PRESS RELEASE

岡山大学
OKAYAMA UNIVERSITY

岡山大学記者クラブ、文部科学記者会、科学記者会　御中

令和 4 年 11 月 30 日
岡　山　大　学

報道解禁
テレビ、ラジオ、インターネット：令和 4 年 11 月 30 日（水）午後 2 時
新聞:令和 4 年 11 月 30 日（水）夕刊より

世界記録更新！　IoT 時代の実用暗号の解読で、2 進数 116 桁の位数の楕円ペアリング暗号曲線に対する攻撃に成功

◆発表のポイント

・実用暗号の一つである楕円ペアリング暗号の楕円曲線に対する攻撃成功記録を更新しました。
・1 つの実験で複数回の攻撃成功を達成しました。
・攻撃手法の効率が徐々に悪化する様子を詳細に記録することにも成功しました。

ICT の推進に伴い、日常的に機微情報を通信でやり取りする昨今、機密情報保護のための要は暗号技術です。これまでも楕円曲線暗号は大規模な解読実験によって安全性の厳密な評価がされてきました。岡山大学学術研究院自然科学学域の野上保之教授の研究チームは楕円ペアリング暗号について、約 1000CPU コアの PC クラスタを用いた大規模な解読実験を実施し、2 進数で 116 桁、つまり 10 進数で 35 桁の大きさを持つペアリング曲線上の楕円離散対数問題の解読に成功しました。

本記録は同チームが中心となって実施した 2017 年の 2 進数で 114 桁の問題の解読記録を約 2 倍(難しさの観点で)更新する快挙です。また、通常、1 回の実験で 1 つの攻撃成功で終えるところを複数回の攻撃をする形式に変更し、現時点で 6 回の攻撃成功に至っており、これも過去に例がない成果です。今後、取得データの分析を進めて学会発表にて詳細を報告する予定です。また、本成果は高機能暗号への攻撃手法の改善手法の考案にも寄与するため、実用暗号の安全性の正確な評価に関する新たな知見を提供するものです。

本実験は国立研究開発法人情報通信研究機構(NICT)の北陸 StarBED 技術センターの設備を活用することで達成されました。当研究グループではテストベッドである StarBED システムを疎結合並列・分散**スーパーコンピュータ**として仕立てることで、記録更新を達成しました。攻撃実験は足掛け 3 年となりますが、丹念な保守作業をいただくことで安定した運用をしていただきました。常時フルパワーで計算しておりましたので「野上先生にお貸ししているコンピュータの後ろ側を通ると明らかに熱いです」と話題にされたことがあります。

野上教授

■発表内容

＜現状＞

機密情報保護のための要である暗号技術の中で楕円曲線暗号は現用の実用システムで中心的な役割を担っています。悪意ある攻撃者はその解読を目標とするため、セキュリティ研究者は攻撃者より優れた手法での模擬攻撃実験を実施し、暗号の安全性の確認をすることが重要です。当研究グループは自らが持つ世界記録を更新する攻撃成功を達成しました。しばらく実験を継続し、さらに追加の攻撃成功データを収集しつつ、詳細分析を加えたうえで高機能暗号の安全性評価に関する新たな知見の学会発表を行う予定です。

＜研究成果の内容＞

当グループは IoT 機器での実装が容易とされる楕円ペアリング暗号に着目し、その中核の問題となる楕円離散対数問題の解読実験を NICT の StarBED システム上に構築した約 1000CPU コアからなるコンピュータを用いて実行しています。2019 年の中旬に実験を開始し、2 進数で 116 桁、つまり 10 進数で 35 桁の大きさを持つペアリング曲線上の楕円離散対数問題の解読実験に取り組んでおり、2022 年 2 月 2 日の初回の攻撃成功を皮切りに、現在までに 6 回の攻撃成功を達成しています。この規模の既存研究では、通常、1 回の攻撃成功をもって実験停止するところ、当グループでは攻撃実験を継続し、複数回の攻撃成功を達成しています。これにより、攻撃に必要な計算量の評価が精密になり、暗号の安全性の評価の精度が向上します。

