名古屋大学

Empowered by Innovation
NEC

プレスリリース

名古屋大学
日本電気株式会社
平成 24 年 8 月 17 日

国際標準暗号 GCM の新たな安全性評価結果

---従来の安全性保証に欠陥が発見されるも、修復に成功---

名古屋大学大学院工学研究科計算理工学専攻の岩田哲准教授，同専攻の大橋佳祐大学院生，日本電気株式会社の峯松一彦主任研究員のグループは，国際標準の認証暗号化方式である GCM（注 1）の安全性保証に欠陥があることを突き止めました．さらに，突き止めた欠陥を取り除き，GCM の安全性保証を修復することに成功しました．

GCM は高い計算効率を有しており，またその安全性が数学的に保証されていると考えられてきたことから多くの標準化プロセスで採用され，政府間・民間で広範に利用されています．しかし，その保証の理論的裏付けは無効であったことが明らかになりました．さらに，突き止めた欠陥を取り除き，GCM の仕様を変更することなくその安全性を数学的に保証することに成功しました．これにより，GCM の内部で用いるブロック暗号（注 2）が安全であれば，現実的な計算量の攻撃方法に対して，その成功確率はある限界値以上にはならないことが示されました．これまで信じられてきた数値よりも大きな限界値のためリスクが増加するものの，この結果は，適切に実装されていれば実用上は GCM を使用することに安全性の問題がないことを示しています．

これらの研究成果を，米国カリフォルニア大学サンタバーバラ校にて平成 24 年 8 月 19 日から 23 日（太平洋標準時）に開催される国際会議 CRYPTO 2012 にて発表します．

【用語】

(注 1) GCM : Galois/Counter Mode，ガロア／カウンタ・モード．データの暗号化と認証を同時に行うための認証暗号化方式と呼ばれる暗号技術．

(注 2) ブロック暗号：データブロックを暗号化するための暗号要素技術．GCM では AES などが用いられる．

国際標準暗号 GCM の新たな安全性評価結果

---従来の安全性保証に欠陥が発見されるも、修復に成功---

【概要】

- 国際標準暗号 GCM に対し，これまでの安全性の保証には欠陥があることを明らかにしました．
- さらに，欠陥を取り除き，仕様を変更することなく GCM の安全性保証を修復することに成功しました．

【背景】

GCM (Galois/Counter Mode，ガロア／カウンタ・モード) は，データの暗号化と認証を同時に行うための認証暗号化方式と呼ばれる暗号技術です．David A. McGrew と John Viega によって 2004 年に設計されました．GCM は高い計算効率を有しており，またその安全性が設計者二人による数学的な証明によって保証されていると考えられてきたことから，GCM は米国の NIST (注 3) をはじめ，IEEE (注 4) や ISO/IEC (注 5) などが進める多くの標準化プロセスにおいて採用されてきました．NSA (注 6) での利用や，インターネット上のデータの保護など，世界中で日常的に利用されています．

GCM では現実的な計算量の攻撃方法に対し，その成功確率がある限界値以上にはならないことを数学的に証明することによって，安全性を保証しています．GCM に対する攻撃方法の開発は，その安全性を検証し，そして理解するうえで重要な研究課題であり，これまでにいくつかの攻撃方法が提案されてきました．これらの攻撃方法の成功確率は GCM が許容する限界値以下であって，したがってその安全性保証を揺るがすものではありません．GCM の安全性は数学的な証明によって保証されていて，そこに欠陥はないものと考えられてきました．

【研究成果】

GCM ではその内部でブロック暗号と呼ばれる共通鍵暗号要素技術を用います．本研究ではまず，このブロック暗号に全く欠陥がないと理想化した場合に，GCM の安全性保証の一部を覆す具体的な攻撃方法の開発に成功しました．理想化した GCM に対して，開発した攻撃方法の成功確率は GCM の安全性保証が正しければ 80×2^{-128} 以下であるはずなのに対し，実際はこの許容範囲を超える 94×2^{-128} 以上になります．したがって，この攻撃方法は GCM の安全性保証に欠陥があることを示しています．

この攻撃方法の成功確率は無視できるほど小さい確率であって（$94\times2^{-128} \fallingdotseq 2.76\times10^{-37}$），したがって現実的な脅威ではなく，理論的な攻撃方法です．また，理想化していない現実のブロック暗号を使用した GCM に対する安全性の保証とは矛盾せず，設計者の安全

性の主張の一部を覆すのみです．さらに，初期値と呼ばれる入力データが 96 ビットに限定されている場合は攻撃ができず，多くの標準では計算効率の観点から GCM の初期値を 96 ビットに限定して使用するように規定，あるいは推奨されています．一方で，開発した攻撃方法は GCM のこれまでの安全性保証の理論的裏付けが無効であったことを示しています．さらに，今回開発した攻撃方法の改良によって，今後現実的に脅威となるような攻撃方法が開発される可能性がゼロではないことを示唆するとともに，GCM の安全性はそもそも数学的に保証できるのか，という未解決問題が存在することを示しています．

これらの問題に対して，欠陥を取り除き，仕様を変更することなく GCM の安全性を数学的に保証することに成功しました．これにより，GCM の内部で用いるブロック暗号が安全であれば，現実的な計算量の攻撃方法に対して，その成功確率はある限界値以上にはならないことが示されました．さらに，初期値を 96 ビットに限定した場合は，より高い安全性を保証することに成功しました．

【結果の意義・今後の展望】

GCM は NIST 推奨の認証暗号化方式であり，その他の多くの標準化プロセスで採用されています．本研究で提案する攻撃方法は，広く標準化されている暗号技術である GCM に対し，設計者の安全性の主張の一部を覆すという意味での理論的攻撃方法を初めて明らかにしたものです．

一方で，GCM の安全性を数学的に証明することに成功しました．これは，そのような証明のない他の暗号技術と大きく異なる点であり，適切に実装されていれば実用上は GCM を使用することに安全性の問題がないことを示しています．しかし，攻撃成功確率の限界値はこれまでに信じられてきた数値よりも大きいため，GCM の使用にあたってはこのリスクを再評価することや，初期値を 96 ビットに限定して使用することが推奨されます．

本研究の成果は GCM の設計には改良の余地があることを示しています．本研究で得られた成果，並びに知見を設計にフィードバックすることによって，より高い安全性を有する認証暗号化方式を設計することが期待されます．

【用語】

(注 3) NIST：米国商務省標準技術局

(注 4) IEEE：米国電気電子学会

(注 5) ISO/IEC：国際標準化機構/国際電気標準会議

(注 6) NSA：米国国防総省国家安全保障局

【発表詳細】
国際会議名：CRYPTO 2012（クリプト 2012, http://www.iacr.org/conferences/crypto2012/）
論文タイトル：Breaking and Repairing GCM Security Proofs
著者：岩田　哲（名古屋大学），大橋　佳祐（名古屋大学），峯松　一彦（ＮＥＣ）

本研究のうち，岩田哲による研究の一部は科研費（若手研究（A), 22680001）による助成によって行われました.