(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年12 月22 日 (22.12.2005)

PCT

(10) 国際公開番号
WO 2005/122464 A1

(51) 国際特許分類[7]: H04L 9/08

(21) 国際出願番号: PCT/JP2004/019633

(22) 国際出願日: 2004 年12 月28 日 (28.12.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-168682 2004 年6 月7 日 (07.06.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 独立行政法人情報通信研究機構 (NATIONAL INSTITUTE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY) [JP/JP]; 〒1848795 東京都小金井市貫井北町４－２－１ Tokyo (JP).

(72) 発明者; および

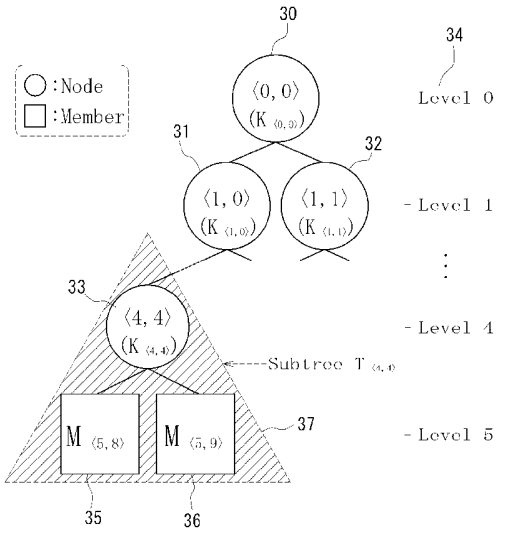
(75) 発明者/出願人 (米国についてのみ): 井上 大介 (INOUE, Daisuke) [JP/JP]; 〒1848795 東京都小金井市貫井北町４－２－１ 独立行政法人情報通信研究機構内 Tokyo (JP). 黒田 正博 (KURODA, Masahiro) [JP/JP]; 〒1848795 東京都小金井市貫井北町４－２－１ 独立行政法人情報通信研究機構内 Tokyo (JP).

(74) 代理人: 新保 斎 (SHIMBO, Itsuki); 〒1120005 東京都文京区水道1-2-10-905 つばめ特許事務所 Tokyo (JP).

[続葉有]

(54) Title: COMMUNICATION METHOD AND COMMUNICATION SYSTEM USING DECENTRALIZED KEY MANAGING SCHEME

(54) 発明の名称: 非集中型鍵管理方式を用いた通信方法及び通信システム



(57) Abstract: There is proposed a decentralized key managing scheme that allows only the members of a group to realize a tree-structured key management without using any key management servers, and there are provided communication method and system that contributes to a safe group communication. Each of the members constituting a group updates the tree-structured data of the whole group (70) and further elects a captain of the corresponding subtree (71) when a new member joins the group. Not any key management servers but the captain together with the other captains and the member, who has joined, produce and share a new key (72) and distribute the new key to the members of the subtrees (73), thereby allowing all of the members of the group to update the key to the new one. When any one withdraws from membership in the group, captains are elected, and the captains share and distribute a new key.

(57) 要約: 鍵管理サーバを使うことなく、グループのメンバだけで木構造の鍵管理を実現する非集中型鍵管理方式を提案し、安全なグループ通信に寄与する通信方法とシステムを提供する。グループを構成する各メンバが、新メンバの加入時にそれぞれグループ全体の木構造データを更新７０し、各部分木におけるキャプテンを選択７１する。鍵管理サーバではなく、キャプテンが他のキャプテンや加入メン

[続葉有]

WO 2005/122464 A1

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

バと新しい鍵を生成して共有７２し、部分木のメンバに新鍵を配布７３することによって、グループの全メンバが新鍵に更新することができる。脱退時にもキャプテンを選択してキャプテンによる新鍵の共有、配布を行う。

明 細 書

非集中型鍵管理方式を用いた通信方法及び通信システム

技術分野

[0001] 本発明は通信ネットワークにおけるグループ内のメンバでグループ鍵を共有し、該鍵で暗号化した通信を行う通信方法及びシステムに関し、特にグループ鍵を非集中型鍵管理方式により管理する構成に係る。

背景技術

[0002] 近年、携帯電話の普及を端緒にしてモバイルセキュリティ技術の研究開発、さらには製品化が盛んとなってきている。また、2Gや3Gのセルラ網をはじめ、様々な特質を持った無線をシームレスに統合する次世代の移動体通信ネットワークの研究が進んでおり、例えば本件発明者らによる非特許文献1に開示される。

この次世代通信ネットワークは、利用するモバイルサービスに合わせて自動的に最適な無線が選ばれるといった機能を持っており、非特許文献2に開示されているように様々な無線が柔軟に同ネットワークにプラグインできるようなアーキテクチャが想定される。

[0003] 非特許文献1:M. Kuroda, M. Inoue, A. Okubo, T. Sakakura, K.Shimizu, and F. Adachi, "Scalable Mobile Ethernet and Fast Vertical Handover," Proc. IEEE Wireless Communications and Networking Conference 2004,Mar. 2004.
非特許文献2:M. Yoshida, M. Kuroda, S. Kiyomoto, and T. Tanaka,"A SecureService Architecture for Beyond 3G WirelessNetwork," Proc. 6th International Symposium onWireless Personal Multimedia Communications, Vol.2, pp. 579-583, 2003.

