2015年暗号と情報セキュリティシンポジウム（SCIS2015）セッション一覧表

2015年1月20～23日　リーガロイヤルホテル小倉

SCIS2015 実行委員会

1日目（1/20）

会場名		13:00–14:00	14:00–14:30	14:30–16:10		16:10–16:30	16:30–18:10	
ロイヤル3(4F)		招待講演 ロイヤル(4F)	休憩	ネットワークセキュリティ	1A1	休憩	Webセキュリティ(1)	1A2
ロイヤル2(4F)				実装(1)	1B1		コンテンツ保護	1B2
ロイヤル1(4F)				公開鍵暗号(1)	1C1		公開鍵暗号(2)	1C2
ダイヤモンド(4F)				共通鍵暗号(1)	1D1		共通鍵暗号(2)	1D2
オーキッド(3F)				暗号プロトコル(1)	1E1		暗号プロトコル(2)	1E2
クリスタル(3F)				バイオメトリクス(1)	1F1		楕円曲線暗号(1)	1F2

2日目（1/21）

	9:00–10:40		10:40 – 11:00	11:00–12:40		12:40–14:20	14:20–16:00		16:00–16:20	16:20–18:00		18:00–19:30	19:30–21:30
ロイヤル3(4F)	マルウェア対策(1)	2A1	休憩	マルウェア対策(2)	2A2	昼食	ネットワーク攻撃検知・対策(1)	2A3	休憩	ネットワーク攻撃検知・対策(2)	2A4	休憩	懇親会 ロイヤル(4F)
ロイヤル2(4F)	実装(2)	2B1		実装(3)	2B2		バイオメトリクス(2)	2B3		楕円曲線暗号(2)	2B4		
ロイヤル1(4F)	認証(1)	2C1		認証(2)	2C2		プライバシー保護(1)	2C3		自動車セキュリティ(1)	2C4		
ダイヤモンド(4F)	情報理論的安全性(1)	2D1		情報理論的安全性(2)	2D2		IDベース暗号	2D3		暗号理論(1)	2D4		
オーキッド(3F)	共通鍵暗号(3)	2E1		共通鍵暗号(4)	2E2		署名(1)	2E3		署名(2)	2E4		
クリスタル(3F)	暗号化状態処理(1)	2F1		暗号化状態処理(2)	2F2		サイドチャネル攻撃(1)	2F3		サイドチャネル攻撃(2)	2F4		

3日目（1/22）

会場名	9:00–10:40		10:40 – 11:00	11:00–12:40		12:40–14:20	14:20–16:00		16:00–16:20	16:20–18:00		18:00–19:00	19:00–21:00
ロイヤル3(4F)	サイドチャネル攻撃(3)	3A1	休憩	サイドチャネル攻撃(4)	3A2	昼食	サイドチャネル攻撃(5)	3A3	休憩	特別講演（16:20–17:20）	3A4	休憩	ナイトセッション ロイヤル(4F)
ロイヤル2(4F)	プライバシー保護(2)	3B1		バイオテンプレート保護	3B2		ユビキタスセキュリティ	3B3		ソフトウェア保護	3B4		
ロイヤル1(4F)	セキュリティ評価・モデル(1)	3C1		自動車セキュリティ(2)	3C2		組み込みセキュリティ	3C3		プライバシー保護(3)	3C4		
ダイヤモンド(4F)	数論応用	3D1		暗号理論(2)	3D2		暗号理論(3)	3D3		暗号理論(4)	3D4		
オーキッド(3F)	Webセキュリティ(2)	3E1		公開鍵暗号(3)	3E2		公開鍵暗号(4)	3E3		暗号化状態処理(3)	3E4		
クリスタル(3F)	暗号プロトコル(3)	3F1		暗号プロトコル(4)	3F2		暗号プロトコル(5)	3F3		暗号プロトコル(6)	3F4		

4日目（1/23）

会場名	9:00–10:40		10:40 – 11:00	11:00–12:40	
ロイヤル3(4F)	モバイルセキュリティ(1)	4A1	休憩	モバイルセキュリティ(2)	4A2
ロイヤル2(4F)	プライバシー保護(4)	4B1		クラウドセキュリティ	4B2
ロイヤル1(4F)	セキュリティ評価・モデル(2)	4C1		認証(3)	4C2
ダイヤモンド(4F)	教育・心理学	4D1		電子透かし	4D2
オーキッド(3F)	乱数(1)	4E1		乱数(2)	4E2
クリスタル(3F)	情報理論的安全性(3)・量子セキュリティ	4F1		フォーマルメソッド	4F2

2015年暗号と情報セキュリティシンポジウムプログラム

招待講演　1月20日 (火)　13:00—14:00

世界におけるサイバー攻撃の現状と対策に関するヒント ～ 今、我々が考えるべきこと ～

伊東 寛 (株式会社ラック 常務理事 ナショナルセキュリティ研究所 所長)

1A1　ネットワークセキュリティ　1月20日 (火)　14:30—16:10

1A1-1　A Behavior-based Engine for Detecting Distributed Internet Attacks and its Performance Investigation

○フォン ヤオカイ (九州大学), 堀 良彰 (佐賀大学), 櫻井 幸一 (九州大学)

1A1-2　挙動に基づくポートスキャン検知手法に向けたパラメータなしの学習アルゴリズムの提案とその性能評価

◎王サン (九州大学/九州先端科学技術研究所), フォンヤオカイ (九州大学/九州先端科学技術研究所), 川本 淳平 (九州大学/九州先端科学技術研究所), 堀良彰 (佐賀大学/九州先端科学技術研究所), 櫻井幸一 (九州大学/九州先端科学技術研究所)

1A1-3　SDN セキュリティ研究動向 －現状と課題－

○堀良彰 (佐賀大学/ISIT), 松本晋一 (九州大学/ISIT), 山内一将 (九州大学/ISIT), 梶原直也 (九州大学/ISIT), 川本淳平 (九州大学/ISIT), 櫻井幸一 (九州大学/ISIT)

1A1-4　識別子による DDoS パケット・フィルタリング

◎鈴木涼太 (神奈川大学大学院工学研究科), 増田和明 (神奈川大学工学部), 森田光 (神奈川大学大学院工学研究科)

1B1　実装 (1)　1月20日 (火)　14:30—16:10

1B1-1　Efficient Implementation of Lattice-based Cryptosystems using JavaScript

◎ Yuan Ye (Kyushu University), Chen-Mou Cheng (Taiwan National University/Kyushu University), Shinsaku Kiyomoto (KDDI Laboratories), Yutaka Miyake (KDDI Laboratories), Tsuyoshi Takagi (Kyushu University, CREST JST)

1B1-2　効率的な固定点マルチスカラー倍算の提案

○川原 祐人 (NTT セキュアプラットフォーム研究所), 小林 鉄太郎 (NTT セキュアプラットフォーム研究所)

1B1-3　A Task Decomposition Based Concurrent Parser for Large Scale Code Checking

○安藤類央 (情報通信研究機構)

1B1-4　Minalpher の x86_64 最適化実装

○青木和麻呂 (NTT), 藤堂洋介 (NTT)

1B1-5　組織暗号の実証実験－自治体における個人情報保護に向けて

○才所敏明 (中央大学研究開発機構), 近藤健 (中央大学研究開発機構), 庄司陽彦 (中央大学研究開発機構), 沼田秀穂 (事業創造大学院大学), 仙石正和 (事業創造大学院大学), 辻井重男 (中央大学研究開発機構)

1C1　公開鍵暗号 (1)　1月20日 (火)　14:30—16:10

1C1-1　結託攻撃に対する再暗号化鍵偽造不可能性を達成するプロキシ再暗号化方式

○林 良太郎 (株式会社 東芝 研究開発センター), 松下 達之 (株式会社 東芝 研究開発センター)

1C1-2　識別不可性難読化に基づく復号の速い代理再暗号化について

○大畑幸矢 (東京大学), 松浦幹太 (東京大学)

1C1-3　公開鍵暗号の平文空間を拡げる漸近的に非常に効率的な方法

○松田 隆宏 (産業技術総合研究所 セキュアシステム研究部門), 花岡 悟一郎 (産業技術総合研究所 セキュアシステム研究部門)

1C1-4　Dual Conversion for Attribute Based Encryption

○ Nuttapong Attrapadung (AIST), Shota Yamada (AIST)

1C1-5　単純な転送規則により転送負荷を軽減した組織暗号の一実装

◎宮本 樹 (大阪電気通信大学), 村上 恭通 (大阪電気通信大学/中央大学研究開発機構)

1D1　共通鍵暗号 (1)　1月20日 (火)　14:30—16:10

1D1-1　KCipher-2 の非線形関数部における構成部品の線形確率

◎中山大介 (東京理科大学), 金子敏信 (東京理科大学)

1D1-2　ストリーム暗号 KCipher-2 の差分攻撃耐性評価

◎西尾 彬 (東京理科大学大学院理工学研究科電気工学専攻), 金子 敏信 (東京理科大学大学院理工学研究科電気工学専攻)

1D1-3　Impossible Differential Attack against 14-Round Piccolo-80 without Relying on Full Code Book

◎ Yosuke Todo (NTT Secure Platform Laboratories)

1D1-4　正規言語を用いた鍵更新可能暗号の安全性解析

◎大宮 翔児 (電気通信大学), 徳重 佑樹 (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)

1E1　暗号プロトコル (1)　1 月 20 日 (火)　14:30—16:10

1E1-1　プライバシーを保護するパターンマッチングプロトコルに関する一考察

○黒木 智也 (北九州市立大学), 佐藤 敬 (北九州市立大学)

1E1-2　プライバシーを考慮した安定ルームメイト問題

◎小嶋 健太 (工学院大学), 真鍋 義文 (工学院大学)

1E1-3　オニオンルーティングの一方式における通信文非結合性問題について

◎佐藤寛悟 (工学院大学), 真鍋義文 (工学院大学)

1E1-4　多値化された秘密分散法の安全性

◎高橋加寿子 (東京理科大学工学研究科電気工学専攻), 須賀祐治 (株式会社インターネットイニシアティブ), 岩村惠市 (東京理科大学工学研究科電気工学専攻)

1E1-5　ツケ払いに適した楽観的公平交換

Jae Hong Seo (Myongji University), 江村 恵太 (NICT), 草川 恵太 (NTT セキュアプラットフォーム研究所), ○米山 一樹 (NTT セキュアプラットフォーム研究所)

1F1　バイオメトリクス (1)　1 月 20 日 (火)　14:30—16:10

1F1-1　モバイルデバイス用手のひら静脈認証ユーザーインターフェース評価

○青木隆浩 (株式会社富士通研究所)

1F1-2　Eye Movement による個人識別方式に関する一検討

◎安部 登樹 (株式会社富士通研究所), 新崎 卓 (株式会社富士通研究所)

1F1-3　尤度比判定に基づくマルチモーダル生体認証に対するモダリティ選択攻撃

○村上 隆夫 (産業技術総合研究所 セキュアシステム研究部門), 高橋 健太 (日立製作所 横浜研究所)

1F1-4　人工物を用いた生体認証装置の性能評価法の提案

○上田周誠 (中央大学理工学部・産業総合技術研究所), 大木哲史 (産業総合技術研究所), 大塚玲 (産業総合技術研究所), 今井秀樹 (東京大学)

