(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-31151
(P2013-31151A)
(43)公開日　平成25年2月7日(2013.2.7)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/10	(2006.01)	H04L	9/00	621A	5J104
H04L	9/08	(2006.01)	H04L	9/00	601B	

審査請求 未請求　請求項の数 57　OL　（全 61 頁）

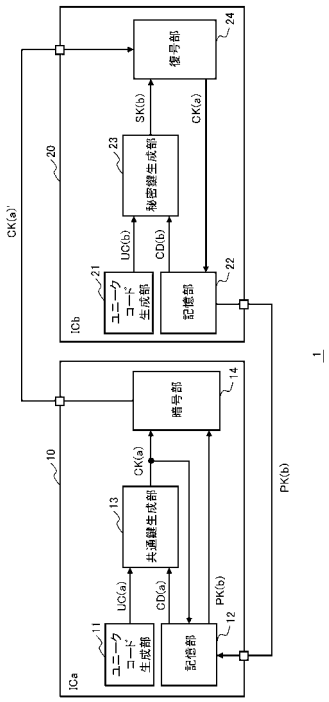
(21)出願番号　特願2012-76387(P2012-76387)
(22)出願日　平成24年3月29日(2012.3.29)
(31)優先権主張番号　特願2011-136131(P2011-136131)
(32)優先日　平成23年6月20日(2011.6.20)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2011-136132(P2011-136132)
(32)優先日　平成23年6月20日(2011.6.20)
(33)優先権主張国　日本国(JP)

(71)出願人　302062931
ルネサスエレクトロニクス株式会社
神奈川県川崎市中原区下沼部１７５３番地
(74)代理人　100103894
弁理士　家入　健
(72)発明者　塩田　茂雅
神奈川県川崎市中原区下沼部１７５３番地
ルネサスエレクトロニクス株式会社内
(72)発明者　古田　茂
神奈川県川崎市中原区下沼部１７５３番地
ルネサスエレクトロニクス株式会社内
(72)発明者　廣川　祐之
神奈川県川崎市中原区下沼部１７５３番地
ルネサスエレクトロニクス株式会社内

最終頁に続く

(54)【発明の名称】暗号通信システムおよび暗号通信方法

(57)【要約】　（修正有）
【課題】暗号通信システムのセキュリティを向上させることである。
【解決手段】本発明にかかる暗号通信システムは、半導体装置１０と半導体装置２０とを備える。半導体装置１０は、ユニークコードＵＣ（ａ）と訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する共通鍵生成部１３と、共通鍵生成部１３で生成された共通鍵ＣＫ（ａ）を半導体装置２０の公開鍵ＰＫ（ｂ）を用いて暗号化する暗号部１４と、を備える。半導体装置２０は、ユニークコードＵＣ（ｂ）と訂正データＣＤ（ｂ）とを用いて秘密鍵ＳＫ（ｂ）を生成する秘密鍵生成部２３と、暗号部１４で暗号化された共通鍵ＣＫ（ａ）’を秘密鍵ＳＫ（ｂ）を用いて復号する復号部２４と、を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
第１の半導体装置と第２の半導体装置とを備える暗号通信システムであって、
前記第１の半導体装置は、
前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと、当該第１のユニークコードを訂正する第１の訂正データとを用いて共通鍵を生成する共通鍵生成部と、
前記共通鍵生成部で生成された前記共通鍵を前記第２の半導体装置の公開鍵を用いて暗号化する暗号部と、を備え、
前記第２の半導体装置は、
前記第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードと、当該第２のユニークコードを訂正する第２の訂正データとを用いて前記第２の半導体装置の秘密鍵を生成する秘密鍵生成部と、
前記暗号部で暗号化された共通鍵を前記秘密鍵を用いて復号する復号部と、を備える、
暗号通信システム。
【請求項２】
前記第１の半導体装置および前記第２の半導体装置は前記共通鍵を用いて通信する、請求項１に記載の暗号通信システム。
【請求項３】
前記第１の訂正データは、
前記第１のユニークコードのビットのうちエラー率の高いビットをマスクするためのマスクデータと、
前記第１のユニークコードのビットのうちエラー率の低いビットを訂正するためのエラー訂正コードと、を含む、
請求項１または２に記載の暗号通信システム。
【請求項４】
前記第１の訂正データは、更に、前記マスクデータおよび前記エラー訂正コードを用いてエラー訂正された第１のユニークコードに対して所定の演算を実施するための演算パラメータを含む、請求項３に記載の暗号通信システム。
【請求項５】
前記共通鍵生成部は、
前記第１のユニークコードを前記マスクデータを用いてマスクし、
前記エラー訂正コードを用いて、前記マスクされた第１のユニークコードのエラーを訂正し、
前記演算パラメータを用いて、前記マスクデータおよび前記エラー訂正コードを用いてエラー訂正された第１のユニークコードに対して演算を実施する、
請求項４に記載の暗号通信システム。
【請求項６】
前記第１および第２の半導体装置はセキュアマイコンを用いて構成されている、請求項１乃至５のいずれか一項に記載の暗号通信システム。
【請求項７】
前記第１および第２の半導体装置は汎用マイコンを用いて構成されている、請求項１乃至５のいずれか一項に記載の暗号通信システム。
【請求項８】
前記第１および第２の半導体装置は車載用のマイコンである、請求項１乃至７のいずれか一項に記載の暗号通信システム。
【請求項９】
前記第１および第２の半導体装置の一方は故障診断ユニットである、請求項８に記載の暗号通信システム。
【請求項１０】

前記第１および第２の半導体装置の一方はカーナビゲーションシステムである、請求項８に記載の暗号通信システム。

【請求項１１】

第１の半導体装置と第２の半導体装置とを備える暗号通信システムであって、

前記第１の半導体装置は、

前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと、当該第１のユニークコードを訂正する第１の訂正データとを用いて前記第１の半導体装置の秘密鍵を生成する秘密鍵生成部と、

前記秘密鍵と平文とを用いて署名データを生成する署名データ生成部と、を備え、

前記第２の半導体装置は、前記署名データと前記第１の半導体装置の公開鍵とを用いて検証用データを生成し、当該検証用データと前記平文とを比較する検証部を備える、

暗号通信システム。

【請求項１２】

前記第２の半導体装置は、前記第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードと、当該第２のユニークコードを訂正する第２の訂正データとを用いて前記第１の半導体装置の公開鍵を生成する公開鍵生成部を備える、請求項１１に記載の暗号通信システム。

【請求項１３】

前記第１の訂正データは、

前記第１のユニークコードのビットのうちエラー率の高いビットをマスクするためのマスクデータと、

前記第１のユニークコードのビットのうちエラー率の低いビットを訂正するためのエラー訂正コードと、を含む、

請求項１１または１２に記載の暗号通信システム。

【請求項１４】

前記第１の訂正データは、更に、前記マスクデータおよび前記エラー訂正コードを用いてエラー訂正された第１のユニークコードに対して所定の演算を実施するための演算パラメータを含む、請求項１３に記載の暗号通信システム。

【請求項１５】

前記秘密鍵生成部は、

前記第１のユニークコードを前記マスクデータを用いてマスクし、

前記エラー訂正コードを用いて、前記マスクされた第１のユニークコードのエラーを訂正し、

前記演算パラメータを用いて、前記マスクデータおよび前記エラー訂正コードを用いてエラー訂正された第１のユニークコードに対して演算を実施する、

請求項１４に記載の暗号通信システム。

【請求項１６】

前記第１および第２の半導体装置はセキュアマイコンを用いて構成されている、請求項１１乃至１５のいずれか一項に記載の暗号通信システム。

【請求項１７】

前記第１および第２の半導体装置は汎用マイコンを用いて構成されている、請求項１１乃至１５のいずれか一項に記載の暗号通信システム。

【請求項１８】

前記第１および第２の半導体装置は車載用のマイコンである、請求項１１乃至１７のいずれか一項に記載の暗号通信システム。

【請求項１９】

前記第１および第２の半導体装置の一方は故障診断ユニットである、請求項１８に記載の暗号通信システム。

【請求項２０】

前記第１および第２の半導体装置の一方はカーナビゲーションシステムである、請求項

１８に記載の暗号通信システム。
【請求項２１】
第１乃至第３の半導体装置を備える暗号通信システムであって、
前記第３の半導体装置は、第１のユニークコードを訂正する第１の訂正データを前記第１の半導体装置に、第２のユニークコードを訂正する第２の訂正データを前記第２の半導体装置にそれぞれ供給可能に構成され、
前記第１の半導体装置は、当該第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと前記第３の半導体装置から供給された前記第１の訂正データとを用いて共通鍵を生成する第１の共通鍵生成部を備え、
前記第２の半導体装置は、当該第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードと前記第３の半導体装置から供給された前記第２の訂正データとを用いて共通鍵を生成する第２の共通鍵生成部を備える、
暗号通信システム。
【請求項２２】
前記第３の半導体装置は、各々の半導体装置と、当該各々の半導体装置で生成される各々の共通鍵とに対応づけられた訂正データを格納したデータベースを備える、
請求項２１に記載の暗号通信システム。
【請求項２３】
前記第３の半導体装置は、前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと共通鍵とを用いて前記第１の訂正データを生成し、前記第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードと前記共通鍵とを用いて前記第２の訂正データを生成する訂正データ生成部を備える、
請求項２１に記載の暗号通信システム。
【請求項２４】
前記第３の半導体装置は、前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと第１の共通鍵とを用いて第１の訂正データを生成し、前記第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードと第２の共通鍵とを用いて第２の訂正データを生成する訂正データ生成部を備え
前記第１の半導体装置が備える前記第１の共通鍵生成部は前記第１の共通鍵を生成し、
前記第２の半導体装置が備える前記第２の共通鍵生成部は前記第２の共通鍵を生成し、
前記第１の半導体装置および前記第３の半導体装置は前記第１の共通鍵を用いて通信し、前記第２の半導体装置および前記第３の半導体装置は前記第２の共通鍵を用いて通信する、
請求項２１に記載の暗号通信システム。
【請求項２５】
前記第１の訂正データは暗号化された状態で前記第１の半導体装置に供給され、前記第２の訂正データは暗号化された状態で前記第２の半導体装置に供給される、
請求項２１乃至２４のいずれか一項に記載の暗号通信システム。
【請求項２６】
前記訂正データ生成部は、
前記第１のユニークコードを複数回取得し、
前記取得した第１のユニークコードのビットのうちエラー率の高いビットをマスクするためのマスクデータを生成し、
前記取得した第１のユニークコードのビットのうちエラー率の低いビットを訂正するためのエラー訂正コードを生成する、
請求項２３または２４に記載の暗号通信システム。
【請求項２７】
前記訂正データ生成部は更に、前記マスクデータおよび前記エラー訂正コードを用いてエラー訂正された第１のユニークコードと前記共通鍵とを用いて演算パラメータを生成する、請求項２６に記載の暗号通信システム。

【請求項２８】
前記第３の半導体装置はセキュアマイコンを用いて構成され、
前記第１および第２の半導体装置は汎用マイコンを用いて構成されている、
請求項２１乃至２７のいずれか一項に記載の暗号通信システム。
【請求項２９】
前記第１乃至第３の半導体装置は車載用のマイコンである、請求項２１乃至２８のいずれか一項に記載の暗号通信システム。
【請求項３０】
前記第１および第２の半導体装置は車載用のマイコンであり、前記第３の半導体装置はゲートウェイ部であり、前記第１および第２の半導体装置は前記ゲートウェイ部を介して通信する、請求項２４に記載の暗号通信システム。
【請求項３１】
前記第１および第２の半導体装置の一方は故障診断ユニットである、請求項２９または３０に記載の暗号通信システム。
【請求項３２】
前記第１および第２の半導体装置の一方はカーナビゲーションシステムである、請求項２９または３０に記載の暗号通信システム。
【請求項３３】
第１の半導体装置と第２の半導体装置とを用いた暗号通信方法であって、
前記第１の半導体装置において、
前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと、当該第１のユニークコードを訂正する第１の訂正データとを用いて共通鍵を生成し、
前記生成された共通鍵を前記第２の半導体装置の公開鍵を用いて暗号化し、
前記第２の半導体装置において、
前記第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードと、当該第２のユニークコードを訂正する第２の訂正データとを用いて前記第２の半導体装置の秘密鍵を生成し、
前記暗号化された共通鍵を前記秘密鍵を用いて復号する、
暗号通信方法。
【請求項３４】
第１の半導体装置と第２の半導体装置とを用いた暗号通信方法であって、
前記第１の半導体装置において、
前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと、当該第１のユニークコードを訂正する第１の訂正データとを用いて前記第１の半導体装置の秘密鍵を生成し、
前記秘密鍵と平文とを用いて署名データを生成し、
前記第２の半導体装置において、前記署名データと前記第１の半導体装置の公開鍵とを用いて検証用データを生成し、当該検証用データと前記平文とを比較する、
暗号通信方法。
【請求項３５】
第１乃至第３の半導体装置を用いた暗号通信方法であって、
前記第３の半導体装置から前記第１の半導体装置に第１のユニークコードを訂正する第１の訂正データを送付し、
前記第１の半導体装置において、当該第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと前記第３の半導体装置から供給された前記第１の訂正データとを用いて共通鍵を生成し、
前記第３の半導体装置から前記第２の半導体装置に第２のユニークコードを訂正する第１の訂正データを送付し、
前記第２の半導体装置において、当該第２の半導体装置に固有の値であってランダムな

エラーを含む第２のユニークコードと前記第３の半導体装置から供給された前記第２の訂正データとを用いて共通鍵を生成する、
暗号通信方法。
【請求項３６】
第１の半導体装置と第２の半導体装置とを備える暗号通信システムであって、
前記第１の半導体装置は、
前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコードと、当該第１のユニークコードを訂正する第１の訂正データとを用いて第１の共通鍵を生成する第１の共通鍵生成部と、
前記第１の共通鍵生成部で生成された第１の共通鍵と、前記第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードとを用いて、当該第２のユニークコードを訂正する第２の訂正データを生成する訂正データ生成部と、を備え、
前記第２の半導体装置は、前記第２のユニークコードと前記第２の訂正データとを用いて第１の共通鍵を生成する第２の共通鍵生成部を備える、
暗号通信システム。
【請求項３７】
前記第２の半導体装置は、前記第２のユニークコードを前記第１の半導体装置の公開鍵を用いて暗号化する暗号部を更に有し、
前記第１の半導体装置は、前記暗号部で暗号化された第２のユニークコードを前記第１の半導体装置の秘密鍵を用いて復号する復号部を更に有する、
請求項３６に記載の暗号通信システム。
【請求項３８】
前記暗号通信システムは更に、各々の半導体装置と、当該各々の半導体装置の公開鍵とを対応づけて格納したデータベースを備えるサーバを有し、
前記第２の半導体装置は、当該第２の半導体装置の秘密鍵と平文とを用いて署名データを生成し、
前記第１の半導体装置は、前記第２の半導体装置の署名データと、前記サーバから送付された前記第２の半導体装置の公開鍵とを用いて検証用データを生成し、当該検証用データと前記平文とを比較する検証部を更に備える、
請求項３６または３７に記載の暗号通信システム。
【請求項３９】
前記第２の半導体装置が備える暗号部は更に、前記第１の共通鍵生成部で生成された第１の共通鍵と前記第２のユニークコードとを用いて第２の訂正データを生成するための訂正データ生成プログラムを前記第１の半導体装置の公開鍵を用いて暗号化し、
前記第１の半導体装置が備える復号部は更に、前記暗号化された訂正データ生成プログラムを前記第１の半導体装置の秘密鍵を用いて復号し、
前記第１の半導体装置は、前記復号された訂正データ生成プログラムを実行して、前記第１の共通鍵と前記第２のユニークコードとを用いて前記第２の訂正データを生成する、
請求項３７に記載の暗号通信システム。
【請求項４０】
前記第１の半導体装置および前記第２の半導体装置は前記第１の共通鍵を用いて通信する、請求項３６乃至３９のいずれか一項に記載の暗号通信システム。
【請求項４１】
前記第１の共通鍵生成部は更に、前記第１の半導体装置に固有の第１のユニークコードと第３の訂正データとを用いて第２の共通鍵を生成し、
前記第１の半導体装置は前記第２の共通鍵を用いて第３の半導体装置と通信すると共に、前記第２の半導体装置は前記第１の半導体装置を介して前記第３の半導体装置と通信する、請求項４０に記載の暗号通信システム。
【請求項４２】
前記第１の訂正データは、

前記第１のユニークコードのビットのうちエラー率の高いビットをマスクするための第１のマスクデータと、
前記第１のユニークコードのビットのうちエラー率の低いビットを訂正するための第１のエラー訂正コードと、を含む、
請求項３６乃至４１のいずれか一項に記載の暗号通信システム。
【請求項４３】
前記第１の訂正データは、更に、前記第１のマスクデータおよび前記第１のエラー訂正コードを用いてエラー訂正された第１のユニークコードに対して所定の演算を実施するための第１の演算パラメータを含む、請求項４２に記載の暗号通信システム。
【請求項４４】
前記第１の共通鍵生成部は、
前記第１のマスクデータを用いて前記第１のユニークコードをマスクし、
前記第１のエラー訂正コードを用いて、前記マスクされた第１のユニークコードのエラーを訂正し、
前記第１の演算パラメータを用いて、前記第１のマスクデータおよび前記第１のエラー訂正コードを用いてエラー訂正された第１のユニークコードに対して演算を実施する、
請求項４３に記載の暗号通信システム。
【請求項４５】
前記第２の訂正データは暗号化された状態で前記第１の半導体装置から前記第２の半導体装置に送付される、請求項３６乃至４４のいずれか一項に記載の暗号通信システム。
【請求項４６】
前記訂正データ生成部は、
前記第２のユニークコードを複数回取得し、
前記取得した第２のユニークコードのビットのうちエラー率の高いビットをマスクするための第２のマスクデータを生成し、
前記取得した第２のユニークコードのビットのうちエラー率の低いビットを訂正するための第２のエラー訂正コードを生成し、
前記第２のマスクデータおよび前記第２のエラー訂正コードを用いてエラー訂正された第２のユニークコードと前記第１の共通鍵とを用いて第２の演算パラメータを生成する、
請求項３６乃至４５のいずれか一項に記載の暗号通信システム。
【請求項４７】
前記訂正データを生成する処理は、複数の半導体装置において分散して実施される、請求項４６に記載の暗号通信システム。
【請求項４８】
前記第１の半導体装置はセキュアマイコンを用いて構成されている、請求項３６乃至４７のいずれか一項に記載の暗号通信システム。
【請求項４９】
前記第１および第２の半導体装置は汎用マイコンを用いて構成されている、請求項３６乃至４７のいずれか一項に記載の暗号通信システム。
【請求項５０】
前記第１および第２の半導体装置は車載用のマイコンである、請求項３６乃至４９のいずれか一項に記載の暗号通信システム。
【請求項５１】
前記第１の半導体装置は車内ネットワークを構成している車載用のマイコンであり、
前記第２の半導体装置はカーナビゲーションシステムである、請求項３６乃至４９のいずれか一項に記載の暗号通信システム。
【請求項５２】
第１の半導体装置と第２の半導体装置とを用いた暗号通信方法であって、
前記第１の半導体装置において、
前記第１の半導体装置に固有の値であってランダムなエラーを含む第１のユニークコー

ドと、当該第１のユニークコードを訂正する第１の訂正データとを用いて第１の共通鍵を生成し、
前記生成された第１の共通鍵と、前記第２の半導体装置に固有の値であってランダムなエラーを含む第２のユニークコードとを用いて、当該第２のユニークコードを訂正する第２の訂正データを生成し、
前記第２の半導体装置において、前記第２のユニークコードと前記第２の訂正データとを用いて第１の共通鍵を生成する、
暗号通信方法。
【請求項５３】
前記第２の半導体装置において、前記第２のユニークコードを前記第１の半導体装置の公開鍵を用いて暗号化し、
前記第１の半導体装置において、前記暗号化された第２のユニークコードを前記第１の半導体装置の秘密鍵を用いて復号する、
請求項５２に記載の暗号通信方法。
【請求項５４】
前記第２の半導体装置において、当該第２の半導体装置の秘密鍵と平文とを用いて署名データを生成し、
前記第１の半導体装置において、各々の半導体装置と、当該各々の半導体装置の公開鍵とを対応づけて格納したデータベースを備えるサーバから送付された前記第２の半導体装置の公開鍵と、前記第２の半導体装置の署名データと、を用いて検証用データを生成し、当該検証用データと前記平文とを比較する、
請求項５２または５３に記載の暗号通信方法。
【請求項５５】
前記第２の半導体装置において、前記第１の共通鍵と前記第２のユニークコードとを用いて前記第２の訂正データを生成するための訂正データ生成プログラムを、前記第１の半導体装置の公開鍵を用いて暗号化し、
前記第１の半導体装置において、
前記暗号化された訂正データ生成プログラムを復号し、
前記復号された訂正データ生成プログラムを実行して、前記第１の共通鍵と前記第２のユニークコードとを用いて前記第２の訂正データを生成する、
請求項５３に記載の暗号通信方法。
【請求項５６】
前記第１の半導体装置および前記第２の半導体装置は前記第１の共通鍵を用いて通信する、請求項５２乃至５５のいずれか一項に記載の暗号通信方法。
【請求項５７】
前記第１の半導体装置において、当該第１の半導体装置に固有の第１のユニークコードと第３の訂正データとを用いて第２の共通鍵を生成し、
前記第１の半導体装置は前記第２の共通鍵を用いて第３の半導体装置と通信し、前記第２の半導体装置は前記第１の半導体装置を介して前記第３の半導体装置と通信する、請求項５６に記載の暗号通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は暗号通信システムおよび暗号通信方法に関し、特にセキュリティの向上を実現できる暗号通信システムおよび暗号通信方法に関する。
【背景技術】
【０００２】
通信システムにおいては、通信データの盗聴や改竄などを防ぐために通信データを暗号化している。この暗号化を実現する技術の一つに、通信を行なう両者が共通の暗号鍵（以下、共通鍵（Common key）という）を使用する共通鍵暗号方式（Common key cryptosyste

m）がある。共通鍵暗号方式では、第三者に知られることなく、通信を行なう両者に共通鍵を共有させる必要がある。これを実現する技術の一つにＲＳＡ（登録商標）や楕円曲線暗号などを用いた公開鍵暗号方式（Public key cryptosystem）がある。

【０００３】

特許文献１には、不正複製ＩＣの利用を防止することが可能な集積回路を提供する技術が開示されている。特許文献２には、物理的に複製不可能な固有データを生成する回路またはその他の構成要素を利用して、ＲＳＡ公開鍵または秘密鍵等のセキュリティワードを生成し、電子機器に使用される集積回路チップのセキュリティを確保する技術が開示されている。

【０００４】

特許文献３には、ローカルエリアネットワークを介して共通の暗号鍵を用いた暗号通信を行う通信システムにおいて、鍵交換に要する時間を短縮することができる技術が開示されている。特許文献４には、アドホック無線接続によるデータ送受信においてデータの完全性を簡単に検証することができる技術が開示されている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２０１０－２２６６０３号公報
【特許文献２】特表２０１０－５２７２１９号公報
【特許文献３】特開２００５-３４１５２８号公報
【特許文献４】特開２００２-２６８９９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

例えば、半導体装置ＩＣｘと半導体装置ＩＣｙとの間で共通鍵ＣＫ（ｘ）を用いて暗号通信を実施する場合、ＩＣｘとＩＣｙとで共通鍵ＣＫ（ｘ）を共有する必要がある。ＩＣｘが共通鍵ＣＫ（ｘ）を保有している場合、ＩＣｘは予め取得したＩＣｙの公開鍵ＰＫ（ｙ）を用いて共通鍵ＣＫ（ｘ）を暗号化し、暗号化された共通鍵ＣＫ（ｘ）'をＩＣｙへ送付する。そして、ＩＣｙは、ＩＣｙの秘密鍵ＳＫ（ｙ）を用いて、暗号化された共通鍵ＣＫ（ｘ）'を復号することで、共通鍵ＣＫ（ｘ）を取得することができる。このように、公開鍵暗号方式を用いてＩＣｘからＩＣｙへ共通鍵ＣＫ（ｘ）を送付することで、第三者に知られることなくＩＣｘとＩＣｙとで共通鍵ＣＫ（ｘ）を共有することができる。これにより、ＩＣｘとＩＣｙとの間で共通鍵暗号方式を用いて暗号通信を実施することができる。

【０００７】

ＩＣｘからＩＣｙへ共通鍵ＣＫ（ｘ）を送付する際は、共通鍵ＣＫ（ｘ）が暗号化されているため、共通鍵ＣＫ（ｘ）の情報が第三者に漏洩することはない。しかしながら、半導体装置（半導体チップ）ＩＣｘ、ＩＣｙの不揮発性メモリには共通鍵ＣＫ（ｘ）や秘密鍵ＳＫ（ｙ）などの重要なデータが格納されている。このため、半導体装置が不正に解析された場合、共通鍵ＣＫ（ｘ）や秘密鍵ＳＫ（ｙ）などの重要なデータが漏洩してしまうという問題がある。

【０００８】

また、上記の半導体装置ＩＣｘと半導体装置ＩＣｙのようにセキュアな通信が確立している暗号通信システムに新たに半導体装置ＩＣｚを追加する場合は、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証する必要がある。しかしながら、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証するには、例えば高価なセキュアサーバを暗号通信システムに組み込む必要がある。このため、暗号通信システムのコストが増加するという問題がある。

【課題を解決するための手段】

【０００９】

本発明にかかる暗号通信システムは、第１の半導体装置と第２の半導体装置とを備える。第１の半導体装置は、第１の半導体装置の製造ばらつき等に起因する固有のコードである第１のユニークコードと、第１のユニークコードを訂正するための第１の訂正データとを用いて共通鍵を生成し、公開鍵を用いて共通鍵を暗号化し第２の半導体装置に送信する。また、第２の半導体装置は、第２の半導体装置の製造ばらつき等に起因する固有のコードである第２のユニークコードと、第２のユニークコードを訂正するための第２の訂正データとを用いて第２の半導体装置の秘密鍵を生成し、この秘密鍵により第１の半導体装置から送られてきた暗号化された共通鍵を復号する。以上の動作により第１の半導体装置と第２の半導体装置は同一の共通鍵を持つことになり、この共通鍵によりセキュリティの高い通信を可能とするものである。

【００１０】

本発明にかかる暗号通信システムは、第１の半導体装置と第２の半導体装置とを備える。第１の半導体装置は、第１の半導体装置の製造ばらつき等に起因する固有のコードである第１のユニークコードと、第１のユニークコードを訂正するための第１の訂正データとを用いて第１の半導体装置の秘密鍵を生成し、この秘密鍵と平文とを用いて署名データを生成し第２の半導体装置に送信する。第２の半導体装置は、送信された署名データと第１の半導体装置の公開鍵とを用いて検証用データを生成し、当該検証用データと平文とを比較することで、第１の半導体装置が秘密鍵を保有するか否かを判断する。以上の動作により、第１の半導体装置は重要なデータである秘密鍵を直接保持する必要がないため、第１の半導体装置と第２の半導体装置とにおける電子署名の実施において、セキュリティを向上させることができる。

