2024 年 12 月 13 日

第 9 回 宮地研究室
情報セキュリティフォーラム

プログラム

MiYaJi Laboratory

目　次

参加 Zoom ミーティング
https://zoom.us/j/98431810445?pwd=CiF2UHbwxHeu6qqC8lPzHJ5lcRH7nC.1

ミーティング ID: 984 3181 0445
パスコード: 449915

第 9 回 宮地研究室 情報セキュリティフォーラム

趣旨

昨今，あらゆるモノがインターネットにつながる IoT が多くの注目を集め，新たなビジネスの拡大が期待されています．宮地研究室においても最新のトピックに対応するために，積極的に研究成果の対外発表を行うと共に，外部の講師による招待講演を行い，最新の研究成果，社会のニーズの動向を取り入れるように努力しております．

また，本年度は大阪大学に研究室を開設してから 9 年目となり，大阪大学内外から多数の学生が研究室に参加し，大阪大学における研究室活動も軌道に乗りました．修了生（重複，在校生，研究生を含む）も合計 221 名（博士卒 22 名，修士卒 126 名，学士卒 29 名），在学生(32 名，研究生 1 名）となり，国内でも有数の歴史と伝統のある研究室となっております．

宮地研究室では，セキュリティ人材の輩出にむけて，学部生 Basic SecCap，大学院生 SecCap そして 2018 年度より開講しました社会人向け教育プログラム ProSec を運用しております．阪大 ProSec では大学の助教ポジションの人から官公庁，メーカなどの企業，また，税理士事務所など多岐にわたる社会人学生がセキュリティ研究に励んでいます．

日々の研究室活動では，宮地先生のご指導の下，樽谷優弥 講師，奥村伸也 助教，博士後期課程の学生 6 名と博士前期課程の学生 18 名，学部の学生 8 名，研究生 1 名が各種セキュアプロトコル，暗号解析，AI セキュリティ，耐量子暗号，プライバシなど幅広く情報セキュリティの各分野の研究に取り組んでおります．2022 年より，セコム財団の支援による未知の攻撃の予測研究も実施しております．本フォーラムは，産業界及び教育機関，官公庁などにおける情報セキュリティに関する情報交換を行い，最新の情報セキュリティに関する活発な議論を，組織を超えて行うことを目的としています．

皆様のご参加を心よりお待ちしております．

日時：2024 年 12 月 13 日（金）

国立大学法人　大阪大学 大学院工学研究科

交流会世話人　樽谷 優弥，奥村 伸也

第 1 部 式次第

場所　大阪大学 吹田キャンパス センテラスサロン(3F)

総合司会: 藤本 聖

12:45　　開場

13:00-13:10 開会の挨拶　宮地 充子

13:10-14:40　**Session 1.**（座長：He Bingchang)

13:10-13:40 題名　攻撃手段をスコア化して行う
ペネトレーションテストの自動化手法の紹介
講演者　木藤 圭亮 (Keisuke Kito)

13:40-13:55 題名　TBA
講演者　稲村 勝樹 (Masaki Inamura)

13:55-14:20 題名　外部偽造不可能性を持つ公開鍵導出可能
鍵隔離プライバシー保護署名の一般的構成について
講演者　江村 恵太(オンライン) (Keita Emura)

14:20-14:35 題名　汎用なデータに対するプライバシーを保護した機械学習
講演者　柳下 智史 (Tomoshi Yagishita)

14:35-14:50 自己紹介①

14:50-15:05 休憩 ＆ movie

15:05-16:35　**Session 2.**（座長：Mohamed Bourefis)

15:05-15:30 題名　クロスチェーンコミュニケーションにおけるプライバシー保護された
効率的な M+1st price sealed bid auction
講演者　宮地 秀至 (Hideaki Miyaji)

15:30-15:45 題名　Updatable Public Key Encryption with Unlimited Update Times
based on lattice
講演者　Chen Kaiming

15:45-16:10 題名　ブロックチェーンを用いた電子投票について
講演者　面 和成 (Kazumasa Omote)

16:10-16:20 自己紹介②

16:20-16:30 2024 年度宮地研究室・修了生活動報告　奥村 伸也

16:30-16:35 2025 年度宮地研究室運営予定紹介と
第 10 回宮地研究室セキュリティ交流会予定　樽谷 優弥

写真・動画撮影：田村 昂輔, 山田 麟太郎

※講演時間：質疑応答 5 分

※自己紹介（一人 1 分）順番は下記参照

第２部　（ランプセミナー）式次第

場所　大阪大学 吹田キャンパス センテラスサロン(3F)

