リーク電流に起因するLSI暗号回路の脆弱性に関する研究

研究代表者　　史　又華　　早稲田大学　高等研究所　准教授

1 まえがき

情報処理技術の発達により、現代社会では個人情報などの機密情報を電子機器でやりとりするのが一般的になってきている。また、これから本格的な到来が予想されるアンビエント情報化社会は、人間社会の様々な場所でデジタル化された情報技術を活用する社会である。これはありとあらゆる場所で、個人個人がコンピュータにアクセスでき、必要な情報を必要な時にやりとりでき、人間生活を強力にバックアップしてくれる社会である。言い換えれば、それだけ情報技術に依存した人間社会が到来するということである。

情報化社会は便利である反面、機密データの盗聴、改ざんによる悪用の脅威に常にさらされている。ひとたび悪意のある第三者にクレジットカードの番号や、パスワードを盗まれれば、ネットワークサービス全体の信頼性が低下し、サービスとして成り立たなくなる。それを防ぐため、機密情報を安全にやりとりする手段に暗号技術がある。なかでも、クレジットカードやUSBメモリなどに記録される情報を安全にやりとりするための技術の一つに、暗号 LSI(Large Scale Integration) がある。暗号 LSI は DES(Data Encryption Standard) や AES(Advanced Encryption Standard)などのブロック暗号の演算を高速に演算するハードウェアである。暗号LSIを利用することにより、機密情報を第三者にはわからない暗号化した形で高速に扱うことができる。しかし、数学的な理論上安全とされていた暗号をハードウェア実装する場合、暗号化演算中に、消費電力、タイミング情報などの物理的な情報が外部に漏れ、そこから機密情報を復号できることが、リスクとなっている。そのため、LSI暗号回路の脆弱性を解明する必要がある。

LSI 暗号回路が内部情報を暴露する要因は、暗号回路に用いられる論理回路の電流値が変動するためである。従来、CMOS回路における電力損失の最大の要因は、CMOSのスイッチング動作に起因するダイナミック電力であった。ダイナミック電力は、電源電圧の２乗に比例し、クロック周波数に比例する。これ対して、現在もう１つの大きな電力損失要因として挙げられているのが、CMOSデバイスから漏れ出すリーク電流に起因するリーク電力である。このリーク電力は、プロセスの微細化が進むと、ダイナミック電力と同程度にまで増加すると予想されている。したがって、リーク電流に起因するLSI暗号回路の安全性評価は重要と考えられる。そのため、本研究では、微細プロセスで増大するリーク電流を測定/解析することで、暗号回路の秘密鍵に関する情報が読み取られる可能性について解明する。更に、このような攻撃を防御できる暗号LSI回路設計技術を確立する。

2 電力解析攻撃

90年代後半から、暗号アルゴリズムが実装された暗号回路に対する物理的な様々な攻撃法（内部情報の不正な取得を試みること）が提案され、情報セキュリティに対する新たな脅威となってきた。特に、暗号回路の処理時間や消費電力といったいわゆるサイドチャネル情報を解析する“サイドチャネル攻撃”と呼ばれる攻撃法は、強力な攻撃法として注目されている。

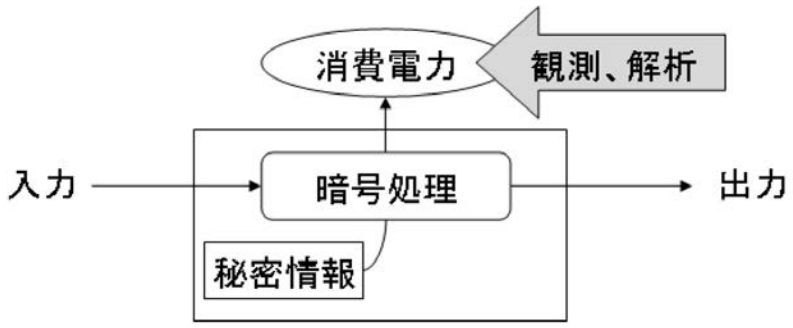


図１： 電力解析攻撃

表１：AES 暗号回路に対する電力解析攻撃手法[４]

