【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７部門第３区分
【発行日】令和4年1月19日(2022.1.19)

【国際公開番号】WO2020/213114
【出願番号】特願2021-514734(P2021-514734)
【国際特許分類】
H04L 9/32(2006.01)
【FI】
H04L 9/32 200A
H04L 9/32 200E

【手続補正書】
【提出日】令和3年10月15日(2021.10.15)
【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】
メッセージ認証コード（ＭＡＣ）の対象となるｍ個のアイテムＭ［１］，．．．，Ｍ［ｍ］から構成されるメッセージ　Ｍ＝（Ｍ［１］，．．．，Ｍ［ｍ］）を入力するメッセージ入力部と、
生成する前記ＭＡＣの数ｓ（ｓは正の整数）について、組み合わせグループテストのパラメータであるｔ行ｍ列のグループテスト行列Ｈを生成するためのグループテスト行列生成部と、
前記メッセージＭについて、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆと、前記グループテスト行列Ｈの行インデックスをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇを用いて、
前記グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに前記Ｍ［ｊ］と前記インデックスｊとを入力し、得られた前記擬似ランダム関数Ｆの出力のすべての和をとり、ｉ番目の中間タグＳ［ｉ］とし、
前記ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号ＧのＴｗｅａｋａｂｌｅ暗号化関数で前記中間タグＳ［ｉ］を暗号化して得られた出力を、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応するタグＴ［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行い、ＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）を生成する復号可能な線形グループテストＭＡＣ適用部と、
前記復号可能な線形グループテストＭＡＣ適用部により生成されたＭＡＣタグリストを出力するＭＡＣタグリスト出力部と、を備える
ことを特徴とするＭＡＣタグリスト生成装置。
【請求項２】
前記グループテスト行列Ｈは、
正の整数ａ，ｂについて（ａ，ｂ）＝ａ！／（ａ－ｂ）！ｂ！をａ個からｂ個選択する場合の数とし、
（（ａ，ｂ））を集合｛１，２，．．．，ａ｝の大きさｂの部分集合の全体としたうえで、
（ｎ，ｄ）×（ｎ，ｋ）２値行列であり、適当な順序で列と行のインデックスを（（ｎ，ｄ））の要素と（（ｎ，ｋ））の要素に対応させたうえで、ある（（ｎ，ｄ））の要素Ｄ

が（（ｎ，ｋ））の要素Ｋについて、
前記要素Ｄが前記要素Ｋに含まれるときに、
前記グループテスト行列Ｈの（Ｄ，Ｋ）エントリを１とし、それ以外を０とする行列の有限体ＧＦ（２）上の基底からなる、正の整数のパラメータ（ｎ，ｋ，ｄ）を持つＭａｃｕｌａ行列である請求項１のＭＡＣタグリスト生成装置。
【請求項３】
ある整数ｒ＞１についてｍ＝２ｒ－１，ｔ＝ｒ＋１を満たし、
ｍ＋１行ｍ＋１列のアダマール行列Ｈａｄ（ｒ）から第１行目と第１列目を削除し、さらに行列要素である－１と１のうち、－１を０とすることで得られるｍ行ｍ列バイナリ行列ｍｏｄＨａｄ（ｒ）をとり、前記グループテスト行列Ｈは、前記ｍ行ｍ列バイナリ行列の有限体ＧＦ（２）上の基底からなり、
テスト行列拡大ルールＲは、前記グループテスト行列Ｈを前記テスト行列拡大ルールＲに従って行の拡大を行った場合にｍｏｄＨａｄ（ｒ）となる請求項１のＭＡＣタグリスト生成装置。
【請求項４】
グループテスト行列Ｈが、正整数ｓについて行数と列数が共に２（２ｓ）＋２ｓ＋１の正方行列Ｐの一次独立なｔ個の行ベクトルからなる部分行列であって、
前記正方行列Ｐは、有限体ＧＦ（２ｓ）を座標成分とする２次元射影空間上の点と直線によって定まる接続行列であり、
テスト行列拡大ルールＲによって生成されるテストベクトルが前記正方行列Ｐの全ての行ベクトルである請求項１のＭＡＣタグリスト生成装置。
【請求項５】
前記グループテスト行列Ｈが、正整数ｓと３以上２ｓ＋１以下の整数ｒについて、行数がｒ×（２ｓ－１）＋１、列数が２（２ｓ）－１＋ｒの行列Ａ＿ｒにおける一次独立なｔ個の行ベクトルからなる部分行列であって、
前記行列Ａ＿ｒは、有限体ＧＦ（２ｓ）を座標成分とする２次元アフィン空間の原点を通過する予め指定したｒ本の直線上にあるｒ×（２ｓ－１）＋１個の点と、それらの点のいずれかを通過する２（２ｓ）－１＋ｒ本の直線によって定まる接続行列であり、
テスト行列拡大ルールＲによって生成されるテストベクトルが前記行列Ａ＿ｒの全ての行ベクトルである請求項１のＭＡＣタグリスト生成装置。
【請求項６】
