2021 年 12 月 10 日

第 6 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

第６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五年目となり，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 176 名（博士卒 14 名，修士卒 104 名，学士卒 25 名），在学生(33 名，研究生 2 名）となり，国内でも有数の歴史ある研究室となっております．

宮地研究室では，enPiT2 Basic 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 enPiT-PRO ProSec のプロジェクトを推進しております．

また，日々の研究室活動では，宮地先生のご指導の下，高野祐輝 特任准教授，奥村伸也 助教，Yangguang Tian 助教，博士後期課程の学生 8 名と博士前期課程の学生 17 名，学部の学生 8 名，研究生 2 名が精力的に研究に取り組んでおります．

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．フォーラムは次の 2 部構成です．

第 1 部 ： 最新の研究動向及び産業界における最近のトピックスの紹介

第 2 部 ： 最近のトピックスに関するディスカッション

皆様のご参加を心よりお待ちしております．

日時：2021 年 12 月 10 日（金）第 1 部 13:00 - 17:15

第 2 部 17:30 - 19:10

国立大学法人　大阪大学 大学院工学研究科

交流会世話人　高野 祐輝，奥村 伸也，Yangguang Tian

第 1 部 式次第

場所　大阪大学吹田キャンパス センテラス

司会　Yangguang Tian

13:00-13:05 開会の挨拶　宮地 充子

（EST：9th Dec. 11 pm, BDT：10:00 am-）

13:05-14:35　**Session 1.**（座長：Yangguang Tian）

13:05-13:35 題名　メッセージ長拡張可能な耐量子暗号を用いたコミットメント方式

講演者　宮地 秀至

13:35-14:05 題名　特許法の中身

講演者　金沢 史明

14:05-14:35 題名　NTT の秘密計算

講演者　道廣 大喜

14:35-14:50 休憩

14:50-16:50　**Session 2.**（座長：Nasratullah Ghafoori）

14:50-15:20 題名　Efficient Modular Inversion Resisting Side Channel Attack

講演者　金 垚安

15:20-15:50 題名　ビデオ会議システムにおけるエンドツーエンド暗号化技術の安全性

講演者　伊藤 竜馬

15:50-16:20 題名　鍵付き完全準同型暗号について

講演者　江村 恵太

16:20-16:50 題名　NFT のセキュリティリスクについて

講演者　面 和成

16:50-17:00　2021 年度宮地研究室・修了生活動報告　奥村 伸也

17:00-17:05　2022 年度宮地研究室運営予定紹介と

第 7 回宮地研究室セキュリティ交流会予定　宮地 充子

17:05-17:10　閉会の挨拶　高野 祐輝

17:10-17:15　記念撮影

※公演時間（講演：25 分，質疑応答：5 分）

写真・動画撮影：渡辺　暸、和泉　海

第 2 部 式次第

場所　大阪大学吹田キャンパス センテラス

司会　奥村 伸也

17:30-17:35　開会の挨拶　CHENG Chen-mou

17:35-19:05　自己紹介※※　（司会　奥村 伸也）

19:05-19:10　閉会の挨拶　多田 充

17:35-18:20	Hector，三本，江村，金，宮地(秀)，金沢，　Po-Chu，Nasratullah，Sai，多田，猪本，細谷，劉，Chen-mou，李，高，傅，伊藤，新井，大久保，上原，尾崎，面，斎藤，Mamun
18:20-19:05	Rashed，高橋，長尾，松原，小木曽，渡辺，王，和泉，杉野，上杉，川口，前野，松岡，山下，山月，道廣，田辺，野村，Bingchang，Kaiming，Tian，奥村，高野，宮地

