# PUF 性能解析プログラム
# マニュアル

Version 1.0

June 24, 2011

（独）産業技術総合研究所

情報セキュリティ研究センター（RCIS）

## 1. はじめに

本ドキュメントは，（独）産業技術総合研究所 情報セキュリティ研究センターが公開する PUF 性能解析プログラムの使用方法を説明する．本プログラムは，以下の論文の性能評価で使用されたものに修正を加えたものである．本プログラムおよび PUF データは，**学術研究目的に限り無償で利用可能**である．

Y.Hori, T.Yoshida, T.Katashita, and A.Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," Proc. ReConFig2010, pp.298-303, 2010.

本プログラムは以下の Web サイトで入手することができる．

http://staff.aist.go.jp/akashi.satoh/SASEBO/ja/puf/index.html

公開されているアーカイブに含まれるプログラムは以下の通り．

| プログラム | 説明 |
|---|---|
| example1_GetPufPerformance.m | デバイス内の性能（Randomness, Steadiness, Correctness, Diffuseness）を算出.<br>GetPufPerformance を呼び出すラッパー. |
| example2_InterDiff.m | デバイス間の性能（Uniqueness）を算出.<br>あらかじめ example1_GetPufPerformance.m を実行してデバイス内性能を算出しておく必要がある. |
| GetPufPerformance.m | デバイス内性能を算出する. |
| entropy2.m | エントロピーを算出する．min_entropy または shannon_entropy のどちらかを呼び出す. |
| entropy2_min.m | min-entropy を算出する. |
| entropy2_shannon.m | Shannon-entropy を算出する. |

## 2. プログラムの使用法

1. プログラムとデータを上述の URL からダウンロードする.
2. ダウンロードしたプログラムとデータを適当なフォルダに置いて解凍する.
3. MATLAB を起動し，コマンドウィンドウから解凍したプログラムフォルダに移動する．または，解凍したプログラムフォルダを検索パスに含める.
4. example1_GetPufPerformance.m を実行する．「フォルダーの参照」ウィンドウが立ち上がるので，先ほど解凍したデータフォルダを指定する.
5. example2_InterDiff.m を実行する．「フォルダーの参照」ウィンドウが立ち上がるので，先ほどと同じデータフォルダを指定する.

【技術的な問合せ先】
（独）産業技術総合研究所
情報セキュリティ研究センター
〒305-8568
茨城県つくば市梅園 1-1-1　中央第 2 事業所
TEL：029-861-5284　FAX:029-861-5285