SCIS2022 プログラム 2022年1月11日公開 (修正 2022年1月12日)

番号の読み方：[Day][会場][セッション番号]-[発表順]
例：番号1A2-3は「1日目のAという会場の2番目のセッションにおける3番目の発表」です
※会場名は変更されることがあります

Day 1 2022/1/18 (火)

番号	セッション名	発表タイトル	著者：◎登壇者（SCIS論文賞対象者）、○登壇者	座長
1A1	耐量子計算機暗号1			林卓也
1A1-1		数体篩法実装は双子smooth素数の探索に役立つか?	○青木 和麻呂(文教大学情報学部),大槻 紗季(東京大学大学院情報理工学系研究科),小貫 啓史(東京大学大学院情報理工学系研究科),高木 剛(東京大学大学院情報理工学系研究科)	
1A1-2		Quantum Resistance on Modes of Operation in Block Ciphers	◎Jeeun Lee(Korea Institute for Advanced Study)	
1A1-3		A Practical Lattice-based Threshold Signature	◎Yi Xu(Japan Advanced Institute of Science and Technology(JAIST)),Yuntao Wang(Japan Advanced Institute of Science and Technology(JAIST)),Eiichiro Fujisaki(Japan Advanced Institute of Science and Technology(JAIST))	
1A1-4		SABERにおける数論変換のC言語実装	◎青木大地(NECセキュアシステム研究所),岡村利彦(NECセキュアシステム研究所),峯松一彦(NECセキュアシステム研究所),高木剛(東京大学大学院)	
1A1-5		A study of the Kipnis-Shamir approach against the Rainbow signature scheme	○Yasuhiko Ikematsu(Kyushu University),Shuhei Nakamura(Nihon University)	
1A1-6		多変数多項式署名Rainbowに対する新たな乱数固定のフォルト攻撃	◎加藤拓(東京大学大学院 情報理工学系研究科 数理情報学専攻),清村優太郎(NTT 社会情報研究所),高木剛(東京大学大学院 情報理工学系研究科 数理情報学専攻)	
1B1	システムセキュリティ1			松本悦宜
1B1-1		動的解析ログを用いたマルウェアの早期目的推定に向けた特徴量の予測手法に関する検討	◎朝倉 紗斗至(電気通信大学),中川 恒(株式会社FFRIセキュリティ),押場 博光(株式会社FFRIセキュリティ),市野 将嗣(電気通信大学)	
1B1-2		信頼情報を基にした業務高信頼化方式	○角田 忠信(富士通株式会社),山口 純平(富士通株式会社),坂巻 慶行(富士通株式会社),山本 里奈(富士通株式会社),兒島 尚(富士通株式会社)	
1B1-3		Weighted Signed Networkを用いた公平な業務信頼度の計算方法	○山口純平(富士通株式会社),坂巻慶行(富士通株式会社),角田忠信(富士通株式会社),山本里奈(富士通株式会社),兒島尚(富士通株式会社)	
1B1-4		An Access Control System for Verifiable Credentials with Selective Disclosure	◎林俊安(金沢大学),鄭振牟(金沢大学),満保雅浩(金沢大学)	
1B1-5		TEEを活用したIDベース認証付き鍵交換の実装に関する考察	○工藤史堯(NTT社会情報研究所),飯島悠介(NTT社会情報研究所),永井彰(NTT社会情報研究所)	
1B1-6		スマートフォンを活用した金融決済サービスのセキュリティをどう向上させるか	○宇根正志(日本銀行),田村裕子(日本銀行)	
1C1	サイドチャネル攻撃1			藤本大介
1C1-1		耐量子鍵カプセル化メカニズムに対する一般化サイドチャネル攻撃	○上野 嶺(東北大学/JST CREST/JSTさきがけ),草川 恵太(日本電信電話株式会社 NTT社会情報研究所),田中 裕太郎(東北大学/JST CREST),伊東 燦(東北大学/JST CREST),高橋 順子(日本電信電話株式会社 NTT社会情報研究所),本間 尚文(東北大学/JST CREST)	
1C1-2		フーリエ解析ベース攻撃に対するECDSAのエラーレートに基づく解析	◎大崎俊輔(筑波大学情報学群情報科学類),國廣昇(筑波大学システム情報系)	
1C1-3		動的 FPGA 電源電流の RTL 解析に基づく電力解析攻撃への耐性予測	◎日室雅貴(岡山大学),五百旗頭健吾(岡山大学),豊田啓孝(岡山大学)	
1C1-4		パイプライン化されたAES S-boxへのフォールト攻撃に対する安全性評価	◎平田遼(電気通信大学),宮原大輝(電気通信大学),李陽(電気通信大学),三浦典之(大阪大学),崎山一男(電気通信大学)	
1C1-5		サイドチャネル攻撃により得られるBinary GCD演算系列に対するエラーモデル	◎谷健太(筑波大学システム情報工学研究群),國廣昇(筑波大学システム情報系)	
1D1	ブロックチェーン1			石井将大
1D1-1		NFT流通における深層学習を用いた分散型真正性検証プロトコルの提案	◎木村圭吾(筑波大学),今村光良(野村アセットマネジメント株式会社),面和成(筑波大学/NICT)	
1D1-2		NFT 流通市場に対するEditable Metadata 脆弱性の一考察	◎清水嶺(大阪大学),矢内直人(大阪大学),今村光良(野村アセットマネジメント),Jason Paul Cruz(大阪大学),岡村真吾(奈良工業高等専門学校)	
1D1-3		NFT流通プロセスにおける不正検知のための監査システム	◎東知哉(神戸大学),白石善明(神戸大学),今村光良(野村アセットマネジメント),掛井将平(名古屋工業大学),廣友雅徳(佐賀大学),森井昌克(神戸大学)	
1D1-4		暗号資産に関する全世界におけるサイバーインシデントの調査とリスクの考察	◎都築 祐人(筑波大学),伊藤 奎政(筑波大学),岸淵 涼平(筑波大学),曹 彦(筑波大学),矢田 昇平(筑波大学),面 和成(筑波大学)	
1D1-5		プライバシーに考慮した身分証明を使ったトークン取引の新方式の提案と実証システムの試作	○佐藤出(富士通株式会社),藤本真吾(富士通株式会社)	
1E1	秘密計算1			安永憲司
1E1-1		TTPを用いて1台のサーバで構成可能な秘密分散法による秘匿計算	○岩村恵市(東京理科大学),白井洸多(東京理科大学),稲村勝樹(広島市立大学)	
1E1-2		Computational Irrelevancy: Bridging the Gap between Pseudo- and Real Randomness in MPC Protocols	◎Nariyasu Heseri(東京大学情報理工学系研究科数理情報学専攻),Koji Nuida(Kyushu University / AIST)	
1E1-3		HQC暗号を応用した秘匿内積計算プロトコル（III）	◎中山太雅(佐賀大学),廣友雅徳(佐賀大学),福田洋治(近畿大学),毛利公美(岐阜大学),白石善明(神戸大学)	
1E1-4		プログレッシブ型視覚暗号に対する安全性評価に関する考察	◎レ タン タイ ビン(防衛大学校),田中 秀磨(防衛大学校)	
1F1	共通鍵暗号1			藤堂洋介
1F1-1		RoccaとAEGISファミリーのラウンド関数の安全性評価	◎竹内 信幸(兵庫県立大学),阪本 光星(兵庫県立大学),五十部 孝典(兵庫県立大学)	
1F1-2		倍ブロック長圧縮関数の量子衝突計算困難性について	○廣瀬勝一(福井大学),桑門秀典(関西大学)	
1F1-3		Fibonacci数列を利用したS-box及び転置関数によるAESへの有効性調査	○阿部友美(東京理科大学),五十嵐保隆(東京理科大学)	
1F1-4		軽量ブロック暗号 DLBCA に対する MILP を用いた Integral 攻撃	◎廣見紗妃(東京理科大学 理工学研究科 電気工学専攻),五十嵐保隆(東京理科大学 理工学研究科 電気工学専攻)	
1F1-5		軽量ブロック暗号DoTに対するMILPを用いた線形攻撃	◎青柳光祐(東京理科大学),五十嵐保隆(東京理科大学)	
1A2	耐量子計算機暗号2			青木大地
1A2-1		NIST PQC Round3候補の鍵カプセル化方式の匿名性	○草川 恵太(NTT社会情報研究所)	
1A2-2		同種写像暗号B-SIDHの実験による計算量評価と効率的な素数pの条件	◎大槻紗季(東京大学大学院情報理工学系研究科),青木和麻呂(文教大学情報学部),小貫啓史(東京大学大学院情報理工学系研究科),高木剛(東京大学大学院情報理工学系研究科)	
1A2-3		耐量子計算機署名Mod FalconのToom-Cook法及びRadix4 FFTによる高速化	◎福原大毅(東京都立大学),髙橋雄人(東京都立大学),山村和輝(NTT社会情報研究所),齋藤恆和(NTT社会情報研究所),横山俊一(東京都立大学)	
1A2-4		近似イデアルGCD問題に基づく不定方程式暗号のバリエーションについて	○秋山 浩一郎(株式会社東芝 研究開発センター),池松 泰彦(九州大学 マス・フォア・インダストリ研究所)	
1A2-5		A New Efficient Variant of the XL Algorithm Using the Arithmetic over Polynomial Matrices	◎古江弘樹(東京大学),工藤桃成(東京大学)	
1A2-6		MQ問題の解決のためのHybrid approachの改良の検討	○坂田康亮(東京大学)	
1B2	システムセキュリティ2			山本匠
1B2-1		フォレンジック調査の補助のためのWindows APIコールログを用いた不正プログラムの動作再現ツール	◎松田 尚也(近畿大学),福田 洋治(近畿大学),廣友 雅徳(佐賀大学),白石 善明(神戸大学)	
1B2-2		Hybrid Zero Trust Architectureにおける機械学習を用いた不正操作の検知	◎石出港士(東洋大学),岡田怜士(東洋大学),吉倉昌利(東洋大学),松田亘(NTT),藤本万里子(東洋大),満永拓邦(東洋大)	
1B2-3		ファームウェア更新に対するIETF RATS準拠リモートアテステーションの設計	◎内匠真也(株式会社東芝),藤松由里恵(株式会社東芝),金井遵(株式会社東芝)	
1B2-4		IPカメラのセキュリティに対する調査手法の検討と判明した問題点の考察	○下山 啓(情報セキュリティ大学院大学),松井 俊浩(情報セキュリティ大学院大学)	
1B2-5		オンラインサンドボックスにおけるMITRE ATT&CKマッピング機能に係る実態調査	◎藤井 翔太(株式会社 日立製作所/岡山大学 大学院自然科学研究科),山岸 伶(株式会社 日立製作所),山内 利宏(岡山大学 学術研究院自然科学学域)	
1B2-6		患者異常監視システムにおいて患者異常と機器異常を切り分ける方式の提案・評価と支援システムの構想	○佐々木良一(東京電機大学)	
1C2	ハードウェアセキュリティ1			吉田直樹
1C2-1		最終ラウンド候補の認証機能付き軽量暗号に対する高位合成の評価	◎竹本 修(名城大学大学院),池崎 良哉(名城大学大学院),野崎 佑典(名城大学),吉川 雅弥(名城大学)	
1C2-2		RAMBleedによるOpenSSL暗号鍵導出	◎冨田千尋(神戸大学大学院工学研究科),瀧田慎(兵庫県立大学大学院情報科学研究科),福島和英(株式会社KDDI総合研究所 情報セキュリティグループ),仲野有登(株式会社KDDI総合研究所 情報セキュリティグループ),白石善明(神戸大学大学院工学研究科),森井昌克(神戸大学大学院工学研究科)	
