平成３０年４月１２日判決言渡

平成２９年（行ケ）第１００５１号　審決取消請求事件

口頭弁論終結の日　平成３０年２月８日

判　　決

原　　告　アンスティテュ　ミーヌーテレコム

同訴訟代理人弁理士　木　村　高　久

同　小　幡　義　之

被　　告　特　許　庁　長　官

同指定代理人　高　木　進

同　石　井　茂　和

同　佐　久　聖　子

同　野　崎　大　進

同　板　谷　玲　子

主　　文

１　原告の請求を棄却する。

２　訴訟費用は原告の負担とする。

３　この判決に対する上告及び上告受理申立てのための付加期間を３０日と定める。

事　実　及　び　理　由

第１　請求

特許庁が不服２０１４－２６７９２号事件について平成２８年１０月１３日にした審決を取り消す。

第２　前提事実（いずれも当事者間に争いがない。）

１　特許庁における手続の経緯等

原告は，発明の名称を「その暗号変換により特に情報漏洩観測攻撃から保護される暗号回路」とする発明について，平成２２年１月１８日（パリ条約による優先権主張外国庁受理２００９年１月２０日　仏国）に特許出願をした（特願２０１１－５４６７７１号。以下「本願」という。）。これに対し，平成２６年１月１５日付けで拒絶理由が通知されたことから，原告は，同年５月２日に手続補正書等を提出したが，同年９月４日付けで拒絶査定がされた。

そこで，原告は，同年１２月２６日，特許庁に対し，拒絶査定不服審判を請求した。これに対し，特許庁は，当該審判請求を不服２０１４－２６７９２号事件として審理をし，原告に対し，平成２７年９月１７日付けで拒絶理由を通知した。これを受け，原告は，平成２８年３月２５日，特許請求の範囲の変更を内容とする別紙手続補正書を提出したが，特許庁は，同年１０月１３日，「本件審判の請求は，成り立たない。」との審決をした（出訴期間として９０日を附加した。以下「本件審決」という。）。その謄本は，同月２５日，原告に送達された。

原告は，平成２９年２月２２日，本件訴えを提起した。

２　本願発明

本願に係る発明は，別紙手続補正書により補正された特許請求の範囲請求項１～５に記載された事項により特定されるものであるところ（以下，請求項の順に「本願発明１」のようにいい，本願発明１～５を併せて「本願発明」という。また，本願に係る別紙明細書及び図面を「本願明細書等」という。），その記載は，以下のとおりである。

【請求項１】

暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路（２１）であって，前記回路は，前記回路に専用の第２の鍵 $k_i$ であって，前記回路のサイドチャネルを利用した攻撃から回路を保護することを可能とする第２の鍵 $k_i$ を

含むことを特徴とする回路であって，

前記関数鍵 $k_c$ は XOR 演算によって前記２つの鍵を組み合わせることにより前記第２の鍵 $k_i$ によってマスクされ，入力変数 x はマスク鍵

【数１】

$$k_c \oplus k_i$$

によって暗号化され，

前記暗号回路は，FPGA タイプのプログラマブル回路において実現され，

前記暗号回路は，前記 FPGA タイプのプログラマブル回路のプログラミングファイル（２５）を暗号化するための第３の鍵 $k_b$ を含み，

前記第２の鍵 $k_i$ は PUF（Physically Unclonable Function）により生成されることを特徴とする回路。

【請求項２】

前記第２の鍵 $k_i$ によって導入されるマスキングは HO-DPA 攻撃から保護されることを特徴とする，請求項１に記載の回路。

【請求項３】

前記第２の鍵 $k_i$ の基数は前記関数鍵 $k_c$ の基数に等しいことを特徴とする，請求項１または２に記載の回路。

【請求項４】

前記第３の鍵 $k_b$ の基数は前記関数鍵 $k_c$ の前記基数よりも大きいかまたは等しいことを特徴とする，請求項１に記載の回路。

【請求項５】

前記暗号化アルゴリズムは DES アルゴリズムであることを特徴とする，請求項１～４のいずれか１項に記載の回路。

３　本件審決の理由の要旨

本件審決の理由は，別紙審決書（写し）記載のとおりであるが，要するに，

以下のとおり，本願発明１は，特許法（以下「法」という。）３６条６項２号及び同条４項１号の要件を欠き，これを引用する本願発明２～５も同様であり，また，本願発明１は，国際公開第２００７／１０２８９８号公報（甲１。以下「引用文献１」という。）記載の発明（以下「引用発明」という。）に，特開２００３－５１８２０号公報（甲２。以下「引用文献２」という。）ないし周知慣用の技術に基づいて当業者が容易になし得るものであり，本願発明１の奏する作用効果もこれらから当然予測される範囲内のものに過ぎず，格別顕著なものということはできないから，法２９条２項により特許を受けることができず，本願発明２～５について検討するまでもなく，本願は拒絶すべきものであるとした。

(1)　法３６条６項２号について

一般に，データの暗号化と復号化とが対となって別々の装置を用い，ある装置（例えば送信側）で暗号化されたデータは別の装置（例えば受信側）で復号化されることによりデータを暗号化する目的が実現されるところ，本願発明１は「暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路（２１）であって，…第２の鍵 $k_i$ は PUF（Physically Unclonable Function）により生成される」事項を有することから，前記「PUF により生成される」「第２の鍵 $k_i$」に係る暗号化と復号化が対となると解されるが，例えば復号化側の別の装置では（PUF はクローン不能であるから，前記別の装置では第２の鍵 $k_i$ と同じ鍵を持つことはできないので）復号化できないと解される。本願明細書等の記載（【０００２】）には，前記２つの側（送信側と受信側）が同一である場合の言及はあるとしても，本願発明１は「同一」であるとの限定はしておらず，前記２つの側が同一である場合，別々である場合のいずれの場合も，暗号化されたデータをどのように復号化するのかが不明であって，どのように（復号可能に）暗号化するのか明確に記載されたものとはいえず，しかも，技術的意義も不明である。

このため，本願発明は，法３６条６項２号の要件を満たしていない。

(2)　法３６条４項１号について

本願発明１は「$k_c \oplus k_i$ によって暗号化され，…第２の鍵 $k_i$ は PUF（Physically Unclonable Function）により生成される」事項を有する回路の発明であるが，当該暗号化に関連する復号化について発明の詳細な説明には説明されておらず，前記第２の鍵 $k_i$ は PUF（物理的クローン不能関数）により生成されるものであるから，マスク鍵（$k_c \oplus k_i$）により暗号化された入力変数 x を何を用いてどのように復号すればよいのか，暗号化／復号化に係る回路は唯一の回路を用いるのか，別の回路を用いるのか，前記唯一の回路を用いて暗号化と復号化をする技術的意義はどのようなものなのか不明であり，また，別の回路を用いるならいかにして同じ PUF により生成される第２の鍵 $k_i$ を有する別の回路が得られるのか不明である。

したがって，本願明細書等に係る発明の詳細な説明は，当業者が本願発明を実施することができる程度に明確かつ十分に記載されたものではない。

(3)　法２９条２項について

ア　引用発明

DES 暗号アルゴリズムを実行するための暗号キーを含む DES 計算ユニット，キーマスキングユニット，メモリを含む暗号ハードウェアであって，

前記ハードウェアは，マスクを用いるマスキング方法（偽またはダミー演算）の使用により，あるラウンドにおける暗号化アルゴリズム置換（S ボックス）演算の（キー側の）入力値のサイドチャネル攻撃からのハードウェアエンジンを保護することを可能とするマスクを含むハードウェアであって，

前記キーは XOR 演算によって前記キーとマスクとを用いてマスキングをかけたキーを生じさせ，入力データは前記マスキングをかけたキーに

よって XOR 演算が適用されて暗号化され，

前記マスクは事前に構築されたマスキング表を用いて生成されることを特徴とする暗号ハードウェア。

イ　対比

本願発明１と引用発明とを対比すると，一致点及び相違点は，以下のとおりである。

［一致点］

暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路であって，前記回路は，第２の鍵 $k_i$ であって，前記回路のサイドチャネルを利用した攻撃から回路を保護することを可能とする第２の鍵 $k_i$ を含むことを特徴とする回路であって，

前記関数鍵 $k_c$ は XOR 演算によって前記２つの鍵を組み合わせることにより前記第２の鍵 $k_i$ によってマスクされ，入力変数 x はマスク鍵

【数１】

$k_c \oplus k_i$

によって暗号化され，

前記第２の鍵 $k_i$ は手段を用いることにより生成されることを特徴とする回路。

［相違点１］

回路に係る第２の鍵 $k_i$（マスク）であることに関し，本願発明１は「回路に専用の」第２の鍵 $k_i$ であるのに対し，引用発明は，そのような事項を有していない点。

［相違点２］

本願発明１は，「暗号回路は，FPGA タイプのプログラマブル回路のプログラミングファイルを暗号化するための第３の鍵 $k_b$ を含」むのに対し，引用発明は，そのような事項を有していない点。

［相違点３］

前記第２の鍵 $k_i$ は手段を用いることにより生成されることに関し，本願発明１は「PUF（Physically Unclonable Function）」により生成されるのに対し，引用発明は，そのような事項を有していない点。

ウ　判断

(ｱ)　相違点１及び３について

引用文献２には，「マスクは，物理的アンクローンナブルな物理的パラメータネットワーク（Function；関数，機能）により生成される」技術が示されている。

また，引用発明と引用文献２とは，いずれも暗号化保護のための技術に係るものである。

そうすると，引用発明において，回路に係る第２の鍵 $k_i$（マスク）であることに関し，「前記回路に専用の」第２の鍵 $k_i$ であるとなすこと，及び，前記第２の鍵 $k_i$（マスク）は所定の手段を用いることにより生成されることに関し，「PUF（Physically Unclonable Function）」により生成されるとなすことは，引用文献２の前記技術を参酌することにより当業者が容易になし得ることである。

(ｲ)　相違点２について

特表２００４－５１９１１１号公報（甲４。以下「参考文献１」という。）及び特表２００８－５１２９０９号公報（甲５。以下「参考文献２」という。）に見られるように，FPGA プログラムが意図する特定の組の FPGA 以外の FPGA をプログラムするための FPGA プログラムの使用を阻止するため，あるいは，単一のセキュアな集積回路チップ上に暗号処理要素を設けることを目的として「暗号化回路は，FPGA タイプのプログラマブル回路において実現され，前記回路は，前記 FPGA タイプのプログラマブル回路のプログラミングファイルを暗号化するための鍵

を含む」技術は，周知の技術であったと認められる。

そうすると，引用発明において「前記暗号回路は，FPGA タイプのプログラマブル回路において実現され，前記暗号回路は，前記 FPGA タイプのプログラマブル回路のプログラミングファイルを暗号化するための第３の鍵 $k_b$ を含」むとなすことは，前記周知の技術を参酌することにより容易になし得ることである。

