バイオメトリクス的手法を用いた
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バイオメトリクス的手法を用いた 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（Arbiter PUF）で使用されたものに修正を加えたものである．

H. Kang, Y. Hori, T. Katashita, A. Satoh, "Performance Evaluation for PUF-based Authentication Systems with Shift Post-processing: Additional Experimental Results," The 2011 Symposium on Cryptography and Information Security (SCIS2011), Kitakyushu, Japan, Jan. 25-28, 2011.

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
¥preparation¥making_3d_data_1.m	SASEBO-GII から得た PUF の Response ファイルを 3 次元データに成形する．
¥preparation¥making_50_20_data_2.m	3 次元の Response データから 50 種の ID, 20 回の Test のデータを取り出す．（実験の簡略化のため）
¥reliability¥puf_eval_gen.m	SC (Same Challenge) Intra-PUF の計算を行う．
¥reliability¥puf_eval_imp.m	DC (Different Challenge) Intra-PUF の計算を行う．
¥reliability¥match_id.m ¥security¥match_id.m	Response データ間の Hamming distance を算出する．
¥reliability¥function_cal_far_frr.m	SC Intra-PUF と DC Intra-PUF の EER (Equal Error Rate) 等の結果をグラフに表示する．
¥security¥sc_inter_a_pufs.m	SC Inter-PUF の計算を行う．
¥security¥dc_inter_a_pufs.m	DC Inter-PUF の計算を行う．
¥security¥function_cal_far_frr_SC_SC.m	SC Intra-PUF と SC Inter-PUF の EER 等の結果をグラフに表示する．（注意：DC Inter-PUF は利用しないため表示しない）

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）上表や Web サイトの図を参考にし，該当する MATLAB ファイルを実行することで必要なデータが計算される．

【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