

# 量子情報社会に向けた数理的アプローチ

開催時期 2018-09-17 13:00～2018-09-19 11:45

場所 〒814-0002 福岡市早良区西新2-16-23 九州大学 西新プラザ 大会議室A

## 量子情報社会に向けた数理的アプローチ

Mathematical approach for quantum information society

※ この研究集会はマス・フォア・インダストリ研究所 共同利用研究の公開プログラムです。

開催期間 2018年9月17日(月) ～ 9月19日(水)

開催場所 〒814-0002 福岡市早良区西新2-16-23  
[九州大学西新プラザ 大会議室A](#), [アクセス](#)

【プログラ  
ム】

(全11講  
演) 13:00 開場  
13:15 - 13:25 開会式

13:30 - 14:30

講演者：青野 良範 (NICT)

講演タイトル：**LOTUS: a conservative PKE/KEM scheme**

14:45 - 15:45

講演者：秋山 浩一郎 (東芝)

講演タイトル：**A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus(TM))**

16:00 - 17:00

講演者：鶴丸 豊広 (三菱電機)

講演タイトル：**Leftover Hashing Lemma as Quantum Error Correction**

9月18日(火)

9:00 開場

9:30 - 10:30

講演者：池松 泰彦 (東京大学)

講演タイトル：**The multivariate encryption scheme HFERP**

10:40 - 11:40

講演者：鹿野 豊 (慶応義塾大学)

講演タイトル : **How to understand the cloud quantum computer**

13:10 - 14:10

講演者 : 栗原 大武 (北九州高専)

講演タイトル : **POVM from the viewpoints of combinatorics**

14:20 - 15:20

講演者 : 吉田 雅一 (長崎県立大学)

講演タイトル : **Solutions to a retrodiction problem by using quantum error-correcting codes**

15:30 - 16:30

講演者 : Phong Nguyen (INRIA / 東京大学)

講演タイトル : **Searching for Short Lattice Vectors**

16:40 - 17:40

講演者 : 照屋 唯紀 (産業技術総合研究所)

講演タイトル : **Observations on Random Sampling Reduction Algorithms**

18:10~ 懇親会

9月19日(水)

9:00 開場

9:30 - 10:30

講演者 : 國廣 昇 (東京大学)

講演タイトル : **Quantum Factoring Circuit: Resource Estimation and Survey of Experimental Realization**

10:45 - 11:45

講演者 : 細山田 光倫 (NTT)

講演タイトル : **On the post-quantum security of symmetric key cryptography**

アブストラクトは [[こちら](#)] をご覧ください.

世話人

阿部 拓郎 (九州大学)

落合 啓之 (九州大学)

高島 克幸 (三菱電機)

縫田 光司 (東京大学)

安田 雅哉 (九州大学)