(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2011-223544
(P2011-223544A)
(43)公開日　平成23年11月4日(2011.11.4)

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

審査請求 有　請求項の数 12　ＯＬ　（全 26 頁）

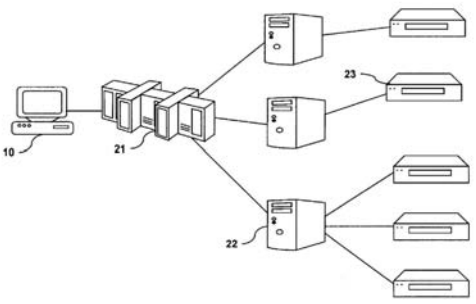
(21)出願番号　特願2010-203604 (P2010-203604)
(22)出願日　平成22年9月10日 (2010.9.10)
(31)優先権主張番号　10-2010-0032408
(32)優先日　平成22年4月8日 (2010.4.8)
(33)優先権主張国　韓国 (KR)

(71)出願人　510132956
ザ　インダストリ　アンド　アカデミック　コーポレーション　イン　チュンナム　ナショナル　ユニバーシティ（アイエーシー）
大韓民国　デジョン　３０５－７６４，ユソン－グ，グン－ドン，２２０，チュンナムユニバーシティ
(74)代理人　100082072
弁理士　清原　義博
(72)発明者　キム　スンジュ
大韓民国　４４０－７４６　キョンギド　スウォンシ　ソンギュングヮン　ユニバーシティー　＃２７３０３

最終頁に続く

(54)【発明の名称】強力なＳＣＡＤＡシステムのハイブリッドキー管理方法及びセッションキー生成方法

(57)【要約】　（修正有）
【課題】マスター端末とサブ端末との間には公開キー基盤の暗号化を適用し、サブ端末と遠隔端末との間には高い効率性を有する対称キー基盤の暗号化を適用することで、有効であると共にマスター端末に保存するキーの数を減らす代替プロトコルをサポートできる強力なＳＣＡＤＡシステムのハイブリッドキー管理方法を提供する。
【解決手段】マスター端末(ＭＴＵ)２１、多数のサブ端末(ＳＵＢ－ＭＴＵ)２２及び多数の遠隔端末(ＲＴＵ)２３が順次的な階層で構成されるＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記マスター端末と各サブ端末が自分の秘密数を生成し電子署名して交換するステップと、前記マスター端末がグループキーを生成するステップと、前記マスター端末が各サブ端末に前記グループキーを配分するが、前記グループキーは前記秘密数により暗号化及び復号化される初期配分ステップと、を含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
マスター端末(ＭＴＵ)、多数のサブ端末(ＳＵＢ－ＭＴＵ)及び多数の遠隔端末(ＲＴＵ)が順次的な階層で構成されるＳＣＡＤＡシステムのハイブリッドキー管理方法において、
前記マスター端末と各サブ端末が自分の秘密数を生成し電子署名して交換するステップと、
前記マスター端末がグループキーを生成するステップと、
前記マスター端末が各サブ端末に前記グループキーを配分し、前記グループキーは前記秘密数により暗号化及び復号化される初期配分ステップと、を含むこと
を特徴とする強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【請求項２】
前記初期配分ステップは、前記マスター端末が自分の秘密数とサブ端末の秘密数の倍で前記グループキーを累乗して前記サブ端末に伝送するステップと、
前記サブ端末が受信した累乗されたグループキーを自分の秘密数とマスター端末の秘密数の倍で逆累乗してグループキーを求めるステップと、を含むこと
を特徴とする請求項１に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【請求項３】
前記方法は、新しいサブ端末(以下、加入端末)が加入されると、前記加入端末にグループキーを配分する加入配分ステップを含み、
前記加入配分ステップは、前記加入端末が自分の秘密数を生成するステップと、
前記マスター端末と前記加入端末が各々の秘密数を認証書で暗号化して交換するステップと、
前記初期配分ステップと同一の方式に従って、前記マスター端末が前記加入端末に前記グループキーを伝送するステップと、を含むこと
を特徴とする請求項２に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【請求項４】
前記方法は、少なくとも一つのサブ端末が脱退すれば、グループキーを再分配する再分配ステップをさらに含み、
前記再分配ステップは、前記マスター端末がグループキーを再生成するステップと、
前記初期分配ステップと同一の方式に従って、前記マスター端末が脱退しない各サブ端末に再生成されたグループキーを伝送するステップと、を含むこと
を特徴とする請求項３に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【請求項５】
前記方法は、少なくとも一つのサブ端末(以下、交替される端末)が他のサブ端末(以下、交替する端末)に交替されると、グループキーを取り替える代替配分ステップをさらに含み、
前記代替配分ステップは、前記再分配ステップと同一の方式に従って、前記マスター端末がグループキーを再生成し、交替されない各サブ端末に再生成されたグループキーを伝送するステップと、
前記加入分配ステップと同一の方式に従って、前記マスター端末が交替する端末に再生成されたグループキーを伝送するステップと、を含むこと
を特徴とする請求項４に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【請求項６】
前記端末は、受信する相手の秘密数を相手の認証書で検証すること
を特徴とする請求項１～５のいずれか１項に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。

【請求項７】
前記秘密数は、代数群の部分群の生成子をランダム数ほど累乗して生成し、前記ランダム数は、代数群に属する数としてランダムに生成されること
を特徴とする請求項１～５のいずれか１項に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【請求項８】
前記秘密数は、次の［数１］により生成されること
を特徴とする請求項７に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【数１】
秘密数＝$g^{r_i} \bmod p$
ただし、$r_i \in Z_q$は端末のランダム数(マスター端末の場合ｉ＝０、サブ端末の場合ｉ∈[１、ｍ]、ｍはサブ端末の個数)、ｇは位数ｑの部分群の生成子、ｐは与えられた小さな数ｋ∈Ｎに対して、ｐ＝ｋ・ｑ＋１を満足する素数。

【請求項９】
前記初期配分ステップで、次の［数２］によってグループキーK_gを累乗して中間キーIK_iを計算し、次の［数３］によって累乗されたグループキー(または中間キー)IK_iを逆累乗してグループキーK_gを計算すること
を特徴とする請求項８に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【数２】

$$IK_i = (K_g)^{g^{r_0 r_i}} \bmod p$$

【数３】

$$K_g = K_g^{g^{r_0 r_i} / g^{r_0 r_i}} \bmod p$$

【請求項１０】
前記グループキーはツリー構造で生成し、前記ツリー構造は前記マスター端末に対応するルートノードから前記サブ端末に対応する中間ノードまでｎ次ツリーで構成し、中間ノードの子ノードを２進ツリーで構成するが、前記２進ツリーの葉ノードは前記中間ノードのサブ端末に連結される遠隔端末に対応して生成されること
を特徴とする請求項１～５のいずれか１項に記載の強力なＳＣＡＤＡシステムのハイブリッドキー管理方法。
【請求項１１】
マスター端末(ＭＴＵ)、多数のサブ端末(ＳＵＢ－ＭＴＵ)及び多数の遠隔端末(ＲＴＵ)が順次的な階層で構成される強力なＳＣＡＤＡシステムのハイブリッドキーを利用したセッションキー生成方法において、
前記マスター端末がグループキーをツリー構造で生成し、前記ツリー構造が前記マスター端末に対応するルートノードから前記サブ端末に対応する中間ノードまでｎ次ツリーで構成し、中間ノードの子ノードを２進ツリーで構成するが、前記２進ツリーの葉ノードは前記中間ノードのサブ端末に連結される遠隔端末に対応して生成するステップと、
前記マスター端末が各サブ端末または各遠隔端末に前記グループキーを配分するが、前記サブ端末または各遠隔端末は自分に対応するノードの下位ノード及び上位ノードのグループキーの配分を受けて保存するステップと、
前記マスター端末が前記ツリー構造のノードを選択し、選択したノードの下位ノードに対応するサブ端末または遠隔端末と通信するためのセッションキーを前記選択したノードの

グループキーで生成するステップと、を含み、
配分するステップで、前記マスター端末と各サブ端末は自分の秘密数を生成して電子署名して交換し、前記グループキーは前記秘密数により暗号化及び復号化されて配分されること
を特徴とする強力なＳＣＡＤＡシステムのハイブリッドキーを利用したセッションキー生成方法。
【請求項１２】
前記セッションキーは、前記グループキーと、タイムスタンプ及びシーケンス番号が結合された値をハッシュして生成すること
を特徴とする請求項１１に記載の強力なＳＣＡＤＡシステムのハイブリッドキーを利用したセッションキー生成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、マスター端末(ＭＴＵ)、多数のサブ端末(ＳＵＢ－ＭＴＵ)及び多数の遠隔端末(ＲＴＵ)が順次的な階層で構成されるＳＣＡＤＡシステムにおいて、グループキーを生成して電子署名を利用してグループキーを配分する強力なＳＣＡＤＡシステムのハイブリッドキー管理方法及びセッションキー生成方法に関する。
【０００２】
また、本発明は、マスター端末とサブ端末との間には公開キー基盤の暗号化を適用し、サブ端末と遠隔端末との間には高い効率性を有する対称キー基盤の暗号化を適用する、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法及びセッションキー生成方法に関する。
【背景技術】
【０００３】
一般的に、精油所、発電プラント及び製造施設のような現代の産業施設は命令/制御システムを具備する。このような産業上の命令/制御システムは通常ＳＣＡＤＡ(Ｓｕｐｅｒｖｉｓｏｒｙ Ｃｏｎｔｒｏｌ ａｎｄ Ｄａｔａ Ａｃｑｕｉｓｉｔｉｏｎ)システムと指称される。
【０００４】
ＳＣＡＤＡシステムを開放ネットワークに連結しようとする要求が増加するにしたがって、ＳＣＡＤＡシステムは広範囲なネットワーク保安問題に露出されてきた。ＳＣＡＤＡシステムが攻撃により損傷されると、社会に広範囲の否定的影響を及ぼす。このような攻撃を防止するために、多くの研究者がＳＣＡＤＡシステムの保安を研究中である。
【０００５】
多くの研究者がＳＣＡＤＡ用のキー管理技術を提案した。ＳＫＥ(Ｋｅｙ Ｅｓｔａｂｌｉｓｈｍｅｎｔ ｆｏｒ ＳＣＡＤＡ ｓｙｓｔｅｍｓ)とＳＫＭＡ(ＳＣＡＤＡ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ Ａｒｃｈｉｔｅｃｔｕｒｅ)が提案され、最近は、ＡＳＫＭＡ(Ａｄｖａｎｃｅｄ ＳＣＡＤＡ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ Ａｒｃｈｉｔｅｃｔｕｒｅ)とＡＳＫＭＡ＋(Ａｄｖａｎｃｅｄ ＳＣＡＤＡ Ｋｅｙ Ｍａｎａｇｅｍｅｎｔ Ａｒｃｈｉｔｅｃｔｕｒｅ＋)が提案された。
【０００６】
前記ＡＳＫＭＡ技術は、本出願人が出願した特許文献１(ＳＣＡＤＡシステム通信環境に効率的なキー管理方法)に開示されている。前記特許文献１は、グループキーの共有キーをツリー構造で生成して、遠隔端末またはサブ端末が自分に該当するノードの上位ノード及び下位ノードの共有キーを共有するＳＣＡＤＡシステム通信環境の共有キー管理方法及びセッションキー生成方法に関するものである。特に、前記特許文献１は、ＳＣＡＤＡシステムのグループキーを２進ツリー構造で生成し、中間ノードの共有キーが更新されると、更新される中間ノードからルートノードまでの経路上ノードの共有キーを全部更新し、前記経路上ノードの共有キーは自分の共有キーと経路に存在しない子ノードの共有キー

