US 20230231696A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231696 A1**

CHEN (43) **Pub. Date: Jul. 20, 2023**

(54) **METHOD FOR PERFORMING POWER DISTURBING OPERATION TO REDUCE SUCCESS RATE OF CRYPTOSYSTEM POWER ANALYSIS ATTACK, CRYPTOSYSTEM PROCESSING CIRCUIT, AND ELECTRONIC DEVICE**

(71) Applicant: **Realtek Semiconductor Corp.**, Hsinchu (TW)

(72) Inventor: **YUEFENG CHEN**, Suzhou City (CN)

(73) Assignee: **Realtek Semiconductor Corp.**, HsinChu (TW)

(21) Appl. No.: **17/885,581**

(22) Filed: **Aug. 11, 2022**

(30) **Foreign Application Priority Data**

Jan. 20, 2022 (CN) 202210068877.9

Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)
H04L 9/08 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/003*** (2013.01); ***H04L 9/0869*** (2013.01)

(57) **ABSTRACT**

A method for performing a power disturbing operation to reduce a success rate of cryptosystem power analysis attack, an associated cryptosystem processing circuit and an associated electronic device are provided. The method includes: generate at least one random number; generating a plurality of power disturbing parameters respectively corresponding to a plurality of bit calculation phases according to the at least one random number, where the plurality of bit calculation phases represent a plurality of cryptosystem processing phases related to a predetermined cryptosystem, and correspond to a plurality of private key bits of a private key, respectively; and according to the plurality of power disturbing parameters, enabling at least one predetermined circuit of a plurality of predetermined circuits in the plurality of bit calculation phases, respectively, to use power corresponding to the plurality of power disturbing parameters to perform the power disturbing operation in the plurality of bit calculation phases, respectively.