(ｳ) したがって，本願発明１は，引用発明，引用文献２ないし周知慣用の技術に基づいて当業者が容易になし得るものであり，その奏する作用効果は，引用発明，引用文献２ないし周知慣用の技術の奏する作用効果から当然予測される範囲内のものに過ぎず，格別顕著なものということはできないのであり，法２９条２項により特許を受けることができない。

第３　当事者の主張

１　原告の主張

(1)　取消事由１（本願発明１の認定の誤り）

ア　本願発明１における関数鍵 $k_c$ とは，暗号化アルゴリズムを実行する鍵のことであり，具体的には，DES アルゴリズム２３に入力されてこれを実行し，入力変数 x から暗号文 y を出力することに機能する鍵である（本願明細書等の図４）。より具体的には，関数鍵 $k_c$ は，本願明細書等の図１又は２において Feistel 関数 f に入力されて暗号化処理に適用される鍵である（裁判所注：図１及び２には「Feisted」とあるが，正しくは「Feistel」である。以下，図１又は２に言及する場合を含め，後者により表記する。）。ここで，「暗号化アルゴリズム」の操作とは，本願発明１の「暗号化アルゴリズムを実行する」操作であり，関数鍵 $k_c$ によって暗号化アルゴリズムを実行して暗号文 y を出力する操作を意味する。

他方，マスク鍵 $k_c \oplus k_i$ とは，あくまで入力変数 x を暗号化するだけのも

のである。ここで，「暗号化」の操作とは，本願発明１の「入力変数 x はマスク鍵 $k_c \oplus k_i$ によって暗号化され」る操作であり，暗号化アルゴリズムの操作の一部である。

イ　一般に，鍵を用いて入力変数 x を暗号化する際に，サイドチャネルを利用した攻撃によって情報の漏洩が生じるおそれがある。そこで，本願発明１では，マスク鍵 $k_c \oplus k_i$ を用いて入力変数 x を暗号化する。このため，マスク鍵 $k_c \oplus k_i$ は，サイドチャネルを利用した攻撃の攻撃者によって解読される（可能性のある）鍵である（本願明細書等【００２８】）。

本願明細書等の記載（【００４０】）及び図４にあるとおり，関数鍵 $k_c$ は，暗号化アルゴリズムを実行して入力変数 x から暗号文すなわち暗号化された変数 y（=DES（x，$k_c$））を出力することに機能する。このため，最終的に入力変数 x から生成して出力される暗号文を復号する（攻撃者にとっては解読する）ためには，Feistel 関数 f に入力されて暗号化処理に適用される鍵，つまり暗号化アルゴリズムを実行することに機能する関数鍵 $k_c$ を知る必要がある。しかるに，サイドチャネルを利用した攻撃の攻撃者によって漏洩される（可能性のある）鍵は，上記のとおり，マスク鍵 $k_c \oplus k_i$ でしかない。サイドチャネルを利用した攻撃によって攻撃者が上記マスク鍵を知ったとしても，そこから関数鍵 $k_c$ を推測することは，第２の鍵 $k_i$ が未知であるため容易なことではなく，このため，暗号文から平文である入力変数 x を復号する（攻撃者にとっては解読する）ことはできない（本願明細書等【００４６】）。本願発明１の意義は，以上の点にある。

ウ　しかし，本件審決は，本願発明１の認定に当たり，本願発明１の上記意義をなんら認定しなかった。この点で本件審決には誤りがある。

(2)　取消事由２（本願発明１と引用発明との一致点及び相違点の認定の誤り）

ア　引用文献１には「マスキングをかけたキーを使用して DES 暗号アルゴ

リズムを実行し，結果を出力データとしてメモリ３１に再び書き込む。」（引用文献１に対応する特表２００９－５１６９６４号公報（甲１７）の【００３４】。以下，引用文献１の訳（段落番号を含む。）は同公報による。）との記載がある。このため，引用発明において暗号アルゴリズムを実行し，暗号文を出力させることに機能するキーは，マスキングをかけたキーである。

他方，引用文献１には「アルゴリズムのSボックスの入力側におけるアルゴリズムの実行のその部分を直接標的にすることができる。」（【０００６】）と記載されており，サイドチャネルを利用した攻撃がされるのは，S ボックスの入力側である。また，引用文献１の図２には，S ボックス S1 の入力側に，キーK1 をマスク[15]によってマスクしたキーを用いてデータ１を暗号化することが示されている。このため，引用発明においてサイドチャネルを利用した攻撃の攻撃者によって漏洩される（可能性のある）キーは，マスキングをかけたキーである。

以上より，引用発明において暗号文を復号する（攻撃者にとっては解読する）ためには，マスキングをかけたキーを知れば足り，マスキングをかける対象となるキーを知る必要はない。

イ　したがって，本願発明１と引用発明とを対比すると，本願発明１では，マスキングの対象となるキー，すなわち第２の鍵 $k_i$ によってマスキングされる対象となる関数鍵 $k_c$ が，暗号化アルゴリズムを実行して暗号文を出力することに機能するのに対して，引用発明の「暗号キー」は，それ単独で暗号化アルゴリズムを実行して暗号文を出力することに機能するものではなく，暗号キーとマスクとが XOR 演算された「マスキングをかけたキー」が暗号アルゴリズムを実行して暗号文を出力することに機能する，という点で異なる。

ウ　そうすると，本件審決は，本願発明１と引用発明との一致点として「暗

号化アルゴリズムを実行するための関数鍵 $k_c$」を認定している点で誤りである。

(3) 取消事由３（容易想到性に関する認定の誤り）

ア 相違点２に関する本件審決の認定・判断については，実質的に争わない。

イ 相違点１及び３について

(ｱ) 前記のとおり，本願発明１と引用発明とは，本願発明１では，マスキングの対象となるキー，すなわち第２の鍵 $k_i$ によってマスキングされる対象となる関数鍵 $k_c$ が，暗号化アルゴリズムを実行して暗号文を出力することに機能するのに対して，引用発明の「暗号キー」は，それ単独で暗号化アルゴリズムを実行して暗号文を出力することに機能するものではなく，暗号キーとマスクとが XOR 演算された「マスキングをかけたキー」が暗号アルゴリズムを実行して暗号文を出力することに機能する，という点で異なる。

このため，本願発明１では，サイドチャネルを利用した攻撃によって攻撃者がマスク鍵 $k_c \oplus k_i$ を知ったとしても，そこから関数鍵 $k_c$ を推測することは，第２の鍵 $k_i$ が未知であるため容易なことではなく，その結果，暗号文を復号する（攻撃者にとっては解読する）ことはできないのに対し，引用発明では，サイドチャネルを利用した攻撃によって攻撃者がマスキングをかけたキーを知ることができれば暗号文を復号することができてしまうという点で，両者は発明の作用効果の点でも異なる。

さらに，引用発明では，真のマスクを用いた真の演算以外に，ダミーマスクを用いたダミー演算を実行する必要があるとともに，真のメッセージ以外にダミーメッセージを生成する必要があるのに対し，本願発明１では，ダミー演算及びダミーメッセージの生成は不要である。

このように，本願発明１は，引用発明に対して顕著な作用効果を奏功することから，引用発明から容易に想到されるものではない。

(ｲ) 引用文献２には「データ d はメモリ２（MEM）に直接には蓄積されず，集積回路チップの物理的パラメータネットワークにより提供される量の測定値（ブロック４，MES）からくる物理データ p と組合される（ブロック３，COMB）。値 f（d，p）はこの組合せの関数で，メモリ２（例えば EEPROM）に蓄積される。」（【００３７】）と記載されている。したがって，引用文献２には，データ d と物理データ p を組み合わせ，その結果の値 f（d，p）をメモリに蓄積するという発明が記載されている。

しかし，引用文献２に示されるデータ d，物理データ p，値 f（d，p）は，いずれも，本願発明１の「第２の鍵 $k_i$ によってマスクされる鍵であって，暗号化アルゴリズムを実行する関数鍵 $k_c$」，「暗号化アルゴリズムを実行する関数鍵 $k_c$ をマスクする第２の鍵 $k_i$」，「入力変数 x をマスクするマスク鍵 $k_c \oplus k_i$（暗号化アルゴリズムを実行する関数鍵 $k_c$ と第２の鍵 $k_i$ が XOR 演算によって組み合わせられた鍵）」に相当しない。

そうである以上，引用発明に引用文献２を組み合わせても，本願発明１は容易に想到されるものではない。

(ｳ) 引用発明１におけるマスク[0]，マスク[1]，…マスク[63]は，テーブル表より既知の鍵である。これに対し，引用文献２には，マスクが物理的にアンクローンナブルであることが示されている。

しかるに，引用発明のマスク[0]等を「物理的にアンクローンナブル」なマスクに置換したとしても，引用発明において，設計者にとって未知である「物理的にアンクローンナブル」なマスクを含むメッセージデータが暗号アルゴリズムから出力されることとなりメッセージデータを復号化することができない。

そうである以上，引用発明に引用文献２を組み合わせることには阻害事由があり，これらを組み合わせて本願発明１を容易に想到することは

できない。

(ｴ) 参考文献１及び参考文献２には本願発明１の「第２の鍵 $k_i$ によってマスクされる鍵であって，暗号化アルゴリズムを実行する関数鍵 $k_c$」，「暗号化アルゴリズムを実行する関数鍵 $k_c$ をマスクする第２の鍵 $k_i$」，「入力変数 x をマスクするマスク鍵 $k_c \oplus k_i$（暗号化アルゴリズムを実行する関数鍵 $k_c$ と第２の鍵 $k_i$ が XOR 演算によって組み合わせられた鍵）」に相当する構成は何ら示されていない。

そうである以上，引用発明に参考文献１及び２を組み合わせても，本願発明１は容易に想到されるものではない。

(4) 取消事由４（実施可能要件に関する認定の誤り）

ア(ｱ) 本願発明を実施するための事項は，以下のとおり，本願明細書等に記載されており，実施可能要件を満たしている。

(ｲ) 本願明細書等の「関数鍵 $k_c$ が回路２１の暗号化を実施する役割を果たす。この暗号化は例えばレジスタ２２の内部で入力変数 x を暗号化された変数 y=DES（x，$k_c$）に変換する DES アルゴリズム２３である。」（【００４０】）との記載及び図４によれば，本願明細書等には，回路２１に，入力変数 x が入力されるとともに関数鍵 $k_c$ が入力され，回路２１で DES アルゴリズムを実行し，暗号文 y=DES（x，$k_c$）を出力するという事項が記載されているということができる。これは，本願の請求項１の「暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路（２１）」の記載に相当する。

また，本願明細書等の「暗号鍵９，k はまた Feistel 関数１０によりマスク m によってマスクされる。」（【００２７】）との記載並びに図１及び２によれば，図１及び２の回路に示される鍵 $k_c$ が，マスク m によってマスクされる暗号鍵であるということが理解される。そして，本願明細書等には，図１及び２に示される回路の説明として「K⊕M つ