【００１１】

このとき、第１の半導体装置の公開鍵は、第２の半導体装置の製造ばらつき等に起因する固有のコードである第２のユニークコードと、第２のユニークコードを訂正するための第２の訂正データとを用いて生成してもよい。

【００１２】

本発明にかかる暗号通信システムは、第１乃至第３の半導体装置を備える。第３の半導体装置は、第１のユニークコードを訂正するための第１の訂正データを第１の半導体装置に送付し、第１の半導体装置は、第１の半導体装置の製造ばらつき等に起因する固有のコードである第１のユニークコードと、第３の半導体装置から供給された第１の訂正データとを用いて共通鍵を生成する。また、第３の半導体装置は、第２のユニークコードを訂正するための第２の訂正データを第２の半導体装置に送付し、第２の半導体装置は、第２の半導体装置の製造ばらつき等に起因する固有のコードである第２のユニークコードと、第３の半導体装置から供給された第２の訂正データとを用いて共通鍵を生成する。以上の動作により第１の半導体装置と第２の半導体装置は同一の共通鍵を持つことになり、この共通鍵によりセキュリティの高い通信を可能とするものである。

【００１３】

このとき、第３の半導体装置は、各々の半導体装置と、当該各々の半導体装置で生成される各々の共通鍵とに対応づけられた訂正データを格納したデータベースを備えていていもよい。

【００１４】

また、第３の半導体装置は、第１の半導体装置の製造ばらつき等に起因する固有のコードである第１のユニークコードと共通鍵とを用いて第１の訂正データを生成し、第２の半導体装置の製造ばらつき等に起因する固有のコードである第２のユニークコードと共通鍵とを用いて第２の訂正データを生成してもよい。

【００１５】

また、第３の半導体装置は、第１の半導体装置の製造ばらつき等に起因する固有のコードである第１のユニークコードと第１の共通鍵とを用いて第１の訂正データを生成し、第２の半導体装置の製造ばらつき等に起因する固有のコードである第２のユニークコードと第２の共通鍵とを用いて第２の訂正データを生成してもよい。このとき、第１の半導体装

置は第１の共通鍵を保持し、第２の半導体装置は第２の共通鍵を保持し、第３の半導体装置は第１および第２の共通鍵を保持することができる。よって、第１の半導体装置および第３の半導体装置は第１の共通鍵を用いて通信し、第２の半導体装置および第３の半導体装置は第２の共通鍵を用いて通信し、第１の半導体装置および第２の半導体装置は第３の半導体装置を介して通信することができる。

【００１６】

更に、本発明にかかる暗号通信システムは、第１の半導体装置と第２の半導体装置とを備える。第１の半導体装置は、第１の半導体装置の製造ばらつき等に起因する固有のコードである第１のユニークコードと、第１のユニークコードを訂正するための第１の訂正データとを用いて第１の共通鍵を生成する。更に、第１の半導体装置は、第２の半導体装置の製造ばらつき等に起因する固有のコードである第２のユニークコードと第１の共通鍵とを用いて、第２のユニークコードを訂正するための第２の訂正データを生成し、生成された第２の訂正データを第２の半導体装置に送付する。また、第２の半導体装置は、第１の半導体装置で生成された第２の訂正データと第２のユニークコードとを用いて第１の共通鍵を生成する。以上の動作により、第１の半導体装置と第２の半導体装置は同一の共通鍵を保持することができる。よって、第１の半導体装置と第２の半導体装置は、第１の共通鍵を用いてセキュリティの高い通信を実施することができる。

【００１７】

ここで、第２の半導体装置は、第２のユニークコードを第１の半導体装置の公開鍵を用いて暗号化して第１の半導体装置に送付し、第１の半導体装置は、暗号化された第２のユニークコードを第１の半導体装置の秘密鍵を用いて復号してもよい。

【００１８】

また、本発明にかかる暗号通信システムは、各々の半導体装置と、当該各々の半導体装置の公開鍵とを対応づけて格納したデータベースを備えるサーバを有していてもよい。そして、第２の半導体装置は、第２の半導体装置の秘密鍵と平文とを用いて署名データを生成し、この署名データを第１の半導体装置に送付する。第１の半導体装置は、サーバから送付された第２の半導体装置の公開鍵と、第２の半導体装置から送付された署名データとを用いて検証用データを生成し、この検証用データと平文とを比較することで、第２の半導体装置が秘密鍵を保持するか否かを判断することができる。

【００１９】

また、第２の半導体装置は、第１の共通鍵と第２のユニークコードとを用いて第２の訂正データを生成するための訂正データ生成プログラムを、第１の半導体装置の公開鍵を用いて暗号化して、第１の半導体装置に送付してもよい。第１の半導体装置は、暗号化された訂正データ生成プログラムを復号し、復号された訂正データ生成プログラムを実行して、第１の共通鍵と第２のユニークコードとを用いて第２の訂正データを生成してもよい。

【００２０】

また、第１の共通鍵生成部は、第１の半導体装置の製造ばらつき等に起因する固有のコードである第１のユニークコードと、第１のユニークコードを訂正するための第３の訂正データとを用いて第２の共通鍵を生成してもよい。これにより、第１の半導体装置は第１の共通鍵を用いて第２の半導体装置と、第２の共通鍵を用いて第３の半導体装置と通信し、第２の半導体装置は第１の半導体装置を介して第３の半導体装置と通信することができる。

【００２１】

また、本発明にかかる暗号通信システムは、車載用の半導体装置に適用してもよい。

【発明の効果】

【００２２】

本発明により、セキュリティの向上を実現できる暗号通信システムおよび暗号通信方法を提供することができる。また、本発明により、セキュアな通信を実施している暗号通信システムに、半導体装置を容易に追加することができる暗号通信システムおよび暗号通信方法を提供することができる。

【図面の簡単な説明】
【００２３】
【図１】実施の形態１にかかる暗号通信システムを示すブロック図である。
【図２】実施の形態１にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図３】共通鍵生成部の動作を説明するためのフローチャートである。
【図４】共通鍵生成部で処理されるユニークコードの一例を示す表である。
【図５】実施の形態２にかかる暗号通信システムを示すブロック図である。
【図６】実施の形態２にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図７】実施の形態３にかかる暗号通信システムを示すブロック図である。
【図８】実施の形態３にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図９】実施の形態４にかかる暗号通信システムを示すブロック図である。
【図１０】実施の形態４にかかる暗号通信システムのデータベースに格納されているデータの一例を示す表である。
【図１１】実施の形態４にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図１２】実施の形態５にかかる暗号通信システムを示すブロック図である。
【図１３】実施の形態５にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図１４】訂正データ生成部の動作を説明するためのフローチャートである。
【図１５】実施の形態６にかかる暗号通信システムを示すブロック図である。
【図１６】実施の形態６にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図１７】実施の形態１乃至６にかかる暗号通信システムを車載用半導体装置に適用した場合を示すブロック図である。
【図１８】実施の形態８にかかる暗号通信システムを示すブロック図である。
【図１９】実施の形態８にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図２０】共通鍵生成部の動作を説明するためのフローチャートである。
【図２１】共通鍵生成部で処理されるユニークコードの一例を示す表である。
【図２２】訂正データ生成部の動作を説明するためのフローチャートである。
【図２３】複数の半導体装置を用いて訂正データを生成する場合を示す図である。
【図２４】実施の形態９にかかる暗号通信システムを示すブロック図である。
【図２５】実施の形態９にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図２６】実施の形態１０にかかる暗号通信システムを示すブロック図である。
【図２７】実施の形態１０にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図２８】実施の形態１１にかかる暗号通信システムを示すブロック図である。
【図２９】実施の形態１１にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図３０】実施の形態１２にかかる暗号通信システムを示すブロック図である。
【図３１】実施の形態１２にかかる暗号通信システムの動作を説明するためのフローチャートである。
【図３２】実施の形態１２にかかる暗号通信システムの構成を示すブロック図である。
【図３３】実施の形態８乃至１２にかかる暗号通信システムを車載用半導体装置に適用した場合を示すブロック図である。
【発明を実施するための形態】

【００２４】
＜実施の形態１＞
以下、図面を参照して本発明の実施の形態について説明する。
図１は、実施の形態１にかかる暗号通信システムを示すブロック図である。本実施の形態にかかる暗号通信システム１は、半導体装置ＩＣａ（第１の半導体装置）１０と半導体装置ＩＣｂ（第２の半導体装置）２０とを有する。半導体装置１０は、ユニークコード生成部１１、記憶部１２、共通鍵生成部１３、および暗号部１４を有する。
【００２５】
ユニークコード生成部１１は、半導体装置１０に固有の値であってランダムなエラーを含むユニークコード（第１のユニークコード）ＵＣ（ａ）を生成し、共通鍵生成部１３に出力する。ここで、ユニークコードＵＣ（ａ）は、半導体装置１０が備える素子固有の物理的な特性により決まる値である。例えば、ユニークコード生成部１１は、半導体装置１０が備えるメモリ素子の起動時の値を用いてユニークコードＵＣ（ａ）を生成することができる。ユニークコードは、ＩＣの設計は同一であるが実際に製造されるＩＣは個々にばらつきを有するという性質を利用して生成されるコードである。このような技術は、ＰＵＦ（Physical Unclonable Function）と呼ばれ、同一の回路を備えたＩＣを１の半導体ウェハーに複数個同時に同一の製造装置により製造しても、個々のＩＣ毎で固有のコードを得ることができると共に、別のＩＣでの複製を困難にすることができる技術である。この技術を用いることにより、耐タンパチップのような特殊なハードウェアを使用することなく、データの高い秘匿性を実現することができる。
【００２６】
記憶部１２は、例えば、訂正データ（第１の訂正データ）ＣＤ（ａ）、共通鍵生成部１３で生成された共通鍵ＣＫ（ａ）、および半導体装置２０の公開鍵ＰＫ（ｂ）を格納することができる。記憶部１２は、揮発性メモリ（例えば、ＳＲＡＭ）と不揮発性メモリ（例えば、フラッシュメモリ）とを有し、訂正データＣＤ（ａ）および公開鍵ＰＫ（ｂ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部１２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置１０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置１０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。
【００２７】
共通鍵生成部１３は、ユニークコード生成部１１から出力されたユニークコードＵＣ（ａ）と、記憶部１２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する。
【００２８】
ユニークコード生成部１１で生成されるユニークコードＵＣ（ａ）は、ユニークコード生成時の外的要因、例えば、温度、電圧等によって変動するビットの値を含むデータである。このため、ユニークコード生成部１１で生成されるユニークコードＵＣ（ａ）には、（１）値が安定したビット、（２）高確率で変動するビット（つまり、値の変動が比較的大きいビット）、（３）低確率で変動するビット（つまり、値の変動が比較的小さいビット）の３つが含まれる。このように、ユニークコード生成部１１で生成されるユニークコードＵＣ（ａ）は、（２）高確率で変動するビットと（３）低確率で変動するビットとを含む。よって、ユニークコードＵＣ（ａ）は生成される毎に異なる値となる。
【００２９】
高確率で変動するビットは製造工程で把握することができる。よって、製造工程において各ビットを判定することで、高確率で変動するビットをマスクするマスクデータを作成することができる。そして、このマスクデータを用いて、ユニークコード生成部１１で生成されたユニークコードＵＣ（ａ）をマスクすることで、ユニークコードＵＣ（ａ）に含まれる高確率で変動するビットを削除することができる。ここで、高確率で変動するビッ

トの位置は半導体装置毎に異なるため、マスクデータは半導体装置に固有のデータとなる。

【００３０】

低確率で変動するビットは、外的要因や残存する電荷などに起因して変動するため、予め予測することが困難である。このため、低確率で変動するビットは、例えばＢＣＨ符号やリードソロモン符号に代表されるＥＣＣコードを製造時に生成し、このＥＣＣコードを用いて処理をする。以下で、共通鍵生成部１３の動作について具体的に説明する。

【００３１】

図３は、共通鍵生成部１３の動作を説明するためのフローチャートであり、図４は共通鍵生成部１３で処理されるユニークコードの一例を示す表である。まず、共通鍵生成部１３は、ユニークコード生成部１１からユニークコードＵＣ（ａ）を読み込む（ステップＳ１１）。このとき読み込まれたユニークコードＵＣ（ａ）は、値が変動しやすいビットを除外するようなエラー訂正が実施されていないユニークコードである。

【００３２】

次に、訂正データＣＤ（ａ）に含まれるマスクデータを用いて、読み込まれたユニークコードＵＣ（ａ）をマスクする（ステップＳ１２）。ここで、マスクデータは、ユニークコードＵＣ（ａ）のビットのうちビットの値が変動するようなエラー率の高いビットをマスクするためのデータである。図４に示す例では、ユニークコードＵＣ（ａ）の１ビット目と６ビット目のビットのエラー率が高いため、マスクデータが"０"となっている。これ以外のビットは、エラー率が低いビットまたは値が安定しているビットであるため、マスクデータが"１"となっている。つまり、マスクが必要なビットのマスクデータは"０"となり、マスクが不要なビットのマスクデータは"１"となる。そして、マスクデータを用いてユニークコードＵＣ（ａ）をマスクすることで、ユニークコードＵＣ（ａ）の１ビット目と６ビット目のビットを削除したマスク処理後のユニークコードＵＣ（ａ）'を得ることができる（マスク処理により削除したビットは"Ｘ"で示している）。その後、マスク処理後のユニークコードＵＣ（ａ）'は左詰めされる。

【００３３】

次に、訂正データＣＤ（ａ）に含まれるＥＣＣコード（エラー訂正コード）を用いて、マスク処理後のユニークコードＵＣ（ａ）'に含まれる値の変動率が低いビットのエラーを除去する訂正をすることによりユニークコードＵＣ（ａ）''を得る（ステップＳ１３）。図４に示す例では、ＥＣＣコードを用いてマスク処理後のユニークコードＵＣ（ａ）'を処理することにより、１ビット目のビットが"０"から"１"に訂正されている。

【００３４】

次に、訂正データＣＤ（ａ）に含まれる演算パラメータを用いて、エラー訂正後のユニークコードＵＣ（ａ）''に所定の演算を実施する（ステップＳ１４）。図４に示す例では、エラー訂正後のユニークコードＵＣ（ａ）''にＮＯＴ演算を実施している。この演算処理後のユニークコードＵＣ（ａ）鍵ＣＫ（ａ）となる。なお、ＮＯＴ演算は一例であり、エラー訂正後のユニークコードＵＣ（ａ）''に実施する演算はどのような演算であってもよい。この演算パラメータを変更することで、必要に応じて共通鍵ＣＫ（ａ）を変更することができる。また、演算パラメータを用いてエラー訂正後のユニークコードＵＣ（ａ）''に所定の演算を実施することで、共通鍵ＣＫ（ａ）をユニークコードＵＣ（ａ）と見かけ上類似しないコードとすることができる。よって、セキュリティレベルを更に向上させることができる。また、エラー訂正後のユニークコードＵＣ（ａ）''に実施する演算は省略することもできる。この場合は、マスクデータおよびＥＣＣコードを用いて処理されたユニークコードＵＣ（ａ）''が、共通鍵ＣＫ（ａ）となる。このようにして生成された共通鍵ＣＫ（ａ）は、記憶部１２および暗号部１４に出力される。

【００３５】

なお、訂正データＣＤ（ａ）に含まれるマスクコード、ＥＣＣコード、および演算パラメータは、半導体装置１０の固有データとして予め生成されて記憶部１２に格納されている。訂正データＣＤ（ａ）の生成方法については後述する（実施の形態５、図１４参照）

。またＥＣＣコードは、ユニークコード生成部１１から読み出したユニークコードＵＣ（ａ）に含まれる値の変動率が高いビットを抽出するために、複数回のユニークコードＵＣ（ａ）の読出し動作を行った後、マスク処理後のユニークコードＵＣ（ａ）'を基にＥＣＣコードが生成される。

【００３６】

以上で説明したように、共通鍵生成部１３は共通鍵ＣＫ（ａ）を生成する機能を有すると同時に、訂正データＣＤ（ａ）を用いてユニークコードＵＣ（ａ）を訂正する機能も有する。図１に示す秘密鍵生成部２３、図５に示す秘密鍵生成部３３、図７に示す秘密鍵生成部５３、公開鍵生成部６３、図９に示す共通鍵生成部７３、８３、図１２に示す共通鍵生成部１１３、１２３、図１５に示す共通鍵生成部１４３、１５３も同様に、訂正データＣＤを用いてユニークコードＵＣを訂正するユニークコード訂正部として機能する。なお、本願明細書では、便宜上、生成される鍵毎に共通鍵生成部、秘密鍵生成部、公開鍵生成部と表現しているが、これらの構成および動作は基本的には同様である。

【００３７】

共通鍵ＣＫ（ａ）は使い捨て(ワンタイム)鍵とする、または固定鍵とすることのいずれかが用途により決定される。例えば不揮発性メモリにデータを暗号化して格納するための固定鍵とするのであれば、半導体装置１０のユニークコードＵＣ（ａ)として得られるビットパターンから共通鍵ＣＫ（ａ）としてのビットパターンを得られるように訂正データＣＤ(ａ)を決定すればよいため、複数の訂正データＣＤ（ａ）を作っておくことも容易である。またＩＣａとＩＣｂとの間での通信セッションごとに用いる使い捨て鍵とする場合は、複数の訂正データＣＤ（ａ）毎に異なるビットパターンを得られるように訂正データＣＤ（ａ）を決定すればよい。

【００３８】

図１の暗号部１４は、共通鍵生成部１３で生成された共通鍵ＣＫ（ａ）を半導体装置２０の公開鍵ＰＫ（ｂ）を用いて暗号化する。ここで、暗号化に用いられる公開鍵ＰＫ（ｂ）は、予め半導体装置２０から半導体装置１０に送付されて記憶部１２に格納されていてもよい。また、暗号化に用いられる公開鍵ＰＫ（ｂ）は、暗号部１４で共通鍵ＣＫ（ａ）を暗号化する際に、半導体装置２０から暗号部１４に直接供給されるように構成してもよい。

【００３９】

半導体装置２０は、ユニークコード生成部２１、記憶部２２、秘密鍵生成部２３、および復号部２４を有する。ユニークコード生成部２１は、半導体装置２０に固有の値であってランダムなエラーを含むユニークコード（第２のユニークコード）ＵＣ（ｂ）を生成し、秘密鍵生成部２３に出力する。なお、ユニークコード生成部２１の構成および動作は、上記で説明したユニークコード生成部１１と基本的に同様である。

【００４０】

記憶部２２は、訂正データ（第２の訂正データ）ＣＤ（ｂ）、公開鍵ＰＫ（ｂ）、および復号部で復号された共通鍵ＣＫ（ａ）を格納することができる。記憶部２２は、例えば揮発性メモリと不揮発性メモリとを有し、訂正データＣＤ（ｂ）および公開鍵ＰＫ（ｂ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部２２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置２０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【００４１】

秘密鍵生成部２３は、ユニークコードＵＣ（ｂ）と訂正データＣＤ（ｂ）とを用いて半導体装置２０の秘密鍵ＳＫ（ｂ）を生成する。なお、秘密鍵生成部２３において秘密鍵ＳＫ（ｂ）を生成する方法は、上記共通鍵生成部１３が共通鍵ＣＫ（ａ）を生成する方法と基本的に同様である。

【００４２】
復号部２４は、半導体装置１０の暗号部１４で暗号化された共通鍵ＣＫ（ａ）'を秘密鍵ＳＫ（ｂ）を用いて復号して共通鍵ＣＫ（ａ）を生成する。
【００４３】
次に、本実施の形態にかかる暗号通信システムの動作について、図２に示すフローチャートを用いて説明する。まず、半導体装置ＩＣｂ（２０）は、半導体装置ＩＣａ（１０）に半導体装置ＩＣｂ（２０）の公開鍵ＰＫ（ｂ）を送付する（ステップＳ１）。送付された公開鍵ＰＫ（ｂ）は、半導体装置１０の記憶部１２に格納される。次に、半導体装置１０の共通鍵生成部１３は、ユニークコード生成部１１から出力されたユニークコードＵＣ（ａ）と、記憶部１２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ２）。暗号部１４は、共通鍵生成部１３で生成された共通鍵ＣＫ（ａ）を半導体装置２０の公開鍵ＰＫ（ｂ）を用いて暗号化して、暗号化された共通鍵ＣＫ（ａ）'を生成する（ステップＳ３）。その後、半導体装置１０から半導体装置２０に暗号化された共通鍵ＣＫ（ａ）'が送付される（ステップＳ４）。
【００４４】
半導体装置２０の秘密鍵生成部２３は、ユニークコードＵＣ（ｂ）と訂正データＣＤ（ｂ）とを用いて、半導体装置２０の秘密鍵ＳＫ（ｂ）を生成する（ステップＳ５）。復号部２４は、暗号化された共通鍵ＣＫ（ａ）'を秘密鍵ＳＫ（ｂ）を用いて復号して共通鍵ＣＫ（ａ）を生成する（ステップＳ６）。上記処理により、半導体装置１０と半導体装置２０は共に共通鍵ＣＫ（ａ）を保持することができる。よって、半導体装置１０および半導体装置２０は共通鍵ＣＫ（ａ）を用いて暗号通信することが可能となる（ステップＳ７）。なお、上記各ステップは矛盾がない限り適宜順番を変更することができる。例えば、半導体装置１０がステップＳ２とＳ３を実施するのと並行して、半導体装置２０においてステップＳ５を実施してもよい。
【００４５】
本発明の課題で説明したように、半導体装置ＩＣｘと半導体装置ＩＣｙとの間で共通鍵ＣＫ（ｘ）を用いて暗号通信を実施する場合、ＩＣｘとＩＣｙとで共通鍵ＣＫ（ｘ）を共有する必要がある。ＩＣｘが共通鍵ＣＫ（ｘ）を保有している場合、ＩＣｘは予め取得したＩＣｙの公開鍵ＰＫ（ｙ）を用いて共通鍵ＣＫ（ｘ）を暗号化し、暗号化された共通鍵ＣＫ（ｘ）'をＩＣｙへ送付する。そして、ＩＣｙは、ＩＣｙの秘密鍵ＳＫ（ｙ）を用いて、暗号化された共通鍵ＣＫ（ｘ）'を復号することで、共通鍵ＣＫ（ｘ）を取得することができる。このように、公開鍵暗号方式を用いてＩＣｘからＩＣｙへ共通鍵ＣＫ（ｘ）を送付することで、第三者に知られることなくＩＣｘとＩＣｙとで共通鍵ＣＫ（ｘ）を共有することができる。これにより、ＩＣｘとＩＣｙとの間で共通鍵暗号方式を用いて暗号通信を実施することができる。
【００４６】
ＩＣｘからＩＣｙへ共通鍵ＣＫ（ｘ）を送付する際は、共通鍵ＣＫ（ｘ）が暗号化されているため、共通鍵ＣＫ（ｘ）の情報が漏洩することはない。しかしながら、半導体装置（半導体チップ）ＩＣｘ、ＩＣｙの不揮発性メモリ（記憶部）には共通鍵ＣＫ（ｘ）や秘密鍵ＳＫ（ｙ）などの重要なデータが格納されている。このため、半導体装置が不正に解析されると、共通鍵ＣＫ（ｘ）や秘密鍵ＳＫ（ｙ）などの重要なデータが漏洩してしまうという問題があった。
【００４７】
これに対して、本実施の形態にかかる暗号通信システムでは、半導体装置１０の共通鍵生成部１３において、半導体装置１０に固有の情報成分と変動性のある情報成分とを含むユニークコードＵＣ（ａ）と、当該ユニークコードＵＣ（ａ）を訂正する訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成している。また、半導体装置２０の秘密鍵生成部２３において、半導体装置２０に固有の情報成分と変動性のある情報成分とを含むユニークコードＵＣ（ｂ）と、当該ユニークコードＵＣ（ｂ）を訂正する訂正データＣＤ（ｂ）とを用いて、半導体装置２０の秘密鍵ＳＫ（ｂ）を生成している。よって、共通鍵ＣＫ

（ａ）や秘密鍵ＳＫ（ｂ）などの重要なデータを記憶部１２、２２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（ａ）や秘密鍵ＳＫ（ｂ）などの重要なデータが漏洩することはない。

【００４８】

また秘密鍵ＳＫ（ｂ）は公開鍵ＰＫ（ｂ）に対応した鍵であることが必要であるが、半導体装置２０のユニークコードＵＣ（ｂ）として得られるビットパターンから秘密鍵ＳＫ（ｂ）としてのビットパターンを得られるように訂正データＣＤ（ｂ）を決定すればよいため、複数の訂正データＣＤ（ｂ）を作っておくことも容易である。

【００４９】

半導体装置を解析して不正にデータを取得する方法としては、以下のような方法がある。

（１）半導体装置をＦＩＢ（Focused Ion Beam）を用いて加工し、プローブを用いて半導体装置を物理的に解析する方法。

（２）半導体装置にレーザなどの電磁波を照射したり、電源端子にノイズを挿入したりすることでＣＰＵを暴走させて不正にデータを取得するフォルトツリー解析。

（３）半導体装置の消費電流量を観測し、鍵データを解析するリーク解析。

【００５０】

このような不正な解析を回避するために、高いセキュリティレベルが必要な分野では、セキュリティレベルの高いマイコン（以下、セキュアマイコンという）が用いられている。このセキュアマイコンには、配線領域へのシールド、光や信号ノイズを検出する機能、信号に乱数信号を組み合わせて電流をかく乱する機能などが実装されている。すなわち、上述のリーク解析による鍵データの不正取得では、特定のデータに基づく一定の演算を行うことで生じる消費電力の特徴パターンを抽出することから、複数の訂正データＣＤ（ａ）やＣＤ（ｂ）から乱数等により適宜に選択するように構成することで、消費電力の特徴パターンをかく乱することが可能となる。

【００５１】

このように、セキュアマイコンを用いることで第三者が不正に半導体装置を解析することを防止することができる。しかしながら、セキュアマイコンを用いた場合は、不正解析を防止できる反面、その耐タンパ性により半導体装置メーカー等が不良解析や故障解析を実施することができなくなるという問題があった。特に、自動車に用いられる車載用のマイコン（ＥＣＵ等）では、高信頼性が必要であるため、半導体装置の不良解析や故障解析が必要となる。このような理由から、車載用のマイコンにはセキュアマイコンよりもセキュリティレベルが低い汎用のマイコン（以下、汎用マイコンという）が広く用いられてきた。したがって、車載用のマイコンでは、汎用マイコンを使用しつつ、半導体装置のセキュリティレベルを向上させることが可能な暗号通信システムが必要とされていた。