攻撃手法	特徴	攻撃区間
DPA	推定する部分鍵に対応した中間値の特定の 1 ビットの値によって 2 組に分けた，電力波形の平均の差を計算し，その平均波形とビット値の相関を調べる．最も基本的かつ汎用的な攻撃．	10 ラウンド
M-DPA	推定する部分鍵に対応した中間値の複数ビットを用い，そのハミング重みが閾値以上であるか否かによって，電力波形を 2 組に分類するする．その電力波形の平均の差を計算して，ハミング重みとの相関を調べる．攻撃精度は回路の実装法に大きく依存する．	10 ラウンド
B-DPA	推定する部分鍵に対応した中間値の複数ビットに対する DPA の結果を結合する汎用的な攻撃．	10 ラウンド
CPA	推定する部分鍵に対応した中間値を格納するレジスタが遷移したときのハミング距離と消費電力の関係を調べる．未対策の回路であれば，B-DPA の 1/10 以下の波形数で攻撃可能．	データ出力
PPA	CPA の拡張でハミング距離に重み付けを行うが，その効率的な係数の設定方法は提案されていない．	データ出力
M2-DPA	電力波形の中のある 2 つの区間の相関を解析する攻撃法．攻撃精度は実装に依存する．	10 ラウンド
W2-DPA	DPA が平均波形の差を求めるのに対して，2 乗平均の差を計算する汎用的な攻撃．	10 ラウンド

サイドチャネル攻撃の一つであり、電力解析は 1998 年、Kocher らによって提唱された。電力解析では、電力を測定・解析することで、暗号化を行う際に使用する秘密情報を求める(図 1 参照)。暗号回路を構成しているトランジスタのゲートに電圧が加えられた時、電流はトランジスタを通過し、電力を消費する。この消費電力はダイナミック電力と呼ばれ、ゲートの遷移確率に依存している。一般的に入力値によってこのゲートの遷移確率は異なるため、消費電力から入力値に関する情報を推測、抽出することが出来る。LSI 暗号回路へのダイナミック電力を用いる解析手法に関する研究は、90 年代後半に始まってから、多くの研究者によって絶えずに続けられている。たとえば、単純電力解析 (Single Power Analysis: SPA) [1]、差分電力解析 (Differential Power Analysis: DPA) [2]、および相関電力解析 (Correlation Power Analysis: CPA) [3]が提案された。このようなスイッチング動作時のダイナミック電力解析方法によれば、暗号解読に要す計算量よりも遥かに少ない手間で秘密鍵を特定できることがあり、現実的に対処が必要な脅威として近年、研究が行われている。表 1 に AES 暗号回路の実装に向け、代表的な電力解析攻撃手法を示す。

そのため、現在の暗号回路設計においてはスイッチング動作時のダイナミック電力攻撃に対して耐性のある設計が求められており、暗号回路内の秘密情報がダイナミック電力などのサイドチャネル情報に相関をもって現れないように、注意深くデバイスを設計することが求められている。

一方、プロセスの微細化が進むと、リーク電力はダイナミック電力と同程度に増加することを予想されている。しかし、既存研究ではほぼスイッチング動作時のダイナミック電力を注目し、繰り返し測定することで秘密情報を解析している。したがって、リーク電流に起因する LSI 暗号回路の安全性評価は重要と考えられる。そのため、本報告は微細プロセスで増大するリーク電流を測定/解析することで、暗号回路の脆弱性を示す。

3 リーク電流特性の実験結果と考察

本報告は、45nm プロセスで作られた CMOS 回路素子をトランジスタレベルでのシミュレーションを行うこ

とで、基本ゲートで生じるリーク電流の電源電圧・温度特性を取得し、さらにリーク電流の入力ベクトル依存性を明らかにした。回路シミュレータは Synopsys 社製の Hspice を用いた。また、トランジスタモデルはゲートリークを考慮した BSIM4.0 [5] を用い、セルライブラリは、45nm プロセスである Nangate 社のオープンセルライブラリ Nangate45nmFreePDK [6] を用いた。対象とする論理ゲートは、AND、NAND、OR、XOR、3 入力 NAND 等である。また、暗号回路の部分的な回路として一般的なブロック暗号で使われる、暗号回路中の秘密鍵と中間値の XOR 演算部を想定した小規模の暗号回路を DFF とクロック信号から、シミュレーションを行った。