まり秘密鍵 K それ自体がマスク M により暗号化される。」との記載（【００２８】）があるところ，上記回路の（マスク m によってマスクされる）暗号鍵 $k_c$ は，（マスク M によってマスクされる）秘密鍵 K と同一である。ここで，秘密鍵とは，暗号文 y の復号化に必要な鍵であって暗号化アルゴリズム F（x，k）を実行するための鍵 k であると定義される。そうすると，本願明細書等の上記記載並びに図１及び２には，秘密鍵 $k_c$ が，マスク m によって，$K \oplus M$ という形式でマスクされて暗号化されるものの，図１及び２に示される回路で暗号化アルゴリズム F（x，$k_c$）を実行すると，暗号文 y=F（x，$k_c$）が出力される（秘密鍵 $k_c$ が暗号文 y の復号化に必要な鍵である）ことが示されているといえる。これは，本願の請求項１の「暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路（２１）」の記載に相当する。

(ｳ) 本願の請求項１の「入力変数 x は，マスク鍵 $k_c \oplus k_i$ によって暗号化され」につき，本願明細書等の図４には，関数鍵 $k_c$ が，マスク（第２の鍵）$k_i$ と XOR ゲートで XOR 演算されて（$k_c \oplus k_i$），DES アルゴリズム２３の内部のレジスタ２２に入力されることが示されている。他方，同図には，入力変数 x が，DES アルゴリズム２３に入力されることも示されている。このため，DES アルゴリズム２３に入力された入力変数 x は，DES アルゴリズム２３の内部のレジスタ２２に入力されたマスク鍵 $k_c \oplus k_i$ によって暗号化されることを，当業者であれば理解する。

また，本願明細書等の「左右のデータレジスタに保存される前に，メッセージのデータは左で XOR ゲート７および右で XOR ゲート８という手段によりマスクデータと組み合わされることによってマスクされる。暗号鍵９，k はまた Feistel 関数１０によりマスク m によってマスクされる。」（【００２７】）との記載並びに図１及び２によれば，XOR ゲート８で，メッセージデータ（入力変数 x）と第２の鍵 $k_i$ が XOR 演算

（$x \oplus k_i$）されていること，及びこの演算結果がレジスタ６を経て Feistel 関数１０に入力され，E で示される箇所を経て，関数鍵 $k_c$ と XOR 演算（$x \oplus k_i \oplus k_c$）されていることが，それぞれ理解される。排他的論理和⊕（XOR 演算子）は，その左辺と右辺を交換しても計算結果は同じであり（交換法則），計算の優先順位を変えても計算結果は同じである（結合法則）ことから，Feistel 関数１０に入力され，E で示される箇所を経て得られた $x \oplus k_i \oplus k_c$ は，$x \oplus (k_c \oplus k_i)$となる。そうすると，図１及び２には，「マスク鍵 $k_c \oplus k_i$ によって入力変数 x が暗号化され（$x \oplus (k_c \oplus k_i)$）」という事項が示されているといえる。

(ｴ) 本願明細書等の記載（【００３７】）及び図３によれば，図３において，入力データ X が $x \oplus k_c$ であり，マスク M が第２の鍵 $k_i$ であるとすると，レジスタ３１の前段の XOR 演算部で $x \oplus k_c \oplus k_i$ の演算がされ，いずれのレジスタにおいても第２の鍵 $k_i$ によってマスキングがされることにより，$x \oplus k_c$ は漏洩されないが，レジスタ３５の後段の XOR 演算部からは第２の鍵 $k_i$ がデマスキングされた E（$x \oplus k_c$）が出力されるという事項が示されているといえる。

また，本願明細書等の図２においても，図３と同様に，Feistel 関数１０内の E の後段の XOR 演算部で $x \oplus k_c \oplus k_i$ の演算がされ，いずれのレジスタにおいても第２の鍵 $k_i$ によってマスキングがされて，$x \oplus k_c$ は漏洩されないが，XOR 演算部１３，１４からは，第２の鍵 $k_i$ がデマスキングされた暗号文が出力されるという事項が示されているといえる。

イ(ｱ) 本願発明は，その名称が示すとおり「その暗号変換により特に情報漏洩観測攻撃から保護される暗号回路」に関し，暗号回路においてサイドチャネル攻撃から保護されることを課題とする。したがって，本願発明の暗号回路を実施するための事項を発明の詳細な説明に記載すれば足り，暗号回路を実施するための事項以外の事項である復号を実施するた

めの事項が発明の詳細な説明に記載されていないことをもって，実施可能要件を満たしていないということにはならない。

(イ) マスク鍵 $k_c \oplus k_i$ によって暗号化された入力変数 x を，暗号回路から「$y=DES(x, k_c)$」として第２の鍵 $k_i$ を用いない形式で出力することは可能である。

すなわち，本願明細書等の図２に示されるとおり，本願発明においては，暗号化アルゴリズムに XOR ゲート７，８，１２，１３，１４を付加することによって，第２の鍵 $k_i$ は，マスク鍵 $k_c \oplus k_i$ のために使用される一方で，XOR 演算を繰り返すことによって最終的に消去される。このため，出力１５（同図）から最終的に得られた暗号文 y を解読するためには，関数鍵 $k_c$ さえ知り得ればよく，第２の鍵 $k_i$ を要しない。このことは，本願発明の出願時における当業者の技術常識をもって理解し得る。

ウ 以上より，実施可能要件に関する本件審決の認定は誤りである。

(5) 取消事由５（明確性要件に関する認定の誤り）

本願の請求項１に「マスク鍵 $k_c \oplus k_i$ によって暗号化された入力変数 x を，暗号回路から第２の鍵 $k_i$ を用いない形式で出力でき，出力されたものを関数鍵 $k_c$ によって復号できる」ことが記載されていることについては，取消事由４と同様である。

したがって，明確性要件に関する本件審決の認定は誤りである。

２ 被告の主張

(1) 取消事由１（本願発明１の認定の誤り）に対し

ア 本件審決は，特許請求の範囲に記載された事項により特定されるものとして本願発明１の認定を行ったものであり，その認定に誤りはない。

イ(ア) 原告は，本願発明１における関数鍵 $k_c$ とは，暗号化アルゴリズムを実行する鍵のことであり，具体的には，DES アルゴリズム２３に入力

されてこれを実行し，入力変数 x から暗号文 y を出力することに機能する鍵のことであり，「暗号化アルゴリズム」の操作とは，本願の請求項１に記載の「暗号化アルゴリズムを実行する」操作であり，関数鍵 $k_c$ によって暗号化アルゴリズムを実行して（最終的に）暗号文を出力する操作を意味する旨主張する。

しかし，本願発明１に係る特許請求の範囲には「暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路（２１）であって」と記載されているに過ぎず，「関数鍵 $k_c$」につき，「暗号化アルゴリズムを実行するための関数鍵 $k_c$」であることや「関数鍵 $k_c$ を含む暗号回路」と特定されているものの，「関数鍵 $k_c$」が単独で「暗号化アルゴリズムを実行する鍵のことであ」ることや「関数鍵 $k_c$ によって暗号化アルゴリズムを実行して（最終的に）暗号文を出力する」ことは，何ら特定されていない。

したがって，原告の上記主張は，本願の特許請求の範囲の記載に基づくものではない。

(イ) 原告は，最終的に入力変数 x から生成して出力される暗号文を復号する（攻撃者にとっては解読する）ためには，Feistel 関数 f に入力されて暗号化処理に適用される鍵，つまり暗号化アルゴリズムを実行することに機能する関数鍵 $k_c$ を知る必要がある，関数鍵 $k_c$ が暗号化アルゴリズムを実行して入力変数 x から暗号文，つまり暗号化された変数 y を出力することに機能することは，本願明細書（【００４０】，図４）に「$y=DES(x, k_c)$」として記載されているなどと主張する。

しかし，本願発明１の特許請求の範囲には「入力変数 x はマスク鍵【数１】$k_c \oplus k_i$ によって暗号化され」と記載されているに過ぎず，「入力変数 x はマスク鍵 $k_c \oplus k_i$ で暗号化」されることは特定されているものの，「関数鍵 $k_c$ が暗号化アルゴリズムを実行して入力変数 x から暗号

文，つまり暗号化された変数 y を出力することに機能」することや，「$y=DES（x，k_c）$」として出力されることについては，何ら特定されていない。

したがって，原告の上記主張は，本願の特許請求の範囲の記載に基づくものではない。

(ｳ) 原告は，本件明細書等の図１及び２の記載を根拠として，「暗号化」の操作とは本願の請求項１の「入力変数 x はマスク鍵 $k_c \oplus k_i$ によって暗号化され」る操作であり，マスク鍵 $k_c \oplus k_i$ によって入力変数 x を暗号化するという，暗号化アルゴリズムの操作の一部を意味するなどと主張するけれども，後記（(4)イ）のとおり，上記図１及び２の実施例は，本願発明１に係る特許請求の範囲に対応する実施例ではない。

(ｴ) 仮に，原告の主張する本願発明１の意義を参酌してクレームを限定解釈し，「関数鍵 $k_c$」が単独で「暗号化アルゴリズムを実行する鍵のことであ」ることや「関数鍵 $k_c$ によって暗号化アルゴリズムを実行して（最終的に）暗号文 $y=DES（x，k_c）$ を出力する」ことを本願発明１の構成として認定した場合であっても，引用発明においても，「関数鍵 $k_c$ によって暗号化アルゴリズムを実行して（最終的に）暗号文 $y=DES（x，k_c）$ を出力する」ことが実質的に記載されているといえるから，上記本願発明１の構成は，実質的な相違点とならない。

したがって，原告主張に従って本願発明１の上記構成を認定したとしても，容易想到性判断の結論には影響しない。

(2) 取消事由２（本願発明１と引用発明との一致点及び相違点の認定の誤り）に対し

ア 原告は，鍵 $k_c$ に関し，本願発明１の関数鍵 $k_c$ は，暗号化アルゴリズムを実行して暗号文を出力することに機能するものである旨主張する。

しかし，前記のとおり，本願発明１の特許請求の範囲には「暗号化ア

ルゴリズムを実行するための関数鍵 $k_c$ を含む暗号化回路（２１）であって」と記載されているに過ぎず，「暗号文を出力することに機能」するものであることは何ら特定されていないから，原告の上記主張は，本願の特許請求の範囲の記載に基づくものではない。

イ　原告は，引用発明につき，引用発明の「暗号キー」は，それ単独で暗号化アルゴリズムを実行して暗号文を出力することに機能するものではなく，暗号キーとマスクとが XOR 演算された「マスキングをかけたキー」が暗号化アルゴリズムを実行して暗号文を出力することに機能する旨主張する。