1C2-3		Intel SGX における2 つのリモートアテステーションの利点と欠点の考察	◎矢川 嵩(筑波大学. 産業技術総合研究所),照屋 唯紀(産業技術総合研究所),須崎 有康(産業技術総合研究所),阿部 洋丈(筑波大学)	
1C2-4		TEEの保護を用いたProvenance AuditingのIoT機器への適用	◎竹村太一(産業技術総合研究所， 電気通信大学),須崎有康(産業技術総合研究所),山本嶺(電気通信大学)	
1C2-5		実環境を想定したトロイ回路を対象とした機械学習によるハードウェアトロイ識別	◎栗原樹(早稲田大学),長谷川健人(KDDI総合研究所),福島和英(KDDI総合研究所),清本晋作(KDDI総合研究所),戸川望(早稲田大学)	
1C2-6		STM32 上の AES コプロセッサを用いた OCB の高性能ソフトウェア実装	○金 剛山(電気通信大学),菅原 健(電気通信大学)	
1D2	生体認証・バイオメトリクス1			肥後春菜
1D2-1		不正な認証を防ぐための顔画像の非識別化に関する検討	◎内田秀継(富士通株式会社),安部登樹(富士通株式会社),山田茂史(富士通株式会社)	
1D2-2		攻撃発生確率を考慮した生体認証システムのリスク分析手法に関する一検討	○大木哲史(静岡大学),成田惇(静岡大学),内田秀継(富士通株式会社 先端融合技術研究所),安部登樹(富士通株式会社 先端融合技術研究所),山田茂史(富士通株式会社 先端融合技術研究所)	
1D2-3		収集Wi-Fiデータから算出される統計量を利用した行動認証手法	◎大河澪耶(東京大学大学院 情報理工学系研究科),小林良輔(東京大学大学院 情報理工学系研究科),山口利恵(東京大学大学院 情報理工学系研究科)	
1D2-4		Vision Transformerを用いた顔なりすまし攻撃検知手法とその評価	◎渡邉浩太(東北大学大学院),伊藤康一(東北大学大学院),青木孝文(東北大学大学院)	
1D2-5		Fuzzy鍵を用いたグループ署名技術	◎川名のん(日立製作所),長沼健(日立製作所),高橋健太(日立製作所),中村渉(日立製作所),本宮志江(日立製作所),羽渕峻行(日立製作所)	
1D2-6		エンターテイメントとセキュリティを融合した本人認証アプリの試作と評価	◎鈴木真樹史(工学院大学),藤川真樹(工学院大学)	

I E2	暗号プロトコルI			辛星漢
I E2-I		IoTネットワークにおける検証者指定署名方式	○渡邉 洋平(電気通信大学 / ジャパンデータコム株式会社),矢内 直人(大阪大学 / ジャパンデータコム株式会社),四方 順司(横浜国立大学)	
I E2-2		Concurrent Group Operations on TreeKEM	◎小柳優悟(東京工業大学),石井将大(東京工業大学),田中圭介(東京工業大学)	
I E2-3		ProVerifによる検索可能暗号の形式的安全性検証について	◎鈴木孝誠(信州大学),山本博章(信州大学),三重野武彦(エプソンアヴァシス（株）、信州大),荒井研一(長崎大学),岡崎裕之(信州大学),布田裕一(東京工科大学)	
I E2-4		実用に向けたPKI-IDクロスドメイン認証鍵交換の評価	◎飯島 悠介(NTT社会情報研究所),向山 明夫(NTT社会情報研究所),永井 彰(NTT社会情報研究所),工藤 史堯(NTT社会情報研究所)	
I E2-5		鍵失効可能な検索可能暗号	○平野 貴人(三菱電機株式会社),川合 豊(三菱電機株式会社),小関 義弘(三菱電機株式会社),渡邉 洋平(電気通信大学),岩本 貢(電気通信大学),太田 和夫(電気通信大学)	
I E2-6		参加者情報を秘匿する非同期グループメッセージング方式	○江村 恵太(情報通信研究機構),梶田 海成(日本放送協会),野島 良(情報通信研究機構),小川 一人(情報通信研究機構),大竹 剛(日本放送協会)	
I F2	共通鍵暗号2			井上明子
I F2-I		軽量ブロック暗号LBC-IoTに対するMILPを用いた線形攻撃耐性評価	◎安士颯真(東京理科大学),五十嵐保隆(東京理科大学)	
I F2-2		プロービング攻撃による漏洩情報を用いたAES鍵復元アルゴリズムの改良	◎植村友紀(電気通信大学),渡邉洋平(電気通信大学/産業技術総合研究所),李陽(電気通信大学),三浦典之(大阪大学),岩本貢(電気通信大学),崎山一男(電気通信大学),太田和夫(電気通信大学/産業技術総合研究所)	
I F2-3		Bernstein-Vazirani量子アルゴリズムに基づくランダムブール関数の隠れシフト問題の求解について	◎八藤後 彬(茨城大学大学院 理工学研究科 情報工学専攻),米山 一樹(茨城大学大学院 理工学研究科 情報工学専攻)	
I F2-4		少命令セット組込みプロセッサにおけるARX型暗号アルゴリズムの実装と評価	◎楊明宇(東京工業大学),卯木あゆ美(東京工業大学),李陽(電気通信大学),崎山一男(電気通信大学),原祐子(東京工業大学)	
I F2-5		Elephantに対する鍵回復，識別及び偽造攻撃	◎土生亮(名古屋大学),岩田哲(名古屋大学)	
I F2-6		軽量ブロック暗号CRAFTのハッシュ関数への応用に関する考察	◎西尾明日駆(東京理科大学),五十嵐保隆(東京理科大学)	
I A3	公開鍵暗号I			Jo Hyungrok
I A3-I		究極の本人確認のための3層構造公開鍵暗号の提案－第3報	○辻井 重男(中央大学研究開発機構),吉田 昇(株式会社SRAホールディングス),佐々木浩二(株式会社アドイン研究所),鈴木 伸治(株式会社アドイン研究所),才所 敏明(中央大学研究開発機構),山澤 昌夫(中央大学研究開発機構),五太子 政史(中央大学研究開発機構),四方 光(中央大学),橘谷田 真樹(関西医科大学)	
I A3-2		被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線に対する同種条件下の完全分類	◎村井公輔(中央大学理工学研究科情報工学専攻),志村真帆呂(東海大学理学部情報数理学科),飯島努(株式会社光電製作所),趙晋輝(中央大学理工学研究科情報工学専攻)	
I A3-3		A Study of Non-malleability Definitions on Timed Commitments	◎Zehua Shang(Kyoto University),Mehdi Tibouchi(Kyoto University. NTT Secure Platform Laboratories),Masayuki Abe(Kyoto University. NTT Secure Platform Laboratories)	
I B3	ネットワークセキュリティI			毛利公一
I B3-I		対話的に通信制御が可能なマルウェア解析システム	◎濱島 圭佑(京都大学),小谷 大祐(京都大学),岡部 寿男(京都大学)	
I B3-2		Adversarial Attack against DNN-based DDoS Intrusion Detection System	Mariama Mbow(Kyushu University),Hiroshi Koide(Kyushu University),Kouichi Sakurai(Kyushu University)	
I B3-3		脆弱性の概念実証コードに対する網羅的な攻撃パケット生成を用いた侵入検知システムのシグネチャ自動生成	◎小林 雅季(京都大学),鐘本 楊(NTT社会情報研究所),小谷 大祐(京都大学),岡部寿男(京都大学)	
I B3-4		ハニーポットで観測される絨毯爆撃型DRDoS攻撃の分析	◎毛 清昕(横浜国立大学大学院環境情報学府 吉岡研究室),牧田 大佑(横浜国立大学大学院環境情報研究院/先端科学高等研究院),吉岡 克成(横浜国立大学大学院環境情報研究院/先端科学高等研究院),松本 勉(横浜国立大学大学院環境情報研究院/先端科学高等研究院)	
I C3	ハードウェアセキュリティ2			須崎有康
I C3-I		消費電力波形の形状を考慮したIoTデバイス異常動作検知手法	◎久古幸汰(早稲田大学),高崎和成(早稲田大学),戸川望(早稲田大学)	
I C3-2		GRUおよびLSTMを利用した定常状態電力波形推定手法の評価	◎高崎和成(早稲田大学),木田良一(株式会社ラック),金子博一(株式会社ラック),戸川望(早稲田大学)	
I C3-3		グラフ学習を用いたハードウェアトロイ識別における説明性の検討	◎山下一樹(早稲田大学),長谷川健人(KDDI総合研究所),披田野清良(KDDI総合研究所),清本晋作(KDDI総合研究所),戸川望(早稲田大学)	
I C3-4		勾配ブースティング決定木と識別結果伝搬法によるハードウェアトロイ識別	◎根岸良太郎(早稲田大学),栗原樹(早稲田大学),戸川望(早稲田大学)	
I D3	AIセキュリティI			三浦尭之
I D3-I		Privacy-preserving Blockchain-based Global Data Sharing for Federated Learning with Non-IID Data	◎Zhuotao Lian(The University of Aizu),Qingkui Zeng(Nanjing University of Information Science and Technology.),Chunhua Su(The University of Aizu)	
I D3-2		GAN構造を用いたポイズニング検知	○清水俊也(富士通)	
I D3-3		JPEG圧縮由来の歪み信号に対する応答特性に基づくAdversarial Examples検知手法	◎角森健太(岡山大学),山崎裕真(岡山大学),栗林稔(岡山大学),舩曳信生(岡山大学),越前功(NII)	
I D3-4		イメージセンサインターフェースへのフォルト攻撃でトリガする DNN へのバックドア攻撃	◎大山 達哉(立命館大学),大倉 俊介(立命館大学),吉田 康太(立命館大学),藤野 毅(立命館大学)	
I E3	暗号プロトコル2			國廣昇
I E3-I		暗号のための脳機能拡張：信用できる計算機が不要な署名方式の提案	◎松本 彩花(東京工業大学),尾形 わかは(東京工業大学),高橋 健太(日立製作所),西垣 正勝(静岡大学)	
I E3-2		金銭的ペナルティに基づく公平な秘密計算におけるラウンド数の改善	○中井 雄士(電気通信大学),品川 和雅(茨城大学，産業技術総合研究所)	
I E3-3		復号制御付IDベース暗号の安全性に関する考察	◎宮永 英和(神奈川大学大学院),藤岡 淳(神奈川大学),佐々木 太良(神奈川大学),岡野 裕樹(NTT社会情報研究所),永井 彰(NTT社会情報研究所),鈴木 幸太郎(豊橋技術科学大学),米山 一樹(茨城大学)	
I E3-4		最大鍵漏洩攻撃に対して安全で計算効率のよいPKI-ID混在認証鍵交換	◎青栁光太郎(豊橋技術科学大学),岡野裕樹(日本電信電話株式会社),永井彰(日本電信電話株式会社),藤岡淳(神奈川大学),鈴木幸太郎(豊橋技術科学大学)	
I E3-5		メッセージ長を拡張する耐量子コミットメント方式	◎宮地秀至(大阪大学),王 イントウ(北陸先端大),宮地充子(大阪大学)	
I F3	プライバシー保護I			中村徹
I F3-I		プライバシー情報提供の可否に関する調査-経年変化に関する考察-	○金森 祥子(国立研究開発法人情報通信研究機構),佐藤 広英(信州大学/国立研究開発法人情報通信研究機構),太幡 直也(愛知学院大学/国立研究開発法人情報通信研究機構),野島 良(国立研究開発法人情報通信研究機構)	
I F3-2		パーソナルデータの等結合に適した匿名化技術の考察	○千田浩司(NTT),紀伊真昇(NTT),市川敦謙(NTT),野澤一真(NTTドコモ),長谷川慶太(NTTドコモ),堂面拓也(NTTドコモ),中川智尋(NTTドコモ),青野博(NTTドコモ),寺田雅之(NTTドコモ)	
I F3-3		Attested Execution Secure Processor-based Architecture for Self-Sovereign Identity Systems Preserving Privacy	○Koichi Moriyama(Institute of Information Security),Akira Otsuka(Institute of Information Security)	
