本電信電話株式会社) 鈴木幸太郎 (日本電信電話株式会社) 内山成憲 (日本電信電話株式会社)	
4F1-2	ベクトル型 ElGamal 暗号について	1831
	金子 晃 (お茶の水女子大学)	
4F1-3	Resonance Properties of Chebyshev Chaotic Sequences	1837
	吉村朋大 (九州大学) 羽根竜一 (九州大学) 香田徹 (九州大学)	
4F1-4	二次体上の楕円曲線暗号	1843
	市田宗一郎 (鹿児島大学) 村島定行 (鹿児島大学)	
4F1-5	Multi-Keys Tripartite Key Agreement from Pairing	1849
	Lihua (University of Tsukuba) Wang Takeshi Okamoto (University of Tsukuba) Tsuyoshi Takagi (Technische Universitat Darmstadt) Eiji Okamoto (University of Tsukuba)	
4A2	データ保護	1月28日 10:55 ~ 12:35
4A2-1	Digital Forensics 適用を考慮にいれた電子情報の法的な安全性確保	1855

	藤村 明子 (NTT 情報流通プラットフォーム研究所) 塩野入 理 (NTT 情報流通プラットフォーム研究所) 金井 敦 (NTT 情報流通プラットフォーム研究所)	
4A2-2	電子媒体上の第三者のデータの没収について	1861
	奥村徹 (奥村 & 田中法律事務所)	
4A2-3	プライバシー保護のための個人データの消去に関する一考察	1867
	羽田知史 (日本アイビーエム)	
4A2-4	Usage Control Model for Data Confidentiality Problem in Database Service Provider	1873
	Amril Syalim (Graduate School of Information Science and Electrical Engineering, Kyushu University) Toshihiro Tabata (Faculty of Information Science and Electrical Engineering, Kyushu University) Kouichi Sakurai (Faculty of Information Science and Electrical Engineering, Kyushu University)	
4B2	エンドポイントセキュリティ -2・ P2P	1月28日 10:55 ~ 12:35
4B2-1	ネットワークゲームのチート防止策の実装	1879
	吉本晴洋 (東京大学) 繁富利恵 (東京大学) 今井秀樹 (東京大学)	
4B2-2	A Secure Multi-party Computation Scheme for Privacy-preserving Association Rules Mining	1885
	Chunhua SU (Kyushu University, Department of Computer Science and Communication Engineering) Kouichi SAKURAI (Kyushu University, Department of Computer Science and Communication Engineering)	
4B2-3	インセンティブコンピューティングのピア型 P2P を利用した実装方式	1891
	大隅正志 (横浜国立大学) 四方順司 (横浜国立大学) 松本勉 (横浜国立大学)	
4B2-4	Real-Time Intrusion Detection Mechanism based on Anomaly Behavior Segments	1897
	Ki Woong Ko (SK Teletech) Kyeong Tae Kim (Gwangju Institute of Science and Technology) Hyung Chan Kim (Gwangju Institute of Science and Technology) R. S. Ramakrishna (Gwangju Institute of Science and Technology) Kouichi Sakurai (Kyushu University)	
4B2-5	リーキーパケット方式を適用したリアルタイム IDS イベント異常分析手法	1903
	島田英一 (慶應義塾大学) 荒川豊 (慶應義塾大学) 竹森敬祐 (株式会社 KDDI 研究所) 笹瀬巖 (慶應義塾大学)	
4C2	Web セキュリティ -2・ ソフトウェア保護	1月28日 10:55 ~ 12:35
4C2-1	携帯電話を用いた二次元バーコードによる名刺管理システム	1909
	永井邦昭 (東京工科大学) 宇田隆哉 (東京工科大学) 伊藤雅仁 (東京工科大学) 市村哲 (東京工科大学) 田胡和哉 (東京工科大学) 松下温 (東京工科大学)	