しかし，引用文献１の記載（【０００８】，【００１１】）によれば，引用文献１の暗号化アルゴリズムは，ランダム順で真及びダミーキーを使用しており，ダミーキーから間違った結果はダミーメモリロケーションに格納されるが，Zero でマスキングされたキーは「真のキー」として，その結果は真の結果としてメモリに格納される。ここで，Zero でマスキングされたキーはマスキングされないキーと等価であることは明らかであるので，引用発明の「『DES 暗号アルゴリズム』を実行するための暗号キーを含む DES 計算ユニット，キーマスキングユニット，メモリを含む暗号ハードウェア」における「暗号キー」には，マスキングされたダミーキーだけでなく，マスキングされないキーと等価である「真のキー」が含まれる。すなわち，引用発明の「暗号キー」には，本願発明１の「関数鍵 $k_c$」に相当するものも含まれるといえる。

したがって，引用発明に関する原告の上記主張は，引用文献１の記載の理解を誤ったものである。

(3)　取消事由３（容易想到性に関する認定の誤り）に対し

ア　原告は，本願発明１では，マスキングの対象となるキー，つまり第２の鍵 $k_i$ によってマスキングされる対象となる関数鍵 $k_c$ が，暗号化アルゴリ

ズムを実行して暗号文を出力することに機能するのに対して，引用発明では，マスキングをかけたキーが暗号アルゴリズムを実行して暗号文を出力することに機能するという点で異なるため，本願発明１は引用発明に対して顕著な作用効果を奏功する旨主張する。

しかし，原告の上記主張は，前記(1)イ(ｱ)，(ｲ)及び(2)イのとおり，本願発明１についてはその特許請求の範囲の記載に基づくものとはいえず，引用発明についても，引用文献１の記載の理解を誤ったものである。

イ　原告は，引用文献１に引用文献２を組み合わせても，引用文献２に示されるデータ d，物理データ p，値 f(d，p)は，いずれも，本願発明の「第２の鍵 $k_i$によってマスクされる鍵であって，暗号化アルゴリズムを実行する関数鍵 $k_c$」，「暗号化アルゴリズムを実行する関数鍵 $k_c$ をマスクする第２の鍵 $k_i$」，「入力変数 x をマスクするマスク鍵 $k_c \oplus k_i$（暗号化アルゴリズムを実行する関数鍵 $k_c$ と第２の鍵 $k_i$ が XOR 演算によって組み合わせられた鍵）」に相当しないから，相違点１及び３に係る構成には想到し得ない旨主張する。

しかし，前記のとおり，本願の特許請求の範囲の記載では「暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路」，「入力変数 x はマスク鍵 $k_c \oplus k_i$ によって暗号化」との特定がされているものの，「第２の鍵 $k_i$によってマスクされる鍵であって，暗号化アルゴリズムを実行する関数鍵 $k_c$」，「暗号化アルゴリズムを実行する関数鍵 $k_c$ をマスクする第２の鍵 $k_i$」，「入力変数 x をマスクするマスク鍵 $k_c \oplus k_i$（暗号化アルゴリズムを実行する関数鍵 $k_c$ と第２の鍵 $k_i$ が XOR 演算によって組み合わせられた鍵）」という態様は，本願の特許請求の範囲で特定されていない。

したがって，原告の上記主張は，本願の特許請求の範囲の記載に基づくものではない。

(4)　取消事由４（実施可能要件に関する認定の誤り）及び取消事由５（明確

性要件に関する認定の誤り）に対し

ア　本願発明を暗号回路として実施するための事項が本願明細書等に記載されているということはできない。

すなわち，暗号回路といえるためには，復号可能な暗号化を実行することが必要であることは，暗号技術分野の技術常識である。そして，本願の請求項では，入力変数 x をマスク鍵 $k_c \oplus k_i$ で暗号化しているから，暗号化の際と復号化の際には同じ秘密鍵が必要となるという共通鍵暗号の技術常識に照らし，復号化の際には暗号化の際に使用したマスク鍵 $k_c \oplus k_i$ が必要となる。

しかし，サイドチャネル攻撃によって暗号化の際に使用した秘密鍵は特定されてしまうことから，秘密鍵 $k_c$ を使用する代わりにマスク鍵 $k_c \oplus k_i$ を使用して暗号化を行ったとしても，暗号解読に必要なマスク鍵 $k_c \oplus k_i$ が特定されてしまうことになる。これは，本願の請求項１の「サイドチャネルを利用した攻撃から回路を保護することを可能とする第２の鍵 $k_i$ を含むことを特徴とする回路」という記載と整合しないから，上記請求項の記載は技術的に不明瞭となっている。

また，本願明細書等の実施例（図２及び４）によっても，入力変数 x をマスク鍵 $k_c \oplus k_i$ で暗号化しながら，出力暗号文として「$y=DES(x, k_c)$」が出力されることが，当業者に実施可能な程度に具体的に記載されているということはできない。

したがって，本願の請求項は技術的に不明瞭であるから，明確性要件を満たしているとはいえず，また，本願明細書等には，本願の請求項に係る発明である回路を暗号回路として実施するための事項が記載されていないから，実施可能要件を満たしているとはいえない。

イ　本願明細書等の図２について

(ｱ)　原告は，本願明細書等の図２を根拠として，第２の鍵 $k_i$ は，マスク

鍵 $k_c \oplus k_i$ のために使用されるが，XOR 演算を繰り返すことによって消去され，最終的に得られた暗号文 $x \oplus k_c$ を解読するためには，関数鍵 $k_c$ さえ知り得ればよく，第２の鍵 $k_i$ を要しない旨主張する。

(ｲ) しかし，図２では，入力変数 x であるメッセージに初期置換 IP１を行い（IP(x)），第２の鍵 $k_i$ にも初期置換 IP２を行い（$IP(k_i)$），IP１の出力 IP(x)と IP２の出力 $IP(k_i)$を XOR ゲート８で XOR 演算して（$IP(x) \oplus IP(k_i)$），レジスタ６に格納している。そして，レジスタ６に格納された $IP(x) \oplus IP(k_i)$に拡大置換 E を行い（$E(IP(x) \oplus IP(k_i))$），出力 $E(IP(x) \oplus IP(k_i))$と関数鍵 $k_c$ とで XOR 演算を行い（$E(IP(x) \oplus IP(k_i)) \oplus k_c$），S ボックス９への入力としている。

このうち，IP１の出力 IP(x)と IP２の出力 $IP(k_i)$を XOR ゲート８で XOR 演算（$IP(x) \oplus IP(k_i)$）している点は，入力変数 x であるメッセージを第２の鍵 $k_i$ との XOR 演算によりマスクしているということができる。他方，S ボックス９への入力 $E(IP(x) \oplus IP(k_i)) \oplus k_c$ において，関数鍵 $k_c$ と第２の鍵 $k_i$ に着目すると，関数鍵 $k_c$ と第２の鍵 $k_i$ とで直接 XOR 演算を行っていない。そうすると，「関数鍵 $k_c$ は XOR 演算によって…第２の鍵 $k_i$ によってマスクされ」ているとはいえない。

(ｳ) また，初期置換 IP の入力は６４ビット幅であるから，第２の鍵 $k_i$ のビット幅は６４ビットである。他方，拡大置換 E の出力は４８ビット幅であるから，拡大置換 E の出力 $E(IP(x) \oplus IP(k_i))$のビット幅は４８ビットである。

ここで，XOR 演算は，同じビット幅を有する２つの２進数を入力とする２項演算であるという技術常識を踏まえると，拡大置換 E の出力 $E(IP(x) \oplus IP(k_i))$との XOR 演算の対象となっている関数鍵 $k_c$ のビット幅は，拡大置換 E の出力 $E(IP(x) \oplus IP(k_i))$のビット幅と同じ４８ビットである。

「入力変数をマスク鍵 $k_c \oplus k_i$ で暗号化」するためには，少なくとも第

２の鍵 $k_i$ と関数鍵 $k_c$ とが間接的に XOR 演算していること，すなわち，$E(IP(x)\oplus IP(k_i))\oplus k_c$ の演算順序を入れ換えて，例えば $E(IP(x)\oplus IP(k_i\oplus k_c))$ のように変換可能である必要があるが，初期置換 IP 及び拡大置換 E は，ビット位置の入れ替えやビット幅の拡大を行っているから，初期置換 IP 及び拡大置換 E 並びに XOR 演算の演算順序は入れ換え可能であるとはいえない。仮に初期置換 IP 及び拡大置換 E 並びに XOR 演算の演算順序が入れ換え可能であったとしても，ビット幅の異なる第２の鍵 $k_i$（ビット幅６４ビット）と関数鍵 $k_c$（ビット幅４８ビット）とは XOR 演算できない。

したがって，図２の実施例において，第２の鍵 $k_i$ と関数鍵 $k_c$ とは，間接的にも XOR 演算しているとはいえない。

(ｴ) 以上より，図２の実施例において，第２の鍵 $k_i$ と関数鍵 $k_c$ とは，直接的にも間接的にも XOR 演算しているとはいえないから，同実施例は「入力変数をマスク鍵 $k_c\oplus k_i$ で暗号化」しておらず，「関数鍵 $k_c$ は XOR 演算によって…第２の鍵 $k_i$ によってマスクされ」ているとはいえない。そうすると，同実施例は，本願の請求項に係る発明に対応する実施例ということはできない。

したがって，図２の実施例に基づく原告の主張は，本願の請求項の記載に基づく主張でないから，理由がない。

(ｵ) 仮に図２に記載の実施例が「入力変数をマスク鍵 $k_c\oplus k_i$ で暗号化」しているとしても，少なくとも，図２の S’１６は，DES アルゴリズムの基本構成である S ボックス９と区別され，S ボックス９とは異なり，２つの４８ビット幅の入力を持っている。しかし，図２の S’１６がどのような演算を行っているのかについて，本願明細書等には何ら記載も示唆もない。このため，図２に記載の実施例を当業者が実施することはできず，実施可能要件を満たしているとはいえない。

第４　当裁判所の判断

１　本願発明

本願発明に係る特許請求の範囲請求項の記載は，前記（第２の２）のとおりである。

２　本願明細書等の記載等

(1)　技術分野（【０００１】）

本発明はそれらの暗号化により特に情報漏洩観測攻撃から保護される暗号回路に関する。

(2)　背景技術

通信および情報処理のための手段のローミング能力が増すとともに，新しい攻撃が考えられるようになっている。実行速度の点から，それを構成する電子回路，例えば DPA 攻撃によるエネルギー消費量の点から，またはその放射挙動，例えば EMA 攻撃による磁気放射の点からシステムの時間的挙動を観測することにより大量の情報が漏洩しうる。サイドチャネルへのこれらの攻撃に対しては，特に，