I F3-4		安全性と有用性を両立する半導体ウェハマップのデータマスキングの検討	○花谷 嘉一(株式会社東芝 研究開発センター),和田 紘帆(東芝インフラシステムズ株式会社)	
I F3-5		属性推定攻撃を考慮する匿名化データの安全性指標の提案	○紀伊真昇(NTT 社会情報研究所),市川敦謙(NTT 社会情報研究所),三浦尭之(NTT 社会情報研究所),芝原俊樹(NTT 社会情報研究所)	
I A4	公開鍵暗号2			阿部正幸
I A4-I		Lossy Trapdoor function の幾つかの亜種について	○星野 文学(長崎県立大学)	
I A4-2		効率的な漏洩耐性鍵隔離暗号	◎淺野京一(電気通信大学),岩本貢(電気通信大学),渡邉洋平(電気通信大学 / 産業技術総合研究所)	
I A4-3		匿名放送型暗号及び認証における非漸近的タイトな下界と最適構成法について	◎小林大航(横浜国立大学大学院環境情報学府),渡邉洋平(電気通信大学),峯松一彦(NEC/横浜国立大学先端科学高等研究院),四方順司(横浜国立大学大学院環境情報研究院)	
I A4-4		公開鍵暗号の平文空間の効率的な拡張方法について	○松田 隆宏(国立研究開発法人 産業技術総合研究所)	
I B4	ネットワークセキュリティ2			藤井翔太
I B4-I		標的型マルウェアの通信先情報に基づくC&Cサーバ監視による攻撃誘引	◎細見勇介(立命館大学),津田侑(情報通信研究機構),鄭俊俊(立命館大学),毛利公一(立命館大学)	
I B4-2		情報指向ネットワークにおける分散コンテンツ配送による安全性と効率の改善	◎佐久田 尚(東京理科大学),岩村 恵市(東京理科大学)	
I B4-3		教師なし学習を用いた低レートDoS攻撃検知手法の設計と実装	◎椢場 叶耀(東北大学大学院情報科学研究科),ギリエ ルイス(東北大学電気通信研究所),和泉 諭(仙台高等専門学校)	
I C4	サイドチャネル攻撃2			上野嶺
I C4-I		RISC－VとSubRISC+におけるLED暗号のBitslice実装の評価	◎渡辺陸(電気通信大学大学院),楊 明宇(東京工業大学大学院),原 祐子(東京工業大学),崎山 一男(電気通信大学),李 陽(電気通信大学)	
I C4-2		ハードウェア実装AESに対するAggregated Mono-Bit modelモデルを利用した深層学習サイドチャネル攻撃	◎橋本 尚志(立命館大学),福田 悠太(立命館大学),吉田 康太(立命館大学),黒田 訓宏(立命館大学),藤野 毅(立命館大学)	
I C4-3		電磁波サイドチャネルとスクリーミングチャネルの同時収集攻撃の検証	◎松川 侑生(電気通信大学),杉本 悠馬(電気通信大学),菅原 健(電気通信大学),崎山 一男(電気通信大学),李 陽(電気通信大学)	
I C4-4		ECDSAハードウェア実装におけるテンプレート攻撃と格子攻撃による秘密鍵復元の検討	◎阿部浩太郎(東京大学),池田誠(東京大学)	
I D4	AIセキュリティ2			土田光
I D4-I		Data Lineage Management with Unlearning Method for Machine Learning Security and Privacy Issues	○Haibo ZHANG(Department of Information Science and Technology. Kyushu University),Toru NAKAMURA(KDDI Research Inc.),Takamasa ISOHARA(KDDI Research Inc.),Kouichi SAKURAI(Department of Information Science and Technology. Kyushu University)	
I D4-2		部分観測マルコフ決定過程によるニューラルエージェント強化学習を使用した自律型SQL インジェクション攻撃手法	◎佐竹達也(情報セキュリティ大学院大学),大塚玲(情報セキュリティ大学院大学)	
I D4-3		機械学習を用いたフォグ環境の異常検知効率の考察	○牧野俊太郎(東洋大学),岡田怜士(東洋大学),満永拓邦(東洋大学)	
I D4-4		Intel SGXによる安全で高速なDNN推論の実装方式	○藤原啓成(株式会社 日立製作所),佐藤尚宜(株式会社 日立製作所)	

I E4	教育・心理学 I			未定
I E4-1		OS更新の促進アプローチに関する長期実証実験	◎佐野絢音(株式会社KDDI総合研究所),澤谷雪子(株式会社KDDI総合研究所),山田明(株式会社KDDI総合研究所),窪田歩(株式会社KDDI総合研究所),磯原隆将(株式会社KDDI総合研究所)	
I E4-2		Twitter上における意図的な大規模情報拡散の因子となる特徴点分析	◎林 尚弘(明治大学),鳴田 里聖(明治大学大学院),田畑 唯斗(明治大学大学院),笠井 遥輝(明治大学大学院),高山 眞樹(明治大学大学院),齋藤 孝道(明治大学)	
I E4-3		AIシステムの利用者視点からのトラスト構築の考察	○島 成佳(長崎県立大学),小川 隆一(独立行政法人情報処理推進機構),佐川 陽一(独立行政法人情報処理推進機構)	
I F4	物理的暗号 I			須賀祐治
I F4-1		灯台とABCプレースの物理的ゼロ知識証明	◎深澤拓朗(工学院大学),真鍋義文(工学院大学)	
I F4-2		秘匿置換を用いた効率的なn入力多数決カードプロトコル	◎安部芳紀(電気通信大学),中井雄士(電気通信大学),渡邉洋平(電気通信大学/産業技術総合研究所),岩本貢(電気通信大学),太田和夫(電気通信大学/産業技術総合研究所)	
I F4-3		最小のカード枚数による対称関数の秘密計算について	◎四方隼人(東北大学),豊田航大(東北大学),宮原大輝(電気通信大学),水木敬明(東北大学)	

Day 2 2022/1/19 (水)

番号	セッション名	発表タイトル	著者：◎登壇者（SCIS論文賞対象者）、○登壇者	座長
2A1	耐量子計算機暗号3			青野良範
2A1-1		格子暗号におけるノイズの数論変換の実装について	○米村智子(株式会社東芝),秋山浩一郎(株式会社東芝)	
2A1-2		SQISignの公開鍵の安全性	○小貫啓史(東京大学大学院情報理工学系研究科)	
2A1-3		SIKEに対するvOW法の内部関数の新計算手法	○神戸祐太(株式会社すうがくぶんか/立教大学),高橋康(立教大学),相川勇輔(三菱電気),エ藤桃成(東京大学),安田雅哉(立教大学),高島克幸(早稲田大学),横山和弘(立教大学)	
2A1-4		Implementations on identity-based signature schemes based on variants of CSIDH	○Hyungrok Jo(Yokohama National University. IAS),Junji Shikata(Yokohama National University)	
2B1	システムセキュリティ3			高田一樹
2B1-1		ドキュメント化されていないヘッダを活用した機械学習によるマルウェア分類	○小久保 博崇(富士通株式会社),大山 恵弘(筑波大学)	
2B1-2		データ分布情報を用いたレンジクエリに対するボリューム漏洩攻撃	◎小谷俊輔(筑波大学システム情報工学研究群),國廣昇(筑波大学システム情報系)	
2B1-3		確率モデルと実験による増分故障解析の安全性評価	◎加藤光(電気通信大学),菅原健(電気通信大学),崎山一男(電気通信大学),李陽(電気通信大学)	
2B1-4		脆弱性自動検知に向けたバイナリプログラム解析ツールの開発	○泉田大宗(IIJ技術研究所),橋本政朋(千葉工業大学),森彰(産業技術総合研究所)	
2C1	ウェブセキュリティ1			未定
2C1-1		FIDO認証を用いたECサイトのセキュリティ強化手法	◎内藤猛(東洋大学),岡田怜士(東洋大学),松本悦宜(Capy株式会社),満永拓邦(東洋大学)	
2C1-2		脆弱性のテスト環境を併用利用した攻撃検知・防御支援システム	◎張 邯尹(東京情報大学大学院 総合情報学研究科),中川 佑人(東京情報大学大学院 総合情報学部),花田 真樹(東京情報大学大学院 総合情報学部),村上 洋一(東京情報大学大学院 総合情報学部),早稲田 篤志(東京情報大学大学院 総合情報学部),三村 隆夫(株式会社セキュアブレイン),石田 裕貴(株式会社セキュアブレイン),布広 永示(東京情報大学大学院 総合情報学部)	
2C1-3		ゼロトラストアーキテクチャにおけるブラウザフィンガープリントを利用したアクセス制御	○高木祥一(情報セキュリティ大学院大学),大久保隆夫(情報セキュリティ大学院大学)	
2C1-4		Cookie Bomb攻撃を検知するブラウザ拡張機能	◎岡澤 佳寛(東京電機大学大学院),齊藤 泰一(東京電機大学)	
2C1-5		パッシブフィンガープリントによる多値分類モデルを用いたID推定の試み	◎升田尚幸(明治大学),神章洋(明治大学大学院),渡名喜瑞稀(明治大学大学院),藤井達也(明治大学大学院),高山眞樹(明治大学大学院),齋藤孝道(明治大学)	
2D1	AIセキュリティ3			宇根正志
2D1-1		勾配系の説明付きモデルに対するデータフリーモデル抽出攻撃	◎三浦尭之(NTT社会情報研究所 / 大阪大学),芝原俊樹(NTT社会情報研究所),矢内直人(大阪大学)	
2D1-2		部分観測マルコフ決定過程に基づいたニューラルエージェントを使用したペネトレーションテスト手法の提案	◎米田智紀(情報セキュリティ大学院大学),大塚玲(情報セキュリティ大学院大学)	
2D1-3		ビザンチンロバストな連合学習における学習モデル保護の基礎検討	○中井 綱人(三菱電機株式会社),鈴木 大輔(三菱電機株式会社),藤野 毅(立命館大学)	
2D1-4		角膜鏡面ハイライトに基づくDeepFake画像検出について	◎清水 一樹(金沢大学),満保 雅浩(金沢大学)	
2D1-5		機械学習を用いた暗号プロトコルの安全性検証フレームワーク	大野 乾太郎(NTT コンピュータ＆データサイエンス研究所),◎中林 美郷(NTT 社会情報研究所)	
2E1	秘密計算2			品川和雅
2E1-1		ネットワーク上のユーザー間の主観的評価を秘匿する秘匿信頼度計算技術	○坂巻 慶行(富士通),山口 純平(富士通),角田 忠信(富士通),山本 里奈(富士通),兒島 尚(富士通)	
2E1-2		同一のカードを用いた秘密計算	○高橋 俊彦(新潟大学工学部)	
2E1-3		Generating Residue Number System Bases	Jean-Claude Bajard(Sorbonne University),Kazuhide Fukushima(KDDI Research, Inc),Shinsaku Kiyomoto(KDDI Research, Inc),Thomas Plantard(University of Wollongong),○Arnaud Sipasseuth(KDDI Research, Inc),Willy Susilo(University of Wollongong)	
2E1-4		秘密計算によるk-means法とk-means++法	○三品気吹(NTT社会情報研究所),五十嵐大(NTT社会情報研究所),濱田浩気(NTT社会情報研究所),菊池亮(NTT社会情報研究所)	
2F1	セキュリティ評価1			澤田賢治
2F1-1		情報理論的安全性を有する宇宙ロケット用セキュア通信方式の性能実証飛行	○森岡澄夫(インターステラテクノロジズ株式会社),尾花賢(法政大学),吉田真紀(情報通信研究機構)	
2F1-2		Distant Supervisionによるサイバーセキュリティ文書のマルチラベル分類	○石井 将大(東京工業大学),森 健人(東京工業大学),桑名 亮一(東京工業大学),松浦 知史(東京工業大学)	
