暗号への脅威「サイドチャネル攻撃」とその対策

崎山一男・太田和夫（電気通信大学情報通信工学科，暗号理論・暗号実装）
さきやま　かずお　　おおた　かずお

暗号技術――情報を保護する技術は，現代の情報化社会において不可欠な存在であり，その重要性は増すばかりである．その技術の基盤となっている暗号理論によれば「安全に利用できる」はずの暗号方式が，実装方法によっては「秘密が漏れてしまう」暗号方式となる危険性が報告されている．

今日，ディジタル情報通信技術は大いに発展し，個人の日常生活にも深く浸透している．情報を保護する暗号技術が情報化社会の利便性を享受するためのライフラインとして機能している．

暗号理論と暗号実装

現在のディジタル情報システムにおいて，その営みを支えているのは，システムの心臓であるLSI(large scale integrated circuit)である．世の中にあるすべてのディジタル情報がLSIで処理されている，といっても過言ではない．理論研究により生み出された種々の暗号方式もまたLSIに実装され，情報の保護を担うシステムとして広く普及している．銀行のICカードがその代表である．このように，暗号理論と暗号を安全に実装する技術(暗号実装)とは不可分な関係にあるといえる．

ところが，1999年に発表されたある論文が，暗号理論と実装の関係に一石を投じることとなった．理論的には安全な暗号でも，実装の仕方によっては情報漏れの危険性があることが示されたのである．暗号実装に思わぬ「落とし穴」が発見されたのである．

このことを説明するためには，まず，現代の暗号理論における暗号方式を簡単に説明する必要がある．暗号理論では有線・無線にかかわらず通信路(channel)上の情報の保護を考える．たとえば，花子が太郎にデートの待ち合わせについてメッセージを送る場合を考えよう．この待ち合わせの情報は，他の誰にもばれないようにしたい．しかし，通信路上のデータは誰でも取得できることが前提であるため，花子はメッセージの内容が読まれることのないように，メッセージを暗号化する．太郎だけが暗号化されたメッセージを復号化することができ，デートの待ち合わせ情報を花子と共有することができる．

太郎はあらかじめ用意した自分だけが知っている秘密の情報(秘密鍵)を使って復号化を行う．実際には，太郎はディジタル機器を用いて復号化処理を行う．秘密鍵は太郎が所有するディジタル機器に格納されており，誰にも読みだされないよう保護されている．秘密鍵が読みだされてしまうと，太郎が復号化を行うときの処理を真似して，花子からの暗号化されたメッセージは復号化され，メッセージの内容が読まれてしまうからである．つまり，ディジタル機器に格納されている秘密の情報は決して読みだされないということが，暗号理論では前提となっているのである．

秘密情報が“脇道”から漏れる？

次のクイズをご存知だろうか？「新しい家に引っ越してきた．2階には3つの白熱球の照明器があり，それらのスイッチは1階にしかない．3

つの照明器を制御する3つのスイッチがあり，今はすべてオフとなっている．どのスイッチがどのライトにつながっているかは不明だが，スイッチと照明器は組になっており，1つのスイッチで，1つの照明器しか点灯・消灯できないようになっている．1階のスイッチにラベルを貼って，照明器との対応付けをしたいのだが，できる限り1階と2階の往復回数を少なくしたい．さて，1階と2階を何往復すれば，すべてのスイッチに正しくラベルを貼ることができるだろうか？」

一般に正解とされているのは，次の手順による1往復である．「どれか2つのスイッチをオンにし，しばらく経った後にオンした2つのスイッチのうち1つをオフにし，2階に上がる．照明は1つだけ点いており，その照明がオンとなっているスイッチとつながっていることがわかる．残りの2つの照明器のうち，白熱球を手で触り，熱を感じられるほうが，オンからオフに切り換えたスイッチに対応しており，他方がまったく操作しなかったスイッチと対応している」というものである．

