【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22年2月12日(2010.2.12)

【公開番号】特開2007-234001(P2007-234001A)
【公開日】平成19年9月13日(2007.9.13)
【年通号数】公開・登録公報2007-035
【出願番号】特願2007-20267(P2007-20267)
【国際特許分類】
Ｇ０６Ｋ　19/073　(2006.01)
Ｇ０６Ｋ　19/07　(2006.01)
Ｇ０６Ｆ　21/06　(2006.01)
【ＦＩ】
Ｇ０６Ｋ　19/00　Ｐ
Ｇ０６Ｋ　19/00　Ｈ
Ｇ０６Ｋ　19/00　Ｎ
Ｇ０６Ｆ　12/14　５６０Ｅ

【手続補正書】
【提出日】平成21年12月22日(2009.12.22)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
外部機器と信号の送受信を無線通信で行う送受信回路と、演算処理中のサイドチャネル攻撃を阻止する機能を有する演算回路とを備えた半導体装置において、
前記演算回路は、
前記演算処理中のサイドチャネル攻撃を阻止する処理を行うプログラムが記憶された第１のメモリと、
前記第１のメモリより前記プログラムを読み出して、当該プログラムを実行する中央処理装置と、
前記プログラムの命令に従って、前記信号に基づいたデータの逆変換処理を行う補助演算装置と、
前記補助演算装置において、前記逆変換処理の演算時間を設定するための乱数を生成する乱数生成器と、
前記逆変換処理されたデータを記憶する第２のメモリと、
を有し、
前記乱数を用いて前記逆変換処理する時間を制御することを特徴とする半導体装置。
【請求項２】
外部機器と信号の送受信を無線通信で行う送受信回路と、演算処理中のサイドチャネル攻撃を阻止する機能を有する演算回路とを備えた半導体装置において、
前記演算回路は、
前記演算処理中のサイドチャネル攻撃を阻止する処理を行うプログラムが記憶された第１のメモリと、
前記第１のメモリより前記プログラムを読み出して、当該プログラムを実行することにより、前記外部からの信号に基づいたデータの逆変換処理を行う中央処理装置と、
前記中央処理装置において、前記逆変換処理の演算時間を設定するための乱数を生成す

る乱数生成器と、
を有し、
前記乱数を用いて前記逆変換処理する時間を制御することを特徴とする半導体装置。
【請求項３】
請求項１または請求項２において、
前記変換処理は、４５を底とする指数・対数演算と、２５７を基数とする剰余処理の逆演算を行う処理であることを特徴とする半導体装置。
【請求項４】
請求項１乃至請求項３において、
前記外部機器より受信される信号は、フレーム開始のコード、フラグのコード、コマンドのコード、データのコード、巡回冗長検査のコード、及びフレーム終了のコードにより構成される信号であることを特徴とする半導体装置。
【請求項５】
請求項１乃至請求項４のいずれか１項において、
前記プログラムは、前記外部より受信される信号の種類を判断する第１のルーチンと、前記逆変換処理の演算回数を判断する第２のルーチンにより構成されることを特徴とする半導体装置。
【請求項６】
請求項１乃至請求項５のいずれか１項において、
前記演算回路は、インターフェース、制御レジスタ、コード抽出回路、及び符号化回路を含むコントローラを有することを特徴とする半導体装置。
【請求項７】
請求項１乃至請求項６のいずれか１項において、
前記外部との信号の送受信を行う回路は、アンテナ、共振回路、電源回路、リセット回路、クロック生成回路、復調回路、変調回路、及び電源管理回路を有することを特徴する半導体装置。
【請求項８】
請求項１乃至請求項７のいずれか１項において、
前記乱数生成器は、第１のメモリセルを有する読み出し回路とデコーダにより制御されるメモリセルアレイを有し、
前記乱数の値は、前記第１のメモリセルの閾値電圧と前記メモリセルアレイより選択された第２のメモリセルの閾値電圧の差により決定されることを特徴とする半導体装置。
【請求項９】
請求項１乃至請求項８のいずれか１項に記載の半導体装置を備えたことを特徴とするＲＦＩＤ用ＩＣチップ、ＩＤチップ、ＩＣタグ、ＩＤタグ、ＲＦタグ、無線タグ、電子タグ、またはトランスポンダ。