ランプセミナーは軽食を食べながら，セキュリティの近況を交換したいと思います．
オンラインで参加される方も，ぜひ，軽食などつまみながらご出席ください．

司会　De Goyon Mathieu

17:00-17:05　開会の挨拶　面 和成（Kazumasa Omote）
17:05-18:55　自己紹介③，コミュニケーションゲーム等
　18:00-18:05　修了生代表挨拶　平澤 庄次郎（Shojiro Hirasawa）
18:55-19:00　閉会の挨拶　宮地 充子

※ 自己紹介（一人１分）順番は下記のとおり．

佐藤 克洋，Chen Kaiming，林田 幸大，宮下 翔太郎，稲村 勝樹，江村 恵太，三宅 秀享，
岡本 健，上原 真悟，北澤 繁樹，宮地 秀至，木藤 圭亮，柴田 紗由美，山田 麟太郎，
久保 陽登，浅井 裕希，田村 昂輔，城戸 良祐，東 龍之介，長井 厚樹，岡田 健汰，
藤本 聖，大石 朝陽，面 和成，Chen-Mou Cheng，平澤 庄次郎，辻村 都倭，
De Goyon Mathieu，Pierre Boudvillain，Mohamed Bourefis，辻本 悠人，Pengxuan Wei，
樽谷 優弥，加藤 優一，酒井 涼多，He Bingchang，船津 颯介，川原 尚己，峰田 敏行，
筒井 大揮，宮地 充子，柳下 智史，倉本 将吾，岡田 侑里英，奥村 伸也

参加者名簿

	氏名	所属等	卒業年度，在職期間	備考
1	宮地 充子	教授		
2	奥村 伸也	助教		
3	樽谷 優弥	講師		
4	宮地 秀至	立命館大学	2022 年 博士後期	講演者
5	稲村 勝樹	広島市立大学	1999 年 博士前期	講演者
6	上原 真悟	NTTdata	2022 年 博士前期	オンライン
7	江村 恵太	金沢大学	2009 年 博士後期	講演者(オンライン)
8	岡本 健	筑波技術大	2001 年 博士後期	オンライン
9	面 和成	内閣府，筑波大学	2001 年 博士後期	講演者
10	北澤 繁樹	三菱電機	2000 年 博士後期	オンライン
11	木藤 圭亮	三菱電機	2015 年 博士前期	講演者
12	平澤 庄次郎	ビッグローブ	2008 年 博士前期	
13	三宅 秀享	東芝	2001 年 博士前期	オンライン
14	宮下 翔太郎	株式会社クニエ	2020 年 博士前期	
15	Chen-Mou Cheng	Chongqing University		オンライン
16	Sai Veerya Mahadevan	博士後期 4 年		
17	Nasratullah Ghafoori	同上		
18	De Goyon Mathieu	博士後期 3 年		
19	Chen Kaiming	同上		講演者
20	Mohamed Bourefis	博士後期 1 年		
21	He Bingchang	同上		
22	岡田 健汰	博士前期 2 年		
23	川原 尚己	同上		

	氏名	所属等	卒業年度，在職期間	備考
24	佐藤 克洋	同上		
25	田村 昂輔	同上		
26	長井 厚樹	同上		
27	東 龍之介	同上		
28	廣瀬 健二朗	同上		
29	船津 颯介	同上		
30	林田 幸大	同上		
31	Pengxuan Wei	同上		
32	Pierre Boudvillain	研究生		
33	岡田 侑里英	博士前期 1 年		
34	加藤 優一	同上		
35	城戸 良祐	同上		
36	久保 陽登	同上		
37	藤本 聖	同上		
38	峰田 敏行	同上		
39	柳下 智史	同上		
40	山田 麟太郎	同上		
41	浅井 裕希	学部 4 年		
42	大石 朝陽	同上		
43	倉本 将吾	同上		
44	酒井 涼多	同上		
45	柴田 紗由美	同上		
46	辻村 都倭	同上		
47	辻本 悠人	同上		

	氏名	所属等	卒業年度，在職期間	備考
48	筒井 大揮	学部 3 年		
49	野村 美恵	アシスタント		

講演内容（要旨）

Session 1.

