サイドチャネル攻撃に対するセキュアプロセッサ SEP-6 の耐タンパ性の評価

田代 恵也† 猪股 俊光† 新井 義和† 曽我 正和††
†岩手県立大学 ソフトウェア情報学部 ††岩手県立大学 地域連携研究センター

1 はじめに

IC カードの普及に伴って，IC カードを対象とする攻撃方法が多種多様化してきている．たとえば，電力解析攻撃やタイミング攻撃，電磁波解析攻撃といったサイドチャネル攻撃があげられる [1].

筆者らは，RSA 暗号による高速なディジタル署名計算機能と秘密鍵保持機能を有する非接触 IC カード用セキュアプロセッサ SEP-6[2] を開発している．SEP-6 に対しては，秘密鍵の全ビットパターンが一度に読み出される，暗号計算中に間接的に使用される秘密鍵の各ビット値が計測されて，秘密鍵が推定される，といったソフトウェア的な攻撃に対する耐タンパ性はすでに検証されている．だが，暗号計算実行時に LSI から発生する漏洩電磁波から秘密鍵を推定する電磁波解析といったハードウェア的な攻撃に対する耐タンパ性は検証されてはいない．

そこで，本研究では，SEP-6 でディジタル署名計算を実行し，計算中の漏洩電磁波の観測を行い，観測結果から秘密鍵の推測ができるかどうかを調べ，SEP-6 のサイドチャネル攻撃に対する耐タンパ性について評価した．

2 秘密鍵保護機能

SEP-6 は，秘密鍵保持機能を実装している．秘密鍵保持機能は，セキュア機構と秘密鍵参照回路によって実現されている．セキュア機構では，プログラムの走行モードを署名計算専用命令実行のセキュアモードと汎用計算命令実行のノーマルモードの 2 つに分け，暗号計算中の中間結果を参照されないようにセキュアモードからノーマルモードへと移行するときに暗号計算中の中間結果格納領域のゼロクリアを行い，中間結果が外部に漏洩することを防止している．

暗号計算処理は，RSA 暗号計算をバイナリ法とモンゴメリ乗算を組み合わせたアルゴリズムを利用している．バイナリ法を利用した RSA 暗号計算では，秘密鍵 K は最上位から 1 ビットずつ参照されて，ダイジェスト D の指数として利用されるのみである．秘密鍵を 1 ビットずつ参照して，その値を D^{K_i} に反映させるのが秘密鍵参照回路である．ここで，i は秘密鍵中の i 桁目を示す．

上記のような機能と回路から SEP-6 では，秘密鍵の全ビットパターンの一度での読み出し，暗号計算中の秘密鍵の各ビット値の読み出しといったソフトウェア的な攻撃に対する耐タンパ性を実現している [2].

3 SEP-6 の耐タンパ性の評価

3.1 評価環境

ハードウェア的な攻撃に対する耐タンパ性の評価実験は，表 1 と表 2 に示す評価環境および観測時のパラメータで行った．実験ボードとして，図 1 の三菱電機マイコン機器ソフトウェア社の Power Medusa MU200-SX (搭載 FPGA:Altera 社 Strarix EP1S25F1020C7) を使用した．

表 1: 評価環境

機 材	機材名
FPGA	Altera 社 Strarix
スペクトラム・アナライザー	Agilent 社 N1996A
磁界プローブ	NEC 社 磁界プローブ
プリアンプ	MITEQ 社 AM15949907H
VLSI チップ	SEP-6

表 2: 観測時のパラメータ

設定項目	数 値
Center Freq (中央周波数)	3KHz
Strart Freq (始点の周波数)	0KHz
Stop Freq (終点の周波数)	6KHz
Span (周波数の幅)	6KHz
Ref level (X 軸の上限)	-10dBm
Elec Atten (減衰)	10dB
波形のポイント数	200 Points
CPU 動作周波数	10MHz

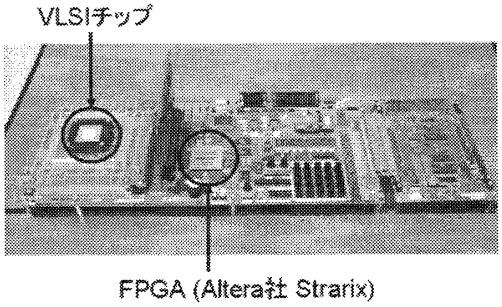

図 1: 実験ボード MU200-SX

Evaluations of Tamper Resistant of a Secure Processor SEP-6 to Side-channel Attacks
† Keiya TASHIRO, Toshimitu INOMATA, Yoshikazu ARAI
†† Masakazu SOGA
Faculty of Software and Information Science, Iwate Prefectural University (†)
Iwate Prefectural University, Iwate Regional Cooperative Research Center (††)

