

# (19) United States

# (12) Patent Application Publication (10) Pub. No.: US 2024/0214193 A1

## Jun. 27, 2024 (43) **Pub. Date:**

### (54) METHOD AND APPARATUS FOR GENERATING WORKING KEY, AND COMPUTER-READABLE STORAGE **MEDIUM**

(71) Applicant: FEITIAN TECHNOLOGIES CO.,

LTD., Beijing (CN)

(72) Inventor: Zhou LU, Beijing (CN)

(21) Appl. No.: 18/288,049

(22) PCT Filed: Jun. 28, 2022

(86) PCT No.: PCT/CN2022/101736

§ 371 (c)(1),

(2) Date: Oct. 24, 2023

#### (30)Foreign Application Priority Data

Sep. 16, 2021 (CN) ...... 202111083495.5

#### **Publication Classification**

(51) Int. Cl. H04L 9/08 (2006.01) (52) U.S. Cl. CPC ...... *H04L 9/0861* (2013.01)

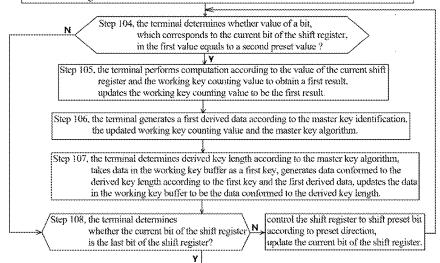
#### (57)ABSTRACT

The invention provides a working key generation method and device and a computer readable storage medium, and belongs to the technical field of information security. The method comprises the following steps: the terminal receiving an operation instruction sent by an upper computer, obtaining a working key purpose and a working key algorithm according to the operation instruction, setting the working key purpose as a first purpose by the terminal, generating derived data according to the first purpose, a master key identifier, a first numerical value and a master key algorithm, determining the length of a working key according to the working key algorithm, obtaining data in a working key buffer area as a key, generating the working key according with the length of the working key according to the key and the derived data, executing corresponding operation according to the operation instruction and the working key, and returning an operation result to the upper computer. Compared with an encryption scheme in the prior art, the method provided by the invention is safer and wider in application range.

Step 101, a terminal receives an operating instruction sent from a host, acquires a master key value, a master key counter value and a master key algorithm identification according to a key index in the operating instruction.

Step 102, the terminal processes the master key counter value according to a first preset algorithm to obtain a master key identification and a first value.

Step 103, the terminal initializes a working key buffer, stores the master key value in the working key buffer, sets the working key counting value, initializes a shift register, sets a current bit of the shift register.



Step 109, the terminal sets the working key usage to be a first usage according to the operating instruction, generates a second derived data according to the first usage, the master key identification, the first value and the master key algorithm.

Step 110, the terminal acquires a working key algorithm according to the operating instruction, determines working key length according to the working key algorithm, takes data in the working key buffer as a second key, generates a working key according to the second key and the second derived data, performs corresponding operation according to the operating instruction and the working key, returns an operating result to the host.