相関値の変化傾向に着目した篩い分けのCPAへの適用

A method of CPA using key screening techniques by a tendency of correlative value change

若林　邦爾†　　岩井　啓輔†　　黒川　恭一†

Kuniji Wakabayashi,　Keisuke Iwai, and　Takakazu Kurokawa

1 はじめに

近年，IC カードや通信機器等の普及により，様々な分野で暗号通信技術が利用され，情報セキュリティの重要性も高まっている．暗号通信技術の評価として，暗号モジュールに対する様々な暗号解読手法が提案、考察されている中で，攻撃の痕跡を残さない攻撃手法の一つとしてサイドチャネル攻撃があり，暗号化された安全な通信の大きな脅威となっている．サイドチャネル攻撃のなかでも，暗号モジュールの消費電力に着目した電力解析として，SPA(Simple Power Analysis)，DPA(Differential Power Analysis)，CPA(Correlation Power Analysis) [1]などが提案されている．このうちCPAは，条件により正解鍵の特定に数千～数十万の電力波形を必要とし，それに伴う演算量も膨大になる特徴がある．それが，実行を困難にしている要因の１つであり，鍵候補を削減することがその対処の１つといえる．ここでは，CPAの過程において各鍵候補の相関値の変化傾向から，不正解な鍵を予め判別した篩い分けを行うことによって，CPAの性能向上を図る．

2 鍵候補の篩い分け

CPAは，暗号回路が動作する際のクロック信号のエッジにおいて，暗号回路内のレジスタの遷移ビット数と消費電力が比例するというモデルを仮定し，電力波形と電力モデルとの相関を算出する手法である．必要な処理時間は，1波形あたりの波形サンプル数，鍵候補数に比例して増大する．

鍵候補の篩い分けをCPAに適用した先行研究[2]では，計算した相関値に対して，設定した閾値を下回った候補鍵と値を降順に並べた場合の適当な順位以下の候補鍵について篩い分けを行うものであった．

ここでは，母集団をある分布をもつ相関値の集合と考え，複数回の試行で得られた相関値の平均は，試行回数が増加するに従い，正規分布に近づくと仮定する．その上で，取得した電力波形を，複数個に分けて相関値を算出し，その平均値および不偏分散から母集団の期待値を推測し，信頼区間 99%の範囲を算出する．その後，平均値がその範囲に含まれない値を示している候補鍵の篩い分けを行う．CPAはAESの最終ラウンドでの部分鍵に対して実施した．

3　実験環境及び結果

3.1 実験環境

評価基板には産業技術総合研究所及び東北大学で開発されたサイドチャネル攻撃用標準評価基板SASEBO-R [3]を用いた．AES回路はPositive Prime Reed-Muller 理論による1段のAND-XORロジックによるS-boxを記述したAES_PPRM1を使用した．オシロスコープにはIWATSU DS-4354ML，電源にはKIKUSUI PMM18-2.5DU を用いた．クロックにはNFCK1615 から12MHz を供給した．CPAには，サイドチャネル攻撃評価用自動測定ソフトウェア[4]を用いた．

3.2 実験結果

3.2.1 相関値の分布

CPAにより得られた16個の8-bit部分鍵のうち0 ～ 7bitの部分鍵における候補鍵全ての分布図と候補鍵0x11の相関値の頻度分布図を図1及び図2に示す．1つの相関値を算出するために用いる波形数が増加するに従って正規分布に近づき，分散が減少していくことが分かる．相関値の平均が，ある値を中心に正規分布に近づく理由は大数の法則により，母集団の期待値が大標本の場合において，標本の平均の確率分布の平均値と一致する傾向があるためであると考える．

残りの 255個の候補鍵の相関値も同様な分布傾向がみられた．試行回数を 500回としたときの平均と分散を図3に示す． 30波形を用いたとき，平均値は0.1304，分散は0.0288であった．

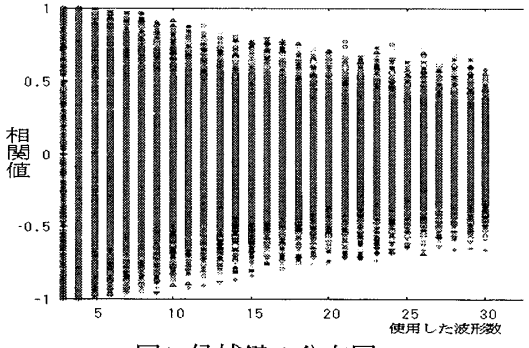
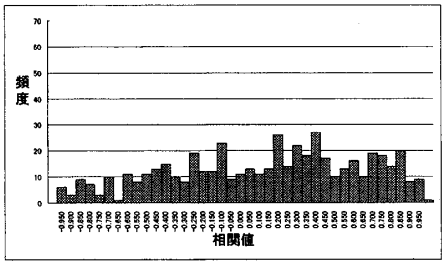
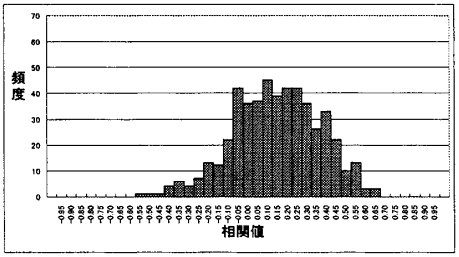


