Next Tech 2050

暗号通信「真の乱数」で安全

玉川大、光ファイバー機器で低コスト

50年に小型化、個人で利用も

情報の漏洩や盗聴を防ぐ暗号通信で、第三者による解読をさらに難しくして安全性を高める手法を玉川大学が開発した。暗号の作製には乱数を駆使するが、数字の配列に全く規則性がない「真の乱数」を光ファイバー網の構築に使うような機器で素早く大量に作り出す。真の乱数であれば、万が一漏洩しても見破られる可能性はほぼなくなる。軍事や金融など秘匿性の高い分野への応用を後押しする。

金融情報や個人のプライバシーなどの機密情報を誰かに送りたい時、3つのステップをふむのが一般的だ。まずは送信先が本当に情報をやりとりしたい相手かどうか確かめる認証、次に暗号の解読に必要な鍵の交換だ。最後に送りたい情報に鍵をかけて暗号文を送信する。受け取った相手は鍵を使って暗号文を元の文に復元する。

「全てのステップで『真の乱数』を使うことで安全性を高められる」と玉川大学の谷沢健教授はこう強調する。認証や鍵の生成、鍵の交換で乱数を利用している。

現状の暗号通信では乱数は数学的な手法で作製している。疑似乱数と呼ばれ、解読される可能性はゼロではない。

一方、量子力学の原理に基づいて乱数を作り出せば、予測不可能で規則性がない真の乱数を作り出せる。

そこで玉川大学量子情報科学研究所が着目したのが、レーザー光で乱数を発生させる手法だ。2010年に海外の研究グループが提唱したもので、谷沢教授らが実証を重ねてきた。

実験に使った機器は光ファイバー網で使われているものだ。谷沢教授は「安価で高速、高品質な『真の乱数』ができた」と期待する。

具体的にはまずビームスプリッタという部品でレーザー光のエネルギーを半分に分散した上でバランス光検出器にかける。分散した光のエネルギーをそれぞれ電気信号に変換する。2つの電気信号の差をとると、真空揺らぎという物理現象が起きてノイズが発生する。

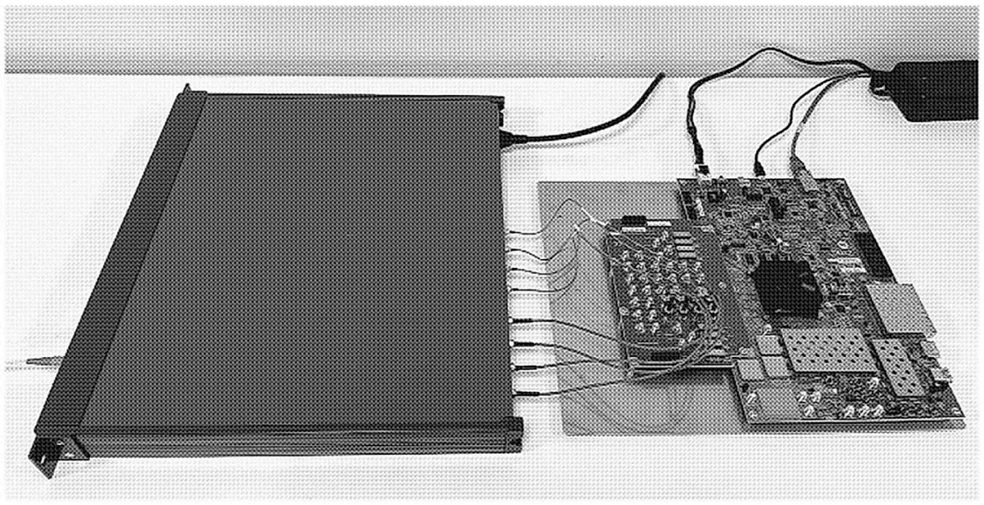
このノイズをアナログデジタル変換器でデジタル信号に置き換える。0と1に変換して真の乱数を生成する。

より早く大量に乱数を生成する改良も手掛けている。谷沢教授らはビームスプリッタのかわりに、光のエネルギーを8つにわける装置を使った。電気信号に変換するバランス光検出器を4つ並列に並べて、それぞれで電気信号の差をとる。アナログデジタル変換器で真の乱数を同時に4つ生成した。

真の乱数を生成する速度は現時点で世界最高という。今後、さらなる高速化や光集積回路技術による小型化を目指す方針だ。

50年には真の乱数を生成する装置の普及を目指している。一連の成果は米国で3月に開催された国際的な学会で発表した。

計算能力が飛躍的に向上するとされる量子コンピューターの登場によって、現在の暗号通信が盗聴される懸念が出ている。量子力学を駆使した乱数発生器の実用化は急がれている。



玉川大学が開発したレーザー光を使って「真の乱数」を生成する装置（同大学提供）

乱数発生器を巡る動きと将来展望

2000年代初頭	単一光子を用いて乱数を発生させる仕組みを考案
10年ごろ	レーザー光などを使って乱数を発生させる技術が提案・実証
23年	玉川大学がレーザー光を用いた手法で世界最高の速度で生成に成功
30~35年	インターネット上で「真の乱数」が入手できるサービスが開始
50年	「真の乱数」を発生する装置が身近に

記者の目

量子力学の原理に基づいて乱数を発生させる発生器が最初に提案されたのは2000年代初頭にさかのぼる。一つの光子をビームスプリッタに入れて、どちらの方向に光子が出るかで0と1からなる乱数を発生させる。

今回の成果のように強い光を入れて乱数をつくる量子乱数発生器は10年ごろに提唱された。実証が進み、ここ10年ほどで研究が加速的に進んでいる。

情報通信の基盤技術としても重要になる。量子力学の応用では量子コンピューターが有名だが、そちらよりも実際の生活に役立つ可能性がある。

実際、谷沢教授は30~35年には量子乱数発生器から生成した「真の乱数」がサービスとして配布され、インターネット上で個人が入手できるようになると予測している。

50年には回路の集積化も進み、発生器の小型化も進む。谷沢教授らは目標の達成に向けて開発中だ。

安価で大量に質の高い「真の乱数」が簡単につくれるようになれば、セキュリティーや数値シミュレーション、ゲームなどへの活用が期待できる。思いがけないような新たなアプリやサービスの創出につながりそうだ。

（藤井寛子）

掲載日 2023年04月07日 日経産業新聞 007ページ