3-1　論理ゲートリーク電流の温度・電源電圧特性

45nm プロセスでの基本論理ゲートのリーク電流特性を明らかにするため、基本論理ゲートのリーク電流の特性を Hspice を用いた計算機シミュレーションの結果から示した（図 2−5 参照）。図中の横軸は論理ゲートへの入力である。2 入力ゲートの場合は {00、01、10、11}、3 入力ゲートの場合は{ 000、001、010、011、100、101、110、111}をとる。温度特性は、各動作電圧で回路の温度毎にリーク電流を測定した値をグラフ化したものである。

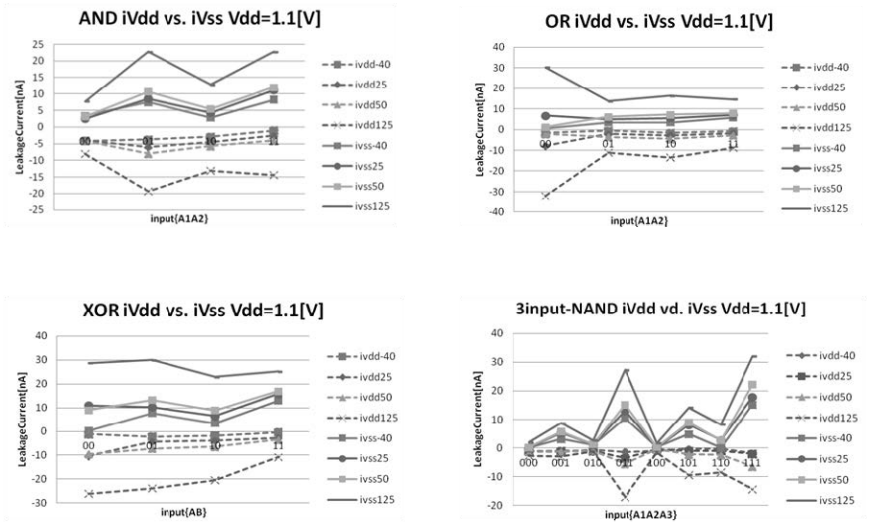


図 2.　基本ゲートリーク電流の温度特性　（電源電圧 1.1V）

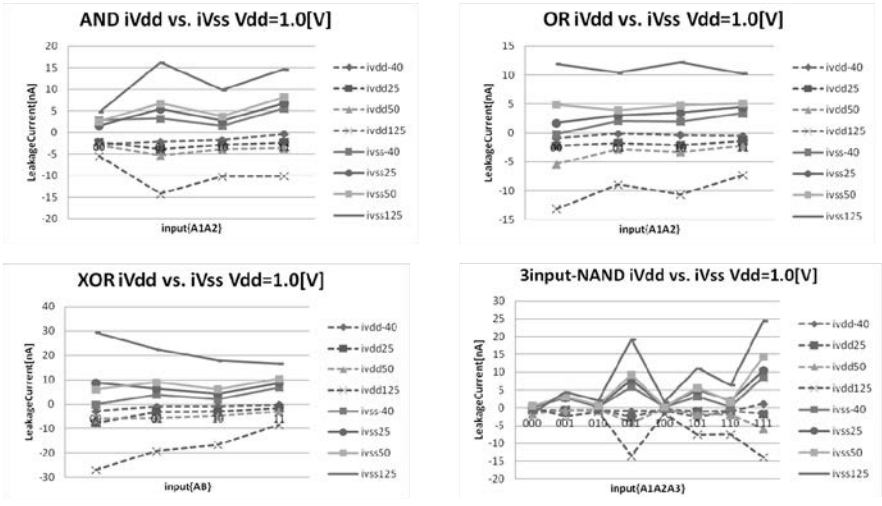


図 3.　基本ゲートリーク電流の温度特性　（電源電圧 1.0V）

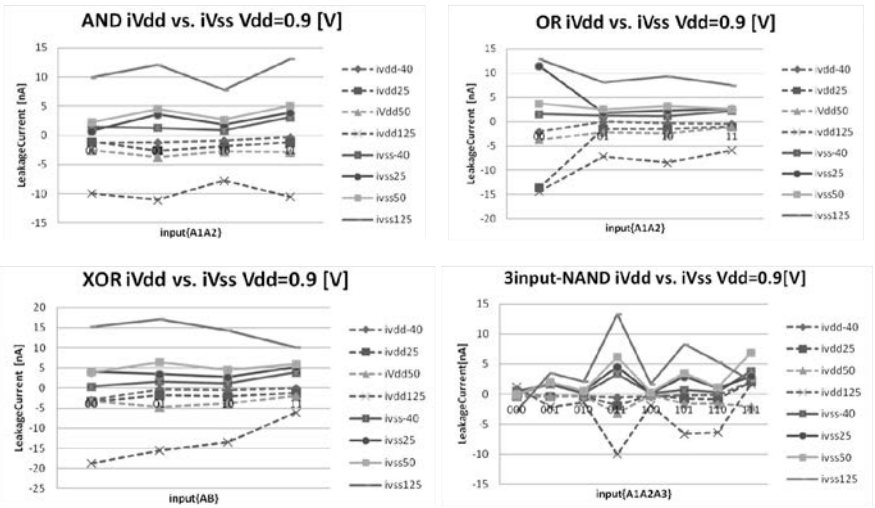


図 4.　基本ゲートリーク電流の温度特性　（電源電圧 0.9V）