図1：候補鍵の分布図

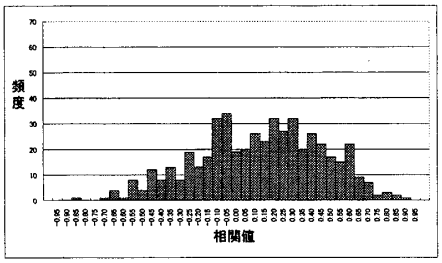
†防衛大学校情報工学科
Department of computer science, National Defense Academy



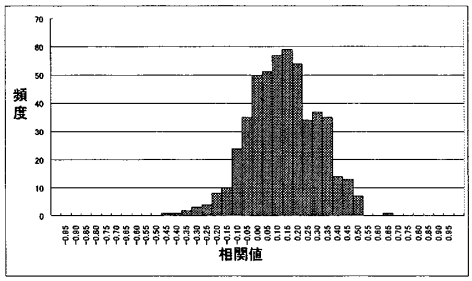
(a)5波形を使用



(c)20波形を使用



(b)10波形を使用



(d)30波形を使用

図2:候補鍵0x11の相関値の分布

3.2.2 篩い分けの実施

図3より，使用波形数が7波形程度にかけて急速に分散が小さくなっていることから，1回の試行回数に使用する波形数を7波形とし，100回の試行により得られた100個の相関値の平均が最大の候補鍵に関して，平均値及び不偏分散から母平均の99%信頼区間を算出した．そして，各候補鍵の平均値の絶対値がこの区間より小さい値を示した候補鍵の篩い分けを行った．0～7bitの部分鍵において，減少した候補鍵は，172個であり，この部分鍵の候補鍵全体で67.18%となった．

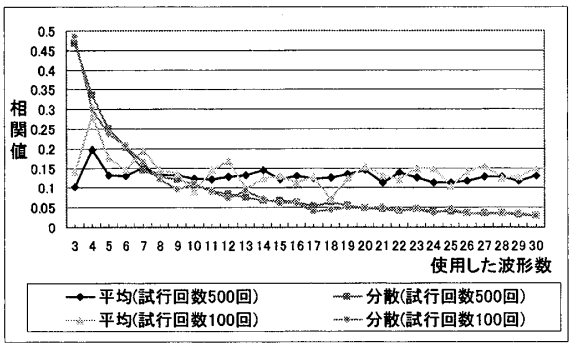


図3:候補鍵0x11の相関値の平均と分散

4 まとめ

CPA における演算量を減少するために，相関値の分布から，母平均及び不偏分散を計算し，それを基に候補鍵の篩い分けを行った．相関値の分布は,5波形ではまとまりがなかったが,波形数を増やしていくと，分散は急速に小さくなり，7波形程度からなだらかに0に近づく．今後はCPA処理に必要な総波形数を，統計手法により減少させるための工夫を考えていく．

参考文献

[1] E.Brier, C.Clavier, and F.Olivier, "Correlation Power Analysis with a Leakage Model," CHES 2004, LNCS 3156, pp.16-29, 2004.

[2] 片下敏宏，佐藤証，菅原健，本間尚文，青木孝文"鍵候補の篩い分けによる CPA の高速化と鍵推定精度の向上" コンピュータセキュリティシンポジウム 2008, D5-1, October 2008.

[3] 産業技術総合研究所情報セキュリティ研究センター，"サイドチャネル攻撃用標準評価基板仕様書第1版，" http://www.rcis.aist.go.jp/files/special/SASEBO/SASEBO-ja/SASEBO_Spec_Ver1.0_Japanese.pdf/, 2007 年3 月.

[4] 岩井啓輔，南崎大作，黒川恭一，"サイドチャネル攻撃評価用自動測定ソフトウェアの開発，" 電子情報通信学会技術研究報告, Vol.108, No.38, ISEC20081-15, pp.9-14, 2008 年5 月.