情報セキュリティ基盤の数理構造と安全性解析

開催時期　2012-09-03 10:00～2012-09-07 17:00

場所　九州大学 伊都キャンパス 数理学研究棟 中セミナー室7

情報セキュリティ基盤の数理構造と安全性解析
Mathematical structures of information security fundamentals and security analysis

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

開催期間　2012年9月3日(月)～9月7日(金)

開催場所　九州大学 伊都キャンパス 数理学研究棟 中セミナー室7
伊都キャンパスへのアクセス，伊都キャンパスマップ

講演　9月4日(火)

11:00 - 12:00
題目：**楕円曲線離散対数問題と関連問題の解法について(1)**
Solving Elliptic Curve Discrete Logarithm Problem and Related Problems (1)
13:30 - 14:30
題目：**楕円曲線離散対数問題と関連問題の解法について(2)**
Solving Elliptic Curve Discrete Logarithm Problem and Related Problems (2)
発表者：伊豆 哲也（富士通研究所）
概要：
組み込み機器などでの利用が広がっている楕円曲線暗号の安全性は楕円曲線離散対数問題 (ECDLP) と呼ばれる数学的問題の難しさに依存している。本講演では、楕円曲線離散対数問題を解くいくつかのアルゴリズムの概要と高速化手法を紹介する。

14:45 - 15:45
題目：**マルチパーティ計算の理論と応用(1)**
Theory and application of multi-party computation (1)
16:00 - 17:00
題目：**マルチパーティ計算の理論と応用(2)**
Theory and application of multi-party computation (2)
発表者：鈴木 幸太郎（NTTセキュアプラットフォーム研究所）
概要：
各参加者の入力を秘匿したまま任意の関数を計算することができるmulti-party computation (MPC)に関して概説する。まず、最も基本となるBen-Or, Goldwasser, Wigderson [BGW88]によるunconditionally secureなMPC方式について説明する。つぎに、[BGW88]方式の一般化や効率化に関する主な結果を紹介する。また、MPCに関する最近の結果や、MPCの応用や実装に関する結

果についても紹介する。

9月5日(水)

13:30 - 14:30
題目：**POVM測定を用いたMean King 問題**
Mean King Problem with POVM measurement
発表者：木村 元（芝浦工大）
概要：
元来Mean King 問題は量子系の不確定性関係に対する考察の一環として考案された問題であるが，一種の鍵共有を通じて，量子暗号への応用が考えられている．従来の定式化では，Kingの測定は測定後の状態がわかる都合の良い設定が用いられているが，本講演では一般のPOVM測定を用いた設定を考え，成功確率の上限・下限を議論する．その結果，量子系の次元の偶・奇性で大きな違いが現れることを示す.
(collaborations with H. Tanaka, H. Hiroki)

14:45 - 15:45
題目：**関数密度問題とハッシュ関数の安全性評価**
Function density problem and hash functions
発表者：阿部 拓郎（京都大）
概要：
本講演では、関数密度問題（FDPと略記する）を導入する。簡単に言うとこれは、与えられた距離空間とその部分空間について、その部分空間が全空間からどれくらい離れているか、換言すれば部分空間が全空間をどれくらいよく近似しているか、を考える問題である。これは純粋に数学的に定式化可能な問題であるが、一般に解答を与えるのは難しい。関数密度問題は数学的研究対象としてそれ自体大変興味深いものであるが、同時に情報セキュリティ方面への応用がある点にも面白さがある。本講演では、関数密度問題を用いたハッシュ関数の衝突耐性に関する安全性評価について述べる。本研究は鍛冶静雄氏、縫田光司氏、沼田泰英氏、前野俊昭氏との共同研究である。

16:00 - 17:00
題目：**discussion**

9月6日(木)

13:30 - 14:30
題目：**暗号学的擬似乱数に関する最近の話題と数理的取り組み**
Recent mathematical topics on cryptographic pseudorandom generators
発表者：縫田 光司（産総研）
概要：
安全な暗号プロトコルにおいては良質な乱数の使用が不可欠である。ただし、真正乱数を大量に生成するのは骨が折れるため、実用上は短い真正乱数を引き伸ばして長い真正（のように見える）乱数として用いる擬似乱数生成の仕組みを適用することが多い。今回の発表では、暗号学的に充分な強度を持つ（と信じられ

る）擬似乱数の生成法や擬似乱数を暗号プロトコルに適用した際の安全性評価に関する、話者の最近の研究について紹介する。

14:45 - 15:45
題目：**Efficient enumeration of all ladder lotteries and its algebraic aspect**
発表者：仲田 研登（岡山大）
概要：
In this talk, we give an efficient algorithm which generates all (reduced)ladder lotteries for a given permutation. Let Red(w) denote the set of reduced words of a permutation w. Then Red(w) is classified to 'commutativity classes of w', in the sense of J. Stembridge. We can regard the set of (reduced) ladder lotteries corresponding to w as the set of commutativity classes of w. As an application of our algorithm, we get the number of commutativity classes of the longest permutation in the symmetric group S_n for n \leq 11.