で更新する方法を提示している。

【０００７】

しかし、以前の研究は有用性(ａｖａｉｌａｂｉｌｉｔｙ)を充分に考慮していない。すなわち、以前の研究はメイン装置に故障が発生した場合に対する解決策を有していない。また、多くのＳＣＡＤＡシステム装置は制御センターから遠隔地にあるので、物理的に安全ではない。したがって、この装置は保存された保安キーを周期的にアップデートする必要がある。しかし、脆弱な装置とキーの数が増加することによってこのようなアップデートプロセスの計算及び通信費用は増加するので、ＳＣＡＤＡシステムは保安及び効率のために伝送されるキーの数を減少させる必要がある。

【０００８】

このようなＳＣＡＤＡシステムのための暗号及び保安に関する要件についてより具体的に説明する。これら要件はＳＣＡＤＡシステムに関する標準及びレポートに基盤して暗号保安要求条件を再確立したものである。

【０００９】

１）アクセス制御(Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ)：ＳＣＡＤＡシステムは組織上のユーザー及び装置を唯一の方式で識別して認証する必要がある。

【００１０】

２）有用性(Ａｖａｉｌａｂｌｉｔｙ)：有用的ではないＳＣＡＤＡシステムは物理的損傷を引き起こして人命を脅かす可能性があるので、ＳＣＡＤＡシステムの有用性は機密性(ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ)より重要である。通常、ＳＣＡＤＡシステムは、常にＯＮ状態を維持するように設計しなければならないので、予備装置(ｓｐａｒｅ ｄｅｖｉｃｅｓ)を有している。もし、メイン装置に故障が発生する場合、できるだけ迅速に予備装置に取り替える必要がある。

【００１１】

３）機密性(Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ)：ノードの間で伝送されるデータは暗号化により保護する必要がある。

【００１２】

４）暗号キーの確立及び管理(Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｋｅｙ Ｅｓｔａｂｌｉｓｈｍｅｎｔ ａｎｄ Ｍａｎａｇｅｍｅｎｔ)：制御システム内で暗号が必要となって採用される場合に、上位組織はサポートプロシージャまたはマニュアルプロシージャを有する自動化されたメカニズムを利用して暗号化キーを確立して管理する必要がある。

－ブロードキャスティング/マルチキャスティング：大部分のＳＣＡＤＡシステムは一定な形態のブロードキャスト機能を具備する。ＳＣＡＤＡシステムはブロードキャスト機能により“非常中断(ｅｍｅｒｇｅｎｃｙ ｓｈｕｔｄｏｗｎ)”のような重要なメッセージを送信することができるので、そのようなブロードキャストメッセージの保護を保障する。

－逆方向保安(ＢＳ)：部分集合(ｓｕｂｓｅｔ)を成すグループキーを知る受動的攻撃者(ｐａｓｓｉｖｅ ａｄｖｅｒｓａｒｙ)に以前のグループキーを知られないようにする。

－グループキー保安(ＧＫＳ)：攻撃者がグループキーをコンピュータで計算することを不可能にする。

－順方向保安(ＦＳ)：隣接した部分集合の以前のグループキーを知る受動的攻撃者に次のグループキーを知られないようにする。

－キー新規性(Ｋｅｙ Ｆｒｅｓｈｎｅｓｓ)：ＲＴＵは制御センターから遠隔地にある。このようなＲＴＵの位置によりＲＴＵは物理的に安全ではないので、合理的な時間内にＲＴＵのキーをアップデートする。

－完全順方向保安(ＰＦＳ)：完全順方向保安は秘密キー中の一つが将来に損傷されても１セットの長期公開キー及び秘密キーから派生されるセッションキーは損傷されないようにする。

【００１３】

５）安全性(Ｉｎｔｅｇｒｉｔｙ)：メッセージ変更及び挿入は物理的損傷を引き起こす

ことができるので、ノードの間のメッセージが不正に変更されないか新しいメッセージが挿入されないことが重要である。したがって、ＳＣＡＤＡシステムは伝送されたメッセージの安全性を保障する必要がある。

【００１４】

６）公開キー基盤施設(Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ)：組織は適切な認証政策下で公開キー認証書を発行するか、適切な認証政策下で公認されたサービス供給者から公開キー認証書を得なければならない。

【００１５】

７）キーの数(Ｎｕｍｂｅｒ ｏｆ Ｋｅｙｓ)：多くのＳＣＡＤＡシステム装置が制御センターから遠隔地にあるので物理的に不安全である。したがって、前記装置は保存した保安キーを周期的にアップデートする必要がある。また、装置が多いキーを具備しながら損傷されると、そのようなキーを具備する他の装置も脆弱になる可能性がある。したがって、キーを有する各装置はアップデートプロセスを実行しなければならない。脆弱な装置とキーの数が増加することによって、アップデートプロセスに必要な計算及び通信費用が増加するので、ＳＣＡＤＡシステムは保安及び効率性のために各装置に保存されるキーの数を減らす必要がある。

【００１６】

また、ＳＣＡＤＡシステムが要求する性能要件(ＳＣＡＤＡ Ｐｅｒｆｏｒｍａｎｃｅ Ｒｅｑｕｉｒｅｍｅｎｔｓ)及びネットワーク構成要件をより具体的に説明する。

【００１７】

まず、ＳＣＡＤＡシステムは装置と実時間で相互作用する必要がある。従来技術によると、ＳＣＡＤＡ通信のために提案された構造は、０.５４０秒以下の最小時間遅延要件を満足させる必要がある。

【００１８】

一般的に、ＳＣＡＤＡ通信リンクは３００～１９２００の伝送速度(ｂａｕｄ ｒａｔｅ)のような低速で動作する。モードバス実行ガイドでは、デフォルト伝送速度が１９２００であり、これが実行できない場合にはデフォルト伝送速度が９６００である。したがって、９６００の伝送速度要件を仮定するのが好ましい。

【００１９】

また、ＳＣＡＤＡシステムが初めて開発された時のシステム構造はメインフレームと基盤とされた。遠隔装置は直列データ伝送によりＭＴＵと直接通信された。第２世代のＳＣＡＤＡシステムは多数のシステムにかけてプロセッシングロードを分散させるために、システム小型化技術(ｓｙｓｔｅｍ ｍｉｎａｔｕｒｉｚａｔｉｏｎ)及びＬＡＮ(ｌｏｃａｌ ａｒｅａ ｎｅｔｗｏｒｋｉｎｇ)技術における開発及び改善を利用した。したがって、ローカルＭＴＵまたは管理者端末(ＨＭＩ)に問題が発生すると、前記装置を迅速に取り替えることが可能であった。したがって、対象になるＳＣＡＤＡシステムの構成(ｔｏｐｏｌｏｇｙ)は第２世代であると仮定することが好ましい。

【００２０】

上述のような要件を満足しながら、特に、有用性のための代替(ｒｅｐｌａｃｅ)プロトコルをサポートしてマスター端末(ＭＴＵ)に保存されるキーの数を減少させる強力なＳＣＡＤＡシステム用のキー管理構造が要求されている。

【先行技術文献】

【特許文献】

【００２１】

【特許文献１】大韓民国特許出願２０１０－０００６１０３号公報

【発明の概要】

【発明が解決しようとする課題】

【００２２】

したがって、本発明は上述したような従来技術の問題点を解決するためになされたもので、その目的は、マスター端末(ＭＴＵ)、多数のサブ端末(ＳＵＢ－ＭＴＵ)及び多数の遠

隔端末(ＲＴＵ)が順次的な階層で構成されるＳＣＡＤＡシステムにおいて、グループキーを生成して電子署名を利用してグループキーを配分する強力なＳＣＡＤＡシステムのハイブリッドキー管理方法及びセッションキー生成方法を提供することにある。

【００２３】

本発明の他の目的は、マスター端末と高性能のサブ端末との間には公開キー基盤の暗号化を適用し、サブ端末と性能が低い遠隔端末との間には高い効率性を有する対称キー基盤の暗号化を適用する、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法及びセッションキー生成方法を提供することにある。

【課題を解決するための手段】

【００２４】

前記目的を達成するために本発明は、マスター端末(ＭＴＵ)、多数のサブ端末(ＳＵＢ－ＭＴＵ)及び多数の遠隔端末(ＲＴＵ)が順次的な階層で構成されるＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記マスター端末と各サブ端末が自分の秘密数(ｓｅｃｒｅｔ ｎｕｍｂｅｒ)を生成して電子署名して交換するステップと、前記マスター端末がグループキーを生成するステップ、前記マスター端末が各サブ端末に前記グループキーを配分するが、前記グループキーは前記秘密数により暗号化及び復号化される初期配分ステップと、を含むことを特徴とする。

【００２５】

また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記初期配分ステップは、前記マスター端末が自分の秘密数とサブ端末の秘密数の倍で前記グループキーを累乗して前記サブ端末に伝送するステップと、前記サブ端末が受信した累乗されたグループキーを自分の秘密数とマスター端末の秘密数の倍で逆累乗してグループキーを求めるステップと、を含むことを特徴とする。

【００２６】

また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記方法は、新しいサブ端末(以下、加入端末)が加入されると、前記加入端末にグループキーを配分する加入配分ステップを含み、前記加入配分ステップは、前記加入端末が自分の秘密数を生成するステップと、前記マスター端末と前記加入端末が各々の秘密数を認証書で暗号化して交換するステップと、前記初期配分ステップと同一の方式に従って、前記マスター端末が前記加入端末に前記グループキーを伝送するステップと、を含むことを特徴とする。

【００２７】

また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記方法は、少なくとも一つのサブ端末が脱退すれば、グループキーを再分配する再分配ステップをさらに含み、前記再分配ステップは、前記マスター端末がグループキーを再生成するステップと、前記初期分配ステップと同一な方式に従って、前記マスター端末が脱退しない各サブ端末に再生成されたグループキーを伝送するステップと、を含むことを特徴とする。

【００２８】

また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記方法は、少なくとも一つのサブ端末(以下、交替される端末)が他のサブ端末(以下、交替する端末)に交替されると、グループキーを取り替える代替配分ステップをさらに含み、前記代替配分ステップは、前記再分配ステップと同一の方式に従って、前記マスター端末がグループキーを再生成して、交替されない各サブ端末に再生成されたグループキーを伝送するステップと、前記加入分配ステップと同一の方式に従って、前記マスター端末が交替する端末に再生成されたグループキーを伝送するステップと、を含むことを特徴とする。

【００２９】

また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記端末は受信する相手の秘密数を相手の認証書で検証することを特徴とする。

【００３０】
また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記秘密数は代数群(ａｌｇｅｂｒａｉｃ　ｇｒｏｕｐ)の部分群(ｓｕｂｇｒｏｕｐ)の生成子をランダム数ほど累乗して生成し、前記ランダム数は代数群に属する数としてランダムに生成されることを特徴とする。
【００３１】
また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記秘密数は次の[数１]により生成されることを特徴とする。
【００３２】
【数１】