3.2 観測方法

観測方法は，Karine Gandolfi[3] らの観測方法をもとにチップの表面に磁界プローブをできる限り近づけ，図 2 に示すようにスタンドで磁界プローブを固定して行った．なお，電磁波を観測するために NEC 社の磁界プローブを使用した．本研究ではスマートカード上のチップではなく，FPGA ボード上に VLSI 化したチップを搭載したものが観測対象であるために，化学的な溶液等を使用した方法は用いていない．

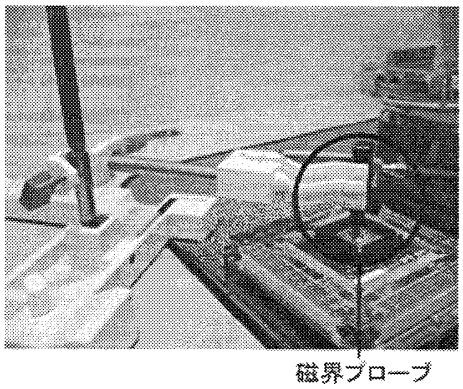

図 2: 観測装置

3.3 評価実験

図 1 の FPGA ボード上に SEP-6 のチップ (VDEC によりチップ化) を搭載し，セキュアモードへ移行するタイミングでトリガ信号を発生させ，セキュアモード移行後にチップ上でディジタル署名計算のプログラムを繰り返し実行し，電磁波の観測を複数回行った．波形の観測点は，チップの観測場所による波形の変化が見られなかったことからチップの中心付近に場所を定めて測定を行った．評価実験の際に使用する秘密鍵のパターンは，以下の通りの 1024 ビットである．

秘密鍵のパターン

- 0x0000 0000 … (0h0000 0000 …)
- 0xFFFF FFFF … (0h1111 1111 …)
- 0xF0F0 F0F0 … (0h1111 0000 …)

4 観測結果

ディジタル署名計算時に実行する命令の 1 クロックを 10MHz としたとき，秘密鍵 1 ビットを使用した計算の命令サイクルが約 3300 クロックなので観測するための各種パラメータは表 2 に示したように設定した．設定した 3KHz 付近の波形に鋭いピークが出現するかどうかを複数個の秘密鍵を用いて観測した波形の比較，評価を行った．もし鋭いピークが出現したときは計算中の秘密鍵の 1 ビットが外部へ漏洩している可能性がある．

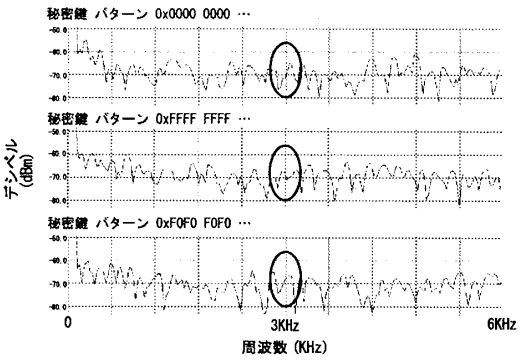

図 3: 署名計算実行時の波形

図 3 は，ディジタル署名計算時に観測された波形である．それぞれ波形の 3KHz の場所を比較したところディジタル署名計算実行時に鋭いピークは出現しなかった．よってディジタル署名計算中の ‘1’ と ‘0’ とで観測される電磁波に顕著な差がでないということを確認できたといえる．

5 おわりに

本研究では，暗号処理を行う際に生じる電磁波に着目し，セキュアプロセッサ SEP-6 のサイドチャネル攻撃に対する耐タンパ性の評価を行った．評価を行った結果，3KHz 付近には鋭いピークは現れず，秘密鍵の 1 ビット計算時の ‘1’ と ‘0’ のときで発生する電磁波に顕著な差がでないことを確認し，耐タンパ性があることがわかった．

今後の課題として，命令サイクルに着目して評価を行うのではなく，観測された波形のどの部分でどのような命令が実行されているのかということを調査し，観測したときに秘密鍵が推測できる可能性があるのかどうかについて調べる必要が明らかになった．

謝 辞

SEP-6 のチップ化は東京大学大規模集積システム設計教育研究センター (VDEC) を通し，シノプシス株式会社，日本ケイデンス株式会社の協力で行われました．

参考文献

[1] 財団法人日本規格協会情報技術標準化研究センター: 平成 15 年度 経済産業省委託 (基準認証研究開発事業) 耐タンパー性に関する標準化調査研究開発報告書 第一部, http://www.jsa.or.jp/stdz/instac/committe/H15report/report-contents/01_06_01.PDF

[2] 高橋 大介, 猪股 俊光, 新井 義和, 曽我 正和: 非接触 IC カード用セキュアプロセッサ SEP-6 の開発, 電子情報通信学会技術研究報告, Vol.106, No392, pp.61-66, (2006)

[3] Karine Gandolfi, Christophe Mourtel, and Francis Olivier: Electromagnetic Analysis:Concrete Results, CHES 2001, pp.251-261, (2001)