奥富秀俊

Hidetoshi Okutomi

単純な規則から複雑な現象を生むカオス現象、これを暗号に使えないか

会社に就職したあとも、大学時代に思いついた暗号のアイデアを忘れることができなかった。そのアイデアは未踏ソフトウェア創造事業のプロジェクトとして採択され、設計と試作が始まった。試作した暗号システムは、長い時間と紆余屈折のすえ、会社で事業化されることになった。

大学生だった奥富秀俊氏（東芝情報システム株式会社勤務）は、授業にはろくに出なかったが、カオス現象という不思議な数理にのめりこんだ。もともと、ノイズがのったバリバリのヘビーメタル系音楽が好きだった奥富氏には、カオス現象がきわめて単純な規則から複雑なノイズを作りだせることがおもしろかったのだ。これを何かに利用できないか、情報にノイズをのせたら、暗号に応用できるのではないか？

1997年、大学を卒業した奥富氏は東芝情報システムに入社した。物理を専攻していたことから半導体部門に配属され、DRAMに使われているアナログ回路の設計に携わることになった。だが、もともとやりたかったカオス現象を応用した暗号のことが頭から離れなかった。

世の中では、ちょうどインターネットが急激に普及していた時期だ。セキュリティが重要になっていくのは明らかだ。カオス現象を使えば、処理時間の少ない簡単なロジックで、これまでよりも解読に時間がかかる暗号方式ができる。そこで、社内のあちこちでさかんにアイデアを話して歩いた。しかし、実績のない入社2年目の社員が職場の事業と結びつかない話をしても、なかなか耳を傾けてもらえるものではない。おまけに、奥富氏が話す暗号は、聞いたことも見たこともないものだ。雲をつかむような話に聞こえただろう。

進展のないまま鬱々として1年半ほど経過したころに、新聞で未踏ソフトウェア創造事業が開始されることを知り、応募することにした。会社でのそれまでの仕事とは関連がなかったが、採択が決まると、さいわいにも会社の理解を得られ、気持ちよく開発を進めることができた。会社の柔軟な対応がなければ、会社にはいられずに辞めることになっていただろう。

カオス現象と暗号

奥富氏が作ろうとしたのは、ストリーム方式の共通鍵暗号だ。共通鍵暗号は、同じ鍵を使って暗号化／復号する。このときブロック暗号方式では、512ビット、あるいは1024ビットごとというようにデータを一定サイズのブロックに分割して暗号化する。一方ストリーム暗号方式では、先頭から順に1ビットずつ、あるいは1バイトずつというようにデータを少量ずつ暗号化する。このような特徴と、暗号化が少量ずつで早く計算できることから、ストリーム暗号は無線ネットワークや携帯電話などの時間的な制約

Hidetoshi Okutomi

がある通信用途に適しているといわれる。

一般に、暗号化に使用する鍵の長さを大きく

すれば暗号解読に時間がかかる。攻撃に対する耐性は強まるが、暗号化と復号の計算に時間がかかり、CPUへの負荷が高くなる。しかし、カオス現象を応用した暗号方式は、簡単な規則から複雑な状態を多数作りだせるという数理特性から、一般の既存の方式と同程度の処理時間で非常に長い鍵を利用できる。一般的な共通鍵暗号の鍵の長さは128～256ビット程度だが、カオス暗号では16384ビット以上の鍵が利用できる。つまり、鍵長が長くても軽量で速いのが特色だ。

2000年度と翌2001年度の2年間、奥富氏は暗号システムの設計と試作に没頭した。開発する暗号システムは、単なる新しい暗号方式のひとつだけではなく認証にも使える。鍵がつくりだすカオスの乱雑波形によって、鍵の所有者を識別できるからだ。そこで、ゆくゆくは認証基盤に応用できるようにしたかった。

また、カオス現象は自然現象なので、暗号ロジックの実装には浮動小数点演算の使用が当たり前だったが、あえて整数演算とビット演算で実装した。組み込み機器への応用を考えてハードウェア化しやすくしたのだが、ここには半導体部門にいた経験が活きた。

プロジェクトの成果を事業化する

2年間のプロジェクトで、カオス現象を応用した暗号方式のベースは完成したが、実用的なモジュールにするためにはなお時間が必要だった。設計した暗号システムはこのまま埋もれてしまうのだろうか。しかし、運良く会社で開発を続けられることになった。「スーパークリエータ」として認められたこともよい方向に働いた。

新しい暗号の実用化には理論の正当性を立証し、専門家に納得してもらわなければならない。それが奥富氏の次の仕事になった。既存の暗号理論には30年をかけて検証技法が蓄積されているが、まったく異なる数理に基づいた奥富氏の暗号には直接当てはめることができない。

ストリーム暗号の汎用的な検証指標は、生成される乱数の品質だ。偏りがなく、理論上の確立モデルに適合していることがよいとされる。既存の検証ツールに誤りと思われる点が見つかるなど、評価方法に難しい問題はあるが、これまでの検証では乱数の品質はよい。

1年を経て、暗号システムはTritiumという名前で製品化され、SIと組み込み機器を組み合わせた事業が始まった。個人情報保護法の施行でセキュリティ技術に対する認識が高まったことと、組み込み機器がネットワークにつながれることが多くなったからだ。現在は、暗号のコア技術をライブラリ化したソフトウェア開発キットやハードウェアIPを販売する一方、監視カメラやデジタルレコーダなどの組み込み機器への応用が始まった。大きなデータでも暗号化・復号のスピードが速いので、サイズの大きい動画やファイルシステムなどに強みがある。

「真にやりたいことを追求し続けたら、運を呼び込むことができました」と奥富氏は語った。

DATA

東芝情報システム株式会社技術企画部基盤技術開発グループ勤務。数理パズルが趣味で、休日はもっぱら数値計算シミュレーションで遊ぶ。13歳ではじめて触れて以来、コンピュータとは切っても切れない縁になった。