前記グループテスト行列生成部は、すべての要素が１である行を含んだグループテスト行列Ｈを生成する請求項１から５いずれか一のＭＡＣタグリスト生成装置。
【請求項７】
メッセージ認証コード（ＭＡＣ）を用いたＭＡＣタグリスト検証の対象となるｍ個のアイテムからなるメッセージＭ＝（Ｍ［１］，．．．，Ｍ［ｍ］）と、ｔ個のＭＡＣのリストであるＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）とを入力するメッセージ入力部と、
ｔ行ｍ列のグループテスト行列Ｈを生成するとともに、複数の２値グループテスト行列Ｈの行インデックスの部分集合であるテスト行列拡大ルールＲを出力するグループテスト行列生成および拡大部と、
ＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）の要素Ｔ［ｉ］を、ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇの復号関数で復号した結果を中間タグＳ［ｉ］とする処理をすべてのｉ＝１，．．．，ｔについて行い中間タグリストＳ＝（Ｓ［１］，．．．，Ｓ［ｔ］）を得るタグ復号部と、
前記メッセージＭについて、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆとを用いて、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応する検証用中間タグＳ＊［ｉ］の生成を、前記グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに、Ｍ［ｊ］とインデックスｊとを入力し、得られたＦの出力のすべての和をとり、ｉ番目の検証用中

間タグＳ＊［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行い、検証用中間タグリストＳ＊＝（Ｓ＊［１］，．．．，Ｓ＊［ｔ］）を生成する復号可能な線形グループテスト中間タグ生成部と、
前記中間タグリストＳと、前記検証用中間タグリストＳ＊と、テスト行列拡大ルールＲと、を用いて、前記テスト行列拡大ルールＲが指定する行インデックスの部分集合に対応してＳとＳ＊をそれぞれで線形結合を行い、拡大中間タグリストｅｘＳ，検証用拡大中間タグリストｅｘＳ＊を出力する中間タグリスト拡大部と、
前記拡大中間タグリストｅｘＳと前記検証用拡大中間タグリストｅｘＳ＊とを比較してメッセージＭの中の各アイテムの検証および改ざん位置の特定を行い、検証結果として出力する中間タグリスト検証部と、
前記中間タグリスト検証部が出力する検証結果を出力する検証結果出力部とを備える
ことを特徴とするＭＡＣタグリスト検証装置。
【請求項８】
メッセージ認証コード（ＭＡＣ）の対象となるｍ個のアイテムＭ［１］，．．．，Ｍ［ｍ］から構成されるメッセージ　Ｍ＝（Ｍ［１］，．．．，Ｍ［ｍ］）を入力するステップと、
生成する前記ＭＡＣの数ｓ（ｓは正の整数）について、組み合わせグループテストのパラメータであるｔ行ｍ列のグループテスト行列Ｈを生成するステップと、
前記メッセージＭについて、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆと、前記グループテスト行列Ｈの行インデックスをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇを用いて、
前記グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに前記Ｍ［ｊ］と前記インデックスｊとを入力し、得られた前記擬似ランダム関数Ｆの出力のすべての和をとり、ｉ番目の中間タグＳ［ｉ］とし、
前記ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号ＧのＴｗｅａｋａｂｌｅ暗号化関数で前記中間タグＳ［ｉ］を暗号化して得られた出力を、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応するタグＴ［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行いＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）を生成するステップと、
前記ＭＡＣタグリストを出力するステップと、を含むＭＡＣタグリスト生成方法。
【請求項９】
メッセージ認証コード（ＭＡＣ）を用いたＭＡＣタグリスト検証の対象となるｍ個のアイテムからなるメッセージＭ＝（Ｍ［１］，．．．，Ｍ［ｍ］）と、ｔ個のＭＡＣのリストであるＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）とを入力するステップと、
ｔ行ｍ列のグループテスト行列Ｈを生成するとともに、複数の２値グループテスト行列Ｈの行インデックスの部分集合であるテスト行列拡大ルールＲを出力するステップと、
ＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）の要素Ｔ［ｉ］を、ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇの復号関数で復号した結果を中間タグＳ［ｉ］とする処理をすべてのｉ＝１，．．．，ｔについて行い中間タグリストＳ＝（Ｓ［１］，．．．，Ｓ［ｔ］）を得るステップと、
前記メッセージＭについて、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆとを用いて、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応する検証用中間タグＳ＊［ｉ］の生成を、前記グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに、Ｍ［ｊ］とインデックスｊとを入力し、得られたＦの出力のすべての和をとり、ｉ番目の検証用中間タグＳ＊［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行い、検証用中間タグリストＳ＊＝（Ｓ＊［１］，．．．，Ｓ＊［ｔ］）を生成するステップと、
前記中間タグリストＳと、前記検証用中間タグリストＳ＊と、テスト行列拡大ルールＲと、を用いて、前記テスト行列拡大ルールＲが指定する行インデックスの部分集合に対応してＳとＳ＊をそれぞれで線形結合を行い、拡大中間タグリストｅｘＳ，検証用拡大中間タ

グリストｅｘＳ＊を出力するステップと、
前記拡大中間タグリストｅｘＳと前記検証用拡大中間タグリストｅｘＳ＊とを比較してメッセージＭの中の各アイテムの検証および改ざん位置の特定を行い、検証結果として出力するステップと、
前記検証結果を出力するステップと、を含むＭＡＣタグリスト検証方法。
【請求項１０】
メッセージ認証コード（ＭＡＣ）の対象となるｍ個のアイテムＭ［１］，．．．，Ｍ［ｍ］から構成されるメッセージ　Ｍ＝（Ｍ［１］，．．．，Ｍ［ｍ］）を入力する処理と、
生成する前記ＭＡＣの数ｓ（ｓは正の整数）について、組み合わせグループテストのパラメータであるｔ行ｍ列のグループテスト行列Ｈを生成する処理と、
前記メッセージＭについて、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆと、前記グループテスト行列Ｈの行インデックスをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇを用いて、
前記グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに前記Ｍ［ｊ］と前記インデックスｊとを入力し、得られた前記擬似ランダム関数Ｆの出力のすべての和をとり、ｉ番目の中間タグＳ［ｉ］とし、
前記ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号ＧのＴｗｅａｋａｂｌｅ暗号化関数で前記中間タグＳ［ｉ］を暗号化して得られた出力を、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応するタグＴ［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行いＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）を生成するステップと、
前記ＭＡＣタグリストを出力する処理と、をコンピュータに実行させるプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
どのような部分系列にメッセージＭを分解し、またそのテストの結果、どのような改ざんアイテム特定が可能になるかは、組み合わせグループテスト（ＣＧＴ）と呼ばれる組み合わせ問題、特に非適応的組み合わせグループテスト（ＮＣＧＴ）と密接に関連がある。ここで、ＣＧＴ、ＮＣＧＴはそれぞれＣｏｍｂｉｎａｔｏｒｉａｌ　Ｇｒｏｕｐ　Ｔｅｓｔｉｎｇ、Ｎｏｎ－ａｄａｐｔｉｖｅ　ＣＧＴの略である。非特許文献３［ＧＡＴ０５］、非特許文献４［Ｍｉｎ１５］では、これらのテストについての検討がなされている。ｍ個のアイテム、ｔ個のテストからなるＣＧＴでは、ｔ行ｍ列の２値行列Ｈ（ここではテスト行列と呼ぶ）を構成し、Ｈに従ってテストを行う。Ｈのｉ行ｊ列目の要素が１であれば、ｉ番目のテストでｊ番目のアイテムをテストに含める、ということを指している。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００３２
【補正方法】変更
【補正の内容】
【００３２】
第１の視点によれば、メッセージ認証コード（ＭＡＣ）の対象となるｍ個のアイテムＭ［１］，．．．，Ｍ［ｍ］から構成されるメッセージ　Ｍ＝（Ｍ［１］，．．．，Ｍ［ｍ］）を入力するメッセージ入力部と、生成する前記ＭＡＣの数ｓ（ｓは正の整数）について、組み合わせグループテストのパラメータであるｔ行ｍ列のグループテスト行列Ｈを生成するためのグループテスト行列生成部と、復号可能な線形グループテストＭＡＣ適用部と、前記復号可能な線形グループテストＭＡＣ適用部により生成されたＭＡＣタグリストを出力するＭＡＣタグリスト出力部と、を備えるＭＡＣタグリスト生成装置が提供される。

