SCAT LINE テレコム技術の未来を拓く情報誌

VALUE POINTER

ＳＣＡＴ研究奨励金を受けて

令和５年度ＳＣＡＴ研究奨励金採用の白矢 琢朗さんをご紹介します。
白矢さんは、現在大阪大学大学院情報科学研究科博士課程に在籍されています。

白矢　琢朗 さん
Takuro Shiraya

大阪大学大学院　情報科学研究科
マルチメディア工学専攻
博士後期課程　２年

モットー：急がず，休まず

〈略歴〉
令和４年３月：兵庫県立大学 工学部
電気電子情工学科卒業
令和６年３月：兵庫県立大学大学院　情報科学研究科
データ計算科学専攻博士前期課程修了
令和７年３月：兵庫県立大学大学院　情報科学研究科
データ計算科学専攻　博士後期課程
中途退学
令和７年４月：大阪大学大学院　情報科学研究科
マルチメディア工学専攻博士後期課程
入学

Q. 何の研究をされていますか?

高速な暗号技術に関する研究を行っています。研究分野は、情報セキュリティの中でも共通鍵暗号と呼ばれる領域です。暗号と聞くと暗号資産などをイメージされる方も多いかもしれませんが、実は私たちが日常的に使っているインターネット通信やオンライン決済など、あらゆる場面で暗号技術が使われています。いわばセキュリティの基盤技術です。現在普及しつつある 5G に続き、2030 年頃には次世代の 6G が実用化されると考えられています。通信が高速化・大容量化するほど、そこで使われる暗号技術も高速でなければ、通信全体の足かせになってしまいます。こうした課題に対し、高速かつ安全な暗号技術を実現することが私の研究テーマです。

暗号の研究には、大きく二つの柱があります。一つは、求められる性能や安全性を満たす暗号を「設計」すること、もう一つは、設計された暗号が本当に攻撃に耐えられるかを検証する「安全性評価」です。

修士課程では、まず安全性評価に取り組みました。具体的には、ソフトウェア上で高速に動作する認証暗号を対象としました。　認証暗号とは、データの秘匿化と改ざん検知を同時に実現する暗号方式です。この暗号の内部処理を数理ソルバーでモデル化し、攻撃に対する耐性を評価しました。博士課程では、この知見を生かし、暗号技術の設計に取り組んでいます。設計においても、構成を選定する際に安全性評価の結果が判断材料となるため、修士時代に評価から始めた経験が大いに役立っています。

Q. これまでにどのような成果がありましたか?

修士課程では、国際的な CAESAR Competition で選定された認証暗号である AEGIS Family や Tiaoxin-346、さらに Beyond 5G を見据えて設計された Rocca/Rocca-S を対象に、差分攻撃や偽造攻撃といった強力な攻撃手法に対する安全性評価を行いました。まずバイト単位での評価に着手し、その後ビット単位へと評価精度を高め、さらにそれまで未評価であった攻撃条件への耐性も検証しました。研究は、学会で口頭発表を行った後

に論文誌へ投稿するという流れで進めました。これらの成果は、査読付きの国際会議1本と査読付き論文誌3本に採録されました。

博士課程では、評価から設計へと軸足を移し、既存暗号がCPU上での実装方法に着目しました。実装するための命令特性を考慮し、CPU上で使われていない演算リソースを活用することで安全性を高める構成や、安全性を維持したまま処理速度を向上させる構成を提案しました。この成果は、国際暗号学会が主催する査読付き論文誌（IACR Communications in Cryptology）に採録されました。

Q. 研究奨励金を受けて良かったことなどお聞かせください

修士課程で始めた研究をもう少し続けたい、研究者としてやっていけるか試してみたいという思いで、博士課程への進学を決意しました。しかし正直なところ、金銭面の不安は進学を決めた後もつきまとっていました。研究奨励金による支援をいただいたことでその不安が大きく軽減され、研究活動に集中できる環境を得られたことは、何よりありがたかったです。

また、応募にあたって研究計画書を書いたことも良い経験でした。博士課程では、外部資金への申請など、研究計画を文章にまとめる機会が格段に増えます。その前に一度しっかりと自分の研究を言語化できたことは、良いトレーニングになりました。そして何より、審査を経て採用していただいたことで、自分の研究の方向性に自信を持つことができました。いずれも奨励金をいただいたからこそ得られたものであり、心から感謝しています。

Q. 今、興味もっていることや趣味などお聞かせください

今、特に関心を持っているのは健康です。研究活動や趣味のゲームなどで日常的に座りがちな生活になりやすいことから、健康面を意識するようになりました。研究活動を続けるうえでは、毎日を良い体調で過ごすことが欠かせないと感じています。その一環として、周囲の人の影響を受けてランニングを始め、これまでにフルマラソンにも3回出場し完走しました。走っている間は研究のことやこれからの進路をじっくり考える時間にもなり、良い気分転換になっているため、これからも継続していきたいと考えています

Q. 将来の目標についてお聞かせください

将来の目標は、企業の現場で研究・開発に携わりながら、社会全体のセキュリティ向上に貢献することです。暗号・セキュリティ分野を志したのは、大学時代に個人情報流出のニュースを繰り返し目にしたことがきっかけでした。情報を守る技術の重要性は今後ますます高まると感じ、大学院ではこの分野を専門とする現在の研究室を選びました。近年はAIの発展で情報の価値がいっそう高まる一方、脅威も高度化しており、それを守る技術の必要性は高まっていると感じています。これまで培った知見を活かし、人々が安心して暮らせる情報社会の実現に向けて頑張りたいです。