2022 年 12 月 12 日

第 7 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

趣旨　. . . . .　1

第１部　式次第　. . . . .　2

第２部　式次第　. . . . .　3

参加者名簿　. . . . .　4

第１部　講演内容（要旨）　. . . . .　7

会場地図　. . . . .　10

第７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７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 194 名（博士卒 17 名，修士卒 106 名，学士卒 28 名），在学生(39 名，研究生４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，王 贇弢 講師，奥村伸也 助教，博士後期課程の学生７名と博士前期課程の学生 22 名，学部の学生 10 名，研究生４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（ランプセミナー）

皆様のご参加を心よりお待ちしております．

日時：2022 年 12 月 12 日（月）第１部 13:00 – 16:45

第２部 17:15 – 19:15

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

司会　金 垚安

13:00-13:05 開会の挨拶　宮地 充子

(EST：11th Dec. 11 pm, BDT：10:00 am-)

13:05-14:35　**Session 1.** (座長：Chen Kaiming)

13:05-13:35 題名　最近の裁判例 2 件の紹介

講演者　金沢 史明

13:35-14:05 題名　決済サービスにおけるセキュリティの現状

講演者　田村 裕子

14:05-14:35 題名　Differential Cryptanalysis of Salsa20 Based on Comprehensive Analysis of PNBs

講演者　Nasratullah Ghafoori

14:35-14:50 休憩

14:50-16:20　**Session 2.** (座長：De Goyon Mathieu)

14:50-15:20 題名　Scalable and Public-Verifiable M+1st Price Aution on Smart Contract

講演者　Po-Chu Hsu

15:20-15:50 題名　暗号資産・ブロックチェーンに関する最近の動向

講演者　面 和成

15:50-16:20 題名　公開鍵検索可能暗号の一般的構成について

講演者　江村 恵太

16:20-16:30　2022 年度宮地研究室・修了生活動報告　王 贇弢

16:30-16:35　2023 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　宮地 充子

16:35-16:40　閉会の挨拶　王 贇弢

16:40-16:45　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，田村 昂輔

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

司会　金 垚安，宮地 秀至

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．

17:15-17:20　開会の挨拶　面 和成

17:20-19:10　自己紹介※※　（司会　前半：金 垚安　後半：宮地 秀至）

19:10-19:15　閉会の挨拶　松中 隆志

17:20-18:15	王(贇)，西田，宮地(秀)，Po-chu，Nasratullah，Sai，伊藤，De Goyon，Chen，新井，上原，大久保，江村，尾崎，斎藤，髙橋，長尾，松原，渡辺，Chen-mou，王(昱)，李，高，和泉，田村

18:15-19:10	三本，金，上杉，田川，寺田，中島，前野，山下，山月，松中，Bingchang，岡田，川田，川原，佐藤，面，田村(昂)，長井，東，舩津，Paul，城戸，Wei，奥村，宮地

※※ 自己紹介の順番は次の通り（卒業生，教員は 3 分，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	奥村 伸也	助教		
3	王 贇弢	講師		
4	鄭 振牟	金沢大学	2015-19 特任准教授	Offline
5	面 和成	筑波大学	2008 年- 特任助教 2011 年- 准教授	講演者
6	田村 裕子	日本銀行	2003 年度 博士後期	講演者 (Online)
7	金沢 史明	特許庁	2004 年度 博士前期	講演者 (Online)
8	西田 梢	テラスカイ	2005 年度 博士後期	Online
9	江村 恵太	NICT	2009 年度 博士後期	講演者 (Online)
10	伊藤 竜馬	NICT	2018 年度 博士後期	Online
11	松中 隆志	ATR	2003 年度 博士前期	
12	三本 知明	ATR	2021 年度 博士後期	
13	宮地 秀至	博士後期 3 年		
14	金 垚安	同上		
15	Po-Chu Hsu	同上		講演者
16	Nasratullah Ghafoori	同上		講演者 (Online)
17	Sai Veerya Mahadevan	博士後期 2 年		
18	De Goyon Mathieu	博士後期 1 年		
19	Chen Kaiming	同上		
20	新井 颯斗	博士前期 2 年		
21	上原 真悟	同上		

