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

ECDSA ハードウェア実装におけるテンプレート攻撃と格子攻撃による秘密鍵復元の検討
Template Attacks on ECDSA Hardware and Key Recovery via Lattice Attacks

阿部 浩太郎 * 池田 誠 *
Kotaro Abe Makoto Ikeda

キーワード サイドチャネル攻撃，ECDSA，テンプレート攻撃，格子攻撃

あらまし

サイドチャネル攻撃は，消費電力などの物理的な情報を利用して暗号デバイスから秘密情報を漏洩させるものであり，暗号実装の安全性を脅かす攻撃である．公開鍵暗号である楕円曲線暗号を利用した ECDSA ではナンス (署名ごとに異なる乱数) と呼ばれるパラメータを用いるが，これは秘密鍵同様に秘密にされるべきパラメータである．楕円曲線暗号における主要な演算にスカラ倍算と呼ばれる演算があるが，ECDSA ではスカラ倍算にナンスの値が用いられるため，安全でない実装の場合にはサイドチャネル攻撃によりナンスの一部を復元可能であることが報告されている．

特に，ナンスの値がすべてのビットについて判明せずとも数ビットでも判明すれば格子攻撃により秘密鍵が復元されることが知られており，[1] によれば 256 ビットの ECDSA では 3 ビットのナンスが目安として 132 個の署名で判明すれば秘密鍵が復元可能であるとされる．

本研究では ASIC に実装された ECDSA 署名生成におけるモンゴメリラダーによるスカラ倍算を対象として攻撃を実行することにより，実装の安全性を評価することを目的とし，まず，強力なサイドチャネル攻撃の一つであるテンプレート攻撃により格子攻撃のために必要なナンスの 3 ビットを推測した．本研究ではテンプレート攻撃には消費電流波形の情報を用いた．テンプレート攻撃は 2 段階から構成される攻撃である．第 1 段階はテンプレート作成 (プロファイリング) であり，攻撃対象デバイスそのものあるいは同種デバイスが攻撃者の制御下に置かれることを仮定し，ナンスの 3 ビットの値に応じた $2^3 = 8$ 通りのテンプレート波形を作成する．第 2 段階はマッチングであり，ターゲット (攻撃用) 波形が得られた実行時に用いられたナンスの値をテンプレート波形とマッチングすることにより確定させる．スカラ倍算の実装はモンゴメリラダーを用いており，ナンスの最上位ビットから 1 ビットずつ処理されていくためマッチングも最上位ビットから順に行うことが可能である．3 ビットを一度に推測するよりも処理される順序に従って 1 ビットずつ推測するほうが，上位側の推測結果を利用して次のビットのマッチングを行うことができるため適していると考えられる．

今回用いたテンプレート波形数は 8 通りのナンスにおいて各 1000 であり合計で 8000，攻撃回数すなわちターゲット波形数は 1000 であった．1000 回の攻撃結果のうちナンスの 3 ビットを正しく推測したものは 484 回であり，約半数の誤りが含まれているため格子攻撃を実行するためには精度が高いと期待される結果のみを選別する必要があった．一定の基準により選別された結果を利用して格子攻撃を実行し秘密鍵候補を計算したところ，格子攻撃試行回数 55 回の約半数である 32 回において ECDSA 秘密鍵を復元することに成功した．

参考文献

[1] K. Abe and M. Ikeda, “Estimating the Effectiveness of Lattice Attacks,” Cryptology ePrint Archive, Report 2021/1489, 2021.

* 東京大学, 東京都文京区本郷 7-3-1, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan