修士学位論文要約（令和４年３月）

公開鍵暗号ソフトウェアへの深層学習に基づく安全性評価に関する研究

齋藤 宏太郎
指導教員：本間 尚文

Deep–Learning Based Security Evaluation of Public–Key Cryptographic Software

Kotaro SAITO
Supervisor: Naofumi HOMMA

In the age of the IoT, devices that provide cryptographic technology are close at hand. Even mathematically secure ciphers may leak secret information due to the physical behavior of the device, and attacks that exploiting this kind of leakage are called side-channel attacks. Public key cryptography, which has traditionally been considered a low threat due to the difficulty of attack scenarios, can be a realistic security hole in the IoT era because side-channel attacks have not been adequately evaluated in research. In addition, in the IoT era, attackers can obtain clones of their target devices and gather information in advance. This information gathering can reduce the cost of an attack. Such a method is called a profiling side-channel attack. One particularly powerful method is the side-channel attack using deep learning (DL-SCA), which has been reported to be highly efficient even when conventional countermeasures are implemented. In this study, security of RSA cryptographic software using Gnu MP, a multiple-length arithmetic library that is currently used as OSS, is evaluated by DL-SCA. Experimental results show that this is no longer valid as a countermeasure.

1. はじめに

IoT の時代では暗号技術を提供するデバイスが身近に存在する．数学的に安全な暗号でも，デバイスの物理的挙動から秘密情報が漏洩する場合があり，これによる攻撃をサイドチャネル攻撃と呼ぶ．従来は攻撃シナリオの困難さから脅威が小さいと考えられていた公開鍵暗号は，サイドチャネル攻撃の評価が十分研究されていない現状があるため，IoT 時代の現実的なセキュリティホールとなりうる．また，IoT の時代では攻撃者はその目的のデバイスのクローンを入手して，あらかじめ情報収集を行うことが可能となる．この事前の情報収集によって，攻撃時のコストを抑えることができる．このような手法をプロファイリング型サイドチャネル攻撃と呼ぶ．特に強力な手法として深層学習を用いたサイドチャネル攻撃（DL-SCA）があり，従来の対策が実装されている場合においても高い攻撃効率を発揮することが報告されている [1]．

本研究では，実際に現在使用される OSS である多倍長演算ライブラリ Gnu MP を用いた RSA 暗号ソフトウェアを構成し，DL-SCA による安全性評価を行う．Gnu MP のアルゴリズム実装は，ダミー処理によるハイディングがサイドチャネル攻撃対策として実装されているが，これが対策としてもはや無効であることを実験的に示す．

2. RSA 暗号ソフトウェアへのサイドチャネル攻撃

RSA 暗号を始めとした公開鍵暗号へのサイドチャネル攻撃では，その処理頻度の少なさや乱数によるマスキングなどにより複数の処理にかかわる波形を用いるようなシナリオが成立しがたい．したがって，単一の処理にかかわるサイドチャネル波形のみを用いて攻撃を行うことが，現実的な攻撃の成立要件となる．

複数の研究において，DL-SCA は非常に高い秘密情報復元効率を示すことが報告されている．したがって，DL-SCA を用いた攻撃手法によって，単一波形による攻撃が達成できる可能性がある．RSA 暗号は秘密鍵として秘密指数 2 つと秘密素数 2 つをもつが，サイドチャネル攻撃によって秘密指数 2 つを復元する．秘密指数の復元が高精度に行える場合，秘密素数は探索により復元することが可能である [2]．ゆえに，攻撃を成立させるためには，秘密素数の探索による復元が可

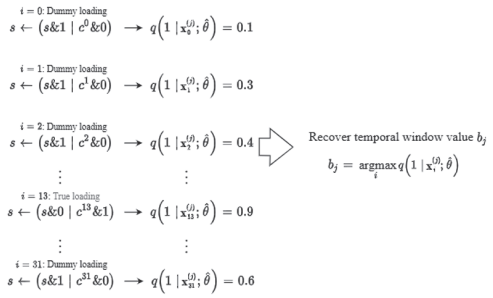

図 1 提案 DL-SCA による指数推定の概略図

能な程度まで秘密指数の値を高い精度で復元することが必要である．一方，誤りを含む秘密鍵から全鍵を復元するアルゴリズム [3]は，誤りビットが一様な確率で分布することを前提する．サイドチャネル攻撃によって窓幅単位で秘密指数が推定されるシナリオでは，誤りビットは窓幅単位で近接して存在するため，このような場合には非効率である課題がある．