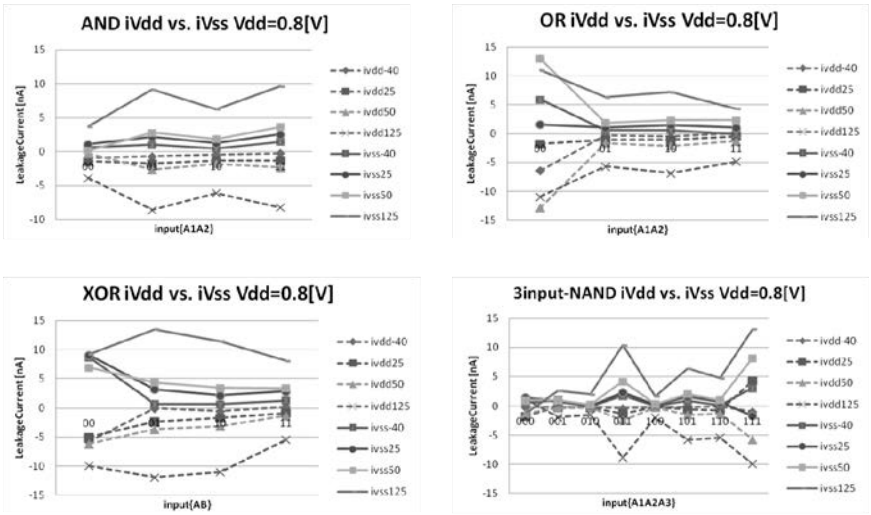


図 5.　基本ゲートリーク電流の温度特性　（電源電圧 0.8V）

図 6 に 45nm 論理ゲートリーク電流の電源電圧特性を示す。暗号回路の重要な要素である XOR ゲートに関して 25℃で電源電圧特性を整理した。図中の横軸は論理ゲートへの入力であり、{00、01、10、11} の値をとる。

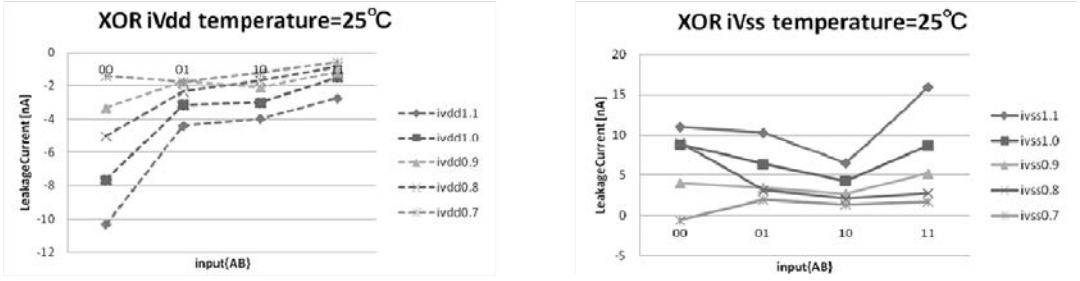


図 6.　XOR ゲートリーク電流の電源電圧特性@25 ℃

BSIM4.0 のモデルによれば、ゲートリーク I_{gate} の電流密度 Jg は式（１）でモデル化される[7]。

$$J_g = A\left(\frac{T_{oxref}}{t_{ox}}\right)^{ntox}\frac{V_g V_{aux}}{t_{ox}^2}e^{-B(\alpha-\beta\ |V_{ox}|)(1+\gamma\ |V_{ox}|)t_{ox}} \quad (1)$$