1A2　Web セキュリティ (1)　1 月 20 日 (火)　16:30—18:10

1A2-1　SSLv3 の延命技術〜SSLv3 は本当に死んだのか

○須賀祐治 (株式会社インターネットイニシアティブ)

1A2-2　マルチサインオン; 認証コレクターの提案

◎石塚 貴 (神奈川工科大学 大学院), 岡本学 (神奈川工科大学 大学院)

1A2-3　OpenSocial における信頼情報に基づくアクセス制御手法の提案

◎浦邊 信太郎 (株式会社 日立ソリューションズ東日本), 児玉 英一郎 (岩手県立大学 ソフトウェア情報学部), 王 家宏 (岩手県立大学 ソフトウェア情報学部), 高田 豊雄 (岩手県立大学 ソフトウェア情報学部)

1A2-4　SPKI 権限証明書を用いた権限委譲方式の実装

◎渡邉 貴文 (明治大学大学院), 大丸 雅人 (明治大学大学院), 磯 侑斗 (明治大学大学院), 西倉 裕太 (明治大学大学院), 宮田 大地 (明治大学), 齋藤 孝道 (明治大学)

1B2　コンテンツ保護　1 月 20 日 (火)　16:30—18:10

1B2-1　3D プリンター用デジタルデータの著作権保護技術

○鈴木雅洋 (神奈川工科大学), ピヤラット シラパスパコォンウォン (神奈川工科大学), 上平員丈 (神奈川工科大学), 高嶋洋一 (NTT サービスエボリューション研究所), 海野浩 (神奈川工科大学)

1B2-2　秘匿領域を有する高密度二次元コードの互換性と識別性に関するスマートフォン実装による評価

〇寺浦 信之 (九州大学), 櫻井 幸一 (九州大学)

1B2-3　Study on Scoring Function of Binary Fingerprinting Codes

〇 Minoru Kuribayashi (Kobe University)

1B2-4　コンテンツベースの情報追跡システムの試作と評価

小櫻文彦 (株式会社富士通研究所), 山岡裕司 (株式会社富士通研究所), 〇伊藤孝一 (株式会社富士通研究所), 津田宏 (株式会社富士通研究所)

1B2-5　コンテンツベースの情報追跡システムの高速化

〇小櫻文彦 (富士通研究所), 山岡裕司 (富士通研究所), 伊藤孝一 (富士通研究所), 津田宏 (富士通研究所)

1C2　公開鍵暗号 (2)　1 月 20 日 (火)　16:30—18:10

1C2-1　開示機能を有する再暗号化鍵匿名プロキシ再暗号化方式

〇冨田雅博 (千葉大学大学院融合科学研究科), 岸本渡 (千葉大学大学院融合科学研究科)

1C2-2　ナップザック型暗号の解読における新しい格子構成ついて

〇境隆一 (大阪電気通信大学), 笠原正雄 (中央大学、早稲田大学)

1C2-3　非可換環を用いた NTRU 方式の拡張

〇安田貴徳 (九州先端科学技術研究所), グザヴィエ・ダハン (お茶の水女子大学), 櫻井幸一 (九州大学、九州先端科学技術研究所)

1D2　共通鍵暗号 (2)　1 月 20 日 (火)　16:30—18:10

1D2-1　平文制御を用いた確率的高階差分特性による TWINE の安全性評価

◎小菅 悠久 (防衛大学校), 岩井 啓輔 (防衛大学校), 田中 秀磨 (防衛大学校), 黒川 恭一 (防衛大学校)

1D2-2　TWINE の新しい高階差分特性

〇芝山直喜 (航空自衛隊), 金子敏信 (東京理科大学)

1D2-3　Involution 性を備えた共通鍵暗号の設計

◎藤堂 洋介 (NTT セキュアプラットフォーム研究所), 菅原 健 (三菱電機株式会社), 村上 ユミコ (三菱電機株式会社), 青木 和麿呂 (NTT セキュアプラットフォーム研究所), 松井 充 (三菱電機株式会社)

1E2　暗号プロトコル (2)　1 月 20 日 (火)　16:30—18:10

1E2-1　ゲノムプライバシ保護を考慮した紛失通信プロトコル

◎照屋唯紀 (産業技術総合研究所), 縫田光司 (産業技術総合研究所 / JST さきがけ), 清水佳奈 (産業技術総合研究所), 花岡悟一郎 (産業技術総合研究所)

1E2-2　正多角形カードを用いた秘密計算プロトコル

◎品川和雅 (筑波大学/産総研), 水木敬明 (東北大学), 縫田光司 (産総研), 金山直樹 (筑波大学), 西出隆志 (筑波大学), 岡本栄司 (筑波大学)

1E2-3　通信量の少ない 3 者計算

〇古川 潤 (日本電気株式会社)

1E2-4　更新を考慮したプライバシ保護協調フィルタリング

◎望月宥志 (工学院大学), 真鍋義文 (工学院大学)

1E2-5　Threshold Two-Move Password Authenticated Key Exchange Protocol

◎京極 達也 (京都大学大学院情報学研究科), 李ミンソン (京都大学大学院情報学研究科), 阿部 正幸 (NTT セキュアプラットフォーム研究所), 岡本 龍明 (NTT セキュアプラットフォーム研究所)

1F2　楕円曲線暗号 (1)　1 月 20 日 (火)　16:30—18:10

1F2-1　GHS 攻撃の対象となる奇標数素数次数拡大体上の楕円曲線 その 2

〇飯島 努 ((株) 光電製作所), 趙 晋輝 (中央大学)

1F2-2　Differential Fault Attacks in a GLS curve

◎ TAECHAN KIM (NTT Secure Platform Laboratories), MEHDI TIBOUCHI (NTT Secure Platform Laboratories)

1F2-3　Sutherland の位数計算法について

磯田 遼 (神奈川大学理学部情報科学科), ○松尾 和人 (神奈川大学理学部情報科学科)

1F2-4　Barreto-Naehrig 曲線に関して

○星野 文学 (NTT セキュアプラットフォーム研究所)

1F2-5　P と 2P の座標に着目する楕円曲線スカラー倍の高速化

○白勢 政明 (公立はこだて未来大学)

2A1　マルウェア対策 (1)　1 月 21 日 (水)　9:00—10:40

2A1-1　暗号ロジック特定手法の提案 その 2

山本 匠 (三菱電機株式会社 情報技術総合研究所), ◎西川 弘毅 (三菱電機株式会社 情報技術総合研究所), 河内 清人 (三菱電機株式会社 情報技術総合研究所), 中嶋 純子 (三菱電機株式会社 情報技術総合研究所), 桜井 鐘治 (三菱電機株式会社 情報技術総合研究所)

2A1-2　動的解析ログの API を用いた機能に基づくマルウェア分類

◎川口 直人 (北陸先端科学技術大学院大学), 面 和成 (北陸先端科学技術大学院大学)

2A1-3　脆弱性評価及び Opcode を用いた Drive-by-Download 攻撃予測手法の提案

◎安達貴志 (北陸先端科学技術大学院大学情報科学研究科), 面和成 (北陸先端科学技術大学院大学情報科学研究科)

2A1-4　近年のハニーポット取得データ解析による C&C トラフィック分類評価

◎山内 一将 (九州大学/九州先端科学技術研究所), 川本 淳平 (九州大学/九州先端科学技術研究所), 堀 良彰 (佐賀大学/九州先端科学技術研究所), 櫻井 幸一 (九州大学/九州先端科学技術研究所)

2A1-5　ホスト型 IDS を用いた不審プロセスの特定

○中里 純二 (情報通信研究機構), 津田 侑 (情報通信研究機構), 高木 彌一郎 (情報通信研究機構), 衛藤 将史 (情報通信研究機構), 井上 大介 (情報通信研究機構), 中尾 康二 (情報通信研究機構)

2B1　実装 (2)　1 月 21 日 (水)　9:00—10:40

2B1-1　多項式環表現を用いた GF(2^8) 合成体逆元演算器の設計

◎上野嶺 (東北大学), 本間尚文 (東北大学), 菅原幸弘 (東北大学), 青木孝文 (東北大学)

2B1-2　再帰関数に対する秘匿計算の実装

◎黒河徳大 (埼玉大学), 小玉新悟 (埼玉大学), 小柴健史 (埼玉大学)

2B1-3　レーザフォールト攻撃に耐性のある論理ゲートの基礎検討と実験評価

◎中野 将志 (立命館大学大学院理工学研究科), 汐崎 充 (立命館大学大学院総合理工学研究機構), 藤野 毅 (立命館大学理工学部)

2B1-4　自己破壊的耐タンパーソフトウェアの試験実装

大石 和臣 (静岡理工科大学), ◎吉田 直樹 (横浜国立大学), 渡邉 直紀 (横浜国立大学), 坂本 純一 (横浜国立大学), 松本 勉 (横浜国立大学)

2C1　認証 (1)　1 月 21 日 (水)　9:00—10:40

2C1-1　共通 1-day パスワード認証システム

糸井 正幸 (株式会社セフティーアングル), ○多田 充 (千葉大学)

2C1-2　About User Anonymity in Password-based Anonymous Authentication

○ SeongHan Shin (AIST), Kazukuni Kobara (AIST)

2C1-3　ユーザビリティ向上のための部分的パスワード共有による影響

◎湯澤 孝介 (金沢大学), 安永 憲司 (金沢大学), 満保 雅浩 (金沢大学)

2C1-4　パターンロックの覗き見耐性向上手法について

◎東川創 (金沢大学), 満保雅浩 (金沢大学)

2C1-5　CHAP のみで多要素認証を実現するプロトコル

○稲村勝樹 (東京電機大学/産業技術総合研究所)

2D1　情報理論的安全性 (1)　1 月 21 日 (水)　9:00—10:40

2D1-1　Matsumoto-Imai 中間写像の Tame 分解に関する考察

◎矢城 信吾 (九州大学大学院), 高木 剛 (九州大学 マス・フォア・インダストリ研究所)

2D1-2　暗号文の耐改変性と復号権限の変更機能をもつ情報理論的に安全な放送型暗号

◎渡邉 洋平 (横浜国立大学/産業技術総合研究所), 花岡 悟一郎 (産業技術総合研究所), 四方 順司 (横浜国立大学)

2D1-3　情報理論的に安全な順序検証機能付き多重認証方式

◎富田信一朗 (横浜国立大学), 渡邉洋平 (横浜国立大学), 四方順司 (横浜国立大学)

2D1-4　推測成功確率に基づいた安全性基準をみたす秘密分散法

○岩本貢 (電気通信大学), 四方順司 (横浜国立大学)

2D1-5　推測確率に基づいた安全性基準をみたす暗号化方式の構成法

岩本 貢 (電気通信大学), ○四方 順司 (横浜国立大学)

2E1　共通鍵暗号 (3)　1 月 21 日 (水)　9:00—10:40

2E1-1　改ざん検知暗号 Minalpher

佐々木 悠 (ＮＴＴ), 藤堂 洋介 (ＮＴＴ), 青木 和麻呂 (ＮＴＴ), 内藤 祐介 (三菱電機), 菅原 健 (三菱電機), 村上 ユミコ (三菱電機), ○松井 充 (三菱電機), 廣瀬 勝一 (福井大), 高橋 克巳 (ＮＴＴ)