2F1-3		Efficient Machine Learning Method for Protocol Fuzzing: Improvement of Sequence-to-Sequence Model and Refined Training Data	○Bo Wang(JVCKENWOOD Corporation),Toshihiro Maruyama(JVCKENWOOD Corporation),Ako Suzuki(JVCKENWOOD Corporation),Yuichi KAJI(Nagoya University)	
2F1-4		Android用ファジングツールの適用及びその性能評価	◎佐久間耀大朗(長崎県立大学),高橋寿一(株式会社ロジギアジャパン),加藤雅彦(長崎県立大学)	
2A2	耐量子計算機暗号4			池松泰彦
2A2-1		NIST PQC Round3候補の鍵カプセル化方式への故障注入攻撃	○草川 恵太(NTT社会情報研究所),伊東 燦(東北大学),上野 嶺(東北大学. PRESTO),高橋 順子(NTT社会情報研究所),本間 尚文(東北大学. CREST)	
2A2-2		Web PKI 業界が耐量子計算機暗号への移行を急がなくて良い 3 つの理由	○伊藤 忠彦(セコム株式会社),肖 俊廷(セコム株式会社)	
2A2-3		NTRU格子の拡張と格子攻撃	◎中邑聡史(NTT 社会情報研究所),安田雅哉(立教大学)	
2B2	システムセキュリティ4			磯原隆将
2B2-1		サイバー攻撃者のインテリジェンス収集のためのディープマルウェア解析	○村上弘和(株式会社 CyCraft Japan),西垣正勝(静岡大学創造科学技術大学院)	
2B2-2		ランサムウェアの解析とその対策に関する研究	◎古門良介(神戸大学院工学研究科),池上雅人(キャノンITソリューション株式会社),住田裕輔(キャノンITソリューション株式会社),岡庭素之(キャノンITソリューション株式会社),白石善明(神戸大学院工学研究科),森井昌克(神戸大学院工学研究科)	
2B2-3		引数情報を用いたAPIコール列に基づくマルウェアのファミリ分類手法	○廣瀬 優希(東京情報大学),花田 真樹(東京情報大学),面 和成(筑波大学),折田 彰(株式会社日立システムズ),関谷 信吾(株式会社日立システムズ),村上 洋一(東京情報大学),早稲田 篤志(東京情報大学),布広 永示(東京情報大学)	
2B2-4		クラウドアプリケーションの完全性を保証するKubernetesマニフェストの署名検証手法	◎北原啓州(IBM東京基礎研究所),渡邉裕治(IBM東京基礎研究所)	
2C2	サイドチャネル攻撃3			原祐子
2C2-1		ハードウェア実装AESに対するMulti-bitラベルを用いたノンプロファイリング深層学習サイドチャネル攻撃	◎福田 悠太(立命館大学),吉田 康太(立命館大学),黒田 訓宏(立命館大学),藤野 毅(立命館大学)	
2C2-2		M&Mにより対策されたAES暗号ハードウェアの乱数依存性について	◎塚原 麻輝(電気通信大学),平田 遼(電気通信大学),宮原 大輝(電気通信大学),李 陽(電気通信大学),崎山 一男(電気通信大学)	
2C2-3		バレルシフタと加算器によるビット非独立なサイドチャネルリークの発生機序とその対策	◎浅野多聞(電気通信大学),菅原健(電気通信大学)	
2D2	AIセキュリティ4			清水俊也
2D2-1		電子指紋は機械学習の二段階攻撃に使えるか？	◎岩花 一輝(大阪大学),三浦 尭之(NTT社会情報研究所),奥田 哲矢(NTT社会情報研究所),矢内 直人(大阪大学)	
2D2-2		モデル抽出攻撃の定式化を通じた体系的な整理	◎小松みさき(株式会社東芝 研究開発センター),花谷嘉一(株式会社東芝 研究開発センター)	
2D2-3		OP-TEEを用いた隔離AIハードウェアアクセラレーションの実装評価	○中井綱人(三菱電機株式会社),鈴木 大輔(三菱電機株式会社),藤野 毅(立命館大学)	
2D2-4		シンプルブラックボックス攻撃の対策手法に関する検討	鵜島廉(金沢大学),◎井林大成(金沢大学),満保雅浩(金沢大学)	
2E2	暗号プロトコル3			河内亮周
2E2-1		チャージ型決済の実現方法とそのセキュリティ	○田村裕子(日本銀行)	
2E2-2		範囲証明つき準同型暗号とその対話的プロトコル	○光成滋生(サイボウズ・ラボ株式会社)	
2E2-3		Invisible and Unlinkable Policy-Based Sanitizable Signatures	◎石坂 理人(KDDI総合研究所),福島 和英(KDDI総合研究所),田中 圭介(東京工業大学大学院)	
2E2-4		指数部検査を省略したFSU方式のピア事後指定安全性	◎小山幸保(神奈川大学),藤岡淳(神奈川大学),佐々木太良(神奈川大学),岡野裕樹(NTT社会情報研究所),永井彰(NTT社会情報研究所)	
2F2	プライバシー保護2			森山光一
2F2-1		データに対する匿名加工を考慮したデジタル署名の検討	肥後 春菜(NEC),一色 寿幸(NEC),森 健吾(NEC),田宮 寛人(NEC),◎土田 光(NEC)	
2F2-2		分散型ID（DID）/検証可能属性証明（VC）技術を利用した自己主権型アイデンティティ情報利活用基盤（SSIUF）に関する考察	○才所敏明(IT企画),辻井重男(中央大学研究開発機構),櫻井幸一(九州大学 大学院システム情報科学研究院)	
2F2-3		動的サンプリングを使用した勾配ブースティング決定木の連合追加学習	◎三浦 啓吾(神戸大学),王 立華(情報通信研究機構),小澤 誠一(神戸大学)	
2A3	公開鍵暗号3			照屋唯紀
2A3-1		指定された追跡可能性を有するグループ署名の双線形群における例示	○穴田 啓晃(長崎県立大学),福光 正幸(北海道情報大学),長谷川 真吾(東北大学)	
2A3-2		Mathematical Structure of Finsler Encryption and Signature	○永野 哲也(長崎県立大学),穴田 啓晃(長崎県立大学)	
2A3-3		カメレオン署名を用いたFIDO認証の権限移譲機能の検討	◎成松怜央(東洋大学),岡田怜士(東洋大学),満永拓邦(東洋大学)	
2A3-4		FK12曲線上のペアリングにおける最終べきアルゴリズムの改良	◎池坂和真(岡山大学),南條由紀(岡山大学),小寺雄太(岡山大学),日下卓也(岡山大学),野上保之(岡山大学)	
2B3	システムセキュリティ5			小久保博崇
2B3-1		準パススルー型ハイパーバイザを用いて取得したメモリデータの分析	◎大森 貴通(豊田工業高等専門学校),平野 学(豊田工業高等専門学校),小林 良太郎(工学院大学)	
2B3-2		ペネトレーションテスト自動化に向けたサイバー攻撃手段の定量的評価法の提案	◎木藤 圭亮(三菱電機株式会社),加藤 駿(三菱電機株式会社),河内 清人(三菱電機株式会社),木下 洋輔(三菱電機株式会社),酒井 康行(三菱電機株式会社),吉村礼子(三菱電機株式会社)	
2B3-3		MITRE ATT&CK Techniques の関連性に基づく攻撃検知の検討	◎葛西裕紀(東洋大学),岡田怜士(東洋大学),満永拓邦(東洋大学)	
2B3-4		NS3を用いたIoTマルウェア感染拡大・攻撃シミュレータの実装	○石田 裕貴(株式会社セキュアブレイン),前田 泰浩(株式会社セキュアブレイン)	

2C3	自動車セキュリティ1		矢嶋純
2C3-1		組込み型ハイパーバイザにおけるVirtIOを利用した不正ファイルアクセス監視方法	◎大野 仁(パナソニック株式会社),今本 吉治(パナソニック株式会社),安齋 潤(パナソニック株式会社)
2C3-2		時系列データベースを用いたCANの侵入検知システムの提案	○倉地 亮(名古屋大学),高田 広章(名古屋大学),足立 直樹(株式会社オートネットワーク技術研究所),上田 浩史(株式会社オートネットワーク技術研究所),宮下 之宏(株式会社オートネットワーク技術研究所)
2C3-3		ISO/SAE 21434プロセスを踏まえた車載IDSの要件分析	○倉地 亮(名古屋大学),佐々木 崇光(パナソニック株式会社),氏家 良浩(パナソニック株式会社),松島 秀樹(パナソニック株式会社)
2D3	ブロックチェーン2		奥田哲矢
2D3-1		ブロックチェーンを用いた重複データ排除機能付きマルチクラウドストレージ監査方式	○廣友雅徳(佐賀大学),嘉戸裕一(神戸大学),白石善明(神戸大学),今村光良(野村アセットマネジメント株式会社),森井昌克(神戸大学)
2D3-2		Conclave: A Collective Stake Pool Protocol	Dimitris Karakostas(University of Edinburgh/Input Output Hong Kong),Aggelos Kiayias(University of Edinburgh/Input Output Hong Kong),◎ラランジェラマリオ(東京工業大学・インプットアウトプットホンコン)
2D3-3		プライバシーを考慮したブロックチェーンを用いた柔軟なコンタクトトレーシング手法	◎福田竜央(筑波大学),面和成(筑波大学/情報通信研究機構)
2E3	暗号理論1		工藤桃成
2E3-1		Algebraic Group ModelにおけるFiat-Shamir Bulletproofsの頑健性について	Chaya Ganesh(Indian Institute of Science),Claudio Orlandi(Aarhus University),Mahak Pancholi(Aarhus University),◎Akira Takahashi(Aarhus University),Daniel Tschudi(Concordium)
2E3-2		A Quantum Search-to-Decision Reduction for the LPN Problem	◎数藤恭平(東京工業大学),手塚真徹(東京工業大学),原啓祐(東京工業大学. 産業技術総合研究所),吉田雄祐(東京工業大学),田中圭介(東京工業大学)
2E3-3		Cryptographic hash functions based on Triplet and Sextet graphs	Hyungrok Jo(Yokohama National University. IAS),◎Shohei Satake(Kumamoto University)
2F3	教育・心理学2		角尾幸保
2F3-1		能力主義的公平なマッチングと効率的な判定アルゴリズム	○中村 徹(KDDI総合研究所),磯原 隆将(KDDI総合研究所)
2F3-2		テレワークにおけるBYOD利用時のセキュリティ等の不安に関する分析	○森 淳子(独立行政法人情報処理推進機構),小山 明美(独立行政法人情報処理推進機構),小川 隆一(独立行政法人情報処理推進機構),竹村 敏彦(城西大学)
2F3-3		Web 上パスワード認証システムに関するUXデザインの実態調査： 不親切なパスワード登録エラーメッセージ表示	◎藤田 真浩(三菱電機株式会社),山中 忠和(三菱電機株式会社),松田 規(三菱電機株式会社),金岡 晃(東邦大学)
2F3-4		Become a Security Monopoly: Gamification to Learn Cyber Defense Matrix	○Chen Chung-Kuan(CyCraft Technology),Kao Wei-Chia(CyCraft Technology),Cheng Chen-mou(Kanazawa University)
2A4	公開鍵暗号4		小貫啓史
2A4-1		BLS12曲線上のペアリングにおけるG2上の有理点生成の高速化	○飯田 智宏(岡山大学大学院自然科学研究科),服部 大地(岡山大学大学院自然科学研究科),松村 陸矢(岡山大学大学院自然科学研究科),南條 由紀(岡山大学大学院自然科学研究科),小寺 雄太(岡山大学大学院自然科学研究科),日下 卓也(岡山大学大学院自然科学研究科),野上 保之(岡山大学大学院自然科学研究科)
