

【公報種別】特許法第 17 条の 2 の規定による補正の掲載
【部門区分】第 6 部門第 3 区分
【発行日】平成 17 年 2 月 3 日 (2005.2.3)

【公開番号】特開 2001-5731 (P2001-5731A)
【公開日】平成 13 年 1 月 12 日 (2001.1.12)
【出願番号】特願 平 11-178750
【国際特許分類第 7 版】

G 0 6 F 12/14

G 0 6 K 19/073

【F I】

G 0 6 F 12/14 3 2 0 B

G 0 6 K 19/00 P

【手続補正書】

【提出日】平成 16 年 3 月 1 日 (2004.3.1)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

2 種の異なる電圧にて 2 値情報が伝達される 1 チップからなる半導体装置であって、
演算装置と、

メモリと、

暗号化装置と、

復号化装置と、

データバスとを有し、

前記演算装置から送信されるデータは前記暗号化装置にて暗号化された後、前記データバスを介して転送され、前記メモリに格納され、

前記メモリから前記データバスを介して読み出されるデータは、前記復号化装置にて復号化されて、前記演算装置に入力されることを特徴とする半導体装置。

【請求項 2】

請求項 1 記載の半導体装置であって、

前記暗号化は、前記演算装置から送信されるデータと鍵データとの排他的論理和により行われ、

前記復号化は、前記メモリから読み出されるデータと前記鍵データとの排他的論理和により行われることを特徴とする半導体装置。

【請求項 3】

請求項 1 記載の半導体装置であって、

前記暗号化は、前記演算装置から送信されるデータと、鍵データと前記演算装置から送信されるデータの送信位置であるアドレスデータの一部とが接続されたデータとの排他的論理和により行われ、

前記復号化は、前記メモリから読み出されるデータと、前記鍵データと前記メモリから読み出されるデータの読出位置であるアドレスデータの一部とが接続されたデータとの排他的論理和により行われることを特徴とする半導体装置。

【請求項 4】

請求項 1 から 3 にいずれかに記載の半導体装置であって、

乱数発生装置を有し、

前記鍵データは、前記乱数発生装置が生成する乱数であることを特徴とする半導体装置。

【請求項 5】

請求項 1 から 4 のいずれかに記載の半導体装置であって、

前記演算装置から書き込み可能な鍵バッファを有し、

前記鍵バッファは、前記鍵データを記憶することを特徴とする半導体装置。

【請求項 6】

請求項 1 から 5 のいずれかに記載の半導体装置であって、

前記暗号化装置は、前記演算装置から送信されるデータの送信位置であるアドレスデータにより暗号化をするか否かを指定し、

前記復号化装置は、前記メモリから読み出されるデータの読出位置であるアドレスデータにより復号化をするか否かを指定することを特徴とする半導体装置。

【請求項 7】

請求項 1 から 6 のいずれかに記載の半導体装置であって、

前記暗号化装置は、前記演算装置から送信されるデータのデータパタンにより暗号化をするか否かを指定し、

前記復号化装置は、前記メモリから読み出されるデータのデータパタンにより復号化をするか否かを指定することを特徴とする半導体装置。

【請求項 8】

2 種の異なる電圧にて 2 値情報が伝達される 1 チップからなる半導体装置であって、
演算装置と、

メモリと、

第 1 暗号化装置と、

第 2 暗号化装置と、

第 1 復号化装置と、

第 2 復号化装置と、

データバスとを有し、

前記演算装置から送信されるデータは前記第 1 暗号化装置にて暗号化されて前記データバスに出力され、

前記演算装置から送信され暗号されたデータは、前記データバスを介して転送され、前記第 1 復号化装置にて復号化されて前記メモリに格納され、

前記メモリから読み出されるデータは前記第 2 暗号化装置にて暗号化されて前記データバスに出力され、

前記メモリから読み出され暗号されたデータは、前記データバスを介して転送され、前記第 2 復号化装置にて復号化されて前記演算装置に入力されることを特徴とする半導体装置。

【請求項 9】

請求項 8 記載の半導体装置であって、

乱数発生装置を有し、

前記鍵データは、前記乱数発生装置が生成する乱数であることを特徴とする半導体装置。