【００５２】

本実施の形態にかかる暗号通信システムでは、共通鍵ＣＫ（ａ）や秘密鍵ＳＫ（ｂ）などの重要なデータを記憶部１２、２２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（ａ）や秘密鍵ＳＫ（ｂ）などの重要なデータが漏洩することはない。このため、半導体装置１０および半導体装置２０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。

【００５３】

なお、共通鍵ＣＫ（ａ）や秘密鍵ＳＫ（ｂ）を生成するために使用される訂正データＣＤ（ａ）、ＣＤ（ｂ）は、共通鍵ＣＫ（ａ）や秘密鍵ＳＫ（ｂ）よりもセキュリティレベルは低いが、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ａ）、ＣＤ（ｂ）が第三者に漏洩することを防ぐために、訂正データＣＤ（ａ）、ＣＤ（ｂ）が格納される半導体装置１０、２０にセキュアマイコンを使用してもよい。

【００５４】

以上で説明したように、本実施の形態にかかる発明により、セキュリティの向上を実現

できる暗号通信システムおよび暗号通信方法を提供することができる。

【００５５】

＜実施の形態２＞

次に、本発明の実施の形態２について説明する。図５は、本実施の形態にかかる暗号通信システム２を示すブロック図である。本実施の形態では、暗号通信システムを電子署名方式に適用している。本実施の形態にかかる暗号通信システム２は、半導体装置ＩＣａ（３０）と半導体装置ＩＣｂ（４０）とを有する。半導体装置３０は、ユニークコード生成部３１、記憶部３２、秘密鍵生成部３３、および署名データ生成部３４を有する。

【００５６】

ユニークコード生成部３１は、半導体装置３０に固有のユニークコードＵＣ（ａ）を生成し、秘密鍵生成部３３に出力する。ユニークコード生成部３１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。

【００５７】

記憶部３２は、訂正データＣＤ（ａ）、平文Ｐｌａｎｅ（ａ）、および半導体装置３０の公開鍵ＰＫ（ａ）を不揮発性メモリに格納することができる。

【００５８】

秘密鍵生成部３３は、ユニークコード生成部３１から出力されたユニークコードＵＣ（ａ）と、記憶部３２に格納されている訂正データＣＤ（ａ）とを用いて、半導体装置３０の秘密鍵ＳＫ（ａ）を生成する。ここで、秘密鍵生成部３３はユニークコード訂正部として機能する。秘密鍵生成部３３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。

【００５９】

署名データ生成部３４は、秘密鍵生成部３３で生成された秘密鍵ＳＫ（ａ）と、記憶部３２に格納されている平文Ｐｌａｎｅ（ａ）とを用いて署名データＳｉｇ（ａ）を生成する。つまり、署名データ生成部３４は電子署名方式における署名生成アルゴリズムを実行する。

【００６０】

半導体装置４０は、記憶部４１と検証部４２とを有する。記憶部４１は、半導体装置３０の公開鍵ＰＫ（ａ）を格納することができる。検証部４２は、電子署名方式の検証アルゴリズムを実行する。すなわち、検証部４２は、署名データＳｉｇ（ａ）と半導体装置３０の公開鍵ＰＫ（ａ）とを用いて検証用データを生成する。ここで、署名データＳｉｇ（ａ）は、半導体装置３０の秘密鍵ＳＫ（ａ）を用いて平文Ｐｌａｎｅ（ａ）を暗号化することで生成されたデータである。よって、署名データＳｉｇ（ａ）を半導体装置３０の公開鍵ＰＫ（ａ）を用いて復号することで得られた検証用データは、半導体装置３０から送られた平文Ｐｌａｎｅ（ａ）に対応するデータである。したがって、検証部４２は、検証用データと平文Ｐｌａｎｅ（ａ）とを比較し、検証用データと平文Ｐｌａｎｅ（ａ）とが一致した場合は、半導体装置３０が秘密鍵ＳＫ（ａ）を保有すると判断することができる。なお、半導体装置３０から供給される公開鍵ＰＫ（ａ）は、半導体装置４０の検証部４２に直接供給されるように構成してもよい。

【００６１】

次に、本実施の形態にかかる暗号通信システムの動作について、図６に示すフローチャートを用いて説明する。まず、半導体装置３０（署名者に対応する）は、半導体装置４０（検証者に対応する）に半導体装置３０の公開鍵ＰＫ（ａ）を送付する（ステップＳ２１）。

【００６２】

次に、半導体装置３０の秘密鍵生成部３３は、ユニークコード生成部３１から出力されたユニークコードＵＣ（ａ）と、記憶部３２に格納されている訂正データＣＤ（ａ）とを用いて、半導体装置３０の秘密鍵ＳＫ（ａ）を生成する（ステップＳ２２）。次に、半導体装置３０の署名データ生成部３４は、電子署名方式における署名生成アルゴリズムを実

行する。つまり、署名データ生成部３４は、秘密鍵生成部３３で生成された秘密鍵ＳＫ（ａ）と、記憶部３２に格納されている平文Ｐｌａｎｅ（ａ）とを用いて署名データＳｉｇ（ａ）を生成する（ステップＳ２３）。

【００６３】

署名データ生成部３４で生成された署名データＳｉｇ（ａ）は、半導体装置４０の検証部４２に送付される（ステップＳ２４）。また、平文Ｐｌａｎｅ（ａ）は、半導体装置４０の検証部４２に送付される（ステップＳ２５）。なお、図５では、平文Ｐｌａｎｅ（ａ）が記憶部３２に格納されている場合を示したが、平文Ｐｌａｎｅ（ａ）が外部から直接署名データ生成部３４および検証部４２に供給されるように構成してもよい。

【００６４】

半導体装置４０の検証部４２は、電子署名方式の検証アルゴリズムを実行する。すなわち、検証部４２は、署名データＳｉｇ（ａ）と半導体装置３０の公開鍵ＰＫ（ａ）とを用いて検証用データを生成し、当該検証用データと平文Ｐｌａｎｅ（ａ）とを比較する（ステップＳ２６）。そして、検証用データと平文Ｐｌａｎｅ（ａ）とが一致した場合（検証アルゴリズムが署名データＳｉｇ（ａ）を受理した場合）は、検証部４２は半導体装置３０が作成した署名データＳｉｇ（ａ）が正当であると判断する。つまり、半導体装置３０が秘密鍵ＳＫ（ａ）を保有すると判断される。一方、検証用データと平文Ｐｌａｎｅ（ａ）とが一致しない場合（検証アルゴリズムが署名データＳｉｇ（ａ）を棄却した場合）は、検証部４２は半導体装置３０が作成した署名データＳｉｇ（ａ）が不当であると判断する。つまり、半導体装置３０が秘密鍵ＳＫ（ａ）を保有しないと判断される。なお、上記各ステップは矛盾がない限り適宜順番を変更することができる。

【００６５】

一般的に、半導体装置ＩＣｘ（署名者に対応する）と半導体装置ＩＣｙ（検証者に対応する）との間で電子署名方式を用いた検証を実施する場合、ＩＣｘは秘密鍵ＳＫ（ｘ）を保持している必要がある。この秘密鍵ＳＫ（ｘ）は半導体装置ＩＣｘの不揮発性メモリ（記憶部）に格納されている。このため、半導体装置が不正に解析されると秘密鍵ＳＫ（ｘ）などの重要なデータが漏洩してしまうという問題があった。

【００６６】

これに対して、本実施の形態にかかる暗号通信システムでは、半導体装置３０の秘密鍵生成部３３において、半導体装置３０に固有のユニークコードＵＣ（ａ）と記憶部３２に格納されている訂正データＣＤ（ａ）とを用いて、半導体装置３０の秘密鍵ＳＫ（ａ）を生成している。よって、重要なデータである秘密鍵ＳＫ（ａ）を記憶部３２に直接格納していないため、半導体装置が不正に解析されたとしても、秘密鍵ＳＫ（ａ）が漏洩することはない。このため、半導体装置３０および半導体装置４０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。なお、半導体装置３０および半導体装置４０で構成される暗号通信システムのセキュリティレベルを更に向上させるために、半導体装置３０、４０にセキュアマイコンを使用してもよい。

【００６７】

以上で説明したように、本実施の形態にかかる発明により、セキュリティの向上を実現できる暗号通信システムおよび暗号通信方法を提供することができる。

【００６８】

＜実施の形態３＞

次に、本発明の実施の形態３について説明する。図７は、本実施の形態にかかる暗号通信システム３を示すブロック図である。本実施の形態では、暗号通信システムを電子署名方式に適用している。また、実施の形態２にかかる暗号通信システム２では、ステップＳ２１において半導体装置３０の公開鍵ＰＫ（ａ）を半導体装置４０に送付していたが、本実施の形態にかかる暗号通信システム３では公開鍵生成部６３を用いて半導体装置５０の公開鍵ＰＫ（ａ）を生成している。

【００６９】

図７に示す本実施の形態にかかる暗号通信システム３は、半導体装置ＩＣａ（５０）と半導体装置ＩＣｂ（６０）とを有する。半導体装置５０は、ユニークコード生成部５１、記憶部５２、秘密鍵生成部５３、および署名データ生成部５４を有する。

【００７０】

ユニークコード生成部５１は、半導体装置５０に固有のユニークコードＵＣ（ａ）を生成し、秘密鍵生成部５３に出力する。ユニークコード生成部５１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。

【００７１】

記憶部５２は、訂正データＣＤ（ａ）および平文Ｐｌａｎｅ（ａ）を不揮発性メモリに格納することができる。

【００７２】

秘密鍵生成部５３は、ユニークコード生成部５１から出力されたユニークコードＵＣ（ａ）と、記憶部５２に格納されている訂正データＣＤ（ａ）とを用いて、半導体装置５０の秘密鍵ＳＫ（ａ）を生成する。ここで、秘密鍵生成部５３はユニークコード訂正部として機能する。秘密鍵生成部５３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。

【００７３】

署名データ生成部５４は、秘密鍵生成部５３で生成された秘密鍵ＳＫ（ａ）と、記憶部５２に格納されている平文Ｐｌａｎｅ（ａ）とを用いて署名データＳｉｇ（ａ）を生成する。つまり、署名データ生成部５４は電子署名方式における署名生成アルゴリズムを実行する。

【００７４】

半導体装置６０は、ユニークコード生成部６１、記憶部６２、公開鍵生成部６３、および検証部６４を有する。ユニークコード生成部６１は、半導体装置６０に固有のユニークコードＵＣ（ｂ）を生成し、公開鍵生成部６３に出力する。ユニークコード生成部６１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。

【００７５】

記憶部６２は、訂正データＣＤ（ｂ）を不揮発性メモリに格納することができる。

【００７６】

公開鍵生成部６３は、ユニークコード生成部６１から出力されたユニークコードＵＣ（ｂ）と、記憶部６２に格納されている訂正データＣＤ（ｂ）とを用いて半導体装置５０の公開鍵ＰＫ（ａ）を生成する。ここで、公開鍵生成部６３はユニークコード訂正部として機能する。公開鍵生成部６３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。

【００７７】

検証部６４は、電子署名方式の検証アルゴリズムを実行する。すなわち、検証部６４は、署名データＳｉｇ（ａ）と半導体装置５０の公開鍵ＰＫ（ａ）とを用いて検証用データを生成する。ここで、署名データＳｉｇ（ａ）は、半導体装置５０の秘密鍵ＳＫ（ａ）を用いて平文Ｐｌａｎｅ（ａ）を暗号化することで生成されたデータである。よって、署名データＳｉｇ（ａ）を半導体装置５０の公開鍵ＰＫ（ａ）を用いて復号することで得られた検証用データは、半導体装置５０から送られた平文Ｐｌａｎｅ（ａ）に対応するデータである。したがって、検証部６４は、検証用データと平文Ｐｌａｎｅ（ａ）とを比較し、検証用データと平文Ｐｌａｎｅ（ａ）とが一致した場合は、半導体装置５０が秘密鍵ＳＫ（ａ）を保有すると判断することができる。

【００７８】

次に、本実施の形態にかかる暗号通信システムの動作について、図８に示すフローチャートを用いて説明する。まず、半導体装置５０（署名者に対応する）の秘密鍵生成部５３は、ユニークコード生成部５１から出力されたユニークコードＵＣ（ａ）と、記憶部５２

に格納されている訂正データＣＤ（ａ）とを用いて、半導体装置５０の秘密鍵ＳＫ（ａ）を生成する（ステップＳ３１）。次に、半導体装置５０の署名データ生成部５４は、電子署名方式における署名生成アルゴリズムを実行する。つまり、署名データ生成部５４は、秘密鍵生成部５３で生成された秘密鍵ＳＫ（ａ）と、記憶部５２に格納されている平文Ｐｌａｎｅ（ａ）とを用いて署名データＳｉｇ（ａ）を生成する（ステップＳ３２）。

【００７９】

一方、半導体装置６０（検証者に対応する）の公開鍵生成部６３は、ユニークコード生成部６１から出力されたユニークコードＵＣ（ｂ）と、記憶部６２に格納されている訂正データＣＤ（ｂ）とを用いて半導体装置５０の公開鍵ＰＫ（ａ）を生成する（ステップＳ３３）。

【００８０】

署名データ生成部５４で生成された署名データＳｉｇ（ａ）は、半導体装置６０の検証部６４に送付される（ステップＳ３４）。また、平文Ｐｌａｎｅ（ａ）は、半導体装置６０の検証部６４に送付される（ステップＳ３５）。なお、図７では、平文Ｐｌａｎｅ（ａ）が記憶部５２に格納されている場合を示したが、平文Ｐｌａｎｅ（ａ）は外部から直接署名データ生成部５４および検証部６４に供給されるように構成してもよい。

【００８１】

半導体装置６０の検証部６４は、電子署名方式の検証アルゴリズムを実行する。すなわち、検証部６４は、署名データＳｉｇ（ａ）と半導体装置５０の公開鍵ＰＫ（ａ）とを用いて検証用データを生成し、当該検証用データと平文Ｐｌａｎｅ（ａ）とを比較する（ステップＳ３６）。そして、検証用データと平文Ｐｌａｎｅ（ａ）とが一致した場合（検証アルゴリズムが署名データＳｉｇ（ａ）を受理した場合）は、検証部６４は半導体装置５０が作成した署名データＳｉｇ（ａ）が正当であると判断する。つまり、半導体装置５０が秘密鍵ＳＫ（ａ）を保有すると判断される。一方、検証用データと平文Ｐｌａｎｅ（ａ）とが一致しない場合（検証アルゴリズムが署名データＳｉｇ（ａ）を棄却した場合）は、検証部６４は半導体装置５０が作成した署名データＳｉｇ（ａ）が不当であると判断する。つまり、半導体装置５０が秘密鍵ＳＫ（ａ）を保有しないと判断される。なお、上記各ステップは矛盾がない限り適宜順番を変更することができる。

【００８２】

本実施の形態にかかる暗号通信システムにおいても、半導体装置５０の秘密鍵生成部５３において、半導体装置５０に固有のユニークコードＵＣ（ａ）と訂正データＣＤ（ａ）とを用いて、半導体装置５０の秘密鍵ＳＫ（ａ）を生成している。よって、重要なデータである秘密鍵ＳＫ（ａ）を記憶部５２に直接格納していないため、半導体装置が不正に解析されたとしても、重要なデータである秘密鍵ＳＫ（ａ）が漏洩することはない。このため、半導体装置５０および半導体装置６０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。

【００８３】

更に、本実施の形態にかかる暗号通信システムでは、半導体装置６０の公開鍵生成部６３において、ユニークコードＵＣ（ｂ）と訂正データＣＤ（ｂ）とを用いて半導体装置５０の公開鍵ＰＫ（ａ）を生成している。よって、半導体装置５０から半導体装置６０に公開鍵ＰＫ（ａ）を送付する必要がないため、使用している暗号方式が第三者に漏れることを防ぐことができ、暗号通信システムのセキュリティを更に向上させることができる。なお、半導体装置５０および半導体装置６０で構成される暗号通信システムのセキュリティレベルを更に向上させるために、半導体装置５０、６０にセキュアマイコンを使用してもよい。

【００８４】

＜実施の形態４＞

次に、本発明の実施の形態４について説明する。上記で説明した実施の形態１乃至３では、共通鍵や秘密鍵を生成するために使用される訂正データＣＤ（ａ）、ＣＤ（ｂ）を半導体装置に格納していた。しかしながら、共通鍵や秘密鍵を生成するために使用される訂

正データＣＤ（ａ）、ＣＤ（ｂ）もセキュリティレベルの高い情報である。よって、訂正データＣＤ（ａ）、ＣＤ（ｂ）が第三者に漏洩しないような暗号通信システムを構成することが好ましい。

【００８５】

図９に示す本実施の形態にかかる暗号通信システム４では、共通鍵を生成するために使用される訂正データを各半導体装置７０、８０に格納するのではなく、訂正データを一括して管理するデータベース９１を有する半導体装置９０を設けている。ここで、半導体装置９０のデータベース９１にはセキュリティレベルの高い訂正データが格納されているので、セキュアマイコンを用いて半導体装置９０を構成することが好ましい。一方、半導体装置７０、８０では、セキュリティレベルの高い共通鍵ＣＫ（１）の情報が不揮発性メモリに格納されないので、汎用マイコンを用いて構成することができる。つまり、記憶部７２、８２には一時的に共通鍵ＣＫ（１）が格納されるが、共通鍵ＣＫ（１）は揮発性メモリに格納されているため、半導体装置７０、８０の電源がオフになると共通鍵ＣＫ（１）の情報は消去される。よって、半導体装置７０、８０にはセキュリティレベルの高い共通鍵ＣＫ（１）は保持されない。以下、本実施の形態にかかる暗号通信システムについて詳細に説明する。

【００８６】

図９に示す暗号通信システム４は、半導体装置７０、８０、９０を有する。半導体装置（第１の半導体装置）７０は、ユニークコード生成部７１、記憶部７２、および共通鍵生成部（第１の共通鍵生成部）７３を有する。

【００８７】

ユニークコード生成部７１は、半導体装置７０に固有のユニークコードＵＣ（ａ）を生成し、共通鍵生成部７３に出力する。ユニークコード生成部７１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。

【００８８】

記憶部７２は、共通鍵生成部７３で生成された共通鍵ＣＫ（１）を揮発性メモリに格納する。共通鍵ＣＫ（１）は、半導体装置７０の電源がオフになると消去される。尚、共通鍵ＣＫ（１）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（１）に対して、半導体装置７０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【００８９】

共通鍵生成部７３は、ユニークコード生成部７１から出力されたユニークコードＵＣ（ａ）と、半導体装置９０から供給された訂正データ（第１の訂正データ）ＣＤ（１、ａ）とを用いて共通鍵ＣＫ（１）を生成する。ここで、共通鍵生成部７３はユニークコード訂正部として機能する。共通鍵生成部７３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。

【００９０】

半導体装置（第２の半導体装置）８０は、ユニークコード生成部８１、記憶部８２、および共通鍵生成部（第２の共通鍵生成部）８３を有する。

【００９１】

ユニークコード生成部８１は、半導体装置８０に固有のユニークコードＵＣ（ｂ）を生成し、共通鍵生成部８３に出力する。ユニークコード生成部８１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。

【００９２】

記憶部８２は、共通鍵生成部８３で生成された共通鍵ＣＫ（１）を揮発性メモリに格納する。共通鍵ＣＫ（１）は、半導体装置８０の電源がオフになると消去される。尚、共通鍵ＣＫ（１）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（１）に対して、半導体装置８０の電

源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【００９３】

共通鍵生成部８３は、ユニークコード生成部８１から出力されたユニークコードＵＣ（ｂ）と、半導体装置９０から供給された訂正データ（第２の訂正データ）ＣＤ（１、ｂ）とを用いて共通鍵ＣＫ（１）を生成する。ここで、共通鍵生成部８３はユニークコード訂正部として機能する。共通鍵生成部８３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。

【００９４】

半導体装置（第３の半導体装置）９０は、訂正データが格納されたデータベース９１を有する。図１０は、データベース９１が有するデータの一例を示す表である。図１０に示すように、データベース９１には、半導体装置の情報（ＩＣａ、ＩＣｂ、ＩＣｃ、・・・、ＩＣｚ）と半導体装置で生成される公開鍵（ＣＫ（１）、ＣＫ（２）、ＣＫ（３）、・・・、ＣＫ（ｎ））とに対応づけられた訂正データ（ＣＤ（１、ａ）、ＣＤ（１、ｂ）、・・・）が格納されている。

【００９５】

例えば、共通鍵ＣＫ（１）を半導体装置ＩＣａで生成する場合は、訂正データＣＤ（１、ａ）を半導体装置ＩＣａに送付する。また、共通鍵ＣＫ（１）を半導体装置ＩＣｂで生成する場合は、訂正データＣＤ（１、ｂ）を半導体装置ＩＣｂに送付する。同様に、例えば、共通鍵ＣＫ（３）を半導体装置ＩＣａで生成する場合は、訂正データＣＤ（３、ａ）を半導体装置ＩＣａに送付する。また、共通鍵ＣＫ（３）を半導体装置ＩＣｂで生成する場合は、訂正データＣＤ（３、ｂ）を半導体装置ＩＣｂに送付する。

【００９６】

本実施の形態にかかる暗号通信システムでは、ユニークコードＵＣ（ａ）、ＵＣ（ｂ）が異なる場合であっても、演算パラメータ（実施の形態１参照）を用いてエラー訂正後のユニークコードＵＣ（ａ）''、ＵＣ（ｂ）''にそれぞれ異なる演算を実施することで、同じ共通鍵ＣＫ（１）を生成することができる。

【００９７】

また、共通鍵ＣＫは、訂正データＣＤの演算パラメータを変更することで変えることができる。つまり、訂正データＣＤの演算パラメータを変更することで、図１０に示す共通鍵ＣＫ（１）、ＣＫ（２）、ＣＫ（３）、・・・、ＣＫ（ｎ）のように、複数の共通鍵を生成することができる。よって、本実施の形態にかかる暗号通信システムでは、半導体装置９０から半導体装置７０、８０に送付する訂正データＣＤを定期的に変更することで、半導体装置７０、８０の共通鍵ＣＫを容易に変更することができ、セキュリティレベルを容易に向上させることができる。

【００９８】

なお、半導体装置９０から半導体装置７０、８０に送付される訂正データＣＤはセキュリティレベルの高い情報であるので、訂正データＣＤを半導体装置７０、８０に送付する際は、公開鍵暗号方式を用いて訂正データＣＤを暗号化して送付してもよい。この場合は、例えば半導体装置７０が半導体装置７０の秘密鍵を保持し、半導体装置９０が訂正データＣＤ（１、ａ）を送付する際に半導体装置７０の公開鍵で訂正データＣＤ（１、ａ）を暗号化する。そして、半導体装置７０が暗号化された訂正データＣＤ（１、ａ）を秘密鍵を用いて復号することで、半導体装置９０から半導体装置７０に暗号化して訂正データを送付することができる。

【００９９】

次に、本実施の形態にかかる暗号通信システム４の動作について、図１１に示すフローチャートを用いて説明する。まず、半導体装置ＩＣｓ（９０）は半導体装置ＩＣａ（７０）に訂正データＣＤ（１、ａ）を送付する（ステップＳ４１）。次に、半導体装置７０の共通鍵生成部７３は、ユニークコード生成部７１から出力されたユニークコードＵＣ（ａ）と、半導体装置９０から送付された訂正データＣＤ（１、ａ）とを用いて共通鍵ＣＫ（１）を生成する（ステップＳ４２）。

【０１００】
　また、半導体装置ＩＣｓ（９０）は半導体装置ＩＣｂ（８０）に訂正データＣＤ（１、ｂ）を送付する（ステップＳ４３）。次に、半導体装置８０の共通鍵生成部８３は、ユニークコード生成部８１から出力されたユニークコードＵＣ（ｂ）と、半導体装置９０から送付された訂正データＣＤ（１、ｂ）とを用いて共通鍵ＣＫ（１）を生成する（ステップＳ４４）。このような処理により、半導体装置７０と半導体装置８０は共に共通鍵ＣＫ（１）を保持することができる。よって、半導体装置７０および半導体装置８０は共通鍵ＣＫ（１）を用いて暗号通信することが可能となる（ステップＳ４５）。なお、上記各ステップは矛盾がない限り適宜順番を変更することができる。
【０１０１】
　なお、半導体装置９０から半導体装置７０、８０に訂正データＣＤを送付する場合は、例えば半導体装置９０から半導体装置７０、８０に定期的に訂正データＣＤを送付してもよい。また、半導体装置７０、８０から訂正データＣＤを送付するように要求があったタイミングで、半導体装置９０から半導体装置７０、８０に訂正データＣＤを送付するようにしてもよい。
【０１０２】
　半導体装置９０と半導体装置７０、８０は互いに有線で接続されていてもよく、また無線で接続されていてもよい。更に、半導体装置９０と半導体装置７０、８０は訂正データＣＤを送受信するときのみ互いに接続されるように構成してもよい。また、半導体装置９０から半導体装置７０、８０にインターネット経由で訂正データＣＤを送付してもよい。この場合は、セキュリティの関係上、上述した方法を用いて訂正データＣＤを暗号化することが好ましい。
【０１０３】
　また、複数組の半導体装置がそれぞれ異なる共通鍵ＣＫで通信するように構成してもよい。例えば半導体装置ＩＣｄ、ＩＣｅ、ＩＣｆが共通鍵ＣＫ（２）を用いて互いに通信するように構成し、且つ半導体装置ＩＣｇ、ＩＣｈ、ＩＣｉが共通鍵ＣＫ（３）を用いて互いに通信するように構成してもよい。この場合は、半導体装置９０から半導体装置ＩＣｄ、ＩＣｅ、ＩＣｆにそれぞれ、共通鍵ＣＫ（２）を生成するための訂正データＣＤ（２、ｄ）、ＣＤ（２、ｅ）、ＣＤ（２、ｆ）が送付される。また、半導体装置９０から半導体装置ＩＣｇ、ＩＣｈ、ＩＣｉにそれぞれ、共通鍵ＣＫ（３）を生成するための訂正データＣＤ（３、ｇ）、ＣＤ（３、ｈ）、ＣＤ（３、ｉ）が送付される。
【０１０４】
　このように、本実施の形態にかかる暗号通信システムでは、訂正データＣＤを一括して管理する半導体装置９０を設けている。このため、共通鍵ＣＫを生成するために使用される訂正データＣＤを各半導体装置７０、８０に格納する必要がないため、暗号通信システムのセキュリティを向上させることができる。ここで、半導体装置９０のデータベース９１にはセキュリティレベルの高い訂正データが格納されているので、セキュアマイコンを用いて半導体装置９０を構成することが好ましい。一方、半導体装置７０、８０では、セキュリティレベルの高い共通鍵ＣＫの情報が不揮発性メモリに格納されないので、汎用マイコンを用いて構成することができる。しかし、暗号通信システムのセキュリティレベルを更に向上させるために、半導体装置７０、８０にセキュアマイコンを使用してもよい。
【０１０５】
　また、本実施の形態にかかる暗号通信システムでは、データベース９１を用いて訂正データＣＤを一括して管理しているので、各半導体装置の共通鍵ＣＫを容易に変更することができる。このため、半導体装置７０、８０の共通鍵ＣＫを定期的に変更することが容易となり、暗号通信システムのセキュリティを更に向上させることができる。
【０１０６】
＜実施の形態５＞
　次に、本発明の実施の形態５について説明する。図１２は本実施の形態にかかる暗号通信システムを示すブロック図である。実施の形態４で説明した暗号通信システムでは、デ

