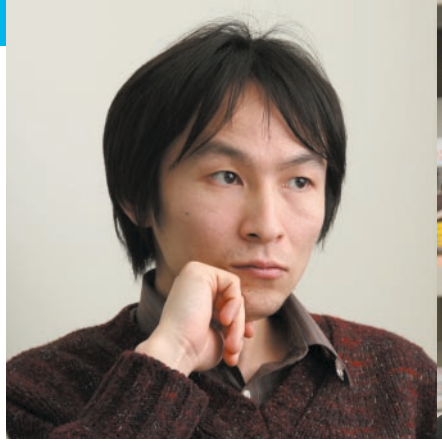


渡辺秀行/光成滋生

Hideyuki Watanabe / Shigeo Mitsunari

世界ではじめて、ストリーム暗号の解読に成功

数学理論を理解し、アルゴリズムを性能の高いプログラムとして実装できるだけの才能をもつ開発者はまれである。未踏ソフトウェア創造事業で放送コンテンツ配信向きの暗号システムを開発した渡辺氏と光成氏は、ふたたびコンビを組み、ストリーム暗号のToyocryptの解読に成功した。

大学で数学を専攻していた光成滋生氏（ユーテン・ネットワークス株式会社技術部シニアエンジニア）は、放送コンテンツの配信に使えそうな、それまでにない方式の暗号を考えていた。光成氏は、「午後のこ〜だ」というMP3エンコーダの作者としても知られている。考えついた暗号システムのあらましは、次のようなものである。

鍵の不正利用を防ぐ暗号方式をつくる

これまでの有料プログラムの配布などでは、配布物を暗号化し、購買した利用者に暗号鍵を渡して使えるようにすることがある。しかし、その鍵がどこかのWebページに置かれて不特定多数の人に渡れば、広範囲に不正利用されることになるだろう。

購買者それぞれに鍵を用意し、購買者のそれぞれにコンテンツを暗号化すれば、鍵が他の人の手に渡っても出所を突き止めやすくなり、不正利用を抑制できる。しかし、配布システムの負担が重い方法なので、今後重要になっていく動画の放送などにはとうてい耐えられない。

光成氏が考えた方式は、あらかじめ名前やメールアドレス、クレジット番号などを鍵に埋め込んで利用者に配布し、暗号化した共通のコンテンツを配信するものだ。最初に利用者用の鍵を配布すれば、配信コンテンツはひとつですむので配信の負担は小さくなる。また、鍵に個人情報が埋め込まれるので、他人に教えるのは躊躇されるし、不正利用されれば鍵の出所を追跡可能だ。この方式は海外でも注目され、昨年末には改善した手法も提案されている。

光成氏はこのアイデアを、大学院の同級生だった渡辺秀行氏（株式会社アイビス専務取締役副社長）に話した。渡辺氏とは、日ごろからアルゴリズムやプログラミングなどでよく話をする間柄だ。その後、未踏ソフトウェア創造事業の制度を知って共同で応募することになると、渡辺氏が書類の作成を引き受けた。

世界を見渡しても、まだ同じ暗号方式は発表されていなかった。アイデアはあっても実装には時間がかかるので、光成氏は動作するものを作るには至らないでいたが、プロジェクトのお金をもらって仕事としてやるようになれば、自分でお尻をたたくことになると考えた。

プロジェクトでは、要となる数学的なモジュール（ペアリングの演算部）も、それまでの実装を超える速度にしたかった。いちばんの基礎となるのは、数百バイトレベルの多倍長演算の