ここで、A と B は、それぞれ $1/\phi_b$ と $\phi_b^{3/2}$ の成分を持つ定数（ϕ_b はキャリアが量子的な効果でトンネルするための障壁の高さ）である。n_{tox} はフィッテングパラメータで初期値は 1 である。T_{ox} は酸化膜厚であり、T_{oxref} は酸化膜厚の参照値ですべてのパラメータが抽出されたあとに決まる。また、α、β、γは物理的なパラメータでデバイステクノロジによって決まる。また V_{aux} は、ECB(electron tunneling from the conduction band) と HVB(hole tunneling from the valence band) または EVB(electron tunneling from the valence band) のキャリアの密度を指し示す関数である。Jg は電流密度であるので、リーク電流とは異なるが、面積を乗ずること電流値となる。ここでは式としてリーク電流を統一的に表現するためにこの形式で表現した。

式（１）より、ゲートリーク電流は、式中に温度の変数は存在せず、ゲート電圧に依存している。今回の実験で得られた特性(例えば図 2) において、温度が下がるほどリーク電流は小さくなり、また電源電圧が下がるほどリーク電流は小さくなっていたのはこれら式の影響である。

今まで、電力解析攻撃を扱った文献では、温度が低いとリーク電流が小さくなり攻撃がしにくいことが指摘[8] されていたが、今回の実験で得られた図 6 の形状から、温度だけでなく、電源電圧を下げることでも攻撃がしにくくなる可能性が高い。

3-2　リーク電流の入力依存性

CMOS 論理素子のリーク電流と入力依存性も検討した。NMOS と PMOS が相互作用を起こることにより、入力値によってリーク電流が変わる。例えば、3 入力 NAND ゲートを例として、リーク電流の大きさについて、スタック効果が観測されている。ここで、2 入力 XOR ゲートの実験結果を HW(Hamming Weight) と HD(Hamming Distance) に基づき整理すると、それぞれ表 2 が得られる。表 2(a)より、ハミングウェイトとリーク電流に一定の相関があるとはいえないことがわかる。CPA が成功するためには、ハミング距離（重み）を算出するレジスタに接続される論理回路の消費電力が、そのレジスタの遷移するビット数と相関を持つ必要があるため、CPA を用いた M. Alioto らの手法[9]は、45nm 暗号 LSI に適応できない可能性がある。また、表 2 の鍵値と入力値から計算されるハミング距離に関しても、一定の強い相関を持っていないことから、既存の DPA や CPA ではリーク電流の測定回数が多くかかり、解析に時間がかかることが予想される。測定回数に関しては、M. Alioto らの手法は、n-bit の鍵に対して 2^m 回の測定回数を必要としている。

表 2　リーク電流の入力依存性

(a) HW とリーク電流の関係

HW	Input{D0K0D1K1}	iVss[nA]	iVdd[nA]
0	0000	-1.70E+02	1.81E+02
1	0001	-3.01E+02	3.12E+02
	0010	-1.85E+01	3.57E+01
	0100	-3.01E+02	3.12E+02
	1000	-1.85E+01	3.57E+01
2	0011	-1.72E+02	1.94E+02
	0110	-1.02E+02	1.21E+02
	1100	-1.72E+02	1.94E+02
	1001	-1.02E+02	1.21E+02
	1010	-9.78E+00	1.17E+02
	0101	-1.74E+02	1.90E+02
3	0111	-2.43E+01	2.65E+01
	1110	-1.29E+02	1.50E+02
	1101	-2.43E+01	2.65E+01
	1011	-1.29E+02	1.50E+02
4	1111	4.47E+01	-2.19E+01