この例では秘密とは無関係に漏えいを一定にすることを伴う秘匿と，

漏えいをランダムにすることを伴う，つまり予測不能でありしたがって利用不可能とするマスキングと，を基にする保護が提案されている。（【０００４】）

これらの２つの技法は情報の取得を狙った攻撃の困難さを増すことを可能とするが，それらはそれでもなお実装欠陥から利益を得るであろう攻撃に対しては依然脆弱である。DPA 攻撃の例は，P.Kocher らによる文献，Differential Power Analysis, In proceedings of CRYPT’99, volume 1666 of LNCS, pages 338-397, Springer-Verlag, 1999 に記載されている。EMA 攻撃の例は K.Gandolfi らによる文献，Electromagnetic Analysis-Concrete Results, In CHES, volume 2162 of LNCS, pages 251-261, Springer-Verlag, 2001 に記載されている。

（【０００５】）

起こりうるまたは立証された脆弱性の例は数多く存在する。

以下が特に挙げられる。

差分論理（WDDL などの）に基づく秘匿は計算フェーズと評価フェーズとプリチャージフェーズとのうちの１つまたは別の間の累積した組み合わせのずれの差への攻撃に対して脆弱となる場合がある。

マスキングは HO-DPA と呼ばれる高階攻撃に敏感な場合がある。（【０００６】）

(3)　課題を解決するための手段

本発明の目的は特にこれらの，特に DPA または EMA タイプの攻撃に対抗することである。この目的のため，本発明の対象は暗号アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路であって，前記回路は $k_c$ とは別の前記回路のそれぞれの例に特有の，回路のサイドチャネルを利用した攻撃から回路を保護することを可能とする第２の鍵 $k_i$ を含むことを特徴とする。（【０００７】）

関数鍵 $k_c$ は例えば XOR 演算によって２つの鍵を組み合わせることにより第２の鍵 $k_i$ によってマスクされ，入力変数 x はマスク鍵

【数１】

$$k_c \oplus k_i$$

によって暗号化されている。（【０００９】）

第２の鍵 $k_i$ は例えば秘密実装によって鍵 $k_c$ を保護する役割を果たす。（【００１０】）

第２の鍵 $k_i$ は例えば特に鍵 $k_i$ でマスキングすることにより保護される２つの秘密関数の囲い込みによってカスタマイズされる標準暗号アルゴリズムからなる秘密アルゴリズムを保護する役割を果たす。（【００１１】）

第２の鍵 $k_i$ は例えば PUF（Physically Unclonable Function）または POK

（Physically Obfuscated Key）タイプの関数により生成される。（【００１２】）

第２の鍵 $k_i$ により導入されるマスキングは HO-DPA 高階攻撃に対して保護されてもよい。（【００１４】）

回路に固有の実装鍵としての役割を果たす第２の鍵 $k_i$ の知識により，例えば保護管理プロシージャを，前記管理を担う特権ユーザが使用することが可能となる。（【００１５】）

これは FPGA タイプのプログラマブル回路で実現されてもよい。（【００１６】）

第２の鍵 $k_i$ は FPGA のプログラミングファイルを介してカスタマイズされてもよい。（【００１７】）

有利には，回路はソフトウェアの実装により実現されてもよい。（【００１８】）

それは例えば前記 FPGA 回路のプログラミングファイル（２５）を暗号化し，これにより外部記憶の機密性および FPGA への鍵 $k_i$ の移転の機密性を付与するための第３の鍵 $k_b$ を含む。（【００１９】）

第２の鍵 $k_i$ の基数は例えば関数鍵 $k_c$ の基数に等しい。これは $k_i$ への隠しチャネル攻撃を $k_c$ への暗号解読攻撃よりも困難にするためである。（【００２０】）

第３の鍵 $k_b$ の基数の基数は関数鍵 $k_c$ の基数よりも大きいかまたは等しい。（【００２１】）

この暗号化アルゴリズムは DES アルゴリズムである。（【００２２】）

(4)　発明を実施するための形態

図１に本発明が適用されうるマスキングのモードを呈示する。特に図１には，特に S.Guille らによる文献，A fast Pipelined MultiMode DES Architecture Operating in IP Representation, Integration, The VLSI Journal, 40(4) pages 479-489,

July 2007, DOI に概要が示されるアーキテクチャに従い実装される DES（Data Encryption Standard）アルゴリズムのマスキングの図が例として呈示される。図１の回路は例えば FPGA（Field Programmable Gate Array）タイプのプログラマブル論理回路で実現される。このアルゴリズムでは，データパスは２つの部分，左と右とに分割される。（【００２５】）

対比のために，図２はマスキングによる保護を保証するためのハードウェアオーバーヘッドを強調する同様の回路を示し，このオーバーヘッドを生じさせる回路は破線により示されている。（【００２６】）

したがって左のデータレジスタ３と右のデータレジスタ４との間に入力メッセージ１が割り当てられる。左のマスクレジスタ５と右のマスクレジスタ６との間にマスク２が割り当てられる。左右のデータレジスタに保存される前に，メッセージのデータは左で XOR ゲート７および右で XOR ゲート８という手段によりマスクデータと組み合わされることによってマスクされる。暗号鍵９，k はまた Feistel 関数１０によりマスク m によってマスクされる。右のレジスタ６のマスクされるデータと右のレジスタ２の半分のマスクは，そこで右のマスクされるデータが第１の換字ボックス９により暗号化され，かつ，そこで右の半分のマスクが第２の換字ボックス１６により暗号化される Feistel 関数の入力を形成する。左のデータレジスタ５と左のマスクレジスタ１のデータは XOR ゲート１１，１２という手段により Feistel 関数の出力においてそれぞれ右のデータと新しいマスクとに組み合わされ，その後右のレジスタにループ状に戻り，左右のデータはその後暗号化されたメッセージを出力１５するように XOR ゲート１３，１４により再び組み合わされる。図１のタイプの回路ではデータレジスタ５，６のみが漏洩すると想定される。（【００２７】）

本発明による回路は漏洩を続けるがそれを暗号化の状態にするため理解できない。したがって例えば DPA または EMA タイプの攻撃を実行する攻撃

者には以下の変数のみがわかる。

【数２】

$K \oplus M$ (1)

つまり秘密鍵 K それ自体がマスク M により暗号化される。鍵 K のこの保護モードは，XOR とも呼ばれかつ

【数３】

$\oplus$

により表される「排他的論理和」演算を用いる Vernam 暗号という名で公知であり，Vernam コードは XOR 演算を用いて暗号化することができるコードである。本発明による暗号回路はしたがって情報漏洩の Vernam 暗号化により隠しチャネルへの攻撃から保護される。（【００２８】）

暗号化アルゴリズムが完全にカスタマイズされる用途分野が存在する。例えば秘密暗号に依存する GSM の公共または私用の範囲または有料テレビがそのようなケースである。この選択を正当化するために通常述べられる主張には，回路と相関関係となる漏えい関数が未知であるためサイドチャネルへの攻撃，いわゆる SCA（Side-Channel Attacks）は不可能ということがある。K.Tiri らの文献，Side-Channel Leakage Tolerant Architectures, In ITNG’06-Proceedings of the Third International Conference on Information Technology, New Generation, pages 204-209, Washington DC, USA, 2006 IEEE Computer Society では，アルゴリズムの実装および機能性を，ハードウェアの量の点でオーバーヘッド有りまたは無しで一度にかつ同時に変更することを提案している。前の２つのプロシージャの欠点は，暗号化が関数的に秘密であることである。これはセキュリティの専門家がシステムおよびその配備を実施する特定の典型的な場合においては容認されうる。しかし暗号化システムの設計および配布を監視することが困難であるほとんどの場合，この筋書きは非常に不確実である。いったん秘密の機能性が回復すると，DPA タイプの攻撃は再度容

易に可能となる。さらに例えば FIPS-140 などの特定の証明方式では，暗号標準をカスタマイズせずに使用することが要求される。これにより特に K.Tiri らによる文献で支持される SCA に耐性のある全プロシージャは禁止とされる。（【００２９】）

本発明によれば，特にこの暗号化の公知の関数の仕様に完全に準拠する一方で暗号化を実施するためには，保護される暗号回路専用のマスクを使用してマスキングによる保護が実施される。本発明による回路には，回路専用のマスク M が単に一定であり，かつ，回路の使用者または設計者にとって未知であるマスキングアーキテクチャが含まれる。（【００３０】）

図１によるマスキングパスは，実際，上述の式（１）に従い１次 DPA 攻撃つまりデータレジスタ５，６のみが漏洩すると想定される攻撃の枠組み内で暗号鍵の Vernam 暗号化を実施することが実証されうる。さらにマスキング周囲のいかなるバリアントもまた本発明を実施するために使用することができ，事実，実装は機能性を保持する一方でリファレンス実装とは異なるように表されることで十分である。マスキングの場合，リファレンス実装はゼロマスク（全ゼロ）を有するものと一致するが，マスクが非ゼロになるとすぐに，実装はしかしながら機能性を変更することなく変化する。ここで，実装に可変性を導入するように表現を変えることもまた可能である。例えば A New DPA Countermeasure Based on Permutation Tables. In SCN, volume 5229 of Lecture Notes in Computer Science, pages 278-292. Springer において，Jean-Sebastian CORON は AES の基本演算部分を２つの全単射，４ビット→４ビットを導入して変更することを提案しているが，そのような方式でそれらを組み立てることにより実際は従来の AES の計算が得られる。この表現の変化もまた秘密実装のきっかけとなりうるが，その情報漏えいはしかしながらこの文献では研究されない。（【００３１】）

したがって漏えいモデルが未知であるため１次相関攻撃は不可能とされ

る。さらに，いわゆる「テンプレート」攻撃などの，測定値のセットまたはカタログの構造に依存する攻撃は各実装が特有であり，汎用のカタログを構築することが不可能であるため実行不可能とされる。（【００３２】）

有利には，本発明において実装の多様性は暗号鍵の数に匹敵するまたは実際同等である。特に「第２の原像」タイプの攻撃はしたがって不可能である。活動中の回路と同じマスクを有する，鍵がプログラム可能な回路を偶然に見つける確率は，正しい鍵を偶然に推測する，つまりブルートフォースアタックによる鍵への全数探索で成功する確率に匹敵するかまたは実際，同等である。（【００３３】）

図１の例では，マスキングを実装するために付加されたハードウェアは左１と右２のマスクレジスタおよびマスクをデータと組み合わせる XOR ゲート１２，１３，１４ならびに右のマスクレジスタの出力を処理する Feistel 関数の換字回路１６で形成される。（【００３４】）

ASIC または FPGA をベースにした実現の枠組み内では，他のタイプの暗号プリミティブのマスキングはソースコード上で直接動作する適切な CAD ツールの支援で自動化されてもよい。（【００３５】）

保護プロシージャは一般にサイドチャネルを介して漏洩するかもしれない秘密を含むあらゆる実装に適用できることを記すことは興味深い。直接の例は暗号鍵の保護であるが，署名鍵は同様の方式で等しく十分に保護される。さらに暗号アルゴリズムのパラメータを保護する代わりに，それが秘密の場合，アルゴリズムそれ自体を保護することもまた可能である。これは通信が２地点間で暗号化されるため（サテライトタワードデコーダ（satellite toward decoder）），共同利用できない暗号が実装されうる有料テレビなどの分野で起こる。したがってその中の１または２以上の要素（換字表または拡散関数などの）を変更する一方で標準化アルゴリズムを使用することは普通である。この方式で，そのセキュリティを弱体化するリスクを冒すことな

