# 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 贇弢 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おります。
- 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おります。
- 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、解読の世界解読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.<br>[2] K. Yamamura, Y. Wang, and E. Fujisaki, *IET Information Security*, pp. 1-11, Wiley, 2022.<br>[3] Y. Wang and T. Takagi, *International Journal of Information Security*, Vol. 20(2), pp. 257-268, Springer, 2021. |
| 連絡先 URL | https://sites.google.com/view/yuntaowang/ |