Hideyuki Watanabe

Shigeo Mitsunari

部分である。演算アルゴリズムの論文を読み、独自のアイデアを織り込んでいった結果、実装は首尾よく世界最速を記録することができた。

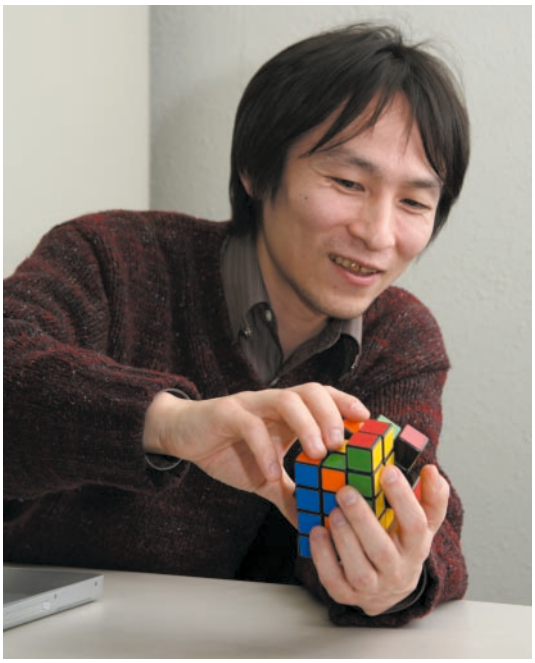
光成氏らが2年間のプロジェクトを終えて、次の応用を考えているところへ、新たな話が降ってきた。

暗号解読プログラムをつくりませんか？

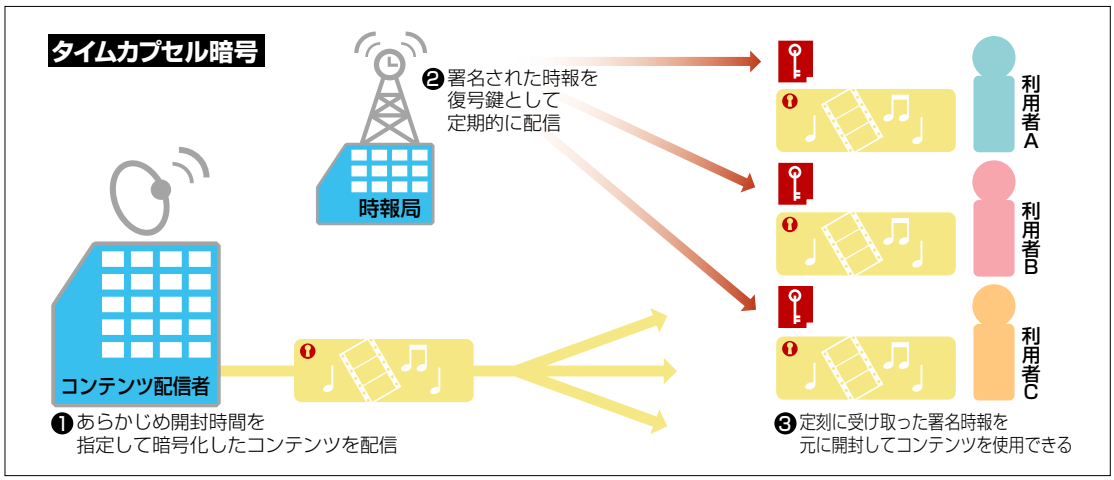
研究会に出席していた光成氏に、杉田誠氏（情報処理推進機構セキュリティーセンター研究員）が「Toyocryptの暗号解読プログラムをつくりませんか？」と声をかけたのは、それからしばらくしてからのことである。

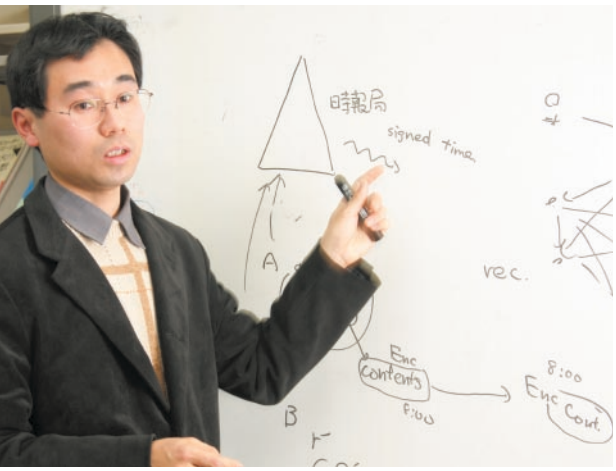
Toyocryptは、国産のストリーム型暗号方式である。ストリーム暗号は、現在よく使われているブロック暗号と比べて、計算に時間がかからず軽量で、またデータの先頭から1ビットあるいは1バイトずつ暗号化／復号するので伝送誤りによる影響が少なく、無線ネットワークや携帯電話などに向くと期待されている。

