

安全安心な情報社会を支える 次世代暗号の研究開発

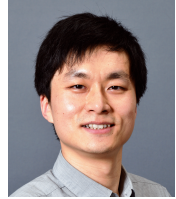


キーワード 耐量子計算機暗号、格子暗号、デジタル署名、安全性評価

王 贇 王 WANG Yuntao

電気電子情報通信工学専攻 講師

通信システム工学講座 サイバーセキュリティ工学領域 宮地研究室



ここがポイント！【研究内容】



- 量子計算機に Shor の量子アルゴリズムを用いて、現在使われている RSA などの暗号技術を短時間に攻撃できて安全性においても非常に脅威になります。そのため、量子計算機に耐性を持つ次世代暗号技術、特に、有力候補である格子暗号方式と格子デジタル署名の研究開発を行っています。
- また、格子暗号を実用化するためにシミュレーターを構築し、安全かつ効率的なパラメータの評価に取り組んでいます。
- さらに、格子アルゴリズムを開発改良し、格子暗号の安全性根拠となる SVP など数学的困難問題において、解読の世界記録を更新しております。

応用分野	情報セキュリティ、プライバシー保護、暗号分野
論文・解説等	[1] L. Wang and Y. Wang, 170次元格子困難問題“SVP Challenge”解読の世界記録達成, 2022. [2] K. Yamamura, Y. Wang, and E. Fujisaki, <i>IET Information Security</i> , pp. 1-11, Wiley, 2022. [3] Y. Wang and T. Takagi, <i>International Journal of Information Security</i> , Vol. 20(2), pp. 257-268, Springer, 2021.
連絡先 URL	https://sites.google.com/view/yuntaowang/



気軽に体の状態が把握できる センシングデバイスの実現を目指して



キーワード 生体信号、信号処理、集積回路、IoT、センシング

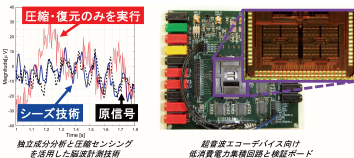
兼本 大輔 KANEMOTO Daisuke

電気電子情報通信工学専攻 准教授

集積エレクトロニクス講座 集積情報デザイン領域 廣瀬研究室



ここがポイント！【研究内容】



病気の早期発見を行うには「いつでもどこでも簡単に体の状態が把握できる」環境の実現が重要です。そこで私は、「集積回路からデバイス実装方法、信号処理（圧縮センシングや機械学習等）」を融合的に研究することで、従来技術の課題解決を行い、小型・軽量・長時間動作が可能な次世代センシングデバイスの実現を目指しています。現在は「脳波や心電図等の生体信号計測ウェアラブルデバイス」や「内視鏡や超音波エコー機器を対象とした医療機器」に関して国内外の研究者と共同研究を進め、様々な世界初の研究成果を発信しています。

応用分野	医療・ヘルスケア分野、IoTデバイス、ポイント・オブ・ケア
論文・解説等	[1] K.Nagai et al., <i>IEICE Trans. Fundamentals</i> , vol.E104-A, no.09, Sep. 2021 (in press) [2] D.Kanemoto et al., <i>IEICE Trans. Fundamentals</i> , vol.E103-A, no.12, pp.1647-1654, Dec. 2020 [3] D. Kanemoto et al., <i>Jpn. J. Appl. Phys.</i> , 60 (2021) SBBL08
連絡先 URL	http://ssc.eei.eng.osaka-u.ac.jp/~dkanemoto/



IoTプラットフォーム工学

時空間数理によるインテリジェントな通信ネットワークの実現



キーワード 通信ネットワーク、時空間確率モデリング、データ分析、5G

木村 達明 KIMURA Tatsuki

電気電子情報通信工学専攻 講師

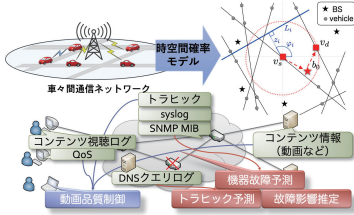
通信ネットワーク工学講座 ロバストネットワーク工学領域 滝根研究室



ここがポイント!【研究内容】

次世代の無線通信ネットワークにおいて高速・大容量通信を実現するインテリジェントなネットワーク制御技術の研究を、確率幾何などの時空間確率モデリングと機械学習をベースとして行っています。

- 無線基地局や端末の位置・動きを空間的な確率過程によりモデル化し、我々が体感する通信品質を理論的に解析する研究
- ドローン空中基地局や車々間通信などの次世代通信ネットワークにおけるリアルタイムな通信品質最適化制御の研究
- 通信ネットワーク内の多様なデータを活用したネットワーク管理や動画品質制御の高度化の研究



応用分野	情報通信ネットワーク、セキュリティ
論文・解説等	[1] T. Kimura, <i>IEEE Trans. Veh. Technol.</i> , 70(4), 3396-3411, 2021. [2] T. Kimura et al., <i>IEEE Trans. Mobile Comput.</i> , 20(4), 1642-1655, 2021. [3] T. Kimura et al., <i>IEEE INFOCOM2020</i> , pp. 1748-1757.
連絡先 URL	http://www2b.comm.eng.osaka-u.ac.jp/~kimura/



磁性と弾性・熱量との相互作用を利用したエネルギー変換材料の開発



キーワード 磁性材料、磁気弾性効果、振動発電、磁気熱量効果、磁気冷凍

藤枝 俊 FUJIEDA Shun

環境エネルギー工学専攻 准教授

共生エネルギーシステム学講座 環境エネルギー材料工学領域 牟田研究室



ここがポイント!【研究内容】

磁性と種々の物性との相互作用に着目して、エネルギー有効利用および環境負荷低減に貢献するエネルギー変換材料の開発に取り組んでいます。これまでに、磁場誘起1次相転移に伴う磁性と熱量の巨大な相互作用を発見し、それを制御して実用的な磁気冷凍材料を開発してきました。最近では、IoT およびロボット技術などを支える振動発電およびアクチュエータの技術革新に向けて、歪み→磁気および磁気→歪みの高効率エネルギー変換材料の開発に注力しています。

デバイスを指で弾いた振動で発電



応用分野	エネルギーハーベスティング、アクチュエータ、冷凍・冷却分野
論文・解説等	[1] 藤枝 俊* 他, 日本金属学会会報 までりあ 59 (2020) 10. [2] M. Hisamatsu, S. Fujieda*, et al., <i>IEEE Trans. Magn.</i> 57 (2021) 2100804. [3] S. Inoue, T. Okada, S. Fujieda*, et al., <i>AIP Adv.</i> 11 (2021) 035021.
連絡先 URL	http://www.see.eng.osaka-u.ac.jp/seems/seems/index.html

