数学と情報セキュリティ科学を巡る知の循環、その実例として

縫田 光司（産業技術総合研究所 情報セキュリティ研究センター）

2010年11月12日(金) –13日(土)　京都大学理学部3号館110講演室・109号室(tea)

RSA暗号や楕円曲線暗号のように、暗号・認証・電子署名などの技術を扱う情報セキュリティ分野において初等整数論や楕円曲線などの数学が応用されていることは比較的認知されているように見受けられる。本発表ではこれら「数学→情報セキュリティ」という波及効果と逆向きの、「情報セキュリティ→数学」という波及効果の実例として、情報セキュリティ分野の研究過程で見出した数学的研究テーマに関する話者のこれまでの研究について紹介する。特に、冒頭に紹介した初等整数論や楕円曲線のようなよく知られた(代数っぽい)題材に留まらず、凸集合の幾何学や確率不等式、組合せ論的数論など様々な分野の数学が登場することを強調しておきたい。

（なお、本発表においては情報セキュリティ分野についての予備知識は仮定せず、また各コマごとにself-containedな内容にする予定である。）

Program

11月12日(金)

14:30-16:30　**「フィンガープリント符号とガウスの求積法」**

機密電子データの不正流出元を特定するための符号(フィンガープリント符号)を題材に、数学との関わりを紹介する。例えば、話者らによる最近の研究によって、ガウスの求積法(Gaussian quadrature)で用いられるノードと重みの値をパラメータとして使用すると性能の良い符号が生成できることが明らかになった。本発表ではそれらの結果について述べる。

11月13日(土)

10:00-12:00　**「擬似乱数の安全性評価とルート２の二進数展開」**

ある擬似乱数生成アルゴリズムに関する話者の研究では、アルゴリズムにおける不適切なパラメータの割合の評価式を、ルート２の二進無限小数展開におけるある特別な部分列の出現率を用いて与えた。さらに、その部分列の出現率を、同じ無限小数における「１」の出現率を用いて評価できることを明らかにした。本発表ではこの結果について紹介する。

14:00-16:00　**「量子情報セキュリティの長期的安全性と凸集合の幾何学」**

いわゆる「量子暗号」に代表される量子力学に基づく情報セキュリティ技術について、もし将来的に量子力学を超越する物理現象が発見され(て、それが暗号攻撃に利用され)たとしても安全性が保たれるかどうか予測するための研究が近年行われている。本発表では、話者らの研究を含むそれらの研究と、局所凸位相ベクトル空間における凸集合の幾何学的性質との関連について紹介する。

世話人：　阿部 拓郎（京都大学大学院工学研究科 機械理工学専攻）