[0004] 次世代の移動体通信ネットワークでは、従来のクライアント・サーバ型のサービスだけでなく、複数の利用者が多様な携帯端末を使って動的なグループを形成し, メンバ同士が安全に情報共有を行えるグループ型のサービスにも期待が寄せられている。このような安全なグループ通信の実現に必要な機能には、データの守秘や完全性の検証、送信元の認証、メンバ管理などが挙げられるが、グループのメンバが共有す

るグループ鍵の管理もまた非常に重要な研究課題である。

[0005] メンバの加入・脱退が起こり得る動的なグループでは、新しくグループに加入するメンバ(以下、加入メンバと呼ぶ。)が加入以前の情報にアクセスできないよう、またグループから脱退するメンバ(以下、脱退メンバと呼ぶ。)が脱退以後の情報にアクセスできないよう、グループ鍵を更新する必要がある。

グループ鍵の更新機能を有する鍵管理方式は、鍵を集中管理するサーバや無線基地局などを必要とする方式(非特許文献3ないし11に開示)と、グループのメンバ全員が協力してDH鍵共有を行いグループ鍵を更新するContributory Key Agreement と呼ばれる方式(非特許文献12ないし16に開示)とに大別できる。

[0006] なお、DH鍵共有は、周知の如くディフィー氏及びヘルマン氏によって開発された鍵共有方式であり、該鍵共有方式では、離散対数問題を利用して、秘密鍵そのものではなく、乱数と秘密鍵から生成した公開情報(公開鍵)を送受信する。これにより、通信内容を第三者に盗聴されても、直ちに秘密鍵を知られることはなく、安全に鍵情報を共有することができる方式である。

[0007] 非特許文献3:H. Harney, C. Muckenhirn, and T. Rivers, "Group Key Management Protocol (GKMP) Specification," IETF, RFC 2093, 1997.

非特許文献4:H. Harney, C. Muckenhirn, and T. Rivers, "Group Key Management Protocol (GKMP) Architecture," IETF, RFC 2094, 1997.

非特許文献5:D. Wallner, E. Harder, R. Agee, "Key Management for Multicast: Issues and Architectures," IETF, RFC 2627, 1999.

非特許文献6:C. K. Wong, M. Gouda, and S. Lam, "Secure Group Communication Using Key Graphs," IEEE/ACM Trans. on Networking, Vol. 8, No. 1, pp. 16-30, 2000.

非特許文献7:R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast Security: A Taxonomy and Efficient Constructions," Proc.IEEE Infocom '99, Vol.2, pp. 708-716, 1999.

非特許文献8:D.A. McGrew, and A.T. Sherman, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees," IEEE Trans. on Software

Engineering, Vol.29, No. 5, pp. 444-458, 2003.

非特許文献9:A. Perrig, D. Song, and J.D. Tygar, "ELK: A NewProtocol for Efficient Large-Group Key Distribution," Proc. IEEE Security and Privacy Symposium, pp. 247-262, 2001.

非特許文献10:A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, " SPINS: Security Protocols for Sensor Networks," Proc. Mobile Computing and Networking 2001, pp. 189-199, 2001.

非特許文献11:Y. W. Law, R. Corin, S. Etalle, and P. H. Hartel, "A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks, " Proc. Personal Wireless Communications 2003, pp. 27-39, 2003.

非特許文献12:D. G. Steer, L. Strawczynski, W. Diffie, and M.Wiener, "A Secure Audio Teleconference System,"Proc. Advances in Cryptology-CRYPTO '88, pp. 520-528, 1988.

非特許文献13:M. Burmester, and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," Proc. Advances in Cryptology-EUROCRYPT '94, pp. 275-286,1994.

非特許文献14:M. Steiner, G. Tsudik, and M. Waidner, "Key Agreement in Dynamic Peer Groups," IEEE Trans. on Parallel and Distributed Systems, Vol. 11, No. 8, pp 769-780,2000.

非特許文献15:J. Alves-Foss, "An Efficient Secure Authenticated Group Key Exchange Algorithm for Large and Dynamic Groups," Proc. 23rd National Information Systems Security Conference, pp. 254-266, 2000.

非特許文献16:Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups," ACM Conference on Computer and Communications Security 2000, pp. 235-244, 2000.