2E1-2　Integral Attack に対する SPECK32 の安全性評価

◎先小山 翔 (神戸大学大学院), 森井 昌克 (神戸大学大学院)

2E1-3　Simon48 に対する Integral 攻撃

◎飯塚 大貴 (神戸大学大学院工学研究科), 藤堂 洋介 (NTT セキュアプラットフォーム研究所), 森井 昌克 (神戸大学大学院工学研究科)

2E1-4　23 段のブロック暗号 HIGHT への Splice-and-Cut 技法を用いた中間一致攻撃

○五十嵐保隆 (鹿児島大学), 金子敏信 (東京理科大学), 瀬戸口聡 (鹿児島大学), 福島誠治 (鹿児島大学), 八野知博 (鹿児島大学)

2E1-5　Evaluation of an Approach for Security Enhancement of Certain Lightweight Stream Ciphers

○ Miodrag Mihaljevic (Institute of Industrial Science, The University of Tokyo), Kanta Matsuura (Institute of Industrial Science, The University of Tokyo)

2F1　暗号化状態処理 (1)　1 月 21 日 (水)　9:00—10:40

2F1-1　Anonymity for Fully Homomorphic Encryption

◎ Ryosuke Nakata (Tokyo Institute of Technology), Keisuke Tanaka (Tokyo Institute of Technology, JST)

2F1-2　準同型暗号による秘匿統計計算

○安田雅哉 (株式会社富士通研究所), 下山武司 (株式会社富士通研究所), 小暮淳 (株式会社富士通研究所)

2F1-3　Ring-LWE ベースの準同型暗号の実装

○下山武司 (富士通研究所), 安田雅哉 (富士通研究所), 小暮淳 (富士通研究所)

2F1-4　ある CKA2 安全な検索可能暗号方式のトラップドアサイズを削減するための安全な分割手法

○平野 貴人 (三菱電機株式会社), 川合 豊 (三菱電機株式会社), 岩本 貢 (電気通信大学), 太田 和夫 (電気通信大学)

2F1-5　クラウドストレージにおけるメッセージと鍵の準同型性を用いた情報保管プロトコルの提案

◎武菁 (九州工業大学), 大内悠馬 (九州工業大学), 荒木俊輔 (九州工業大学), 宮崎武 (北九州市立大学), 上原聡 (北九州市立大学), 礒崎賢一 (九州工業大学)

2A2　マルウェア対策 (2)　1 月 21 日 (水)　11:00—12:40

2A2-1　Man-in-the-Browser 攻撃を検出可能なトランザクション認証手法の提案

○半田 富己男 (大日本印刷株式会社), 矢野 義博 (大日本印刷株式会社)

2A2-2　特徴選択によるマルウェアの最適化レベル推定精度向上

◎包 含 (東京大学), 碓井 利宣 (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)

2A2-3　マルウェア検知および分類に向けたコンパイラ再最適化

◎碓井 利宣 (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)

2A2-4　Linux ディストリビューションにおける Buffer Overflow 攻撃への対策技術の適応状況

◎馬場 隆彰 (明治大学), 金子 洋平 (明治大学大学院), 鈴木 舞音 (明治大学大学院), 上原 崇史 (明治大学大学院), 角田 佳史 (明治大学大学院), 宮崎 博行 (明治大学), 齋藤 孝道 (明治大学)

2A2-5　リリースされたバイナリに適用するスタックベース BoF 攻撃緩和技術の試作と評価

○齋藤 孝道 (明治大学), 上原 崇史 (明治大学大学院), 金子 洋平 (明治大学大学院), 鈴木 舞音 (明治大学大学院), 角田 佳史 (明治大学大学院), 堀 洋輔 (明治大学大学院), 馬場 隆彰 (明治大学), 宮崎 博行 (明治大学)

2B2　実装 (3)　1 月 21 日 (水)　11:00—12:40

2B2-1　PUF の出力値を用いる鍵導出技術の得失比較

○駒野 雄一 (株式会社 東芝), 清水 秀夫 (株式会社 東芝)

2B2-2　MDR-ROM を用いてサイドチャネル攻撃対策 AES と PUF を実現した鍵生成 LSI の実装評価

◎竹内章浩 (立命館大学), 西村隆志 (立命館大学), 汐崎充 (立命館大学), 藤野毅 (立命館大学)

2B2-3　FIB 加工とプローブ測定に対する RS ラッチの挙動（I）

○鳥居 直哉 (富士通研究所), 山本 大 (富士通研究所), 武仲 正彦 (富士通研究所), 松本 勉 (横浜国立大学)

2B2-4　FIB 加工とプローブ測定に対する RS ラッチの挙動（II）

○山本 大 (富士通研究所), 鳥居 直哉 (富士通研究所), 武仲 正彦 (富士通研究所), 松本 勉 (横浜国立大学)

2C2　認証 (2)　1 月 21 日 (水)　11:00—12:40

2C2-1　ID ベース暗号による IoT 向け相互認証方式の提案

○酒見由美 (株式会社富士通研究所), 武仲正彦 (株式会社富士通研究所), 金岡晃 (東邦大学)

2C2-2　SymPC を用いた通過端末を確認可能な認証プロトコル

◎大内悠馬 (九州工業大学), 荒木俊輔 (九州工業大学), 碓崎賢一 (九州工業大学)

2C2-3　IEEE 802.21d のグループ鍵配布プロトコルの安全性証明

○花谷 嘉一 (株式会社 東芝), 大場 義洋 (株式会社 東芝)

2C2-4　なりすましを困難にする耐タンパハードウェアを用いた認証技術

◎清村 優太郎 (NTT セキュアプラットフォーム研究所), 吉田 麗生 (NTT セキュアプラットフォーム研究所), 山本 具英 (NTT セキュアプラットフォーム研究所), 小林 鉄太郎 (NTT セキュアプラットフォーム研究所)

2C2-5　可変長タグによるメッセージ認証の提案とその安全性の考察

○村上ユミコ (三菱電機株式会社), 小林信博 (三菱電機株式会社)

2D2　情報理論的安全性 (2)　1 月 21 日 (水)　11:00—12:40

2D2-1　Wiretap Channels with Side Information at the Transmitter

○ Hachiro Fujita (Tokyo Metropolitan University)

2D2-2　複数のパスワードを考慮したパスワード認証付き秘密分散法

◎野崎 隆之 (神奈川大学), 平間 大樹 (神奈川大学), 藤岡 淳 (神奈川大学)

2D2-3　改ざん攻撃を検出できる (n,n) および (2,n) しきい値秘密分散法

◎中村 渉 (東京大学), 山本 博資 (東京大学)

2D2-4　Improvement of Robust Secret Sharing with Optimal Cheater Resiliency

Partha Sarathi Roy (University of Calcutta, India), Avishek Adhikari (University of Calcutta, India), Rui Xu (Kyushu University, Japan), ○ Kirill Morozov (Kyushu University, Japan), Kouichi Sakurai (Kyushu University, Japan)

2E2　共通鍵暗号 (4)　1 月 21 日 (水)　11:00—12:40

2E2-1　CLOC における Tweak 関数の最適性

◎小林 隼人 (名古屋大学), 峯松 一彦 (日本電気株式会社), 岩田 哲 (名古屋大学)

2E2-2　オンライン認証暗号の衝突解析

◎白仁友康 (中央大学大学院), 峯松一彦 (日本電気株式会社)

2E2-3　WPA における RC4 の内部状態に関する新しい線形相関

◎伊藤竜馬 (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, JST CREST)

2E2-4　Joux-Lucks の 3-collisions 探索アルゴリズムに対する改良および計算量の詳細な検討

◎鴨志田 優一 (電気通信大学), 徳重 佑樹 (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)

2F2　暗号化状態処理 (2)　1 月 21 日 (水)　11:00—12:40

2F2-1　置換を平文とする準同型暗号から完全準同型暗号を構成する方法

○縫田 光司 (産業技術総合研究所/JST さきがけ)

2F2-2　Somewhat 準同型暗号上の行列ベクトル積の為の効率的なパッキング手法

◎陸 文杰 (筑波大学), 佐久間 淳 (筑波大学 JST CREST)

2F2-3　Canetti-Halevi-Katz 変換による代理人再暗号化方式の一般的構成法

河西 真瑠那 (横浜国立大学), ○清藤 武暢 (日本銀行), 渡邉 洋平 (横浜国立大学), 四方 順司 (横浜国立大学)

2F2-4　セキュリティアップデータブル準同型暗号を用いた秘匿データの線形回帰計算

○青野 良範 (情報通信研究機構), 林 卓也 (情報通信研究機構), レ チュウ フォン (情報通信研究機構), 王 立華 (情報通信研究機構)

2F2-5　プライバシー保護条件付き情報開示 III

辻井重男 (中央大学 研究開発機構), ○只木孝太郎 (中央大学 研究開発機構)

2A3　ネットワーク攻撃検知・対策 (1)　1 月 21 日 (水)　14:20—16:00

2A3-1　早期対応を目的とした統合型 DRDoS 攻撃観測システムの構築

○牧田大佑 (情報通信研究機構/横浜国立大学), 西添友美 (横浜国立大学), 小出駿 (横浜国立大学), 筒見拓也 (横浜国立大学), 金井文宏 (横浜国立大学), 森博志 (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), 井上大介 (情報通信研究機構), 中尾康二 (情報通信研究機構)

2A3-2　プロトコル非準拠のハニーポットによる DRDoS 攻撃の観測

◎西添友美 (横浜国立大学), 牧田大佑 (横浜国立大学/情報通信研究機構), 吉岡克成 (横浜国立大学), 松本勉 (横浜国立大学)

2A3-3　ハニーポット監視による DRDoS 攻撃の早期規模推定

◎浦川 順平 (株式会社 KDDI 研究所), 澤谷 雪子 (株式会社 KDDI 研究所), 山田 明 (株式会社 KDDI 研究所), 窪田 歩 (株式会社 KDDI 研究所), 牧田 大祐 (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)

2A3-4　DNS ログ解析による悪性 Web サイト抽出法と解析への影響を考慮した匿名化手法の提案

◎田中 晃太郎 (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)

2A3-5　スパース構造学習を用いたボットネット検出法の性能評価

◎向井脩 (九州大学), 川村勇気 (九州大学), 川喜田雅則 (九州大学), 竹内純一 (九州大学)

2B3　バイオメトリクス (2)　1 月 21 日 (水)　14:20—16:00

2B3-1　スマートフォン上で得られるタッチ情報を利用した手書きサイン認証システムに関する研究

◎田中優輝 (東京理科大学大学院), 吉田孝博 (東京理科大学大学院), 半谷精一郎 (東京理科大学大学院)

2B3-2　CELP エンコーダのコードブック情報を利用する話者認証の検討

◎西澤直樹 (東京理科大学大学院), 吉田孝博 (東京理科大学大学院), 半谷精一郎 (東京理科大学大学院)