ータベース９１で訂正データを一括管理していたが、本実施の形態にかかる暗号通信システムでは、半導体装置１３０が備える訂正データ生成部１３２を用いて、半導体装置ＩＣａ（１１０）および半導体装置ＩＣｂ（１２０）に送付する訂正データを生成している。これ以外は、実施の形態４にかかる暗号通信システムと基本的に同様である。以下、詳細に説明する。

【０１０７】

図１２に示す暗号通信システム５は、半導体装置１１０、１２０、１３０を有する。半導体装置１１０は、ユニークコード生成部１１１、記憶部１１２、および共通鍵生成部１１３を有する。

【０１０８】

ユニークコード生成部１１１は、半導体装置１１０に固有のユニークコードＵＣ（ａ）を生成し、共通鍵生成部１１３および半導体装置１３０の訂正データ生成部１３２に出力する。ユニークコード生成部１１１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。

【０１０９】

記憶部１１２は、共通鍵生成部１１３で生成された共通鍵ＣＫ（１）を揮発性メモリに格納する。共通鍵ＣＫ（１）は、半導体装置１１０の電源がオフになると消去される。尚、共通鍵ＣＫ（１）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（１）に対して、半導体装置１１０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０１１０】

共通鍵生成部１１３は、ユニークコード生成部１１１から出力されたユニークコードＵＣ（ａ）と、半導体装置１３０から供給された訂正データＣＤ（１、ａ）とを用いて共通鍵ＣＫ（１）を生成する。ここで、共通鍵生成部１１３はユニークコード訂正部として機能する。共通鍵生成部１１３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。

【０１１１】

半導体装置１２０は、ユニークコード生成部１２１、記憶部１２２、および共通鍵生成部１２３を有する。

【０１１２】

ユニークコード生成部１２１は、半導体装置１２０に固有のユニークコードＵＣ（ｂ）を生成し、共通鍵生成部１２３および半導体装置１３０の訂正データ生成部１３２に出力する。ユニークコード生成部１２１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。

【０１１３】

記憶部１２２は、共通鍵生成部１２３で生成された共通鍵ＣＫ（１）を揮発性メモリに格納する。共通鍵ＣＫ（１）は、半導体装置１２０の電源がオフになると消去される。尚、共通鍵ＣＫ（１）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（１）に対して、半導体装置１２０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０１１４】

共通鍵生成部１２３は、ユニークコード生成部１２１から出力されたユニークコードＵＣ（ｂ）と、半導体装置１３０から供給された訂正データＣＤ（１、ｂ）とを用いて共通鍵ＣＫ（１）を生成する。ここで、共通鍵生成部１２３はユニークコード訂正部として機能する。共通鍵生成部１２３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。

【０１１５】

半導体装置１３０は、記憶部１３１および訂正データ生成部１３２を有する。記憶部１

３１は、共通鍵ＣＫ（１）を不揮発性メモリに格納している。ここで、共通鍵ＣＫ（１）の情報は半導体装置１３０の電源をオフにしても消去されない。よって、半導体装置が不正に解析されることで共通鍵ＣＫ（１）の情報が第三者に漏洩してしまうことを防ぐために、半導体装置１３０をセキュアマイコンで構成することが好ましい。なお、半導体装置１１０、１２０については、実施の形態４の場合と同様に、汎用マイコンを用いることができる。

【０１１６】

訂正データ生成部１３２は、半導体装置１１０のユニークコードＵＣ（ａ）と記憶部１３１に格納されている共通鍵ＣＫ（１）とを用いて訂正データＣＤ（１、ａ）を生成する。また、訂正データ生成部１３２は、半導体装置１２０のユニークコードＵＣ（ｂ）と記憶部１３１に格納されている共通鍵ＣＫ（１）とを用いて訂正データＣＤ（１、ｂ）を生成する。

【０１１７】

訂正データ生成部１３２が訂正データを生成する場合の動作について、図１４を用いて詳細に説明する。なお、以下では、訂正データ生成部１３２が訂正データＣＤ（１、ａ）を生成する場合について説明するが、訂正データ生成部１３２が訂正データＣＤ（１、ｂ）を生成する場合も同様である。

【０１１８】

まず、半導体装置ＩＣａ（１１０）からユニークコードＵＣ（ａ）を複数回取得する（ステップＳ６１）。次に、ステップＳ６１で取得したユニークコードＵＣ（ａ）を統計的に処理し、ユニークコードＵＣ（ａ）の各ビットを、（１）値が安定したビット、（２）高確率で変動するビット（つまり、値の変動が比較的大きいビット）、（３）低確率で変動するビット（つまり、値の変動が比較的小さいビット）の３つに分類する。そして、（２）高確率で変動するビットを用いてマスクデータを生成する（ステップＳ６２）。このとき、例えばユニークコードＵＣ（ａ）の各ビットのうち、所定の閾値よりも高い確率で変動するビットの位置を示す情報をマスクデータとする。例えば、図４に示したマスクデータでは、高確率で変動するビットの位置（つまり、マスクする位置）を"０"で示している。

【０１１９】

次に、ステップＳ６２で生成したマスクデータを用いてユニークコードＵＣ（ａ）をマスクし、高確率で変動するビットを削除する。そして、マスク後のユニークコードＵＣ（ａ）'（つまり、値が安定したビットと低確率で変動するビットを含むユニークコード）のエラーを訂正できるＥＣＣコードを生成する（ステップＳ６３）。ＥＣＣコードは、例えばＢＣＨ符号やリードソロモン符号である。

【０１２０】

次に、ステップＳ６２で生成したマスクデータおよびステップＳ６３で生成したＥＣＣコードを用いて処理をしたユニークコードＵＣ（ａ）''（つまり、値が安定したビットを含むユニークコード）と、記憶部１３１に格納されている共通鍵ＣＫ（１）とを用いて、演算パラメータを生成する（ステップＳ６４）。すなわち、演算パラメータは、訂正されたユニークコードＵＣ（ａ）''から共通鍵ＣＫ（１）を生成するために必要なパラメータである。

【０１２１】

上記処理により生成されたマスクデータ、ＥＣＣコード、および演算パラメータを訂正データＣＤ（１、ａ）として半導体装置ＩＣａ（１１０）に送付する（ステップＳ６５）。

【０１２２】

次に、本実施の形態にかかる暗号通信システム５の動作について、図１３に示すフローチャートを用いて説明する。まず、半導体装置ＩＣａ（１１０）は半導体装置ＩＣｓ（１３０）の訂正データ生成部１３２にユニークコードＵＣ（ａ）を送付する（ステップＳ５１）。次に、半導体装置１３０の訂正データ生成部１３２は、送付されたユニークコード

ＵＣ（ａ）と共通鍵ＣＫ（１）とを用いて訂正データＣＤ（１、ａ）を生成する（ステップＳ５２）。ここで、訂正データ生成部１３２が訂正データＣＤ（１、ａ）を生成するには、ユニークコードＵＣ（ａ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ａ）を複数回取得するためにステップＳ５１を繰り返す。生成された訂正データＣＤ（１、ａ）は、半導体装置１１０に送付される（ステップＳ５３）。半導体装置１１０の共通鍵生成部１１３は、ユニークコード生成部１１１から出力されたユニークコードＵＣ（ａ）と、半導体装置１３０から送付された訂正データＣＤ（１、ａ）とを用いて共通鍵ＣＫ（１）を生成する（ステップＳ５４）。

【０１２３】

また、半導体装置ＩＣｂ（１２０）は半導体装置ＩＣｓ（１３０）の訂正データ生成部１３２にユニークコードＵＣ（ｂ）を送付する（ステップＳ５５）。次に、半導体装置１３０の訂正データ生成部１３２は、送付されたユニークコードＵＣ（ｂ）と共通鍵ＣＫ（１）とを用いて訂正データＣＤ（１、ｂ）を生成する（ステップＳ５６）。ここで、訂正データ生成部１３２が訂正データＣＤ（１、ｂ）を生成するには、ユニークコードＵＣ（ｂ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ｂ）を複数回取得するためにステップＳ５５を繰り返す。生成された訂正データＣＤ（１、ｂ）は、半導体装置１２０に送付される（ステップＳ５７）。半導体装置１２０の共通鍵生成部１２３は、ユニークコード生成部１２１から出力されたユニークコードＵＣ（ｂ）と、半導体装置１３０から送付された訂正データＣＤ（１、ｂ）とを用いて共通鍵ＣＫ（１）を生成する（ステップＳ５８）。

【０１２４】

このような処理により、半導体装置１１０と半導体装置１２０は共に共通鍵ＣＫ（１）を保持することができる。よって、半導体装置１１０および半導体装置１２０は共通鍵ＣＫ（１）を用いて暗号通信することが可能となる（ステップＳ５９）。なお、上記各ステップは矛盾がない限り適宜順番を変更することができる。例えば、ステップＳ５１～Ｓ５４とステップＳ５５～Ｓ５８は並行して実施してもよい。

【０１２５】

このように、本実施の形態にかかる暗号通信システムにおいても、訂正データを一括して管理する半導体装置１３０を設けている。このため、共通鍵を生成するために使用される訂正データを各半導体装置１１０、１２０に格納する必要がないため、暗号通信システムのセキュリティを向上させることができる。ここで、半導体装置１３０の記憶部１３１にはセキュリティレベルの高い訂正データが格納されているので、セキュアマイコンを用いて半導体装置１３０を構成することが好ましい。一方、半導体装置１１０、１２０では、セキュリティレベルの高い共通鍵ＣＫの情報が不揮発性メモリに格納されないので、汎用マイコンを用いて構成することができる。しかし、暗号通信システムのセキュリティレベルを更に向上させるために、半導体装置１１０、１２０にセキュアマイコンを使用してもよい。

【０１２６】

＜実施の形態６＞

次に、本発明の実施の形態６について説明する。図１５は本実施の形態にかかる暗号通信システムを示すブロック図である。実施の形態５で説明した暗号通信システムでは、半導体装置ＩＣａ（１１０）と半導体装置ＩＣｂ（１２０）とが同一の共通鍵ＣＫ（１）を有する場合について説明した。本実施の形態にかかる暗号通信システムでは、半導体装置ＩＣａ（１４０）と半導体装置ＩＣｂ（１５０）とが異なる共通鍵を有し、半導体装置ＩＣｓ（１６０）を介して通信している。これ以外は、実施の形態５にかかる暗号通信システムと基本的に同様である。以下、詳細に説明する。

【０１２７】

図１５に示す暗号通信システム６は、半導体装置１４０、１５０、１６０を有する。半導体装置１４０は、ユニークコード生成部１４１、記憶部１４２、および共通鍵生成部１４３を有する。

【０１２８】
ユニークコード生成部１４１は、半導体装置１４０に固有のユニークコードＵＣ（ａ）を生成し、共通鍵生成部１４３および半導体装置１６０の訂正データ生成部１６２に出力する。ユニークコード生成部１４１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。
【０１２９】
記憶部１４２は、共通鍵生成部１４３で生成された共通鍵（第１の共通鍵）ＣＫ（１）を揮発性メモリに格納する。共通鍵ＣＫ（１）は、半導体装置１４０の電源がオフになると消去される。
【０１３０】
共通鍵生成部１４３は、ユニークコード生成部１４１から出力されたユニークコードＵＣ（ａ）と、半導体装置１６０から供給された訂正データＣＤ（１、ａ）とを用いて共通鍵ＣＫ（１）を生成する。ここで、共通鍵生成部１４３はユニークコード訂正部として機能する。共通鍵生成部１４３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。
【０１３１】
半導体装置１５０は、ユニークコード生成部１５１、記憶部１５２、および共通鍵生成部１５３を有する。
【０１３２】
ユニークコード生成部１５１は、半導体装置１５０に固有のユニークコードＵＣ（ｂ）を生成し、共通鍵生成部１５３および半導体装置１６０の訂正データ生成部１６２に出力する。ユニークコード生成部１５１の基本的な構成および動作は、実施の形態１で説明したユニークコード生成部１１と同様であるので重複した説明は省略する。
【０１３３】
記憶部１５２は、共通鍵生成部１５３で生成された共通鍵（第２の共通鍵）ＣＫ（２）を揮発性メモリに格納する。共通鍵ＣＫ（２）は、半導体装置１５０の電源がオフになると消去される。
【０１３４】
共通鍵生成部１５３は、ユニークコード生成部１５１から出力されたユニークコードＵＣ（ｂ）と、半導体装置１６０から供給された訂正データＣＤ（２、ｂ）とを用いて共通鍵ＣＫ（２）を生成する。ここで、共通鍵生成部１５３はユニークコード訂正部として機能する。共通鍵生成部１５３の基本的な構成および動作は、実施の形態１で説明した共通鍵生成部１３と同様であるので重複した説明は省略する。
【０１３５】
半導体装置１６０は、記憶部１６１および訂正データ生成部１６２を有する。記憶部１６１は、共通鍵ＣＫ（１）および共通鍵ＣＫ（２）を不揮発性メモリに格納している。ここで、共通鍵ＣＫ（１）および共通鍵ＣＫ（２）の情報は半導体装置１６０の電源をオフにしても消去されない。よって、半導体装置が不正に解析されることで共通鍵ＣＫ（１）および共通鍵ＣＫ（２）の情報が第三者に漏洩してしまうことを防ぐために、半導体装置１６０をセキュアマイコンで構成することが好ましい。なお、半導体装置１４０、１５０については、実施の形態５の場合と同様に、汎用マイコンを用いることができる。
【０１３６】
訂正データ生成部１６２は、半導体装置１４０のユニークコードＵＣ（ａ）と記憶部１６１に格納されている共通鍵ＣＫ（１）とを用いて訂正データＣＤ（１、ａ）を生成する。また、訂正データ生成部１６２は、半導体装置１５０のユニークコードＵＣ（ｂ）と記憶部１６１に格納されている共通鍵ＣＫ（２）とを用いて訂正データＣＤ（２、ｂ）を生成する。
【０１３７】
次に、本実施の形態にかかる暗号通信システム６の動作について、図１６に示すフローチャートを用いて説明する。まず、半導体装置ＩＣａ（１４０）は半導体装置ＩＣｓ（１

６０）の訂正データ生成部１６２にユニークコードＵＣ（ａ）を送付する（ステップＳ７１）。次に、半導体装置１６０の訂正データ生成部１６２は、送付されたユニークコードＵＣ（ａ）と共通鍵ＣＫ（１）とを用いて訂正データＣＤ（１、ａ）を生成する（ステップＳ７２）。ここで、訂正データ生成部１６２が訂正データＣＤ（１、ａ）を生成するには、ユニークコードＵＣ（ａ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ａ）を複数回取得するためにステップＳ７１を繰り返す。生成された訂正データＣＤ（１、ａ）は、半導体装置１４０に送付される（ステップＳ７３）。半導体装置１４０の共通鍵生成部１４３は、ユニークコード生成部１４１から出力されたユニークコードＵＣ（ａ）と、半導体装置１６０から送付された訂正データＣＤ（１、ａ）とを用いて共通鍵ＣＫ（１）を生成する（ステップＳ７４）。

【０１３８】

また、半導体装置ＩＣｂ（１５０）は半導体装置ＩＣｓ（１６０）の訂正データ生成部１６２にユニークコードＵＣ（ｂ）を送付する（ステップＳ７５）。次に、半導体装置１６０の訂正データ生成部１６２は、送付されたユニークコードＵＣ（ｂ）と共通鍵ＣＫ（２）とを用いて訂正データＣＤ（２、ｂ）を生成する（ステップＳ７６）。ここで、訂正データ生成部１６２が訂正データＣＤ（２、ｂ）を生成するには、ユニークコードＵＣ（ｂ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ｂ）を複数回取得するためにステップＳ７５を繰り返す。生成された訂正データＣＤ（２、ｂ）は、半導体装置１５０に送付される（ステップＳ７７）。半導体装置１５０の共通鍵生成部１５３は、ユニークコード生成部１５１から出力されたユニークコードＵＣ（ｂ）と、半導体装置１６０から送付された訂正データＣＤ（２、ｂ）とを用いて共通鍵ＣＫ（２）を生成する（ステップＳ７８）。

【０１３９】

このような処理により、半導体装置１４０と半導体装置１６０は共に共通鍵ＣＫ（１）を保持することができる。よって、半導体装置１４０および半導体装置１６０は共通鍵ＣＫ（１）を用いて暗号通信することが可能となる（ステップＳ７９）。また、半導体装置１５０と半導体装置１６０は共に共通鍵ＣＫ（２）を保持することができる。よって、半導体装置１５０および半導体装置１６０は共通鍵ＣＫ（２）を用いて暗号通信することが可能となる（ステップＳ８０）。したがって、半導体装置１４０と半導体装置１５０は、半導体装置１６０を介して通信することができる（ゲートウェイ構成）。なお、上記各ステップは矛盾がない限り適宜順番を変更することができる。例えば、ステップＳ７１～Ｓ７４とステップＳ７５～Ｓ７８は並行して実施してもよい。

【０１４０】

このように、本実施の形態にかかる暗号通信システムにおいても、訂正データを一括して管理する半導体装置１６０を設けている。このため、共通鍵を生成するために使用される訂正データを各半導体装置１４０、１５０に格納する必要がないため、暗号通信システムのセキュリティを向上させることができる。ここで、半導体装置１６０の記憶部１６１にはセキュリティレベルの高い訂正データが格納されているので、セキュアマイコンを用いて半導体装置１６０を構成することが好ましい。一方、半導体装置１４０、１５０では、セキュリティレベルの高い共通鍵ＣＫの情報が不揮発性メモリに格納されないので、汎用マイコンを用いて構成することができる。しかし、暗号通信システムのセキュリティレベルを更に向上させるために、半導体装置１４０、１５０にセキュアマイコンを使用してもよい。

【０１４１】

＜実施の形態７＞

次に、本発明の実施の形態７について説明する。図１７は実施の形態１乃至６にかかる暗号通信システムを車載用半導体装置に適用した場合を示すブロック図である。図１７に示すように、車両１８０にはゲートウェイ部１７０、故障診断ユニット１７１、エンジン制御ユニット１７２、ブレーキ制御ユニット１７３、ランプ制御ユニット１７４、ドアロック制御ユニット１７５、鍵挿入制御ユニット１７６、カーナビゲーションシステム１７

８、およびＤＣＭ（Data Communication Module）１７９が設けられている。
【０１４２】
ゲートウェイ部１７０は、各ユニット１７１～１７６およびカーナビゲーションシステム１７８で構成されるネットワークを中継するための機器である。ゲートウェイ部１７０にはセキュアマイコンＩＣｓが設けられている。故障診断ユニット１７１は、車両１８０を構成する部品が故障しているか診断するユニットである。故障診断ユニット１７１には半導体装置ＩＣａが設けられている。エンジン制御ユニット１７２は、エンジン動作における電気的な制御（燃料供給、点火タイミングの調整等）を総合的に行うためのユニットである。エンジン制御ユニット１７２には半導体装置ＩＣｂが設けられている。ブレーキ制御ユニット１７３は、ＡＢＳ（Antilock Brake System）などブレーキを制御するためのユニットである。ブレーキ制御ユニット１７３には半導体装置ＩＣｃが設けられている。ランプ制御ユニット１７４は、車両のヘッドライトやウインカー等を制御するためのユニットである。ランプ制御ユニット１７４には半導体装置ＩＣｄが設けられている。
【０１４３】
ドアロック制御ユニット１７５は、ドアのロックを制御するためのユニットである。ドアロック制御ユニット１７５には半導体装置ＩＣｅと、鍵１７７と無線通信するための通信部が設けられている。鍵挿入制御ユニット１７６は、挿入された鍵１７７が正規のユーザの鍵であるかを判断するためのユニットである。鍵挿入制御ユニット１７６には、半導体装置ＩＣｆと、鍵１７７と無線通信するための通信部が設けられている。鍵１７７は、半導体装置ＩＣｇと、ドアロック制御ユニット１７５および鍵挿入制御ユニット１７６と無線通信するための通信部が設けられている。各ユニット１７１～１７６、および鍵１７７に設けられている半導体装置ＩＣａ～ＩＣｇには、例えば汎用マイコンを用いることができる。
【０１４４】
カーナビゲーションシステム１７８にはセキュアマイコンＩＣｈが設けられている。ＤＣＭ１７９は、車両内における各ユニット１７１～１７６から取得した情報を外部のサーバ１８１に送信したり、サーバ１８１から情報を取得したりするための通信モジュールである。
【０１４５】
各ユニット１７１～１７６およびカーナビゲーションシステム１７８はそれぞれゲートウェイ部１７０と接続されており、各ユニット１７１～１７６はゲートウェイ部１７０を介して互いに通信可能に構成されている。このとき、各ユニット１７１～１７６とゲートウェイ部１７０との間の通信に用いる共通鍵は、ユニット毎に異なるようにしてもよい。例えば故障診断ユニット１７１とゲートウェイ部１７０との通信に共通鍵ＣＫ（１）を用い、エンジン制御ユニット１７２とゲートウェイ部１７０との通信に共通鍵ＣＫ（２）を用いるように構成してもよい。なお、この場合は、図１５に示した実施の形態６にかかる暗号通信システム６における半導体装置ＩＣａ（１４０）が故障診断ユニット１７１に対応し、半導体装置ＩＣｂ（１５０）がエンジン制御ユニット１７２に対応し、半導体装置ＩＣｓ（１６０）がゲートウェイ部１７０に対応している。
【０１４６】
各ユニット１７１～１７６とゲートウェイ部との間の通信で用いられる共通鍵を生成するために用いられる訂正データＣＤは、例えばゲートウェイ部１７０の半導体装置ＩＣｓやカーナビゲーションシステム１７８の半導体装置ＩＣｈに格納することができる。また、共通鍵を生成するために用いられる訂正データＣＤは、サーバ１８１から供給されるようにしてもよい。サーバ１８１から訂正データＣＤが供給されることで、各ユニット１７１～１７６とゲートウェイ部１７０との通信で用いられる共通鍵を容易に変更することができる。サーバ１８１から供給された訂正データＣＤは、例えばゲートウェイ部１７０の半導体装置ＩＣｓやカーナビゲーションシステム１７８の半導体装置ＩＣｈに格納することができる。
【０１４７】

また、カーナビゲーションシステム１７８は、各ユニット１７１～１７６から取得した情報（例えば、故障情報など）を、ＤＣＭ１７９を介してサーバ１８１に送信することができる。このとき、ＤＣＭ１７９とサーバ１８１との間の通信を暗号化してもよい。

【０１４８】

図１７に示した例では、各ユニット１７１～１７６がゲートウェイ部１７０を介して通信している構成を示した。しかし、各ユニット１７１～１７６が互いに同一の共通鍵を用いて通信するように構成してもよい。この場合は、例えば各ユニット１７１～１７６が共通バスを介して互いに接続されるように構成する。各ユニット１７１～１７６に格納される共通鍵は、例えば実施の形態１（図１）、実施の形態４（図９）、実施の形態５（図１２）で説明した方法を用いることで生成することができる。

【０１４９】

＜実施の形態８＞

図１８は、実施の形態８にかかる暗号通信システムを示すブロック図である。本実施の形態にかかる暗号通信システム２０１は、半導体装置ＩＣａ（第１の半導体装置）２１０と半導体装置ＩＣｚ（第２の半導体装置）２２０とを有する。半導体装置ＩＣａ（２１０）は他の半導体装置（不図示）とセキュアなネットワークを構成している。本実施の形態では、半導体装置ＩＣａ（２１０）を含むセキュアなネットワークに、半導体装置ＩＣｚ（２２０）を新たに追加する場合について説明する。

【０１５０】

半導体装置２１０は、ユニークコード生成部２１１、記憶部２１２、共通鍵生成部（第１の共通鍵生成部）２１３、および訂正データ生成部２１４を有する。

ユニークコード生成部２１１は、半導体装置２１０に固有の値であってランダムなエラーを含むユニークコード（第１のユニークコード）ＵＣ（ａ）を生成し、共通鍵生成部２１３に出力する。ここで、ユニークコードＵＣ（ａ）は、半導体装置２１０が備える素子固有の物理的な特性により決まる値である。例えば、ユニークコード生成部２１１は、半導体装置２１０が備えるメモリ素子の起動時の値を用いてユニークコードＵＣ（ａ）を生成することができる。ユニークコードは、ＩＣの設計は同一であるが実際に製造されるＩＣは個々にばらつきを有するという性質を利用して生成されるコードである。このような技術は、ＰＵＦ（Physical Unclonable Function）と呼ばれ、同一の回路を備えたＩＣを１の半導体ウェハーに複数個同時に同一の製造装置により製造しても、個々のＩＣ毎で固有のコードを得ることができると共に、別のＩＣでの複製を困難にすることができる技術である。この技術を用いることにより、耐タンパチップのような特殊なハードウェアを使用することなく、データの高い秘匿性を実現することができる。

【０１５１】

記憶部２１２は、訂正データ（第１の訂正データ）ＣＤ（ａ）と、共通鍵生成部２１３で生成された共通鍵（第１の共通鍵）ＣＫ（ａ）とを格納することができる。記憶部２１２は、揮発性メモリ（例えば、ＳＲＡＭ）と不揮発性メモリ（例えばフラッシュメモリ）とを有し、訂正データＣＤ（ａ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部２１２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２１０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置２１０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０１５２】

共通鍵生成部２１３は、ユニークコード生成部２１１から出力されたユニークコードＵＣ（ａ）と、記憶部２１２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する。

【０１５３】

ユニークコード生成部２１１で生成されるユニークコードＵＣ（ａ）は、ユニークコー

ド生成時の外的要因、例えば、温度、電圧等によって変動するビットの値を含むデータである。このため、ユニークコード生成部２１１で生成されるユニークコードＵＣ（ａ）には、（１）値が安定したビット、（２）高確率で変動するビット（つまり、値の変動が比較的大きいビット）、（３）低確率で変動するビット（つまり、値の変動が比較的小さいビット）の３つが含まれる。このように、ユニークコード生成部２１１で生成されるユニークコードＵＣ（ａ）は、（２）高確率で変動するビットと（３）低確率で変動するビットとを含む。よって、ユニークコードＵＣ（ａ）は生成される毎に異なる値となる。

