ISS-SP-181

# サイドチャネル情報における固有性解析

Uniqueness Analysis on Side-Channel Information

粕谷桃伽 [1]　町田卓謙 [2]　崎山一男 [2]
Momoka Kasuya　Takanori Machida　Kazuo Sakiyama

電気通信大学 情報理工学部 総合情報学科 [1]　電気通信大学 大学院情報理工学研究科 総合情報学専攻 [2]
Department of Informatics, The University of Electro-Communications

## 1　はじめに

サイドチャネル情報を用いた認証に関する研究がなされている [2]．このサイドチャネル認証では，チャレンジ・レスポンス認証でのレスポンスに加えて，サイドチャネル情報を用いることでより安全に認証を行うことを目的としている．先行研究 [1] では，いくつかの異なる波形数に対して，識別可能な ID 数をそれぞれ実験的に導出した．これに対し，本稿では，波形数に対する ID 数の一般式を求める．

## 2　サイドチャネル情報の固有性解析実験

実験の概要を図 1 に示す．被認証装置として，CycloneIV が搭載された FPGA ボード (DE0-nano) を用い，AES-comp [3] を実装する．動作周波数は 50MHz とする．また，認証装置として数値計算言語 (MATLAB) を使用する．共有している秘密鍵から作成したハミング距離 (HD) モデルと取得した漏洩電磁波との相関係数を求める (受入試行)．また，ランダムに選んだ異なる鍵から作成した HD モデルと，漏洩電磁波との相関係数を求める (拒否試行)．なお，HD モデルは AES 暗号化処理の 4 ラウンド目の入出力値から作成した．

認証システムの構築にあたり，他人受入，本人拒否を防ぐために，これらの試行の間の相関係数にマージンが存在するように閾値 $h$ を設定する必要がある．しかし，本稿では，マージンはないものとし，識別可能な最大の ID 数の一般式を導出することとする．受入/拒否試行のそれぞれの平均値と分散から，相関係数の確率密度を正規分布で近似し，他人受入と本人拒否が等確率となるような閾値 $h$ を決める．最大の ID 数は，等確率の逆数とする．

## 3　結果・考察

1 標本コルモゴロフ・スミルノフ検定を用いて，有意水準を 1%に設定し，受入/拒否試行の相関係数がそれぞれ正規分布に近似できることを確認した．今回の実験では，正規分布における平均値は，波形数に依存しなかったが，分散は波形数 $n$ に反比例していた．このことを考慮し，波形数に対する識別可能な最大の ID 数 $H$ を次の一般式で求めることができた．

$$H = \frac{2}{1 - \mathrm{erf}\,\alpha\sqrt{n}}$$

erf は誤差関数である．また，定数 $\alpha$ を以下の式で表される．

$$\alpha = \frac{\mu_1 - \mu_2}{\sqrt{2\beta_1} + \sqrt{2\beta_2}}$$

ここで，$\mu_1$，$\mu_2$ は受入/拒否試行の平均値，$\beta_1$，$\beta_2$ は波形数を変化させたときの受入/拒否試行における分散の比例定数である．

波形数に対する識別可能な最大の ID 数 $H$ は図 2 の直線で示される．図からわかるように，今回得られた一般式は測定ベースの値とよく一致している．ただし，定数 $\alpha$ の値に大きく依存するため，その同定には注意が必要である．また，64 ビット程度の ID を識別するためには，おおよそ 800 波形で十分であることがわかった．

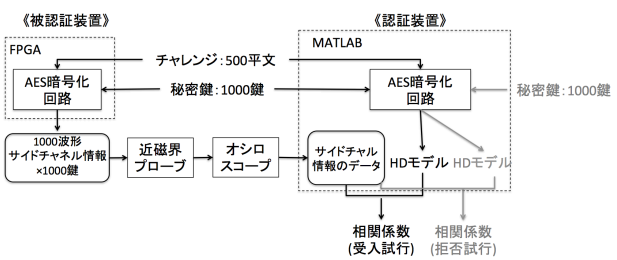


図 1　実験の概要

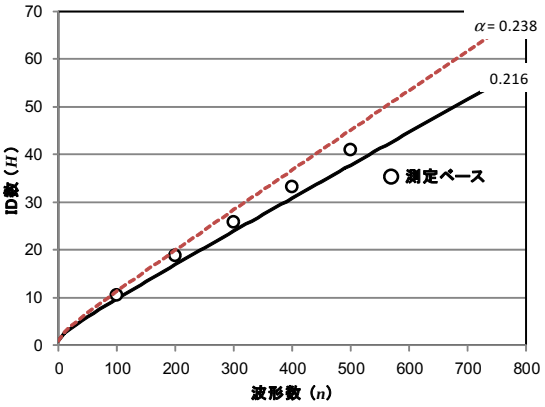


図 2　波形数に対する識別可能な ID 数

**謝辞**

本研究は JSPS 科研費 15K12035 の助成を受けたものである．

**参考文献**

[1] 粕谷桃伽, 町田卓謙, 崎山一男. AES 暗号を用いたサイドチャネル認証における識別可能なデバイス数. 2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 2016.

[2] 松原有沙, 李陽, 林優一, 崎山一男. サイドチャネル認証に向けた基礎的考察. ISEC2014, pp.1-8, 2014.

[3] Cryptographic Hardware Project, Tohoku University. http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.html. (7 月 1 日閲覧)