題名	攻撃手段をスコア化して行うペネトレーションテストの自動化手法の紹介
講演者	木藤 圭亮
要旨	ペネトレーションテスト（以下、ペンテスト）は実際にシステムや機器に侵入を試みて、システムの脆弱性がないかどうかを確かめるテスト手法である。 近年のサイバーセキュリティの国際規格や、法規制によってペンテストの需要が高まっているが、ペンテストはサイバー攻撃を熟知したペンテスターと呼ばれる専門家によって実施される必要がある。 そこでテスト対象に合わせて適切な攻撃手段選択を行うために、攻撃手段の適合度をスコア化することでペネトレーションテストの自動化を行う手法を紹介する。 本発表の内容は Black Hat Europe 2023 Arsenal にて発表した内容である。

題名	TBA
講演者	稲村 勝樹
要旨	TBA

題名	外部偽造不可能性を持つ公開鍵導出可能鍵隔離プライバシー保護署名の一般的構成について
講演者	江村 恵太
要旨	ステルスアドレス（と決定性ウォレット）の安全性向上とプライバシー保護を目的として，Liu ら（EuroS&P 2019）により公開鍵導出可能鍵隔離プライバシー保護署名（PDPKS: Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key）が提案されている．本研究では，既存の偽造不可能性では送金者であったとしても正当な署名を作成できないことに着目し，送金者と受金者以外は正当な署名を作成できないことを定式化した外部者偽造不可能性を導入する．さらに公開鍵暗号と署名からの外部偽造不可能性を持つ PDPKS 方式の一般的構成を与える．公開鍵暗号としては CCA 安全性，匿名性，強ロバスト性を，署名としては強存在的偽造不可能性に加え，Cremers ら（IEEE S¥&P 2021）により導入された強保守的独占所有性（S-CEO: strong conservative exclusive ownership）を仮定する．提案一般的構成によりランダムオラクルを用いない初の PDPKS 方式が得られる．本内容はコンピュータセキュリティシンポジウム（CSS）2024 にて発表した内容である．

題名	汎用なデータに対するプライバシ―を保護した機械学習

講演者	柳下 智史
要旨	近年，個人データの利用が増加する中で，プライバシー保護の重要性がますます高まっている．差分プライバシー（Differential Privacy，DP）は，ノイズを加えることでプライバシーを保護する技術である．DP は中央サーバー上でプライバシーを管理するが，局所差分プライバシー（Local Differential Privacy、LDP）はローカルでプライバシーを管理することができ，ユーザーのプライバシー保護の観点からは LDP の方が優れている．既存の研究では，LDP を機械学習に適用するためのフレームワークである SUPM が提案されており，その中で WALDP というデータ型に関係なく全ての属性を均一に扱うプライバシーメカニズムが提案されている．しかし、この方法は連続値に特化したものである．本研究では，離散値を含むデータベースにも適用可能なプライバシー保護型機械学習手法を提案する．カテゴリデータに関して，目的変数における 1 の生起確率に従ってドメインを圧縮することで，ノイズの影響を減らし，既存研究と比較して，より小さい ε で高い精度を達成している．