そして、復号可能な線形グループテストＭＡＣ適用部は、前記メッセージＭについて、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆと、前記グループテスト行列Ｈの行インデックスをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇを用いて、前記グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに前記Ｍ［ｊ］と前記インデックスｊとを入力し、得られた前記擬似ランダム関数Ｆの出力のすべての和をとり、ｉ番目の中間タグＳ［ｉ］とし、前記ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号ＧのＴｗｅａｋａｂｌｅ暗号化関数で前記中間タグＳ［ｉ］を暗号化して得られた出力を、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応するタグＴ［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行い、ＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）を生成する。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００３３
【補正方法】変更
【補正の内容】
【００３３】
第２の視点によれば、メッセージ認証コード（ＭＡＣ）を用いたＭＡＣタグリスト検証の対象となるｍ個のアイテムからなるメッセージＭ＝（Ｍ［１］，．．．，Ｍ［ｍ］）と、ｔ個のＭＡＣのリストであるＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）とを入力するメッセージ入力部と、ｔ行ｍ列のグループテスト行列Ｈを生成するとともに、複数の２値グループテスト行列Ｈの行インデックスの部分集合であるテスト行列拡大ルールＲを出力するグループテスト行列生成および拡大部と、ＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）の要素Ｔ［ｉ］を、ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇの復号関数で復号した結果を中間タグＳ［ｉ］とする処理をすべてのｉ＝１，．．．，ｔについて行い中間タグリストＳ＝（Ｓ［１］，．．．，Ｓ［ｔ］）を得るタグ復号部と、復号可能な線形グループテスト中間タグ生成部と、中間タグリスト拡大部と、中間タグリスト検証部と、前記中間タグリスト検証部が出力する検証結果を出力する検証結果出力部とを備えるＭＡＣタグリスト検証装置が提供される。そして、前記復号可能な線形グループテスト中間タグ生成部は、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆとを用いて、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応する検証用中間タグＳ＊［ｉ］の生成を、前記グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに、Ｍ［ｊ］とインデックスｊとを入力し、得られたＦの出力のすべての和をとり、ｉ番目の検証用中間タグＳ＊［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行い、検証用中間タグリストＳ＊＝（Ｓ＊［１］，．．．，Ｓ＊［ｔ］）を生成する。前記中間タグリスト拡大部は、前記中間タグリストＳと、前記検証用中間タグリストＳ＊と、テスト行列拡大ルールＲと、を用いて、前記テスト行列拡大ルールＲが指定する行インデックスの部分集合に対応してＳとＳ＊をそれぞれで線形結合を行い、拡大中間タグリストｅｘＳ、検証用拡大中間タグリストｅｘＳ＊を出力する。そして、前記中間タグリスト検証部は、前記拡大中間タグリストｅｘＳと前記検証用拡大中間タグリストｅｘＳ＊とを比較してメッセージＭの中の各アイテムの検証および改ざん位置の特定を行い、検証結果として出力する。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】変更
【補正の内容】
【００３４】
第３の視点によれば、メッセージ認証コード（ＭＡＣ）の対象となるｍ個のアイテムＭ［