2A4-2		準同型暗号を用いたE2EE画像重ね合わせの検討	◎上野真奈(NTT社会情報研究所),光成滋生(サイボウズ・ラボ),小林鉄太郎(NTT社会情報研究所),村上啓造(NTT社会情報研究所)
2A4-3		Linked Data 型 Verifiable Credentials の構成と安全性	○山本 暖(株式会社インターネットイニシアティブ),須賀 祐治(株式会社インターネットイニシアティブ),佐古 和恵(早稲田大学)
2A4-4		複数の鍵生成局を持つ鍵失効機能付きIDベース暗号	◎鈴木裕大(神奈川大学),藤岡淳(神奈川大学),佐々木太良(神奈川大学),岡野裕樹(NTT社会情報研究所),永井彰(NTT社会情報研究所)
2B4	ネットワークセキュリティ3		菊池浩明
2B4-1		IoTマルウェア基礎情報の調査	○周家興(東京電機大学),寺田真敏(東京電機大学)
2B4-2		プロキシログから抽出した通信パターンによる異常検知	◎名倉 悠(大阪府立大学大学院人間社会システム科学研究科),青木 茂樹(大阪府立大学大学院人間社会システム科学研究科),宮本 貴朗(大阪府立大学大学院人間社会システム科学研究科)
2B4-3		文書類似性モデル評価手法による潜在意味解析に基づくセキュリティレポート検索の評価	○添田綾香(神戸大学),長澤龍成(神戸大学),白石善明(神戸大学),冨田裕涼(岐阜大学),箕浦翔悟(岐阜大学),毛利公美(岐阜大学),森井昌克(神戸大学)
2C4	ウェブセキュリティ2		江田智尊
2C4-1		深層強化学習によるWebアプリケーションのペネトレーションテストの自動化に向けて	○久野 朔(東京大学生産技術研究所),松浦 幹太(東京大学生産技術研究所)
2C4-2		フィッシングを識別するための機械学習におけるデータセットの影響	○中本 雄一(長崎県立大学),加藤 雅彦(長崎県立大学)
2C4-3		リクエストパラメータ変換によるWebアプリケーション脆弱性診断ツールの精度向上に関する研究	◎木村正太朗(情報セキュリティ大学院大学),大久保隆夫(情報セキュリティ大学院大学)
2C4-4		Google検索結果から当選詐欺サイトへのリダイレクトチェーンの収集自動化	◎白井 優武(東京電機大学大学院),三谷 和也(東京電機大学大学院),齊藤 泰一(東京電機大学)
2D4	ブロックチェーン3		面和成
2D4-1		LPWAネットワークに適したノード間分散台帳方式の分割に関する一考察	◎江口 力哉(早稲田大学),佐古 和恵(早稲田大学),徳武 孝紀(早稲田大学),丸山 優祐(早稲田大学),佐藤 俊雄(早稲田大学),余 恪平(早稲田大学),文 鄭(早稲田大学),斉 欣(早稲田大学),柴田 巧一(Skeed)
2D4-2		Interhead Hydra: Two Heads are Better than One	◎Maxim Jourenko(東京大学),Mario Larangeira(東京工業大学. IOHK),Keisuke Tanaka(東京工業大学)
2D4-3		LPWAネットワーク上の分散台帳を用いたポイント取引システムの端末設計	◎丸山 優祐(早稲田大学),佐古 和恵(早稲田大学),徳武 孝紀(早稲田大学),江口 力哉(早稲田大学),佐藤 俊雄(早稲田大学),余 恪平(早稲田大学),文 鄭(早稲田大学),斉 欣(早稲田大学),柴田 巧一(Skeed)
2D4-4		分散台帳への秘密鍵の封入による協同運用可能な公開鍵証明書発行基盤の実装と評価	◎熊谷圭太(名古屋工業大学),掛井将平(名古屋工業大学),白石善明(神戸大学),齋藤彰一(名古屋工業大学)
2E4	暗号プロトコル4		中西透
2E4-1		状態更新を含むプロトコルに対するTamarin Proverを用いたリプレイ攻撃の検証に向けて	◎佐藤瑞己(茨城大学),米山一樹(茨城大学)
2E4-2		ユーザの持つメモリが定数な検証可能な動的検索可能暗号	◎小澤響平(信州大学),山本博章(信州大学),藤原洋志(信州大学)
2E4-3		Malicious Private Key Generators in Identity-Based Authenticated Key Exchange	◎Kazuma Wariki(Kanagawa University Graduate School),Atsushi Fujioka(Kanagawa University),Taroh Sasaki(Kanagawa University),Kazuki Yoneyama(Ibaraki University),Yuki Okano(NTT Social Informatics Laboratories),Akira Nagai(NTT Social Informatics Laboratories),Koutarou Suzuki(Toyohashi University of Technology)
2E4-4		強フォワード秘匿性を満たす匿名一方向認証鍵交換	◎石橋 錬(茨城大学大学院理工学研究科),米山 一樹(茨城大学)
2F4	物理的暗号2		駒野雄一
2F4-1		シャッフル1回のみの秘密計算に必要なカード枚数について	◎葛馬知紀(東北大学),五十鈴川頼宗(東北大学),豊田航大(東北大学),宮原大輝(電気通信大学),水木 敬明(東北大学)
2F4-2		3値入力可能な可換半群の条件を満たす非コミットメント型AND演算拡張カードベースプロトコルの構成	○須賀祐治(株式会社インターネットイニシアティブ)
2F4-3		一様で閉じたシャッフルの効率的な実装	◎岩成慶太(電気通信大学),中井雄士(電気通信大学),渡邉洋平(電気通信大学/産業技術総合研究所),栃窪孝也(日本大学),岩本貢(電気通信大学)
2F4-4		カードベース暗号を題材にした小中学生向け授業の報告	○品川 和雅(茨城大学 / 産総研)
2A5	耐量子計算機暗号5		穴田啓晃
2A5-1		New Post-Quantum Digital Signature Scheme based on MinRank Problem	○Bagus Santoso(The University of Electro-Communications),Yasuhiko Ikematsu(Kyushu University),Shuhei Nakamura(Nihon University),Takanori Yasuda(Okayama University of Science)
2A5-2		適切な素数選択によるKLPTアルゴリズムを利用した同種写像構成計算	◎高橋 康(富士通株式会社),神戸 祐太(立教大学),安田 雅哉(立教大学),横山 和弘(立教大学)
2A5-3		Montgomery曲線のx座標を用いた3-同種計算の最小演算コスト	○守谷共起(東京大学),小貫啓史(東京大学),相川勇輔(三菱電機),高木剛(東京大学)
2A5-4		超特別アーベル多様体によるエクスパンダー族の構成とその暗号応用に向けて	◎相川勇輔(三菱電機),田中亮吉(京都大学),山内卓也(東北大学)
2B5	ネットワークセキュリティ4		平野学
2B5-1		逆引きDNSの登録状況とDNSSECの暗号アルゴリズムに関する実態調査	◎山口詩織(長崎県立大学),岡田雅之(長崎県立大学)
2B5-2		疑似攻撃ログによるAIを用いた攻撃検知技術の強化	○山本 匠(三菱電機株式会社),中井 綱人(三菱電機株式会社),大塚 瑠莉(三菱電機株式会社),Ye Wang(Mitsubishi Electric Research Laboratories),Kyeong Jin Kim(Mitsubishi Electric Research Laboratories),Toshiaki Koike-Akino(Mitsubishi Electric Research Laboratories),Iván Sanz Gorrachategui(University of Zaragoza),Aolin Ding(Rutgers University),阿部衛(東邦大学)
2B5-3		IoT環境における動的セキュリティ管理システム	◎竹内佑樹(法政大学),金井敦(法政大学),谷本茂明(千葉工業大学),佐藤周行(東京大学)
2B5-4		IPアドレスをサブジェクトに含んだWebサーバ証明書の調査と分析	○金岡 晃(東邦大学),小山 裕輝(東邦大学),岡田 雅之(長崎県立大学)
2C5	自動車セキュリティ2		菅原健
2C5-1		車載Ethernet環境におけるフロープローブの性能評価	◎加賀有貴(パナソニック株式会社),岸川剛(パナソニック株式会社),安達貴洋(パナソニック株式会社),平野亮(パナソニック株式会社),氏家良浩(パナソニック株式会社),芳賀智之(パナソニック株式会社),松島秀樹(パナソニック株式会社)
2C5-2		車載イーサネット向けイベント送信付き周期型通信における侵入検知手法の検討	◎増川 京佑(住友電気工業株式会社),塚本 博之(住友電気工業株式会社),福田 國統(住友電気工業株式会社),三好 孝典(住友電気工業株式会社),濱田 芳博(住友電気工業株式会社),上口 翔悟(株式会社オートネットワーク技術研究所),足立 直樹(株式会社オートネットワーク技術研究所),上田 浩史(株式会社オートネットワーク技術研究所)
2C5-3		サイバーキルチェーンに基づく車両における攻撃行動把握手法の検討	福田 國統(住友電気工業株式会社),○三好 孝典(住友電気工業株式会社),濱田 芳博(住友電気工業株式会社),礒山 芳一(住友電気工業株式会社),上田 浩史(株式会社オートネットワーク技術研究所)
2C5-4		Reputation Framework for VANETs from Blockchain Structure	○Maharage Nisansala Sevwandi Perera(Advanced Telecommunications Research Institute International),Toru Nakamura(KDDI Research),Masayuki Hashimoto(Advanced Telecommunications Research Institute International),Hiroyuki Yokoyama(Advanced Telecommunications Research Institute International),Chen-Mou Cheng(Kanazawa University),Kouichi Sakurai(Kyushu University)

2D5	AIセキュリティ５		矢内直人
2D5-1		AI認証：説明可能AIによるニューラルネットの識別	◎芦澤奈実(NTT社会情報研究所),鈴木亮平(NTT社会情報研究所),桐淵直人(NTT社会情報研究所),大木哲史(静岡大学大学院総合科学技術研究科),峰野博史(静岡大学大学院総合科学技術研究科),西垣正勝(静岡大学大学院総合科学技術研究科)
2D5-2		人工知能を伴う監視カメラによる全方位からの撮影に対する耐人物検出機能を持つ衣類の作成	◎金井 春輝(東京工科大学大学院),宇田 隆哉(東京工科大学大学院)
2D5-3		シンボルが削除されたIoTマルウェアにおける自然言語処理を用いた関数名推定	◎イボット アリジャン(筑波大学),大山 恵弘(筑波大学)
2E5	量子暗号１		早稲田篤志
2E5-1		拡張したMean King問題を応用した量子鍵配送の安全性の検討Ⅱ：識別可能性と情報攪乱	◎米田昌矢(大阪産業大学),吉田雅一(大阪産業大学)
2E5-2		Advantage of the key relay protocol over secure network coding	○加藤 豪(NTTコミュニケーション科学基礎研究所),藤原 幹生(NICT),鶴丸 豊広(三菱電機株式会社)
2E5-3		QMAに対するCertified Everlastingゼロ知識証明	◎廣岡 大河(京都大学基礎物理学研究所),森前 智行(京都大学基礎物理学研究所),西巻 陵(NTT社会情報研究所),山川 高志(NTT社会情報研究所)
