PUF についてのサーベイ論文（仮）

あらまし　フィジカリー・アンクローナブル・ファンクション（PUF）とは，主に半導体技術を用いて作られた集積回路を大量生産した際に生じる，制御不能な製造ばらつきを利用してその個体にランダムな関数を作る技術のことである．この技術は，個体の識別に用いることで模造品の作成を防ぐだけでなく，制御不能な性質を利用することで暗号アルゴリズムに組み合わせて使うことも期待されている．本稿では PUF について調査した内容を，その発展の歴史を踏まえて述べる．

キーワード　暗号ハードウェア，ハードウェアセキュリテイ，PUF

†

DOI:10.14923/transj.???????????

Abstract

Key words Physically Unclonable Function