秘密数＝$g^{r_i} \bmod p$
ただし、$r_i \in Z_q$は端末のランダム数(マスター端末の場合ｉ＝０、サブ端末の場合ｉ∈[１、ｍ]、ｍはサブ端末の個数)、ｇは位数ｑの部分群の生成子、ｐは与えられた小さな数ｋ∈Ｎに対して、ｐ＝ｋ・ｑ＋１を満足する素数(ｐｒｉｍｅ　ｎｕｍｂｅｒ)。

【００３３】
また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記初期配分ステップで、次の[数２]によってグループキーK_gを累乗して中間キーIK_iを計算して、次の[数３]によって累乗されたグループキー(または中間キー)IK_iを逆累乗してグループキーK_gを計算することを特徴とする。
【００３４】
【数２】

$$IK_i=(K_g)^{g^{r_0 r_i}} \bmod p$$

【００３５】
【数３】

$$K_g=K_g^{g^{r_0 r_i}/g^{r_0 r_i}} \bmod p$$

【００３６】
また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキー管理方法において、前記グループキーはツリー構造で生成するが、前記ツリー構造は前記マスター端末に対応するルートノードから前記サブ端末に対応する中間ノードまでｎ次ツリーで構成し、中間ノードの子ノードを２進ツリーで構成するが、前記２進ツリーの葉ノードは前記中間ノードのサブ端末に連結される遠隔端末に対応して生成されることを特徴とする。
【００３７】
また、本発明は、マスター端末(ＭＴＵ)、多数のサブ端末(ＳＵＢ－ＭＴＵ)及び多数の遠隔端末(ＲＴＵ)が順次的な階層で構成される強力なＳＣＡＤＡシステムのハイブリッドキーを利用したセッションキー生成方法において、前記マスター端末はグループキーをツリー構造で生成するステップと、前記マスター端末は各サブ端末または各遠隔端末で前記グループキーを配分するが、前記サブ端末または各遠隔端末は自分に対応するノードの下位ノード及び上位ノードのグループキーの配分を受けて保存するステップと、前記マスター端末は前記ツリー構造のノードを選択し、選択したノードの下位ノードに対応するサブ端末または遠隔端末と通信するためのセッションキーを前記選択したノードのグループキーで生成するステップと、を含み、前記配分ステップで、前記マスター端末と各サブ端末は自分の秘密数を生成して電子署名して交換し、前記グループキーは前記秘密数により暗号化及び復号化されて配分されることを特徴とする。
【００３８】
また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキーを利用したセッション

キー生成方法において、前記ツリー構造は、前記マスター端末に対応するルートノードから前記サブ端末に対応する中間ノードまでｎ次ツリーで構成し、中間ノードの子ノードを２進ツリーで構成するが、前記２進ツリーの葉ノードは前記中間ノードのサブ端末に連結される遠隔端末に対応して生成されることを特徴とする。

【００３９】

また、本発明は、強力なＳＣＡＤＡシステムのハイブリッドキーを利用したセッションキー生成方法において、前記セッションキーは、前記グループキーと、タイムスタンプ及びシーケンス番号が結合された値をハッシュして生成することを特徴とする。

【発明の効果】

【００４０】

上述のように、本発明による強力なＳＣＡＤＡシステムのハイブリッドキー管理方法及びセッションキー生成方法によれば、マスター端末とサブ端末との間には公開キー基盤の暗号化を適用し、サブ端末と遠隔端末との間には高い効率性を有する対称キー基盤の暗号化を適用することで、有効であるとともにマスター端末に保存するキーの数を減らす代替プロトコルをサポートできる効果が得られる。

【図面の簡単な説明】

【００４１】

【図１】本発明を実施するためのＳＣＡＤＡシステムの全体構成を示した図である。

【図２】本発明の一実施の形態によるＳＣＡＤＡシステム構造の一例を示した図である。

【図３】本発明の一実施の形態によるＳＣＡＤＡシステムのハイブリッドキー管理方法を説明したフローチャートである。

【図４】本発明の一実施の形態によって生成したグループキーのツリー構造を例示した図である。

【図５】（Ａ）～（Ｂ）は、本発明の一実施の形態による追加プロトコルを例示した図である。

【図６】本発明の一実施の形態による脱退プロトコルを例示した図である。

【図７】本発明の一実施の形態による代替プロトコルを例示した図である。

【図８】（Ａ）～（Ｂ）は、本発明の一実施の形態による総遅延時間を例示した図である。

【図９】（Ａ）～（Ｃ）は、本発明の一実施の形態によるマスター端末に保存されるキーの数を比較、または総計算時間を比較する図である。

【発明を実施するための形態】

【００４２】

以下、添付図面を参照して本発明の望ましい実施の形態について詳細に説明する。

【００４３】

また、本発明の説明において同一部分には同一符号を付けて、その反復説明は省略する。

【００４４】

まず、本発明を実施するためのＳＣＡＤＡシステムの全体構成の一例について図１を参照して説明する。

【００４５】

図１に示したように、本発明を実施するためのＳＣＡＤＡシステムは、管理者端末(ＨＭＩ：Ｈｕｍａｎ－Ｍａｃｈｉｎｅ Ｉｎｔｅｒｆａｃｅ)１０、マスター端末(ＭＴＵ：Ｍａｓｔｅｒ Ｔｅｒｍｉｎａｌ Ｕｎｉｔ)２１、サブ端末(ＳＵＢ－ＭＴＵ：ＳＵＢ Ｍａｓｔｅｒ Ｔｅｒｍｉｎａｌ Ｕｎｉｔ)２２、遠隔端末(ＲＴＵ：Ｒｅｍｏｔｅ Ｔｅｒｍｉｎａｌ Ｕｎｉｔ)２３で構成される。特に、マスター端末２１、サブ端末２２、遠隔端末２３は順次的な階層構造を有する。

【００４６】

管理者端末１０は基盤施設のプロセスデータを管理者に表示する装置として、管理者がこれを通じて基盤施設をモニタリングして制御する端末装置である。そのために、管理者

端末１０はコンピュータ機能を有した端末装置で構成される。

【００４７】

遠隔端末２３は基盤施設に直接設置されてプロセスデータを収集して伝送するか制御命令によって実行する端末装置である。一般的に、ＳＣＡＤＡシステムに適用される基盤施設は地域的に広く分布されているので、遠隔端末２３も地域的に散在されている。

【００４８】

サブ端末２２は特定の遠隔端末２３と通信してこれらを制御する。マスター端末２１は全体的にプロセスデータを収集して制御する装置である。すなわち、マスター端末２１はサブ端末２２を制御してサブ端末２２を介して遠隔端末２３をモニタリングして制御する。

【００４９】

マスター端末２１、サブ端末２２、遠隔端末２３がお互いに暗号化された通信を実行するためにはセッションキーを利用する。すなわち、送信する端末と受信する端末の間でセッションキーを生成してお互いに分ける。そして、送信端末は伝送しようとするメッセージをセッションキーで暗号化して伝送し、受信端末は暗号化されたメッセージを受信してセッションキーで復号化する。

【００５０】

セッションキーはメッセージを送受信する特定セッションでだけ利用するキーとして、セッションを異にすると相違して生成される。セッションキーが露出されても他のセッションは安全である。しかし、セッションキーは各端末の間で共有しているキーを利用して生成される。すなわち、セッションキーは端末の間で共有しているキーとタイムスタンプをハッシュして生成される。したがって、安全な通信のためには何よりキーの管理が重要である。

【００５１】

本発明の強力なＳＣＡＤＡシステムのためのハイブリッドキー管理方法は、マスター端末２１により全体的に二つの階層で管理される。すなわち、本発明の一実施の形態によると、マスター端末２１がグループキーを生成してこれをサブ端末２２に伝達する。マスター端末２１が全体の共有キーを主体的に管理する。

【００５２】

一方、ＳＣＡＤＡシステムでサブ端末２２が削除されるか追加されると、キーの保護のために前記サブ端末２２と共有したキーを全部更新しなければならない。したがって、マスター端末２１は前記キーを更新して、これをサブ端末２２に伝達する。

【００５３】

次に、本発明によるＳＣＡＤＡシステムのハイブリッドキー管理方法を説明するための表記方式及びシステム構造について図２を参照して説明する。

【００５４】

以下で、次の表記が使用される。
・ｍ：サブ端末(ｓｕｂ－ＭＴＵ)の数
・ｒ：サブ端末(ｓｕｂ－ＭＴＵ)当たりＲＴＵの最大数
・ＧＭ：非空(ｎｏｎｅｍｐｔｙ)集合のノード。この集合は２個のＭＴとＲＴの互いに素な部分集合(ｄｉｓｊｏｉｎｔ　ｓｕｂｓｅｔｓ)に分けられる。すなわち、ＧＭ＝ＭＴ∪ＲＴ
・ＲＴ：$RT=\{TR_1, \ldots, RT_{m\cdot r}\}$はＲＴＵの集合である。
・ＭＴ：$MT=\{MT_0, \ldots, MT_m\}$はＭＴＵまたはｓｕｂ－ＭＴＵの非空集合である。
・ｇ：位数ｑのサブグループの発生器
・ｐ：小さなｋ∈Ｎに対してｐ＝ｋｑ＋１になるようにする素数
・ｑ：代数グループの位数
・r_i：MT_iのランダム数$r_i \in Z_q$
・IK_i：MT_iの中間キー
・K_{ij}^{k}：２進ツリーでのレベル(深さ)ｉのMT_kのｊ番目のキー

【００５５】
図２に示したように、ＣＫＤプロトコル、Ｉｏｕｌｕｓフレームワーク及び論理キー構造を実行する。本発明によるプロトコルはＭＴ部分５０とＲＴ部分６０の二つの部分を有する。ＭＴ部分５０はＣＫＤプロトコルによりグループキーを作り、ＲＴ部分６０は論理キー階層構造で構成される。
【００５６】
図２のように、各RT_iは葉ノードから中間ノードへのキーが知っている。各MT_i($i \neq 0$)は葉ノードからルートノードへの経路上にあるすべてのキーを知っている。ＭＴ部分５０とＲＴ部分６０はＩｏｌｕｓフレームワークを通じて連結される。MT_0(ＭＴＵ)はＧＳＣ(Ｇｒｏｕｐ　Ｓｅｃｕｒｉｔｙ　Ｃｏｎｔｒｏｌｌｅｒ)の役目を実行する。したがって、MT_0は全体グループとMT_0とMT_i($1 \leqq i \leqq m$)との間のグループキーを管理する。MT_i($1 \leqq i \leqq m$)はＧＳＩ(Ｇｒｏｕｐ　Ｓｅｃｕｒｉｔｙ　Ｉｎｔｅｒｍｅｄｉａｒｙ)としての役目を実行し、ｒ個のＲＴで構成されるその部分集合のサブグループキーを管理する。ＲＴ部分６０の構造及びＲＴ部分６０とＭＴ部分５０の連結関係はＡＳＫＭＡ＋プロトコルでの関係と同一である。
【００５７】
次に、本発明の一実施の形態によるＳＣＡＤＡシステムのハイブリッドキー管理方法について図３～図６を参照して説明する。
【００５８】
本発明の一実施の形態によるキー管理方法は、初期化ステップ(ステップＳ１０)、サブ端末２２が追加されるか削除される時のキーの更新ステップ(ステップＳ２０)、及びサブ端末２２またはマスター端末２１が予備装備に交替される時のキーの更新ステップ(ステップＳ３０)に分けられる。
【００５９】
まず、前記マスター端末２１はキーのツリー構造を生成する(ステップＳ１０)。図４に示したように、ツリー構造のルートノード３１はマスター端末２１に対応する。また、中間ノード３２はサブ端末２２に対応し、葉ノード３４は遠隔端末２３に対応する。
【００６０】
一方、ルートノード３１と中間ノード３２の間はｎ次ツリーで構成される。
【００６１】
また、中間ノード３２と葉ノード３４の間は２進ツリー構造で構成される。中間ノード３２と葉ノード３４の間のノードを“一般ノード３３”と称する。
【００６２】
前記ツリー構造においてグループキーを生成する方法の一例は、次のようである。
【００６３】