【０１５４】

高確率で変動するビットは製造工程で把握することができる。よって、製造工程において各ビットを判定することで、高確率で変動するビットをマスクするマスクデータを作成することができる。そして、このマスクデータを用いて、ユニークコード生成部２１１で生成されたユニークコードＵＣ（ａ）をマスクすることで、ユニークコードＵＣ（ａ）に含まれる高確率で変動するビットを削除することができる。ここで、高確率で変動するビットの位置は半導体装置毎に異なるため、マスクデータは半導体装置に固有のデータとなる。

【０１５５】

低確率で変動するビットは、外的要因や残存する電荷などに起因して変動するため、予め予測することが困難である。このため、低確率で変動するビットは、例えばＢＣＨ符号やリードソロモン符号に代表されるＥＣＣコードを製造時に生成し、このＥＣＣコードを用いて変動性のあるビットを除外するようなエラー訂正を行う。以下で、共通鍵生成部２１３の動作について具体的に説明する。

【０１５６】

図２０は、共通鍵生成部２１３の動作を説明するためのフローチャートであり、図２１は共通鍵生成部２１３で処理されるユニークコードの一例を示す表である。まず、共通鍵生成部２１３は、ユニークコード生成部２１１からユニークコードＵＣ（ａ）を読み込む（ステップＳ１１１）。このとき読み込まれたユニークコードＵＣ（ａ）は、変動性のあるビットを除外するようなエラー訂正が実施されていないユニークコードである。

【０１５７】

次に、訂正データＣＤ（ａ）に含まれるマスクデータを用いて、読み込まれたユニークコードＵＣ（ａ）をマスクする（ステップＳ１１２）。ここで、マスクデータは、ユニークコードＵＣ（ａ）のビットのうちビットの値が変動するようなエラー率の高いビットをマスクするためのデータである。図２１に示す例では、ユニークコードＵＣ（ａ）の１ビット目と６ビット目のビットのエラー率が高いため、マスクデータが"０"となっている。これ以外のビットは、エラー率が低いビットまたは値が安定しているビットであるため、マスクデータが"１"となっている。つまり、マスクが必要なビットのマスクデータは"０"となり、マスクが不要なビットのマスクデータは"１"となる。そして、マスクデータを用いてユニークコードＵＣ（ａ）をマスクすることで、ユニークコードＵＣ（ａ）の１ビット目と６ビット目のビットを削除したマスク処理後のユニークコードＵＣ（ａ）'を得ることができる（マスク処理により削除したビットは"Ｘ"で示している）。その後、マスク処理後のユニークコードＵＣ（ａ）'は左詰めされる。

【０１５８】

次に、訂正データＣＤ（ａ）に含まれるＥＣＣコード（エラー訂正コード）を用いて、マスク処理後のユニークコードＵＣ（ａ）'に含まれる値の変動率が低いビットのエラーを訂正することによりユニークコードＵＣ（ａ）''を得る（ステップＳ１１３）。図２１に示す例では、ＥＣＣコードを用いてマスク処理後のユニークコードＵＣ（ａ）'を処理することにより、１ビット目のビットが"０"から"１"に訂正されている。

【０１５９】

次に、訂正データＣＤ（ａ）に含まれる演算パラメータを用いて、エラー訂正後のユニークコードＵＣ（ａ）''に所定の演算を実施する（ステップＳ１１４）。図２１に示す例では、エラー訂正後のユニークコードＵＣ（ａ）''にＮＯＴ演算を実施している。この演

算処理後のユニークコードＵＣ（ａ）が共通鍵ＣＫ（ａ）となる。なお、ＮＯＴ演算は一例であり、エラー訂正後のユニークコードＵＣ（ａ）''に実施する演算はどのような演算であってもよい。この演算パラメータを変更することで、必要に応じて共通鍵ＣＫ（ａ）を変更することができる。また、演算パラメータを用いて、エラー訂正後のユニークコードＵＣ（ａ）''に所定の演算を実施することで、共通鍵ＣＫ（ａ）をユニークコードＵＣ（ａ）と見かけ上類似しないコードとすることができる。よって、セキュリティレベルを向上させることができる。また、エラー訂正後のユニークコードＵＣ（ａ）''に実施する演算は省略することもできる。この場合は、マスクデータおよびＥＣＣコードを用いて処理したユニークコードＵＣ（ａ）''が、共通鍵ＣＫ（ａ）となる。このようにして生成された共通鍵ＣＫ（ａ）は、記憶部２１２に出力される。

【０１６０】

以上で説明したように、共通鍵生成部２１３は共通鍵ＣＫ（ａ）を生成する機能を有すると同時に、訂正データＣＤ（ａ）を用いてユニークコードＵＣ（ａ）を訂正する機能も有する。すなわち、共通鍵生成部２１３はユニークコード訂正部としても機能する。

なお、訂正データＣＤ（ａ）に含まれるマスクコード、ＥＣＣコード、および演算パラメータは、半導体装置２１０の固有データとして予め生成されて記憶部２１２に格納されている。訂正データＣＤ（ａ）の生成方法については、訂正データ生成部２１４が訂正データＣＤ（ｚ）を生成する場合と同様である。

【０１６１】

訂正データ生成部２１４は、半導体装置２２０のユニークコード（第２のユニークコード）ＵＣ（ｚ）と共通鍵ＣＫ（ａ）とを用いて訂正データ（第２の訂正データ）ＣＤ（ｚ）を生成する。訂正データ生成部２１４が訂正データを生成する場合の動作について、図２２を用いて詳細に説明する。

【０１６２】

まず、半導体装置ＩＣｚ（２２０）からユニークコードＵＣ（ｚ）を複数回取得する（ステップＳ１２１）。次に、ステップＳ１２１で取得したユニークコードＵＣ（ｚ）を統計的に処理し、ユニークコードＵＣ（ｚ）の各ビットを、（１）値が安定したビット、（２）高確率で変動するビット（つまり、値の変動が比較的大きいビット）、（３）低確率で変動するビット（つまり、値の変動が比較的小さいビット）の３つに分類する。そして、（２）高確率で変動するビットを用いてマスクデータを生成する（ステップＳ１２２）。このとき、例えばユニークコードＵＣ（ｚ）の各ビットのうち、所定の閾値よりも高い確率で変動するビットの位置を示す情報をマスクデータとする。例えば、図２１に示したマスクデータでは、高確率で変動するビットの位置（つまり、マスクする位置）を"０"で示している。

【０１６３】

次に、ステップＳ１２２で生成したマスクデータを用いてユニークコードＵＣ（ｚ）をマスクし、高確率で変動するビットを削除する。そして、マスク後のユニークコードＵＣ（ｚ）''（つまり、値が安定したビットと低確率で変動するビットを含むユニークコード）の変動性のあるビットを除外するための訂正ができるＥＣＣコードを生成する（ステップＳ１２３）。ＥＣＣコードは、例えばＢＣＨ符号やリードソロモン符号である。

【０１６４】

次に、ステップＳ１２２で生成したマスクデータおよびステップＳ１２３で生成したＥＣＣコードを用いて処理をしたユニークコードＵＣ（ｚ）''（つまり、値が安定したビットを含むユニークコード）と、記憶部１２に格納されている共通鍵ＣＫ（ａ）とを用いて、演算パラメータを生成する（ステップＳ１２４）。すなわち、演算パラメータは、訂正されたユニークコードＵＣ（ｚ）''から共通鍵ＣＫ（ａ）を生成するために必要なパラメータである。上記処理により生成されたマスクデータ、ＥＣＣコード、および演算パラメータを訂正データＣＤ（ｚ）として半導体装置ＩＣｚ（２２０）に送付する（ステップＳ１２５）。

【０１６５】

なお、訂正データＣＤ（ｚ）を生成するための処理（ステップＳ１２１～Ｓ１２５）は、複数の半導体装置を用いて分散させて実施してもよい。図２３は、複数の半導体装置ＩＣａ、ＩＣｂ、ＩＣｃ、ＩＣｄを用いて訂正データＣＤ（ｚ）を生成する場合を示す図である。ここで、半導体装置ＩＣａ、ＩＣｂ、ＩＣｃ、ＩＣｄはセキュアなネットワークを構成している。

【０１６６】

図２３に示す例では、半導体装置ＩＣａがステップＳ１２１、Ｓ１２５を実施している。つまり、半導体装置ＩＣａは半導体装置ＩＣｚとの窓口として機能する。半導体装置ＩＣｂはステップＳ１２２（マスクデータの生成）を実施している。半導体装置ＩＣｃはステップＳ１２３（ＥＣＣコードの生成）を実施している。半導体装置ＩＣｄはステップＳ１２４（演算パラメータの生成）を実施している。なお、図２３に示す例は一例であり、各ステップを実施する半導体装置は、任意に割り当てることができる。このように、訂正データＣＤ（ｚ）を生成するための処理（ステップＳ１２１～Ｓ１２５）を、複数の半導体装置に分散させることで、暗号通信システムのセキュリティレベルを向上させることができ、また一つの半導体装置に負荷が集中することを回避することができる。

【０１６７】

図１８に示す半導体装置２２０は、ユニークコード生成部２２１、記憶部２２２、および共通鍵生成部（第２の共通鍵生成部）２２３を有する。ユニークコード生成部２２１は、半導体装置２２０に固有の値であってランダムなエラーを含むユニークコードＵＣ（ｚ）を生成し、訂正データ生成部２１４および共通鍵生成部２２３に出力する。なお、ユニークコード生成部２２１の構成および動作は、上記で説明したユニークコード生成部２１１と基本的に同様である。

【０１６８】

記憶部２２２は、共通鍵生成部２２３で生成された共通鍵ＣＫ（ａ）を格納することができる。記憶部２２２は、揮発性メモリに共通鍵ＣＫ（ａ）を格納する。よって、記憶部２２２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２２０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置２２０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０１６９】

共通鍵生成部２２３は、ユニークコード生成部２２１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部２１４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵（第１の共通鍵）ＣＫ（ａ）を生成する。なお、共通鍵生成部２２３が共通鍵ＣＫ（ａ）を生成する方法は、上述した共通鍵生成部２１３が共通鍵ＣＫ（ａ）を生成する方法と基本的に同様である。

【０１７０】

次に、本実施の形態にかかる暗号通信システムの動作について、図１９に示すフローチャートを用いて説明する。まず、半導体装置ＩＣａ（２１０）の共通鍵生成部１３は、ユニークコード生成部２１１から出力されたユニークコードＵＣ（ａ）と、記憶部２１２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１０１）。その後、半導体装置ＩＣａ（２１０）は他の半導体装置ＩＣｂ～ＩＣｙ（不図示）と共通鍵ＣＫ（ａ）を用いて通信を開始する（ステップＳ１０２）。

【０１７１】

半導体装置２２０は、半導体装置２１０の訂正データ生成部２１４に半導体装置２２０のユニークコードＵＣ（ｚ）を送付する（ステップＳ１０３）。半導体装置２１０の訂正データ生成部２１４は、半導体装置２２０のユニークコードＵＣ（ｚ）と、記憶部２１２に格納されている共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成する（ステップＳ１０４）。訂正データ生成部２１４が訂正データＣＤ（ｚ）を生成するには、ユニークコードＵＣ（ｚ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ｚ）を

複数回取得するためにステップＳ１０３を繰り返す。

【０１７２】

生成された訂正データＣＤ（ｚ）は半導体装置２２０の共通鍵生成部２２３に送付される（ステップＳ１０５）。半導体装置２２０の共通鍵生成部２２３は、ユニークコード生成部２２１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部２１４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１０６）。上記処理により、新たに追加された半導体装置２２０は共通鍵ＣＫ（ａ）を保持することができる。よって、新たに追加された半導体装置（ＩＣｚ）２２０は、半導体装置（ＩＣａ）２１０および他の半導体装置ＩＣｂ～ＩＣｙと共通鍵ＣＫ（ａ）を用いて暗号通信することが可能となる（ステップＳ１０７）。本処理は前述の通り、送付データＵＣ（ｚ）より、ＣＤ（ｚ）を算出し、返信する処理である。悪意をもったアタッカが準備したＩＣｚを使い、本処理を繰り返す、又は違うデータＵＣ（ｚ）を繰り返し送り続け、共通鍵生成部のアルゴリズムを、ＣＤ（ｚ）及び処理中の電流波形データより、解析される可能性がある。この為、セキュリティレベルを向上させるため、図１９に示したフローに回数制限（例えば３～５回程度）を持たせることが、望ましい。

【０１７３】

本発明の課題で説明したように、セキュアな通信が確立している暗号通信システムに新たに半導体装置ＩＣｚを追加する場合は、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証する必要がある。しかしながら、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証するには、例えば高価なセキュアサーバを暗号通信システムに組み込む必要がある。このため、暗号通信システムのコストが増加するという問題があった。

【０１７４】

これに対して本実施の形態にかかる暗号通信システムでは、半導体装置２１０が備える訂正データ生成部２１４において、半導体装置２２０に固有の値であってランダムなエラーを含むユニークコードＵＣ（ｚ）と、共通鍵ＣＫ（ａ）とを用いて、当該ユニークコードＵＣ（ｚ）を訂正する訂正データＣＤ（ｚ）を生成し、半導体装置２２０の共通鍵生成部２２３において、この訂正データＣＤ（ｚ）と半導体装置２２０のユニークコードＵＣ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成している。すなわち、半導体装置ＩＣａ（２１０）と半導体装置ＩＣｚ（２２０）が同じルールに基づいて共通鍵ＣＫ（ａ）を生成することが担保されることで、半導体装置ＩＣａ（２１０）を含むセキュアなネットワークに半導体装置ＩＣｚ（２２０）を追加することの安全性を担保する。

よって、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証するために、高価なセキュアサーバを暗号通信システムに組み込む必要がないので、セキュアな通信を実施している暗号通信システムに、半導体装置を容易かつ低コストに追加することができる。

【０１７５】

また、本実施の形態にかかる暗号通信システムでは、半導体装置２１０の共通鍵生成部２１３において、半導体装置２１０に固有のユニークコードＵＣ（ａ）と訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成している。また、半導体装置２２０の共通鍵生成部２２３において、半導体装置２２０に固有のユニークコードＵＣ（ｚ）と訂正データＣＤ（ｚ）とを用いて、共通鍵ＣＫ（ａ）を生成している。よって、重要なデータである共通鍵ＣＫ（ａ）を記憶部２１２、２２２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（ａ）のデータが漏洩することはない。よって、本実施の形態にかかる暗号通信システムにより、セキュリティの向上を実現しつつ、セキュアな通信を実施している暗号通信システムに、半導体装置を容易かつ低コストに追加することができる。

【０１７６】

ここで、半導体装置を解析して不正にデータを取得する方法としては、以下のような方法がある。

（１）半導体装置をＦＩＢ（Focused Ion Beam）を用いて加工し、プローブを用いて半導体装置を物理的に解析する方法。
（２）半導体装置にレーザなどの電磁波を照射したり、電源端子にノイズを挿入したりすることでＣＰＵを暴走させて不正にデータを取得するフォルトツリー解析。
（３）半導体装置の消費電流量を観測し、鍵データを解析するリーク解析。
【０１７７】
このような不正な解析を回避するために、高いセキュリティレベルが必要な分野では、セキュリティレベルの高いマイコン（以下、セキュアマイコンという）が用いられている。このセキュアマイコンには、配線領域へのシールド、光や信号ノイズを検出する機能、信号に乱数信号を組み合わせて電流をかく乱する機能などが実装されている。
【０１７８】
このように、セキュアマイコンを用いることで第三者が不正に半導体装置を解析することを防止することができる。しかしながら、セキュアマイコンを用いた場合は、不正解析を防止できる反面、その耐タンパ性により半導体装置メーカー等が不良解析や故障解析を実施することができなくなるという問題があった。特に、自動車に用いられる車載用のマイコン（ＥＣＵ等）では高信頼性が必要であるため、半導体装置の不良解析や故障解析が必要となる。このような理由から、車載用のマイコンにはセキュアマイコンよりもセキュリティレベルが低い汎用のマイコン（以下、汎用マイコンという）が広く用いられてきた。したがって、車載用のマイコンでは、汎用マイコンを使用しつつ、半導体装置のセキュリティレベルを向上させることが可能な暗号通信システムが必要とされていた。
【０１７９】
本実施の形態にかかる暗号通信システムでは、共通鍵ＣＫ（ａ）などの重要なデータを記憶部２１２、２２２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（ａ）などの重要なデータが漏洩することはない。このため、半導体装置２１０および半導体装置２２０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。
【０１８０】
なお、半導体装置２１０において共通鍵ＣＫ（ａ）を生成するために使用される訂正データＣＤ（ａ）は、共通鍵ＣＫ（ａ）よりもセキュリティレベルは低いが、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ａ）が第三者に漏洩することを防ぐために、訂正データＣＤ（ａ）が格納される半導体装置２１０にセキュアマイコンを使用してもよい。
【０１８１】
また、半導体装置２１０から半導体装置２２０に送付される訂正データＣＤ（ｚ）は、ユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とに関連するデータであるため、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ｚ）を半導体装置２１０から半導体装置２２０に送付する際は、公開鍵暗号方式を用いて訂正データＣＤ（ｚ）を暗号化して送付してもよい。この場合は、例えば半導体装置２２０が半導体装置２２０の秘密鍵を保持し、半導体装置２１０が訂正データＣＤ（ｚ）を送付する際に半導体装置２２０の公開鍵で訂正データＣＤ（ｚ）を暗号化する。そして、半導体装置２２０が暗号化された訂正データＣＤ（ｚ）を秘密鍵を用いて復号する。これにより、半導体装置２１０から半導体装置２２０に暗号化して訂正データを送付することができる。
【０１８２】
以上で説明したように、本実施の形態にかかる発明により、セキュアな通信を実施している暗号通信システムに、半導体装置を容易に追加することができる暗号通信システムおよび暗号通信方法を提供することができる。
【０１８３】
＜実施の形態９＞
次に、本発明の実施の形態９について説明する。図２４は、本実施の形態にかかる暗号通信システム２０２を示すブロック図である。半導体装置ＩＣｚから出力されるユニーク

コードＵＣ（ｚ）は、その特性上エラー情報を含むためセキュリティレベルが比較的低い情報である。このため、実施の形態８にかかる暗号通信システムでは、半導体装置ＩＣｚから半導体装置ＩＣａにユニークコードＵＣ（ｚ）を送付する際にユニークコードＵＣ（ｚ）を暗号化していなかった。しかしながら、ユニークコードＵＣ（ｚ）はエラー情報も含むが半導体装置ＩＣｚに固有の情報であるため、暗号化して送付することが好ましい。よって、本実施の形態にかかる暗号通信システムでは、半導体装置ＩＣｚから半導体装置ＩＣａにユニークコードＵＣ（ｚ）を送付する際に、ユニークコードＵＣ（ｚ）を暗号化している。

【０１８４】

図２４に示す暗号通信システム２０２は、半導体装置ＩＣａ（２３０）と半導体装置ＩＣｚ（２４０）とを有する。半導体装置２３０は、ユニークコード生成部２３１、記憶部２３２、共通鍵生成部２３３、訂正データ生成部２３４、および復号部２３５を有する。

【０１８５】

ユニークコード生成部２３１は、半導体装置２３０に固有のユニークコードＵＣ（ａ）を生成し、共通鍵生成部２３３に出力する。ユニークコード生成部２３１の基本的な構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。

【０１８６】

記憶部２３２は、訂正データＣＤ（ａ）と、半導体装置２３０の公開鍵ＰＫ（ａ）および秘密鍵ＳＫ（ａ）と、共通鍵生成部２３３で生成された共通鍵ＣＫ（ａ）とを格納することができる。記憶部２３２は、例えば揮発性メモリと不揮発性メモリとを有し、訂正データＣＤ（ａ）、公開鍵ＰＫ（ａ）、および秘密鍵ＳＫ（ａ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部２３２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２３０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置２３０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０１８７】

共通鍵生成部２３３は、ユニークコード生成部２３１から出力されたユニークコードＵＣ（ａ）と、記憶部２３２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する。ここで、共通鍵生成部２３３はユニークコード訂正部として機能する。共通鍵生成部２３３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。

【０１８８】

訂正データ生成部２３４は、半導体装置２４０のユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とを用いて訂正データ（第２の訂正データ）ＣＤ（ｚ）を生成する。訂正データ生成部２３４の基本的な構成および動作は、実施の形態８で説明した訂正データ生成部２１４と同様であるので重複した説明は省略する。

【０１８９】

復号部２３５は、半導体装置２４０の暗号部２４４で暗号化されたユニークコードＵＣ（ｚ）_ｃを、半導体装置２３０の秘密鍵ＳＫ（ａ）を用いて復号してユニークコードＵＣ（ｚ）を生成する。

【０１９０】

半導体装置２４０は、ユニークコード生成部２４１、記憶部２４２、共通鍵生成部２４３、および暗号部２４４を有する。ユニークコード生成部２４１は、半導体装置２４０に固有のユニークコードＵＣ（ｚ）を生成し、暗号部２４４および共通鍵生成部２４３に出力する。なお、ユニークコード生成部２４１の構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。

【０１９１】

記憶部２４２は、共通鍵生成部２４３で生成された共通鍵ＣＫ（ａ）を格納することができる。記憶部２４２は、揮発性メモリに共通鍵ＣＫ（ａ）を格納する。よって、記憶部２４２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２４０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置２４０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０１９２】

共通鍵生成部２４３は、ユニークコード生成部２４１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部２３４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成する。ここで、共通鍵生成部２４３はユニークコード訂正部として機能する。共通鍵生成部２４３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。

【０１９３】

暗号部２４４は、ユニークコード生成部２４１で生成されたユニークコードＵＣ（ｚ）を半導体装置２３０の公開鍵ＰＫ（ａ）を用いて暗号化する。ここで、暗号化に用いられる公開鍵ＰＫ（ａ）は、予め半導体装置２３０から半導体装置２４０に送付されて記憶部２４２に格納されていてもよい。また、暗号化に用いられる公開鍵ＰＫ（ａ）は、暗号部２４４でユニークコードＵＣ（ｚ）を暗号化する際に、半導体装置２３０から暗号部２４４に直接供給されるように構成してもよい。暗号化されたユニークコードＵＣ（ｚ）＿ｃは半導体装置２３０の復号部２３５に出力される。

【０１９４】

次に、本実施の形態にかかる暗号通信システムの動作について、図２５に示すフローチャートを用いて説明する。まず、半導体装置ＩＣａ（２３０）の共通鍵生成部２３３は、ユニークコード生成部２３１から出力されたユニークコードＵＣ（ａ）と、記憶部２３２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１３０）。その後、半導体装置ＩＣａ（２３０）は他の半導体装置ＩＣｂ～ＩＣｙ（不図示）と共通鍵ＣＫ（ａ）を用いて通信を開始する（ステップＳ１３１）。

【０１９５】

次に、半導体装置ＩＣｚ（２４０）は、半導体装置ＩＣａ（２３０）に対して訂正データＣＤ（ｚ）の送付を要求する（ステップＳ１３２）。訂正データＣＤ（ｚ）の送付を要求された半導体装置２３０は、半導体装置２４０に対して半導体装置２３０の公開鍵ＰＫ（ａ）を送付する（ステップＳ１３３）。半導体装置２４０の暗号部２４４は、半導体装置２３０の公開鍵ＰＫ（ａ）を用いてユニークコードＵＣ（ｚ）を暗号化する（ステップＳ１３４）。なお、半導体装置２３０の公開鍵ＰＫ（ａ）は、予め半導体装置２４０の記憶部２４２に格納しておいてもよい。この場合は、ステップＳ１３２、Ｓ１３３を省略することができる。

【０１９６】

半導体装置２４０は、暗号化されたユニークコードＵＣ（ｚ）＿ｃを半導体装置２３０の復号部２３５に送付する（ステップＳ１３５）。半導体装置２３０の復号部２３５は、暗号化されたユニークコードＵＣ（ｚ）＿ｃを、半導体装置２３０の秘密鍵ＳＫ（ａ）を用いて復号してユニークコードＵＣ（ｚ）を生成する（ステップＳ１３６）。

【０１９７】

半導体装置２３０の訂正データ生成部２３４は、半導体装置２４０のユニークコードＵＣ（ｚ）と、記憶部２３２に格納されている共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成する（ステップＳ１３７）。訂正データ生成部２３４が訂正データＣＤ（ｚ）を生成するには、ユニークコードＵＣ（ｚ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ｚ）を複数回取得するためにステップＳ１３４～Ｓ１３６を繰り返す。

【０１９８】

生成された訂正データＣＤ（ｚ）は半導体装置２４０の共通鍵生成部２４３に送付される（ステップＳ１３８）。半導体装置２４０の共通鍵生成部２４３は、ユニークコード生成部２４１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部２３４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１３９）。上記処理により、新たに追加された半導体装置２４０は共通鍵ＣＫ（ａ）を保持することができる。よって、新たに追加された半導体装置（ＩＣｚ）２４０は、半導体装置（ＩＣａ）２３０および他の半導体装置ＩＣｂ～ＩＣｙと共通鍵ＣＫ（ａ）を用いて暗号通信することが可能となる（ステップＳ１４０）。

【０１９９】

このように、本実施の形態にかかる暗号通信システムでは、半導体装置２３０が備える訂正データ生成部２３４において、半導体装置２４０に固有のユニークコードＵＣ（ｚ）と、共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成し、半導体装置２４０の共通鍵生成部２４３において、この訂正データＣＤ（ｚ）と半導体装置２４０のユニークコードＵＣ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成している。よって、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証するために、高価なセキュアサーバを暗号通信システムに組み込む必要がないので、セキュアな通信を実施している暗号通信システムに、半導体装置を容易かつ低コストに追加することができる。

【０２００】

また、本実施の形態にかかる暗号通信システムでは、共通鍵ＣＫ（ａ）などの重要なデータを記憶部２３２、２４２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（ａ）などの重要なデータが漏洩することはない。このため、本実施の形態にかかる暗号通信システムでは、半導体装置２３０および半導体装置２４０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。

【０２０１】

なお、半導体装置２３０において共通鍵ＣＫ（ａ）を生成するために使用される訂正データＣＤ（ａ）や半導体装置２３０の秘密鍵ＳＫ（ａ）は、共通鍵ＣＫ（ａ）よりもセキュリティレベルは低いが、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ａ）や秘密鍵ＳＫ（ａ）が第三者に漏洩することを防ぐために、訂正データＣＤ（ａ）および秘密鍵ＳＫ（ａ）が格納される半導体装置２３０にセキュアマイコンを使用してもよい。

【０２０２】

また、半導体装置２３０から半導体装置２４０に送付される訂正データＣＤ（ｚ）は、ユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とに関連するデータであるため、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ｚ）を半導体装置２３０から半導体装置２４０に送付する際は、公開鍵暗号方式を用いて訂正データＣＤ（ｚ）を暗号化して送付してもよい。