※※ 自己紹介の順番は次の通り（卒業生，教員は 3 分 00 秒，在学生は 1 分 30 秒程度）．

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	高野 祐輝	特任准教授	2004 年度 博士前期 2018 年- 講師,	
3	奥村 伸也	助教		
4	Yangguang Tian	助教		
5	鄭　振牟	金沢大学	2015-19 特任准教授	Online
6	多田 充	千葉大学	1998-2001 助手	Online
7	面 和成	筑波大学	2008 年- 特任助教 2011 年- 准教授	講演者 (Online)
8	小木曽 俊夫	国土交通省	2001 年度 博士前期	Offline
9	金沢 史明	特許庁	2004 年度 博士前期	講演者 (Online)
10	江村 恵太	NICT	2009 年度 博士後期	講演者 (Online)
11	Mohammad S.I. MAMUN	Cybersecurity National Research Council of Canada	2014 年度 博士後期	Online
11	杉野 寿美代（旧姓:石下）	防衛省陸上自衛隊	2015 年度 博士前期	Online
12	道廣 大喜	NTT 研究所	2015 年度 博士前期	講演者 (Online)
13	Rashed MAZUMDER	Jahangirnagar University	2017 年度 博士後期	Online
14	伊藤 竜馬	NICT	2018 年度 博士後期	講演者 (Online)
15	松岡 勇介	NTT ドコモ	2019 年度 博士前期	Online
16	小寺 健太	博士後期 3 年		
17	Hector Hougaard	同上		
18	三本　知明	同上		
19	金 垚安	博士後期 2 年		講演者
20	宮地　秀至	同上		講演者

	氏名	所属等	卒業年度	備考
21	Po-Chu Hsu	同上		
22	Nasratullah Ghafoori	博士後期 1 年		
23	Sai Veerya Mahadevan	同上		
24	猪本 卓也	博士前期 2 年		
25	細谷 昂平	同上		
26	劉 小竜	同上		
27	李 君如	同上		
28	高 月	同上		
29	傅 一舟	同上		
30	新井 颯斗	博士前期 1 年		
31	上原 真悟	同上		
32	大久保 佑弥	同上		
33	尾崎 純平	同上		
34	斎藤 文弥	同上		
35	高橋 朋伽	同上		
36	長尾 佳高	同上		
37	松原 功樹	同上		
38	渡辺 暸	同上		
39	王 昱森	同上		
40	和泉 海	学部 4 年		
41	上杉 慧至	同上		
42	川口 哲弘	同上		
43	前野 優太	同上		
44	山下 慎太郎	同上		

	氏名	所属等	卒業年度	備考
45	山月 達太	学部 4 年		
46	田辺 一葵	学部 3 年		
47	He Bingchang	研究生		
48	Chen Kaiming	同上		
49	野村 美恵	アシスタント		

第 1 部 講演内容（要旨）

Session 1.

題名	メッセージ長拡張可能な耐量子暗号を用いたコミットメント方式
講演者	宮地 秀至
要旨	コミットメント方式はゼロ知識証明などの基本的な暗号作業に不可欠な要素である．近年，格子暗号は耐量子暗号として実用化に向けた研究が行われている．その一つに格子暗号を用いたコミットメント方式の研究が行われている．コミットメント方式では，短いメッセージだけでなく任意のメッセージを出力する必要がある．大きなメッセージを送信するためには，メッセージ文字列のサイズを大きくすることがコミットメント方式の重要な課題の一つである．メッセージ文字列のサイズを大きくするために Baum らは，2018 年に大きなメッセージサイズの送信を可能にするコミットメント方式を構築した．しかし，入力の部分にメッセージだけでなくメッセージ以外の目的で利用される空間が適用されており，メッセージに適用可能な空間はより大きくできる余地がある．本提案では，Baum らが提案したコミットメント方式のメッセージ空間をより大きくするコミットメント方式を提案し，その安全性である束縛性と秘匿性を証明する．

題名	特許法の中身
講演者	金沢 史明
要旨	特許法に含まれる条文とその条文の意味を、誤解を恐れずに、紹介する。

題名	NTT の秘密計算
講演者	道廣 大喜
要旨	近年、データを利活用してサービスや意思決定に活かす機運が高まっていると同時に、個人に関わる情報がますます取得蓄積されることからプライバシーに対する意識も高まっている。こうした背景から秘密計算技術が注目を集めている。秘密計算はデータを暗号化したまま計算・処理する技術であり世界的に研究開発が進められている。本講演では NTT が研究開発している秘密計算技術について取り組み事例を交えて紹介する。

Session 2.