まず、マスター端末２１はランダムな数r_0を選択して、$g^{r_0} \bmod p$を計算した後、そこに電子署名してサブ端末２２に伝送する。前記メッセージの伝送を受けたサブ端末２２は、電子署名値の有効性をチェックした後、有効であれば、ランダムな数r_iを選択して、$g^{r_i} \bmod p$を計算した後、電子署名してマスター端末２１に伝送する。ここで、ｉはサブ端末２２のインデックス番号であり、r_iは$r_i \in Z_q$を満足するランダムな数である。ここで、ｑは代数群(algebraic group)の位数であり、ｐは小さな量の定数ｋがある時、ｐ＝ｋｑ＋１を満足する素数である。

【００６４】

次に、多数のサブ端末２２とマスター端末２１は、$g^{r_i r_0} \bmod p$（ｉ∈[ｉ、ｍ]）を計算する。ここで、ｍはサブ端末２２の数を示す。

【００６５】

次に、マスター端末２１は電子署名値の有効性を検査し、もし、有効であれば、グループキーK_gをランダムに選択して、$IK_i=(K_g)^{g^{r_i r_0}} \bmod p$（ｉ∈[ｉ、ｍ]）を計算した後、該当値に電子署名する。マスター端末２１とサブ端末２２は今までの過程を事前に予め計算しておくことができる。

【００６６】

次に、マスター端末２１がIK_i（ｉ∈[ｉ、ｍ]）を電子署名してサブ端末２２に伝送する。サブ端末２２は伝送を受けた値を$K_g=K_g^{g^{r_i r_0}/g^{r_i r_0}} \bmod p$（ｉ∈[ｉ、ｍ]）で 計算してグループキー$K_g$を得る。

【００６７】

次に、前記ツリー構造でサブ端末２２が削除されるか追加される時のキーの更新ステップ(ステップＳ２０)の具体的な方法は、次のようである。

【００６８】

ｍ個のサブ端末２２が存在するグループにｍ＋１番目のサブ端末２２が新たに加入する方法は、次のようである。

【００６９】

まず、マスター端末２１が初期化ステップ(ステップＳ１０)で生成した$g^{r_0} \bmod p$の値に電子署名した後、新たに加入するサブ端末２２に伝送する。前記メッセージの伝送を受けたサブ端末２２は電子署名値の有効性をチェックし、有効であれば、ランダムな数r_{m+1}を選択して、$g^{r_{m+1}} \bmod p$を計算した後、電子署名してマスター端末２１に伝送する。ここで、ｍ＋１は新たに加入するサブ端末２２のインデックス番号である。

【００７０】

次に、新たに加入するサブ端末２２とマスター端末２１は、$g^{r_i r_{m+1}} \bmod p$を計算する。

【００７１】

次に、マスター端末２１は電子署名値の有効性を検査し、もし、有効であれば、新しいグループキーK'_gをランダムに選択して、$IK'_i=(K'_g)^{g^{r_i r_{m+1}}} \bmod p$（ｉ∈[ｉ、ｍ]）を計算した後、該当値に電子署名する。

【００７２】

次に、マスター端末２１がIK'_i(ｉ∈[ｉ、m])を電子署名して既存のサブ端末２２と新たに加入したサブ端末２２に伝送する。サブ端末２２は伝送を受けた値を$K'_g=K'^{g''_i/g''}_g \bmod p$(ｉ∈[ｉ,m])で計算してグループキーK`$_g$を得る。

【００７３】

原則的に、ランダム値ｒ$_i$は毎回アップデートする必要があるが、ＳＳＬの“ｓｅｓｓｉｏｎ ｃａｃｈｅ ｍｏｄｅ”ように効率性のためにｒ$_i$値を反復使用する。もちろん、特定の周期で該当値はアップデートされる。

【００７４】

本発明の初期化プロトコルはｒ$_i$Ｓをさらに利用するが、ＩＫ´を計算するために指数(ｅｘｐｏｎｅｎｔｉａｌｓ)を使用するので、各グループ構成員は他のグループ構成員のｇ^{r_0r_i}がわからない。これは追加(ｊｏｉｎまたは加入)プロトコルだけではなく脱退(ｌｅａｖｅ)及び代替(ｒｅｐｌａｃｅ)プロトコルにも適用できる。

【００７５】

図５は、上述のような加入プロトコルの簡単な図示的な例を示す。新しいｓｕｂ－ＭＴＵはＭＴ$_5$であり、ｍ＝４である。本例の詳細な説明は次のようである。

【００７６】

・ステップ１：MT$_0$がデジタル署名を利用して初期化ステップで発生した$g^{r_0} \bmod p$を新しい装置MT$_5$に伝送する。

・ステップ２：新しい装置MT$_5$は電子署名の有効性を確認した後、ランダムな数ｒ$_5$を選択して、$g^{r_5} \bmod p$を計算した後、これを電子署名を利用してMT$_0$に伝送する。

・ステップ３：新しい装置MT$_5$とMT$_0$は$g^{r_0r_5} \bmod p$を計算する。

・ステップ４：MT$_0$は電子署名の有効性を確認した後、ランダム数であるグループキーK´$_g$を発生させて、$IK_i' = (K'_g)^{g^{r_i}} \bmod p$(ｉ∈[１、５])を計算して、これを署名する。

・ステップ５：MT$_0$は電子署名を利用してＩＫ$_i$´(ｉ∈[１、５])をMT$_i$に再伝送する。

・ステップ６：メッセージを受信すれば、各構成員MT$_i$(ｉ∈[１、５])は、$K'_g = K_x^{g^{r_0r_i}} \bmod p$を計算する。

【００７７】

次に、ｍ個のサブ端末２２があるグループでｊ番目のサブ端末２２が脱退する場合のキーをアップデートする方法は、次のようである。

【００７８】

まず、マスター端末２１が新しいグループキー K`$_g$をランダムに選択して、

$IK'_i=(K'_g)^{g''} \bmod p$(ｉ≠ｊ ａｎｄ ｉ∈[ｉ、m])を計算した後、該当値に電子署名する。

【００７９】

次に、マスター端末２１がＩＫ´$_i$を電子署名して、脱退するサブ端末２２を除いて残りのサブ端末２２に伝送する。サブ端末２２は伝送を受けた値を$K'_g=K'^{g''_i/g''_j}_g \bmod p$(ｉ≠ｊ ａｎｄ ｉ∈[ｉ、m])で計算してグループキー K`$_g$を得る。

【００８０】

図６は、上述のような脱退(または削除)プロトコルの単純な図示的な例を示す。脱退するｓｕｂ－ＭＴＵはＭＴ$_4$であり、ｍ＝４である。前記例の詳細な説明は次のようである。

【００８１】

・ステップ１：MT_0が新しいグループキー $K`_g$を発生させて、 $IK_i' = (K'_g)^{g^{r''}} \bmod p$（i∈[1、3]、i≠j)を計算して、これを署名する。
・ステップ２：電子署名を利用してMT_0がIK_i'（i∈[1、3]、i≠j)をMT_iに伝送する。
・ステップ３：メッセージを受ければ、各構成員 MT_i（i∈[1、3]、i≠j)は、$K'_g = (K'_g)^{g^{r_i r''}} \bmod p$を計算する。

【００８２】
ＲＴＵ脱退プロトコルはＡＳＫＭＡ＋プロトコルと同一の手続きを実行する。
【００８３】
次に、サブ端末２２またはマスター端末２１が予備装備に切り替える時のキーの更新ステップ(ステップ３０)に関して説明する。
【００８４】
有用性を支持するために予備装備に取り替える代替プロトコルを提供する。ＳＣＡＤＡシステムの一部装置に故障が発生すると、この装置は予備装置に交替しなければならない。この場合に、脱退(leave)プロトコルと加入(join)プロトコルが同時に実行される。したがって、代替(replace)プロトコルは脱退及び加入プロトコルの組合せ体である。
【００８５】
もし、ｓｕｂ－ＭＴＵ装置MT_nに故障が発生すると、MT_nは予備装備ｓｕｂ－ＭＴＵ装置にスイッチングされる。ｉ＝ｎであるサブ端末２２が予備装備に交替される時のキー更新方法は次のようである。
【００８６】
まず、マスター端末２１が新しいグループキー $K`_g$をランダムに選択して、$IK'_i=(K'_g)^{g^{r'_i}} \bmod p$（i≠j and i∈[i、m])を計算した後、該当値に電子署名する。
【００８７】
次に、マスター端末２１がIK'_iを電子署名して交替されるサブ端末２２を除いて残りのサブ端末２２に伝送する。サブ端末２２は伝送を受けた値を$K'_g=K'^{g^{r'_i}g^{r''}}_g \bmod p$（i≠j and i∈[i、m])で計算してグループキー K'_gを得る。
【００８８】
次に、マスター端末２１がg'°ｍｏｄ ｐ値に電子署名した後、交替される予備サブ端末２２に伝送する。前記メッセージの伝送を受けた予備サブ端末２２は電子署名値の有効性をチェックし、有効であれば、新しいランダムな数$r`_n$を選択して、$g^{r'_n} \bmod p$を計算した後、電子署名してマスター端末２１に伝送する。
【００８９】
次に、交替された予備サブ端末２２とマスター端末２１は、$g^{r'_n r''} \bmod p$を計算する。
【００９０】
次に、マスター端末２１は電子署名値の有効性を検査し、もし、有効であれば、$IK'_n=(K'_g)^{g^{r'_n}} \bmod p$を計算した後、該当値に電子署名する。
【００９１】
次に、マスター端末２１がIK'_nを電子署名して既存のサブ端末２２と新たに交替されたサブ端末２２に伝送する。サブ端末２２は伝送を受けた値を$K'_g=K'^{g^{r'_n}g^{r''}}_g \bmod p$で計算してグループキー$K`_g$を得る。
【００９２】

もし、マスター端末２１が交替されると、初期化ステップ(ステップＳ１０)を再実行するようになる。

【００９３】

図７は、代替プロトコルの簡単な図示的な例を示す。故障が発生した装置はＭＴ４であり、ｍ＝４である。本例の詳細な説明は次のようである。

【００９４】

・ステップ１：MT_0が新しいグループキー$K`_g$を発生させて、$IK'_i = (K'_g)^{g^{mi}} \bmod p$(ｉ∈[１、３])を計算して、これを署名する。