22	大久保 佑弥	同上		
	氏名	所属等	卒業年度	備考
23	尾崎 純平	同上		
24	斎藤 文弥	同上		
25	高橋 朋伽	同上		
26	長尾 佳高	同上		
27	松原 功樹	同上		
28	渡辺 暸	同上		
29	王 昱森	同上		
30	李 君如	同上		
31	高 月	同上		
32	和泉 海	博士前期 1 年		
33	上杉 慧至	同上		
34	田川 雄大	同上		
35	寺田 誠志郎	同上		
36	中島 克也	同上		
37	前野 優太	同上		
38	山下 慎太郎	同上		
39	山月 達太	同上		
40	He Bingchang	同上		
41	岡田 健汰	学部 4 年		
42	川田 元	同上		
43	川原 尚己	同上		
44	佐藤 克洋	同上		
45	田村 昂輔	同上		

46	長井 厚樹	同上		
	氏名	所属等	卒業年度	備考
47	東 龍之介	同上		
48	船津 颯介	同上		
49	Paul Kunal	同上		
50	城戸 良祐	学部 3 年		
51	Pengxuan Wei	研究生		
52	野村 美恵	アシスタント		

第 1 部 講演内容（要旨）

Session 1.

題名	最近の裁判例 2 件の紹介
講演者	金沢 史明
要旨	以下の裁判例 2 件を，誤解を恐れずに単純化して，紹介する． ・東京地裁 令和元年(ワ)第 25152 号(令和 4 年 3 月 24 日判決言渡) ・知財高裁 平成 30 年(ネ)第 10077 号(令和 4 年 7 月 20 日判決言渡)

題名	決済サービスにおけるセキュリティの現状
講演者	田村 裕子
要旨	近年，金融サービスを提供する手段として，スマートフォンの存在感が一段と増しており，これを利用した新しいサービスが次々と展開されている．こうした金融サービスがスマートフォンに搭載されるようになると，それらを狙った犯罪も増えてくることが懸念される．実際に，他人のクレジットカードや銀行口座をスマートフォン・アプリに登録し，取引や決済が不正に行われた事件も発生している．本講演では，過去に発生した事例を参照しながら，スマートフォンを利用した決済サービスのセキュリティについて考察を行う．