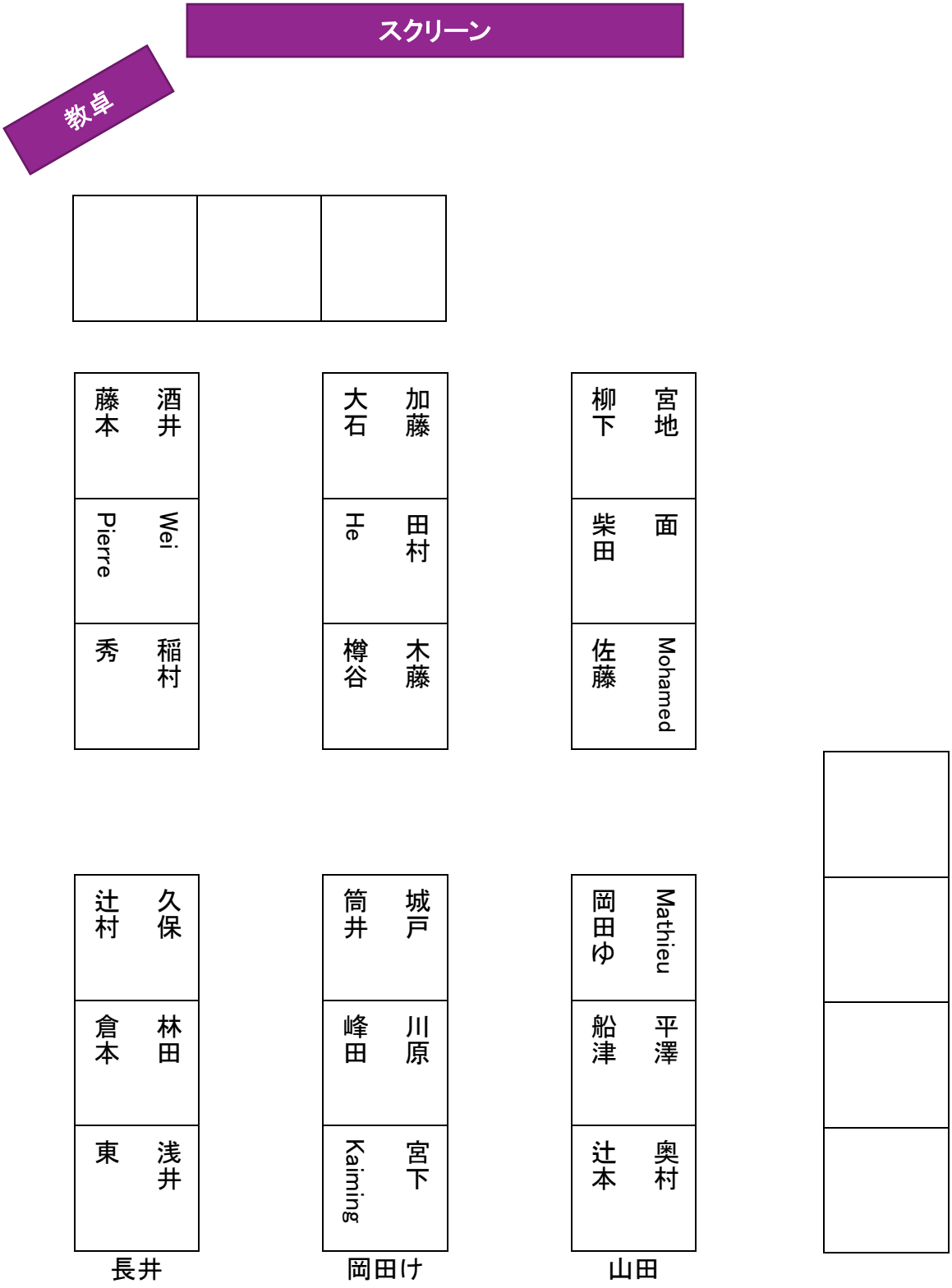
Session 2.

題名	クロスチェーンコミュニケーションにおけるプライバシー保護された効率的な M+1st price sealed bid auction
講演者	宮地秀至
要旨	既存の M+1 価格密封入札オークション方式は，オークション終了後に落札者の入札額をオープンする必要があるコミットメント方式を採用しており，プライバシーが保護されていない．さらに，クロスチェーンコミュニケーションでは複数のブロックチェーン参加者が入札者として存在するため，既存のコミットメント方式で構築することは非効率的である．本情報セキュリティフォーラムでは，クロスチェーンコミュニケーション方式において，プライバシーを保護し，効率的な M+1 価格封印入札オークションを明らかにする．

題名	Updatable Public Key Encryption with Unlimited Update Times based on lattice
講演者	Chen Kaiming
要旨	Updatable Public Key Encryption (UPKE) is an encryption scheme that enables forward secrecy in secure messaging protocols by updating the public and private keys. In the lattice-based UPKE, the update operations will accumulate the error noise in the public key, which leads to decryption failures. This drawback limits the upper bound of their update times, which becomes a challenge. In this paper, we aim to remove this bound and achieve a post-quantum UPKE with infinity update times based on the ring learning with error assumption. We formally prove the correctness and security of our proposal, demonstrating its lower communication cost compared to the existing solution. Furthermore, we show that our proposal can extend to other

	lattice-based encryption schemes where additions are available over the public and private key spaces.

題名	ブロックチェーンを用いた電子投票について
講演者	面 和成
要旨	電子投票の研究は 1980 年頃からなされており，特に最近ではブロックチェーンを用いた電子投票の研究が盛んに行われている．その一方で，投票者の意思による投票（自由投票）が脅迫者によって脅かされるリスクについての考察が不足している．本発表では，ブロックチェーンを用いた電子投票の課題について説明するとともに，最近提案したブロックチェーンベースの新たな電子投票手法を紹介する．


スクリーン
教卓
酒井 藤本
Wei Pierre
稲村 秀
加藤 大石
田村 He
木藤 樽谷
宮地 柳下
面 柴田
Mohamed 佐藤
久保 辻村
林田 倉本
浅井 東
城戸 筒井
川原 峰田
宮下 Kaiming
Mathieu 岡田ゆ
平澤 船津
奥村 辻本
長井
岡田け
山田

会場地図

大阪大学　吹田キャンパス センテラスサロン(3F)