・ステップ２：電子署名を利用してMT_0がIK'_i(ｉ∈[１、３])をMT_iに伝送する。

・ステップ３：メッセージを受ければ、各構成員MT_i(ｉ∈[１、３])は$K'_g = (K'_g)^{g^{r'_i}} \bmod p$を計算する。

・ステップ４：MT_0は電子署名を利用して前記予備ｓｕｂ－ＭＴＵ MT_4'に$g^{r'_0} \bmod p$を伝送する。

・ステップ５：MT_4'は電子署名の有効性を確認して、新しいランダムな数r_4'を選択して、$g^{r'_4} \bmod p$を計算し、これを電子署名を利用してMT_0に伝送する。

・ステップ６：MT_4'とMT_0は$g^{r'_0 r'_4} \bmod p$を計算する。

・ステップ７：MT_0は電子署名の有効性を確認して、ランダム数であるグループキーK_g'を発生させて、$IK_i' = (K_g)^{g^{mi}} \bmod p$を計算し、これを署名する。

・ステップ８：MT_0は電子署名を利用してIK_4'をMT_4'に伝送する。

・ステップ９：メッセージを受信すれば、MT_4'は$K_g' = (K'_g)^{g^{mi} r'_i} \bmod p$を計算する。

【００９５】

次に、本発明によるセッションキー生成方法について説明する。

【００９６】

サブセッションでは、ユニキャスト、ブロードキャスト及びマルチキャスト用のデータ暗号化アルゴリズムを提供する。セッションキーの更新のために、ＴＶＰ(ｔｉｍｅ ｖａｒｉａｎｔ ｐａｒａｍｅｔｅｒ)が使用される。ＴＶＰはタイムスタンプとシーケンスナンバーの組合せである。

【００９７】

すなわち、セッションキーは通信しようとする端末間で共有しているキーを利用して生成する。したがって、キーの生成、保存、更新は上述の方法に従う。

【００９８】

ユニキャストに使用されるセッションキーの場合、次のような式を通じて生成される。

【００９９】

【数４】

$$SK_U = H(K^k_{h,j}, TVP)$$

【０１００】

ここで、$K^k_{h,j}$は高さがｈであるツリーの葉ノードのキーである。ＴＶＰは時間変数を示す。データはセッションキーSK_Uを利用して暗号化される。

【０１０１】

ブロードキャストとマルチキャストでは、データ暗号化のためのセッションキーが各構成員により共有情報を利用して発生される。ブロードキャスティングやマルチキャスティングに使用されるセッションキーの場合、次のような式を通じて生成される。

【０１０２】

【数５】

$$SK_B = H(K_g, TVP)$$

【０１０３】

ここで、K_gはグループメンバーの間で共有されるキーである。すなわち、前記キーK_gはすべてのグループ構成員または前記グループの一部構成員の間で共有されるキーである。したがって、前記構造３０のキーを通じて暗号化セッションを設定することができる。

【０１０４】

次に、本発明によるＲＴＵのキーをアップデートする期間(周期)について説明する。

【０１０５】

一般的に、ＲＴＵは遠隔地に位置するので、物理的に不安全である。したがって、前記ＲＴＵは保存されたキーを周期的にアップデートする必要がある。そのようなキーをアップデートする時間間隔がとても短ければ、ＳＣＡＤＡ通信において時間遅延を増加させる。したがって、通信効率と保安を満足させるキーをアップデートする適切な期間を求めなければならない。したがって、前記期間を求めるために[数６]のようにＱｏＳ関数を定義する。

【０１０６】

【数６】

ＱｏＳ＝ＣＩ＋ＳＩ

ＣＩとＳＩは通信インデックスと保安インデックスを示す。ＣＩはＲＴＵのキーをアップデートするために発生する遅延時間を基盤で計算される。ＴをＳＣＡＤＡシステムでの通信期間とし、δをキーをアップデートすることにより発生する遅延時間であると仮定すれば、ＣＩは次の[数７]のように計算される。

【０１０７】

【数７】

$$CI = \frac{T-\delta}{T}$$

【０１０８】

キーをアップデートするための期間はδに反比例するので、上の式は次のように変更できる。

【０１０９】

【数８】

$$CI = \frac{T-\delta}{T} = \frac{T-k/t_p}{T}$$

ここで、ｋは定数であり、t_pは現在と次のキーをアップデートする間の時間である。

【０１１０】

ＳＩはＲＴＵに対する成功的な攻撃の可能性により計算される。前記ＲＴＵに対する成功的な攻撃が実生活において独立的なイベントで認識されると、前記イベントを示すため

にプアソン(Ｐｏｉｓｓｏｎ)過程が採用できる。
【０１１１】
【数９】

$$\frac{(\lambda t)^n}{n!},n=0,1,\ldots$$

ここで、ｎは時間(＝ｔ)の間のイベントの数であり、λはＲＴＵに対する成功的な攻撃の数の平均である。本発明の保安目標は、現在及び次のキーをアップデートする間にＲＴＵに対する成功的な攻撃が発生しないようにすることである。したがって、ｎ＝０、ｔ＝t_pに対して次の式が得られる。
【０１１２】
【数１０】

$$SI=e^{-\lambda t_p}$$

プアソン(poisson)過程で、λはＳＣＡＤＡネットワークに対するすべての可能な攻撃の数の平均を示す。しかし、ＲＴＵのキーに攻撃対象が限定されることがある。この時、攻撃理由はＲＴＵのキーをアップデートするためのスキームの論理エラーまたは実行エラーに分けられる。論理エラーにより発生する攻撃の例は順方向保安、逆方向保安などである。実行エラーにより発生する攻撃はＲＴＵに対する侵略的攻撃(ｉｎｖａｓｉｖｅ ａｔｔａｃｋｓ)と非侵略的攻撃(ｎｏｎ－ｉｎｖａｓｉｖｅ ａｔｔａｃｋｓ)に分けられる。ＲＴＵに対する侵略的攻撃の例は前記ＲＴＵのハードウェアモジュールの逆エンジニアリング(ｒｅｖｅｒｓｅ ｅｎｇｉｎｅｅｒｉｎｇ)である。ＲＴＵに対する非侵略的攻撃の例はサイドチャンネル攻撃またはＲＴＵにおけるソフトウェアの逆エンジニアリングである。
【０１１３】
ＳＩは、次のように再計算される。
【０１１４】
【数１１】

$$SI=e^{-(\lambda_l+\lambda_i+\lambda_{ni})t_p}$$

ここで、λ_lは論理エラーにより発生する成功的な攻撃の数の平均であり、λ_iは成功的な侵略的攻撃の数の平均であり、λ_{ni}は実行エラーにより発生する成功的な非侵略的攻撃の数の平均である。しかし、本発明は保安分析によって論理エラーを有する。したがって、本発明のλ_lを０で指定することができる。
【０１１５】
最終的に、ＱｏＳ関数はt_pにより表現できる。
【０１１６】

【数１２】

$$QoS=\frac{T-k/t_p}{T}+e^{-(\lambda_l+\lambda_i+\lambda_{mi})t_p}$$

前記ＱｏＳ関数を最大化するために、前記ＱｏＳ関数の微分はｔ$_p$で０になる必要がある。

【０１１７】

【数１３】

$$\frac{dQoS(t_p)}{dt_p}=\frac{k}{Tt_p^2}-\lambda_l+\lambda_i+\lambda_{mi}e^{-(\lambda_l+\lambda_i+\lambda_{mi})t_p}$$

【０１１８】

したがって、前記ＲＴＵのキーをアップデートするための最適の期間が得られる。

【０１１９】

次に、本発明によって発生する効果をより具体的に説明する。

【０１２０】

本発明の費用について評価と分析を行う。関心分野は２個の分野である。(１)通信遅延時間は０.５４０秒未満とする。(２)ＭＴＵに保存されるキーの数は以前の技術でのキーの数より少ない必要がある。分析環境は次のように仮定する。

・ ＭＴの数：３３
・ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ因子(ｐ)のサイズ：１０２４ｂｉｔ
・ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ因子(ｑ)のサイズ：１６０ｂｉｔ
・ 累乗ランタイム：０.００００８秒
・ ＲＳＡ－１０２４サイニングランタイム：０.００１４８秒
・ ＲＳＡ－１０２４検証ランタイム：０.０００００７秒
・ ＡＥＳ－１２８/ＣＢＣランタイム：０.００００００９秒
・ 署名アルゴリズム：ＲＳＡ １０２４署名
・ 認証書フォーマット：Ｘ.５０９ｖ３

【０１２１】

Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ因子(ｐ、ｑ)を選択して、ランタイムのためにＣｒｙｐｔｏ＋＋５.６.０Ｂｅｎｃｈｍａｒｋｓを参照した。ＲＳＡとＸ.５０９が最も一般的に使用される公開キー暗号化システム及び認証フォーマットなので、これらを選択した。

【０１２２】

一般的に、ＳＣＡＤＡシステムのメッセージサイズは１０００ｂｉｔ未満である。したがって、メッセージ暗号化/復号時間は０.０００００１８秒である。グループキー設定ステップが１累乗動作及び１検証動作を具備するため、グループキー設定時間は０.０００１５秒である。したがって、このような数値と伝送時間の総和が総遅延時間である。

