SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

サイドチャネル攻撃により得られるBinary GCD演算系列に対するエラーモデル

Error model for Binary GCD operation sequences obtained by side-channel attacks

谷健太 * 國廣昇 *
Kenta Tani Noboru Kunihiro

キーワード サイドチャネル攻撃，Flush+Reload攻撃，Performance Degradation攻撃，Binary GCDアルゴリズム

あらまし

Binary GCDアルゴリズムは，右シフト演算と減算を繰り返すことで，二つの自然数の最大公約数を求めるアルゴリズムである．OpenSSLのバージョン1.0.0-1.1.0hおよび1.0.2b-1.0.2oでは，RSA暗号の秘密鍵である二つの素数を生成する際にBinary GCDアルゴリズムが使用される．Aldayaらは，このBinary GCDアルゴリズムの脆弱性を指摘している[1]．攻撃者は，この脆弱性を利用し，サイドチャネル攻撃によって，秘密鍵を入力とするBinary GCDアルゴリズムの演算系列を収集する．このとき，サイドチャネル攻撃で得られる演算系列にはエラーが含まれる．

Aldayaらは，さらに，Binary GCDアルゴリズムのエラーが含まれる演算系列からRSA暗号の秘密鍵を復元できることを示している．そのため，サイドチャネル情報にエラーが付いていたとしても，攻撃者がそのエラーを訂正できれば秘密鍵を復元することが可能である．Aldayaらの研究を受けて，我々は，SCIS 2021 [2]およびCSS 2021 [3]において，別のアプローチでエラー訂正を行うアルゴリズムを提案している．特に，CSS 2021 [3]で提案したアルゴリズムは演算系列に含まれるエラーの確率分布情報を利用してエラー訂正を行なっている．数値実験の結果，我々の提案したアルゴリズムの方がより効率的にエラー訂正を行い，秘密鍵を復元可能であることがわかった．エラーの確率分布情報を攻撃者が既知であれば，攻撃者はより高い確率で演算系列のエラーを訂正し，秘密鍵を入手することが可能である．そのため，正確なエラーモデルを導出すれば，どの程度のエラーが含まれているとき攻撃が成功するかをより厳密に評価することができる．

本稿では，まず，Aldayaらが提案する演算系列を取得する攻撃を用いて，OpenSSLでRSA暗号の鍵生成を行う計算機に対して実際にサイドチャネル攻撃を行う．本稿での攻撃環境において，サイドチャネル攻撃のパラメータを調整し，サイドチャネル情報を収集する．次に，正しい演算系列において減算が連続しないことに注目して，得られたサイドチャネル情報を解析する．最後に，解析した結果を用いて，エラーの確率分布を分析し，エラーモデルの導出を行う．これにより，エラーの定性的な議論に留まらず，Binary GCDアルゴリズムの脆弱性を利用した攻撃のより厳密な評価が可能となる．

参考文献

[1] A. C. Aldaya, C. P. García, L. M. A. Tapia, and B. B. Brumley. Cache-timing attacks on RSA key generation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, Vol. 2019, No. 4, pp. 213–242, 2019.

[2] 谷健太, 國廣昇． RSA暗号の鍵生成におけるBinary GCDアルゴリズムの安全性評価（2E4-1）．SCIS2021.

[3] 谷健太, 國廣昇. エラー付きLS系列に対するエラー訂正アルゴリズム（3D1-3）．CSS2021.

* 筑波大学, 〒305–8577 茨城県つくば市天王台1-1-1, University of Tsukuba, 1-1-1, Tennodai, Tsukuba, Ibaraki, 305–8577, Japan
s2120617@s.tsukuba.ac.jp