見ているだけでは，白熱球が点灯・消灯という2つの状態しかないと思いこんでしまう点にクイズのおもしろさがある．白熱球は点灯時に熱が伴う．この当たり前の物理現象がこのクイズのミソとなっているのだ．白熱球を交換する際に熱くて交換できなかった，という経験があれば，簡単に答を出すことができるかもしれない．

このクイズの場合，発熱という物理現象を利用した．つまり，白熱球の球面から手に熱が伝播することにより，新たな情報が得られたのである．この情報の伝達経路(白熱球から手)は，本来の情報の経路(白熱球から眼)とは別の“脇からの情報路”という意味で，サイドチャネル(side channel)からの情報と呼ぶことができる．

はたして，暗号処理システムにおいてもサイドチャネルは存在するのであろうか？　それはどのようなものであるか？　次に，暗号処理LSIを例にあげ，LSI内部の秘密情報が，サイドチャネルから漏えいする危険性があることを紹介する．

サイドチャネル攻撃の実際: RSA暗号処理LSIのケーススタディから

LSIにはデータを入力・出力するための信号ピンが存在する．これらのピンは，本来の情報を伝達するための経路であり，暗号処理機能実現のために必要な信号のやりとりに使われる．LSIは微細な電気回路が集積されており，その動作には電力供給が必須である．つまり，LSIは機能のための入出力ピンに加え，電力供給に必要なピンが存在する．この電力供給のための経路がサイドチャネルとなり，思いもよらぬ情報が漏れる可能性がある．もう少し詳しく説明しよう．先述のとおり，暗号処理LSIには通常，秘密鍵が組み込まれており，秘密鍵を用いて暗号化・復号化といった処理が実行される．したがって，秘密鍵の値によりLSIでの処理は異なり，消費される電力もこの秘密鍵の値により異なるのである．つまり，電力供給のためのピンから，処理中の消費電力を測定すると，秘密鍵が特定できる場合があるのである．

公開鍵暗号で有名なRSA[(1)]暗号を例として，消費電力と秘密鍵の関係を調べてみよう．まず，RSA暗号の暗号化・復号化の処理は，ある数のべき乗をNで割ったときの余りを求めることで実現されている(剰余系におけるべき乗算)．ここでは詳細は述べないが，復号化では，暗号文Cを秘密鍵であるdを用いて$C^d \bmod N$を計算すると，元のメッセージに復号できる．以下簡単のため，べき乗算，乗算，自乗算はすべて剰余系における演算を意味するものとする．

RSA暗号の復号化処理に必要なべき乗算C^dにおいて，素直にCをd回乗算するというナイーブな方法は非現実的である．なぜなら，現在dには1024ビット以上の値が用いられるため，2^{1024}回の乗算が必要となるからである．1秒間に1兆回の乗算を行うLSIが存在し，それを使ったとしても復号化処理には約300桁の年数を費やす．人は長くても3桁の寿命であるから，太郎が花子のメッセージを復号し，読むことは不可能である．

そこで，乗算の回数を減らすための工夫を行う．

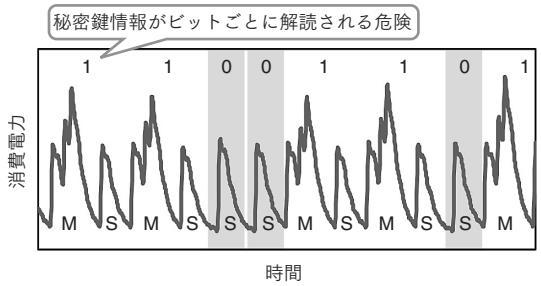

図1——RSA 復号化処理中の消費電力の時間変化．正確には，LSI と直列接続した抵抗における電圧差を測定し，電力に換算したもの．図中 S，M に対応する電力ピークはそれぞれ，剰余系における自乗算と乗算によるものである．S と M の出現パターンに不規則性が見られ，これにより秘密鍵が特定できる．

