情報通信研究機構

NICT 先端研究 (198)

多変数公開鍵暗号 安全性・処理効率を両立

サイバーセキュリティ研究所・セキュリティ基盤研究室 研究員 伊藤 琢真

17年都立大院修士課程修了、18年8月にNICT入所。暗号、プライバシー保護技術、暗号技術の安全性評価と実装に関する研究開発に従事。

近年、世界的に量子コンピューターの開発が活発に進められており、従来のコンピューターでは計算しえないレベルの計算が可能になることで、量子コンピューターによって効率よく解読されてしまうことが懸念されている。そのため、量子コンピューターを利用しても解読が困難な耐量子計算機暗号と呼ばれる暗号技術の研究開発と標準化が、特に米国を中心に進められている。

耐量子計算機暗号の代表的な候補として、連立方程式を利用した暗号である多変数公開鍵暗号が挙げられる。多変数公開鍵暗号は使用する連立方程式が解かれると解読されてしまう。連立方程式の難しさは変数の個数で決まる。具体的には変数の個数が多いほど難しい問題となり、暗号の安全性は高まる。しかし変数の個数が多いほど暗号処理に必要な時間も増加してしまう。

したがって、安全性と暗号処理の効率のバランスがとれた変数の個数、すなわち適切な暗号パラメーターの算出が必要不可欠である。そのため、多変数公開鍵暗号の解読コンテストにおいて多変数公開鍵暗号に利用されるさまざまなタイプの連立方程式が提示されており、その暗号の安全な暗号パラメーターの検討が行われている。

情報通信研究機構（NICT）は東京都立大学との共同研究で、解読コンテストの一部の問題を効率よく解くためのアルゴリズムを開発し、解読に10年はかかると予想される問題を76日で解くことに成功した。本成果は多変数公開鍵暗号の暗号パラメーターの新たな選定指標として利用される。さらに、この記録は世界記録として認定されており、現在もこの記録は破られていない。

NICTでは今後も多変数公開鍵暗号だけではなく、さまざまな耐量子計算機暗号の安全性評価の研究を実施し、耐量子計算機暗号の安全な運用に貢献していく。

（火曜日に掲載）

2変数の連立方程式の例

$$\begin{cases} 3x^2+4xy+6y^2-6x+4y=1 \\ 5x^2+8xy+7y^2-5x+3y=4 \\ 9x^2+5xy-8y^2-4x+2y=3 \end{cases}$$

$$x=3, y=-2$$

▲2変数の連立方程式の例（NICT提供）