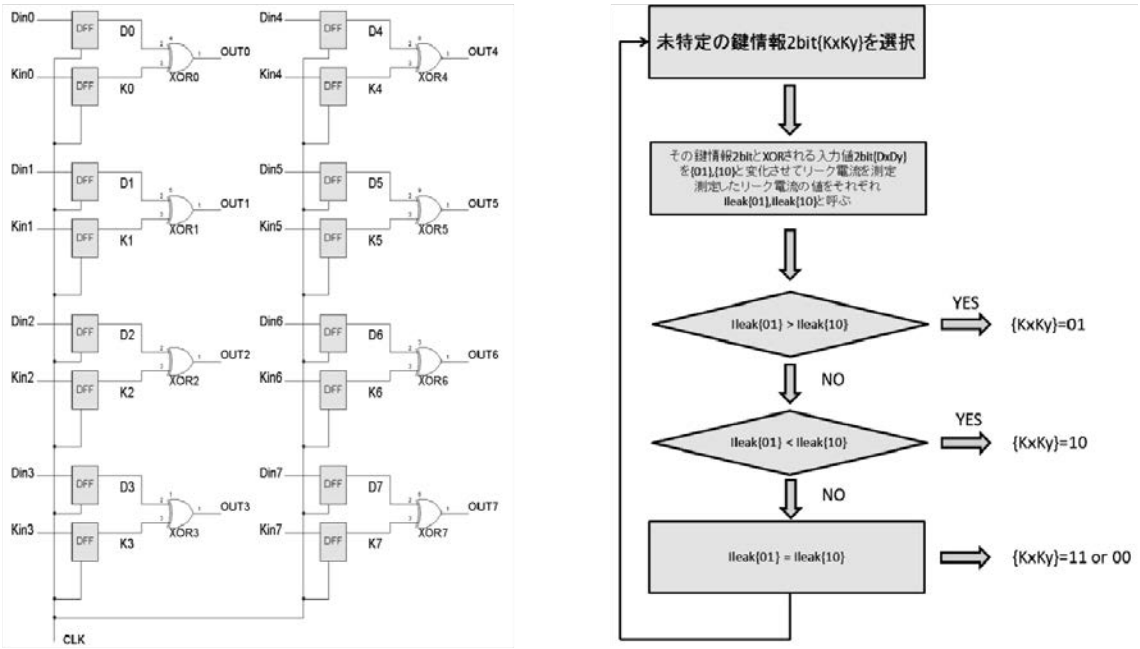
(b) HD とリーク電流の関係

HD	Input{D0K0}	KEY{K0K1}	XORout	iVdd[nA]	iVss[nA]
0	00	00	00	-1.70E+02	1.81E+02
	01	00	01	-1.85E+01	3.57E+01
	10	00	10	-1.85E+01	3.57E+01
	11	00	11	-9.78E+00	1.17E+02
1	00	01	01	-3.01E+02	3.12E+02
	01	01	00	-1.72E+02	1.94E+02
	10	01	11	-1.02E+02	1.21E+02
	11	01	10	-1.29E+02	1.50E+02
	00	10	10	-3.01E+02	3.12E+02
	01	10	11	-1.02E+02	1.21E+02
	10	10	00	-1.72E+02	1.94E+02
	11	10	01	-1.29E+02	1.50E+02
2	00	11	11	-3.01E+02	3.12E+02
	01	11	10	-1.02E+02	1.21E+02
	10	11	01	-1.72E+02	1.94E+02
	11	11	00	-1.29E+02	1.50E+02

4 リーク電力解析攻撃の提案と実装

一般的なブロック暗号で用いられる XOR 演算を想定した小規模の暗号化回路に対して、リーク電流を用いた攻撃手法を提案した。また、シミュレータを用いた測定結果に提案手法を適応することで有効性を示す。

CMOS 論理素子のリーク電流と入力依存性の結果により、n bit の XOR 演算に関して、リーク電流の値が測定でき、任意の 2bit を操作すれば、測定できたリーク電流値の大小から、XOR 演算される鍵情報を導出できるという仮説を立てることができる。ただし、鍵値 {K0K1} の値が{00} または{11}の場合は、入力値によらず同じリーク電流の値を示すので、鍵情報を 0 か 1 か判断するためには、鍵情報 n bit の少なくとも 1bit が異なっている必要がある。しかし、任意の 2bit すべてを 01 あるいは 10 と変えて測定した結果がすべて同じであれば、鍵情報はすべて 0 かすべて 1 のどちらかに特定できることとなり、鍵情報は導出できる。