[0008] 前者は鍵を集中管理するエンティティがSingle Point of Failure となる可能性を持ち、またAd Hoc ネットワークなどのサーバレスなグループ通信には応用が難しい。後者はグループ鍵更新の際にグループの全てのメンバがベキ乗剰余演算を行う必

要があり、計算力の乏しい携帯端末などを含むグループ通信には不向きである。

[0009] ところで、従来のグループ鍵の更新方法としては、Logical Key Hierarchy(LKH)(非特許文献5及び6に開示)として知られる、木構造で鍵を管理する方式が非常に効率的である。

しかし、このような鍵を集中管理する方法では上記の問題がある他、メンバの加入時・脱退時によりコストの少ない鍵管理方式が望まれている。

[0010] なお、鍵管理サーバを用いた特許文献としては、特許文献17や特許文献18に開示されるような技術が公知であり、特許文献17では鍵管理サーバが一括管理する方式を開示しており、その際にはグループが大規模であると鍵の更新にかかるコストが大きくなる問

題がある。また、特許文献18はサブグループを管理するサーブグループ鍵管理サーバを別に設けるが、あくまでも鍵を管理するサーバであって、木構造の上位にあるサーバが管理する方法である。

[0011] 特許文献17:特開平9-319673号公報

特許文献18:特開2004-023237号公報

発明の開示

発明が解決しようとする課題

[0012] 本発明は上記従来技術に鑑みて創出されたものであって、鍵管理サーバを使うことなく、グループのメンバだけで木構造の鍵管理を実現する非集中型鍵管理方式を提案し、安全なグループ通信に寄与する通信方法とシステムを提供することを目的とする。

課題を解決するための手段

[0013] 本発明は、上記の課題を解決するために、次のような通信方法を提供する。

すなわち、請求項1に記載の発明は、通信ネットワーク中で複数のメンバが加入可能なグループを組織し、該グループ内で通信データの暗号化もしくは認証に用いるグループ鍵を共有するとともに、グループ鍵を最上位の根に割り当て、サブグループ鍵を枝の分岐点であるノードに割り当て、各メンバを最下位の部分木の先端である葉に割り当てて、各メンバはグループ鍵及びグループ鍵から自己に至るまでの全ての

サブグループ鍵を保持して通信を行う通信方法である。

そして、あらかじめグループに属する各メンバにはグループ全体の木構造データ及び、グループ鍵、全てのサブグループ鍵を記憶させておき、新しいメンバの加入を各メンバが加入脱退検知手段により検知すると次の各ステップを含む。

[0014] (1) 各メンバが、木構造データ更新手段により、加入メンバを所定の規則に従って木構造の葉に割り当て、自己の記憶する木構造データを更新する木構造データ更新ステップ。

(2) メンバが、キャプテン当否判定手段により、新しい木構造データから所定の規則に従って自己が部分木のキャプテンとなるか否かを判定するキャプテン当否判定ステップ。

(3) 該キャプテンが、新鍵生成配布手段により、少なくとも自己の部分木の各メンバとの間で新鍵を生成し配布する新鍵生成配布ステップ。

[0015] 請求項2に記載の発明は、上記請求項1の通信方法における新鍵生成配布ステップが、該加入メンバと各キャプテンとが、新鍵共有手段により、互いに新しいグループ鍵又はサブグループ鍵の生成情報を通信し、新鍵を生成して共有する新鍵共有ステップと、各キャプテンが、新鍵配布手段により、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布する新鍵配布ステップとの各ステップからなることを特徴とする。

[0016] 請求項3に記載の発明は、上記請求項1の通信方法における新鍵生成配布ステップが、加入メンバと最下位のキャプテンが新鍵を共有すると共に、順次下位のキャプテンが1階層上位のキャプテンと新鍵を共有する新鍵共有ステップと、各キャプテンが、新鍵配布手段により、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、下位のキャプテンから順次に、該キャプテンが属する部分木の新鍵で1階層上位の新鍵を暗号化して加入メンバに送信する新鍵配布ステップとの各ステップからなることを特徴とする。

[0017] 請求項4に記載の発明は、上記請求項1ないし3に記載の発明の構造データ更新ステッ

プにおいて、加入メンバを葉に割り当てる所定の規則が、木構造全体の最下位でか

つ最右側のノードにおける最左側の葉、又は最下位でかつ最左側のノードにおける最右側の葉として割り当てることを特徴とする。

[0018] 請求項5に記載の発明は、上記請求項1ないし3に記載の発明のキャプテン当否判定ステップにおいて、キャプテンとなるか否かを判定する所定の規則が、ある部分木におけるキャプテンとなるメンバは、その部分木の上位側からみて加入メンバがいる側の枝と反対側の枝の葉のメンバから選択することを特徴とする。

[0019] 請求項6に記載の発明は、上記木構造が2分木であることを特徴とするものである。

[0020] 請求項7に記載の発明は、メンバの脱退を各メンバが加入脱退検知手段により検知すると、各ステップを含むことを特徴とする。

(1) 各メンバが、キャプテン当否判定手段により、脱退メンバを除いた木構造データから所定の規則に従って自己が部分木のキャプテンとなるか否かを判定するキャプテン当否判定ステップ。

(2) 該キャプテンが、新鍵生成配布手段により、少なくとも自己の部分木のメンバ及び他のキャプテンとの間で新鍵を生成し配布する新鍵生成配布ステップ。

(3) 各メンバが、木構造データ更新手段により、所定の規則に従って脱退メンバの属する部分木のメンバを葉として再割り当てし、自己の記憶する木構造データを更新する木構造データ更新ステップ。

[0021] 請求項8に記載の発明は、前記通信方法における新鍵生成配布ステップが、脱退メンバの生じた最下位の部分木のキャプテンと、脱退メンバの属する部分木のその他全てのキャプテンとが、新鍵共有手段により、互いに新しいグループ鍵又はサブグループ鍵の生成情報を通信し、新鍵を生成して共有する新鍵共有ステップと、各キャプテンが、新鍵配布手段により、生成された新鍵を1階層下位の従前のサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、脱退メンバの生じた最下位の部分木のキャプテンが、新鍵配布手段により、不足している新鍵をその部分木の従前のサブグループ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布ステップとの各ステップからなることを特徴とする。

[0022] 請求項9に記載の発明は、前記通信方法における新鍵生成配布ステップが、脱退メンバの生じた最下位の部分木のキャプテンから順次に、下位のキャプテンが1階層

上位のキャプテンと新鍵を共有する新鍵共有ステップと、各キャプテンが、新鍵配布手段により、自己の部分木の各メンバに新鍵を配布すると共に、脱退メンバの生じた部分木のキャプテンが、新鍵配布手段により、不足している新鍵をその部分木の従前のサブグループ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布ステップとの各ステップからなることを特徴とする。

[0023] 請求項10に記載の発明は、前記キャプテン当否判定ステップにおいて、キャプテンとなるか否かを判定する所定の規則が、ある部分木におけるキャプテンとなるメンバは、その部分木の上位側からみて加入メンバがいる側の枝と反対側の枝の葉のメンバから選択することを特徴とするものである。

[0024] 請求項11に記載の発明は、請求項7ないし10の発明において木構造が2分木とするものである。

[0025] 本発明は、次のような通信システムを提供することができる。

すなわち、請求項12に記載の発明によれば、通信ネットワーク中で複数のメンバが加

入可能なグループを組織し、該グループ内で通信データの暗号化もしくは認証に用いるグループ鍵を共有するとともに、グループ鍵を最上位の根に割り当て、サブグループ鍵を枝の分岐点であるノードに割り当て、各メンバを最下位の部分木の先端である葉に割り当てて、各メンバはグループ鍵及びグループ鍵から自己に至るまでの全てのサブグループ鍵を保持して通信を行う通信システムを提供する。

[0026] そして、各メンバとなる端末装置に、次の各手段を備える。

(1) グループ全体の木構造データ及び、グループ鍵、全てのサブグループ鍵を記憶する記憶手段。

(2) 新しいメンバの加入又はメンバの脱退を検知する加入脱退検知手段。

(3) 加入メンバを所定の規則に従って木構造の葉に割り当て、自己の記憶する木構造データを更新するか、又は所定の規則に従って脱退メンバの属する部分木のメンバを葉として再割り当てし、自己の記憶する木構造データを更新するかの少なくともいずれかの処理を行う木構造データ更新手段。

(4) 木構造データから所定の規則に従って自己が部分木のキャプテンとなるか否

かを判定するキャプテン当否判定手段。

(5) キャプテンとなった場合に、少なくとも自己の部分木のメンバとの間で新鍵を生成し配布する新鍵生成配布手段。

[0027] 請求項13に記載の発明によれば、通信システムにおける端末装置の新鍵生成配布手段が、加入メンバ及びキャプテン間で、互いに新しいグループ鍵又はサブグループ鍵の生成情報を通信し、新鍵を生成して共有する新鍵共有手段と、キャプテンの時に、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布する新鍵配布手段とからなることを特徴とする。

[0028] 請求項14に記載の発明によれば、通信システムにおける端末装置の新鍵生成配布手段が、加入メンバと最下位のキャプテンが新鍵を共有すると共に、順次下位のキャプテンが1階層上位のキャプテンと新鍵を共有する新鍵共有手段と、キャプテンの時に、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、下位のキャプテンから順次に、該キャプテンが属する部分木の新鍵で1階層上位の新鍵を暗号化して加入メンバに送信する新鍵配布手段とからなることを特徴とする。

[0029] 請求項15に記載の発明は、前記の通信システムにおける端末装置の新鍵生成配布手段が、脱退メンバの生じた最下位の部分木のキャプテンと、脱退メンバの属する部分木のその他全てのキャプテンとが、互いに新しいグループ鍵又はサブグループ鍵の生成情報を通信し、新鍵を生成して共有する新鍵共有手段と、キャプテンの時に、生成された新鍵を1階層下位の従前のサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、脱退メンバの生じた最下位の部分木のキャプテンが、不足している新鍵をその部分木の従前のサブグループ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布手段とからなるものである。

[0030] 請求項16に記載の発明は、通信システムにおける端末装置の新鍵生成配布手段が、脱退メンバの生じた最下位の部分木のキャプテンから順次に、下位のキャプテンが1階層上位のキャプテンと新鍵を共有する新鍵共有手段と、キャプテンの時に、新鍵配布手段により、自己の部分木の各メンバに新鍵を配布すると共に、脱退メンバの生じた部分木のキャプテンが、不足している新鍵をその部分木の従前のサブグルー

プ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布手段とからなるものである。

[0031] 請求項17に記載の発明は、請求項12ないし16の通信システムにおいて、木構造データ更新手段で用いる加入メンバを葉に割り当てる所定の規則が、木構造全体の最下位で
かつ最右側のノードにおける最左側の葉、又は最下位でかつ最左側のノードにおける最右側の葉として割り当てることを特徴とするものである。

[0032] 請求項18に記載の発明は、上記通信システムにおいてキャプテン当否判定手段で用いるキャプテンとなるか否かを判定する所定の規則が、ある部分木におけるキャプテンとなるメンバは、その部分木の上位側からみて加入メンバがいる側の枝と反対側の枝の葉のメンバから選択することを特徴とするものである。

[0033] 請求項19に記載の発明は、請求項12ないし18の通信システムにおいて、前記木構造が2分木であることを特徴とする。

発明の効果

[0034] 以上の発明により次の効果を奏する。

すなわち、請求項1ないし6に記載の非集中型鍵管理方式を用いた通信方法によれば、メンバの加入時にサーバレスで安全にグループ鍵を共有する鍵管理方式を提供することができ、コストの抑制にも寄与する。

[0035] 請求項7ないし11に記載の非集中型鍵管理方式を用いた通信方法によれば、メンバの脱退時にサーバレスで安全にグループ鍵を共有する鍵管理方式を提供することができ、コストの抑制にも寄与する。

[0036] 請求項12ないし19に記載の発明によれば、上記通信方法を実装し、非集中型鍵管理方式を用いた通信システムを提供することができる。

図面の簡単な説明

[0037] [図1]本発明に係る通信システムを構成する端末装置の構成図である。

[図2]FDLKHのノード及びメンバの関係を説明する説明図である。

[図3]FDLKHのノード及びメンバの関係を一般化した説明図である。

[図4]本発明の方式によるメンバ加入時の処理を説明する説明図である。

[図5]本発明の方式によるメンバ脱退時の処理を説明する説明図である。

[図6]本発明の方式によるメンバ加入時の処理の流れ図である。

[図7]本発明の方式によるメンバ脱退時の処理の流れ図である。

[図8]本発明の第2の実施例に係る加入プロトコルの流れ図である。

[図9]本発明の第3の実施例に係る加入プロトコルの流れ図である。

[図10]本発明の第4の実施例に係る脱退プロトコルの流れ図である。

[図11]本発明の第5の実施例に係る脱退プロトコルの流れ図である。

[図12]FDLKH(dedicated方式)のメンバ加入において、メンバ数に対する共通鍵暗号系のコストの変化を示すグラフである。

[図13]FDLKH(distributed方式)のメンバ加入において、メンバ数に対する共通鍵暗号系のコストの変化を示すグラフである。

[図14]FDLKH(dedicated方式)のメンバ脱退において、メンバ数に対する共通鍵暗号系のコストの変化を示すグラフである。

[図15]FDLKH(distributed方式)のメンバ脱退において、メンバ数に対する共通鍵暗号系のコストの変化を示すグラフである。

符号の説明

[0038] 70 木構造データ更新ステップ

71 キャプテン選択ステップ

72 新鍵共有ステップ

73 新鍵配布ステップ

発明を実施するための最良の形態

[0039] 以下、本発明の実施形態を、図面に示す実施例を基に説明する。なお、実施形態は下記に限定されるものではない。

実施例 1

[0040] 図1は本発明に係る通信システムにおける端末装置の構成図である。図示のように、端末装置(1)にはCPU(10)と、ネットワーク通信を司るネットワークアダプタ(20)、データを記憶するメモリ(21)が付設されている。このような構成は、公知のパーソナルコンピュータや、携帯電話端末、携帯情報通信端末などに備えられており、本発明

はこれらの装置に実装可能である。

[0041] そして、CPU(10)では、ネットワーク上でグループを構成する他のメンバの加入や脱退を検知する加入脱退検知部(11)による処理や、グループ全体で鍵を管理するための木構造データを更新処理する木構造データ更新部(12)による処理の他、本発明の方法を実現するキャプテン当否判定部(13)、新鍵共有部(14)、新鍵配布部(15)の各処理を行う。

[0042] なお、本発明において鍵を生成及び共有する処理については、ネットワーク通信における公開鍵暗号系を用いた暗号鍵の生成及び共有処理が周知であり、これらの周知技術を適用することができる。

[0043] 次に、本発明に係るグループ鍵の概念につき説述する。グループ鍵はグループの全てのメンバが共有する共通鍵暗号の鍵であり、グループを流れる通信はこのグループ鍵によって暗号化される。