暗号と暗号解読は、「盾」と「矛」の関係にある切り離すことのできない対の技術である。暗号解読による攻撃実証は、暗号を安心して使うためにはかかせない。歴史の長いブロック暗号については研究が進み、弱い暗号は淘汰され、強い暗号のみが生き残っているが、ストリーム暗号はまだ解読実証の実績に乏しかった。



Toyocrypt自身の暗号アルゴリズムについては、理論的には解読が可能だと学会で発表されていたが、実証した例はなかった。いや、理論の研究者の多くはプログラミングを得意としていない。高度な数学を理解できるソフトウェア技術者もなかなかいない状況で、解読の実証はあまり進んでいなかったのだ。Toyocryptは、実用ではあまり使われていないが、解読できることを実証すれば、今後開発する暗号方式をその解読方法に耐えるように改良していける。解読技術はその安全性の評価に役立つ。光成氏ら





なら、きっと性能のよいプログラムを開発できる。杉田氏の打診にはそんな背景があったのだ。

解読プログラムは、数学への理解とプログラミング手腕がなければできない

Toyocryptの解読では、変数が多数ある連立方程式を効率よく解ける、グレブナー基底という数学を使う。声をかけられた光成氏は、この機会にグレブナー基底を勉強しようと思い、渡辺氏といっしょに引き受けることにした。

プロジェクトでは、杉田氏がToyocrypt解読プログラムを試験実装したあと、光成氏と渡辺氏が一からつくり変えて高速化した。光成氏も渡辺氏も、始めてから数カ月は本を読むことに時間を割いた。暗号解読プログラムは、アルゴリズムを小分けにした計算プログラムの部品をつくって組み立てていく。まず小さいサブルーチンをつくり、組み合わせて簡単な問題を解かせ、それを少しずつ複雑にしていく。はじめは、小規模な問題を解かせても、メモリの使用量がどんどん上がってウンともスンともいわない。修正していくとすんなり解けることもあるのだが、プログラム部品のどれかに間違いがあると、データを与えてもいっこうに結果が出てこない。間違いなのか、時間がかかっても仕方がないものなのかの判断が難しかった。

プログラムの性能は、最初の設計と実装上の細かいチューニングがものを言う。アルゴリズムの試験実装として作られた当初のプログラムは、用意した鍵をIPAのグリッドシステム（Opteronプロセッサを積んだマシン64台/128CPU）で27分かけて解読したが、渡辺氏が最後に完成したときには、ノートPCでの解読時間が30秒程度にまで短縮された。

Toyocryptの解読が発表されると、大きな話題になった。その成果から、両氏は2005年情報化月間推進会議議長表彰を受けている。完成した暗号解析用グレブナー基底探索プログラムIPA-SMWは、IPAから公開されている。

いまはタイムカプセル暗号が面白い

光成氏らの関心は現在、タイムカプセル暗号にある。未踏ソフトウェア創造事業で開発した技術を応用し、暗号化したコンテンツをある時刻になったら開封できるようにするものだ。たとえば、事前に配信しておいたプレスリリースを決まった時刻にいっせいに見られるようにしたり、新作の映画を同時に封切ることができる。前もってコンテンツを配信しておけるので、サーバーにアクセスが集中する心配がない。

コンテンツ事業者は、開封時刻を指定してコンテンツを暗号化し、あらかじめ配信しておく。信頼できる時報局は署名された時報を定期的に送信する。この暗号方式は、署名された時刻そのものが復号鍵となっているため、利用者は定刻にその署名された時報を元にコンテンツを開封して使用できるようになる。

最近海外でも、同じような理論の技術でさかんに研究されるようになってきた。時流にも乗っているのではないか。光成氏はいろいろな利用方法が考えられそうだと期待をかけている。

DATA

渡辺秀行：株式会社アイビス専務取締役副社長
http://www.ibis.ne.jp/

光成滋生：ユーテン・ネットワークス株式会社技術部シニアエンジニア
http://homepage1.nifty.com/herumi/
（タイムカプセル暗号：http://homepage1.nifty.com/herumi/mtt/tc.html）