(a) 部分的な暗号回路　　(b) 提案手法の流れ

図 7.　提案手法の概要

図 7(a)のような一般的なブロック暗号で使われる XOR 演算回路の小規模な構成を考える。前提条件として、プロセスばらつき、温度ばらつき、ノイズの影響は全くない理想的な環境であることを仮定する。攻撃者は暗号回路中の入力{$D_0D_1D_2D_3$ $D_4D_5D_6D_7$}任意の 2bit を他の bit を固定したまま操作可能であるとし、その際のリーク電流の値を測定できる。ただし、XOR 演算される秘密鍵情報{$K_0K_1K_2K_3$ $K_4K_5K_6K_7$}は攻撃者に未知で、さらに XOR 演算結果は攻撃者が観測できないものとする。今、攻撃者の目標は、リーク電流の値から XOR される秘密情報秘密鍵情報{$K_0K_1K_2K_3$ $K_4K_5K_6K_7$}を全 bit 特定することである。提案手法の流れは以下のようになる。

1. 未特定の鍵情報値 2bit{KxKy}を選択する。
2. その鍵情報 2bit と XOR される入力値を{01} と{10} と変化させ、リーク電流を測定する。この際測定できたリーク電流の絶対値を I_{leak}[01]、I_{leak}[10]と呼ぶ。
3. 測定したリーク電流の絶対値を比較する。次の比較した結果を元に、鍵情報を次の 3 条件で判断する。
   (a) I_{leak}[01] ＜ I_{leak}[10] ⇒ {KxKy} ＝ {10}
   (b) I_{leak}[01] ＞ I_{leak}[10] ⇒ {KxKy} ＝ {01}
   (c) I_{leak}[01] ＝ I_{leak}[10] ⇒ {KxKy} ＝ {11} or {00}
4. 条件(a) または(b) で鍵情報が特定できた場合は、次の 2bit を選択する。
5. 条件(c) で判断できない場合は、今選択した 2bit の中の 1bit と新しい 1bit と比較し、3 の条件にあてはめる。
6. 上記を全 bit 特定できるまで繰り返す。

表 3. 提案手法による解析用の測定結果（2bit 以外が 0 の場合）

KEY {0010 1011}に対する入力とリーク電流値			
	$D_0D_1D_2D_3$ $D_4D_5D_6D_7$	iVdd[nA]	iVss[nA]
①	0100 0000	-1.81E+01	1.14E+02
②	1000 0000	-1.81E+01	1.14E+02
③	0010 0000	-2.38E+02	3.25E+02
④	0001 0000	-1.81E+01	1.14E+02
⑤	0000 1000	-2.38E+02	3.25E+02
⑥	0000 0100	-1.81E+01	1.14E+02
⑦	0000 0010	-2.38E+02	3.25E+02
⑧	0000 0001	-2.38E+02	3.25E+02

表 3 に、簡単のため任意の 2bit 以外が 0 の特殊なケースを示す。シミュレータ上のデータに置いて、秘密鍵値{$K_0K_1K_2K_3$ $K_4K_5K_6K_7$}は、{0010 1011}とした(攻撃者には未知)。

提案手法の流れに沿って、上位 2bit{K0K1}から特定する。上位 2bit を変えて測定した結果①と②を比較する。この際、I_{leak}[01] ＝ I_{leak}[10] であるから、{K0K1}は{11}または{00}であることがわかる。次に、①と③を比較する。①のデータが鍵値{K1K2} に対して{10}を入力する場合に相当し、③のデータが{01}を入力する場合に相当する。これより I_{leak}[01] ＞ I_{leak}[10] なので {K1K2} は、{01} と求まる。この時同時に、{K0} も {0} であると求まる。次に、③と④を比較すると、I_{leak}[01] ＜ I_{leak}[10] なので{K2K3}は、{10}と求まる。今、ここまで秘密鍵情報上位 4bit{ K0K1K2K3} が{0010}と求まった。次に、⑤と⑥を比較すると I_{leak}[01] ＜ I_{leak}[10] なので{K4K5}は、{10}と求まる。次に⑦と⑧を比較すると、I_{leak}[01] ＝ I_{leak}[10] であるから、{K6K7}は{11}または{00}であることがわかるここで、⑥と⑦を比較すると、I_{leak}[01] ＞ I_{leak}[10] なので {K5K6}は、{01} と求まる。このことから、{K7} も {1} であると求まる。以上を総合して、秘密鍵値{$K_0K_1K_2K_3$ $K_4K_5K_6K_7$}は、{0010 1011} と求めることができる。