１］，．．．，Ｍ［ｍ］から構成されるメッセージ　Ｍ＝（Ｍ［１］，．．．，Ｍ［ｍ］）を入力するステップと、生成する前記ＭＡＣの数ｓ（ｓは正の整数）について、組み合わせグループテストのパラメータであるｔ行ｍ列のグループテスト行列Ｈを生成するステップと、前記メッセージＭについて、前記グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆと、前記グループテスト行列Ｈの行インデックスをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号Ｇを用いて、前記２値グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、前記擬似ランダム関数Ｆに前記Ｍ［ｊ］と前記インデックスｊとを入力し、得られた前記擬似ランダム関数Ｆの出力のすべての和をとり、ｉ番目の中間タグＳ［ｉ］とし、前記ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅブロック暗号ＧのＴｗｅａｋａｂｌｅ暗号化関数で前記中間タグＳ［ｉ］を暗号化して得られた出力を、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応するタグＴ［ｉ］とする処理を、すべてのｉ＝１，．．．，ｔについて行いＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）を生成するステップと、前記復号可能な線形グループテストＭＡＣ適用手段が求めたＭＡＣタグリストを出力するステップと、を含むＭＡＣタグリスト生成方法が提供される。本方法は、上記したメッセージＭを入力として、ＭＡＣタグリストを出力するコンピュータという、特定の機械に結びつけられている。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００５２
【補正方法】変更
【補正の内容】
【００５２】
図８は、行列Ｈのｉ番目の行ベクトルＨ［ｉ］がｉ番目のテストでどのアイテムをＭＡＣタグ計算に含めるかを示す。具体的には、Ｈ［ｉ］で１が立つすべての列のインデックスｊについて、Ｍ［ｊ］とｊを連結してＦに入力し、Ｆ（Ｍ［ｊ］，ｊ）を得る。各ｊについてすべてのＦ（Ｍ［ｊ］，ｊ）の和（例えば排他的論理和）をとる。さらにこのすべてのＦ（Ｍ［ｊ］，ｊ）の和と、ｉとをＧへ入力して得られた値をｉ番目のテストに対応するＭＡＣ値Ｔ［ｉ］とする。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００６６
【補正方法】変更
【補正の内容】
【００６６】
復号可能な線形グループテストＭＡＣ適用部１０３は、メッセージＭについて、グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆと、Ｔｗｅａｋａｂｌｅブロック暗号Ｇと、を用いて、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応するタグＴ［ｉ］を生成する。具体的には、復号可能な線形グループテストＭＡＣ適用部１０３は、グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、Ｍ［ｊ］とインデックスｊを擬似ランダム関数Ｆに入力する。そして、復号可能な線形グループテストＭＡＣ適用部１０３は、擬似ランダム関数Ｆに入力して得られた出力すべての和をとり、ｉ番目の中間タグＳ［ｉ］とする。さらに、復号可能な線形グループテストＭＡＣ適用部１０３は、ｉをＴｗｅａｋとしたＴｗｅａｋａｂｌｅ暗号化関数Ｇで中間タグＳ［ｉ］を暗号化し、得られた出力をタグＴ［ｉ］とする。復号可能な線形グループテストＭＡＣ適用部１０３は、すべてのｉ＝１，．．．，ｔについて、上記ＭＡＣタグＴ［ｉ］の計算を行うことで、ＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）を生成する（図８、９参照）。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００７３

【補正方法】変更
【補正の内容】
【００７３】
タグ復号部２０３は、ＭＡＣタグリストＴ＝（Ｔ［１］，．．．，Ｔ［ｔ］）をそれぞれＴｗｅａｋａｂｌｅブロック暗号Ｇの復号関数で復号し、中間タグＳ［ｉ］＝Ｇ－１（ｉ，Ｔ［１］）を得て、中間タグリストＳ＝（Ｓ［１］，．．．，Ｓ［ｔ］）を出力する。なお、以下、Ｔｗｅａｋａｂｌｅブロック暗号　Ｇによる、Ｔｗｅａｋをｉ、平文をＭとした暗号化処理をＧ（ｉ，Ｍ）と表記し、Ｔｗｅａｋをｉ、暗号文をＣとした復号処理をＧ－１（ｉ，　Ｃ）と表記する。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】０１０３
【補正方法】変更
【補正の内容】
【０１０３】
復号可能な線形グループテスト中間タグ生成部２０４は、メッセージＭについて、グループテスト行列Ｈと、可変長入力固定長出力の擬似ランダム関数Ｆを用いて、ｉ（ｉ＝１，．．．，ｔ）番目のテストに対応する検証用中間タグＳ＊［ｉ］を生成する。具体的には、復号可能な線形グループテスト中間タグ生成部２０４は、グループテスト行列Ｈのｉ行目で１が立つすべての列のインデックスｊ（ｊ＝１，．．．，ｍ）について、Ｍ［ｊ］とインデックスｊを擬似ランダム関数Ｆに入力し、得られたＦの出力のすべての和をとり、ｉ番目の検証用中間タグＳ＊［ｉ］とする。復号可能な線形グループテスト中間タグ生成部２０４は、すべてのｉ＝１，．．．，ｔについて、検証用中間タグＳ＊［ｉ］の計算を行い、検証用中間タグリストＳ＊＝（Ｓ＊［１］，．．．，Ｓ＊［ｔ］）を生成する。