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

Efficient Modular Inversion Resisting Side Channel Attack

Yaoan Jin * Atsuko Miyaji†

Keywords: constant time modular inversion (CTMI), constant time GCD, side channel attack (SCA).

Abstract

With the development of side channel attack (SCA), theoretically proved secure cryptosystems, digital signatures, protocols, etc. are no longer secure on internet of things (IoT) devices and PCs. Specifically, targeting the SCA weakness of binary euclidean algorithm (BEA) and binary extended euclidean algorithm (BEEA), which are used to compute greatest common divisor (GCD) and modular inversion (MI) respectively, simple power analysis (SPA), cache-timing attack (CTA), machine learning-based profiling attack (ML-PA) were conducted on RSA key generation and ECDSA with high success rate. As for countermeasures, one can hide the secret input values by appropriate masking procedure. Otherwise, the constant-time modular inversion (CTMI) algorithm based on Fermat's little theorem (FLT) maybe a good choice. However it can not compute GCD and is not efficient for general inputs. [WB14] and [BY19] proposed CTMI algorithms respectively, which are not based on FLT. Their algorithms can work on more computation tasks including modular inversion but also lost efficiency. Small number of iterations and simple computations during one iteration are good characteristics of a CTMI algorithm. We propose a new CTMI algorithm, which combines the basic idea of BEEA and the fact, $\forall A, B \in Z, GCD(A, B) = GCD(B, A - B) = GCD(A, A - B)$, satisfies these characteristics. Our CTMI algorithms resisting SCA can compute the same computation tasks as [BY19]. Compared with [BY19] and FLT, Our CTMI algorithms computes both GCD and MI much efficiently by experiments.

* Graduate School of Engineering, Osaka University, 2-1 Yamadaoka, Suita, Osaka, Japan. jin@cy2sec.comm.eng.osaka-u.ac.jp

† Graduate School of Engineering, Osaka University, 2-1 Yamadaoka, Suita, Osaka, Japan and Japan Advanced Institute of Science and Technology, 1-1 Asahidai, Nomi, Ishikawa, Japan. miyaji@comm.eng.osaka-u.ac.jp

1 Related work

[WB14] proposed a CTMI algorithm by improving Kaliski's algorithm to a constant-time version. The basic idea is that computing the contents of all branches then selecting the correct values from them according to the defined signal variables during each iteration. Because the total bit length of the inputs (a number a and a prime p) reduces at least one every iteration in the CTMI algorithm. [WB14] fixed the number of iterations as $2 \cdot bitlen(p)$.

[BY19] also proposed a CTMI algorithm. The computations during one iteration are more simple than [WB14], but its number of iterations defined by $\lfloor (49d + 57)/17 \rfloor (d \geq 46)$, where $d = max(bitlen(a), bitlen(p))$, is much more.

2 Our work

Our setting of the constant number of iterations is the same as [WB14]. The main computations in our CTMI algorithm are base on:

$$\begin{cases} GCD(a,b) = GCD(a, \frac{b-a}{2}), odd(a), odd(b) \\ GCD(a,b) = GCD(\frac{b}{2}, b-a), odd(a), even(b). \\ GCD(a,b) = GCD(\frac{a}{2}, b-a), even(a), odd(b). \end{cases} \quad (1)$$

where $a, b \in Z$ and $a \leq b$. Note that there are branches in our algorithm, but the computations in each branch are the same without dummy computations. It is easy to remove branches from our algorithm by tricks. Our algorithm can also compute Montgomery inversion. We analyze SCA security and efficiency of our work from a theoretical and experimental point of view.

References

[1] [BY19] Bernstein, Daniel J., and Bo-Yin Yang., "Fast constant-time gcd computation and modular inversion." *IACR Transactions on Cryptographic Hardware and Embedded Systems*, (2019): 340-398.

[2] [WB14] Bos, Joppe W, "Constant time modular inversion." *Journal of Cryptographic Engineering* (2014): 275-281.