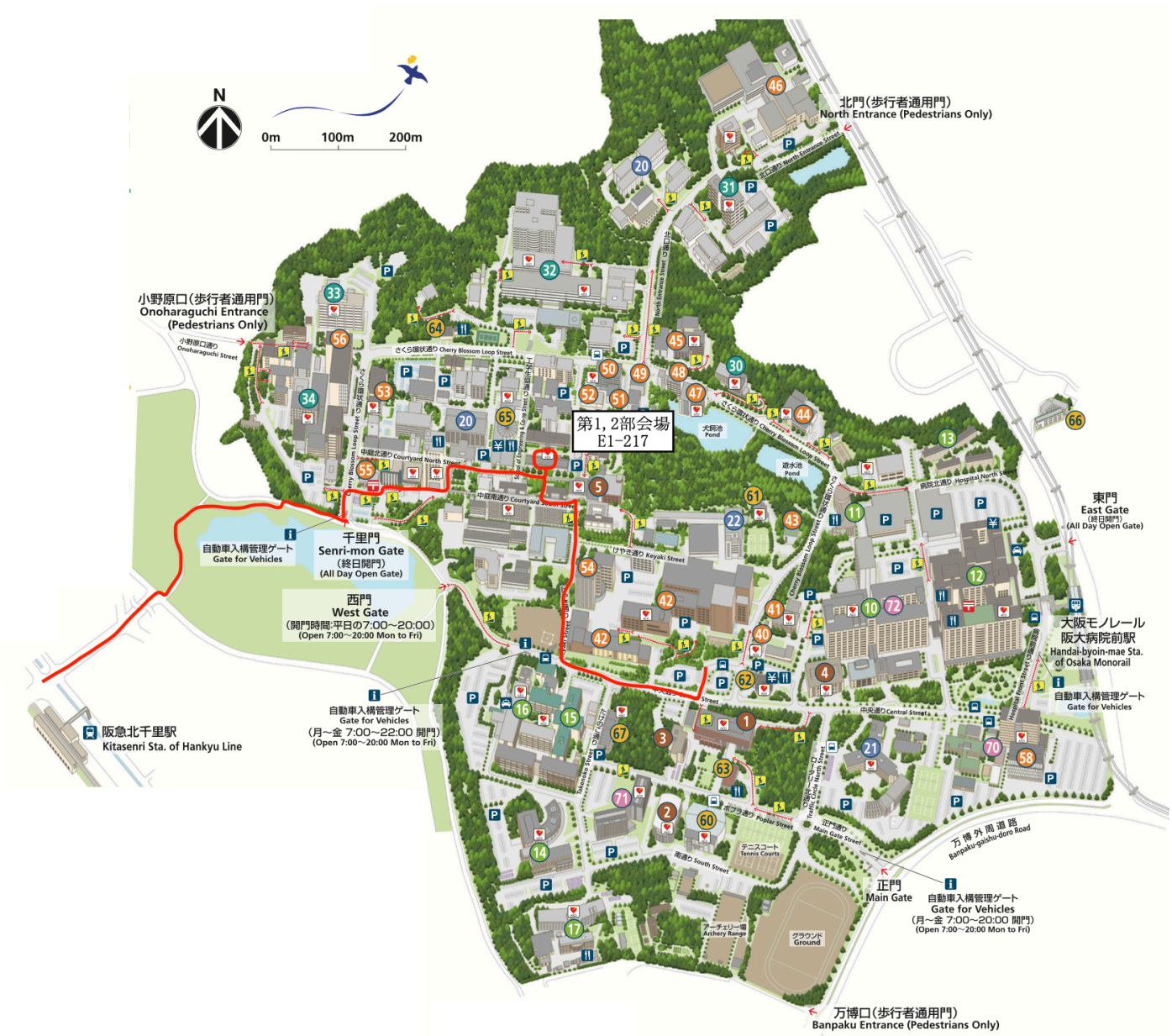
題名	Differential Cryptanalysis of Salsa20 Based on Comprehensive Analysis of PNBs
講演者	Nasratullah Ghafoori
要旨	This paper focuses on the differential cryptanalysis of the Salsa20 stream cipher. The existing differential cryptanalysis approaches first study the differential bias of the Salsa20 stream cipher and then search for *probabilistic neutral bits* (PNBs). However, the differential bias and the set of PNBs obtained in this method are not always the optimal solution. To figure out a better solution, we apply the *differential cryptanalysis based on the comprehensive analysis of PNBs* on the reduced-round Salsa20. At first, we comprehensively analyze the neutrality measure of all keybits concerning all output differential OD bits. Afterward, we select the OD bit position with the best neutrality measure and look for the corresponding input differential ID with the best differential bias. Taking everything into account, the proposed approach could be used to attack Salsa20/8 with a time complexity of 2^144.75 and a data complexity of $2^{55.74}$.

Session 2.

題名	Scalable and Public-Verifiable M+1st Price Auction on Smart Contract
講演者	Po-Chu Hsu
要旨	The second-price sealed-bid auction, also called the Vickrey auction, is studied by Nobel prize winner William Vickrey that can incentify the bidders to bid their true value and maximize the seller's income. In the auction, each bidder submits a sealed bid to the manager at the same time. The highest bidder wins the auction and only needs to pay the second-highest price. To compare sealed bids without revealing them, trusted managers are commonly used. However, a trusted manager does not exist in the real world. Smart Contracts can act as a distributed and publicly verifiable manager. We built an auction protocol by using Smart Contract as the manager and overcome the problem that Smart Contract cannot hide secrets. We also largely improved the efficiency and scalability such that our auction protocols can be used in the real world.

題名	暗号資産・ブロックチェーンに関する最近の動向
講演者	面 和成
要旨	暗号資産・ブロックチェーンは近年，実用面だけでなく研究面においても注目を集めている．その一方で，暗号資産に関するインシデントが数多く発生しておりそのリスクを把握しておくことも重要である．本発表では，情報セキュリティ分野においてブロックチェーン研究が世界的に増加している点や暗号資産に関するインシデント被害が年々増加傾向にある点などについて報告する．

題名	公開鍵暗号検索可能暗号の一般的構成について
講演者	江村 恵太
要旨	公開鍵検索可能暗号について，匿名 ID ベース暗号からの一般的構成を紹介する．さらに公開鍵検索可能暗号において，検索時に送付するトラップドアからキーワードに関する情報が漏洩している問題の対策手法，検索がヒットしない条件定義の重要性，および PEKS の拡張方式として平文一致確認可能暗号について紹介する．

会場地図

大阪大学　吹田キャンパス