量子ドットネットワークを用いた Physically Unclonable Function に基づく人工物認証技術の検討
Artifact-metrics Based on Physically Unclonable Function Using Quantum-dot Network

°柴田涼平 [1]*，下村優 [1]，竪直也 [2]，谷田純 [1]，小倉裕介 [1]
°Ryohei Shibata[1], Suguru Shimomura[1], Naoya Tate[2], Jun Tanida[1], Yusuke Ogura[1]
1. 大阪大学大学院情報科学研究科，2. 九州大学大学院システム情報科学研究院
1.Graduate School of Information Science and Technology, Osaka University
2.Graduate School of Information Science and Electrical Engineering, Kyushu University
*r-shibata@ist.osaka-u.ac.jp

A physically unclonable function (PUF) is gaining attention due to its capability in high-level security for the Internet of Things (IoT) society. In this study, we investigated a PUF using quantum-dot networks to apply it to secure authentication of artificial objects. In the experiments, we evaluated the fundamental performance using fluorescence images of the quantum-dot networks and confirmed their potential capabilities relating to uniqueness.

現在，IoT の利用拡大に伴い，安心で安全な物体認証として Physically Unclonable Function（PUF）認証 [1] が注目されている．PUF 認証とは物体を製造した際に生じる複製困難な物理的特徴を関数として用いて認証する技術である．我々は，多数の量子ドット（QD）からなる QD ネットワーク（QDN）を用いた PUF の検討を進めている．QDN は，フェルスター共鳴エネルギー移動（FRET）による多段階のエネルギー移動が行われる QD の構造体である．励起光の照射条件によってエネルギー伝達経路が変化し，非線形な蛍光応答により，時間信号が時空間的な高次元信号に写像される [2]．この性質は，PUF による人工物認証に必要な多数の固有な出力の生成にも有用であると考えられる．本研究では，QDN への時間信号入射に対する空間的な蛍光応答変化を利用した認証の特性を評価し，その効果を検討した．

本手法では，基板上に適当な密度で分散させた QD を用いる．認証は QDN の蛍光応答画像を 1 次元のバイナリビット列に変換したものを使用する．認証対象の物体について，事前に登録されたビット列と被認証者から送られるビット列のハミング距離（HD）をもとに認証の可否を決める．なお，認証の性能を調べるために，同じ PUF 同士の HD をビット数で正規化した inter-HD と，異なる PUF 同士の HD をビット数で正規化した intra-HD を用いた．これらは再現性とユニーク性の指標となる．

実験では，QD（NN-LABS，CS440）を凝集させたガラス基板にパルスレーザー光（波長 403nm、パルス幅 500ps）を集光して QDN を励起し，蛍光応答画像を撮影した．時間的な非線形性の効果を調べるために，30 個の試料に対してシングルパルスとダブルパルスそれぞれで励起し，同じ条件で 10 回ずつ画像を撮影した．図 1 は QDN の蛍光応答の二値化画像の例であり，空間分布に違いが現れている．また，二値化画像の全ての組み合わせから算出した inter-HD と intra-HD のヒストグラムを図 2 に示す．これらの山が分離しており，適切な閾値の設定により正しく認証できることがわかる．また，ダブルパルスを含めた場合，シングルパルスと比べて inter-HD はほぼ変わらず intra-HD は上昇した．これは，再現性を維持しつつユニーク性が向上できることを示しており，QDN の時間的非線形性の有用性が確認できた．

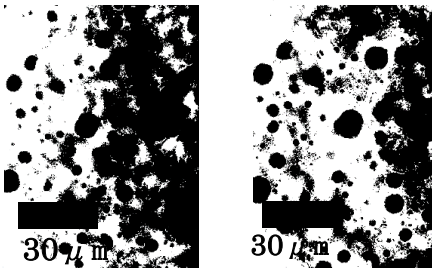

Fig. 1 Examples of the fluorescence response images of the QD network.
Left: Single pulse, Right: Double pulse.

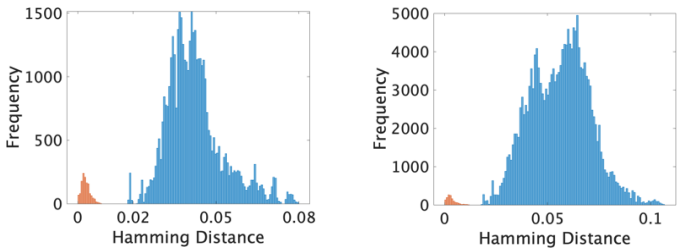

Fig. 2 The histogram of inter-HD (orange) and intra-HD (blue).
Left: Single pulse, Right: Single pulse and Double pulse.

参考文献

1) R. Pappu, B. Recht, J. Taylor and N. Gershenfeld: Science 297 (2002) 2026-2030.
2) N. Tate, Y. Miyata, S. Sakai, A. Nakamura, S. Shimomura, T. Nishimura, J. Kozuka, Y. Ogura and J. Tanida: Opt. Express 30 (2022) 14669-14676.