【０２０３】

以上で説明したように、本実施の形態にかかる発明により、セキュアな通信を実施している暗号通信システムに、半導体装置を容易に追加することができる暗号通信システムおよび暗号通信方法を提供することができる。特に、本実施の形態にかかる暗号通信システムでは、半導体装置２４０のユニークコードＵＣ（ｚ）を暗号化して、半導体装置２３０に送付しているので、暗号通信システムのセキュリティを更に向上させることができる。

【０２０４】

＜実施の形態１０＞

次に、本発明の実施の形態１０について説明する。図２６は、本実施の形態にかかる暗号通信システム２０３を示すブロック図である。本実施の形態では、暗号通信システムを電子署名方式に適用している。本実施の形態にかかる暗号通信システム２０３は、半導体装置ＩＣａ（２５０）、半導体装置ＩＣｚ（２６０）、およびセキュアサーバ２７０を有する。

【０２０５】
半導体装置２５０は、ユニークコード生成部２５１、記憶部２５２、共通鍵生成部２５３、訂正データ生成部２５４、復号部２５５、および検証部２５６を有する。
【０２０６】
ユニークコード生成部２５１は、半導体装置２５０に固有のユニークコードＵＣ（ａ）を生成し、共通鍵生成部２５３に出力する。ユニークコード生成部２５１の基本的な構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。
【０２０７】
記憶部２５２は、訂正データＣＤ（ａ）と、半導体装置２５０の公開鍵ＰＫ（ａ）および秘密鍵ＳＫ（ａ）と、共通鍵生成部２５３で生成された共通鍵ＣＫ（ａ）とを格納することができる。記憶部２５２は、例えば揮発性メモリと不揮発性メモリとを有し、訂正データＣＤ（ａ）、公開鍵ＰＫ（ａ）、および秘密鍵ＳＫ（ａ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部２５２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２５０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。
【０２０８】
共通鍵生成部２５３は、ユニークコード生成部２５１から出力されたユニークコードＵＣ（ａ）と、記憶部２５２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する。ここで、共通鍵生成部２５３はユニークコード訂正部として機能する。共通鍵生成部２５３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。
【０２０９】
訂正データ生成部２５４は、半導体装置２６０のユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成する。訂正データ生成部２５４の基本的な構成および動作は、実施の形態８で説明した訂正データ生成部２１４と同様であるので重複した説明は省略する。
【０２１０】
復号部２５５は、半導体装置２６０の暗号部２６４で暗号化されたユニークコードＵＣ（ｚ）_ｃを、半導体装置２５０の秘密鍵ＳＫ（ａ）を用いて復号してユニークコードＵＣ（ｚ）を生成する。
【０２１１】
検証部２５６は、電子署名方式の検証アルゴリズムを実行する。すなわち、検証部２５６は、署名データＳｉｇ（ｚ）と半導体装置２６０の公開鍵ＰＫ（ｚ）とを用いて検証用データを生成し、当該検証用データと平文Ｐｌａｎｅ（ａ）とを比較する。
【０２１２】
半導体装置２６０は、ユニークコード生成部２６１、記憶部２６２、共通鍵生成部２６３、暗号部２６４、および署名データ生成部２６５を有する。ユニークコード生成部２６１は、半導体装置２６０に固有のユニークコードＵＣ（ｚ）を生成し、暗号部２６４および共通鍵生成部２６３に出力する。なお、ユニークコード生成部２６１の構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。
【０２１３】
記憶部２６２は、共通鍵生成部２６３で生成された共通鍵ＣＫ（ａ）、半導体装置２６０の秘密鍵ＳＫ（ｚ）、および平文Ｐｌａｎｅ（ｚ）を格納することができる。記憶部２６２は、例えば揮発性メモリと不揮発性メモリとを有し、半導体装置２６０の秘密鍵ＳＫ（ｚ）および平文Ｐｌａｎｅ（ｚ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部２６２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２６０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格

納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置２６０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０２１４】

共通鍵生成部２６３は、ユニークコード生成部２６１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部２５４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成する。ここで、共通鍵生成部２６３はユニークコード訂正部として機能する。共通鍵生成部２６３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。

【０２１５】

暗号部２６４は、ユニークコード生成部２６１で生成されたユニークコードＵＣ（ｚ）を半導体装置２６０の公開鍵ＰＫ（ａ）を用いて暗号化する。ここで、暗号化に用いられる公開鍵ＰＫ（ａ）は、予め半導体装置２５０から半導体装置２６０に送付されて記憶部２６２に格納されていてもよい。また、暗号化に用いられる公開鍵ＰＫ（ａ）は、暗号部２６４でユニークコードＵＣ（ｚ）を暗号化する際に、半導体装置２５０から暗号部２６４に直接供給されるように構成してもよい。また、セキュアサーバ２７０から公開鍵ＰＫ（ａ）が供給されるように構成してもよい。暗号化されたユニークコードＵＣ（ｚ）_ｃは半導体装置２５０の復号部２５５に出力される。

【０２１６】

署名データ生成部２６５は、半導体装置２６０の秘密鍵ＳＫ（ｚ）と、平文Ｐｌａｎｅ（ｚ）とを用いて署名データＳｉｇ（ｚ）を生成する。つまり、署名データ生成部２６５は電子署名方式における署名生成アルゴリズムを実行する。

【０２１７】

セキュアサーバ２７０は、半導体装置ＩＣａ、ＩＣｂ、・・・、ＩＣｚと、当該半導体装置ＩＣａ、ＩＣｂ、・・・、ＩＣｚの公開鍵ＰＫ（ａ）、ＰＫ（ｂ）、・・・、ＰＫ（ｚ）とを対応づけて格納したデータベース２７１を備える。本実施の形態では、データベース２７１に格納されている公開鍵情報はセキュリティレベルの高い情報であるので、セキュアサーバ２７０にはセキュリティマイコンを用いることが好ましい。セキュアサーバ２７０に格納されている公開鍵情報は、要求に応じて各半導体装置に送付される。

【０２１８】

次に、本実施の形態にかかる暗号通信システムの動作について、図２７に示すフローチャートを用いて説明する。まず、半導体装置ＩＣａ（２５０）の共通鍵生成部２５３は、ユニークコード生成部２５１から出力されたユニークコードＵＣ（ａ）と、記憶部２５２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１４１）。その後、半導体装置ＩＣａ（２５０）は他の半導体装置ＩＣｂ～ＩＣｙ（不図示）と共通鍵ＣＫ（ａ）を用いて通信を開始する（ステップＳ１４２）。

【０２１９】

次に、半導体装置ＩＣｚ（２６０）は、半導体装置ＩＣａ（２５０）に対して半導体装置ＩＣｚ（２６０）の半導体装置情報（例えば固有ＩＤなど）を送付する（ステップＳ１４３）。半導体装置２６０の半導体装置情報を取得した半導体装置２５０は、セキュアサーバ２７０に対して、半導体装置２６０の公開鍵を送付するように要求する（ステップＳ１４４）。ここで、半導体装置２６０の公開鍵は、半導体装置２５０の検証部２５６において署名データを検証する際に用いられる。セキュアサーバ２７０は、半導体装置２５０の検証部２５６に半導体装置２６０の公開鍵ＰＫ（ｚ）を送付する（ステップＳ１４５）。

【０２２０】

次に、半導体装置２５０は半導体装置２６０に対して署名データを送付するように要求する（ステップＳ１４６）。署名データ送付要求を受信した半導体装置２６０は、署名データ生成部２６５において、秘密鍵ＳＫ（ｚ）と平文Ｐｌａｎｅ（ｚ）とを用いて署名データＳｉｇ（ｚ）を生成する。そして、平文Ｐｌａｎｅ（ｚ）および生成された署名デー

タＳｉｇ（ｚ）は半導体装置２５０の検証部２５６に送付される（ステップＳ１４７）。
【０２２１】
半導体装置２５０の検証部２５６は、電子署名方式の検証アルゴリズムを実行する（ステップＳ１４８）。すなわち、検証部２５６は、セキュアサーバ２７０から供給された半導体装置２６０の公開鍵ＰＫ（ｚ）と、署名データＳｉｇ（ｚ）とを用いて検証用データを生成し、当該検証用データと平文Ｐｌａｎｅ（ｚ）とを比較する。ここで、署名データＳｉｇ（ｚ）は、半導体装置２６０の秘密鍵ＳＫ（ｚ）を用いて平文Ｐｌａｎｅ（ｚ）を暗号化することで生成されたデータである。よって、署名データＳｉｇ（ｚ）を半導体装置２６０の公開鍵ＰＫ（ｚ）を用いて復号することで得られた検証用データは、半導体装置２６０から送られた平文Ｐｌａｎｅ（ｚ）に対応するデータである。したがって、検証部２５６は、検証用データと平文Ｐｌａｎｅ（ｚ）とを比較し、検証用データと平文Ｐｌａｎｅ（ｚ）とが一致した場合は、半導体装置２６０が秘密鍵ＳＫ（ｚ）を保有すると判断することができる。
【０２２２】
よって、検証用データと平文Ｐｌａｎｅ（ｚ）とが一致した場合（検証アルゴリズムが署名データＳｉｇ（ｚ）を受理した場合）は、検証部２５６は半導体装置２６０が作成した署名データＳｉｇ（ｚ）が正当であると判断する。つまり、半導体装置２６０が秘密鍵ＳＫ（ｚ）を保有すると判断される。一方、検証用データと平文Ｐｌａｎｅ（ｚ）とが一致しない場合（検証アルゴリズムが署名データＳｉｇ（ｚ）を棄却した場合）は、検証部２５６は半導体装置２６０が作成した署名データＳｉｇ（ｚ）が不当であると判断する。
【０２２３】
半導体装置２６０が正規の半導体装置であると判断されると、半導体装置２５０は、半導体装置２６０に対して半導体装置２５０の公開鍵ＰＫ（ａ）を送付する（ステップＳ１４９）。半導体装置２６０の暗号部２６４は、半導体装置２５０の公開鍵ＰＫ（ａ）を用いてユニークコードＵＣ（ｚ）を暗号化する（ステップＳ１５０）。なお、半導体装置２５０の公開鍵ＰＫ（ａ）は、半導体装置２５０の指示によりセキュアサーバ２７０から半導体装置２６０に送付されるようにしてもよい。
【０２２４】
半導体装置２６０は、暗号化されたユニークコードＵＣ（ｚ）_ｃを半導体装置２５０の復号部２５５に送付する（ステップＳ１５１）。半導体装置２５０の復号部２５５は、暗号化されたユニークコードＵＣ（ｚ）_ｃを、半導体装置２５０の秘密鍵ＳＫ（ａ）を用いて復号してユニークコードＵＣ（ｚ）を生成する（ステップＳ１５２）。
【０２２５】
半導体装置２５０の訂正データ生成部２５４は、半導体装置２６０のユニークコードＵＣ（ｚ）と、共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成する（ステップＳ１５３）。訂正データ生成部２５４が訂正データＣＤ（ｚ）を生成するには、ユニークコードＵＣ（ｚ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ｚ）を複数回取得するためにステップＳ１５０～Ｓ１５２を繰り返す。
【０２２６】
生成された訂正データＣＤ（ｚ）は半導体装置２６０の共通鍵生成部２６３に送付される（ステップＳ１５４）。半導体装置２６０の共通鍵生成部２６３は、ユニークコード生成部２６１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部２５４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１５５）。上記処理により、新たに追加された半導体装置２６０を電子署名方式を用いて検証することができる。そして、新たに追加された半導体装置２６０が正規の半導体装置である場合、半導体装置２６０は共通鍵ＣＫ（ａ）を保持することができる。よって、新たに追加された半導体装置（ＩＣｚ）２６０は、半導体装置（ＩＣａ）２４０および他の半導体装置ＩＣｂ～ＩＣｙと共通鍵ＣＫ（ａ）を用いて暗号通信することが可能となる（ステップＳ１５６）。
【０２２７】

このように、本実施の形態にかかる暗号通信システムでは、半導体装置２５０が備える訂正データ生成部２５４において、半導体装置２６０に固有のユニークコードＵＣ（ｚ）と、共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成し、半導体装置２６０の共通鍵生成部２６３において、この訂正データＣＤ（ｚ）と半導体装置２６０のユニークコードＵＣ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成している。よって、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証するために、高価なセキュアサーバを暗号通信システムに組み込む必要がないので、セキュアな通信を実施している暗号通信システムに、半導体装置を容易かつ低コストに追加することができる。

【０２２８】

また、本実施の形態にかかる暗号通信システムでは、共通鍵ＣＫ（ａ）などの重要なデータを記憶部２５２、２６２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（ａ）などの重要なデータが漏洩することはない。このため、本実施の形態にかかる暗号通信システムでは、半導体装置２５０および半導体装置２６０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。

【０２２９】

一方、本実施の形態では、セキュアサーバ２７０のデータベース２７１に格納されている公開鍵情報はセキュリティレベルの高い情報である。よって、セキュアサーバ２７０にはセキュリティマイコンを用いることが好ましい。

【０２３０】

なお、共通鍵ＣＫ（ａ）を生成するために使用される訂正データＣＤ（ａ）や半導体装置２６０の秘密鍵ＳＫ（ｚ）は、共通鍵ＣＫ（ａ）よりもセキュリティレベルは低いが、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ａ）や秘密鍵ＳＫ（ｚ）が第三者に漏洩することを防ぐために、訂正データＣＤ（ａ）や秘密鍵ＳＫ（ｚ）が格納される半導体装置２５０、２６０にセキュアマイコンを使用してもよい。

【０２３１】

また、半導体装置２５０から半導体装置２６０に送付される訂正データＣＤ（ｚ）は、ユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とに関連するデータであるため、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ｚ）を半導体装置５０から半導体装置２６０に送付する際は、公開鍵暗号方式を用いて訂正データＣＤ（ｚ）を暗号化して送付してもよい。

【０２３２】

また、本実施の形態ではユニークコードＵＣ（ｚ）を暗号化して送付するために、半導体装置２６０に暗号部２６４を設け、半導体装置２５０に復号部２５５を設けていた。しかし、本実施の形態では、実施の形態８のように、暗号部２６４および復号部２５５を省略して、ユニークコードＵＣ（ｚ）を暗号化しないで送付してもよい。

【０２３３】

以上で説明したように、本実施の形態にかかる発明により、セキュアな通信を実施している暗号通信システムに、半導体装置を容易に追加することができる暗号通信システムおよび暗号通信方法を提供することができる。

【０２３４】

特に、本実施の形態にかかる暗号通信システムでは、セキュアサーバ２７０を用いて公開鍵情報を一括して管理している。この公開鍵情報は、新たに追加される半導体装置を電子署名方式を用いて検証する際に使用される情報であり、セキュリティレベルの高い情報である。このように、セキュリティレベルの高い情報をセキュアサーバ２７０を用いて一括管理することで、半導体装置２５０、２６０にセキュリティレベルの高い情報を格納する必要がなくなり、半導体装置２５０、２６０を汎用のマイコンを用いて構成することができる。よって、暗号通信システムを構成する際のコストを低減することができる。

【０２３５】

＜実施の形態１１＞

次に、本発明の実施の形態１１について説明する。図２８は、本実施の形態にかかる暗号通信システム２０４を示すブロック図である。本実施の形態にかかる暗号通信システム４では、訂正データＣＤ（ｚ）を生成するための訂正データ生成部を設ける代わりに、新規に追加される半導体装置ＩＣｚ（２９０）から半導体装置ＩＣａ（２８０）に訂正データ生成プログラムＰＲＧ（ｚ）を送付している。そして、この訂正データ生成プログラムＰＲＧ（ｚ）を半導体装置ＩＣａ（２８０）で実行することで、訂正データＣＤ（ｚ）を生成している。

【０２３６】

図２８に示す暗号通信システム２０４は、半導体装置ＩＣａ（２８０）と半導体装置ＩＣｚ（２９０）とを有する。半導体装置２８０は、ユニークコード生成部２８１、記憶部２８２、共通鍵生成部２８３、プログラム実行部２８４、および復号部２８５を有する。

【０２３７】

ユニークコード生成部２８１は、半導体装置２８０に固有のユニークコードＵＣ（ａ）を生成し、共通鍵生成部２８３に出力する。ユニークコード生成部２８１の基本的な構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。

【０２３８】

記憶部２８２は、訂正データＣＤ（ａ）と、半導体装置２８０の公開鍵ＰＫ（ａ）および秘密鍵ＳＫ（ａ）と、共通鍵生成部２８３で生成された共通鍵ＣＫ（ａ）とを格納することができる。記憶部２８２は、例えば揮発性メモリと不揮発性メモリとを有し、訂正データＣＤ（ａ）、公開鍵ＰＫ（ａ）、および秘密鍵ＳＫ（ａ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部２８２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２８０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。

【０２３９】

共通鍵生成部２８３は、ユニークコード生成部２８１から出力されたユニークコードＵＣ（ａ）と、記憶部２８２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する。ここで、共通鍵生成部２８３はユニークコード訂正部として機能する。共通鍵生成部２８３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。

【０２４０】

プログラム実行部２８４は、半導体装置２９０から送付された訂正データ生成プログラムＰＲＧ（ｚ）を実行する。訂正データ生成プログラムＰＲＧ（ｚ）を実行することにより、半導体装置２９０のユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成することができる。ここで、プログラム実行部２８４は、典型的にはＣＰＵなどのプロセッサである。また、訂正データ生成プログラムＰＲＧ（ｚ）は、例えば半導体装置２８０のみで実行可能なプログラムであってもよい。また、動作する半導体装置のアーキテクチャに依存しない、ＪＡＶＡ（登録商標）等のプログラムであってもよい。暗号通信システムを構成する半導体装置の中には、ＣＰＵコアのアーキテクチャが異なる場合もある。よって、動作する半導体装置のアーキテクチャに依存しないＪＡＶＡ等のプログラムを用いることで、暗号通信システムの利便性を向上させることができ、また、暗号通信システムのコストを低減させることができる。

【０２４１】

なお、訂正データ生成プログラムＰＲＧ（ｚ）を用いて訂正データＣＤ（ｚ）を生成する処理については、実施の形態８で説明した訂正データ生成部２１４における処理と同様であるので重複した説明は省略する。

【０２４２】

復号部２８５は、半導体装置２９０の暗号部２９４で暗号化されたユニークコードＵＣ（ｚ）_ｃを、半導体装置２８０の秘密鍵ＳＫ（ａ）を用いて復号してユニークコードＵＣ（ｚ）を生成する。

【０２４３】
半導体装置２９０は、ユニークコード生成部２９１、記憶部２９２、共通鍵生成部２９３、および暗号部２９４を有する。ユニークコード生成部２９１は、半導体装置２９０に固有のユニークコードＵＣ（ｚ）を生成し、暗号部２９４および共通鍵生成部２９３に出力する。なお、ユニークコード生成部２９１の構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。
【０２４４】
記憶部２９２は、共通鍵生成部２９３で生成された共通鍵ＣＫ（ａ）および訂正データ生成プログラムＰＲＧ（ｚ）を格納することができる。記憶部２９２は、例えば揮発性メモリと不揮発性メモリとを有し、訂正データ生成プログラムＰＲＧ（ｚ）は不揮発性メモリに格納され、共通鍵ＣＫ（ａ）は揮発性メモリに格納される。よって、記憶部２９２は一時的に共通鍵ＣＫ（ａ）を格納するが、半導体装置２９０の電源がオフになると共通鍵ＣＫ（ａ）の情報は消去される。尚、共通鍵ＣＫ（ａ）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（ａ）に対して、半導体装置２９０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。
【０２４５】
共通鍵生成部２９３は、ユニークコード生成部２９１から出力されたユニークコードＵＣ（ｚ）と、プログラム実行部２８４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成する。ここで、共通鍵生成部２９３はユニークコード訂正部として機能する。共通鍵生成部２９３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。
【０２４６】
暗号部２９４は、ユニークコードＵＣ（ｚ）および訂正データ生成プログラムＰＲＧ（ｚ）を半導体装置２８０の公開鍵ＰＫ（ａ）を用いて暗号化する。ここで、暗号化に用いられる公開鍵ＰＫ（ａ）は、予め半導体装置２８０から半導体装置２９０に送付されて記憶部２９２に格納されていてもよい。また、暗号化に用いられる公開鍵ＰＫ（ａ）は、暗号部２９４でユニークコードＵＣ（ｚ）および訂正データ生成プログラムＰＲＧ（ｚ）を暗号化する際に、半導体装置２８０から暗号部２９４に直接供給されるように構成してもよい。暗号化されたユニークコードＵＣ（ｚ）_ｃおよび訂正データ生成プログラムＰＲＧ（ｚ）_ｃは半導体装置２８０の復号部２８５に出力される。
【０２４７】
次に、本実施の形態にかかる暗号通信システムの動作について、図２９に示すフローチャートを用いて説明する。まず、半導体装置ＩＣａ（２８０）の共通鍵生成部２８３は、ユニークコード生成部２８１から出力されたユニークコードＵＣ（ａ）と、記憶部２８２に格納されている訂正データＣＤ（ａ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１６０）。その後、半導体装置ＩＣａ（２８０）は他の半導体装置ＩＣｂ～ＩＣｙ（不図示）と共通鍵ＣＫ（ａ）を用いて通信を開始する（ステップＳ１６１）。
【０２４８】
次に、半導体装置ＩＣｚ（２９０）は、半導体装置ＩＣａ（２８０）に対して訂正データＣＤ（ｚ）の送付を要求する（ステップＳ１６２）。訂正データＣＤ（ｚ）の送付を要求された半導体装置２８０は、半導体装置２９０に対して半導体装置２８０の公開鍵ＰＫ（ａ）を送付する（ステップＳ１６３）。半導体装置２９０の暗号部２９４は、半導体装置２８０の公開鍵ＰＫ（ａ）を用いてユニークコードＵＣ（ｚ）および訂正データ生成プログラムＰＲＧ（ｚ）を暗号化する（ステップＳ１６４）。なお、半導体装置２８０の公開鍵ＰＫ（ａ）は、予め半導体装置２９０の記憶部２９２に格納しておいてもよい。この場合は、ステップＳ１６２、Ｓ１６３を省略することができる。
【０２４９】
半導体装置２９０は、暗号化されたユニークコードＵＣ（ｚ）_ｃおよび訂正データ生成プログラムＰＲＧ（ｚ）_ｃを半導体装置２８０の復号部２８５に送付する（ステップ

Ｓ１６５）。半導体装置２８０の復号部２８５は、暗号化されたユニークコードＵＣ（ｚ）_ｃおよび訂正データ生成プログラムＰＲＧ（ｚ）_ｃを、半導体装置２８０の秘密鍵ＳＫ（ａ）を用いて復号してユニークコードＵＣ（ｚ）および訂正データ生成プログラムＰＲＧ（ｚ）を生成する（ステップＳ１６６）。

【０２５０】

半導体装置２８０のプログラム実行部２８４は、復号部２８５で復号された訂正データ生成プログラムＰＲＧ（ｚ）を実行する。訂正データ生成プログラムＰＲＧ（ｚ）を実行することにより、半導体装置２９０のユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成することができる（ステップＳ１６７）。なお、訂正データ生成プログラムＰＲＧ（ｚ）が訂正データＣＤ（ｚ）を生成するには、ユニークコードＵＣ（ｚ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ｚ）を複数回取得するためにステップＳ１６４～Ｓ１６６を繰り返す（訂正データ生成プログラムＰＲＧ（ｚ）の送付は除く）。また、訂正データ生成プログラムＰＲＧ（ｚ）は、訂正データＣＤ（ｚ）を生成した後に削除してもよい。

【０２５１】

生成された訂正データＣＤ（ｚ）は半導体装置２９０の共通鍵生成部２９３に送付される（ステップＳ１６８）。半導体装置２９０の共通鍵生成部２９３は、ユニークコード生成部２９１から出力されたユニークコードＵＣ（ｚ）と、プログラム実行部２８４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成する（ステップＳ１６９）。上記処理により、新たに追加された半導体装置２９０は共通鍵ＣＫ（ａ）を保持することができる。よって、新たに追加された半導体装置（ＩＣｚ）２９０は、半導体装置（ＩＣａ）２８０および他の半導体装置ＩＣｂ～ＩＣｙと共通鍵ＣＫ（ａ）を用いて暗号通信することが可能となる（ステップＳ１７０）。

【０２５２】

このように、本実施の形態にかかる暗号通信システムでは、半導体装置２８０が備えるプログラム実行部２８４において、半導体装置２９０に固有のユニークコードＵＣ（ｚ）と、共通鍵ＣＫ（ａ）とを用いて訂正データＣＤ（ｚ）を生成し、半導体装置２９０の共通鍵生成部２９３において、この訂正データＣＤ（ｚ）と半導体装置２９０のユニークコードＵＣ（ｚ）とを用いて共通鍵ＣＫ（ａ）を生成している。よって、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証するために、高価なセキュアサーバを暗号通信システムに組み込む必要がないので、セキュアな通信を実施している暗号通信システムに、半導体装置を容易かつ低コストに追加することができる。

【０２５３】

また、本実施の形態にかかる暗号通信システムでは、共通鍵ＣＫ（ａ）などの重要なデータを記憶部２８２、２９２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（ａ）などの重要なデータが漏洩することはない。このため、本実施の形態にかかる暗号通信システムでは、半導体装置２８０および半導体装置２９０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。

【０２５４】

なお、半導体装置２８０において共通鍵ＣＫ（ａ）を生成するために使用される訂正データＣＤ（ａ）や半導体装置２８０の秘密鍵ＳＫ（ａ）は、共通鍵ＣＫ（ａ）よりもセキュリティレベルは低いが、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ａ）や秘密鍵ＳＫ（ａ）が第三者に漏洩することを防ぐために、訂正データＣＤ（ａ）および秘密鍵ＳＫ（ａ）が格納される半導体装置２８０にセキュアマイコンを使用してもよい。

【０２５５】

また、半導体装置２８０から半導体装置２９０に送付される訂正データＣＤ（ｚ）は、ユニークコードＵＣ（ｚ）と共通鍵ＣＫ（ａ）とに関連するデータであるため、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ｚ）を半導体装置２８０

から半導体装置２９０に送付する際は、公開鍵暗号方式を用いて訂正データＣＤ（ｚ）を暗号化して送付してもよい。

【０２５６】

また、本実施の形態ではユニークコードＵＣ（ｚ）および訂正データ生成プログラムＰＲＧ（ｚ）を暗号化して送付するために、半導体装置２６０に暗号部２６４を設け、半導体装置２５０に復号部２５５を設けていた。しかし、本実施の形態では、実施の形態８のように、暗号部２６４および復号部２５５を省略して、ユニークコードＵＣ（ｚ）および訂正データ生成プログラムＰＲＧ（ｚ）を暗号化しないで送付してもよい。