2B3-3　スマートフォンにおけるキーストロークダイナミクスの移動状態に関する一検討

◎高橋 央弥 (岩手県立大学 ソフトウェア情報学部), 小倉 加奈代 (岩手県立大学 ソフトウェア情報学部), ベッド B. ビスタ (岩手県立大学 ソフトウェア情報学部), 高田 豊雄 (岩手県立大学 ソフトウェア情報学部)

2B3-4　FOCS データベースを用いた目の画像の照合に関する検討

○伊藤 康一 (東北大学), 青山 章一郎 (東北大学), 草薙 大地 (東北大学), 青木 孝文 (東北大学)

2C3　プライバシー保護 (1)　1 月 21 日 (水)　14:20—16:00

2C3-1　A Robust and Computation-Efficient Multi-Server PIR Protocol using Preprocessing

◎ Vannet Thomas (東京大学), Kunihiro Noboru (東京大学)

2C3-2　直交ランダム射影を用いた秘匿内積プロトコル

○菊池 浩明 (明治大学)

2C3-3　複数体上 Active モデルで秘匿性・正当性を保証する秘密分散ベース秘密計算と高速秘密計算ソートへの応用

○五十嵐大 (NTT セキュアプラットフォーム研究所), 菊池亮 (NTT セキュアプラットフォーム研究所), 濱田浩気 (NTT セキュアプラットフォーム研究所), 千田浩司 (NTT セキュアプラットフォーム研究所)

2C3-4　改ざん検知機能付きの実用的な秘密計算システム MEVAL2

◎菊池亮 (NTT セキュアプラットフォーム研究所), 五十嵐大 (NTT セキュアプラットフォーム研究所), 濱田浩気 (NTT セキュアプラットフォーム研究所), 千田浩司 (NTT セキュアプラットフォーム研究所)

2C3-5　キーに重複がある場合の秘密計算向け結合アルゴリズム

○濱田 浩気 (NTT セキュアプラットフォーム研究所), 桐淵 直人 (NTT セキュアプラットフォーム研究所), 五十嵐 大 (NTT セキュアプラットフォーム研究所)

2D3　ID ベース暗号　1 月 21 日 (水)　14:20—16:00

2D3-1　決定性プッシュダウンオートマトンを用いた関数型暗号

◎戸出 光一 (埼玉大学), 小柴健史 (埼玉大学)

2D3-2　Attribute-Based Signatures from Proof of Knowledge of Signatures

○ Hiroaki Anada (Institute of Systems, Information Technologies and Nanotechnologies (ISIT)), Seiko Arita (Institute of Information Security (IISEC)), Kouichi Sakurai (Department of Informatics, Graduate School of ISEE Faculty, Kyushu University)

2D3-3　部分一致検索可能暗号の効率化に向けて

○川合 豊 (三菱電機株式会社), 平野 貴人 (三菱電機株式会社)

2D3-4　CCA 安全かつ暗号文長が短い鍵失効機能付き ID ベース暗号の構成法

◎石田 優 (横浜国立大学), 渡邉 洋平 (横浜国立大学), 四方 順司 (横浜国立大学)

2E3　署名 (1)　1 月 21 日 (水)　14:20—16:00

2E3-1　群構造維持署名に関する考察

○村谷博文 (東芝)

2E3-2　関連鍵攻撃に対する Schnorr 署名方式の安全性について

◎森田 啓 (名大 産総研), 松田 隆宏 (産総研), 花岡 悟一郎 (産総研), 岩田 哲 (名大)

2E3-3　A Secure Signature Scheme with Tight Reduction to the RSA Assumption from Indistinguishability Obfuscation

◎三桝 雄大 (京都大学), 阿部 正幸 (京都大学, NTT セキュアプラットフォーム研究所), 岡本 龍明 (京都大学, NTT セキュアプラットフォーム研究所)

2E3-4　Fail-Stop 署名方式の Q-UC 安全性と結合定理

○野村 昌弘 (千葉大学), 中村 勝洋 (千葉大学)

2F3　サイドチャネル攻撃 (1)　1 月 21 日 (水)　14:20—16:00

2F3-1　内部電流波形に基づく AES 回路のサイドチャネル情報漏洩特性の考察

○五百旗頭健吾 (岡山大学), 田井伸拓 (岡山大学), 籠谷裕人 (岡山大学), 大西紘之 (岡山大学), 前島一仁 (岡山大学), 豊田啓孝 (岡山大学), 渡辺哲史 (岡山県工業技術センター)

2F3-2　Shamir のしきい値法における Cold-Boot Attack による秘密の復元の効率化

○高橋 一馬 (東京工業大学大学院), 尾形 わかは (東京工業大学)

2F3-3　誤り付 AES 鍵スケジュール復元アルゴリズム

◎谷垣友喜 (東京大学), 國廣昇 (東京大学)

2F3-4　レジスタに値を保持しているだけで生じる静的なサイドチャネルリーク

◎中井綱人 (立命館大学大学院), 汐崎充 (立命館大学大学院), 久保田貴也 (立命館大学大学院), 菅原健 (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)

2F3-5　命令置換フォールト攻撃とその対策

◎坂本 純一 (横浜国立大学), 大野 仁 (横浜国立大学), 土屋 遊 (横浜国立大学), 中田 量子 (横浜国立大学), 松本 勉 (横浜国立大学)

2A4　ネットワーク攻撃検知・対策 (2)　1 月 21 日 (水)　16:20—18:00

2A4-1　標的型攻撃ハニーポットにおける業務ネットワーク模擬方法の検討

○河内 清人 (三菱電機株式会社), 桜井 鐘治 (三菱電機株式会社)

2A4-2　攻撃シナリオを用いたログ相関分析によるサイバー攻撃検知

○榊原 裕之 (三菱電機株式会社 情報技術総合研究所), 居城 秀明 (三菱電機株式会社 情報技術総合研究所), 桜井 鐘治 (三菱電機株式会社 情報技術総合研究所)

2A4-3　産業制御システムにおける侵入検知手法の調査と検討

○山口 晃由 (三菱電機 (株)), 清水 孝一 (三菱電機 (株)), 小林 信博 (三菱電機 (株))

2A4-4　攻撃シナリオを用いたサイバー攻撃検知方式におけるシステムの監視負荷低減手法の提案

◎居城 秀明 (三菱電機株式会社), 榊原 裕之 (三菱電機株式会社), 河内 清人 (三菱電機株式会社), 桜井 鐘治 (三菱電機株式会社)

2A4-5　組織内ネットワークにおける標的型攻撃の振る舞い検知に向けた複数センサ連携手法

◎山田 正弘 (富士通株式会社), 森永 正信 (富士通株式会社), 海野 由紀 (富士通株式会社), 鳥居 悟 (富士通株式会社), 武仲 正彦 (富士通株式会社)

2B4　楕円曲線暗号 (2)　1 月 21 日 (水)　16:20—18:00

2B4-1　70 台程度の計算機を並列に用いた 94bit の ECDLP の解読

◎三好俊介 (岡山大学), 野上保之 (岡山大学), 日下卓也 (岡山大学), 山井成良 (東京農工大学)

2B4-2　超特異楕円曲線とそのツイスト曲線との関係

◎赤木 晶一 (岡山大学), 野上 保之 (岡山大学)

2B4-3　ペアリング計算高速化へ向けたパラメータ設定

○米村智子 (株式会社東芝), 高木剛 (九州大学)

2B4-4　Double-Triple の公式を用いた新しいスカラー倍算

◎高橋良太 (JAIST), 宮地充子 (JAIST, JST CREST)

2B4-5　暗号方式のペアリング群タイプの変換可能性に対する多項式時間判定アルゴリズムの提案

◎丹後偉也 (京都大学大学院 情報学研究科 社会情報学専攻), 阿部正幸 (NTT セキュアプラットフォーム研究所), 岡本龍明 (NTT セキュアプラットフォーム研究所), 大久保美也子 (NICT ネットワークセキュリティ研究所)

2C4　自動車セキュリティ(1)　1 月 21 日 (水)　16:20—18:00

2C4-1　CAN における再同期を利用した電気的データ改ざん

松本 勉 (横浜国立大学), ◎中山淑文 (横浜国立大学), 向達泰希 (横浜国立大学), 土屋 遊 (横浜国立大学), 吉岡克成 (横浜国立大学)

2C4-2　車載 ECU に対する CAN 経由のファジング手法

松本 勉 (横浜国立大学), ◎小林優希 (横浜国立大学), 土屋 遊 (横浜国立大学), 吉田直樹 (横浜国立大学), 森田伸義 ((株) 日立製作所), 萱島 信 ((株) 日立製作所)

2C4-3　車載 CAN 通信暗号化デモシステムの構築とサイドチャネル攻撃評価

○久保田貴也 (立命館大学 総合科学技術研究機構), 中野将志 (立命館大学 理工学研究科), 倉地亮 (名古屋大学 大学院情報科学研究科), 本田晋也 (名古屋大学 大学院情報科学研究科), 汐崎充 (立命館大学 総合科学技術研究機構), 藤野毅 (立命館大学 理工学部)

2C4-4　攻撃メッセージの無効化機能を備えたホワイトリスト CAN ハブ

○矢嶋純 (富士通研究所), 武仲正彦 (富士通研究所), 長谷部高行 (富士通研究所)

2C4-5　車載システムにおける低電圧時のマルウェア挙動

◎田中卓 (兵庫県立大学院), 大久保隆夫 (情報セキュリティ大学院)

2D4　暗号理論 (1)　1 月 21 日 (水)　16:20—18:00

2D4-1　Goldreich-Levin の定理の最適性再考

○河内 亮周 (徳島大学)

2D4-2　改善された安全性証明を持つ GGHLite パラメータ

○高安敦 (東京大学), 高島克幸 (三菱電機株式会社)

2D4-3 An Operational Characterization of the Notion of Probability by Algorithmic Randomness and Its Application to Cryptography

○只木孝太郎 (中央大学 研究開発機構)

2D4-4 Black-Box Separations in the Non-Programmable Random Oracle Model: the Cases of Hash-and-Sign Signatures

◎ Zongyang Zhang (AIST, Japan), Yu Chen (Chinese Academy of Sciences, China), Sherman S. M. Chow (Chinese University of Hong Kong, Hong Kong), Goichiro Hanaoka (AIST, Japan), Zhenfu Cao (East China Normal University, China)

2D4-5 Non-Programmable Random Oracle モデルにおける Fiat-Shamir 型署名の安全性証明の限界

◎福光 正幸 (北海道情報大学 情報メディア学部), 長谷川 真吾 (東北大学 大学院情報科学研究科)

2E4 署名 (2) 1 月 21 日 (水) 16:20—18:00

2E4-1 否認可能グループ署名

◎石田 愛 (東京工業大学/AIST), 江村 恵太 (NICT), 花岡 悟一郎 (AIST), 坂井 祐介 (AIST), 田中 圭介 (東京工業大学/JST CREST)

2E4-2 開示者指定グループ署名

◎中川 紗菜美 (筑波大学, AIST), 江村 恵太 (NICT), 花岡 悟一郎 (AIST), 金山 直樹 (筑波大学), 西出 隆志 (筑波大学), 岡本 栄司 (筑波大学)

2E4-3 カメレオンハッシュを用いた Merkle 木に基づく木構造データに対する編集可能署名

◎山本正義 (千葉大学大学院融合科学研究科), 岸本渡 (千葉大学大学院融合科学研究科)