メンバの加入・脱退が起こった際にはグループ鍵の更新が必要となる。グループ鍵の更新方法としてはLogical Key Hierarchy(LKH)として知られる、木構造で鍵を管理する方式が非常に効率的であるが、これは集中型の鍵管理サーバを前提に設計されている。

[0044] そこで、本発明では鍵管理サーバを使うことなく、グループのメンバだけで木構造の鍵管理を実現する非集中型鍵管理方式を提案する。以下、提案方式をFDLKH(Fully Decentralized Key Management Scheme on Logical Key Hierarchy)と呼ぶこととする。

LKHの本質は、グループのメンバを論理的な木のリーフに割り当て、部分木ごとのサブグループグループに分割し、管理サーバがサブグループごとにグループ鍵更新のために使われる鍵を配布することで、1回のグループ鍵更新にかかる暗号化のコストを、メンバ数nに対してO(n)からO(log n)に抑えることにある。

[0045] 本発明に係るFDLKHでは、2分木を用いてメンバをサブグループに分割し、鍵管理サーバの代わりに、各サブグループから1メンバずつが代表として選出され、DH鍵共有と鍵配布を受け持つ。

これによってLKHと同様に暗号化のコストはO(log n)となり、システム全体の鍵の数

はLKHに比べて約半分になる効果を有する。

[0046] 次に、図2はFDLKHで用いる2分木の一部を示す説明図である。木の各ノード(30)ー(33)は、木のレベル(34)l(l=0,1,2,・・・)と、そのレベル(34)における位置m(0 m 2^l-1)を用いて <l,m>と表す。従って、レベル1の位置0(左端)のノード(31)は<1,0>である。

[0047] グループのメンバは、子を持たないノード(つまり葉、リーフ)に割り当てられる。以下、このような割り当てを「メンバがノードを占有する」と表現する。ノード<l,m>を占有するメンバをM<l,m>と表す。例えば、ノード<4,4>の葉となるメンバはM<5,8>(35)とM<5,9>(36)である。

[0048] メンバに占有されていないノードには鍵が割り当てられ、ノード<l,m>に割り当てられる鍵をK<l,m>と表す。

このK<l,m>は、ノード<l,m>を根とする部分木T<l,m>に属するメンバ間で共有される。

例えば、図2におけるノード<4,4>(33)を根とする部分木T<4,4>(37)に属するメンバ間で共有される鍵はK<4,4>であり、本発明ではこれをサブグループ鍵と呼んでいる。

[0049] なお、K<0,0>は、全てのメンバが共有し、すなわちこれがグループ鍵である。本発明では最も上位の鍵であるグループ鍵と、各階層におけるサブグループ鍵をメンバが保持することになる。

すなわち、メンバM<5,8>(35)とM<5,9>(36)が部分木T<4,4>に属して鍵K<4,4>を共有している他、これらのメンバは図示しない部分木T<3,2>, T<2,1>, T<1,0>, T<0,0>にも属するので、両メンバが持つ鍵は、K<4,4>, K<3,2>, K<2,1>, K<1,0> , K<0,0>の計5 つである。

つまり、あるメンバは、その親ノード(1レベル上位のノード)から根ノード<0,0>(最上位のノード)に到る経路上の全ての鍵を持つ。

[0050] 図3は、ノード<l,m>を占有するメンバM<l,m>(40)を基点として2分木を一般化したものである。M<l,m>の親ノードは<l-1,[m/2]>(41)で表され、兄弟メンバ(同じ親ノードに属するメンバ)はM<l,m+$(-1)^m$>(42)である。

親ノードから根ノードに到る全ての祖先ノード(43)は<l-i,[$m/2^i$]>(i=1,・・,l)と一般化

できる。よって、M<l,m>が属する部分木と、所有する鍵は、それぞれT<l-i,[m/2^i]>、K<l-i,[m/2^i]>と表せる。

[0051] 本発明において、グループにメンバの加入・脱退が起こった際には、鍵の更新が必要なノードを根とする部分木ごとに1人のメンバを代表として選び、それらの代表が鍵更新の処理を受け持つようにした。これにより、従来鍵管理サーバを用いていた鍵管理を代表のメンバに分散して処理することができる。

このようなメンバを「キャプテン」と呼ぶこととし、部分木T<l,m>を代表するキャプテンをC<l,m>と表す。

[0052] キャプテンはメンバの加入・脱退が起こった際に、鍵の操作が必要となるノードを根とする部分木を代表して、鍵共有と鍵配布の処理を受け持つ。メンバ加入の際には部分木の各キャプテンと加入メンバがDH鍵共有を行い、メンバ脱退の際にはキャプテン同士がDH鍵共有を行う。

その結果共有した鍵を各キャプテンが部分木のメンバに配布する。M<l,m>が加入もしくは脱退する場合、鍵の操作が必要となるノードはl個あり、ゆえにl人のメンバがキャプテンとして選択される。

