スピン量子ビットを用いた物理複製困難関数（Quantum-PUF）

Application of spin qubits to Physically Unclonable Function

東芝研開セ [1], 理研 [2], 棚本 哲史 [1], 西 義史 [1], 大野圭司 [2]

Toshiba R &D Center [1], Riken[2], Tetsufumi Tanamoto[1], Yoshifumi Nish[1], and Keiji Ono[2],

E-mail: tetsufumi.tanamoto@toshiba.co.jp

IoT(Internet of Things)の進展により、様々なデバイスが繋がり、生活が便利になっていくと同時に、セキュリティ問題が日常的に発生している。セキュリティの課題の一つに個人を特定する ID 機能の強化がある。ID 機能強化に関して、デバイスばらつきを“チップ指紋”として利用する研究開発が進められている（物理複製困難関数：Physically Unclonable Function (PUF)）。これまでに多くの PUF が CMOS 回路ベースで提案されてきた[1][2]。文献[3]ではトランジスタのトラップを利用した PUF であり、与えられた電圧範囲内でトラップが検出できるかどうかで、0 と 1 を決定するが、多数ビットの ID 生成に多数のトランジスタが必要となる。そこで本講演では、トランジスター一つでチップ認証が可能な方法として、トランジスタ内トラップを介した単一電子現象（図 1）を利用する方法を提案する。トラップ電子は単一電子現象の振る舞いをする[4]。単一電子現象のデータからクーロン・ダイヤモンド特性が得られるが、同じサイズに設計したトランジスタでも、トラップの位置、特性が異なるためにトランジスタに特徴的なクーロン・ダイヤモンド特性が得られる（図 2）ので、クーロン・ダイヤモンド特性をトランジスタ指紋とすることができる。

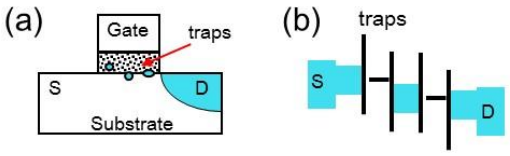

図 1：シリコントランジスタ中のチャネル内トラップを利用した単一電子効果[4,6]

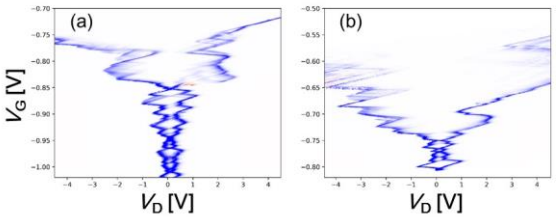

図 2: 同じサイズのトランジスタ (L=125nm, W=220nm) でもトラップの位置が違うので、異なったクーロン・ダイヤモンド特性が得られる。

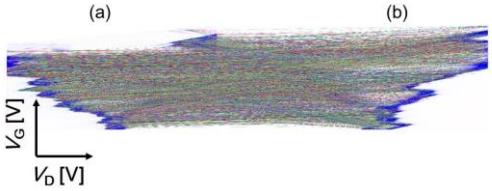

図 3:図 2 の素子(b)の異なった基板バイアスのクーロン・ダイヤモンド特性の間に AKAZE アルゴリズムにより特徴点抽出した結果。

素子間のクーロン・ダイヤモンド特性の比較には、画像処理の特徴点抽出の方法を利用する[5]。これは、クーロン・ダイアやモンドの測定条件が測定時の環境などにより微妙に変化するため、実験データそのままを直接比較するのは困難なためである。図 3 が二つの基板電圧の異なるクーロン・ダイヤモンド特性のデータに画像認識アルゴリズムを利用した結果である。クーロン・ダイヤモンドが変化していてもクーロン・ダイヤモンドの特徴を捕らえることができる。トラップ電子は量子ビットとして振舞うので[6]、以上は量子ＰＵＦと呼ぶことができる。 講演ではより詳細な検討結果について報告する。 [1] G.E. Suh and S. Devadas, DAC’07, p9. [2] http://www.toshiba.co.jp/rdc/detail/1806_01.htm [3] J Chen, et al., VLSI Tech., 2015, T40-T41. [4] Ono et al., APL103, 183107 (2013). [5] https://opencv.org/ [6] Ono et al.,PRL119, 156802 (2017),