くアルゴリズムのカスタム化が達成される。（【００３６】）

図３は別の進行方式を示す。この例では，標準アルゴリズム A はそのままで再利用されるが，実行される関数がもはや A ではなく，合成

【数４】

$$\circ A \circ$$

になるように，それは外部符号（EEin および EEout）で囲い込まれる。この原理の説明が C. Clavier による論文，Secret External Encodings Do Not Prevent Transient Fault Analysis, in CHES’07, volume 4727 of Lecture Notes in Computer Science, pages 181-194 の序章にある。図３の左の部分３０，３１，３２はマスキング技法によって数値 EE(X)の漏洩をどう防ぐことができるかを示す。関数 EE３０は２つのレジスタ３１，３２により囲い込まれ，そこで第１のレジスタ３１はデータ

【数５】

$x \oplus m$

を受信する。並列に配置された

【数６】

$$EE'(a,b).=EE(a) \oplus EE(a \oplus b)$$

として画定される関数 EE’３３はデマスキングが依然として可能であることを保証する。したがって図３の右の部分に示されるハードウェア３３，３４，３５の付加によって，アルゴリズムへの入力 X が何であるとしてもいずれのレジスタも EE(x)を含まない。この方式で，秘密の外部符号 EE についての任意の情報項目をバックトラックすることが不可能となる。以下では，しかしながら，普遍性を失うことなく，暗号鍵の漏えいに対する保護の典型的な場合に重点が置かれる。（【００３７】）

FPGA タイプというソリューションによって各回路が大規模な配置時でさえもそれ独自のコンフィギュレーションを有することが有利に可能となる。

特にFPGAのソリューションでは，それをカスタマイズするために数値を変更するために，特に構成要素専用のマスクなどのシステム全体をリコンパイルする必要はない。これは，Kerckhoffs の原理に背いておらず，それぞれの実装は実際に秘密であるが独特であることを示唆している。実装を妥協することでセットアップすべてを妥協することは認められない。（【００３８】）

特定のFPGA回路の機能性の懐古的な設計は，それが恒久的な可読メモリ内に配置されるファイル内のソフトウェアに関してプログラムされるという事実によって可能とされうる。そのような懐古的な設計を避けるため「ビットストリーム」と呼ばれる，このファイルの暗号化を可能にするFPGAタイプを使用することが可能である。したがって保護はそれ自体が暗号手段により秘密にされる。コード難読化は機械語から高レベル仕様へのバックトラッキングを対象とした演算を複雑化するための追加の受けである。（【００３９】）

図４は本発明による典型的な回路を概略的におよび簡略化した様式で示す。FPGAタイプであるこの回路２１には３つの鍵がある。関数鍵$k_c$が回路２１の暗号化を実施する役割を果たす。この暗号化は例えばレジスタ２２の内部で入力変数xを暗号化された変数y=DES（x，$k_c$）に変換するDESアルゴリズム２３である。（【００４０】）

非機能の鍵 $k_i$ が関数鍵 $k_c$ をマスクする役割を果たす。関数鍵のマスク Mを形成するのはこの鍵 $k_i$ であり，XOR 演算子がこれら２つの鍵を組み合わせて

【数７】

$$k_c \oplus k_i$$

にする。鍵 $k_i$ はしたがってDES実装の関数鍵 $k_c$ を磁気放射または特に瞬間消費の観測による情報漏洩２４から保護する役割を果たす。（【００４１】）

別の非機能の鍵 $k_b$ は「ビットストリーム」ファイル２５の秘密要素，つ

まり少なくとも $k_i$ または実際 $k_c$ を保護する役割を果たす。（【００４２】）

この手法では鍵は以下のような方式でサイズが決められることが好ましい。

$$|k_i| = |k_c| \qquad (2)$$

および

$$|k_b| \geqq |k_c| \qquad (3)$$

$|k_i|$，$|k_b|$，$|k_c|$ はそれぞれ $k_i$ の，$k_b$ の，および $k_c$ の基数を表す。（【００４３】）

本発明によれば，暗号アルゴリズム２３の実装は暗号化された変数 y が変数の暗号鍵 $k_c$ を保護する鍵 $k_i$ と関数的に独立するようにされ，セットアップの情報漏洩は

【数８】

$$2^{|k_i|}$$

ほども多様である（２の $|k_i|$ 乗）。（【００４４】）

DES アルゴリズムの場合，y=DES（x，$k_c$，$k_i$）であり，y は $k_i$ と関数的に独立である。（【００４５】）

【数９】

$k_c \oplus k_i$，$k_i$

と $k_i$ が使用者または設計者にとってを含め完全に未知であることを知った上で $k_c$ を推測する必要があるため，１次攻撃は単により困難とされるだけでなく不可能とされることに留意されたい。これにより本発明は高度の信頼を提供し，

【数１０】

$$2^{|k_i|}$$

よりも少ない計算力を有するいかなる敵対者に対しても安全が立証される。

これは｜$k_i$｜＝｜$k_c$｜の場合の DES アルゴリズムそれ自体のセキュリティレベルに等しい。（【００４６】）

PUF（Physically Unclonable Functions）または POK（Physically Obfuscated Key）タイプの関数（すなわち実装固有の物理的鍵），または回路２１に固有の秘密を，外部から供給される鍵の代わりに PKI と呼ばれる公開鍵基盤または信頼をカスタマイズするための他のあらゆるメカニズムによって生成させることが可能な他のあらゆるシステムを使用することが可能である。（【００４７】）

第２の鍵 $k_i$ はなお回路の作製後にセキュアな筐体内で単一の乱数を用いてプログラムされうる。（【００４８】）

「Shallow Attack」の名でも知られる組み合わせ論理回路への攻撃または HO-DPA 攻撃に対する対抗措置をさらに使用する定数マスクを用いたマスキングメカニズムを使用することもまた可能である。（【００４９】）

S.Mangard らによる文献，Successfully Attacking Masked AES Hardware Implementations, In LNCS, editor, Proceedings of CHES’05, volume 3659 of LNCS, pages 157-171, Springer, September 2005, Edinburgh, Scotland に特に呈示されているような，秘密マスクにほとんど依存しない「グリッチ」とも呼ばれる非機能の遷移の存在を利用したアルゴリズムのマスキングへの攻撃は，それを知らずに回路のシミュレーションを実行することが不可能であるため，秘密実装には当てはまらないことに留意されたい。事実，この攻撃は事前特性化モデルとの相関に依存する。この工程は本発明による回路では ASIC で生成されたマスクの設計または FPGA の「ビットストリーム」ファイルを知っている，またはマスクが選択されるサンプルを所持するであろう熟知しうる攻撃者を除いては実行不可能である。この可能性を防止するため，前に記載された PUF 関数が特に使用できる。（【００５０】）

特定の独自のアルゴリズム，特に２つの秘密符号間でカプセル化された

標準アルゴリズムは，C.Clavier による文献，Secret External Encodings Do Not Prevent Transient Fault Analysis, In CHES, volume 4727 of Lecture Notes in Computer Science, pages 181-194, Springer, 2007 で特に示されるように摂動攻撃に耐性がない。このクラスの攻撃では攻撃者はレジスタの値を例えば 0x00 などの既知の値に固定できることが必要とされる。本発明による実装鍵 $k_i$ により保護される回路では，データレジスタとマスクレジスタとが互いに素である場合，攻撃者はそこで簡単な欠陥を発生させるよりもはるかに困難な複数の欠陥を達成する必要があるため，これは事実上非常に困難である。（【００５１】）

実装鍵 $k_i$ を有する本発明による保護のタイプでは，例えば RTL レベルでは符号化の点において，または物理的レベルではカプセル化の点において欠陥を検知するための通常の保護などの他の保護と有利に併用することができる。これにより受動的な攻撃および能動的な攻撃の両方に対して高度の保護を達成することを可能とする。（【００５２】）

3　以上を踏まえると，本願明細書等には，本願発明について，以下の事項が記載されているものと認められる。

(1)　技術分野

本願発明は，情報漏洩観測攻撃から保護される暗号回路に関するものである（【０００１】）。ここでいう情報漏洩観測攻撃は，例えば，DPA 攻撃によるエネルギー消費量の観点又は EMA 攻撃による磁気放射の観点から，システムの時間的挙動を観測することによるサイドチャネル攻撃のことである（【０００４】）。

(2)　課題

DPA 攻撃及び EMA 攻撃のような情報漏洩観測攻撃に対しては，漏洩を秘密とは無関係に一定にすることによる秘匿，及び漏洩を予測不能にすることで利用不可能とするマスキングを基にする保護が提案されている（【０００

４】）。しかし，これらの２つの技法は，実装欠陥から利益を得るであろう攻撃に対しては依然脆弱である（【０００５】）。例えば，差分論理（WDDL などの）に基づく秘匿は，計算フェーズと評価フェーズとプリチャージフェーズとのうちの１つ又は別の間の累積した組合せのずれの差への攻撃に対して脆弱となる場合があり，また，マスキングは HO-DPA と呼ばれる高階攻撃に敏感な場合がある（【０００６】）。

本願発明の目的は，これらの攻撃，特に DPA 又は EMA タイプの攻撃に対抗することである（【０００７】）。

(3)　課題解決手段

前記目的のため，本願発明は，暗号アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路であって，前記回路は $k_c$ とは別の前記回路のそれぞれの例に特有の，回路のサイドチャネルを利用した攻撃から回路を保護することを可能とする第２の鍵 $k_i$ を含むことを特徴とする（【０００７】）。

関数鍵 kc は，例えば XOR 演算によって２つの鍵を組み合わせることにより第２の鍵 $k_i$ によってマスクされ，入力変数 x はマスク鍵 $k_c \oplus k_i$ によって暗号化されている（【０００９】）。

第２の鍵 $k_i$ は，例えば PUF（Physically Unclonable Function）又は POK（Physically Obfuscated Key）タイプの関数により生成される（【００１２】）。

暗号回路は FPGA タイプのプログラマブル回路で実現されてもよく，第２の鍵 $k_i$ は FPGA のプログラミングファイルを介してカスタマイズされてもよい。暗号回路はソフトウェアの実装により実現されてもよく，この暗号回路は第３の鍵 $k_b$ を含む。第３の鍵 $k_b$ は，前記 FPGA 回路のプログラミングファイルを暗号化し，これにより外部記憶の機密性及び FPGA への鍵 $k_i$ の移転の機密性を付与するためのものである（【００１５】～【００１９】）。

