

ダイヤモンド NV 中心系の拓く新たな認証システムの可能性

Toward quantum authentication with an NV center in diamond.

○倉見谷航洋、須田雄太、後藤優征、関口雄平、佐藤恒司、中村孝秋、黒岩良太、延與梨世、加納浩輝
*小坂英男 (横国大院工)

Koyo Kuramitani, Yuta Suda, Yuusei Goto, Yuhei Sekiguchi, Koji Sato, Takaaki Nakamura, Ryota Kuroiwa, Riyo Enyo, Hiroki Kano,*Hideo Kosaka (Yokohama Natl. Univ.)
E-mail : *kosaka-hideo-yp@ynu.ac.jp

受動的盗聴に対し絶対の安全性があり次世代の情報技術と目される量子暗号通信は、通信末端部における偽証行為などの能動的盗聴行為に対しては脆弱であるという欠点を持つ。この弱点に対しては現状のところ従来の暗号技術で補うほかないが、そこが大きなセキュリティホールとなりうる。

一方で、広域量子情報通信を行う上で不可欠な量子情報中継処理を実装しうるデバイスであるダイヤモンドNV中心の電子スピンおよび核スピン複合系は、副次的な特徴としてダイヤモンド内部に自然発生的に存在する¹³C核スピンのランダムな配置という人為的に複製不可能な要素(便宜的に量子指紋と呼ぶ)を内包している。このような再現不可能な物理的特徴を利用した暗号化の概念はPUF(physical unclonable function)と呼ばれており、堅牢な物理認証技術として半導体分野で一部実用化がなされている。

NV 中心スピン系のもつ量子性と量子指紋という PUF 的要素を併せて利用することにより、量子暗号通信技術は先述の能動的盗聴行為に対する堅牢さをも持ち合わせた、包括的セキュリティ技術として完成するだろう。

本講演では、我々が「カンタムウェアセキ

ュリティ」と呼称する上記セキュリティ技術の概要および展望について語る。さらに、カンタムウェア技術実現の基礎的取り組みとして、認証の肝となる量子指紋情報(ハミルトニアン情報)を詳細かつ効率よく調べるハミルトニアンラーニング[1]と呼ばれる機械学習を用いた手法、及びその成果などについて一部紹介する。この手法と、これまでにNV中心系において成功している光子核子間量子メディア変換[2]やハミルトニアン情報を基にした制御波形の最適化技術等[3]を背景に、カンタムウェアセキュリティ技術や量子センシング、さらには拡張性の高い量子演算器等といった様々な応用が期待される。

日頃よりご議論・ご協力いただく寺地徳之氏、加藤宙光氏、牧野俊晴氏、山崎聡氏、水落憲和氏、松崎雄一郎氏、根本香絵氏に感謝いたします。本研究は総務省 NICT 委託研究、科研費基盤 S、平山新学術領域、ポスト「京」萌芽的課題 1 の支援を得た。

- [1] C.E.Granade, et al., *New. J. Phys.*, **14**,10(2012).
- [2] H.Kosaka and N.Niikura, *Phys. Rev. Lett.*, **114**, 053603(2015).
- [3] N. Khaneja, et. al., *J. Magn. Reson.*, **172**, 296-305(2005).

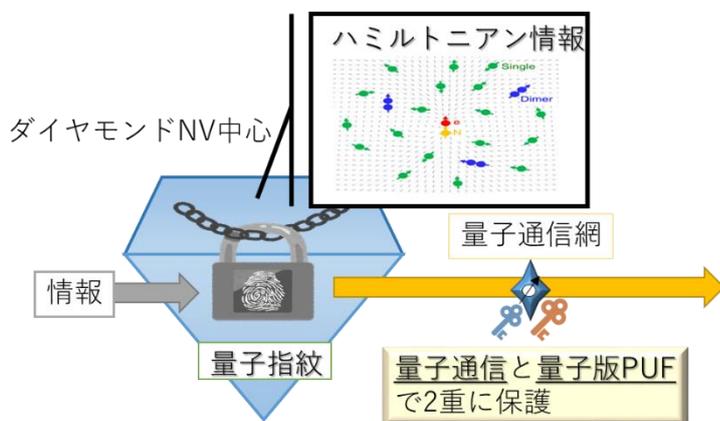


図1 NV 中心を用いたカンタムウェアセキュリティ概略図

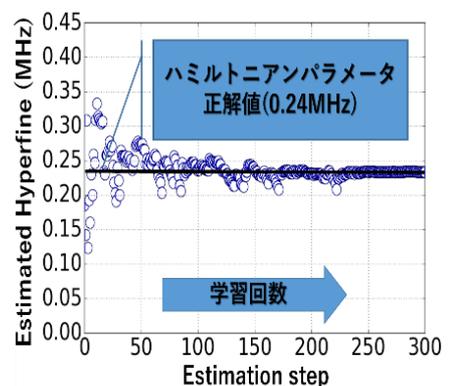


図2 ハミルトニアンラーニング運用評価