【０２５７】

また、上述した例では、新規に追加される半導体装置２９０から半導体装置２８０に訂正データ生成プログラムＰＲＧ（ｚ）が送付される場合について説明した。しかし、訂正データ生成プログラムＰＲＧ（ｚ）は、例えばサーバから半導体装置２８０に送付されるように構成してもよい。

【０２５８】

以上で説明したように、本実施の形態にかかる発明により、セキュアな通信を実施している暗号通信システムに、半導体装置を容易に追加することができる暗号通信システムおよび暗号通信方法を提供することができる。

【０２５９】

特に、本実施の形態にかかる暗号通信システムでは、半導体装置２８０に訂正データ生成部を予め設けていない場合であっても、新規に追加する半導体装置２９０に訂正データ生成プログラムＰＲＧ（ｚ）を格納し、当該訂正データ生成プログラムＰＲＧ（ｚ）を半導体装置２８０で実行することで、訂正データＣＤ（ｚ）を生成することができる。ここで、訂正データ生成プログラムＰＲＧ（ｚ）は、半導体装置２９０の出荷時に格納してもよく、また、出荷後に必要に応じてサーバからダウンロードしてもよい。また、訂正データ生成プログラムＰＲＧ（ｚ）を、動作する半導体装置のアーキテクチャに依存しないＪＡＶＡ等のプログラムとすることで、暗号通信システムの利便性を向上させることができ、また、暗号通信システムのコストを低減させることができる。

【０２６０】

＜実施の形態１２＞

次に、本発明の実施の形態１２について説明する。図３０は、本実施の形態にかかる暗号通信システム２０５を示すブロック図である。本実施の形態にかかる暗号通信システム２０５では、半導体装置ＩＣａ（３００）の共通鍵生成部３０３で複数の共通鍵ＣＫ（１）、ＣＫ（２）を生成している。そして、半導体装置ＩＣａ（３００）と半導体装置ＩＣｚ（３１０）とが共通鍵ＣＫ（２）を用いて通信し、半導体装置ＩＣａ（３００）と半導体装置ＩＣｂ～ＩＣｙとが共通鍵ＣＫ（１）を用いて通信している。つまり、半導体装置ＩＣａ（３００）はルータとしての機能を備える。

【０２６１】

図３０に示す暗号通信システム２０５は、半導体装置ＩＣａ（３００）と半導体装置ＩＣｚ（３１０）とを有する。半導体装置３００は、ユニークコード生成部３０１、記憶部３０２、共通鍵生成部３０３、および訂正データ生成部３０４を有する。

【０２６２】

ユニークコード生成部３０１は、半導体装置３００に固有のユニークコードＵＣ（ａ）を生成し、共通鍵生成部３０３に出力する。ユニークコード生成部３０１の基本的な構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。

【０２６３】

記憶部３０２は、訂正データＣＤ（１）、ＣＤ（２）と、共通鍵生成部３０３で生成された共通鍵ＣＫ（１）、ＣＫ（２）とを格納することができる。記憶部３０２は、例えば揮発性メモリと不揮発性メモリとを有し、訂正データＣＤ（１）、ＣＤ（２）は不揮発性メモリに格納され、共通鍵ＣＫ（１）、ＣＫ（２）は揮発性メモリに格納される。よって

、記憶部３０２は一時的に共通鍵ＣＫ（１）、ＣＫ（２）を格納するが、半導体装置３００の電源がオフになると共通鍵ＣＫ（１）、ＣＫ（２）の情報は消去される。尚、共通鍵ＣＫ（１）、ＣＫ（２）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（１）、ＣＫ（２）対して、半導体装置３００の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０２６４】

共通鍵生成部３０３は、ユニークコード生成部３０１から出力されたユニークコードＵＣ（ａ）と、記憶部３０２に格納されている訂正データ（第３の訂正データ）ＣＤ（１）とを用いて共通鍵（第２の共通鍵）ＣＫ（１）を生成する。また、共通鍵生成部３０３は、ユニークコード生成部３０１から出力されたユニークコードＵＣ（ａ）と、記憶部３０２に格納されている訂正データ（第１の訂正データ）ＣＤ（２）とを用いて共通鍵（第１の共通鍵）ＣＫ（２）を生成する。ここで、共通鍵生成部３０３はユニークコード訂正部として機能する。共通鍵生成部３０３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。

【０２６５】

訂正データ生成部３０４は、半導体装置３１０のユニークコードＵＣ（ｚ）と共通鍵ＣＫ（２）とを用いて訂正データ（第２の訂正データ）ＣＤ（ｚ）を生成する。訂正データ生成部３０４の基本的な構成および動作は、実施の形態８で説明した訂正データ生成部２１４と同様であるので重複した説明は省略する。

【０２６６】

半導体装置３１０は、ユニークコード生成部３１１、記憶部３１２、および共通鍵生成部３１３を有する。ユニークコード生成部３１１は、半導体装置３１０に固有のユニークコードＵＣ（ｚ）を生成し、半導体装置３００の訂正データ生成部３０４に出力する。なお、ユニークコード生成部３１１の構成および動作は、実施の形態８で説明したユニークコード生成部２１１と同様であるので重複した説明は省略する。

【０２６７】

記憶部３１２は、共通鍵生成部３１３で生成された共通鍵ＣＫ（２）を格納することができる。記憶部３１２は、揮発性メモリに共通鍵ＣＫ（２）を格納する。よって、記憶部３１２は一時的に共通鍵ＣＫ（２）を格納するが、半導体装置３１０の電源がオフになると共通鍵ＣＫ（２）の情報は消去される。尚、共通鍵ＣＫ（２）は用途に応じて暗号化等のセキュリティ対策を行い不揮発性メモリに格納してもよく、不揮発性メモリに格納された共通鍵ＣＫ（２）対して、半導体装置３１０の電源オフ時にライト動作によりデータの消去を行なう等の処置を行う対策を行ってもよい。

【０２６８】

共通鍵生成部３１３は、ユニークコード生成部３１１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部３０４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（２）を生成する。ここで、共通鍵生成部３１３はユニークコード訂正部として機能する。共通鍵生成部３１３の基本的な構成および動作は、実施の形態８で説明した共通鍵生成部２１３と同様であるので重複した説明は省略する。

【０２６９】

次に、本実施の形態にかかる暗号通信システムの動作について、図３１に示すフローチャートを用いて説明する。まず、半導体装置ＩＣａ（３００）の共通鍵生成部３０３は、ユニークコード生成部３０１から出力されたユニークコードＵＣ（ａ）と、記憶部２１２に格納されている訂正データＣＤ（１）とを用いて共通鍵ＣＫ（１）を生成する（ステップＳ１７１）。その後、半導体装置ＩＣａ（３００）は他の半導体装置ＩＣｂ～ＩＣｙ（第３の半導体装置）と共通鍵ＣＫ（１）を用いて通信を開始する（ステップＳ１７２）。

【０２７０】

半導体装置３１０は、半導体装置３００の訂正データ生成部３０４に半導体装置３１０のユニークコードＵＣ（ｚ）を送付する（ステップＳ１７３）。半導体装置３００の共通

鍵生成部３０３は、ユニークコード生成部３０１から出力されたユニークコードＵＣ（ａ）と、記憶部３０２に格納されている訂正データＣＤ（２）とを用いて共通鍵ＣＫ（２）を生成する（ステップＳ１７４）。その後、半導体装置３００の訂正データ生成部３０４は、半導体装置３１０のユニークコードＵＣ（ｚ）と、共通鍵ＣＫ（２）とを用いて訂正データＣＤ（ｚ）を生成する（ステップＳ１７５）。訂正データ生成部３０４が訂正データＣＤ（ｚ）を生成するには、ユニークコードＵＣ（ｚ）を複数回取得する必要がある。よって、ユニークコードＵＣ（ｚ）を複数回取得するためにステップＳ１７３を繰り返す。

【０２７１】

生成された訂正データＣＤ（ｚ）は半導体装置３１０の共通鍵生成部３１３に送付される（ステップＳ１７６）。半導体装置３１０の共通鍵生成部３１３は、ユニークコード生成部３１１から出力されたユニークコードＵＣ（ｚ）と、訂正データ生成部３０４から出力された訂正データＣＤ（ｚ）とを用いて共通鍵ＣＫ（２）を生成する（ステップＳ１７７）。上記処理により、半導体装置３００と半導体装置３１０は共に共通鍵ＣＫ（２）を保持することができる。よって、新たに追加された半導体装置３１０は、半導体装置３００と共通鍵ＣＫ（２）を用いて暗号通信することが可能となる（ステップＳ１７８）。一方、半導体装置３００と半導体装置ＩＣｂ～ＩＣｙは共通鍵ＣＫ（１）を用いて通信している。

【０２７２】

図３２は、本実施の形態にかかる暗号通信システムの構成の一例を示すブロック図である。図３２に示すように、半導体装置ＩＣａと半導体装置ＩＣｂ、ＩＣｃは共通鍵ＣＫ（１）を用いて通信をしており、セキュアなネットワークを構成している。また、新たに追加された半導体装置ＩＣｚは、半導体装置ＩＣａと共通鍵ＣＫ（２）を用いて通信する。よって、半導体装置ＩＣａがルータとしての機能を備えることで、新たに追加された半導体装置ＩＣｚは、半導体装置ＩＣｂ、ＩＣｃと半導体装置ＩＣａを介して暗号通信することができる。

【０２７３】

このように、本実施の形態にかかる暗号通信システムでは、半導体装置３００が備える訂正データ生成部３０４において、半導体装置３１０に固有のユニークコードＵＣ（ｚ）と、共通鍵ＣＫ（２）とを用いて訂正データＣＤ（ｚ）を生成し、半導体装置３１０の共通鍵生成部３１３において、この訂正データＣＤ（ｚ）と半導体装置３１０のユニークコードＵＣ（ｚ）とを用いて共通鍵ＣＫ（２）を生成している。よって、追加される半導体装置ＩＣｚが正規の半導体装置であるかを検証するために、高価なセキュアサーバを暗号通信システムに組み込む必要がないので、セキュアな通信を実施している暗号通信システムに、半導体装置を容易かつ低コストに追加することができる。

【０２７４】

また、本実施の形態にかかる暗号通信システムでは、共通鍵ＣＫ（１）、ＣＫ（２）などの重要なデータを記憶部３０２、３１２に直接格納していないため、半導体装置が不正に解析されたとしても、共通鍵ＣＫ（１）、ＣＫ（２）などの重要なデータが漏洩することはない。このため、本実施の形態にかかる暗号通信システムでは、半導体装置３００および半導体装置３１０をセキュリティレベルが比較的低い汎用マイコンを用いて構成したとしても、高いセキュリティレベルを実現することができる。

【０２７５】

なお、共通鍵ＣＫ（１）、ＣＫ（２）を生成するために使用される訂正データＣＤ（１）、ＣＤ（２）は、共通鍵ＣＫ（１）、ＣＫ（２）よりもセキュリティレベルは低いが、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（１）、ＣＤ（２）が第三者に漏洩することを防ぐために、訂正データＣＤ（１）、ＣＤ（２）が格納される半導体装置３００にセキュアマイコンを使用してもよい。

【０２７６】

また、半導体装置３００から半導体装置３１０に送付される訂正データＣＤ（ｚ）は、

ユニークコードＵＣ（ｚ）と共通鍵ＣＫ（２）とに関連するデータであるため、比較的セキュリティレベルの高い情報である。よって、訂正データＣＤ（ｚ）を半導体装置３００から半導体装置３１０に送付する際は、公開鍵暗号方式を用いて訂正データＣＤ（ｚ）を暗号化して送付してもよい。

【０２７７】

以上で説明したように、本実施の形態にかかる発明により、セキュアな通信を実施している暗号通信システムに、半導体装置を容易に追加することができる暗号通信システムおよび暗号通信方法を提供することができる。

【０２７８】

＜実施の形態１３＞

次に、本発明の実施の形態１３について説明する。図３３は実施の形態８乃至１２にかかる暗号通信システムを車載用半導体装置に適用した場合を示すブロック図である。図３３に示すように、車両３６０にはゲートウェイ部３５０、故障診断ユニット３５１、エンジン制御ユニット３５２、ブレーキ制御ユニット３５３、ランプ制御ユニット３５４、ドアロック制御ユニット３５５、鍵挿入制御ユニット３５６が設けられている。

【０２７９】

ゲートウェイ部３５０は、各ユニット３５１～３５６で構成されるネットワークを中継するための機器である。ゲートウェイ部３５０にはセキュアマイコンＩＣａが設けられている。故障診断ユニット３５１は、車両３６０を構成する部品が故障しているか診断するユニットである。故障診断ユニット３５１には半導体装置ＩＣｂが設けられている。エンジン制御ユニット３５２は、エンジン動作における電気的な制御（燃料供給、点火タイミングの調整等）を総合的に行うためのユニットである。エンジン制御ユニット３５２には半導体装置ＩＣｃが設けられている。ブレーキ制御ユニット３５３は、ＡＢＳ（Antilock Brake System）などブレーキを制御するためのユニットである。ブレーキ制御ユニット３５３には半導体装置ＩＣｄが設けられている。ランプ制御ユニット３５４は、車両のヘッドライトやウインカー等を制御するためのユニットである。ランプ制御ユニット３５４には半導体装置ＩＣｅが設けられている。

【０２８０】

ドアロック制御ユニット３５５は、ドアのロックを制御するためのユニットである。ドアロック制御ユニット３５５には半導体装置ＩＣｆと、鍵３５７と無線通信するための通信部が設けられている。鍵挿入制御ユニット３５６は、挿入された鍵が正規のユーザの鍵であるかを判断するためのユニットである。鍵挿入制御ユニット３５６には、半導体装置ＩＣｇと、鍵３５７と無線通信するための通信部が設けられている。鍵３５７には半導体装置ＩＣｈと、通信部が設けられている。各ユニット３５１～３５６、および鍵３５７に設けられている半導体装置ＩＣｂ～ＩＣｈには、例えば汎用マイコンを用いることができる。

【０２８１】

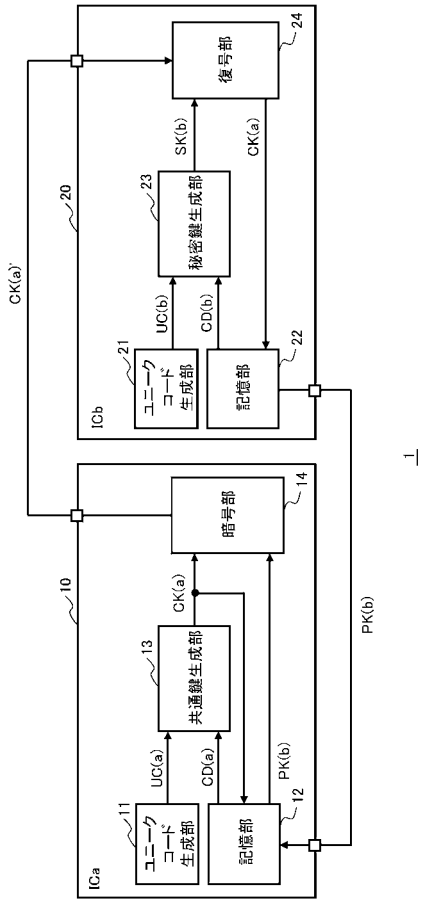
故障診断ユニット３５１、エンジン制御ユニット３５２、ブレーキ制御ユニット３５３、ランプ制御ユニット３５４、ドアロック制御ユニット３５５、および鍵挿入制御ユニット３５６はそれぞれゲートウェイ部３５０と接続されており、各ユニット３５１～３５６はゲートウェイ部３５０を介して互いに通信可能に構成されている。このとき、各ユニット３５１～３５６とゲートウェイ部３５０との間の通信に用いる共通鍵は、ユニット毎に異なるようにしてもよい。例えば故障診断ユニット３５１とゲートウェイ部３５０との通信に共通鍵Ａを用い、エンジン制御ユニット３５２とゲートウェイ部３５０との通信に共通鍵Ｂを用いるように構成してもよい。

【０２８２】

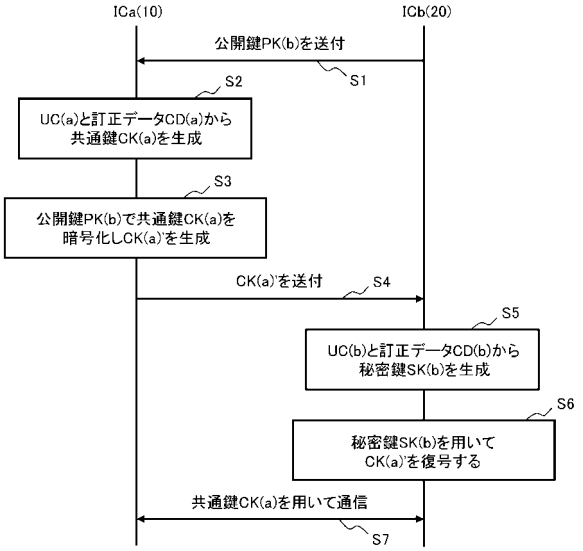
ゲートウェイ部（ＩＣａ）３５０および各ユニット（ＩＣｂ～ＩＣｇ）３５１～３５６は、セキュアなネットワークを構成している。このようなセキュアなネットワークに、半導体装置ＩＣｚを含むカーナビゲーションシステム３５８を新たに追加する際に、実施の形態８乃至１２で説明した方法を用いることで、カーナビゲーションシステム（ＩＣｚ）

３５８をセキュアなネットワークに容易かつ低コストに追加することができる。
【０２８３】
図３３に示した例では、各ユニット３５１～３５６およびカーナビゲーションシステム３５８がゲートウェイ部３５０を介して通信している構成を示した。しかし、各ユニット３５１～３５６およびカーナビゲーションシステム３５８が互いに同一の共通鍵を用いて通信するように構成してもよい。この場合は、例えば各ユニット３５１～３５６およびカーナビゲーションシステム３５８が共通バスを介して互いに接続されるように構成する。また、図３３に示したユニット以外の様々なユニット間の通信にも適用可能である。
【０２８４】
なお、本実施の形態では、実施の形態１～６、８～１２にかかる暗号通信システムを車載用半導体装置に適用した場合について説明した。しかし、実施の形態１～６、８～１２にかかる暗号通信システムは車載用半導体装置以外にも、一般的なＬＡＮ、スマートメータ、スマートグリッド、非接触ＩＣカードなどに適用することができる。このとき、暗号通信システムを構成する半導体装置は互いに有線で通信してもよく、また互いに無線で通信するように構成してもよい。また、上記実施の形態１乃至１３は適宜、互いに組み合わせることができる。
【０２８５】
以上、本発明を上記実施形態に即して説明したが、上記実施形態の構成にのみ限定されるものではなく、本願特許請求の範囲の請求項の発明の範囲内で当業者であればなし得る各種変形、修正、組み合わせを含むことは勿論である。
【符号の説明】
【０２８６】
１　暗号通信システム
１０　半導体装置
１１　ユニークコード生成部
１２　記憶部
１３　共通鍵生成部
１４　暗号部
２０　半導体装置
２１　ユニークコード生成部
２２　記憶部
２３　秘密鍵生成部
２４　復号部
２０１　暗号通信システム
２１０　半導体装置
２１１　ユニークコード生成部
２１２　記憶部
２１３　共通鍵生成部
２１４　訂正データ生成部
２２０　半導体装置
２２１　ユニークコード生成部
２２２　記憶部
２２３　共通鍵生成部

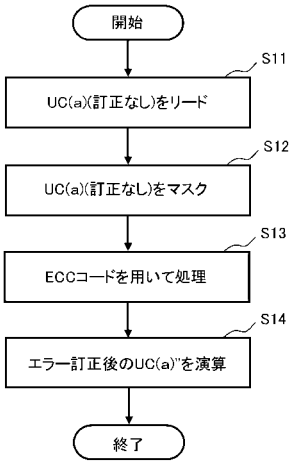
【図１】



【図２】



【図３】

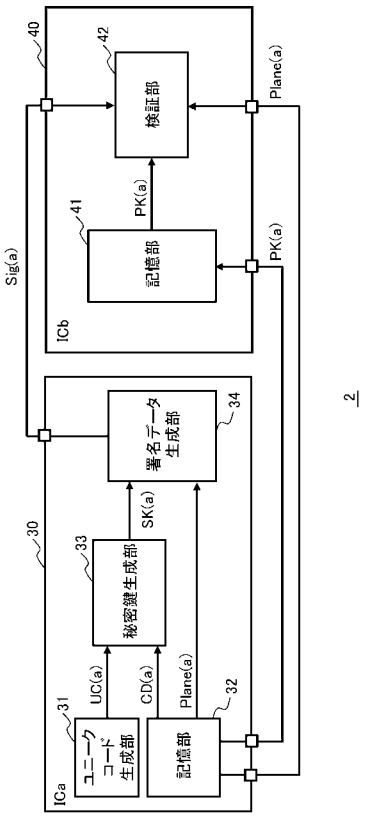


【図４】

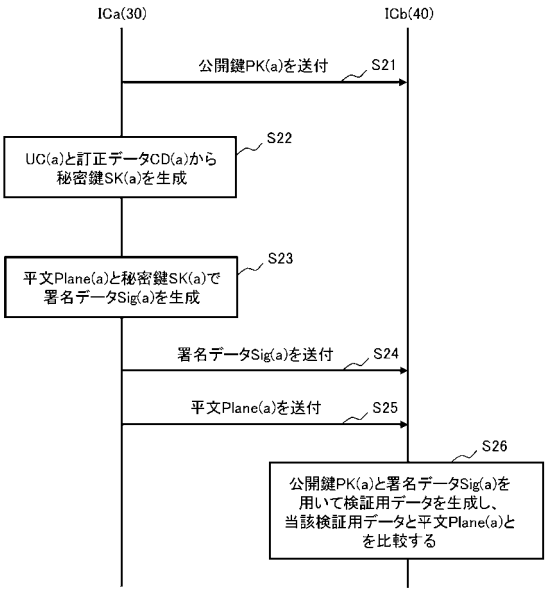
訂正データCD(a)　共通鍵CK(a)

ビット位置	0	1	2	3	4	5	6	7	…
(1)ユニークコードUC(a)(訂正なし)	1	1	0	0	0	1	1	1	…
(2)マスクデータ	1	0	1	1	1	1	0	1	…
(3)マスク処理後のデータ	1	X	0	0	0	1	X	1	…
(4)X箇所を削除後、左詰め	1	0	0	0	1	1	…		
(5)ECC訂正後(1ビット目訂正有り)	1	1	0	0	1	1	…		
(6)NOTで演算	0	0	1	1	0	0	…		

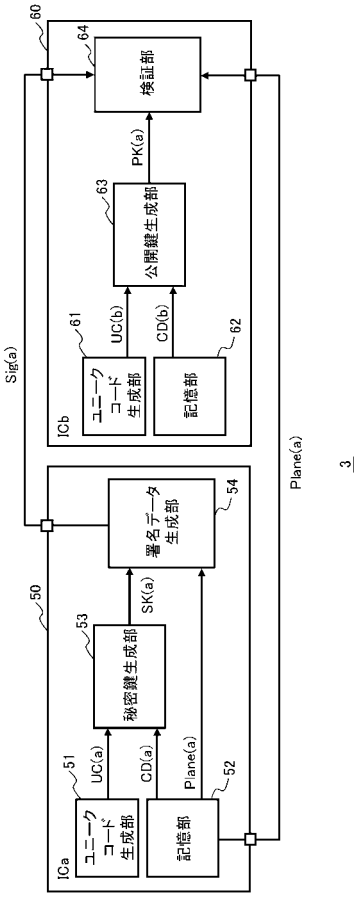
【図５】


2
40
42
検証部
Plane(a)
PK(a)
41
記憶部
PK(a)
Sig(a)
ICb
署名データ生成部
34
30
SK(a)
33
秘密鍵生成部
UC(a)
CD(a)
Plane(a)
31
32
ユニークコード生成部
記憶部
ICa

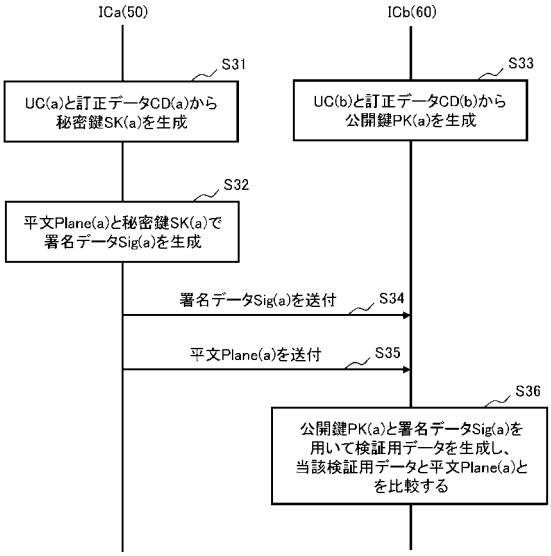
【図６】


ICa(30)
ICb(40)
公開鍵PK(a)を送付
S21
UC(a)と訂正データCD(a)から秘密鍵SK(a)を生成
S22
平文Plane(a)と秘密鍵SK(a)で署名データSig(a)を生成
S23
署名データSig(a)を送付
S24
平文Plane(a)を送付
S25
S26
公開鍵PK(a)と署名データSig(a)を用いて検証用データを生成し、当該検証用データと平文Plane(a)とを比較する

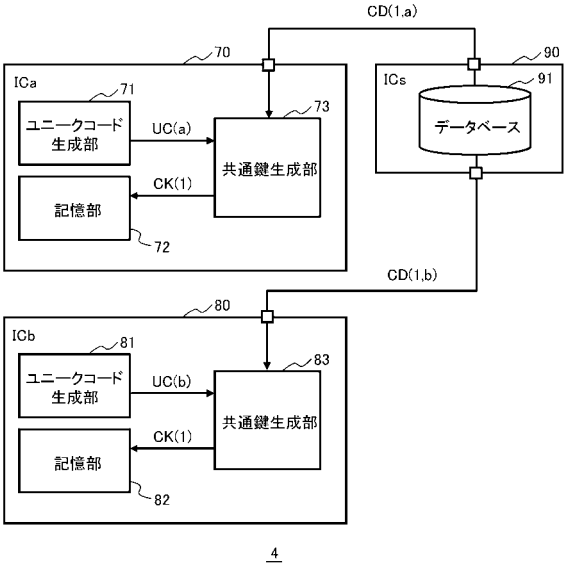
【図７】


3
60
64
検証部
PK(a)
63
公開鍵生成部
UC(b)
CD(b)
61
62
Sig(a)
ユニークコード生成部
記憶部
ICb
Plane(a)
署名データ生成部
54
50
SK(a)
53
秘密鍵生成部
UC(a)
CD(a)
Plane(a)
51
52
ユニークコード生成部
記憶部
ICa

