第1章

あなたが設計したLSIから秘密情報が漏れてます

―― 暗号回路のトレンドはアルゴリズムの標準化から実装の安全性評価へ

佐藤 証

LSIからのデータの読み出しは，I/Oポートを介してのみ行われるわけではない．LSIが演算を行っているときに発する電磁波や熱，音などを測定，解析して，データを読み取ることもできる（いわゆる，サイドチャネル攻撃）．例えば，暗号回路部の処理を解析して秘密かぎを割り出されると，企業秘密や個人情報が読み取られてしまう可能性がある．ここでは，暗号技術の歴史を交えながら，サイドチャネル攻撃についての業界の動向を紹介する．（編集部）

非接触ICカードやRFIDタグといった小型デバイスを用いた無線通信技術が，身近な生活の中にどんどん広がっています．非接触型のICカード方式に対応した自動改札や携帯電話が増えていますし，2005年日本国際博覧会（通称「愛・地球博」）の入場券にRFIDタグが使われたのも記憶に新しいと思います．キャッシュ・カードやクレジット・カードについても，偽造対策のため，接触型ICカードへの移行が進んでいます（右掲のコラム「ICカードのセキュリティ」を参照）．以前は，磁気ストライプに数十バイトのデータが書き込まれていただけでした．

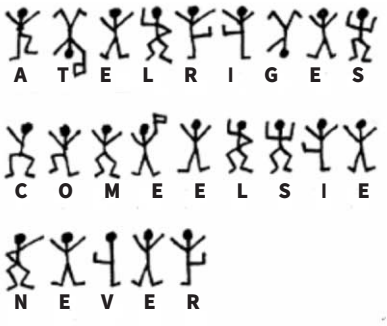

図1　シャーロック・ホームズの踊る人形
文字と人形が1対1に対応している．ホームズは人形の出現頻度の偏りを利用して解読に成功した．

● I/Oピンからでなくてもチップの情報は読みとれる

RFIDや非接触型ICカードの情報のやり取りが電波を通じて行われるように，LSIチップのデータ入出力はI/Oポートの電流・電圧変化を用いて行われます．しかしこれ以外にも，チップ全体の消費電力，配線からの電磁放射，そして熱，音，光など，さまざまな経路を通じて，チップ内部の情報は外部に漏れているのです．このような本来のデータの入出力経路（チャネル）ではないものを利用して，機密情報，とくに暗号化の秘密かぎなどを取り出そうとするのが「サイドチャネル攻撃」です．

2000年前後は暗号アルゴリズムの標準化がセキュリティ業界の大きな話題でした．ここ数年は，暗号モジュールの実装評価についての標準化活動が活発で，その中でもサイドチャネル攻撃とその防御法に関する研究が注目されています．まずは，このような暗号業界の流れを見ていきましょう．

1 暗号アルゴリズムの歴史と標準化

人類が文字を発明して以来，数限りない暗号が考案されています．シャーロック・ホームズの「踊る人形」[1]は有名ですし，古代エジプト文字「ヒエログリフ」も考古学者や言語学者以外の人たちにはある種の暗号といえるでしょう（図1）．ですが，踊る人形はちょっとした規則さえわかればだれでも読み書きできますし，ヒエログリフも当時の人にとっては暗号ではありませんでした．

● 現代暗号は「アルゴリズム」と「かぎ」が分離

これらに対して，現代暗号と呼ばれるものは次の2点が大きく異なります．

◉COLUMN◉ ICカードのセキュリティ

接触型ICカードであれば，どれが通信するべき端末なのかがその場でわかります．一方，非接触型ICカードの場合，だれかが盗み聞きしているかもしれません．RFIDは数十～数百ビットの認識番号（ID）を周りに伝えるだけなので，それほど問題にはなりませんが，かりにキャッシュ・カードやクレジット・カードだったらどうでしょう．影で第三者が成りすましの通信を行っているかもしれないという不安を持つと思います．ですが，キャッシュ・カードやクレジット・カードに用いるような高機能のICカードでは，機密データの暗号化と通信相手の正当性の検証がしっかりと行われているので，接触・非接触にかかわらずそのような心配はありません．

以前，テレビの報道番組でICカード情報をコートの上から読み取る「非接触スキミング」という光景を目にしたことがあります．ですが，初めに相手を確認し，また自分がだれかを知らせなければ通信は始められないので，そのようなID情報は読めてあたりまえなのです．このことと，セキュリティ機能を持たず，すべてのデータが簡単にコピーできる磁気カードのスキミングを同等に扱うのは誤りです．

ICカードのデータは，暗号アルゴリズムだけで守られているわけではありません．物理的な攻撃への対策として，多くのカードは電圧，周波数，光，温度などに対するさまざまなセンサを搭載しています．また，こうしたICカードのカタログには，“simple power analysis（SPA）”，“differential power analysis（DPA）”，“differential fault analysis（DFA）”，“electromagnetic analysis（EMA）”など，不当な方法による情報漏えい（いわゆるサイドチャネル攻撃）の対策についての記載があります．

- アルゴリズムとかぎが分かれている
- アルゴリズムを公開できる

かぎそのものがアルゴリズムの一部となってしまっている昔の暗号は，すべてを秘密にする必要がありました．現代暗号では，アルゴリズムとかぎを分けたことで，公の場でアルゴリズムに関する議論が可能となりました（ただし，特殊用途ではアルゴリズムが公開されていないものもある）．

本誌2004年12月号の表紙を飾ったEnigma（エニグマ）暗号機をご存じの方も少なくないと思います（**写真1**）．ドイツ軍が第2次世界大戦中に使用した機械式暗号機の傑作で，現在でもオークションで100万～300万円ほどの値段で取り引きされています．その原理は，キーを叩くたびに，入出力の配線がランダムにつながれた複数のロータが回転し，文字の変換規則を次々に変えていくというものです（p.102のコラム「Enigma暗号機」を参照）．

Enigma暗号機では，ロータの種類や順番，初期位置などが秘密かぎとなりますが，暗号機の構造（つまりアルゴリズムそのもの）も解析に非常に重要な手がかりを与えてしまいます．この点で，現代暗号とはいえません．

写真1
Enigma暗号機

提供：©Science & Society Picture Library

● 共通かぎ暗号のDESと公開かぎ暗号のRSA

Alan Turing（1912年～1954年）率いる英国の暗号解読チームは，さまざまな手がかりと数学・言語学などの知識を駆使して，Enigmaをはじめとするドイツ軍の暗号を次々と破っていました．また，彼らは暗号解読のために世界初のコンピュータ「Colossus（コロッサス）」を製作しています．

第2次世界大戦後しばらくは，軍事用の武器に相当するとして，暗号の使用に強い制限が課せられていました．それからしだいに規制が緩和され，今では業務から日常生活まで，用途に応じてさまざまな暗号アルゴリズムが利用されています．その中で，とくに有名なアルゴリズムとして，DES（Data Encryption Standard）とRSAが挙げられます．DESは，1977年に米国の連邦標準として制定され，現在，暗号製品の8割以上に実装されていると言われています．また，RSAはDESと同じ年に米国Massachusetts Institute of Technology（MIT）のRivest，Shamir，Adlemanらによって開発されました．RSAは彼らの頭文字を取って名づけられました．この3人はその功績が認められ，2002年にコンピュータ・サイエンスのノーベル賞と称されるチュー