また、2017 年に当グループが中心となって報告した、2 進数で 114 桁の問題への攻撃実験の最中に観測された、攻撃効率の悪化現象について、今回の実験システムでは詳細データを取得することに成功しており、今後の攻撃手法の効率改善に関する知見も得ることができております。

＜社会的な意義＞

楕円ペアリング暗号は現在の実運用システムで主役となっており、多くの研究者からの情報提供により、相当に安全とされる諸元にて運用されていますが、その諸元の新たな根拠の一つを与える成果です。端的には、現在での運用状況で全く心配がないことを追認できたことは間違いありません。一方で、将来の攻撃手法の改善も模索することで、将来における安全な暗号の運用の知見を継続的に与えるための役に立てるよう、今後も努力を継続する決意です。

■研究資金

本研究は科学研究費補助金の支援を一部受けて実施しました（挑戦的研究(開拓)、19H05579）

暗号攻撃実験と安全性評価

IoT 時代では楕円曲線暗号が主役となっている

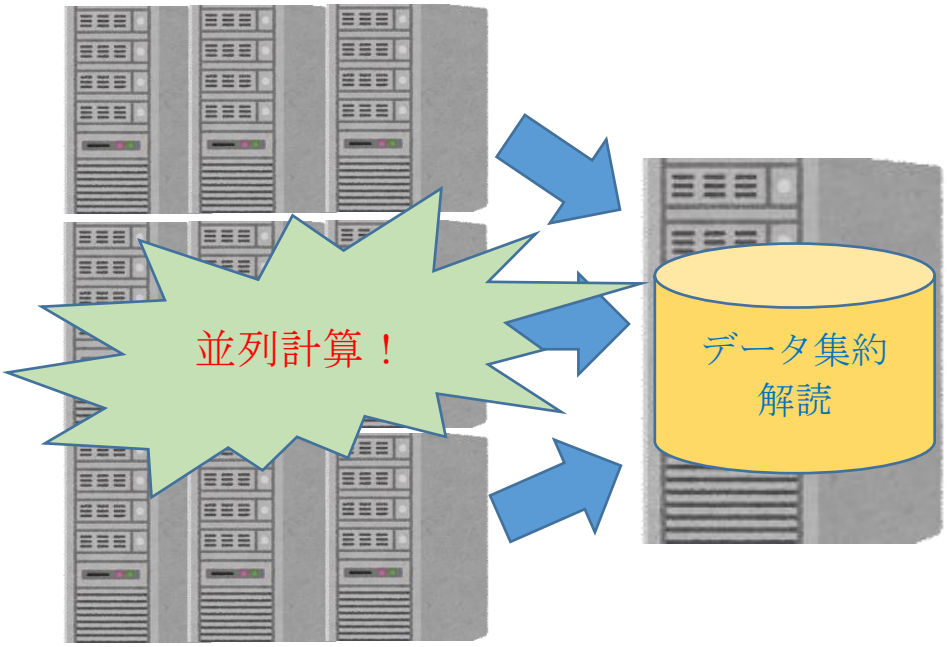
最高の技術で解読できるものは危険

最高の技術で解読できないのは安全だろう

楕円離散対数問題への攻撃で評価する

2017 年に 114bit **楕円離散対数**問題の解読(1 回)に成功
(当時世界記録)

記録更新となる約 2 倍難しい 116bit 楕円離散対数問題の解読に**複数回**成功!



Japan. Committed to the SDGs
岡山大学 OKAYAMA UNIVERSITY
SUSTAINABLE DEVELOPMENT GOALS
岡山大学は持続可能な開発目標（SDGs）を支援しています。

9 産業と技術革新の基盤をつくろう

＜お問い合わせ＞
岡山大学　学術研究院自然科学学域
教授　野上　保之
（電話番号）086-251-8127（FAX）086-251-8255