2023 年 12 月 8 日

第 8 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/98999111703?pwd=SUhETHY0d29Hck1RY3ZMYnNZdzRUdz09

ミーティング ID: 989 9911 1703
パスコード: 696698

第８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 8 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 210 名（博士卒 20 名，修士卒 118 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，王 贇弢 講師，奥村伸也 助教，博士後期課程の学生 5 名と博士前期課程の学生 19 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：2023 年 12 月 8 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　王 贇弢，奥村 伸也

第 1 部 式次第

場所　大阪大学吹田キャンパス E1-217

総合司会:田川

12:30　　開場

12:45-12:55 開会の挨拶　宮地 充子

13:00-14:30　Session 1.

13:00-13:30 題名　ブロックチェーンセキュリティに関する最近の研究の紹介

講演者　面　和成

13:30-14:00 題名　フォワード安全な公開鍵検索可能認証暗号の一般的構成について

講演者　江村　恵太

14:00-14:30 題名　Isogeny-based Multi-signature

講演者　Mathieu de Goyon

14:30-15:00 休憩

15:00-16:30　Session 2.

15:00-15:30 題名　ブロックチェーンに適用可能な

キーバリューコミットメント方式の構成

講演者　宮地秀至

15:30-16:00 題名　On Security Assessment of Symmetric Key Cryptography,

A Case Study of Salsa20 and ChaCha

講演者　Nasratullah Ghafoori

16:00-16:15　2023 年度宮地研究室・修了生活動報告　奥村伸也

16:15-16:30　2024 年度宮地研究室運営予定紹介と

第 8 回宮地研究室セキュリティ交流会予定　王 贇弢

16:30-　　コーヒーブレーク

※公演時間（講演：25 分，質疑応答：5 分）

写真・動画撮影：和泉 海，田村 昂輔，山田麟太郎

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 E1-217

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．

17:00-18;30　　意見交換会①

17:00-17:45　　自己紹介※※　（司会　前半：前野 優太　後半：山月 達太）

17:45-18:30　　意見交換会②

17:00-17:45	Nasratullah，Sai，De Goyon，Chen Kaiming，Mohamed，上杉，田川，寺田，中島，前野，山下，山月，Bingchang，岡田健，川原，佐藤，田村，長井，川田，多田先生，稲村先生，宮地秀先生，奥村先生，王先生

17:45-18:30	林田，東，廣瀬，船津，Wei，城戸，峰田，森園，柳下，山田，岡田侑，杉野，Mazumder 先生，波多野，上原，高橋，Chen-Mou Cheng 先生，宮地先生

※※ 自己紹介の順番は次の通り（卒業生，教員は 3 分，在学生は 2 分程度）．

第 3 部 式次第

場所　大阪大学吹田キャンパス　E1-217

18:30-19:00　題名　preon: digital signature from zk-SNARK

講演者　Chen-Mou Cheng

19:00-19:15　閉会のあいさつ　上杉慧至

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	王 贇弢	講師		
4	宮地 秀至	立命館大学	2022 年 博士後期	講演者
5	伊藤 久繁	三菱	2009 年 博士前期	
6	多田 充	千葉大学		
7	江村 恵太	金沢大学	2009 年 博士後期	講演者
8	面 和成	内閣府，筑波大学	2001 年 博士後期	講演者
9	杉野 寿美代	自衛隊	2015 年 博士前期	
10	Chen-Mou Cheng	Chongqing University		講演者
11	Rashed Mazumder	Jahangirnagar University	2017 年 博士前期	
12	波多野 哲也	半田市役所	2009 年 博士前期	
13	稲村 勝樹	東京電機大学研究推進社会連携センター 准教授	1999 年 博士前期	
14	上原 真悟	NTT データ	2022 年 博士前期	
15	高橋 朋伽	メガチップス	2022 年 博士前期	
16	川田 元	大阪大学大学院情報科学研究科	2022 年 学部	
17	Sai Veerya Mahadevan	博士後期 3 年		
18	Nasratullah Ghafoori	同上		講演者
19	De Goyon Mathieu	博士後期 2 年		講演者
20	Chen Kaiming	同上		

21	上杉 慧至	博士前期 2 年		
22	田川 雄大	同上		
	名前	所属等	卒業年度	備考
23	寺田 誠志郎	同上		
24	中島 克也	同上		
25	前野 優太	同上		
26	山下 慎太郎	同上		
27	山月 達太	同上		
28	He Bingchang	同上		
29	岡田 健汰	博士前期 1 年		
30	川原 尚己	同上		
31	佐藤 克洋	同上		
32	田村 昂輔	同上		
33	長井 厚樹	同上		
34	東 龍之介	同上		
35	船津 颯介	同上		
36	廣瀬健二朗	同上		
37	林田 幸大	同上		
38	Pengxuan Wei	同上		
39	Yang Chaohsun	研究生		
40	城戸 良祐	学部 4 年		
41	峰田 敏行	同上		
42	森園 涼斗	同上		
43	柳下 智史	同上		
44	山田 麟太郎	同上		

45	岡田 侑里英	学部 3 年		
46	野村 美恵	アシスタント		

講演内容（要旨）

Session 1.

題名	ブロックチェーンセキュリティに関する最近の研究の紹介
講演者	面 和成
要旨	ブロックチェーンに関連する研究論文が世界的に増加傾向にある．その一方で，非中央集権型ネットワーク技術の一つであるブロックチェーンへのサイバー攻撃が年々増加しており，新たな攻撃やリスクが発生している．本発表では，ブロックチェーン技術におけるセキュリティ面を中心に，ブロックチェーンへの攻撃，及びブロックチェーンを悪用した攻撃に関するセキュリティ・リスクについての最新の研究内容をいくつかピックアップして紹介する．

題名	フォワード安全な公開鍵検索可能認証暗号の一般的構成について
講演者	江村 恵太
要旨	本講演では，公開鍵検索可能認証暗号（PAEKS: Public key Authenticated Encryption with Keyword Search）にフォワード安全性を付加する一般的構成を紹介する．ここでフォワード安全性とは，過去作成された検索クエリを用いても新たに作成された暗号文に対する検索ができないことを指す．提案構成法は PAEKS 方式と 0/1 エンコーディング（Lin-Tzeng@ACNS2005）から成り，Qin らのペアリングベース PAEKS 方式（ProvSec2021），Cheng-Meng の格子ベース PAEKS 方式を用いることでペアリング/格子ベースフォワード安全 PAEKS 方式がそれぞれ得られる．さらに Emura による PAEKS の一般的構成（ACM APKC 2022/IEICE Trans. 2024）を用いることで，ランダムオラクルを用いないフォワード安全 PAEKS 方式も得られる．

題名	Isogeny-based Multi-signature
講演者	Mathieu de Goyon
要旨	Multi-signatures are protocols that allow multiple signers to produce a joint signature on the same message. In recent years, multi-signature schemes have been proposed in lattice-based cryptography as well as pairing-based cryptography but there are currently no multi-signature schemes in isogeny-based cryptography. We propose a multi-signature scheme by extending the Commutative Supersingular Isogeny based Fiat-Shamir signature (CSI-FiSh), as well as its variant CSI-FiSh with Sharing-friendly Keys (CSI-SharK) to the multiple signers setting. To adapt our scheme to isogeny-based

	cryptography, we use a round-robin during both the key aggregation and the signature aggregation. We also prove the security of our scheme against honest-but-curious adversaries in the Random Oracle Model (ROM) by using the Double Forking Lemma Technique. We finally discuss how to change the protocol to make it actively secure.

Session 2.

題名	ブロックチェーンに適用可能なキーバリューコミットメント方式の構成
講演者	宮地秀至
要旨	コミットメント方式は，受信者が検証可能な暗号方式である．ブロックチェーンは中央集権が期待されるシステムであるが，スケーラビリティが問題になっている．本発表では，コミットメント方式の応用であるキーバリューコミットメント方式を用いてブロックチェーンのスケーラビリティを改善する研究を紹介する．

題名	On Security Assessment of Symmetric Key Cryptography, A Case Study of Salsa20 and ChaCha
講演者	Nasratullah Ghafoori
要旨	Symmetric key cryptography stands as a well-explored field of security. Yet, with the introduction and adoption of new ciphers, the necessity for fresh attack methods emerges. Today, I aim to address the current state of research surrounding the ChaCha stream cipher, notably embraced within TLS 1.3. Its inclusion signifies a significant step forward yet necessitates robust cryptanalysis to ensure its resilience. This speech is dedicated to clarifying the ongoing trends in ChaCha's analysis. I will talk about existing research, uncovering vulnerabilities, and challenges. Additionally, I will highlight our contributions to this field, enhancing our comprehension of ChaCha and fortifying its security.

第 3 部

題名	preon: digital signature from zk-SNARK
講演者	Chen-Mou Cheng
要旨	General-purpose proving systems have been undergoing rapid development in recent years. They are usually a Fiat-Shamir transformed interactive protocol in which a prover can convince a verifier that the prover knows a secret witness for the truthfulness of a somewhat general statement. When this statement is about

	knowledge of a secret, we can construct signature schemes, e.g., following the MPC-in-the-head paradigm, as well as based on zk-STARK. One may (rightly) expect that a major drawback of such an approach is the overhead in terms of space and time one needs to pay in constructing a signature scheme from a general-purpose proving system, as we do not have access to any of the optimization opportunities brought about by specialization. However, we argue for this approach because it can bring a long-term advantage as follows. Once we have a (secure) signature scheme constructed from a general-purpose proving system like this, the flexibility of the latter would easily allow us to enhance the functionalities of the former and build at a minimum cost advanced schemes like group signatures, attribute-based signatures, functional signatures, ..., to name a few, by proving a suitable (and potentially more complicated) statement in the proving system. Thus, the tremendous amount of investment that goes into a unified process of security analysis, standardization, implementation, deployment, as well as post-deployment continual improvement and optimization can pay lucrative dividends across a broader and fast-growing landscape of applications, compared with the alternative approach of independently standardizing all these different signature schemes individually, necessarily having to start from scratch and repeating much of the work every time. Following this philosophy, I will introduce preon, a signature scheme constructed on top of the Aurora zk-SNARK in this talk, detailing some of the trade-offs made in its design, as well as lessons learned in the process.

教卓

一列残す

Nas	奥村	Mohamed	宮地	田川	Wang
中島	森園	山下	山田	Bing chang	秀
川原	廣瀬	田村	Wei	林田	城戸

カメラ

Mathieu	舩津	上杉	Arthur	寺田	峰田
前野	柳下	山月	岡田y	岡田k	Chen
佐藤	江村	長井	川田	東	

会場地図

大阪大学　吹田キャンパス