リング発振器型物理複製困難関数（PUF）と電子工作ロボットへの応用

Application of Physically Unclonable Function to toy robots

東芝研究開発センター　棚本 哲史，高谷 聡

Toshiba R &D Center , Tetsufumi Tanamoto, Satoshi Takaya

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、サイバー攻撃を始め、セキュリティの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、個々の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。これらは Physically Unclonable Function (PUF)として知られ、IC チップに組み込まれつつある。

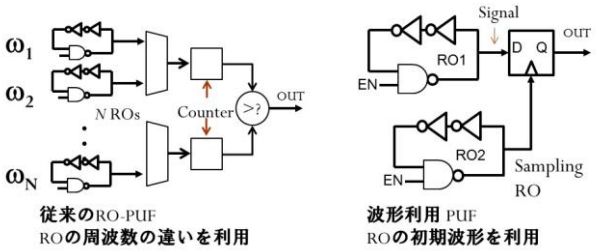

図 1

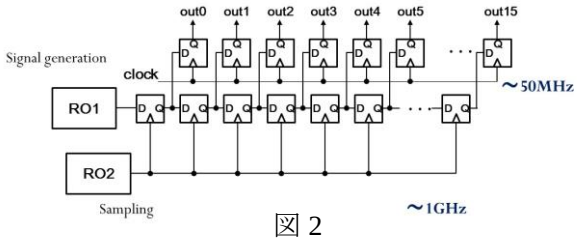

図 2

これまでに多くの PUF が提案されてきた。特にリング発振器ベースの PUF(ring-oscillators PUF:RO-PUF)は FPGA ベースで作成することができるため、広く研究されている。本報告では、我々が取り組んでいる波形ベースの RO-PUF について、市販の FPGA に搭載した結果と電子工作にて作成した簡易ロボットへの適用例を報告する。

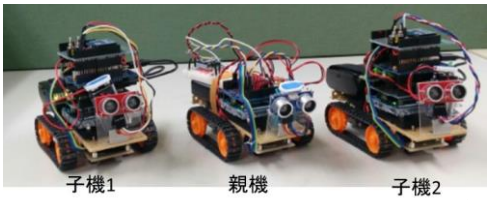

図 3

従来の RO-PUF は二つのリング発振器の間の発振周波数の違いを利用しているが[1]、ID とするべき出力ビット数に対応した数のリング発振器のペアを並列に動作し続ける必要がある点で面積、消費電力で課題があった(図 1)。これに対して我々が提案している波形型リング発振器 PUF では、リング発振器が動き始まる最初の信号を利用して ID を生成する。リング発振器の発振周波数は GHz オーダーであり、FPGA の回路クロックよりはるかに速い。このため、リング発振器のスタート時の信号を取得するためには、同程度の周波数でサンプリングする必要がある。このことから、我々はリング発振器の出力をも一つのリング発振器の出力でサンプリングする構造を提案した(図２)[2]。本報告では市販の FPGA での RO-PUF の動作結果と、Arduino を利用した電子工作ロボットの交信(図 3，4)に適用した結果を報告する。

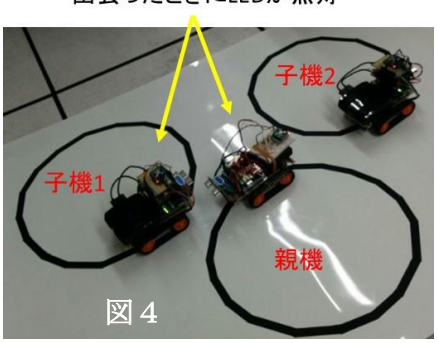

図 4

[1] G.E. Suh and S. Devadas, DAC’07, p9. [2] T. Tanamoto et al., IEEE Trans. Circuits and Systems II: Express Briefs 64, p827(2017).