2E4-4 検証可能暗号化準同型署名

Jae Hong Seo (Myongji University), 江村 恵太 (NICT), ○草川 恵太 (NTT), 米山 一樹 (NTT)

2F4 サイドチャネル攻撃 (2) 1 月 21 日 (水) 16:20—18:00

2F4-1 暗号モジュールからの漏洩電磁波を用いた故障発生タイミング特定手法

◎中村 紘 (東北大学), 林 優一 (東北大学), 水木 敬明 (東北大学), 本間 尚文 (東北大学), 青木 孝文 (東北大学), 曽根 秀昭 (東北大学)

2F4-2 マイクロコントローラ上のプログラム制御フローへの故障注入攻撃

◎梨本 翔永 (東北大学), 遠藤 翔 (東北大学), 本間 尚文 (東北大学), 林 優一 (東北大学), 青木 孝文 (東北大学)

2F4-3 タブレット端末からの電磁波を介した情報漏えいメカニズムの検討

○林優一 (東北大学), 本間尚文 (東北大学), 三浦衛 (東北大学), 青木孝文 (東北大学), 曽根秀昭 (東北大学)

2F4-4 電磁波攻撃センサの設計と実証

○本間尚文 (東北大学), 林優一 (東北大学), 三浦典之 (神戸大学), 藤本大介 (神戸大学), 永田真 (神戸大学), 青木孝文 (東北大学)

3A1 サイドチャネル攻撃 (3) 1 月 22 日 (木) 9:00—10:40

3A1-1 サイドチャネル攻撃における他の回路が発生するノイズの定量的評価

◎田中 将貴 (立命館大学理工学部), 中井 綱人 (立命館大学大学院理工学研究科), 汐? 充 (立命館大学大学院総合理工学研究機構), 久保田 貴也 (立命館大学大学院総合理工学研究機構), 藤野 毅 (立命館大学理工学部)

3A1-2 ドーパントを利用した回路カモフラージュのリバースエンジニアリング

○菅原健 (三菱電機株式会社), 鈴木大輔 (三菱電機株式会社), 藤井亮一 (三菱電機株式会社), 田和茂朗 (三菱電機株式会社), 堀遼平 (立命館大学), 汐崎充 (立命館大学), 藤野毅 (立命館大学)

3A1-3 楕円群演算において無限遠点が特別扱いされることを利用した ECDSA のセーフエラー攻撃

○菅原健 (三菱電機株式会社), 鈴木大輔 (三菱電機株式会社)

3A1-4 線形符号を用いたレジスタへのセーフエラー攻撃対策

○菅原健 (三菱電機株式会社), 鈴木大輔 (三菱電機株式会社), 佐伯稔 (三菱電機株式会社), 平野貴人 (三菱電機株式会社)

3A1-5 TWINE に対するエラー値を考慮したフォールト攻撃

◎野崎佑典 (名城大学理工学研究科情報工学専攻), 吉川雅弥 (名城大学理工学部情報工学科)

3B1　プライバシー保護 (2)　1 月 22 日 (木)　9:00—10:40

3B1-1　相関保存 Pk 匿名化法

○坂野 鋭 ((株)NTT データ)

3B1-2　複数のセンシティブな擬似識別子を含むデータベースの匿名化手法の提案

○清 雄一 (電気通信大学大学院情報システム学研究科), 大須賀 昭彦 (電気通信大学大学院情報システム学研究科)

3B1-3　視聴履歴を対象とした匿名化手法の一提案

○前田 学 (パナソニック株式会社), 松崎 なつめ (パナソニック株式会社), 海上 勇二 (パナソニック株式会社)

3B1-4　特定個人情報保護評価におけるリスク評価項目の分析

瀬戸洋一 (産業技術大学院大学), ○慎 祥揆 (産業技術大学院大学), 畠山智美 (産業技術大学院大学), 佐々木真由美 (産業技術大学院大学)

3B1-5　韓国の個人情報保護の改善に関する紹介

○慎 祥揆 (産業技術大学院大学), 瀬戸 洋一 (産業技術大学院大学)

3C1　セキュリティ評価・モデル (1)　1 月 22 日 (木)　9:00—10:40

3C1-1　ダークネット上の観測点保護のためのパケットサンプリング手法の有効性評価

◎鎌田 恵介 (岩手県立大学大学院 ソフトウェア情報学研究科), 成田 匡輝 (東北文化学園大学 科学技術学部 知能情報システム学科), 小倉 加奈代 (岩手県立大学大学院 ソフトウェア情報学研究科), ベッド バハドゥール ビスタ (岩手県立大学大学院 ソフトウェア情報学研究科), 高田 豊雄 (岩手県立大学大学院 ソフトウェア情報学研究科)

3C1-2　ロイヤルティプログラムのセキュリティインシデントインパクト分析に向けたポイント流動性の定義に対する考察

◎篠田 詩織 (東京大学), 松浦 幹太 (東京大学)

3C1-3　日本のロイヤルティ・プログラムにおける企業間連携とそのセキュリティインシデントによるインパクト

◎ Bongkot JENJARRUSSAKUL (東京大学 生産技術研究所), Kanta MATSUURA (東京大学 生産技術研究所)

3C1-4　web システムのための運用時セキュリティ評価方式の提案

◎関根 基晴 (東京電機大学), 芦野 佑樹 (NEC クラウドシステム研究), 島 成佳 (NEC クラウドシステム研究所), 勅使河原 可海 (東京電機大学), 佐々木 良一 (東京電機大学)

3C1-5　車載システムにおけるリスク分析とセキュリティ要件定義手法の提案

○北村 嘉彦 (パナソニック株式会社 AIS 社), 安齋 潤 (パナソニック株式会社 AIS 社)

3D1　数論応用　1 月 22 日 (木)　9:00—10:40

3D1-1　整数計画問題による binary-LWE 問題の求解アルゴリズム

◎町野 義貴 (東京大学), 青野 良範 (情報通信研究機構), 高安 敦 (東京大学), 國廣 昇 (東京大学)

3D1-2　アナログ情報からの RSA 秘密鍵復元の改良

◎高橋勇貴 (東京大学), 國廣昇 (東京大学)

3D1-3　LPN 問題に対する BKW アルゴリズムの拡張

◎上中谷 健 (東京大学大学院 情報理工学系研究科 数理情報学専攻), 國廣 昇 (東京大学大学院 新領域創成科学研究科 複雑理工学専攻)

3D1-4　多次元 p 進近似格子と暗号理論への応用

◎井上 裕仁 (熊本大学大学院自然科学研究科), 内藤 幸一郎 (熊本大学大学院自然科学研究科)

3E1　Web セキュリティ (2)　1 月 22 日 (木)　9:00—10:40

3E1-1　インターネットノイズに対する偽装応答機能の実装と観測に基づいた意図が不明なリクエストに関する考察

○芦野 佑樹 (NEC クラウドシステム研究所), 島 成佳 (NEC クラウドシステム研究所)

3E1-2　cookie 漏洩に起因する被害の低減手法の構築と考察

◎高橋寛弥 (金沢大学), 安永憲司 (金沢大学), 満保雅浩 (金沢大学)

3E1-3　HTML5 セキュリティ強化実行基盤の提案と実装

○野田 敏達 (株式会社富士通研究所), 金谷 延幸 (独立行政法人情報通信研究機構), 長谷部 高行 (株式会社富士通研究所)

3E1-4　HTML5 セキュリティ強化実行基盤「SEHTML5」を使ったパスワードマネージャ の提案と実装

○金谷延幸 (独立行政法人情報通信研究機構), 野田敏達 (株式会社富士通研究所), 長谷部高行 (株式会社富士通研究所)

3F1　暗号プロトコル (3)　1 月 22 日 (木)　9:00—10:40

3F1-1　回路のエンコード鍵を持つ秘匿回路

◎遠山 裕之 (東京工業大学), 小松 智之 (東京工業大学), 田中 圭介 (東京工業大学, JST CREST)

3F1-2　擬似ランダム関数をもとにした効率的な秘匿回路の構成

◎西山 双輝 (東京工業大学), 遠山 裕之 (東京工業大学), 小松 智之 (東京工業大学), 田中 圭介 (東京工業大学，JST CREST)

3F1-3　実用的な多機能検索可能暗号方式 ～身も蓋もない方式を考えてみた～

○尾形わかは (東京工業大学), 金岡晃 (東邦大学), 松尾真一郎 (情報通信研究機構)

3F1-4　複数キーワードによるランク付き検索可能暗号の改善

◎ユ サンウォン (東京工業大学 通信情報工学専攻), 尾形 わかは (東京工業大学 通信情報工学専攻)

3A2　サイドチャネル攻撃 (4)　1 月 22 日 (木)　11:00—12:40

3A2-1　サイドチャネル認証の為の漏洩モデルに関する一考察

◎松原 有沙 (電気通信大学), 町田 卓謙 (電気通信大学), 林 優一 (東北大学), 崎山 一男 (電気通信大学)

3A2-2　AES ハードウェア実装の任意ラウンドにおける消費電力制御

◎カイ 云峰 (電気通信大学), 李 陽 (電気通信大学), 町田 卓謙 (電気通信大学), 崎山 一男 (電気通信大学)

3A2-3　ハードウェアのプロファイリングによるサイドチャネル波形の予測

○浅井稔也 (名城大学), 吉川雅弥 (名城大学)

3A2-4　アンロールアーキテクチャで実装された PRINCE ハードウェアに対する電力解析の検討

◎ YLI-MÄYRY VILLE (東北大学), 本間尚文 (東北大学), 遠藤翔 (東北大学), 青木孝文 (東北大学)

3B2　バイオテンプレート保護　1 月 22 日 (木)　11:00—12:40

3B2-1　準同型暗号を用いた秘匿生体認証に対する安全性について (その 3)

酒見由美 (株式会社富士通研究所), ○武仲正彦 (株式会社富士通研究所), 鳥居直哉 (株式会社富士通研究所, 横浜国立大学), 安田雅哉 (株式会社富士通研究所), 松本勉 (横浜国立大学)

3B2-2　バイナリ列で表した生体情報がもつ生体特有の偏りの評価

◎松濤智明 (富士通研究所), 山本大 (富士通研究所), 山田茂史 (富士通研究所), 新崎卓 (富士通研究所), 武仲正彦 (富士通研究所)

3B2-3　秘匿生体認証方式の安全性

◎肥後春菜 (NEC), 一色寿幸 (NEC), 森健吾 (NEC), 尾花賢 (法政大学)

3B2-4　テンプレートサイズの小さい秘匿指紋認証方式

肥後春菜 (NEC), ○一色寿幸 (NEC), 森健吾 (NEC), 尾花賢 (法政大学)

3B2-5　尤度比に基づく生体認証方式の脆弱性とウルフ安全性評価

○大木 哲史 (産業技術総合研究所), 大塚 玲 (産業技術総合研究所)

3C2　自動車セキュリティ (2)　1 月 22 日 (木)　11:00—12:40

3C2-1　車載セキュリティ確保におけるセキュアブートの高速化手法について

○倉内 伸和 (パナソニックアドバンストテクノロジー株式会社), 小野 貴敏 (パナソニックアドバンストテクノロジー株式会社), 山本 和成 (パナソニックアドバンストテクノロジー株式会社), 青木 哲朗 (パナソニックアドバンストテクノロジー株式会社), 安齋 潤 (パナソニック株式会社), 北村 嘉彦 (パナソニック株式会社)