簡単な例をあげると，C^{205} を計算する際には，

$$C^{205}=C^{128+64+8+4+1}$$
$$=((((((C^2\times C)^2)^2)^2\times C)^2\times C)^2)^2\times C$$

とする．自乗算をうまく利用することで計算効率を大幅に良くすることができるのである．工夫なしでは 204 回の乗算が必要であるのに対し，自乗算を利用することで 4 回の乗算と 7 回の自乗算で計算可能なことを示している．通常の 1024 ビットの d の場合でも，およそ 500 回程度の乗算と 1000 回程度の自乗算で復号化処理が可能となる．これならば，太郎は 1 秒もかからずにメッセージを復号することができ，花子とのデートの待ち合わせに遅れることもないであろう．

ここで，自乗算を取り入れた場合の RSA 暗号処理 LSI を実装し，消費電力の時間変化を測定すると，たとえば図 1 のようになる．RSA 復号化処理中の消費電力変化から，乗算の処理の部分(M)と自乗算(S)の処理の部分は，波形の形状により区別できてしまう．M→S→M→S→S→S→M…，と処理されていることがわかるが，実は，M→S のペアが鍵のビット “1” に対応し，S が “0” に対応している．つまり，電力波形からいとも簡単に秘密情報を読み取ることができるのである．計算の効率化によって，サイドチャネル攻撃に対する脆弱性が浮き彫りになったともいえる．

この電力解析によるサイドチャネル攻撃(電力解析攻撃)をベースに Kocher はさらに強力な攻撃法を考案し，1999 年に暗号に関する国際会議 CRYPTO において発表した[2]．以後，広く知られるようになった．

対策はあるのか

では，自乗算による計算の効率化と，サイドチャネル攻撃への耐性強化を同時に実現させるにはどうしたらよいだろうか？　対策法として，大きくは次の 2 つのアプローチに大別できる．1 つは，S と M の出現パターンをランダムにし，鍵との依存性をなくすことを狙うもので，もう 1 つは，鍵の値によらず，常に同じパターンとなるようにすることを目標とする．どちらのアプローチにおいても，これまでに数多くの対策法が提案されているが，ここでは，後者について説明する．

S と M の出現パターンを規則的にするアルゴリズムとして Montgomery Powering Ladder 法がある[3]．C^{205} を計算する際に図 2 に示すように 2 つの変数(2 本の縦のラインに相当)を準備し，計算を進めていくとちょうど梯子のような形になる．本アルゴリズムは別の目的で提案されたもの

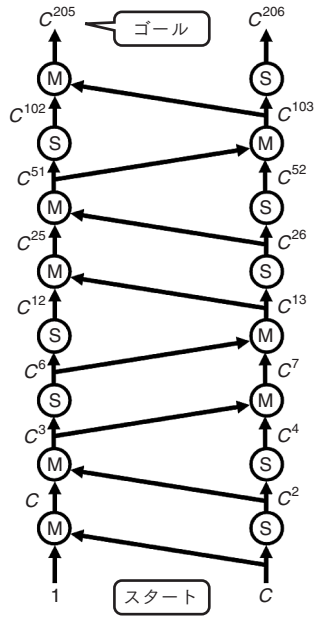

図2——Montgomery Powering Ladder 法．図は C^{205} を Montgomery Powering Ladder 法で計算した場合(205 は 2 進数で 11001101)．一般には，べき乗算 C^d において，d の最上位ビットから 1 ビットごとに剰余系における自乗算(S)と乗算(M)の両方の演算を実行する．ビット値が 1 の場合，左側に M，右に S の演算を置き，0 の場合はその逆とし，初期値(1 と C)から乗算と自乗算を進めていく．