2E5-4		Quantum-Accessible Security of Stateless Hash-based Signature Schemes	◎Quan YUAN(Kyoto University),Mehdi TIBOUCHI(NTT Laboratories. Kyoto University),Masayuki ABE(NTT Laboratories. Kyoto University)
2F5	物理的暗号３		真鍋義文
2F5-1		手札に関する不正者を検出可能な新しい秘密計算カードプロトコルの提案	○小泉康一(福島工業高等専門学校),大槻正伸(福島工業高等専門学校)
2F5-2		パイルスクランブルシャッフルからのグラフ自己同型シャッフルの構成	◎宮本 賢伍(茨城大学),品川 和雅(茨城大学 / 産総研)
2F5-3		有限群の一様分解とその一様閉シャッフルへの応用	金井 和貴(新潟大学),宮本 賢伍(茨城大学),○品川 和雅(茨城大学 / 産総研)
2F5-4		ハイパースペクトルカメラによるカードベース暗号の安全性評価に向けた基礎的検討	◎嶌野雅久(電気通信大学),宮原大輝(電気通信大学),崎山一男(電気通信大学)

Day 3 2022/1/20 (木)

番号	セッション名	発表タイトル	著者：◎登壇者（SCIS論文賞対象者）、○登壇者	座長
3A1	AIセキュリティ6			藤原啓成
3A1-1		ベイズ最適化を用いたデータ・クエリ効率の良いBlack-box Universal Adversarial Attacks	◎由比藤 真(茨城大学),米山 一樹(茨城大学)	
3A1-2		開発エンジニア向け機械学習セキュリティ脅威分析技術	○矢嶋純(富士通株式会社),及川孝徳(富士通株式会社),森川郁也(富士通株式会社),笠原史禎(富士通株式会社),乾真季(富士通株式会社),吉岡信和(早稲田大学)	
3A1-3		機械学習を用いたZigBeeネットワーク上の不正通信検知手法の提案	◎大塩智也(東洋大学),岡田怜士(東洋大学),松田亘(NTT),満永拓邦(東洋大学)	
3B1	自動車セキュリティ3			木田良一
3B1-1		AI safety とsecurity の研究動向：国際と国内・産学官	○櫻井 幸一(九州大学),溝口 誠一郎(DNVビジネスアシュアランスジャパン)	
3B1-2		人工知能搭載システムに対する安全性論証の現状とセキュリティ論証に向けた課題　～自動運転システムの例～	◎溝口 誠一郎(DNVビジネスアシュアランスジャパン株式会社),櫻井 幸一(九州大学大学院システム情報科学研究院)	
3B1-3		車載システムに対するデジタル・フォレンジックに向けての一考察	○味岡 仁雅(警察大学校),倉地 亮(名古屋大学),佐々木 崇光(パナソニック株式会社),黒崎 雄介(警察大学校),片山 隆成(警察大学校),下雅意 美紀(警察大学校)	
3B1-4		サイバーフィジカルシステムの効率の良いセキュリティ設計のためのリスク分析手順の検討	○川西 康之(住友電気工業株式会社),西原 秀明(産業技術総合研究所),吉田 博隆(産業技術総合研究所),山本 秀樹(住友電気工業株式会社)	
3B1-5		Observing CAN Message Timestamps on Automotive Testbeds	○Camille GAY(Yokohama National University / Toyota Motor Corporation),Tsutomu MATSUMOTO(Yokohama National University)	
3C1	ネットワークセキュリティ5			山内利宏
3C1-1		家庭を模したIoT家電ハニーポットを用いた攻撃者の行動の観測および検証	◎大塚瑠莉(三菱電機),吉岡克成(横浜国立大学大学院環境情報研究院/先端科学高等研究院),岡田晃市郎(株式会社レインフォレスト)	
3C1-2		IoTマルウェア配布サーバの継続的監視による検体遷移の調査	◎徐 競博(立命館大学),鄭 俊俊(立命館大学),毛利 公一(立命館大学)	
3C1-3		SDNを利用したセキュアなホームネットワーク	◎松永和也(法政大学),金井敦(法政大学),谷本茂明(千葉工業大学),佐藤周行(東京大学)	
3C1-4		SVMによるエ場ネットワークにおける偽装通信の検知手法のリアルタイム性の検証	◎原田雄基(東京工科大学大学院 コンピュータサイエンス専攻),布田裕一(東京工科大学 コンピュータサイエンス学部),岡崎裕之(信州大学 学術研究院(工学系))	
3D1	公開鍵暗号5			藤崎英一郎
3D1-1		ペアリング高速計算に適した楕円曲線における群所属判定	○安田貴徳(岡山理科大学),石井将大(東京工業大学),照屋唯紀(産業技術総合研究所)	
3D1-2		鍵付き準同型暗号における演算の拡張と安全性	◎篠木 寛騰(東京大学),縫田 光司(九州大学/産業技術総合研究所)	
3D1-3		帰着効率がタイトなhelper付きUnruh変換の提案と効率的なディジタル署名の構成	◎加藤拓(東京大学大学院情報理工学系研究科数理情報学専攻),古江弘樹(東京大学大学院情報理工学系研究科数理情報学専攻),高木剛(東京大学大学院情報理工学系研究科数理情報学専攻)	
3E1	秘密計算3			未定
3E1-1		秘密分散法による5ラウンド決定木評価	Naman Gupta(IIT Delhi),Aikaterini Mitrokotsa(University of St.Gallen),森田啓(University of St.Gallen),◎戸澤一成(東京大学)	
3E1-2		実数に対する四捨五入を利用した秘密分散法による秘匿計算方式の提案	◎納所勇之介(東京理科大学大学院),岩村恵市(東京理科大学大学院),稲村勝樹(広島市立大学大学院)	
3E1-3		秘密分散を用いた秘匿浮動小数点数除算・平方根計算の改良	◎仁平 貴大(東京大学大学院 情報理工学系研究科 数理情報学専攻),縫田 光司(九州大学/産業技術総合研究所)	
3E1-4		秘密計算ライブラリMEVAL3における乗算の高速化実装について	○橋本 順子(NTT社会情報研究所),五十嵐 大(NTT社会情報研究所),菊池 亮(NTT社会情報研究所)	
3F1	セキュリティ評価2			西出隆志
3F1-1		ドアを開け放したのは誰か？IoT機器のセキュリティ問題の改善に向けた根本原因調査	◎乃万 誉也(横浜国立大学大学院環境情報学府),佐々木 貴之(横浜国立大学先端科学高等研究院),神野 亮(株式会社ゼロゼロワン),荻原 雄一(株式会社ゼロゼロワン),志村 俊也(横浜国立大学情報基盤センター),吉岡 克成(横浜国立大学大学院環境情報研究院/先端科学高等研究院),松本 勉(横浜国立大学大学院環境情報研究院/先端科学高等研究院)	
3F1-2		Trust-awareなビジネス設計のためのビジネストラスト分析支援システム	○小牧 大治郎(富士通株式会社),笠波 昌昭(富士通株式会社),坂口 昌隆(富士通株式会社),山口 俊輔(富士通株式会社),野田 敏達(富士通株式会社),兒島 尚(富士通株式会社)	
3F1-3		ビジネストラスト分析のためのユースケース整理とパターン分析	○山口 俊輔(富士通株式会社),笠波 昌昭(富士通株式会社),小牧 大治郎(富士通株式会社),坂口 昌隆(富士通株式会社),野田 敏達(富士通株式会社),兒島 尚(富士通株式会社)	
3F1-4		ステークホルダー信頼関係図を用いたビジネストラスト分析手法	◎笠波 昌昭(富士通株式会社),坂口 昌隆(富士通株式会社),小牧 大治郎(富士通株式会社),山口 俊輔(富士通株式会社),野田 敏達(富士通株式会社),兒島 尚(富士通株式会社)	
3A2	AIセキュリティ7			大木哲史
3A2-1		メンバーシップ推論攻撃に対する交差蒸留を利用した防御手法	Rishav Chourasia(シンガポール国立大学),エンケタイワン バトニヤマ(NECセキュアシステム研究所),伊東 邦大(NECセキュアシステム研究所),◎森 隼基(NECセキュアシステム研究所),寺西 勇(NECセキュアシステム研究所),土田 光(NECセキュアシステム研究所)	
3A2-2		量子化誤差を考慮したAdversarial trainingの提案と評価	◎増田春樹(立命館大学),吉田康太(立命館大学),藤野毅(立命館大学)	
3A2-3		分布外データに対する脆弱性と検知	◎江田 智尊(富士通株式会社),森川 郁也(富士通株式会社)	
3A2-4		物体検出CNNに対する複数配置に着目した遠隔Adversarial Patch攻撃	◎大西健斗(三菱電機株式会社),中井綱人(三菱電機株式会社),鈴木大輔(三菱電機株式会社)	
3B2	プライバシー保護3			王立華
3B2-1		eKYCにおける安全な失効機能 - 中央銀行デジタル通貨のプライバシー保護	○宝木 和夫(産業技術総合研究所),久保田 隆(早稲田大学),ウォルゲムト スベン(セコム),梅澤 克之(湘南工科大学),小柳 洋貴(湘南工科大学),渡邊 創(産業技術総合研究所)	
3B2-2		糖尿病罹患リスクを予測するヘルスケアデータの匿名化コンテストPWS Cup 2021データの解析	○菊池 浩明(明治大学),馬 瑞強(明治大学)	
3B2-3		Webアクセス履歴データにおける本人一致率の評価	◎加藤拓弥(金沢大学),満保雅浩(金沢大学)	
3B2-4		Users' Interest in Algorithmic Transparency Aspects of Privacy Tools	○Vanessa Bracamonte(KDDI Research. Inc.),Takamasa Isohara(KDDI Research. Inc.)	
3C2	ハードウェアセキュリティ3			長谷川健人
3C2-1		敵対的サンプル攻撃を適用した回路設計情報におけるニューラルネットワークを用いたハードウェアトロイ識別に関する特徴量の検討	◎加藤友浩(早稲田大学基幹理工学部情報通信学科),山下一樹(早稲田大学大学院基幹理工学研究科),長谷川健人(株式会社KDDI総合研究所),披田野清良(株式会社KDDI総合研究所),清本晋作(株式会社KDDI総合研究所),戸川望(早稲田大学大学院基幹理工学研究科)	
3C2-2		高速RNSモンゴメリ乗算器の小面積化のためのパラメータ選択法	◎芳賀陸雄(奈良先端科学技術大学院大学),森本康太(奈良先端科学技術大学院大学),藤本大介(奈良先端科学技術大学院大学),川村信一(産学技術総合研究所),林優一(奈良先端科学技術大学院大学)	
3C2-3		物理的サイバー攻撃検知手法の一検討　ーハードウェアトロイの検知ー	◎西田 泰太(住友電気工業株式会社),清水 晶太(住友電気工業株式会社),櫻澤 聡(住友電気工業株式会社),伊澤 真人(住友電気工業株式会社),加藤 勇夫(住友電気工業株式会社)	
3C2-4		ナノ人工物メトリックシステムの実験的精度評価	◎高濱阜史郎(横浜国立大学),吉田直樹(横浜国立大学),松本 勉(横浜国立大学)	
3D2	暗号プロトコル5			未定
3D2-1		低リソースデバイス制御のための匿名放送型認証技術の提案	○青野 良範(情報通信研究機構),四方 順司(横浜国立大学)	
3D2-2		LWE問題を用いたマジック状態生成機能の検証	◎竹内 勇貴(NTT コミュニケーション科学基礎研究所),水谷 明博(三菱電機株式会社 情報技術総合研究所),廣政 良(三菱電機株式会社 情報技術総合研究所),相川 勇輔(三菱電機株式会社 情報技術総合研究所),谷 誠一郎(NTT コミュニケーション科学基礎研究所)	
3D2-3		高効率な失効機能付きIDベース認証鍵交換の構成	◎中川 皓平(NTT社会情報研究所),割木 寿将(神奈川大学),岡野 裕樹(NTT社会情報研究所),藤岡 淳(神奈川大学),永井 彰(NTT社会情報研究所)	
3D2-4		QUICへのIDベース認証鍵交換TFNSの適用と実装評価	○村上啓造(NTT社会情報研究所),岡野裕樹(NTT社会情報研究所),青木信雄(広島市立大学),永井彰(NTT社会情報研究所)	