[0053] ある部分木のキャプテンとなるメンバは、その部分木の根ノードからみて、加入・脱退メンバがいる側の枝と逆側の枝の子孫から選択される。

図4はメンバM<3,3>(50)が加入する例であり、部分木T<2,1>のキャプテンC<2,1>にはノード<2,1>の逆側の枝の子孫であるメンバM<3,2>(51)が選択される。同様に、部分木T<1,0>のキャプテンC<1,0>にはメンバM<3,0>(52)が、部分木(木構造全体)T<0,0>のキャプテンC<0,0>にはメンバM<3,4>(53)が選択される。

[0054] 同様に、図5はメンバM<3,0>(60)が脱退する例であり、メンバM<3,1>(61), M<3,3>(62), M<2,3>(63)が、それぞれキャプテンC<2,0>, C<1,0>, C<0,0>となる。

次に、部分木にキャプテンの候補となるメンバが複数いる場合を考える。例えば、図4のT<1,0>ではM<3,0>(52)とM<3,1>(54)が、T<0,0>ではM<3,4>(53)とM<3,5>(55)とM<2,3 >(56)がキャプテンの候補である。

[0055] 本発明において、各メンバはキャプテン当否判定部(13)で自己がキャプテンとなるか否かを共通の選択アルゴリズムにより判定する。

最も簡便な選択アルゴリズムとしては、各メンバがメモリ(21)に常時記憶している木構造データを参照し、上記に従って、自己がその部分木の根ノードからみて、加入・脱退メンバがいる側の枝と逆側の枝の子孫であるか、子孫が複数ある場合には左端のメンバであるか否かを順に判定し、いずれも満たす場合に、自己をその部分木のキャプテンと確定する。

[0056] この方法は、部分木ごとにキャプテンとなるメンバを固定する方法であり、メンバの計算力に格差があり、高い計算力を持つメンバに処理をある程度集中させたいようなグループに向いている。そこで例えば、計算力に従ってあらかじめメンバに序列をつけておき、自己の序列が最も高い場合に自己をキャプテンと確定するようにしてもよい。

[0057] また別の方法は、キャプテンの候補となるメンバの間で、キャプテンの役割を持ち回りする変動型の方法である。この方法は、メンバが互いに対等な関係で、処理の負荷を平坦化したいようなグループに向いている。従って、部分木内で例えば左から右に順にキャプテンを持ち回らせるなどの選択アルゴリズムを用いることができる。

[0058] 本発明の非集中型鍵管理方式では、メンバが加入又は脱退する際に、次のように木構造データを更新する。木構造データの更新は、CPU(10)の木構造データ更新部(12)においてメモリ(21)のデータを書き換える方法で処理される。

[0059] すなわち、本発明においてグループの全てのメンバは、2分木の情報を共有している。メンバの加入・脱退が起こると、メンバ各々が2分木の形状を更新する。

図4に示すメンバ加入の際、加入メンバ(50)は2分木の中で最もレベルが小さく、最も左側のノード(57)の右の子として加入する。これは本実施例における規則であり、逆に最も右側のノード<2,3>の左の子(右の子でも良い)として加入するなど、任意の所定の規則を用いることができる。

図4では加入メンバはM<3,3>となる。M<3,3>の加入に伴い、ノード<2,1>を占有していたM<2,1>が1つ下層に移動し、ノード<2,1>の左の子M<3,2>となる。

[0060] メンバ脱退は2分木の任意のノードで起こり得る。図5ではM<3,0>(60)の脱退に伴い、M<3,0>(60)の兄弟メンバであったM<3,1>(61)が1つ上層に移動し、親ノード<2,0>を占有してM<2,0>(64)となる。脱退メンバの兄弟ノードがメンバに占有されてい

ない(例えば図5のM<2,3>(63)が脱退する)場合は、その兄弟ノードを根とする部分木ごと上層に移動させ、部分木の子孫ノードの名前を更新する。つまり、T<2,2>をT<1,1>とする。

[0061] 上述の通り、各メンバは加入脱退検知部(11)でメンバの加入や脱退をネットワークから検知すると、上記の規則に従って、加入メンバの場合には2分木の中で最もレベルが小さく、最も左側のノード(57)の右の子として加入させて木構造データを更新し、メンバが脱退する場合には、兄弟メンバを1階層上位に移動させたり、兄弟ノードがメンバに占有されていない時には、その兄弟ノードを根とする部分木ごと上層に移動させたりして木構造データを更新する。

[0062] なお、加入メンバに対しては、加入メンバの親ノードを根とする部分木のキャプテンが

2分木の情報を送信し、加入メンバはメモリ(21)に記憶する。

また、加入前のメンバ数が2のベキ数で、完全2分木を形成している場合は、根ノード<0,0>を新たに作り、元の根ノードを<1,0>に移して、<1, 0>以下の子孫ノードの名前を更新し、加入メンバを根ノードの右の子M<1,1>とするようにしてもよい。