第２の鍵 $k_i$ の基数は，例えば関数鍵 $k_c$ の基数に等しく，第３の鍵 $k_b$ の基

数の基数は関数鍵 $k_c$ の基数よりも大きいかまたは等しい（【００２０】，【００２１】）。

この暗号化アルゴリズムは DES アルゴリズムである（【００２２】）。

(4)　効果

第２の鍵 $k_i$ は，例えば秘密実装によって鍵 $k_c$ を保護する役割を果たし，また，例えば鍵 $k_i$ でマスキングすることにより保護される２つの秘密関数の囲い込みによってカスタマイズされる標準暗号アルゴリズムからなる秘密アルゴリズムを保護する役割を果たす（【００１０】，【００１１】）。

第２の鍵 $k_i$ により導入されるマスキングは，HO-DPA 攻撃に対して保護されてもよい（【００１４】）。

第２の鍵 $k_i$ の基数を関数鍵 $k_c$ の基数に等しくしたため，$k_i$ への隠しチャネル攻撃は $k_c$ への暗号解読攻撃よりも困難になる（【００２０】）。

４　検討

(1)　便宜上，取消事由４（実施可能要件に関する判断の誤り）について，まず検討する。

(2)ア　本願発明の技術思想

(ｱ)　本願明細書等の記載（【００００７】）によれば，本願発明の目的は「特に DPA または EMA タイプの攻撃に対抗すること」であって，この目的を達成するために「本発明の対象は暗号アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路であって，前記回路は $k_c$ とは別の前記回路のそれぞれの例に特有の，回路のサイドチャネルを利用した攻撃から回路を保護することを可能とする第２の鍵 $k_i$ を含むことを特徴とする。」とされている。ここで，DPA 攻撃及び EMA 攻撃がサイドチャネルを利用した攻撃であることは，本願明細書等の記載（【００００４】）及び技術常識から明らかであるから，段落【００００７】の上記記載によれば，本願発明の第２の鍵 $k_i$ は，DPA 攻撃及び EMA 攻撃のようなサ

イドチャネルを利用した攻撃から暗号回路を保護するという目的を達成するためのものと認められる。

また，本願明細書等には，関数鍵 $k_c$ が第２の鍵 $k_i$ と XOR 演算されてマスク鍵 $k_c \oplus k_i$ となる旨の記載（【０００９】）に続き，「第２の鍵 $k_i$ は例えば秘密実装によって鍵 $k_c$ を保護する役割を果たす。」（【００１０】）との記載がある。他方，段落【００４１】には，関数鍵 $k_c$ と非機能の鍵 $k_i$ とを XOR 演算して $k_c \oplus k_i$ にする旨の記載に続き，「鍵 $k_i$ はしたがって DES 実装の関数鍵 $k_c$ を磁気放射または特に瞬間消費の観測による情報漏洩２４から保護する役割を果たす。」との記載がある。この「磁気放射または特に瞬間消費の観測による情報漏洩２４」が EMA 攻撃及び DPA 攻撃で用いるサイドチャネルからの情報漏洩のことを指していることは，段落【０００４】及び技術常識から明らかである。そうすると，段落【００４１】の上記記載は，段落【０００９】及び段落【００１０】の上記各記載をより具体的に記載したものであると認められる。そして，これらの記載から，第２の鍵 $k_i$ は，関数鍵 $k_c$ と XOR 演算をすることにより関数鍵 $k_c$ のマスクとして働き，関数鍵 $k_c$ を DPA 攻撃及び EMA 攻撃から保護する役割を果たすものと理解される。

そうすると，本願発明の目的である「サイドチャネルを利用した攻撃から回路を保護すること」は，段落【０００９】，【００１０】及び【００４１】で言及されているサイドチャネルを利用した攻撃から関数鍵 $k_c$ を保護することを意味し，この保護は関数鍵 $k_c$ を第２の鍵（又は非機能の鍵）$k_i$ でマスクする，すなわち $k_c$ と $k_i$ を XOR 演算することによって達成されるものと理解される。換言すれば，本願発明の暗号回路においてサイドチャネルを利用した攻撃の目標として想定されているのは関数鍵 $k_c$ であり，この関数鍵 $k_c$ をそのような攻撃から保護するために第２の鍵 $k_i$ を必要とし，関数鍵 $k_c$ を第２の鍵 $k_i$ と XOR 演算すること

によってマスクする（マスク鍵 $k_c \oplus k_i$ とする）という方法によって，関数鍵 $k_c$ の保護が達成されるものと把握される。

さらに，本願明細書等には，サイドチャネルを利用した攻撃の具体的な目標として関数鍵 $k_c$ 以外のものは記載されていない。

このように，本願発明が想定している攻撃目標は関数鍵 $k_c$ であり，それ以外の攻撃目標を想定しない以上，本願発明の暗号回路が出力する暗号文 y の秘密性は関数鍵 $k_c$ に依拠し，暗号文の計算手順（すなわち本願発明の「暗号化アルゴリズム」）に依拠するものではないと認められる。そうであれば，関数鍵 $k_c$ が判明すれば，本願発明により出力される暗号文 y を解読し得ることになる。これは，本願発明の暗号回路が出力する暗号文 y の暗号鍵が関数鍵 $k_c$ であることを意味する。すなわち，本願発明は，秘密情報である関数鍵 $k_c$ を用いて平文 x から暗号文 y を計算する関数を F で表したとき，$y=F(x, k_c)$ を満たす暗号文 y を出力する暗号回路であると認められる（以下，この技術思想を「本願技術思想①」という。）。

このように理解することは，本願明細書等の「関数鍵 $k_c$ が回路２１の暗号化を実施する役割を果たす。この暗号化は例えばレジスタ２２の内部で入力変数 x を暗号化された変数 $y=DES(x, k_c)$ に変換する DES アルゴリズム２３である。」（【００４０】）との記載とも整合する。

(イ) また，前記のとおり，本願発明の暗号回路の保護は関数鍵 $k_c$ を第２の鍵 $k_i$ でマスクすることによって達成される。このため，本願発明の暗号回路において実際に実行される計算処理に当たっては，関数鍵 $k_c$ を第２の鍵 $k_i$ と分離した形で使用してはならず，常にマスク鍵 $k_c \oplus k_i$ を用いなければならないこととなる。すなわち，本願発明の暗号回路において実際に実行される計算処理に当たっては，単体の関数鍵 $k_c$ の入力を要する上記関数 F とは別の計算方法により，単体の関数鍵 $k_c$ を直接

用いず上記マスク鍵のみを用いることによって暗号文 y を計算する必要がある（ただし，マスク鍵自体を生成する部分において関数鍵 $k_c$ を直接用いることは許される。）。

このような，単体の関数鍵 $k_c$ を直接用いずマスク鍵のみを用いることにより平文 x から暗号文 y を計算する関数を G で表すと，本願発明の暗号回路は，暗号文 y の実際の計算を $y=G(x, k_c \oplus k_i)$ によって計算するものであると認められる（以下，この技術思想を「本願技術思想②」という。）。

イ(ｱ) 上記本願技術思想①及び②によれば，本願発明の暗号回路を具現化するためには，暗号回路によって実際に計算された暗号文と，暗号化アルゴリズム F に基づいて計算された暗号文とが等しいこと，すなわち

$G(x, k_c \oplus k_i) = F(x, k_c)$

を満たすことが要求される（以下，この要求を「本願発明の技術的要求」という。）。

しかし，本願発明の技術的要求を満たす関数 G を構成する計算方法が，当業者の技術常識に鑑みて自明であると認めるに足りる証拠はない。そこで，$G(x, k_c \oplus k_i)$ の具体的な計算方法が本願明細書等に示されているかについて，以下検討する。

(ｲ) 本願明細書等の記載のうち，本願発明の技術分野，背景技術及び課題を解決するための手段の記載（【０００１】～【００２４】）並びに本願発明の実施形態のうち図４に係る部分の記載（【００４０】～【００５２】）には，前記のとおり，本願技術思想①及び②が開示されている。しかし，本願発明の技術的要求を満たす関数 G の具体的態様について開示したものと理解される記載は見当たらない。

また，特許請求の範囲の記載は，上記記載の内容を超えるものではなく，関数 G の具体的態様は記載されていない。

(ｳ) a　本願明細書等の記載のうち，図１及び２並びにこれらに関する段落【００２５】～【００３６】の部分を見ると，DES アルゴリズムのマスキングの図として，図１及び２が示されており，両図は同様の回路であるとされている（【００２５】，【００２６】）。そして，図１の IP２に対して入力される「マスク」は，図２においては $k_i$ として示されていることから，図１及び２において IP に入力されるマスク $k_i$ は，本願発明の第２の鍵 $k_i$ であると認められる。

また，図１及び２における S９への入力に注目すると，E から出力される $x_m$ が $k_c$ と XOR 演算されていることから，図１及び２に示される $k_c$ は，関数鍵 $k_c$ であると認められる。

b　しかし，図１及び２の回路において，マスク鍵 $k_c \oplus k_i$ は作成されていない。

上記のとおり，関数鍵 $k_c$ と XOR 演算されるものは $x_m$ であるところ，これは，「右のマスクされるデータ（$R_i$）」６に E を適用したもの（$E(R_i)$）である。図１及び２によれば，この $R_i$ は，「メッセージ」に IP１を適用したものの右半分と，第２の鍵 $k_i$ に IP２を適用したものの右半分との XOR 演算の結果であって，第２の鍵 $k_i$ とは異なる。

他方，$x_m \oplus k_c$ の計算結果を数式で表すと，メッセージを MES とし，値の右半分を得る関数を RH とした場合，

$$x_m \oplus k_c = E(R_i) \oplus k_c = E(RH(IP(MES)) \oplus RH(IP(k_i))) \oplus k_c$$

となる。ここで，E は技術常識に鑑みて拡大置換 E を意味し，入力の３２ビットのうち１６ビットが重複して使用されて出力４８ビットに置換されるものである（乙１）。そうすると，E は XOR 演算に対して分配的に作用し，

$$x_m \oplus k_c = E(RH(IP(MES))) \oplus E(RH(IP(k_i))) \oplus k_c$$

となる。この計算結果のうち，$k_c$ 及び $k_i$ に関する部分のみを取り出し

てみても，$k_c \oplus E(RH(IP(k_i)))$（以下「式(A)」という。）が計算されているに過ぎず，明らかに $k_c \oplus k_i$ とは異なる。

仮に，IP が DES の初期置換であって単にビット位置を入れ替えているに過ぎないから無視できるとし，かつ，右半分の演算のみに注目することで RH を無視できるとしても，前記のとおり E は拡大置換であるからこれを無視することはできず，$k_c \oplus E(k_i)$は，$k_c \oplus k_i$ はもちろん $E(k_c) \oplus E(k_i)$とも異なるものとなる。

c　以上のとおり，本願明細書等の図１及び２に示される回路においては，そもそもマスク鍵 $k_c \oplus k_i$ が計算されているとは認められないことから，両図の回路をもって関数 G（x，$k_c \oplus k_i$）の具体的態様を開示したものということはできない。

d　また，段落【００２８】記載の「【数２】$K \oplus M$」は，２つの値が XOR 演算されているという点で本願発明のマスク鍵と共通するものの，記号が異なることから，本願発明を説明したものとは認められない。