【図８】


ICa(50)
ICb(60)
S31
UC(a)と訂正データCD(a)から秘密鍵SK(a)を生成
S33
UC(b)と訂正データCD(b)から公開鍵PK(a)を生成
S32
平文Plane(a)と秘密鍵SK(a)で署名データSig(a)を生成
署名データSig(a)を送付
S34
平文Plane(a)を送付
S35
S36
公開鍵PK(a)と署名データSig(a)を用いて検証用データを生成し、当該検証用データと平文Plane(a)とを比較する

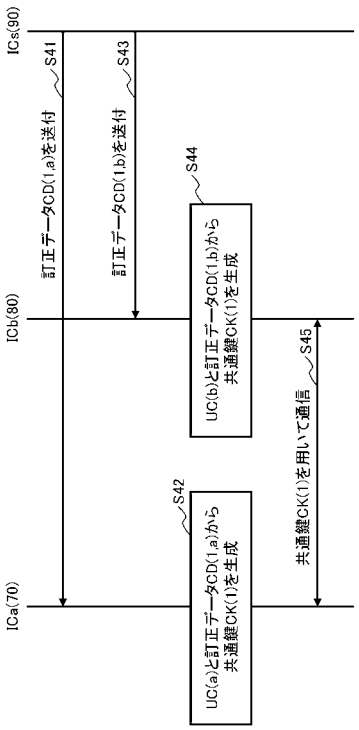
【図９】



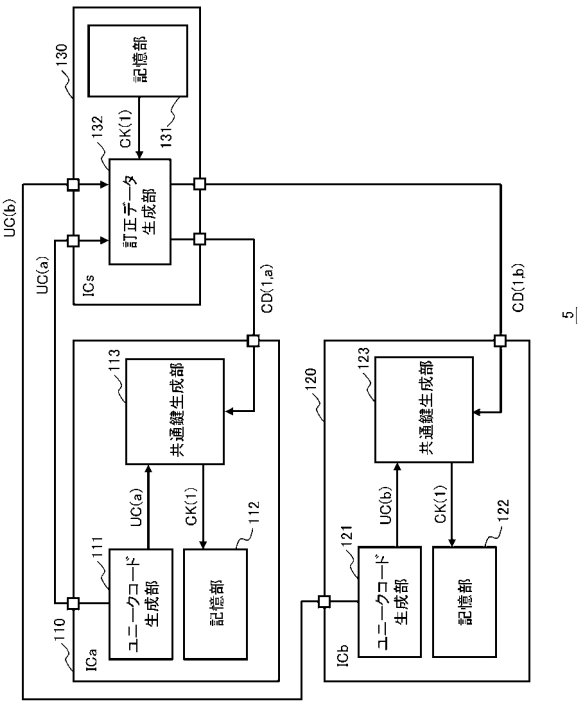
【図１０】

	CK(1)	CK(2)	CK(3)	・・・	CK(n)
ICa	CD(1,a)	CD(2,a)	CD(3,a)	・・・	CD(n,a)
ICb	CD(1,b)	CD(2,b)	CD(3,b)	・・・	CD(n,b)
ICc	CD(1,c)	CD(2,c)	CD(3,c)	・・・	CD(n,c)
・・・	・・・	・・・	・・・	・・・	・・・
ICz	CD(1,z)	CD(2,z)	CD(3,z)	・・・	CD(n,z)

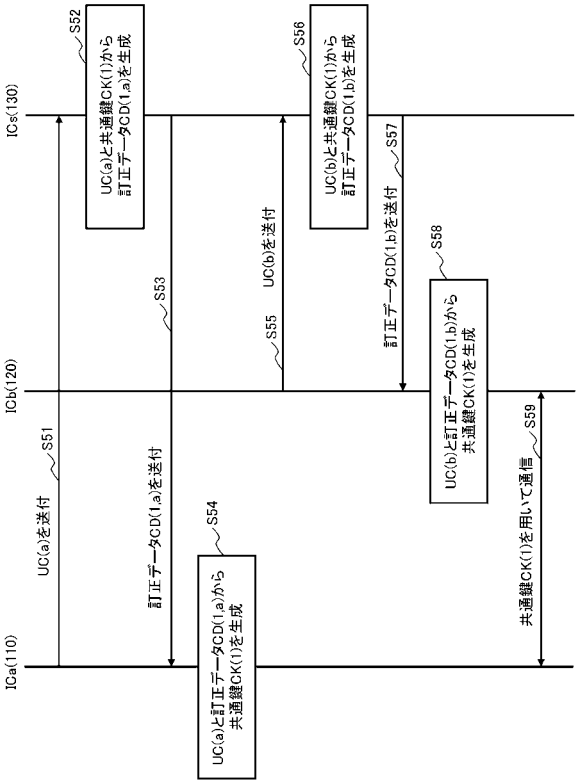
【図１１】



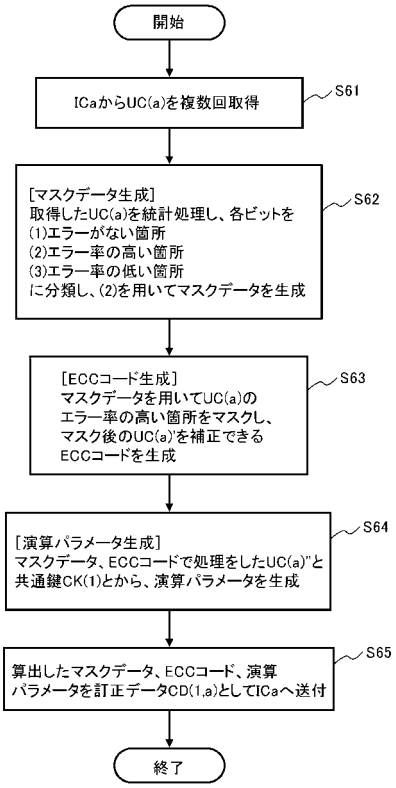
【図１２】



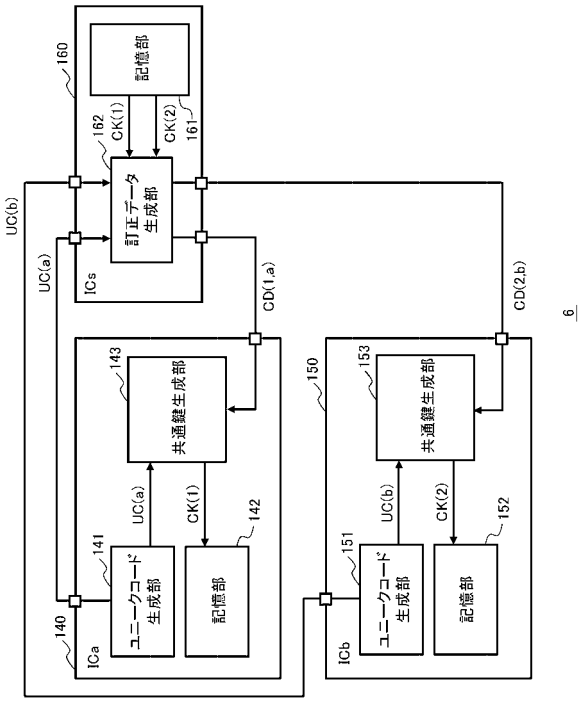
【図１３】



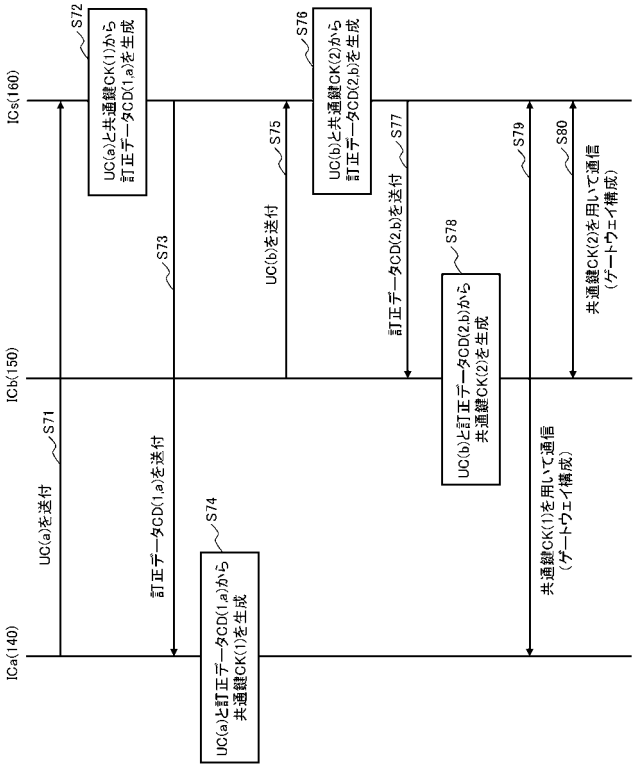
【図１４】



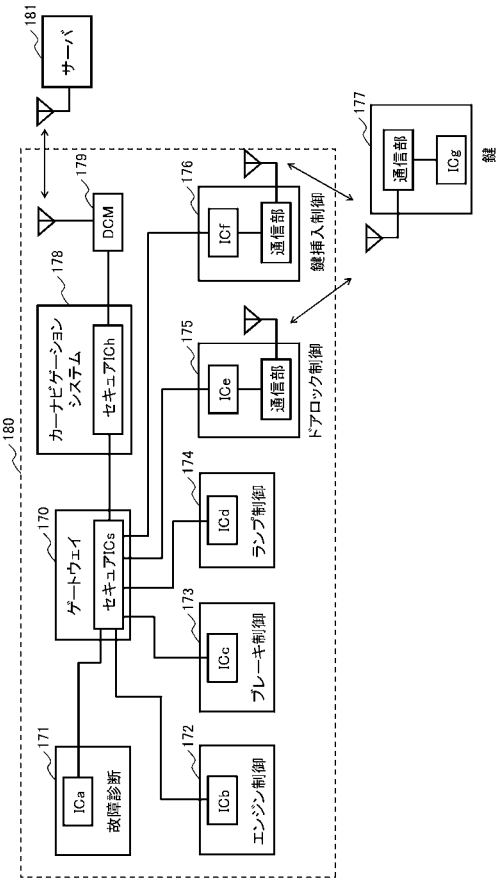
【図１５】



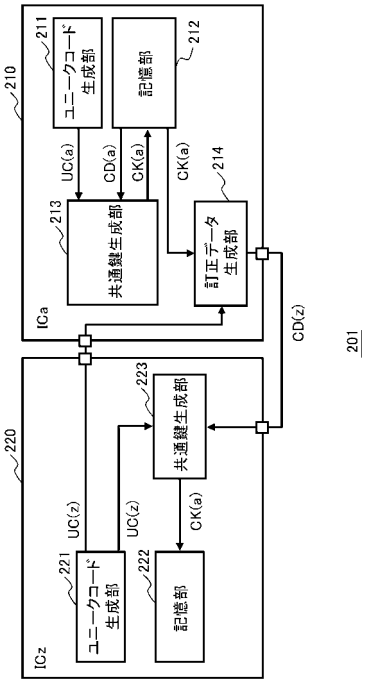
【図１６】



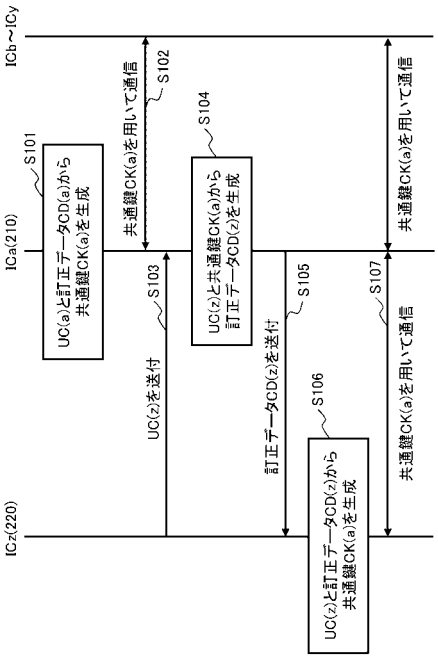
【図１７】



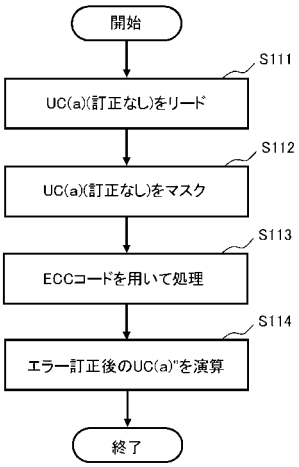
【図１８】



【図１９】



【図２０】



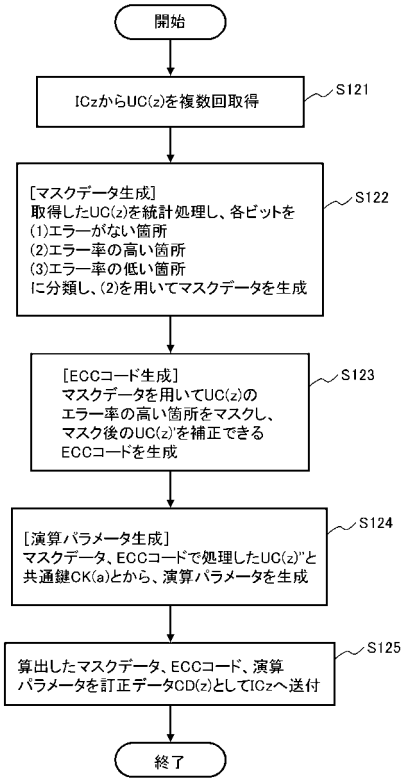
【図２１】

ビット位置	0	1	2	3	4	5	6	7	…
(1)ユニークコードUC(a)(訂正なし)	1	1	0	0	0	1	1	1	…
(2)マスクデータ	1	0	1	1	1	1	0	1	…
(3)マスク処理後のデータ	1	X	0	0	0	1	X	1	…
(4)X箇所を削除後、左詰め	1	0	0	0	1	1	…		
(5)ECC訂正後(1ビット目訂正有り)	1	1	0	0	1	1	…		
(6)NOTで演算	0	0	1	1	0	0	…		

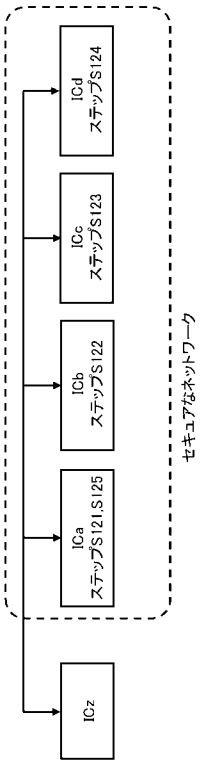
訂正データCD(a)

共通鍵CK(a)

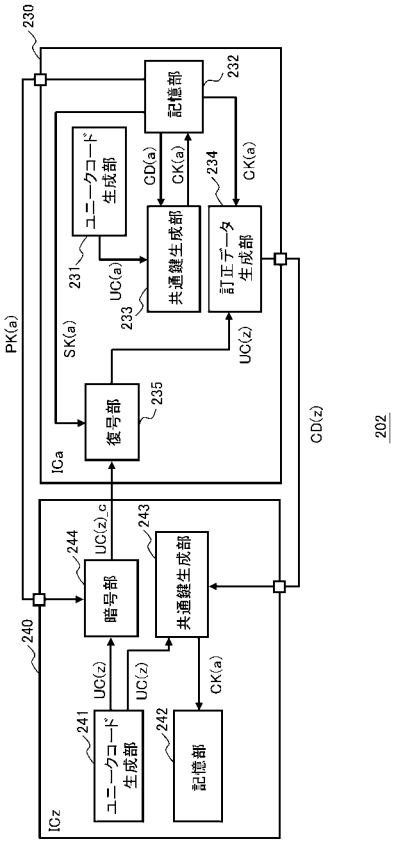
【図２２】



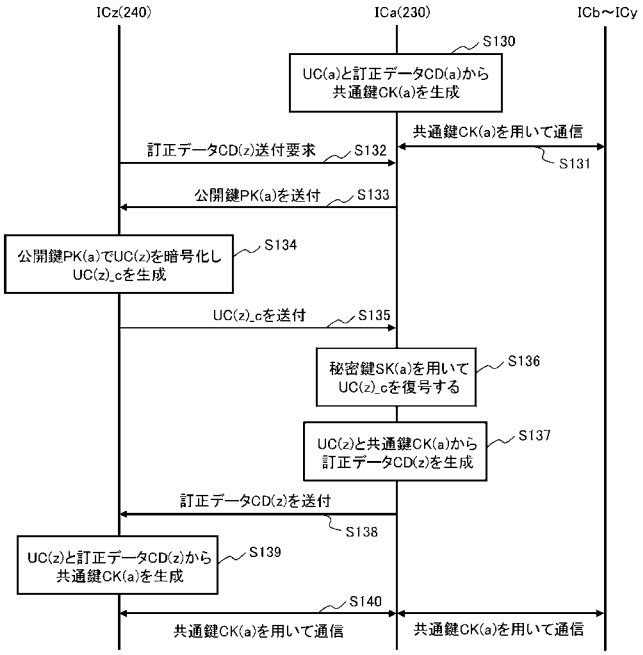
【図２３】



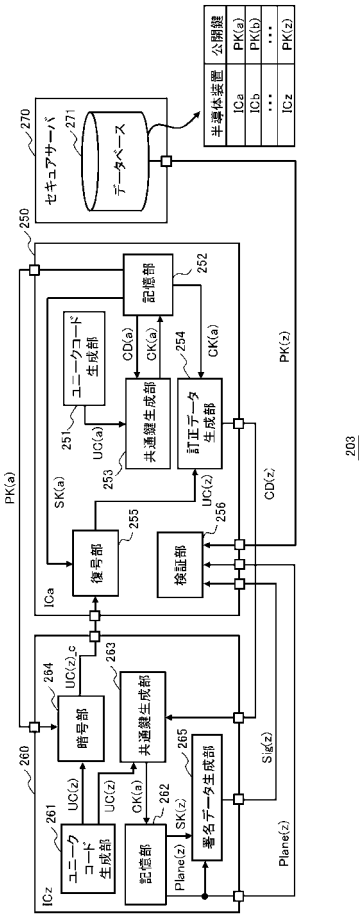
【図２４】



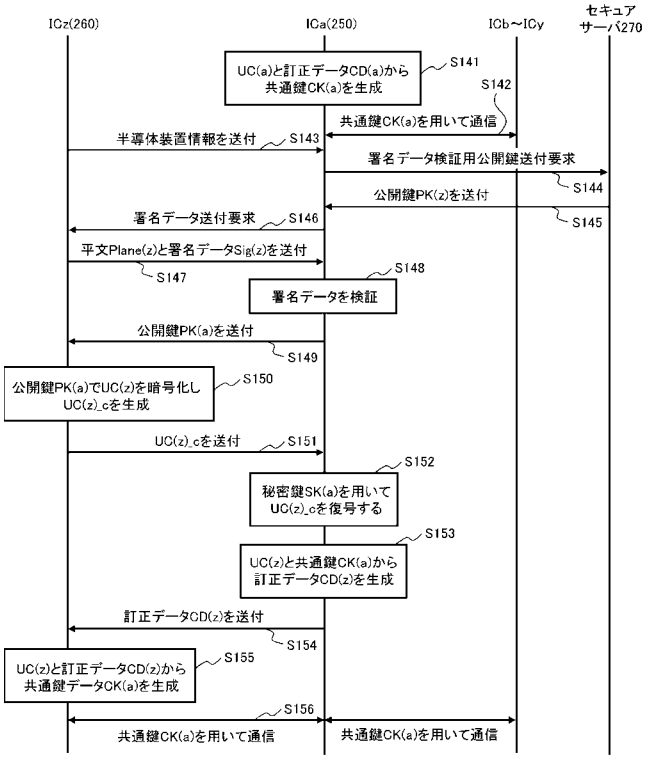
【図２５】



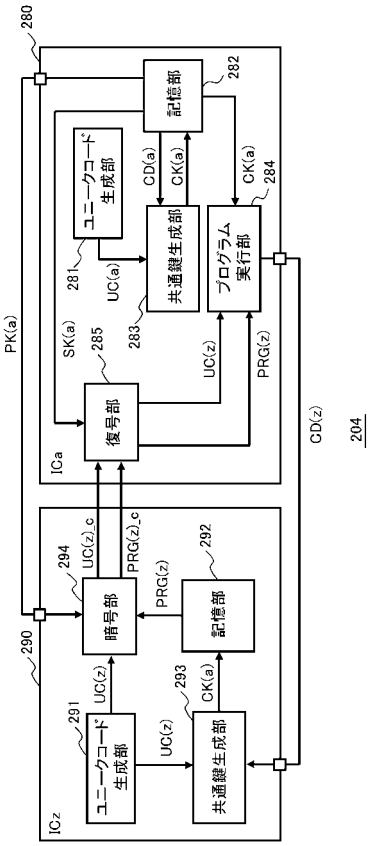
【図２６】



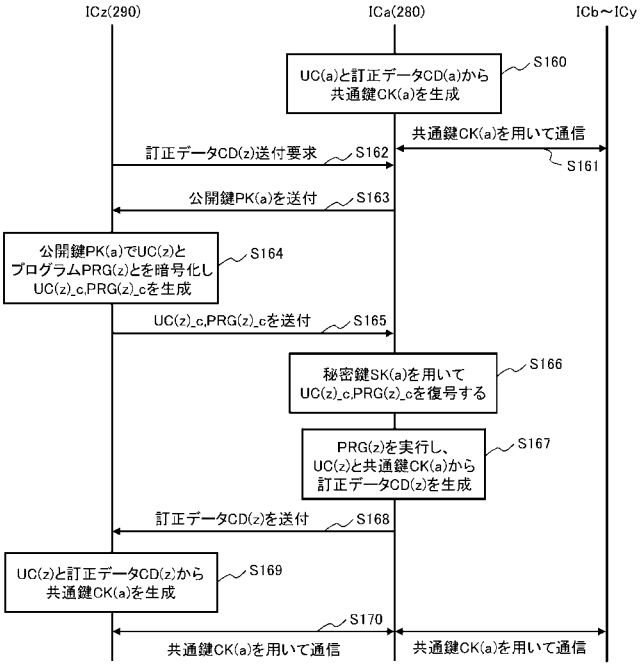
【図２７】



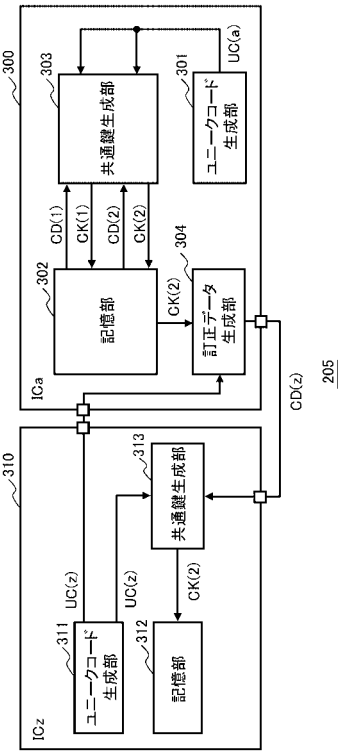
【図２８】



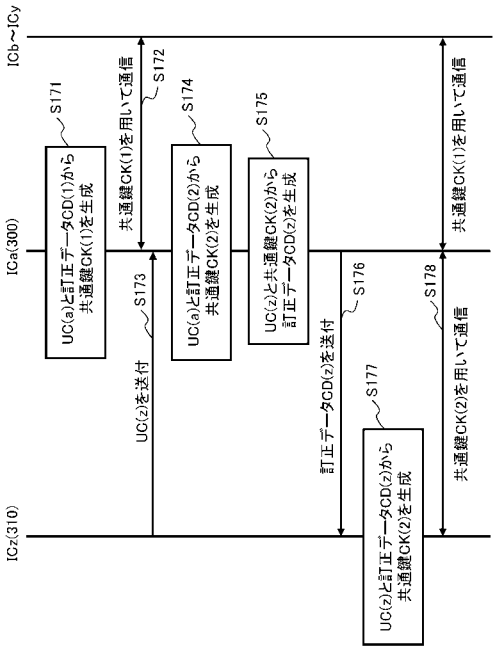
【図２９】



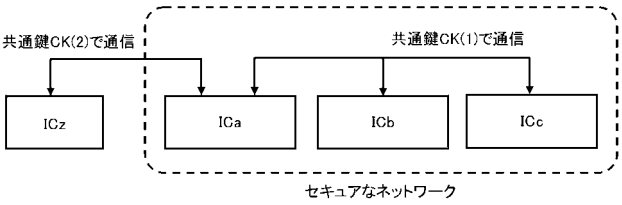
【図３０】



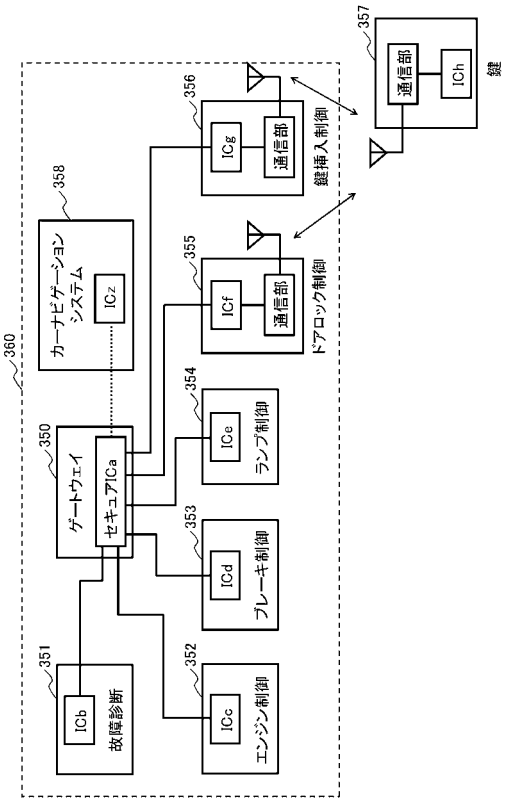
【図３１】



【図３２】



【図３３】


360
350
ゲートウェイ
セキュアICa
351
ICb
故障診断
352
ICc
エンジン制御
353
ICd
ブレーキ制御
354
ICe
ランプ制御
355
ICf
通信部
ドアロック制御
356
ICg
通信部
鍵挿入制御
357
通信部
ICh
鍵
358
カーナビゲーション
システム
ICz

フロントページの続き

(72)発明者　山崎　暁
神奈川県川崎市中原区下沼部１７５３番地　ルネサスエレクトロニクス株式会社内
(72)発明者　押田　大介
神奈川県川崎市中原区下沼部１７５３番地　ルネサスエレクトロニクス株式会社内

Ｆターム(参考) 5J104 AA16　EA19　NA02　NA37