3D2-5		追跡可能集約署名に対する潜在的な攻撃とその対処法に関する考察	○山下恭佑(産業技術総合研究所),石井龍(東京大学/産業技術総合研究所),照屋唯紀(産業技術総合研究所),坂井祐介(産業技術総合研究所),花岡悟一郎(産業技術総合研究所),松浦幹太(東京大学),松本勉(横浜国立大学/産業技術総合研究所)	
3E2	ブロックチェーン4			尾形わかは
3E2-1		分散台帳技術におけるユーザの同意に基づくアクセス制御フレームワーク	○掛井将平(名古屋工業大学),今村光良(野村アセットマネジメント株式会社),白石善明(神戸大学),廣友雅徳(佐賀大学),齋藤彰一(名古屋工業大学)	
3E2-2		Comparison of transaction cost on different fair exchange protocols	◎HUAN ZHANG(Kyoto university),Mehdi Tibouchi(NTT Corporation. Kyoto university),Miguel Ambrona(NTT Corporation),Masayuki Abe(NTT Corporation. Kyoto university)	
3E2-3		トークン型電子現金方式のCentral Bank Digital Currency(CBDC) への適用可能性に関する初期検討	◎荒川幸寛(京都大学大学院),奥田哲矢(ＮＴＴ社会情報研究所),齋藤恆和(ＮＴＴ社会情報研究所),ティブシ・メディ(ＮＴＴ社会情報研究所),阿部正幸(ＮＴＴ社会情報研究所)	

3F2	ウェブセキュリティ３			齊藤泰一
3F2-1		Private Relayアクセスにおける端末識別の試み	◎渡名喜 瑞稀(明治大学大学院),神 章洋(明治大学大学院),利光 能直(明治大学大学院),髙山 眞樹(明治大学大学院),齋藤 孝道(明治大学)	
3F2-2		レスポンスの情報を用いたWebAPIのアクセスコントロールに関する脆弱性診断方式	◎田谷 透(東京情報大学大学院 総合情報学研究科),花田 真樹(東京情報大学 総合情報学部),村上 洋一(東京情報大学 総合情報学部),早稲田 篤志(東京情報大学 総合情報学部),石田 裕貴(株式会社セキュアブレイン),三村 隆夫(株式会社セキュアブレイン),布広 永示(東京情報大学 総合情報学部)	
3F2-3		WebAuthnを基にしたWebサービスにおける端末追加のためのプロトコルの評価	◎網川澪(北海道情報大学),福光正幸(北海道情報大学)	
3F2-4		セキュアチャネル上の認証プロトコルの形式検証	◎中林 美郷(NTT 社会情報研究所),奥田 哲矢(NTT 社会情報研究所)	
3F2-5		MITB攻撃対象の傾向分析と脅威情報活用に関する考察	○高田一樹(株式会社セキュアブレイン),太刀川剛(株式会社セキュアブレイン),内田隆徳(ジェノアテクノロジーズ株式会社),邦本理夫(株式会社セキュアブレイン)	
3A3	暗号理論３			平野貴人
3A3-1		Algebraic Group Model上でのSchnorr署名のMulti-User Securityに関する一考察	○福光 正幸(北海道情報大学),長谷川 真吾(東北大学)	
3A3-2		モノの秘匿性を考慮した「モノの電子署名」	◎林 リウヤ(東京大学生産技術研究所 / 産業技術総合研究所),浅野 泰輝(東京大学生産技術研究所 / 産業技術総合研究所),林田 淳一郎(東京大学生産技術研究所 / 産業技術総合研究所),松田 隆宏(産業技術総合研究所),山田 翔太(産業技術総合研究所),勝又 秀一(産業技術総合研究所),坂井 祐介(産業技術総合研究所),照屋 唯紀(産業技術総合研究所),シュルツ ヤコブ(産業技術総合研究所),アッタラパドゥン ナッタポン(産業技術総合研究所),花岡 悟一郎(産業技術総合研究所),松浦 幹太(東京大学生産技術研究所),松本 勉(横浜国立大学大学院/産業技術総合研究所)	
3A3-3		対話的追跡機能付き集約署名における署名送信間隔に関する制約と評価	◎石井 龍(産業技術総合研究所 / 東京大学),山下 恭佑(産業技術総合研究所),宋 子豪(横浜国立大学),照屋 唯紀(産業技術総合研究所),坂井 祐介(産業技術総合研究所),花岡 悟一郎(産業技術総合研究所),松浦 幹太(東京大学),松本 勉(産業技術総合研究所 / 横浜国立大学)	
3A3-4		組み合わせ AONT の安全性に関するエントロピー解析	◎赤尾 奏名汰(九州大学大学院 システム情報科学府),顧 玉杰(九州大学大学院 システム情報科学研究院),櫻井 幸一(九州大学大学院 システム情報科学研究院)	
3A3-5		暗号プロトコルの転用性と堅固性：歴史と現状と課題	○櫻井 幸一(九州大学)	
3A3-6		「モノの電子署名」の複数物体への拡張	◎浅野 泰輝(東京大学生産技術研究所),林 リウヤ(東京大学生産技術研究所. 産業技術総合研究所),林田 淳一郎(東京大学生産技術研究所. 産業技術総合研究所),松田 隆宏(産業技術総合研究所),山田 翔太(産業技術総合研究所),勝又 秀一(産業技術総合研究所),坂井 祐介(産業技術総合研究所),照屋 唯紀(産業技術総合研究所),シュルツ ヤコブ(産業技術総合研究所),アッタラパドゥン ナッタポン(産業技術総合研究所),花岡 悟一郎(産業技術総合研究所),松浦 幹太(東京大学生産技術研究所),松本 勉(横浜国立大学大学院/産業技術総合研究所)	
3B3	生体認証・バイオメトリクス２			未定
3B3-1		加飾印刷技術とマルチモーダル人工物メトリクス（第2報）	◎于圣昆(工学院大学),種崎湧斗(工学院大学),藤川真樹(工学院大学),七井靖(防衛大学校)	
3B3-2		Face Parsingを用いた顔認証モデルの解釈	◎河合洋弥(東北大学),神津岳志(東北大学),伊藤康一(東北大学),Hwann-Tzong Chen(National Tsing Hua University),青木孝文(東北大学)	
3B3-3		位置情報を活用した認証手法における認証精度と検知時間との関係	○小林良輔(三菱電機インフォメーションシステムズ株式会社),山口利恵(東京大学)	
3B3-4		特徴量間のユークリッド距離を類似度とするキャンセラブルバイオメトリクス	◎肥後春菜(NEC),一色寿幸(NEC),森健吾(NEC),尾花賢(法政大学)	
3C3	ハードウェアセキュリティ４			梨本翔永
3C3-1		レーザーを用いた MEMS 圧力センサへのシグナルインジェクション攻撃	◎田中 樹(電気通信大学),菅原 健(電気通信大学)	
3C3-2		高速フーリエ変換と機械学習を用いたIoT機器の異常検知	○木田良一(株式会社ラック),金子博一(株式会社ラック)	
3C3-3		PMBusのセキュリティに関する一考察	◎岡田 悠聖(長崎県立大学),塩原 孝弘(TDK株式会社),加藤 雅彦(長崎県立大学)	
3C3-4		ワクチン低温物流に関わる温度センサのアナログサイバーセキュリティ	ヤン ロン(ミシガン大学),サラ ランパッジ(フロリダ大学),○菅原 健(電気通信大学),ケビン フー(ミシガン大学)	
3C3-5		レーザー振動計を用いた MLCC からの音響サイドチャネルリークの測定	◎土井康平(電気通信大学),菅原 健(電気通信大学)	
3D3	システムセキュリティ６			木藤圭亮
3D3-1		fastTextとLSTMを用いたマルウェア検知手法の提案	◎岸端 晃毅(岩手県立大学 ソフトウェア情報学研究科),成田 匡輝(岩手県立大学 ソフトウェア情報学研究科)	
3D3-2		VMMを用いたプログラム実行時の証拠取得機能における取得対象の拡張と改ざん耐性の向上	◎伊藤 寛史(岡山大学 大学院自然科学研究科),中村 徹(KDDI総合研究所/国際電気通信基礎技術研究所),磯原 隆将(KDDI総合研究所),山内 利宏(文字数制限のため，コメントに記載)	
3D3-3		IoT機器における効率的な真贋判定方式	○千葉伸浩(NTT社会情報研究所),瀧口浩義(NTT社会情報研究所),中嶋良彰(NTT社会情報研究所)	
3D3-4		ゼロトラストを利用したIRMによる情報流出対策の考察	◎宇野 正人(東京通信大学),角尾 幸保(東京通信大学)	
3D3-5		NASを標的とするランサムウェア攻撃のハニーポットと動的解析による分析	◎安井浩基(横浜国立大学),井上貴弘(横浜国立大学),佐々木貴之(横浜国立大学先端科学高等研究院),田辺瑠偉(横浜国立大学先端科学高等研究院),吉岡克成(横浜国立大学大学院環境情報研究院/先端科学高等研究院),松本勉(横浜国立大学大学院環境情報研究院/先端科学高等研究院)	
3E3	秘密計算４			未定
3E3-1		大規模データにも対応した秘密計算階層型クラスタリング	○三品気吹(NTT社会情報研究所),五十嵐大(NTT社会情報研究所),濱田浩気(NTT社会情報研究所),菊池亮(NTT社会情報研究所)	
3E3-2		秘匿SQL Window関数プロトコルの提案	◎須藤 弘貴(NTT社会情報研究所),菊池 亮(NTT社会情報研究所)	
3E3-3		データベースの等結合後に加重合計を求める秘密計算プロトコル	○富田潤一(NTT),紀伊真昇(NTT),濱田浩気(NTT),市川敦謙(NTT),千田浩司(NTT)	
3E3-4		プライバシを保護したRNNによる非対話型文書分類	◎齋藤拓巳(東京工業大学),岡響(アイマトリックス研究所株式会社),中橋彬(アイマトリックス研究所株式会社),尾形わかは(東京工業大学)	
3E3-5		多項式補間による整数型準同型大小比較/除算の改良	◎森村洸生(筑波大学),西出隆志(筑波大学)	
3E3-6		出力埋め込み可能な紛失擬似ランダム関数に基づく多者間秘匿積集合プロトコルの効率化	◎清水 聖也(電気通信大学),中井 雄士(電気通信大学),渡邉 洋平(電気通信大学 / 産業技術総合研究所),岩本 貢(電気通信大学)	
3F3	コンテンツ保護 I			鳥居直哉
3F3-1		オンライン会議システム上の画面キャプチャによる情報漏洩の対策の一検討	○鎌苅康大(岡山大学),栗林稔(岡山大学),舩曳信生(岡山大学)	
3F3-2		準同型暗号を用いたOpaque Predicateの提案	◎平能 耀介(茨城大学),大瀧 保広(茨城大学)	
3F3-3		Intel SGXを用いたアルゴリズム変換型プロキシ再暗号化システムの実装・評価	◎西平 侑磨(東海大学),鈴木 達也(筑波大学),渡邉 英伸(広島大学),大東 俊博(東海大学/情報通信研究機構)	
3F3-4		Secure codes with two-stage traitor tracing	○顧 玉杰(九州大学)	

Day 4 2022/1/21 (金)

番号	セッション名	発表タイトル	著者：◎登壇者（SCIS論文賞対象者）、○登壇者	座長
4A1	公開鍵暗号6			米山一樹
4A1-1		Optimal Lattice Trapdoor for the Klein-GPV and Peikert Sampler	◎Chao Sun(Kyoto University),Thomas Espitau(NTT Corporation),Mehdi Tibouchi(NTT Corporation. Kyoto University),Masayuki Abe(NTT Corporation. Kyoto University)	
4A1-2		上質の電子署名アルゴリズム	○安田 英幸(個人)	
4A1-3		位数が4kの有限体上楕円曲線の点の位数の判定法	○白勢政明(公立はこだて未来大学)	
4A1-4		F4-styleアルゴリズムのMQ問題に対する多項式選択方法	◎伊藤琢真(情報通信研究機構),黒川貴司(情報通信研究機構),篠原直行(情報通信研究機構),内山成憲(東京都立大学)	
4B1	ネットワークセキュリティ6			細井琢朗
4B1-1		Attack graphを用いたサイバーレンジシナリオの自動生成	○中田亮太郎(一橋大学),大塚 玲(情報セキュリティ大学院大学)	