3C2-2　車載ネットワークにおける CAN フィルタの提案

◎氏家 良浩 (パナソニック株式会社 先端研究本部), 岸川 剛 (パナソニック株式会社 先端研究本部), 芳賀 智之 (パナソニック株式会社 先端研究本部), 松島 秀樹 (パナソニック株式会社 先端研究本部), 田邉 正人 (パナソニック株式会社 ＡＩＳ社), 北村 嘉彦 (パナソニック株式会社 ＡＩＳ社), 安齋 潤 (パナソニック株式会社 ＡＩＳ社)

3C2-3　車載ネットワークを保護するセキュリティECU の提案: 導入インパクトを抑えた CAN 保護手法のコンセプトとその評価

○芳賀 智之 (パナソニック株式会社 先端研究本部), 岸川 剛 (パナソニック株式会社 先端研究本部), 氏家 良浩 (パナソニック株式会社 先端研究本部), 松島 秀樹 (パナソニック株式会社 先端研究本部), 田邉 正人 (パナソニック株式会社 ＡＩＳ社), 北村 嘉彦 (パナソニック株式会社 ＡＩＳ社), 安齋 潤 (パナソニック株式会社 ＡＩＳ社)

3C2-4　車載ネットワークを保護するセキュリティECU の提案: HW/SW 協調による更新可能な CAN の保護手法とその評価

◎岸川 剛 (パナソニック株式会社 先端研究本部), 氏家 良浩 (パナソニック株式会社 先端研究本部), 芳賀 智之 (パナソニック株式会社 先端研究本部), 松島 秀樹 (パナソニック株式会社 先端研究本部), 田邉 正人 (パナソニック株式会社 AIS 社), 北村 嘉彦 (パナソニック株式会社 AIS 社), 安齋 潤 (パナソニック株式会社 AIS 社)

3C2-5　車載ネットワークにおける監視・検証モード切換えの提案

◎田邉 正人 (パナソニック株式会社 AIS 社), 北村 嘉彦 (パナソニック株式会社 AIS 社), 安齋 潤 (パナソニック株式会社 AIS 社), 岸川 剛 (パナソニック株式会社 先端研究本部), 氏家 良浩 (パナソニック株式会社 先端研究本部), 芳賀 智之 (パナソニック株式会社 先端研究本部), 松島 秀樹 (パナソニック株式会社 先端研究本部)

3D2　暗号理論 (2)　1 月 22 日 (木)　11:00—12:40

3D2-1　Streaming Algorithms for Sampling from Discrete Gaussian Distributions

◎ Maxim Jourenko (RWTH Aachen University, Tokyo Institute of Technology), Ryosuke Nakata (Tokyo Institute of Technology), Keisuke Tanaka (Tokyo Institute of Technology, JST CREST)

3D2-2　Streaming Signature

◎ Ryosuke Nakata (Tokyo Institute of Technology), Maxim Jourenko (RWTH Aachen University, Tokyo Institute of Technology), Keisuke Tanaka (Tokyo Institute of Technology, JST CREST)

3D2-3　属性ベース暗号の秘密鍵サイズの効率化

◎澤井優樹 (東京工業大学), 中田亮介 (東京工業大学), 田中圭介 (東京工業大学，JST CREST)

3D2-4　代理人再暗号化における CCA1 安全性に対する再暗号化オラクルの導入

◎見村朔 (東京工業大学), 澤井優樹 (東京工業大学), 中田亮介 (東京工業大学), 田中圭介 (東京工業大学，JST CREST)

3D2-5　効率的な万能算術回路の構成

◎小松智之 (東京工業大学), 田中圭介 (東京工業大学，JST CREST)

3E2　公開鍵暗号 (3)　1 月 22 日 (木)　11:00—12:40

3E2-1　MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems

○ Takanori Yasuda (ISIT), Xavier Dahan (Ochanomizu University), Yun-Ju Huang (Kyushu University), Tsuyoshi Takagi (Kyushu University, CREST), Kouichi Sakurai (Kyushu University, ISIT)

3E2-2　Semi-smooth RSA 数の素因数分解問題に基づく一般化 Lossy Trapdoor 関数

○山川 高志 (東京大学), 山田 翔太 (産総研), 花岡悟一郎 (産総研), 國廣 昇 (東京大学)

3E2-3　Security Notion and Construction on Bidirectional Proxy Re-Encryption

○ Jian Weng (Jinan University), Kouichi Sakurai (Kyushu University)

3E2-4　CCA-Secure Multi-hop Unidirectional Proxy Re-Encryption from Indistinguishability Obfuscation

○ Jian Weng (JInan University), Kouichi Sakurai (Kyushu University)

3E2-5　Attack on a public key trace and revoke scheme of a broadcast encryption

○ Jian Weng (Jina University), Kouichi Sakurai (Kyushu University)

3F2　暗号プロトコル (4)　1 月 22 日 (木)　11:00—12:40

3F2-1　PKI ベースから ID ベース認証鍵交換への一般的変換法

○鈴木幸太郎 (NTT セキュアプラットフォーム研究所), 米山一樹 (NTT セキュアプラットフォーム研究所)

3F2-2　属性に基づく認証鍵交換方式

○小林鉄太郎 (NTT), 星野文学 (NTT), 鈴木幸太郎 (NTT)

3F2-3　ID 認証鍵交換における自己訂正を用いた鍵管理方式

◎齋藤恆和 (NTT セキュアプラットフォーム研究所), 永井彰 (NTT セキュアプラットフォーム研究所), 小林鉄太郎 (NTT セキュアプラットフォーム研究所)

3F2-4　Lottery Protocol for Cryptocurrency

◎久米 潤一郎 (京都大学), 阿部 正幸 (NTT, 京都大学), 岡本 龍明 (NTT, 京都大学)

3F2-5　通信量が改善された DLIN 仮定に基づく検証可委譲計算

○高島克幸 (三菱電機)

3A3　サイドチャネル攻撃 (5)　1 月 22 日 (木)　14:20—16:00

3A3-1　Piccolo に対する階層的なフォールト攻撃手法

◎野原康平 (名城大学理工学研究科情報工学専攻), 吉川雅弥 (名城大学理工学部情報工学科)

3A3-2　Simon に対するフォールト攻撃

○高橋順子 (NTT セキュアプラットフォーム研究所), 福永利徳 (日本電信電話株式会社 技術企画部門)

3A3-3　差分フォルト解析においてクリティカルなグリッチ注入タイミングの測定

◎前島 一仁 (岡山大学大学院自然科学研究科), 五百旗頭 健吾 (岡山大学大学院自然科学研究科), 渡辺 哲史 (岡山県工業技術センター), 籠谷 裕人 (岡山大学大学院自然科学研究科), 豊田 啓孝 (岡山大学大学院自然科学研究科)

3A3-4　サイドチャネル攻撃対策 RSM 方式を用いた AES 暗号回路の電力解析攻撃耐性評価

◎堤大樹 (立命館大学大学院), 中井綱人 (立命館大学大学院), 汐崎充 (立命館大学大学院), 久保田貴也 (立命館大学大学院), 藤野毅 (立命館大学)

3B3　ユビキタスセキュリティ　1 月 22 日 (木)　14:20—16:00

3B3-1　端末にインストールされているフォント情報を用いた OS とアプリケーションの特定

◎塚本耕司 (明治大学大学院), 磯侑斗 (明治大学大学院), 桐生直輝 (明治大学大学院), 高須航 (明治大学大学院), 山田智隆 (明治大学大学院), 武居直樹 (明治大学大学院), 細井理央 (明治大学), 齋藤孝道 (明治大学)

3B3-2　編集距離を用いたロバストな Browser Fingerprint 間の識別方式の提案

◎山田 智隆 (明治大学大学院), 磯 侑斗 (明治大学大学院), 桐生 直輝 (明治大学大学院), 塚本 耕司 (明治大学大学院), 高須 航 (明治大学大学院), 武居 直樹 (明治大学大学院), 齋藤 孝道 (明治大学)

3B3-3　センサネットワークに適したグループ鍵配送方式の提案

◎金子 良 (東京理科大学大学院工学研究科電気工学専攻), 岩村 惠市 (東京理科大学大学院工学研究科電気工学専攻)

3B3-4　放送・通信の 4 類型と情報セキュリティ概念の高度化—第 2 報—組織通信と公共情報コモンズ（L アラート）

○辻井重男 (中央大学研究開発機構), 吉田正彦 (総務省), 柴崎哲也 (財団法人マルチメディア振興センター), 小林正幸 (財団法人マルチメディア振興センター), 川喜多孝之 (財団法人マルチメディア振興センター)

3C3　組み込みセキュリティ　1 月 22 日 (木)　14:20—16:00

3C3-1　制御・車載システムにおけるセキュリティ機能要件に関する考察

○大和田徹 ((株) 日立製作所 横浜研究所), 内山宏樹 ((株) 日立製作所 横浜研究所), 伯田恵輔 ((株) 日立製作所 横浜研究所), 森田伸義 ((株) 日立製作所 横浜研究所), 萱島信 ((株) 日立製作所 横浜研究所)

3C3-2　制御システムにおける鍵更新頻度の抑制に適したシーケンス番号の更新・確認手法

○伯田 恵輔 ((株) 日立製作所 横浜研究所), 森田 伸義 ((株) 日立製作所 横浜研究所), 大和田 徹 ((株) 日立製作所 横浜研究所), 萱島 信 ((株) 日立製作所 横浜研究所)

3C3-3　車載ネットワーク向けメッセージ認証方式の提案

◎森田伸義 ((株) 日立製作所 横浜研究所), 伯田恵輔 ((株) 日立製作所 横浜研究所), 大和田徹 ((株) 日立製作所 横浜研究所), 萱島信 ((株) 日立製作所 横浜研究所)

3C3-4　車載制御ネットワークにおける送信周期監視システムの提案

○倉地 亮 (名古屋大学大学院情報科学研究科), 高田 広章 (名古屋大学大学院情報科学研究科), 上田 浩史 (株式会社オートネットワーク技術研究所), 堀端 啓史 (株式会社オートネットワーク技術研究所)

3C3-5　制御システムにおけるライブフォレンジックの適用可能性に関する実験的評価

○田村 研輔 (警察庁), 松浦 幹太 (東京大学)

3D3　暗号理論 (3)　1 月 22 日 (木)　14:20—16:00

3D3-1　防御不可能なタンパリング以外のほぼ全てのタンパリングから暗号回路を守る方法

○藤崎英一郎 (ＮＴＴセキュアプラットフォーム研究所), 草川恵太 (ＮＴＴセキュアプラットフォーム研究所)

3D3-2　Optimizing obfuscation: towards smaller matrix branching programs

◎ Jinsu Kim (Seoul National University), Mehdi Tibouchi (NTT Secure Platform Laboratories)

3D3-3　汎用的結合可能性における匿名性の定式化

◎森山大輔 (情報通信研究機構), Moti Yung (Google/Columbia 大学)