4C2-2	安心と安全を考慮した不安度評価モデルに関する考察	1915
	日景奈津子 (岩手県立大学) 村山優子 (岩手県立大学)	
4C2-3	乱数を用いたプログラム制御構造の難読化手法の提案	1921
	豊福達也 (九州大学) 田端利宏 (九州大学) 櫻井幸一 (九州大学)	
4C2-4	署名生成ソフトウェアのランタイムデータ探索による耐タンパー性評価	1927
	本田洋之 (横浜国立大学) 松本勉 (横浜国立大学)	
4D2	共通鍵暗号	1月28日 10:55 ~ 12:35
4D2-1	MUGI の再同期攻撃に対する耐性評価	1933
	野坂哲郎 (東京理科大学) 渡辺大 (株式会社 日立製作所) 金子敏信 (東京理科大学)	
4D2-2	VSC128 に対する選択初期値攻撃	1939
	角尾 幸保 (株式会社 NEC) 齊藤 照夫 (NEC ソフトウェア北陸) 宮尾 紘太 (中央大学) 洲崎 智保 (NEC ソフトウェア北陸) 川幡 剛嗣 (NEC ソフトウェア北陸)	
4D2-3	16 ラウンド RC6 に適用可能なカイ 2 乗攻撃 について	1945
	高野祐輝 (北陸先端科学技術大学院大学) 宮地充子 (北陸先端科学技術大学院大学)	
4D2-4	KASUMI に対する攻撃方程式の効率的な解法	1951
	南部俊一 (東京理科大学) 杉尾信行 (株式会社 NTT ドコモ) 金子敏信 (東京理科大学)	
4D2-5	Most IVs of FMS Attack-Resistant WEP Implementation Leak Secret Key Information	1957
	Toshihiro Ohigashi (The University of Tokushima) Yoshiaki Shiraishi (Kinki University) Masakatu Morii (The University of Tokushima)	

4E2	サイドチャネル攻撃-4	1月28日 10:55 ~ 12:35
4E2-1	Security Information Flow Analysis for Data Diode with Embedded Software	1963
	Yu Sasaki (University of Queensland) Colin Fidge (University of Queensland)	
4E2-2	マスク付き入力の多項式展開によるガロア体上の逆元演算マスク法	1969
	山口晃由 (三菱電機) 佐藤恒夫 (三菱電機) 山田敬喜 (三菱電機)	
4E2-3	Tempest fonts の安全性に関する一考察	1975
	田中秀磨 (独立行政法人情報通信研究機構) 滝澤修 (独立行政法人情報通信研究機構) 山村明弘 (独立行政法人情報通信研究機構)	
4E2-4	剰余平方算処理の電力差分を利用した楕円曲線暗号に対する DPA 攻撃	1981
	秋下 徹 (ソニー株式会社) 高木 剛 (Technische Universitaet Darmstadt)	
4E2-5	Side Channel Attacks on the Countermeasures Using Randomized Binary Signed Digits ...	1987
	Dong-Guk Han (Center for Information Security Technologies (CIST)) Katsuyuki Okeya (Hitachi Laboratory) Tae Hyun Kim (Center for Information Security Technologies (CIST)) Yoon Sung Hwang (Korea University) Yong Ho Park (Sejong Cyber Univ.)	
4F2	ID暗号	1月28日 10:55 ~ 12:35
4F2-1	タイトな証明可能安全性を持つ ID ベース暗号	1993
	五味 剛 (東京大学) Nuttapong Attrapadung (東京大学) 花岡 悟一郎 (東京大学) 今井 秀樹 (東京大学)	
4F2-2	k-Resilient ID-based Hybrid 暗号について	1999
	荒木 俊則 (東京工業大学) 尾形わかは (東京工業大学)	
4F2-3	On the Signature Derived from Any Identity-Based Encryption	2005
	崔洋 (東京大学) 花岡悟一郎 (東京大学) 張銳 (東京大学) 藤崎 英一郎 (NTT Labs) 今井秀樹 (東京大学)	
4F2-4	Maurer-Yacobi 型 ID 暗号方式の再考察	2011
	阿部 航 (電気通信大学) 國廣 昇 (電気通信大学) 太田 和夫 (電気通信大学)	
4F2-5	ペアリングを用いた ID 情報に基づく多重署名についての考察	2017
	丹羽 朗人 (東芝ソリューション (株) S I 技術開発センター)	