

**CRYPTOGRAPHIC OPERATION METHOD, WORKING KEY CREATION METHOD,
CRYPTOGRAPHIC SERVICE PLATFORM, AND CRYPTOGRAPHIC SERVICE
DEVICE**

5

ABSTRACT

The present specification provides a cryptographic operation method, a working key creation method, a cryptographic service platform, and a cryptographic service device. In a security module connected to the cryptographic service platform, a key management function is provided by a primary security module. The primary security module is used for generating a key. Both the primary security module and secondary security modules can provide a cryptographic operation function required by the cryptographic service platform. A master key of each secondary security module is generated by the primary security module. A working key of a business system is also generated by the primary security module. In addition, the cryptographic service platform stores a working key ciphertext encrypted by the master key of the primary security module and a working key ciphertext encrypted by the master key of each secondary security module. Neither the master key nor a working key plaintext, which functions as sensitive security parameters, exceeds a boundary of the security module, such that the security of the key is not put at risk, thereby meeting key security requirements. The cryptographic service platform can also be compatible with various security modules so as to provide a more stable cryptographic service.

Fig. 4