

A B S T R A C T

In a decryption apparatus according to an embodiment, a holding means pre-holds a verification formula. A determination means performs a calculation based on the verification formula read from the holding means by
5 substituting, into the verification formula, the part of the re-encrypted data received from a re-encryption apparatus and the public key of a re-encryption key generation apparatus and the private key of the decryption apparatus, to determine
10 whether or not the verification formula holds true. An output means outputs verification success when a result of the determination indicates that the verification formula holds true.