仮に当該記載が本願発明を説明したものだとすると，当該記載の「秘密鍵 K」は保護対象となる鍵であるから，その機能の面から本願発明の関数鍵 $k_c$ に該当すると解されるが，【数２】と式(A)とを比較すると，$M=E(RH(IP(k_i)))$であると推測されるところ，$E(RH(IP(k_i)))$は明らかに第２の鍵 $k_i$ そのものとは異なる値である。したがって，当該記載は，本願発明と整合せず，やはり本願発明を説明するものということはできない。

e　図１及び２に関する本願明細書等のその他の記載にも，関数 G の具体的態様を開示したものと見られる記載はない。

したがって，本願明細書【００２５】～【００３６】並びに図１及び２には，関数 G の具体的態様が記載されているとはいえない。

(ｴ) 本願明細書等の記載のうち，図３及びこれに関連する段落【００３７】～【００３９】には，本願発明の関数鍵 $k_c$ に対応する概念が記載されていない。そうである以上，これらの記載及び図に関数 G（x，$k_c \oplus k_i$）の具体的態様が記載されているとはいえない。

なお，図３は図１及び２において Feistel 関数 f を示す囲みと一見類似するようにみえるけれども，図１及び２と図３にそれぞれ現れる要素の異同ないし対応関係は不明というほかなく，また，図１及び２に関する説明（【００２５】～【００３６】）に続いて「図３は別の進行方式を示す。」（【００３７】）と記載されていることに鑑みると，図１及び２と図３との間には技術的関連性はなく，相互に独立したものと見るのが相当である。このため，図１～３を総合的に見ても，関数 G の具体的態様は明らかでない。

ウ 以上より，本願明細書等には関数 G の具体的態様が記載されていないというべきである。そうである以上，本願発明を具現化して実施することはできない。

したがって，本願明細書等の発明の詳細な説明の記載は，本願発明の属する技術の分野における通常の知識を有する者がその実施をすることができる程度に明確かつ十分に記載したものということはできないから，法３６条４項１号に違反する。これと同旨をいう本件審決に誤りはない。

エ 原告の主張について

(ｱ) 原告は，本願明細書等の記載（【００２７】，【００２８】）並びに図１及び２から，両図に示される回路の（マスク m によってマスクされる）暗号鍵 $k_c$ が，（マスク M によってマスクされる）秘密鍵 K と同一であり，かつ，秘密鍵とは，暗号文 y の復号化に必要な鍵であって暗号化アルゴリズム F（x，k）を実行するための鍵 k であると定義されるから，図１及び２に示される回路で暗号化アルゴリズム F（x，$k_c$）を

実行すると，暗号文 y=F（x，$k_c$）が出力される（秘密鍵 $k_c$ が暗号文 y の復号化に必要な鍵である）ということが示されているといえ，これは，本願の請求項１の「暗号化アルゴリズムを実行するための関数鍵 $k_c$ を含む暗号回路（２１）」の記載に相当する旨主張する。

しかし，前記のとおり，本願明細書等の図１及び２並びにそれらを説明する段落【００２５】～【００３６】を参照しても，両図の S'がどのような関数であるかが不明であるため，そこに示される暗号回路の動作は不明であり，その回路が暗号文 y=F（x，$k_c$）を出力するものであるか否かは定かではない。

また，本願明細書等には「図１に本発明が適用されうるマスキングのモードを呈示する。」（【００２５】），「対比のために，図２はマスキングによる保護を保証するためのハードウェアオーバーヘッドを強調する同様の回路を示し，このオーバーヘッドを生じさせる回路は破線により示されている。」（【００２６】）との記載があるが，これらの記載の意味は明確とはいえず，図１及び２の回路が DES と同じ出力を保証しているとまでは読み取れない。

さらに，本願発明は関数鍵 $k_c$ を第２の鍵 $k_i$ で XOR 演算してマスク鍵 $k_c \oplus k_i$ を作成し，入力変数 x をマスク鍵で暗号化するものであるところ，前記のとおり，図１及び２の回路においてはマスク鍵 $k_c \oplus k_i$ が計算されていないのであるから，両図の回路が本願発明の実施形態であるとは認められない。

(イ) 原告は，本願明細書等の図４には，関数鍵 $k_c$ がマスク（第２の鍵）$k_i$ と XOR 演算されたマスク鍵 $k_c \oplus k_i$ が DES アルゴリズム２３の内部のレジスタ２２に入力されること，及び入力変数 x が DES アルゴリズム２３に入力されることが示されているから，DES アルゴリズム２３に入力された入力変数 x は，DES アルゴリズム２３の内部のレジスタ２２に

入力されたマスク鍵 $k_c \oplus k_i$ によって暗号化されることを当業者であれば理解する旨主張するとともに，本願明細書等の記載（【００２７】）並びに図１及び２によれば，図１ないし図２の XOR ゲート８で，メッセージデータ（入力変数 x）と第２の鍵 $k_i$ が XOR 演算（$x \oplus k_i$）され，その演算結果がレジスタ６を経て Feistel 関数１０に入力され，E で示される箇所を経て，関数鍵 $k_c$ と XOR 演算（$x \oplus k_i \oplus k_c$）されていることが理解されるところ，排他的論理和⊕（XOR 演算子）は交換法則及び結合法則が成立し，これらを適用すれば，$x \oplus k_i \oplus k_c$ は $x \oplus (k_c \oplus k_i)$ となるから，図１及び２には「マスク鍵 $k_c \oplus k_i$ によって入力変数 x が暗号化され（$x \oplus (k_c \oplus k_i)$）」という事項が示されている旨主張する。

しかし，まず，本願明細書等の図４を参照しても，レジスタ２２に格納されたマスク鍵 $k_c \oplus k_i$ が DES アルゴリズム２３において果たす役割については記載されていないことから，レジスタ２２に格納されたマスク鍵により入力変数 x が暗号化されることを読み取ることはできない。かつ，レジスタ２２について，本願明細書等には「関数鍵 $k_c$ が回路２１の暗号化を実施する役割を果たす。この暗号化は例えばレジスタ２２の内部で入力変数 x を暗号化された変数 y=DES（x，$k_c$）に変換する DES アルゴリズム２３である。」（【００４０】）との記載はあるものの，当該記載はレジスタ２２にマスク鍵 $k_c \oplus k_i$ が入力されることすら開示していない。

また，本願明細書等の図１及び２については，前記のとおり，そもそも，両図の回路は本願発明の実施形態とはいえない。しかも，原告の主張に係る計算手順の説明は，初期置換 IP，値の右半分を得る関数 RH（図示されない）及び拡大置換 E の影響を無視したものであって，妥当でない。仮に IP，RH 及び E の影響を無視し得るとしても，図１及び２の計算手順は，入力変数 x と第２の鍵 $k_i$ とを XOR し，その結果と関数

鍵 $k_c$ とを XOR することにより $x \oplus k_i \oplus k_c$ を得ており，マスク鍵 $k_c \oplus k_i$ を計算してから入力変数 x とマスク鍵とを XOR するものではない。すなわち，この点に関する原告の主張は，図１及び２の計算手順を無視したものというべきである。

(ｳ) 原告は，本願明細書等の記載（【００３７】）及び図３によれば，同図において，入力データ X が $x \oplus k_c$ であり，マスク M が第２の鍵 $k_i$ であるとすると，レジスタ３１の前段の XOR 演算部で $x \oplus k_c \oplus k_i$ の演算がされ，いずれのレジスタにおいても第２の鍵 $k_i$ によってマスキングがされることにより，$x \oplus k_c$ は漏洩されないが，レジスタ３５の後段の XOR 演算部からは，第２の鍵 $k_i$ がデマスキングされた EE（$x \oplus k_c$）が出力されるという事項が示されていること，図２においても，図３と同様に，Feistel 関数１０内の E の後段の XOR 演算部で $x \oplus k_c \oplus k_i$ の演算がされ，いずれのレジスタにおいても第２の鍵 $k_i$ によってマスキングがされて，$x \oplus k_c$ は漏洩されないが，XOR 演算部１３，１４からは，第２の鍵 $k_i$ がデマスキングされた暗号文が出力されるという事項が示されている旨主張する。

しかし，前記のとおり，そもそも，本願明細書等の図１及び２の回路は本願発明の実施形態であるとはいえないし，図２の Feistel 関数１０内の E の後段の XOR 演算部で演算された結果は，原告の主張する $x \oplus k_c \oplus k_i$ ではなく，$E(RH(IP(MES)) \oplus RH(IP(k_i))) \oplus k_c$ である。仮に，図２の Feistel 関数１０内の E の後段の XOR 演算部で演算された結果が $x \oplus k_c \oplus k_i$ であったとしても，原告の主張は図２における $x \oplus k_c$，$k_i$，S 及び S’がそれぞれ図３における X，M，EE 及び EE’に対応することを前提とするところ，本願明細書等の記載からそのような対応関係を理解し得ないことは前記イ(ｴ)のとおりである。

(ｴ) 原告は，暗号回路を実施するための事項以外の事項である復号を実

施するための事項が発明の詳細な説明に記載されていないことをもって，実施可能要件を満たしていないということにはならない旨主張するけれども，前記のとおり，本願明細書等は，暗号回路としての本願発明を実施するための事項（本願発明の技術的要求を満たすような具体的な関数 G）が理解できるように記載されていない。

(ｵ) 原告は，本願発明において，第２の鍵 $k_i$ は，マスク鍵 $k_c \oplus k_i$ のために使用される一方で，XOR 演算を繰り返すことによって消去されるから，本願明細書等の図２の出力１５から最終的に得られた暗号文 y を解読するためには，関数鍵 $k_c$ さえ知り得ればよく，第２の鍵 $k_i$ を要しない旨主張する。

しかし，原告の上記主張は，暗号文 y（=DES（x，$k_c$））と $x \oplus k_c$ とを混同するものであり，その前提に誤りがある。

(ｶ) その他原告がるる指摘する事情を考慮しても，この点に関する原告の主張は採用し得ない。

(3) 以上のとおり，本願明細書等の発明の詳細な説明の記載は実施可能要件を満たさないとする本件審決に誤りはなく，少なくとも原告主張に係る取消事由４については理由がない。そうすると，その余について論ずるまでもなく，原告の請求は理由がないというべきである。

5 結論

よって，原告の請求は理由がないからこれを棄却することとし，主文のとおり判決する。

知的財産高等裁判所第３部

裁判長裁判官 ＿＿＿＿＿＿＿＿＿＿

鶴 岡 稔 彦

裁判官　　杉　浦　正　樹

裁判官　　寺　田　利　彦