3D3-4　検証者が報酬を下げることができない合理的な証明

◎稲澤 啓太 (金沢大学), 安永 憲司 (金沢大学), 満保 雅浩 (金沢大学)

3D3-5　1 ビット Projection-KDM 安全性の完備性

◎北川 冬航 (東京工業大学，産業技術総合研究所), 松田 隆宏 (産業技術総合研究所), 花岡 悟一郎 (産業技術総合研究所), 田中 圭介 (東京工業大学，JST CREST)

3E3　公開鍵暗号 (4)　1 月 22 日 (木)　14:20—16:00

3E3-1　複数の鍵発行機関が存在可能な関数型暗号に対する失効機能の実現

◎土田光 (筑波大学), 金山直樹 (筑波大学), 西出隆志 (筑波大学), 岡本栄司 (筑波大学), Kwangjo Kim (KAIST)

3E3-2　秘密鍵に四系列の乱数を用いるナップザック暗号

○村上恭通 (大阪電気通信大学/中央大学研究開発機構), 濱正真佑 (大阪電気通信大学), 笠原正雄 (早稲田大学/中央大学研究開発機構)

3E3-3　Homomorphic authentication for network coding

○ Chi CHENG (IMI, Kyushu University), Tsuyoshi TAKAGI (IMI, Kyushu University)

3E3-4　PQCrypto 2014 参加報告

○安田貴徳 (九州先端科学技術研究所)

3E3-5　A New Progressive BKZ Algorithm

◎ Yuntao Wang (Graduate School of Mathematics, Kyushu University), Yoshinori Aono (National Institute of Communication and Technology), Takuya Hayashi (National Institute of Communication and Technology), Tsuyoshi Takagi (Institute of Mathematics for Industry, Kyushu University / CREST, JST)

3F3　暗号プロトコル (5)　1 月 22 日 (木)　14:20—16:00

3F3-1　New results on cheater identifiable secret sharing

◎ Rui Xu (Kyushu University), Kirill Morozov (Kyushu University), Tsuyoshi Takagi (Kyushu University)

3F3-2　A lightweight security protocol for RFID tags anonymity

◎ wissam razouk (Kyushu University)

3F3-3　共通鍵を利用した伝送路ノイズからの秘密鍵生成

○戸丸辰也 (日立製作所 中央研究所)

3F3-4　共通鍵暗号ベースの再暗号方式の検討その 2

○坂崎尚生 (株式会社 日立製作所), 安細康介 (株式会社 日立製作所)

3F3-5　TLS ハンドシェイクプロトコルのセキュア委託プロトコルの開発

○中嶋 純 (沖電気工業株式会社), 福井 潔 (沖電気工業株式会社)

3A4　特別講演　1 月 22 日 (木)　16:20—17:20

3A4-1　数学と暗号の接点 〜代数曲線、有限体、そしてモチビックゼータ〜

木村俊一 (広島大学大学院 理学研究科数学専攻 代数数理講座 教授)

3B4　ソフトウェア保護　1 月 22 日 (木)　16:20—18:00

3B4-1　コーディングスタイルの特徴量を用いた初心者プログラマーを対象にした著者解析

◎北川裕基 (京都産業大学コンピュータ理工学部), 福本大 (京都産業大学コンピュータ理工学部), 玉田春昭 (京都産業大学コンピュータ理工学部)

3B4-2　メソッド呼び出しのフックを用いた動的コールフローグラフ偽装の試み

○稲垣賢一 (京都産業大学コンピュータ理工学部), 福田收真 (京都産業大学コンピュータ理工学部), 玉田春昭 (京都産業大学コンピュータ理工学部)

3B4-3　メタプログラミング技法を用いた偽装難読化手法

◎福田收真 (京都産業大学大学院先端情報研究科), 玉田春昭 (京都産業大学コンピュータ理工学部), 稲垣賢一 (京都産業大学コンピュータ理工学部)

3B4-4　大量のプログラムを対象としたファジーハッシュを用いたバースマーク手法

◎山本 照明 (京都産業大学 コンピュータ理工学部), 玉田 春昭 (京都産業大学 コンピュータ理工学部), 門田 暁人 (奈良先端科学技術大学院大学 情報科学研究科)

3C4　プライバシー保護 (3)　1 月 22 日 (木)　16:20—18:00

3C4-1　Comparison of Information Loss Metrics for k-Anonymization

◎ Pakin O-sotkraphun (Toshiba Solutions Corporation), Masanobu Koike (Toshiba Solutions Corporation)

3C4-2　A Mondrian-Based k-Anonymization with Low Information Loss

○ Masanobu Koike (Toshiba Solutions Corporation), Pakin O-sotkraphun (Toshiba Solutions Corporation), Hidemasa Ito (Toshiba Solutions Corporation)

3C4-3　k-存在秘匿性: k-匿名性を拡張した実際的なプライバシーモデル

○山岡 裕司 (株式会社富士通研究所), 伊藤 孝一 (株式会社富士通研究所)

3C4-4　k-匿名化が誘発する濡れ衣を軽減するデータベース分割再構成法

◎角野為耶 (東京大学大学院学際情報学府), 荒井ひろみ (東京大学情報基盤センター), 中川裕志 (東京大学情報基盤センター)

3C4-5　k-匿名化に適したログデータ変換手法の提案

◎及川孝徳 (株式会社富士通研究所), 山岡裕司 (株式会社富士通研究所), 伊藤孝一 (株式会社富士通研究所)

3D4　暗号理論 (4)　1 月 22 日 (木)　16:20—18:00

3D4-1　非ブラックボックスシミュレーションによる並行ゼロ知識証明

○清島 奨 (NTT セキュアプラットフォーム研究所)

3D4-2　On Correlated-Input Secure Hash Functions and Reconstructive Extractors

○ Jacob Schuldt (RISEC, AIST)

3D4-3　暗号プリミティブにおける秘密情報の分布と安全性の関係

○高橋 健太 ((株) 日立製作所), 松田 隆宏 (産業技術総合研究所), 村上 隆夫 (産業技術総合研究所)

3D4-4　Degree of Regularity の境界近傍における XL の実行時間解析

◎田中哲士 (九州先端科学技術研究所/九州大学), Chen-Mou Cheng (九州大学), 櫻井幸一 (九州先端科学技術研究所/九州大学)

3D4-5　A Commitment Scheme Based on Chebyshev Polynomials

○ Ji-Jian Chin (Faculty of Engineering, Multimedia University), Syh-Yuan Tan (Faculty of Information Science and Technology, Multimedia University), Hiroaki Anada (Institute of Systems, Information Technologies and Nanotechnologies (ISIT))

3E4　暗号化状態処理 (3)　1 月 22 日 (木)　16:20—18:00

3E4-1　SIMD Operations in GSW-FHE

◎廣政 良 (京都大学), 阿部 正幸 (NTT セキュアプラットフォーム研究所，京都大学), 岡本 龍明 (NTT セキュアプラットフォーム研究所，京都大学)

3E4-2　IND-CCA1 安全性を満たす N-ary 完全準同型暗号

◎安田 聖 (東京工業大学), 石田 愛 (東京工業大学), 北川 冬航 (東京工業大学), 田中 圭介 (東京工業大学，JST CREST)

3E4-3　鍵付き準同型 ID ベース暗号

○江村 恵太 (独立行政法人情報通信研究機構), 花岡 悟一郎 (独立行政法人産業技術総合研究所), 松田 隆宏 (独立行政法人産業技術総合研究所), 縫田 光司 (独立行政法人産業技術総合研究所/JST さきがけ), 山田 翔太 (独立行政法人産業技術総合研究所)

3E4-4　Co-ACD 仮定とそれを基にした準同型暗号方式の安全性評価

ピエール=アラン・フーク (レーヌ大学), タンクレード・ルポワン (クリプトエックスペール), ○メディ・ティブシ (NTT セキュアプラットフォーム研究所)

3F4　暗号プロトコル (6)　1 月 22 日 (木)　16:20—18:00

3F4-1　Corrupt 耐性を持つセッションキー安全な秘密鍵失効機能付き Secret Handshake 方式

◎土屋 喬文 (電気通信大学), 花谷 嘉一 (株式会社東芝 研究開発センター), 岩本 貢 (電気通信大学), 太田和夫 (電気通信大学)

3F4-2　カードを用いた効率的な金持ち比べプロトコル

◎中井雄士 (電気通信大学), 徳重佑樹 (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)

3F4-3　カードベース暗号プロトコルにおける安全な選択処理

◎徳重佑樹 (電気通信大学), 中井雄士 (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)

3F4-4　簡易なブロックサインに対する暗号理論的安全性解析

◎三澤裕人 (電気通信大学), 徳重佑樹 (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)

4A1　モバイルセキュリティ (1)　1 月 23 日 (金)　9:00—10:40

4A1-1　通信と描画挙動の動的解析を用いた Android 広告ライブラリの検知手法

◎梶原直也 (九州大学/九州先端科学技術研究所), 川本淳平 (九州大学/九州先端科学技術研究所), 松本晋一 (九州大学/九州先端科学技術研究所), 堀良彰 (佐賀大学/九州先端科学技術研究所), 櫻井幸一 (九州大学/九州先端科学技術研究所)

4A1-2　Android OS におけるユーザー習熟度を用いたマルウェア被害防止システムの提案

◎小松 勇毅 (岩手県立大学大学院ソフトウェア情報学研究科), 児玉 英一郎 (岩手県立大学ソフトウェア情報学部), 王 家宏 (岩手県立大学ソフトウェア情報学部), 高田 豊雄 (岩手県立大学ソフトウェア情報学部)

4A1-3　悪性コード挿入時の特徴に着目した Android マルウェア検知手法の提案

◎庄田祐樹 (横浜国立大学), 金井文宏 (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)

4A1-4　情報漏洩を防止するシステムの提案

◎吉田麗生 (NTT セキュアプラットフォーム研究所), 秋葉 淳哉 (NTT セキュアプラットフォーム研究所), 小林 鉄太郎 (NTT セキュアプラットフォーム研究所), 宮本 剛 (NTT セキュアプラットフォーム研究所), 鷲尾 知暁 (NTT セキュアプラットフォーム研究所), 冨士 仁 (NTT セキュアプラットフォーム研究所)

4A1-5　ソフトウェアセキュアエレメントを用いた認証アプリケーション〜iOS デバイスへの適用と評価〜

◎奥井 宣広 (株式会社 KDDI 研究所), 仲野 有登 (株式会社 KDDI 研究所), 清本 晋作 (株式会社 KDDI 研究所), 三宅 優 (株式会社 KDDI 研究所)

4B1　プライバシー保護 (4)　1 月 23 日 (金)　9:00—10:40

4B1-1　Tor を利用したアンケートシステム

◎三井慧史 (筑波大学システム情報工学研究科リスク工学専攻), 金山直樹 (筑波大学システム情報系), 西出隆志 (筑波大学システム情報系), 岡本栄司 (筑波大学システム情報系)

4B1-2　Evaluation of Anti-enumeration Defenses for Tor Bridges

◎ Fei Feng (Institute of Industrial Science, The University of Tokyo), Kanta Matsuura (Institute of Industrial Science, The University of Tokyo)

4B1-3　検索エンジンへの入力が与える情報量を低減する手法の提案

◎平出 悠祐 (東海大学大学院), 山本 宙 (東海大学)