既存手法がハミング重みやハミング距離による相関性を利用していたのに対して新しい手法で XOR 演算部を攻撃することが可能であることが結果から示すことができた。しかしながら、解決しなければならない課題も多い。まず、任意の 2bit を反転させる方法であるが、これに関しては暗号 LSI に対してレーザーを用いて bit 反転を起こす、フォールト攻撃が利用できる。また、他の手法でもクロックグリッチを利用した手法や電磁波を用いた手法も研究されており、今後の動向を調査し、本研究に応用できないか検討する必要がある。

また、今回の測定はチップ内の温度ばらつき、プロセスばらつき、ノイズの影響がない理想的な条件でのシミュレーションであった。ノイズの影響は、複数回の測定により平均をとることで影響をさげることができる。しかしながら理想環境でない状態であれば、プロセスや温度ばらつきの影響で、今回の条件で用いた等号条件は使えない。等号成立と不等号成立の大小を見極める検討もしていくことで、実用的な攻撃に近づけることができる。さらに考えられる問題として、表 3 にある差が測定器を用いて測定できるのかという問題が考えられる。しかし測定器に関しては、p [A] 精度の電流計が販売されているため、精度の高い測定することが可能である。

5 リーク電力解析に耐性もつ暗号回路設計

より安全性の高い暗号処理 LSI を実現するという観点から、ダイナミック電力解析の対策を施した暗号回路と未対策の暗号回路におけるリーク電流解析に対する安全性の評価を行った。更に、2 相ラッチを利用し、提案したリーク電流攻撃手法を防御できる暗号 LSI 回路も設計した。

6 結論

本報告では 45nm プロセスで作られた暗号 LSI を想定した回路シミュレーションを行うことで、基本ゲートで生じるリーク電流の電源電圧- 温度特性、入力依存性を明らかにした。また、一般的なブロック暗号で使

われる XOR 演算部を想定した小規模な暗号回路にリーク電流を利用した解析を行うことで内部情報を読み取り、攻撃可能な手法を提案した。提案手法を用いることで、45nm プロセスで作られた部分的な暗号化回路に対して、攻撃者は部分的な暗号化回路入力の任意の 2bit を変えることにより、測定したリーク電流値の比較だけで XOR される秘密鍵を特定することができ、リーク電流に起因する LSI 暗号回路の脆弱性を示した。この結果は、電源電圧・クロック信号などの不正使用による内部情報漏洩を防ぐことが可能になることを示唆する。

【参考文献】

[1] S. Mangrad, “A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion,” In Proceedings of the International Conference on Information Security and Cryptology - ICISC 2002, LNCS2587, pp.343--358, Springer-Verlag, 2002.

[2] P. Kocher, J. Jaffe and B. Jun, “Differential Power Analysis,” In Advances in Cryptology -- CRYPTO'99, LNCS1666, pp.388--397, Springer-Verlag, 1999.

[3] E.Brier, C.Clavier, and F.Olivier, “Correlation Power Analysis with a Leakage Model,” CHES2004, pp.16-29, 2004.

［4］産業技術総合研究所情報セキュリティ研究センター，SASEBO の電力解析攻撃実験，2010 年 1 月.

[5] UC Berkeley Device Group,“ BSIM4.0.0 MOSFET Model, ”available at http://www-device.eecs.berkeley.edu/ bsim3/bsim4.html

[6] Nangate Inc. Open Cell Library v2008 10, Oct. 2008. Downloadable from http://www.nangate.com/openlibrary

[7] K. Cao, W. Lee, W. Liu, X. Jin, P. Su, S. K. H. Fung, J. X. An, B. Yu, and C. Hu,“ BSIM4 Gate Leakage Model Including Source-Drain Partition,” in IEDM Technical Digest, IEDM, pp. 815–818, 2000.

[8] L. Lin and W. Burleson,“ Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems, ”IEEE ISCAS, pp. 252–255, 2008.

[9] M. Alioto, L. Giancane, G. Scotti and A. Trifiletti,“Leakage Power Analysis Attacks: a Novel Class of Attacks to Nanometer Cryptographic Circuits, ” IEEE Trans. on Circuits and Systems I, vol. 57, no. 2, pp. 355–367, Feb. 2010.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
故障解析に耐性を持つラッチを利用した AES 暗号回路	電子情報通信学会・信学技報	2014 年 3 月
サブスレッショルド回路における遅延・エネルギーの温度依存性に関する実験および考察	電子情報通信学会・信学技報	2014 年 3 月