

ABSTRACT

Disclosed are a calculation device for encryption using a public key and an encryption method thereof. The present method comprises: a step for setting a secret key, and generating a public key using the secret key and an error extracted from a discrete Gaussian distribution or a distribution that is within a short statistical distance thereto; and a step for applying the public key to a message, and then performing a rounding process to encrypt the message. Accordingly, encryption efficiency can be enhanced.

Figure 1 accompanies.