

佐久間 淳

筑波大学システム情報系
教授

自己情報コントロール機構を持つプライバシー保護データ収集・解析基盤の構築と個別
化医療・ゲノム疫学への展開

§ 1. 研究実施体制

(1) 佐久間グループ

- ① 研究代表者: 佐久間 淳 (筑波大学システム情報系、教授)
- ② 研究項目
 - ・プライバシー保護データ収集・解析基盤の構築

(2) 津田グループ

- ① 主たる共同研究者: 津田宏治 (東京大学大学院新領域創成科学研究科、教授)
- ② 研究項目
 - ・プライバシー保護ゲノム疫学

(3) 竹内グループ

- ① 主たる共同研究者: 竹内一郎 (名古屋工業大学大学院工学研究科、教授)
- ② 研究項目
 - ・プライバシー保護個別化医療

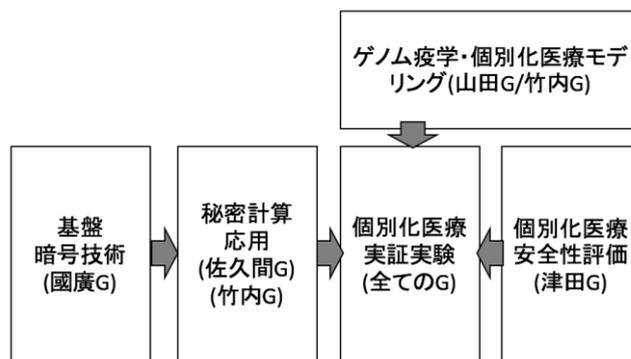
(4) 國廣グループ

- ① 主たる共同研究者: 國廣昇 (東京大学大学院新領域創成科学研究科、准教授)
- ② 研究項目
 - ・プライバシー保護データ収集・解析基盤の構築

(5) 山田グループ

- ① 主たる共同研究者: 山田 芳司 (三重大学先端科学研究支援センター、教授)
- ② 研究項目
 - ・エクソン全領域関連解析による心筋梗塞発症に関連する機能的遺伝子多型の同定

§ 2. 研究実施の概要



今年度は基盤技術から応用に至るまで広範に重要な研究成果が複数上がった。

基盤暗号技術分野では、同じキーワードに関連した暗号文に対してのみ準同型演算を許す準同型暗号(Mis-Operation Resistant Homomorphic Encryption)を開発した。提案法では、暗号文にキーワードを付与し、条件に違反するような演算が実施できない(mis-operation resistant)ような準同型暗号を開発した。今度、個別化医療応用やプライバシー保護疫学等への応用が期待される基礎技術である(CSS2016 最優秀論文賞受賞)。

秘密計算応用では、大規模な記述・予測統計と統計的を計算可能な準同型暗号を用いたライブラリの構築(代表的な原著論文 1, プレスリリース)と、疫学に欠かすことができないロジスティック回帰の秘密計算手法を開発した。ライブラリでは、平均や分散、ヒストグラムやメディアン、線形回帰、カイ二乗検定など主要な基礎的統計計算を広範にカバーする。ロジスティック回帰の秘密計算はその演算に含まれる非線形計算が準同型暗号と相性が悪く、未解決問題であったが、凸最適化の理論にもとづいて非線形計算を近似するとともに、秘密計算上においてその近似制度を明示することによって、解析者によって許容可能な誤差範囲を示しつつロジスティック回帰の秘密計算を実行できるようになった。

個別化医療については、2つの病院で個別化医療実証実験(第一期)が開始された。

ゲノム疫学については、合計 15,896 例において、心筋梗塞を始めとする 13 種類の生活習慣病についてエクソーム全領域関連解析を行い、各疾患の発症に強く関連する遺伝子群および一塩基多型群(SNPs)を特定した(代表的な原著論文 2 ほか)。構築したデータベースを用いて 13 の生活習慣病について、疾患感受性遺伝子群および SNPs を特定し研究成果を 9 編の論文にまとめ医学誌に投稿し(8 編は accept され、7 編は既に掲載)、4 件の特許出願を行い、新聞発表を 2 回行った。

個別化医療によって開示される情報の安全性評価については、疾病のリスク予測に関する結果から、SNP の状態が特定可能であるかを評価し、その特定を困難にする数値区間化手法を提案した。また、ある疾病に関するリスクを知った時に、他の病気のリスクも類推できるかについて検討し、ある条件下ではそれが可能であるリスクを指摘した。

代表的な原著論文

- 1) Wen-jie Lu, Shohei Kawasaki, Jun Sakuma, Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data. The Network and Distributed System Security Symposium 2017 (NDSS 2017), 16 pages, online proceedings.
- 2) Yoshiji Yamada, Jun Sakuma, Ichiro Takeuchi, Yoshiki Yasukochi, Kimihiko Kato, Yoshiji Yamada, Jun Sakuma, Ichiro Takeuchi, Yoshiki Yasukochi, Kimihiko Kato, Mitsutoshi Oguri, Tetsuo Fujimaki, Hideki Horibe, Masaaki Muramatsu, Motoji Sawabe, Yoshinori Fujiwara, Yu Taniguchi, Shuichi Obuchi, Hisashi Kawai, Shoji Shinkai, Seijiro Mori, Tomio Arai, Masashi Tanaka. Identification of STXBP2 as a novel susceptibility locus for myocardial infarction in Japanese individuals by an exome-wide association study. *Oncotarget*, Vol. 8, No. 20, pp. 33527–33535. doi: 10.18632/oncotarget.16536.