Vol.2013-AL-143 No.7
2013/3/1

［招待講演］準同型性暗号による秘密計算

佐久間 淳 †

概要：ネットワークベースのサービスや多様な携帯デバイス等の高度化により，多種多様かつ詳細な個人・組織の実社会情報が蓄積されつつある。これらの安全な利用を目指し，分散秘密情報源からの安全な知識獲得を目指す秘密計算が近年活発に研究されている。秘密計算とは，二人(以上)のエージェントがそれぞれ秘密の入力データセットを持つときに，それらが互いにデータ見せ合うことなくあらかじめ定められた計算を実行し，得られた知識のみの共有を目指す技術である。講演では，情報を秘匿したまま加算や乗算，ある種の論理演算など限られた演算を実行可能な準同型暗号を利用した，秘密計算の技術とその展開，またその限界について解説する。

† 筑波大学