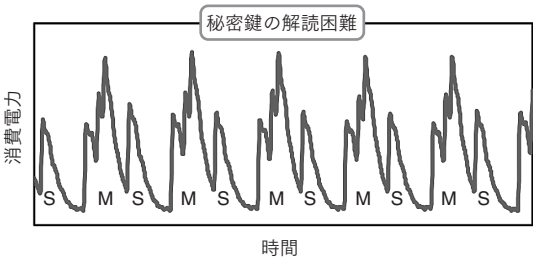

図 3 ――Montgomery Powering Ladder 法によるサイドチャネル攻撃の対策を施した RSA 暗号処理 LSI における消費電力の時間変化．鍵 1 ビットごとに剰余系における自乗算と乗算が実行されている．これにより図 2 に示したような消費電力波形の不規則な S と M の出現パターンはなくなり，秘密鍵の特定が困難となる．

だが，RSA 暗号処理のサイドチャネル攻撃の防御策として用いることもできる．ここではアルゴリズムの詳細な説明は省略する．

図 3 は Montgomery Powering Ladder 法 を 用いた場合の消費電力の時間変化である．この方法では，乗算と自乗算が鍵のビット値にかかわらず常に両方実行されるため，波形から秘密鍵を特定することは図 2 の場合と比べて困難である．

Montgomery Powering Ladder 法による対策では，自乗算を利用した計算に比べ，より多くの乗算が必要となる．したがって，図 1 に示した処理結果と比べて処理速度が低下している．処理速度を犠牲にして安全性の向上が実現できた，という見方もできる．

サイドチャネル解析をめぐる動向

現代暗号におけるサイドチャネル解析の研究は，先に述べた Kocher の研究に端を発する．その研究は米国 Cryptography Research 社で進められ，“サイドチャネル解析ビジネス” を広げようとしている．欧州では，NESSIE（New European Schemes for Signatures, Integrity, and Encryption: 2000〜2002 年）や ECRYPT（European Network of Excellence for Cryptology: 2004〜2008 年）といった欧州委員会の研究プロジェクトを通じて，さらに強力なサイドチャネル攻撃の手法やその対策法が活発に研究されてきた．今後も継続して研究されていくであろう．日本においても，CRYPTREC[(4)]（Cryptography Research and Evaluation Committees）の電力解析実験ワーキンググループを通じて，サイドチャネル攻撃に関する調査・検討が行われている．

今のところ，サイドチャネル攻撃による被害は，社会問題として報告されてはいない．しかしながら，この状況を楽観することなく，サイドチャネル解析による暗号実装の安全性に関する研究動向は注視する必要がある．

*　*

これまでの暗号の理論研究は，サイドチャネルからの情報漏れはないと仮定され，進められてきた．しかしながら先述の例に示したように，実装方法によっては，暗号システムから秘密情報が漏えいする危険性がある．サイドチャネルからの情報漏えいの防御を最終目的とし，暗号の実装研究者は，新たな脅威となる攻撃を想定し，それを未然に防ぐための対抗策を研究している．暗号の理論研究者は，サイドチャネルからの情報漏れを前提とした新たな暗号理論の構築を進めている．いずにせよ，サイドチャネル攻撃の耐性を強化するには処理性能の低下や製造コストの増加といった犠牲が生じてしまう．安全はタダでは手に入らないということだ．コストや性能といった利便性と攻撃に対する安全性のトレードオフを考える際の選択肢を増やし，人が情報とうまく付き合える社会の実現に向けて，最適な技術を提供できるように暗号研究を進めている．

文献および注

（1） R. L. Rivest et al.: Comm. ACM, **21**, 120（1978）
（2） P. Kocher: in ‘Advances in Cryptology――Proc. of CRYPTO ’96’, N. Koblitz ed., Springer-Verlag（1999）pp. 104〜113
（3） P. Montgomery: Math. Computation, **48**, 243（1987）
（4） 総務省および経済産業省が共同で開催する「暗号技術検討会」と，情報通信研究機構（NICT）及び情報処理推進機構（IPA）が共同で開催する「暗号技術監視委員会」，「暗号モジュール委員会」で構成されるプロジェクト．電子政府推奨暗号の安全性を評価・監視し，暗号モジュール評価基準等の策定を検討する．