3. 提案手法

提案手法は，(1)深層学習を用いたサイドチャネル波形の解析による高精度な秘密指数の推定，(2)ヒューリスティック探索アルゴリズムによる秘密鍵全体の復元，の２つの手法によって構成される．まず，乗算オペランド選択時のロード処理またはダミーロード処理時のサイドチャネル波形をプロファイリングデバイスから取得し，これらを分類する深層学習モデルを作成する．攻撃時には，攻撃対象デバイスからRSA 暗号の復号/署名処理 1 回分のサイドチャネル波形を取得し，図 1 のように，それに含まれる真のロード/ダミーロードの系列を深層学習モデルによって決定する．図 1 では，13 番目のロードがもっとも真のロードである確率が高いと推論されているが，この場合の窓値（RSA 暗号の秘密指数の一部）の推定値は 0xD となる．つまり，真のロードが実行される位置は，窓値と直接対応するため，位置を高精度に決定することができれば，秘密指数の推定が可能である．推定誤りが発生した場合は，秘密指数の推定値に窓幅単位のビット誤りが発生する．

秘密鍵の残りの部分である素数は，推定した秘密指数を用いたヒューリスティック探索により復元する．同時に，この探索アルゴリズムによって推定した秘密指数の誤りビットを訂正する．探索には RSA 暗号の鍵同士が満たす関係式を利用することができ，あるビットを決定すると，その 1 つ上位のビットの候補は関係式を解くことで求めることができる．提案手法では，事前に得られている秘密指数の推定値と，探索中に得られた秘密指数の候補の値との比較を行い，窓値単位の値の一致がどれだけ連続しているかの尺度をヒューリスティクスとして導入する．窓幅単位による評価を行うことにより，先行研究 [3]の課題であった誤りビットの分布位置問題を軽減することができる．これにより，正しい探索パス上にある可能性が高いと期待される候補を優先して展開可能となる．

4. 評価実験

まず，DL-SCA により秘密指数の推定を行う実験を行った．秘密指数の推定結果を，表 1 に示す．単純な 2^w 値分類により窓値を推定した場合の精度は鍵長 1,024 ビットの時 11.53%および 2,048 ビットの時 3.624%であったことから，提案手法で分類問題を 2 値分類に簡単化したことによる効果が確認できる．また，一度のべき乗剰余演算の波形から指数を推定する際には，誤りの発生数は鍵長それぞれ高々2 か所または 3 か所であった．結果として，1,024 ビットの場合は 48 回のべき乗剰余演算のうち 38 回，2,048 ビットの場合は 100 回のうち 77 回は誤りを含まずに指数を復元できた．以上の実験結果から，提案する DL-SCA 手法によって非常に高い精度で指数を復元できることを確認できる．

表 1 指数の推定結果（成功確率）

	ロード属性	窓値	指数
1,024 ビット	99.94%	99.80%	79.17%
2,048 ビット	99.66%	99.86%	77.00%

また，秘密指数に窓幅単位の誤りを与え，探索アルゴリズムによって全秘密鍵の復元を行う実験を行った．DL-SCA で発生した誤りの最悪ケース，つまり鍵長 1,024 ビットの時 2 か所，2,048 ビットの時 3 か所のケースにおいても，それぞれ数十秒～数千秒のオーダーで全秘密鍵復元が可能である結果となった．以上より，Gnu MP を用いて構成した RSA 暗号ソフトウェアの秘密鍵復元が，単一のサイドチャネル波形のみによって実行可能であることが示される．

5. まとめ

OSS の一つである Gnu MP で採用されているダミーロード対策を採用している RSA 暗号ソフトウェアに対するサイドチャネル攻撃手法を提案し，その評価を行った．複数の OSS でアルゴリズム的に同様の対策が採用されているため，提案手法はそのような OSS に対しても共通して適用可能であると考えられる．今後の展望として楕円曲線暗号などの他の公開鍵暗号実装に対する提案手法の拡張と適用可能性の検討が挙げられる．

文献

1) E. Prouff, R. Strullu, R. Benadjila, E. Cagli, and C. Canovas, “Study of DeepLearning Techniques for Side-Channel Analysis and Introduction to ASCAD Database,” IACR Cryptol. ePrint Arch., 2018.
2) N. Heninger and H. Shacham, “Reconstructing RSA Private Keys from Random Key Bits,” in Advances in Cryptology - CRYPTO 2009, ser. Lecture Notes in Computer Science, S. Halevi, Ed. Berlin, Heidelberg: Springer, 2009, pp. 1–17.
3) W. Henecka, A. May, and A. Meurer, “Correcting Errors in RSA Private Keys,” in Advances in Cryptology – CRYPTO 2010, ser. Lecture Notes in Computer Science, T. Rabin, Ed. Berlin, Heidelberg: Springer, 2010, pp. 351–369.