4B1-4　安全なデータ追加が可能な秘匿検索方式

○牛田芽生恵 ((株) 富士通研究所), 山岡裕司 ((株) 富士通研究所), 伊藤孝一 ((株) 富士通研究所)

4B1-5　位置情報を利用したサービスにおけるトラストポイントの検討

○疋田 敏朗 (東京大学), 山口 利恵 (東京大学)

4C1　セキュリティ評価・モデル (2)　1 月 23 日 (金)　9:00—10:40

4C1-1　セキュリティ場モデルの提案

◎平本拓也 (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)

4C1-2　ITS におけるプライバシ情報漏洩に関する一考察

○早稲田篤志 (情報通信研究機構), 野島良 (情報通信研究機構)

4C1-3　2014 年情報セキュリティ調査から見えてくる組織 (民間企業・官公庁・教育機関) における現状

○水澤 良平 (情報セキュリティ大学院大学), 原田 要之助 (情報セキュリティ大学院大学), 大賀 麻衣子 (情報セキュリティ大学院大学), 佐々木 崇裕 (情報セキュリティ大学院大学), 福島 健二 (情報セキュリティ大学院大学), 伊藤 国浩 (情報セキュリティ大学院大学), 丹木 就之 (情報セキュリティ大学院大学)

4C1-4　セキュリティリスク分析における脅威抽出方法の改良

○植田 武 (三菱電機株式会社), 泉 幸雄 (三菱電機株式会社), 中嶋 純子 (三菱電機株式会社), 桜井 鐘治 (三菱電機株式会社)

4D1　教育・心理学　1 月 23 日 (金)　9:00—10:40

4D1-1　高度化したサイバー攻撃対策の心理学的アプローチについて

○小川隆一 (日本電気), 島成佳 (日本電気), 福住伸一 (日本電気), 角尾幸保 (日本電気)

4D1-2　情報システム・サービスの利用者の利用意図による安心感と納得感の関係について

◎奥村 香保里 (名古屋工業大学), 毛利 公美 (岐阜大学), 白石 善明 (神戸大学), 岩田 彰 (名古屋工業大学)

4D1-3　ユーザー行動特性分析による個人と組織の IT リスク見える化の試み

○片山佳則 (富士通株式会社), 寺田剛陽 (富士通株式会社), 鳥居悟 (富士通株式会社), 津田宏 (富士通株式会社)

4D1-4　国際会議 ACMCCS2014 参加報告

○穴田 啓晃 (公益財団法人九州先端科学技術研究所), 菊池 亮 (NTT セキュアプラットフォーム研究所), 森達哉 (早稲田大学基幹理工学部 情報通信学科), 國廣 昇 (東京大学大学院 新領域創成科学研究科)

4E1　乱数 (1)　1 月 23 日 (金)　9:00—10:40

4E1-1　制御変数が 4 である有限体上のロジスティック写像による生成系列の周期構成

○土屋和由 (株式会社光電製作所), 野上保之 (岡山大学大学院自然科学研究科)

4E1-2　素体上のロジスティック写像による多値系列の相関分布

○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), 野上 保之 (岡山大学)

4E1-3　整数上のロジスティック写像を用いた擬似乱数生成器におけるコントロールパラメータの更新に関する一考察

◎村岡 英之 (九州工業大学), 荒木 俊輔 (九州工業大学), 宮崎 武 (北九州市立大学), 上原 聡 (北九州市立大学), 礒崎 賢一 (九州工業大学)

4E1-4　β 変換器を用いた乱数生成法

◎松村 和也 (九州大学), 寺司 哲郎 (九州大学), 小田 晃平 (九州大学), 實松 豊 (九州大学)

4F1　情報理論的安全性 (3)・量子セキュリティ　1 月 23 日 (金)　9:00—10:40

4F1-1　計算量的なエントロピー安全性に関する考察

◎池田光晴 (金沢大学理工学域電子情報学類), 安永憲司 (金沢大学理工学域電子情報学系), 満保雅浩 (金沢大学理工学域電子情報学系)

4F1-2　RSA 暗号の高速化手法に対するタイミング攻撃の情報理論的安全性評価

◎小林靖幸 (奈良先端科学技術大学院大学), 楫勇一 (奈良先端科学技術大学院大学), 関浩之 (名古屋大学), 伊藤実 (奈良先端科学技術大学院大学)

4F1-3　Quantum Private Information Retrieval via Quantum Blind Computation

◎ Amit Raj Baral (Saitama Univ.), Takeshi Koshiba (Saitama Univ.), Harumichi Nishimura (Nagoya Univ.)

4F1-4　量子鍵配送におけるセキュリティ測度と鍵生成レートのトレードオフについて

○岩越 丈尚 (玉川大学 量子情報科学研究所)

4A2　モバイルセキュリティ (2)　1 月 23 日 (金)　11:00—12:40

4A2-1　Android Security に関する一考察 2

○古川 和快 (株式会社富士通研究所), 小久保 博崇 (株式会社富士通研究所), 兒島 尚 (株式会社富士通研究所), 武仲 正彦 (株式会社富士通研究所)

4A2-2　Android/Linux 脆弱性についての一考察

◎小久保 博崇 (富士通研究所), 古川 和快 (富士通研究所), 兒島 尚 (富士通研究所), 武仲 正彦 (富士通研究所)

4A2-3　スマートフォン向け安心・安全ソフト流通フレームワークの提案

◎竹中 萌 (岡山大学工学部情報系学科), 山内 利宏 (岡山大学大学院自然科学研究科), 才所 敏明 (株式会社 IT 企画)

4A2-4　環境によって変化するスマートフォンアプリケーション内広告ライブラリの動作検証方法に関する一考察

◎渡邊華奈子 (立命館大学), 田原裕暉 (立命館大学), 大月勇人 (立命館大学), 瀧本栄二 (立命館大学), 川端秀明 (KDDI 研究所), 竹森敬祐 (KDDI 研究所), 毛利公一 (立命館大学)

4A2-5　Android アプリ内の利用者情報を収集するモジュール特定方式

◎田原 裕暉 (立命館大学), 渡邊 華奈子 (立命館大学), 大月 勇人 (立命館大学), 瀧本 栄二 (立命館大学), 川端 秀明 (KDDI 研究所), 竹森 敬祐 (KDDI 研究所), 毛利 公一 (立命館大学)

4B2　クラウドセキュリティ　1 月 23 日 (金)　11:00—12:40

4B2-1　PRINCESS を利用したセキュアな自動車情報共有システム

○王 立華 (（独）情報通信研究機構), 野島 良 (（独）情報通信研究機構), 盛合 志帆 (（独）情報通信研究機構)

4B2-2　LOA を考慮した動的クラウド選択基盤方式

◎篠山裕貴 (法政大学大学院理工学研究科), 金井敦 (法政大学大学院理工学研究科), 谷本茂明 (千葉工業大学), 佐藤周行 (東京大学)

4B2-3　Forward Privacy を考慮した動的な検索可能暗号

◎佐藤尋時 (茨城大学理工学研究科)

4B2-4　計算資源を選ばないクラウドストレージサービス

◎松戸 一真 (千葉大学 工学部), 岸本 渡 (千葉大学大学院融合科学研究科)

4C2　認証 (3)　1 月 23 日 (金)　11:00—12:40

4C2-1　磁束密度のばらつきの抽出による真贋判定の可能性について

◎片平健太郎 (東京理科大学), 姜玄浩 (東京理科大学), 岩村惠市 (東京理科大学)

4C2-2　キネクトの骨格情報による非日常ポーズ認証

○石丸 大輔 (東京理科大学), 姜 玄浩 (東京理科大学), 岩村 惠市 (東京理科大学)

4C2-3　柱状回転体を用いた CAPTCHA の提案

◎木村祐貴 (茨城大学院 理工学研究科)

4C2-4　ウェアラブルデバイスを活用した個人の行動によるユーザ認証の検討

○鈴木宏哉 (東京大学), 山口利恵 (東京大学)

4C2-5　スマートフォンを事例とする多要素認証確率の提案

○山口利恵 (東京大学), 坂本静生 (NEC), 鈴木宏哉 (東京大学)

4D2　電子透かし　1 月 23 日 (金)　11:00—12:40

4D2-1　Image watermarking based on the nonlinear scale spaces feature

◎ Ta Minh Thanh (Tokyo Institute of Technology and JST CREST), Keisuke Tanaka (Tokyo Institute of Technology and JST CREST)

4D2-2　Blind watermarking using the quantized q-logarithm SVD domain

◎ Ta Minh Thanh (Tokyo Institute of Technology and JST CREST), Keisuke Tanaka (Tokyo Institute of Technology and JST CREST)

4D2-3　新しい圧縮方式には新しい電子透かしでしょ

○小川 一人 (日本放送協会), 大竹 剛 (日本放送協会)

4D2-4　音声電子透かしを用いた会議録用音声データの改ざん検知に関する一考察

◎吉田 智紀 (北九州市立大学国際環境工学部), 上原 聡 (北九州市立大学国際環境工学部), 宮崎 武 (北九州市立大学国際環境工学部), 荒木 俊輔 (九州工業大学大学院情報工学研究科)

4E2　乱数 (2)　1 月 23 日 (金)　11:00—12:40

4E2-1　拡大体上の定重み系列について

○戒田 高康 (近畿大学), 鄭 俊如 (九州女子大学), 高橋 圭一 (近畿大学)

4E2-2　剰余環 Z/2^kZ 上チェビシェフ多項式から得られる系列の諸性質

○吉岡大三郎 (崇城大学)

4E2-3　テント写像に基づく擬似ランダムビット列の分析

○奥富秀俊 (東芝情報システム株式会社)

4E2-4　エントロピープール付き擬似乱数生成器の性能分析

◎西野 卓也 (金沢大学), 安永 憲司 (金沢大学), 満保 雅浩 (金沢大学)

4F2　フォーマルメソッド　1 月 23 日 (金)　11:00—12:40

4F2-1　Mizar による多項式オーダー関数の形式化

○岡崎裕之 (信州大学), 布田裕一 (北陸先端技術大学院大学), 師玉康成 (信州大学)

4F2-2　Security Analysis of Re-encryption Scheme Based on Symmetric-key Cryptography

○ Dai Watanabe (Yokohama Laboratory, Hitachi, Ltd.), Hisao Sakazaki (Yokohama Laboratory, Hitachi, Ltd.), Kunihiko Miyazaki (Yokohama Laboratory, Hitachi, Ltd.)

4F2-3　ProVerif による Theft DoS Attack に耐性のあるワンタイムパスワード認証方式の形式的検証

◎岩本 智裕 (東京理科大学), 荒井 研一 (東京理科大学), 金子 敏信 (東京理科大学)

4F2-4　UC コミットメントの形式検証による厳密な仮定の導出に向けて

○櫻田英樹 (NTT コミュニケーション科学基礎研究所), 米山一樹 (NTT セキュアプラットフォーム研究所), 花谷嘉一 (東芝 研究開発センター), 吉田真紀 (情報通信研究機構)

4F2-5　暗号プロトコル安全性検証の可視化に向けて

○吉田真紀 (情報通信研究機構), 水野修 (京都工芸繊維大学)