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

フーリエ解析ベース攻撃に対するECDSAのエラーレートに基づく解析
Error-rate-based analysis of ECDSA against Fourier analysis-based attacks

大﨑 俊輔 * 國廣 昇 †
Shunsuke Osaki Noboru Kunihiro

キーワード サイドチャネル攻撃，ECDSA，安全性評価

あらまし

ECDSA は，楕円曲線を用いたデジタル署名アルゴリズムであり，SSH や SSL/TLS，ビットコインなどにおいて使用されている．そのため，どの程度の秘密情報が漏洩すると，安全性に影響を及ぼすかを評価することは非常に重要である．nonce は署名時に使用されるランダムな秘密情報であり，サイドチャネル攻撃によって漏洩する場合がある．部分情報が漏洩した nonce，それに対応したメッセージのハッシュ値，署名の 3 つ組が，ある一定の個数以上漏洩した場合，Hidden Number Problem（HNP）を解くことによって秘密鍵は復元されることが知られている．

HNP を解き秘密鍵を復元する攻撃手法には，格子簡約による格子ベースの攻撃やフーリエ解析ベースの攻撃がある．格子ベースの攻撃では 160-bit の秘密鍵に対して nonce が 2-bit，256-bit に対しては 4-bit が漏洩していれば効率よく復元することができる．一方でフーリエ解析ベースの攻撃では，160-bit の場合はエラー付きで 1-bit が，256-bit の場合にはエラー付きで 2-bit が得られた場合でも復元可能である．したがって，フーリエ解析ベースでは格子ベースに比べて漏洩する nonce の長さが短い場合でも復元することは可能である．しかし，必要な署名数や計算機資源，時間において効率的ではない．

フーリエ解析ベースの攻撃では秘密鍵の全探索を回避するために，collision search という段階において HNP のインスタンスから線形結合を取ることで，秘密鍵の探索を容易にしている．具体的に，Takahashi らは Schroeppel–Shamir–based algorithm を用いて線形結合を取る手法を提案している [3]．これによって，以前使われていた sort–and–difference algorithm と比較してより少ない署名数とより小さな空間計算量で実行可能となっている．しかし，時間計算量は大きくなっている．Generalized Birthday Problem の部分問題である $\mathcal{K}$–list sum problem[2] は線形結合を取るのにより効率的である．Aranha らは $\mathcal{K}$–list sum algorithm を用いて実装している．そして，1-bit の nonce がエラー付きで得られた際に 192-bit までの秘密鍵の復元に成功している．Aranha らは得られる nonce のエラーレートがある特定の値のときに必要となる署名数，メモリ，時間の評価を行っている [1]．しかし，エラーレートが変化した場合に，それぞれがどのように変化するのかは評価されておらず，明らかではない．

本発表ではまず，エラーレートが変化した場合に必要となる署名数と時間の定式化を行う．さらに，エラーレートの大きさによって，それらのパラメータがどのように変化するのかなどの関係性についての解析を行い，エラーレートがアルゴリズムに与える影響を明らかにする．

参考文献

[1] D. F. Aranha, F. R. Novaes, A. Takahashi, M. Tibouchi, and Y. Yarom. Ladderleak: Breaking ECDSA with less than one bit of nonce leakage. In *CCS '20*, pp. 225–242, 2020.

[2] I. Dinur. An algorithmic framework for the generalized birthday problem. *Des. Codes Cryptogr.*, Vol. 87, No. 8, pp. 1897–1926, 2019.

[3] A. Takahashi, M. Tibouchi, and M. Abe. New bleichenbacher records: Fault attacks on qdsa signatures. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, Vol. 2018, No. 3, pp. 331–371, 2018.

* 筑波大学情報学群情報科学類，〒 305-8573 茨城県つくば市天王台 1-1-1
† 筑波大学システム情報系