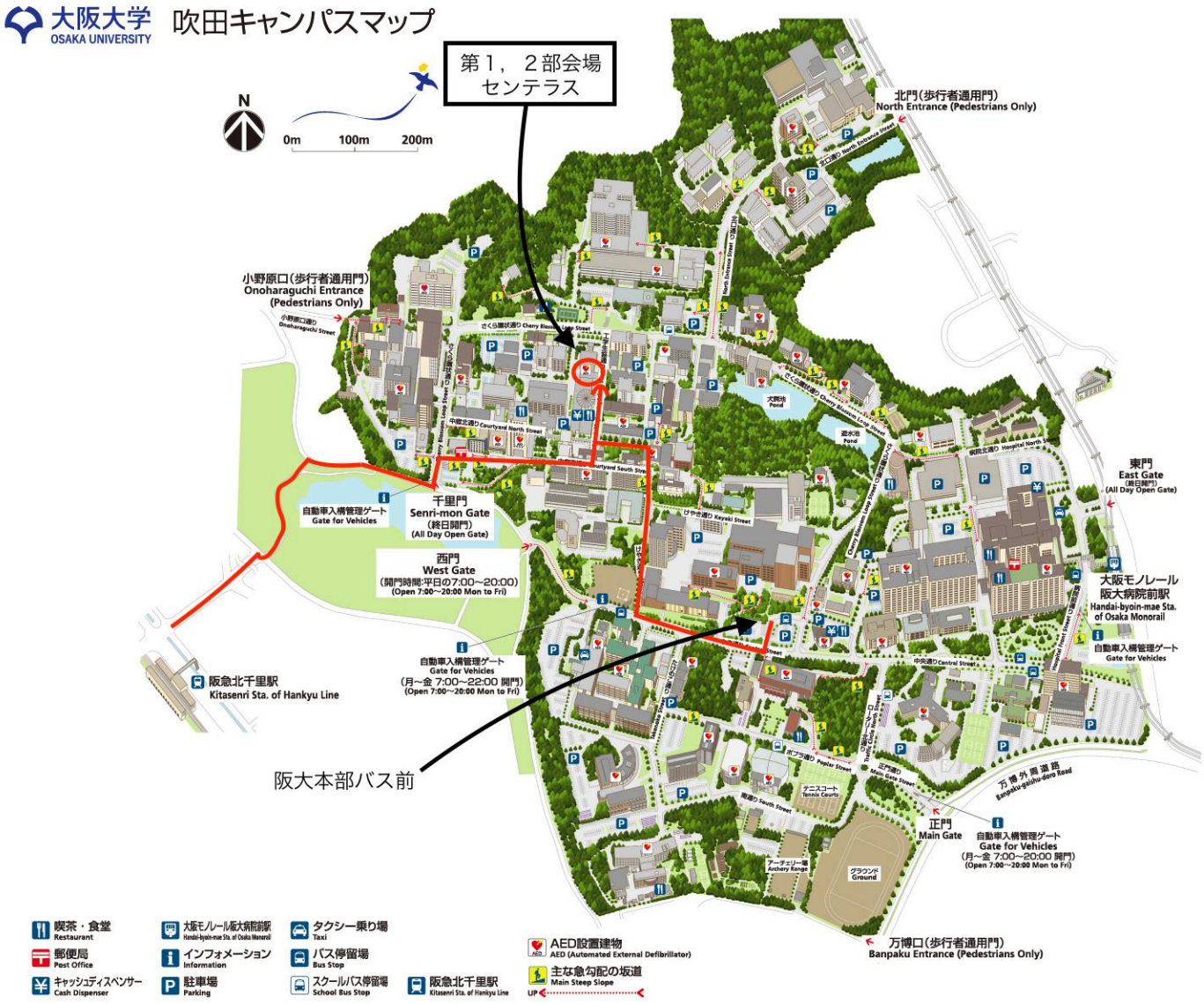
題名	Efficient Modular Inversion Resisting Side Channel Attack
講演者	金 垚安
要旨	With the development of side channel attack (SCA), theoretically proved secure cryptosystems, digital signatures, protocols, etc. are no longer secure on internet of things (IoT) devices or PC. Targeting the SCA weakness of binary extended euclidean algorithm (BEEA), simple power analysis (SPA), cache-timing attack(CTA) and machine learning based profiling attack (ML-PA) were conducted on RSA and ECDSA with high success rate[Ald+17,Ald +19,ACSS17,DELAFE21]. [JW14] and [BY19] proposed constant-time modular inversion methods, which can resist such attacks but lost efficiency. Our new constant-time modular inversion algorithm, which combines the idea of BEEA and the fact, for any integer A and B, GCD(A, B) = GCD(B, A-B) = GCD(A, A-B), differs from them. It can resist SPA, differential power analysis (DPA), timing attack, cache-timing attack of SCA and compute modular inversion faster. We analyse SCA security and efficiency of our work from a theoretical and experimental point of view.

題名	ビデオ会議システムにおけるエンドツーエンド暗号化技術の安全性
講演者	伊藤 竜馬
要旨	新型コロナウイルス感染症の世界的流行に伴い，ビデオ会議システムの利用が世界中で拡大している．また，ユーザのプライバシーを保護するためにエンドツーエンド暗号化（E2EE）技術の必要性も高まっており，多くのビデオ会議システムにおいて E2EE 技術の導入計画が進行中である． 本講演では，代表的なビデオ会議システムの Google Duo，Cisco Webex，Jitsi Meet などで導入される E2EE 技術 SFrame の安全性について紹介する．はじめに，Internet Engineering Task Force（IETF）が公開するインターネットドラフトのバージョン draft-omara-sframe-01 に基づき，SFrame の仕様について紹介する．次に，SFrame に内在する複数の脆弱性を明らかにするとともに，これらの脆弱性を悪用することで偽造攻撃が現実的な計算量で実行できることを示す．最後に，これらの攻撃に対する効果的な対策手法について紹介する． 我々の評価結果については SFrame の設計者に報告済みであり，本講演で紹介する攻撃が全て実現することを確認している．また，SFrame の設計者は我々の脆弱性報告を受けて仕様を修正し，インターネットドラフトのバージョンを draft-omara-sframe-02 に更新した．なお，2021 年 12 月現在，インターネットドラフトのバージョンは draft-omara-sframe-03 である．

題名	鍵付き完全準同型暗号について
講演者	江村 恵太
要旨	安全な暗号方式を構成する際には，元となる数学的問題の困難性と共に，強い安全性モデルを採用する必要がある．例えば，楕円曲線上離散対数問題に基づく CCA 安全な公開鍵暗号は量子コンピュータの出現により安全ではなくなり，格子問題に基づく CPA 安全な公開鍵暗号は（いくら格子問題が量子コンピュータをもってしても困難であるといえども）CCA 攻撃に弱い．本講演では通常 CCA 安全性を達成できない準同型暗号の安全性を向上させた鍵付き準同型暗号について，その歴史と構成アイディア，特に鍵付き完全準同型暗号について紹介する．

題名	NFT のセキュリティリスクについて
講演者	面 和成
要旨	2021 年に入ってから非代替性トークン（NFT）が注目を集めている．NFT は暗号資産と同様にブロックチェーン上で取引されるものであり，アート作品等の所有権移転に用いられている．しかし，NFT に対するセキュリティがあまり考えられていないという現状がある．本発表では，NFT に対する攻撃を整理し，NFT のセキュリティリスクについて考察する．

会場地図


大阪大学 OSAKA UNIVERSITY
吹田キャンパスマップ
第１，２部会場
センテラス
N
0m 100m 200m
北門（歩行者通用門）
North Entrance (Pedestrians Only)
小野原口（歩行者通用門）
Onoharaguchi Entrance
(Pedestrians Only)
千里門
Senri-mon Gate
(終日開門)
(All Day Open Gate)
自動車入構管理ゲート
Gate for Vehicles
西門
West Gate
(開門時間:平日の7:00～20:00)
(Open 7:00～20:00 Mon to Fri)
阪急北千里駅
Kitasenri Sta. of Hankyu Line
自動車入構管理ゲート
Gate for Vehicles
(月～金 7:00～22:00 開門)
(Open 7:00～20:00 Mon to Fri)
阪大本部バス前
東門
East Gate
(終日開門)
(All Day Open Gate)
大阪モノレール
阪大病院前駅
Handai-byoin-mae Sta.
of Osaka Monorail
自動車入構管理ゲート
Gate for Vehicles
正門
Main Gate
自動車入構管理ゲート
Gate for Vehicles
(月～金 7:00～20:00 開門)
(Open 7:00～20:00 Mon to Fri)
万博外周道路
Banpaku-gaishu-doro Road
万博口（歩行者通用門）
Banpaku Entrance (Pedestrians Only)
喫茶・食堂 Restaurant
郵便局 Post Office
キャッシュディスペンサー Cash Dispenser
大阪モノレール阪大病院前駅 Handai-byoin-mae Sta. of Osaka Monorail
インフォメーション Information
駐車場 Parking
タクシー乗り場 Taxi
バス停留場 Bus Stop
スクールバス停留場 School Bus Stop
阪急北千里駅 Kitasenri Sta. of Hankyu Line
AED設置建物 AED (Automated External Defibrillator)
主な急勾配の坂道 Main Steep Slope
UP