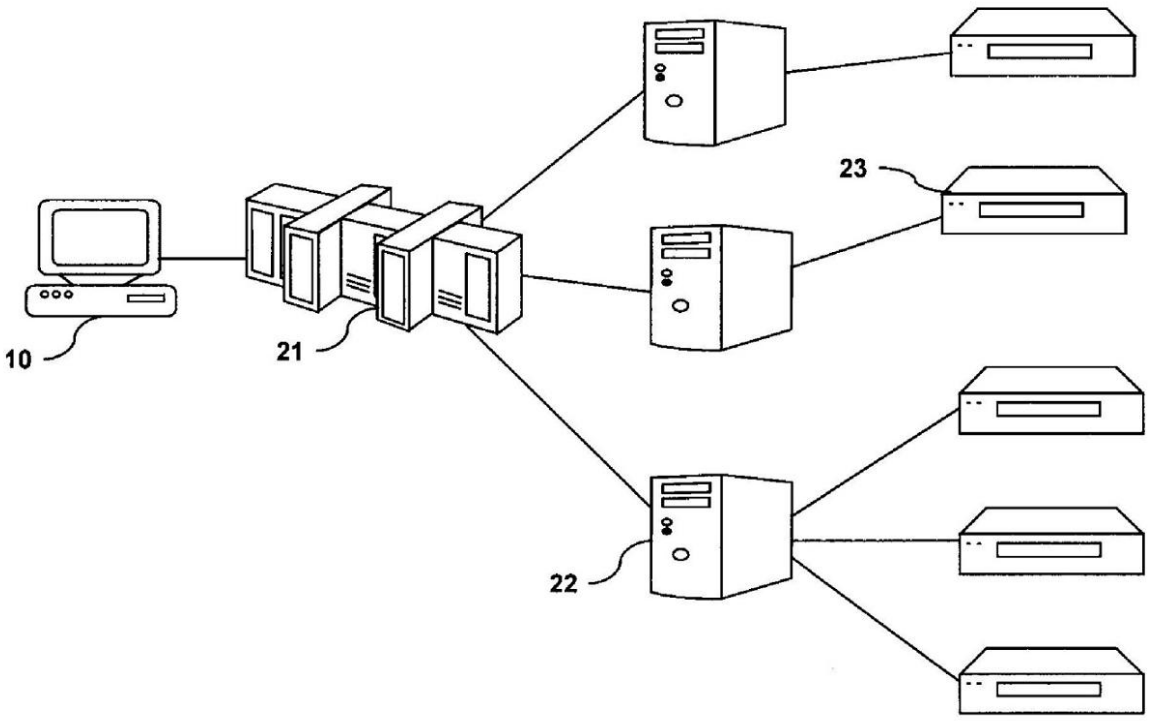
【０１２３】

図８の(ａ）～(ｂ)は、本発明の一実施の形態による総遅延時間を示す。本発明の一例は総遅延時間が９６００伝送速度で０.３３３５０５秒なので、性能要件を満足した。

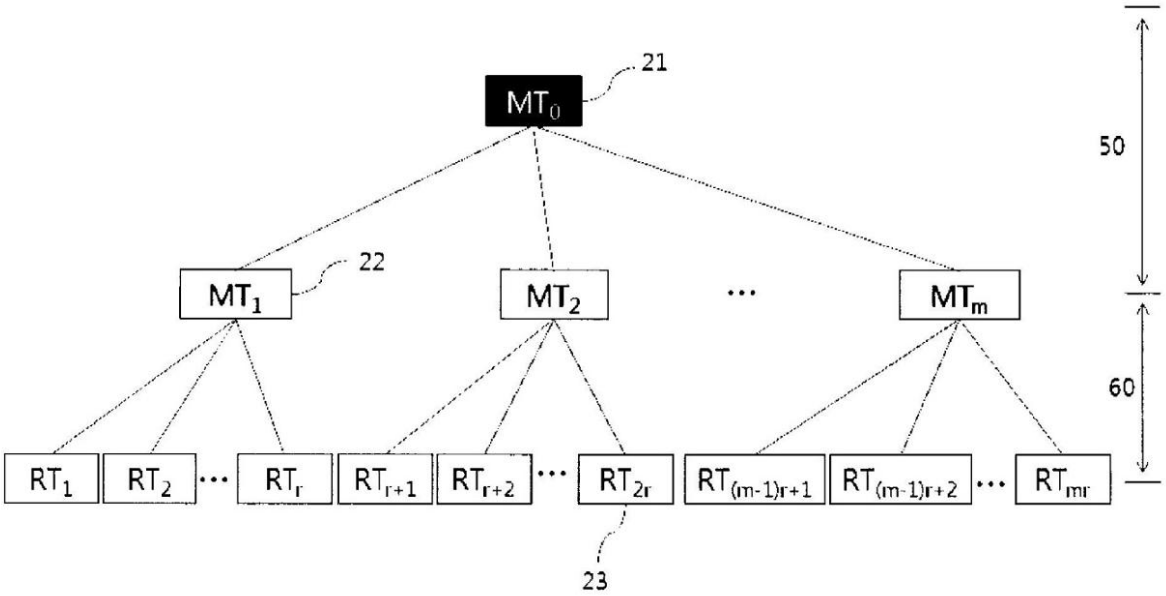
【０１２４】
本発明で、ＭＴＵに保存されたキーの数は他の技術でのキーの数より少ない。図９の(ａ)では、ＳＫＥ、ＳＫＭＡ、ＡＳＫＭＡ、ＡＳＫＭＡ+及び本発明のＭＴＵに保存されたキーの数を比較する。
【０１２５】
図９の(ｂ)は、ＭＴＵ(ｒ＝１２８)に保存されたキーの数を比較するグラフである。
【０１２６】
図９の(ｃ)は、５－ｋｂメッセージ(ｒ＝１２８、ｍ＝４)を有するマルチキャスト目標ノードの数に基盤した総計算時間を比較するグラフである。
【０１２７】
次に、本発明の保安分析(または効果)について説明する。
【０１２８】
１）グループキー保安：能動的攻撃者(Ｍａｌｌｏｒｙ)がグループキーを計算する難しさについて記述する。マロリーはグループ通信上のメッセージを見るか、挿入するか、除去するか、変更することができるが、グループ構成員ではなくて、本発明によるプロトコルがＤｅｃｉｓｉｏｎ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ仮定とＤｉｓｃｒｅｔｅ Ｌｏｇａｒｉｔｈｍ Ｐｒｏｂｌｅｍに依存するので、どのようなキーも知らない。マロリーはサイファテキストからグループキーとプレインテキストに関する情報を得られないので盲目的にサーチするしかない。
【０１２９】
２）順方向保安：マロリーが以前の期間中にグループ構成員であり、グループキーを知っていると仮定する。マロリーがグループを去る時、上述のようにキーをアップデートする。したがって、マロリーは新しいキーを計算するために盲目的にサーチをするしかない。
【０１３０】
３）逆方向保安：マロリーがグループに合流してグループキーを受ける時、そのキーには以前のキーで暗号化された以前のデータパケットが記録されているかもしれないが、本発明のプロトコルはマロリーがグループに合流する時新しいグループキーを使用するので、マロリーが以前のグループキーを得る可能性は無視すべき値とする。したがって、マロリーがキーをアップデートする可能性は無視すべき値として、盲目的なサーチを通じて以前のキーを得るしかない。
【０１３１】
４）キー更新：時間変化因子とキーをハッシュすることでセッションキーが得られる。暗号的に安全なハッシュ関数を使用するので、セッションキーは以前のキーと独立している。また、すべての暗号化キーは各セッション用の新たなキーに取り替えられる。したがって、本発明のプロトコルはキー更新を保障する。
【０１３２】
５）完全順方向保安：完全順方向保安は隣接した部分集合の以前のキーを知っている受動的攻撃者が次のグループキーを見つけることができないことを意味する。本発明は暗号化用で使用する長期秘密を有しないので、攻撃者が盲目的な攻撃を行うこと以外に次のグループキーを見つけることができない。
【０１３３】
６）有用性：本発明は代替プロトコルを支持する。前記代替プロトコルはメール装置に故障が発生する場合に動作し、ＳＣＡＤＡシステムが連続的に作動するようにしながらこれを予備(reverse)装置にスイッチングする。したがって、本発明は有用性を提案する。
【０１３４】
以上、本発明を具体的な実施形態を参照して詳細に説明したが、本発明の範囲は前述の実施形態によって限定されるべきではなく、特許請求の範囲の記載及びこれと均等なものの範囲内で様々な変形が可能なことは、当該技術分野における通常の知識を持つ者には明らかである。

【産業上の利用可能性】
【０１３５】
本発明は、多数の医療機関で使用する同一の意味の他の医療用語に対する概念格子を形成して、質疑用語を同一な意味の医療用語にマッピングする医療用語マッピングシステムの開発に適用することが可能である。
【０１３６】
特に、本発明は、質疑用語と関連された用語を用語ノードで表示される階層構造のグラフで構成して、質疑用語をルートノードとして各用語ノードに上位用語ノードの関連性を支持度で表示する医療用語マッピングシステムを開発することにおいて有用である。
【符号の説明】
【０１３７】
１０　ＨＭＩ端末
２１　マスター端末
２２　サブ端末
２３　遠隔端末
３０　ツリー構造
３１　ルートノード
３２　中間ノード
３３　一般ノード
３４　葉ノード

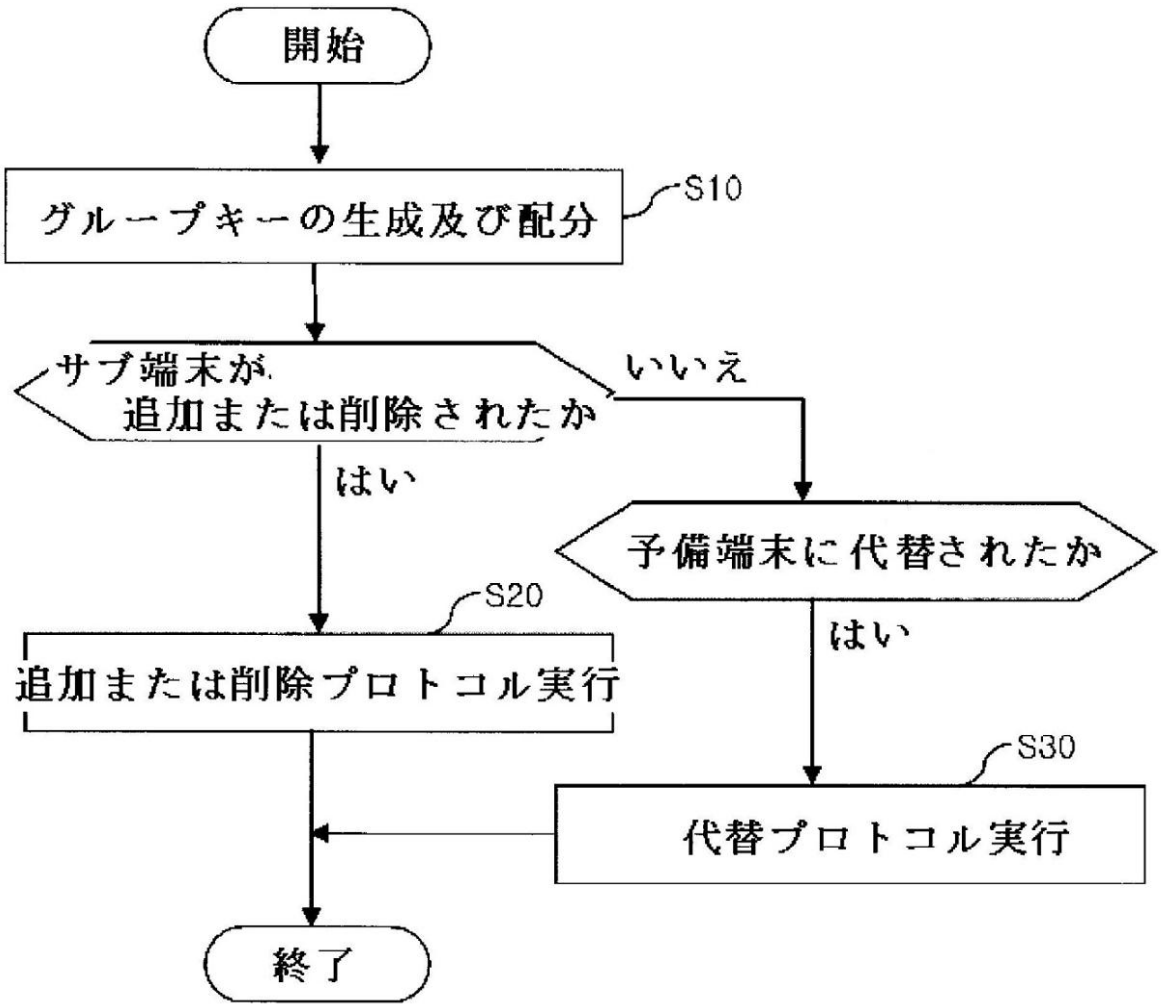
【図１】



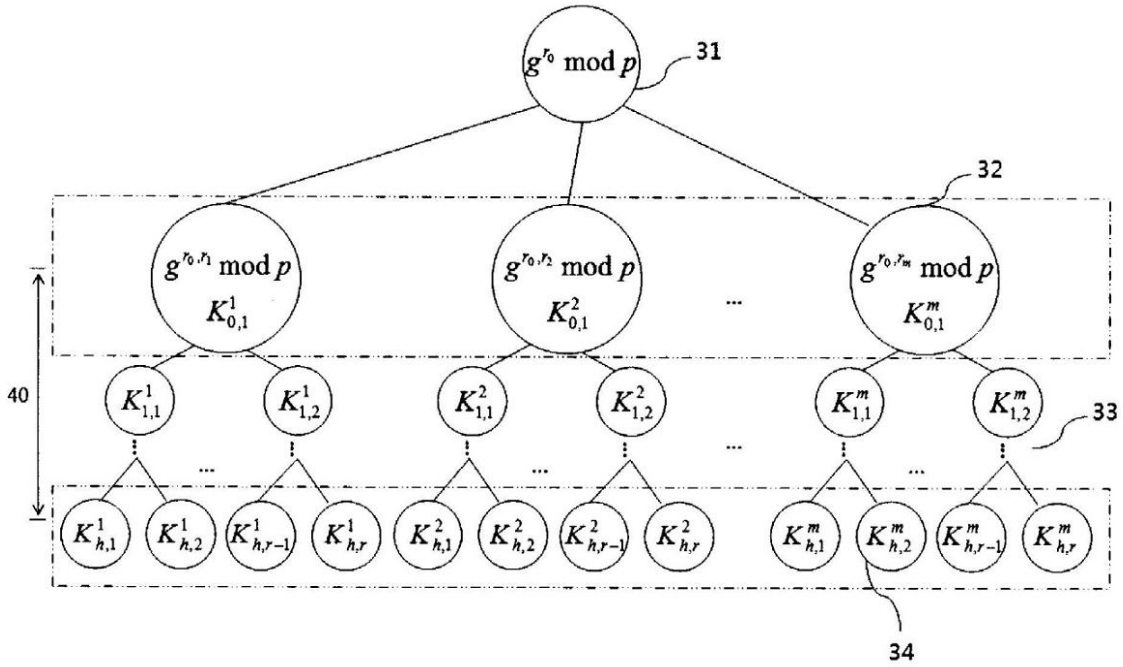
【図２】


MT0
21
50
MT1
22
MT2
…
MTm
60
RT1
RT2
…
RTr
RTr+1
RTr+2
…
RT2r
RT(m-1)r+1
RT(m-1)r+2
…
RTmr
23

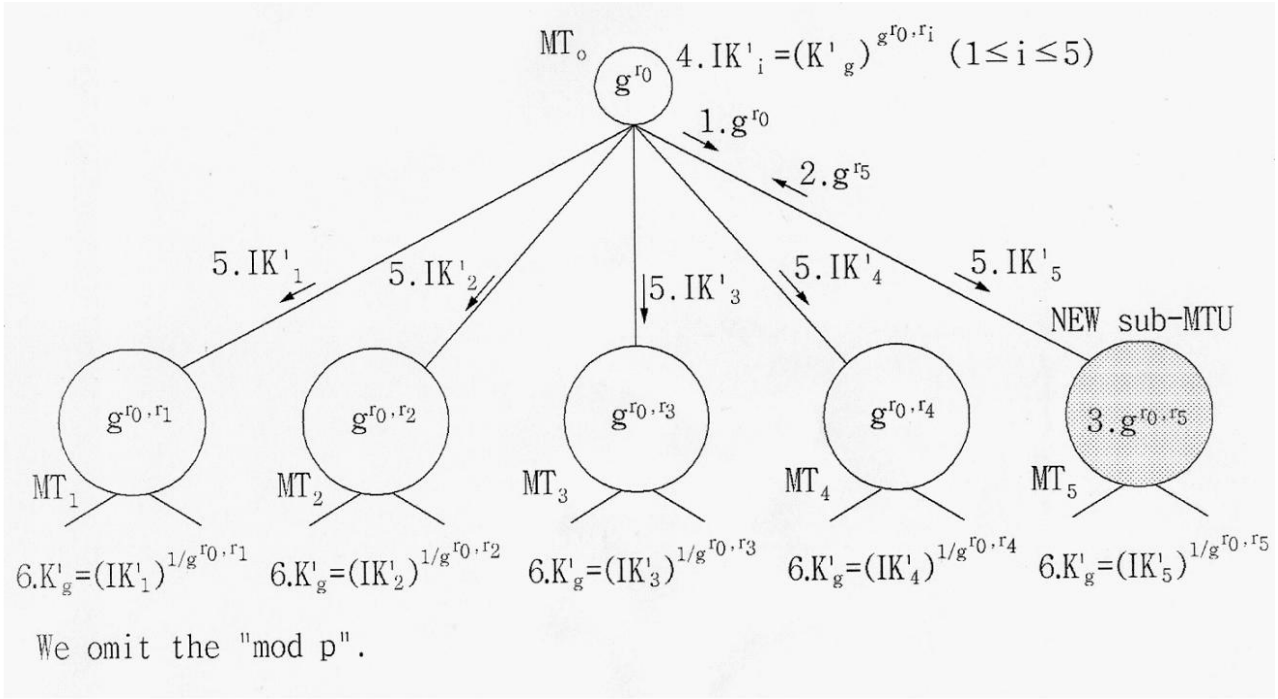
【図３】


開始
グループキーの生成及び配分
S10
サブ端末が
追加または削除されたか
いいえ
はい
予備端末に代替されたか
はい
S20
追加または削除プロトコル実行
S30
代替プロトコル実行
終了

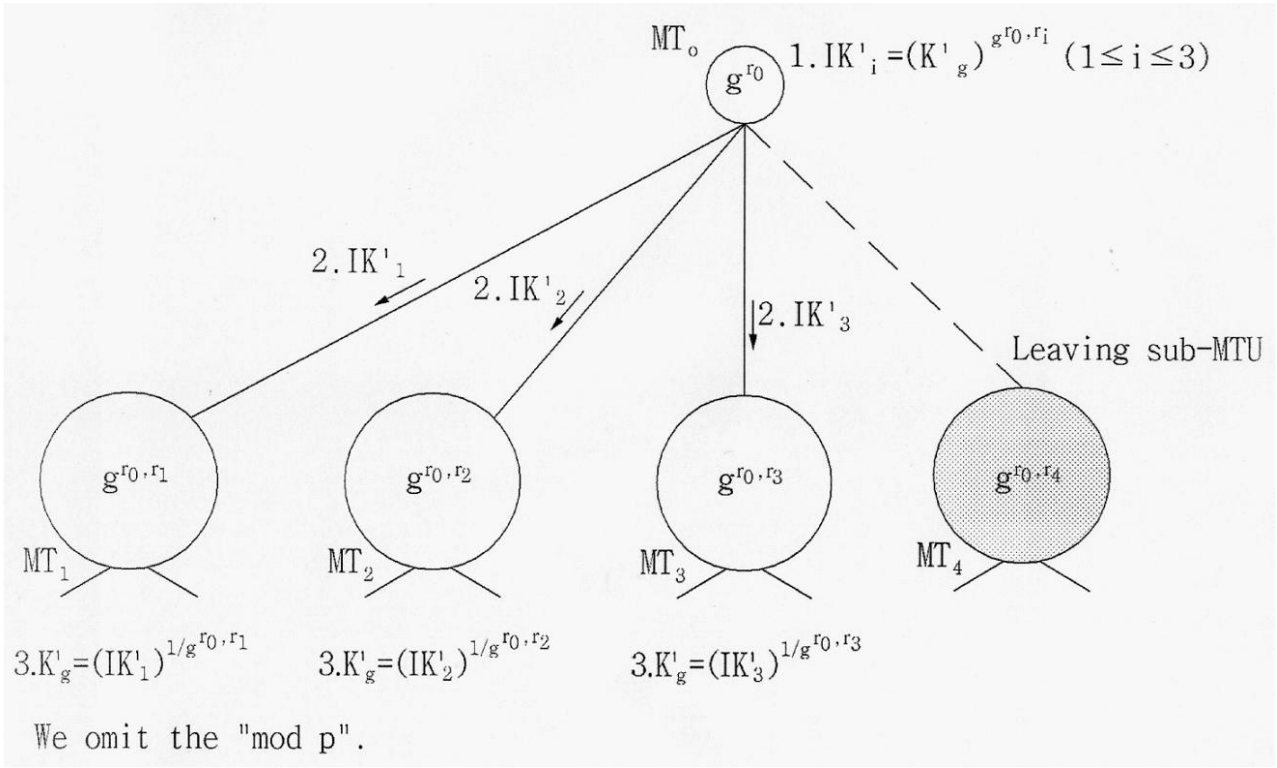
【図４】


$g^{r_0} \bmod p$
31
32
$g^{r_0,r_1} \bmod p$ $K^1_{0,1}$
$g^{r_0,r_2} \bmod p$ $K^2_{0,1}$
$g^{r_0,r_m} \bmod p$ $K^m_{0,1}$
40
33
34

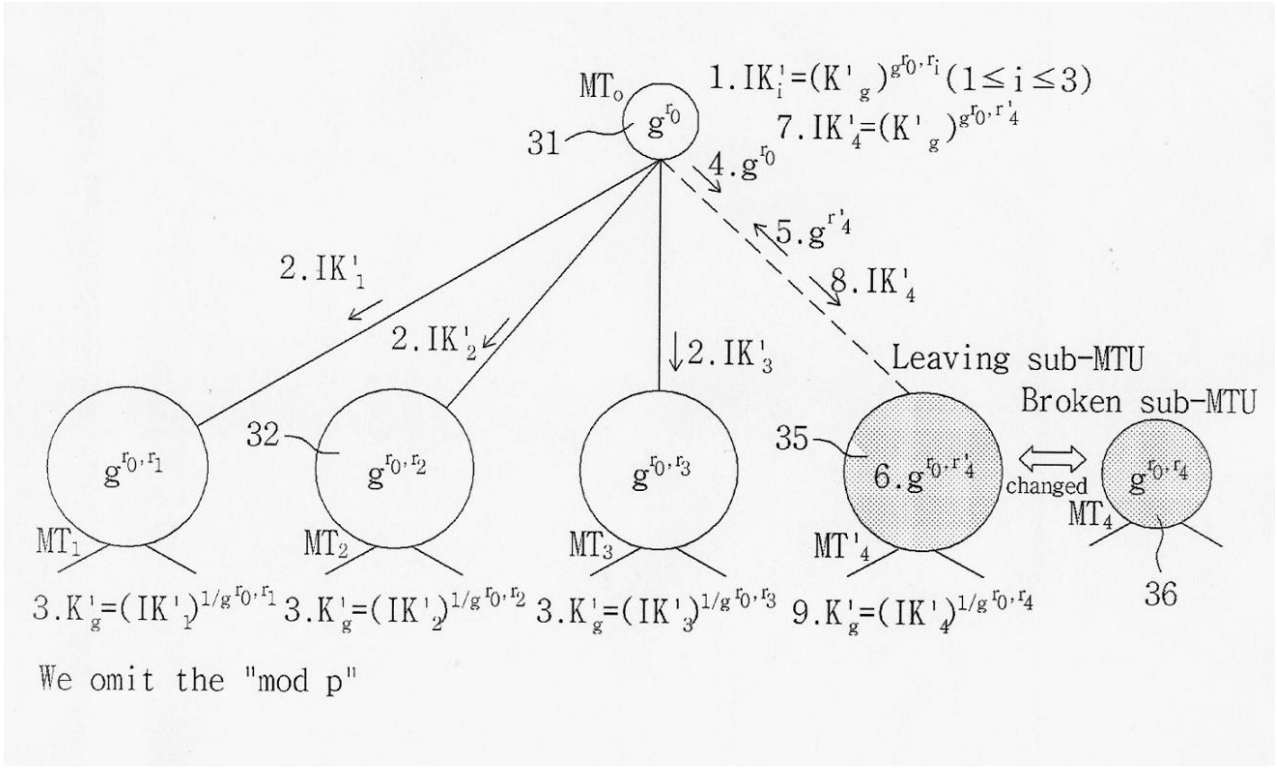
【図５】


MT_o
g^{r0}
$4.IK'_i=(K'_g)^{g^{r0,ri}}$ $(1 \le i \le 5)$
$1.g^{r0}$
$2.g^{r5}$
$5.IK'_1$
$5.IK'_2$
$5.IK'_3$
$5.IK'_4$
$5.IK'_5$
NEW sub-MTU
$g^{r0,r1}$
$g^{r0,r2}$
$g^{r0,r3}$
$g^{r0,r4}$
$3.g^{r0,r5}$
MT_1
MT_2
MT_3
MT_4
MT_5
$6.K'_g=(IK'_1)^{1/g^{r0,r1}}$
$6.K'_g=(IK'_2)^{1/g^{r0,r2}}$
$6.K'_g=(IK'_3)^{1/g^{r0,r3}}$
$6.K'_g=(IK'_4)^{1/g^{r0,r4}}$
$6.K'_g=(IK'_5)^{1/g^{r0,r5}}$
We omit the "mod p".

【図６】

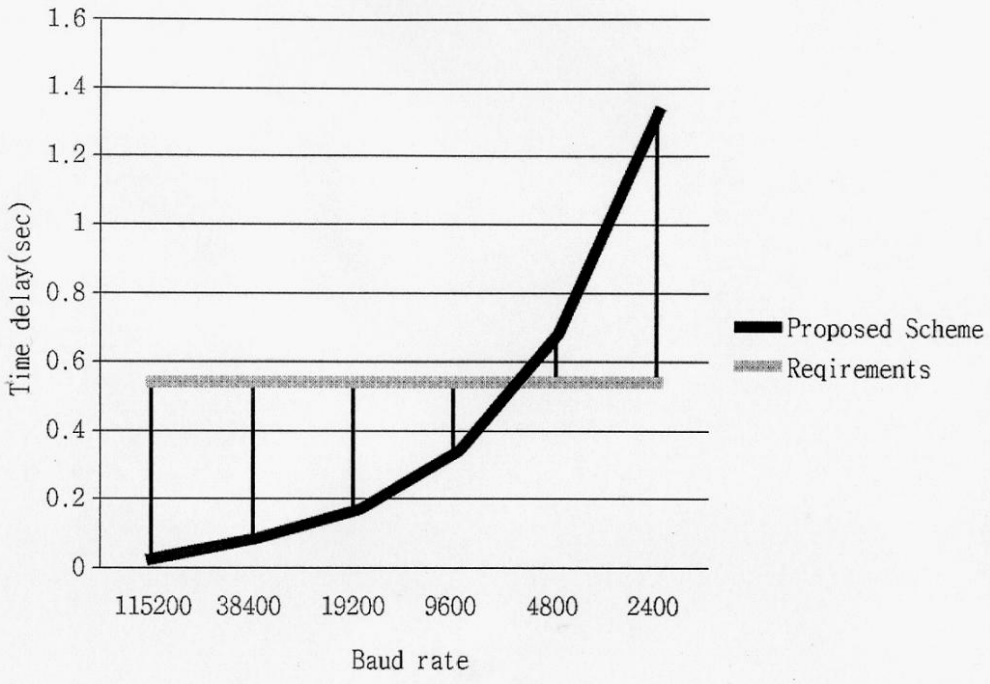

MT$_o$
g^{r_0}
1. $IK'_i=(K'_g)^{g^{r_0,r_i}}$ $(1\leq i\leq 3)$
2. IK'_1
2. IK'_2
2. IK'_3
Leaving sub-MTU
g^{r_0,r_1}
g^{r_0,r_2}
g^{r_0,r_3}
g^{r_0,r_4}
MT$_1$
MT$_2$
MT$_3$
MT$_4$
3. $K'_g=(IK'_1)^{1/g^{r_0,r_1}}$
3. $K'_g=(IK'_2)^{1/g^{r_0,r_2}}$
3. $K'_g=(IK'_3)^{1/g^{r_0,r_3}}$
We omit the "mod p".

【図７】


MT$_o$
g^{r_0}
1. $IK'_i=(K'_g)^{g^{r_0,r_i}}$ $(1\leq i\leq 3)$
7. $IK'_4=(K'_g)^{g^{r_0,r'_4}}$
31
4. g^{r_0}
5. $g^{r'_4}$
8. IK'_4
2. IK'_1
2. IK'_2
2. IK'_3
Leaving sub-MTU
Broken sub-MTU
32
35
g^{r_0,r_1}
g^{r_0,r_2}
g^{r_0,r_3}
6. g^{r_0,r'_4}
changed
g^{r_0,r_4}
MT$_1$
MT$_2$
MT$_3$
MT'$_4$
MT$_4$
36
3. $K'_g=(IK'_1)^{1/g^{r_0,r_1}}$
3. $K'_g=(IK'_2)^{1/g^{r_0,r_2}}$
3. $K'_g=(IK'_3)^{1/g^{r_0,r_3}}$
9. $K'_g=(IK'_4)^{1/g^{r_0,r_4}}$
We omit the "mod p"

【図８】

(a)



(b)

	Total time delay (sec) by baud tate									
	115200 (baud)	38400 (baud)	19200 (baud)	9600 (baud)	4800 (baud)	2400 (baud)	1200 (baud)	600 (baud)	300 (baud)	110 (baud)
Proposed Scheme	0.037949	0.113505	0.226838	0.453505	0.906838	1.813505	3.626838	7.253505	14.50684	39.56381

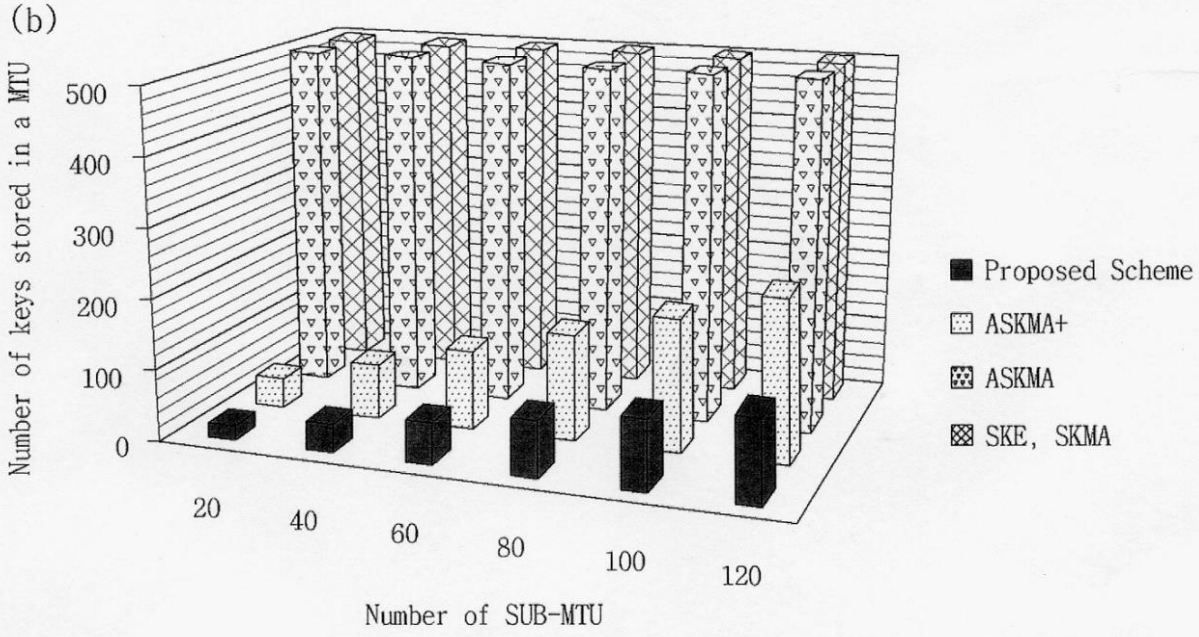
【図９】

(a)

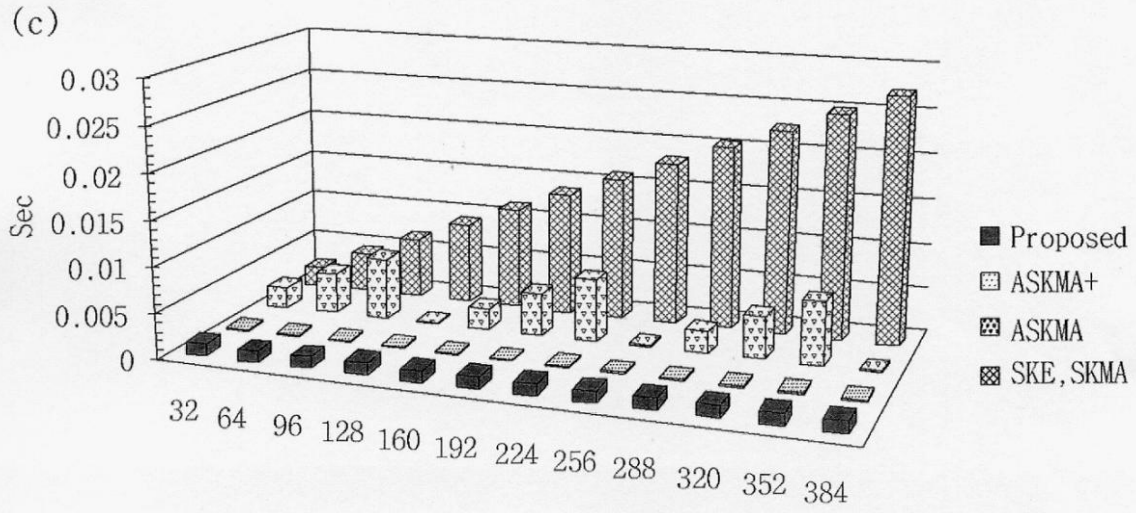
	SKE	SKMA	ASKMA	ASKMA+	Proposed Scheme
MTU	m(1+r)	m(1+r)	2m-1+mr	2m-1	m+2
Each SUB-MTU	1+r	1+r	$r+1+\log_2 m$	$2r+\log_2 m$	2r+1
Each RTU	1	1	$2+\log e_2 m$	$1+\log_2 r$	$1+\log_2 r$

m is the number of SUB-MTUs. r is the maximum number of RTUs per SUB-MTU

(b)



(c)



フロントページの続き

(72)発明者　ウォン　ドンホ
大韓民国　４４０－７４６　キョンギド　スウォンシ　ソンギュングヮン　ユニバーシティー　＃２７３０３
(72)発明者　チョイ　ドンヒョン
大韓民国　４４０－７４６　キョンギド　スウォンシ　ソンギュングヮン　ユニバーシティー　＃２７３０３
(72)発明者　チョン　ハンジェ
大韓民国　４４０－７４６　キョンギド　スウォンシ　ソンギュングヮン　ユニバーシティー　＃２７３０３
(72)発明者　リョウ　ジェチョル
大韓民国　３０５－７５５　デジョン　ユソング　エオエウンドン　ハンビット　エーティーピー　１３２－８０１

Ｆターム(参考) 5J104 AA16　EA07　NA02　NA18