4B1-2		SDN-based Detection Method against DoS/DDoS attacks in an IoT environment	◎Abdul Adhim(東洋大学),Satoshi Okada(東洋大学),Takuho Mitsunaga(東洋大学)	
4B1-3		SDNを用いたDDoS攻撃に対する防御機構構築	◎徳山 凌(東京工科大学大学院 コンピュータサイエンス専攻),布田 裕一(東京工科大学 コンピュータサイエンス学部),鈴木 彦文(信州大学 総合情報センター),岡崎 裕之(信州大学 学術研究院(工学系))	
4B1-4		追跡可能集約署名プロトコルのためのクラウド上シミュレータの提案とプロトタイプ実装	◎宋 子豪(横浜国立大学),安西 陸(横浜国立大学),坂本 純一(横浜国立大学/産業技術総合研究所),吉田 直樹(横浜国立大学),松本 勉(横浜国立大学)	
4B1-5		Rust言語によるフィルタ機能を付加したソフトウェアブリッジの実装と検証	◎細谷 昂平(大阪大学大学院),高野 祐輝(大阪大学大学院),宮地 充子(大阪大学大学院)	
4C1	サイドチャネル攻撃4			宮原大輝
4C1-1		Efficient Modular Inversion Resisting Side Channel Attack	◎Yaoan Jin(大阪大学工学研究科),Atsuko Miyaji(大阪大学工学研究科)	
4C1-2		PIN認証プログラムへの命令改変フォールト攻撃の形式的影響評価	◎林 俊吾(横浜国立大学),坂本 純一(横浜国立大学/産業技術総合研究所),松本 勉(横浜国立大学)	
4C1-3		マスキング対策実装に対するサイドチャネル攻撃成功確率の情報理論的解析	○伊東燦(東北大学工学研究科),上野嶺(東北大学電気通信研究所),本間尚文(東北大学電気通信研究所)	
4C1-4		FPGA実装したAES回路の模擬スイッチング電流波形に基づくサイドチャネル情報漏洩帯域の考察	◎下田洸平(岡山大学),日室雅貴(岡山大学),豊田啓孝(岡山大学),五百旗頭健吾(岡山大学)	
4D1	システムセキュリティ7			鈴木大輔
4D1-1		制御システムに対する脆弱性を考慮したスーパーバイザの設計	◎小川寛太(電気通信大学),阪田恒晟(電気通信大学),澤田賢治(電気通信大学)	
4D1-2		制御システムにおけるインシデント発生後の状態復帰動作の導出方法	◎池田佳輝(電気通信大学),阪田恒晟(電気通信大学),澤田賢治(電気通信大学),藤田淳也(日立製作所),松本典剛(日立製作所)	
4D1-3		シーケンス制御システムに対するホワイトリスト式異常検知のための正常状態遷移のモデル化	◎藤田真太郎(電気通信大学),澤田賢治(電気通信大学)	
4E1	共通鍵暗号3			青木和麻呂
4E1-1		軽量ブロック暗号CHAMに対するBit-based Division Property Using Three Subsetsを用いたIntegral攻撃	◎中曽根 彰人(東京理科大学),五十嵐 保隆(東京理科大学)	
4E1-2		PMACrx：ベクトル入力をサポートする高安全なメッセージ認証コード	◎笠原 颯登(名古屋大学),岩田 哲(名古屋大学)	
4E1-3		単一鍵のTweakableブロック暗号を用いたブロック暗号の安全性	◎辻 健斗(名古屋大学),岩田 哲(名古屋大学)	
4E1-4		NIST軽量暗号最終候補におけるソフトウェア実装性能の評価	◎北原 知明(電気通信大学),日良 僚太 (電気通信大学),原 祐子 (東京工業大学),宮原 大輝(電気通信大学), 李 陽(電気通信大学),崎山 一男(電気通信大学)	
4F1	教育・心理学3			藤田真浩
4F1-1		現実的な攻撃モデルを通した主成分分析のプライバシー的観点からの考察	◎山城大海(筑波大学),面和成(筑波大学)	
4F1-2		コロナ禍におけるセキュリティ・インシデント被害等に対する株価の反応に関する分析	竹村 敏彦(城西大学),○小山 明美(独立行政法人情報処理推進機構),小川 隆一(独立行政法人情報処理推進機構)	
4F1-3		情報モラル教育ゲームの開発（Part.2-2）（情報モラル指導モデルカリキュラム表：e3-1とe3-2の実装と評価）	◎澤田 匡佑(工学院大学大学院 工学研究科情報学専攻),池原 元(工学院大学大学院 工学研究科情報学専攻),藤川 真樹(工学院大学 情報学部)	
4F1-4		顔認証システムの人種バイアスに影響を与える潜在的要因の調査	◎佐藤 佑哉(静岡大学情報学部),土屋 純(静岡大学大学院総合科学技術研究科),成田 惇(静岡大学大学院総合科学技術研究科),西垣 正勝(静岡大学大学院総合科学技術研究科),大木 哲史(静岡大学大学院総合科学技術研究科)	
4F1-5		ブラックボックス型モデル反転攻撃におけるユーザ類似性を考慮した生成モデルの検討	◎井田 天星(静岡大学),竹内 廉(静岡大学),ヴォ ゴック コイ グエン(静岡大学),西垣 正勝(静岡大学),大木 哲史(静岡大学)	
4A2	耐量子計算機暗号6			相川勇輔
4A2-1		Multi-Parallel MMTアルゴリズムによる高次元SDPの解読	◎成定 真太郎(KDDI総合研究所),福島 和英(KDDI総合研究所),清本 晋作(KDDI総合研究所)	
4A2-2		Tuple Sieve Algorithmの並列化の提案	◎Keiichi Imai(Japan Advanced Institute of Science and Technology),Yuntao Wang(Japan Advanced Institute of Science and Technology),Eiichiro Fujisaki(Japan Advanced Institute of Science and Technology)	
4A2-3		トレース写像を用いたRing-LWE問題に対する格子攻撃の再考	○奥村伸也(大阪大学),上村周作(東京大学),工藤桃成(東京大学)	
4B2	システムセキュリティ8			森彰
4B2-1		関数呼び出しグラフと関数埋め込みに基づくマルウェア分類手法	◎林 実奈美(警察大学校),大坪 雄平(警察大学校),大塚 玲(情報セキュリティ大学院大学)	
4B2-2		多点観測型多要素認証：単一クレデンシャルによる多要素認証の達成	◎野崎 真之介(静岡大学),芹澤 歩弥(静岡大学),吉平 瑞穂(静岡大学),藤田 真浩(三菱電機株式会社),柴田 陽一(三菱電機株式会社),山中 忠和(三菱電機株式会社),松田 規(三菱電機株式会社),大木 哲史(静岡大学),西垣 正勝(静岡大学)	
4B2-3		IoTアクチュエータにおけるセキュリティの一考察	○小林信博(長崎県立大学シーボルト校)	
4B2-4		サイバー攻撃に対するレジリエントな縮退運転システムの設計と実装	◎阪田恒晟(電気通信大学),藤田真太郎(電気通信大学),澤田賢治(電気通信大学),遠藤 浩通(日立製作所),松本 典剛(日立製作所)	
4B2-5		Enabling Integrity Protection for GitOps based Application Deployment	◎Kugamoorthy Gajananan(IBM Research - Tokyo),Yuji Watanabe(IBM Research - Tokyo),Hirokuni Kitahara(IBM Research - Tokyo),Ruriko Kudo(IBM Research - Tokyo)	
4C2	ハードウェアセキュリティ5			白勢政明
4C2-1		BLS12-381曲線上ペアリング計算の低レイテンシFPGA実装	◎安西 陸(横浜国立大学),坂本 純一(産業技術総合研究所/横浜国立大学),宋 子豪(横浜国立大学),吉田 直樹(横浜国立大学),松本 勉(横浜国立大学)	
4C2-2		車載カメラの車両・人物検出に対する色調改変攻撃とその対策	○上田晋生(横浜国立大学),一ノ瀬竜矢(横浜国立大学),吉田直樹(横浜国立大学),松本勉(横浜国立大学)	
4C2-3		物理的障壁を考慮した超音波による接触通知フレームワークの提案	◎相場 智也(静岡大学情報学部),土屋 純(静岡大学大学院総合科学技術研究科),成田 惇(静岡大学大学院総合科学技術研究科),西垣 正勝(静岡大学大学院総合科学技術研究科),大木 哲史(静岡大学大学院総合科学技術研究科)	
4C2-4		LiDARベース物体認識システムの攻撃耐性評価用シミュレータ	◎一ノ瀬竜矢(横浜国立大学),上田晋生(横浜国立大学),深津勇貴(横浜国立大学),久保中(横浜国立大学),吉田直樹(横浜国立大学),松本勉(横浜国立大学)	
4C2-5		グラフ学習にもとづく不正回路検知に対する強化学習を用いた自律的な脆弱性検査の提案	◎長谷川 健人(KDDI総合研究所),披田野 清良(KDDI総合研究所),福島 和英(KDDI総合研究所)	
4D2	ブロックチェーン5			花谷嘉一
4D2-1		信頼度を用いた実用的なProof of Personhoodプロトコルの提案	◎兵頭昇虎(東京工業大学),尾形わかは(東京工業大学)	
4D2-2		公開ブロックチェーンのためのプライバシー保護データ共有フレームワーク	◎丁 曄澎(東京大学),佐藤 周行(東京大学)	
4D2-3		自律分散型組織DAOの匿名環境下における内部告発手法	◎津田匠貴(九州工業大学),荒木俊輔(九州工業大学),正田英樹(九州工業大学),安土茂亨(九州工業大学),田中貴規(九州工業大学),中城元臣(九州工業大学)	
4D2-4		分散型アイデンティティの永続的利用とプライバシー保護	○坂本拓也(富士通株式会社),牛田芽生恵(富士通株式会社),福岡尊(富士通株式会社),森永正信(富士通株式会社)	
4D2-5		鍵紛失時における非常ボタン式資金退避手法の実装と評価	○松崎 なつめ(長崎県立大学),喜多 義弘(長崎県立大学)	
4D2-6		検証可能なマッチング方式の一提案	◎福岡　尊(富士通株式会社),坂本　拓也(富士通株式会社),牛田　芽生恵(富士通株式会社)	
4E2	秘密計算5			千田浩司
4E2-1		整数型平文空間における非線形2変数準同型演算の高速化	◎前田大輔(筑波大学),西出隆志(筑波大学)	
4E2-2		準同型暗号に基づく秘密計算の能動的攻撃者に対する秘匿性について	○縫田 光司(九州大学/産業技術総合研究所)	
4E2-3		ブロック暗号RAGHAVの高階差分特性	○芝山 直喜(航空自衛隊),五十嵐 保隆(東京理科大学)	
4E2-4		Google Adiantumに対する量子攻撃	◎栗原昂汰(名古屋大学),岩田哲(名古屋大学)	
4E2-5		WPA2/WPA3無線LAN機器に対する新たなDoS攻撃とその効果	◎西井大智(神戸大学),中嶋祥吾(神戸大学),白石善明(神戸大学),森井昌克(神戸大学)	
4F2	セキュリティ評価3			未定
4F2-1		デジタルフォレンジック調査選定に資するリスクコミュニケータの提案	◎佐々木 葵(静岡大学),天笠 智哉(静岡大学),井坂 佑介(静岡大学),奥村 紗名(静岡大学),堀川 博史(静岡大学),村上 弘和(CyCraft Japan),大木 哲史(静岡大学),西垣 正勝(静岡大学)	
4F2-2		電子証明書を取り巻く仕組みの分析とその活用	◎野村 健太(デロイトトーマツサイバー合同会社),高田 雄太(デロイトトーマツサイバー合同会社),熊谷 裕志(デロイトトーマツサイバー合同会社),神薗 雅紀(デロイトトーマツサイバー合同会社),白石 善明(神戸大学)	
4F2-3		データ流通におけるトラスト管理モデルの技術的課題分析	○磯原 隆将(KDDI総合研究所),中村 徹(KDDI総合研究所),清本 晋作(KDDI総合研究所),田中 俊昭(兵庫県立大学大学院)	
4F2-4		Theoretical Security against adversarial examples on Gaussian Processes	◎前嶋啓彰(情報セキュリティ大学院大学; NTTテクノクロス株式会社),大塚玲(情報セキュリティ大学院大学)	
4F2-5		機械学習ベースマルウェア検知モデルに対するclean-labelバックドア攻撃とその対策について	○鄭万嘉(筑波大学),面和成(筑波大学)	