[0063] 本発明では、従来の鍵管理サーバを用いることなく、キャプテンがグループ鍵及びサブグループ鍵を生成して各メンバに配布することを特徴とし、新鍵生成配布手段により生成及び配布の態様は任意に定めることができる。

メンバの加入・脱退の際にはグループ鍵を更新するために、2分木のノードに割り当てられる鍵の生成や変更あるいは破棄が行われる。これら3つの処理を総称して「鍵の操作」と呼ぶ。

[0064] メンバの加入・脱退の際に鍵の操作が必要となるノードは、加入もしくは脱退メンバの親ノードから根ノードに到る全ての祖先ノードである。図4のメンバ加入の例では<2,1>

, <1,0>, <0,0>が鍵の操作の必要なノードである。ここで、ノード<2,1>の鍵は新たに生成される。

図5のメンバ脱退の例では<2,0>, <1,0>, <0,0>が鍵の操作の必要なノードである。ここで、ノード<2,0>の鍵は破棄される。

[0065] 鍵の破棄は他のメンバとの協調を必要とせず、破棄すべき鍵を持つメンバがそれぞれ処理を行う。鍵の生成・変更に関しては他のメンバとの協調が必要である。一般にM<l,m>がグループに加入する際、鍵の生成・変更が必要なノードは<l-i,[m/2^i]>(i=1,・・,l)と表せる。一方、M<l,m>がグループから脱退する際に、鍵の変更が必要なノードは、鍵が破棄される親ノードを除いた<l-j,[m/2^j]>(j=1,・・,l)と表せる。

[0066] 以下に実施態様としてメンバ加入時の2例、メンバ脱退時の2例をそれぞれ実施例2ないし5に説述する。

実施例 2

[0067] まず、メンバ加入時の新鍵生成配布手段を、CPU(10)の新鍵共有部(14)と新鍵配布部(15)とで構成し、図6に示す加入プロトコルを処理する実施例を説述する。(本方式をFDLKHのdedicated方式と呼ぶ。)

上述した通り、メンバ(50)が加入する場合、加入脱退検知部(11)で検知すると、各メンバにおいて木構造データ更新部(12)が木構造データの更新処理(70)を行う。次いで、キャプテン当否判定部(13)の処理を各メンバが行うことにより、木構造におけるキャプテンが選択(71)される。

加入メンバ(50)には、キャプテン(51)が木構造データを送信する。

[0068] そして、新鍵共有処理(72)に進む。ここで、新鍵の生成・変更にはDH鍵共有を用いる。メンバ加入の際には加入メンバと各キャプテンがDH鍵共有を行う。各キャプテンは、DH鍵共有で共有した値を暗号学的に安全な一方向性ハッシュ関数hに入力し、その結果得られた出力を部分木の根ノードに割り当てる共通鍵暗号の鍵とする。

[0069] 図4において、加入メンバM<3,3>と、キャプテンとして選択されたメンバM<3,2>, M<3,0>, M<3,4>が、公開情報である素数p とZp^*の生成元g、ならびにメンバそれぞれが持つ秘密の乱数$X_{M<l,m>} \in Z_{p-1}$を用いて以下を新鍵共有部(14)の処理により計算する。

(数1) $Y_{M<l,m>}=g^{XM<l,m>} \bmod p$

[0070] M<3,3>と各キャプテンM<3,2>, M<3,0>, M<3,4>は数1の結果を以下のように送信する。このとき、ユニキャストもしくはマルチキャストで送信するが、man-in-the-middle攻撃

を防ぐためにはディジタル署名等の付加が必要である。ユニキャスト、マルチキャストによる送信方法及び、ディジタル署名の付加技術については周知である。

[0071] $M\langle 3,3\rangle \rightarrow [M\langle 3,2\rangle, M\langle 3,0\rangle, M\langle 3,4\rangle] : Y_{M\langle 3,3\rangle}$

$M\langle 3,2\rangle \rightarrow M\langle 3,3\rangle : Y_{M\langle 3,2\rangle}$

$M\langle 3,0\rangle \rightarrow M\langle 3,3\rangle : Y_{M\langle 3,0\rangle}$

$M\langle 3,4\rangle \rightarrow M\langle 3,3\rangle : Y_{M\langle 3,4\rangle}$

なお、上記において、A→B:XはAがBへデータXを送信することを示す。

[0072] 各メンバにおいて、新鍵共有部(14)において数1の結果を受信すると、DH鍵共有のベキ乗剰余演算を行い、その結果の値をハッシュ関数hに入力して演算する。これにより、M<3,3>とM<3,2>, M<3,0>, M<3,4>は、それぞれ以下の鍵を共有することができる。

$K'\langle 2,1\rangle = h(g^{XM\langle 3,3\rangle XM\langle 3,2\rangle} \bmod p)$

$K'\langle 1,0\rangle = h(g^{XM\langle 3,3\rangle XM\langle 3,0\rangle} \bmod p)$

$K'\langle 0,0\rangle = h(g^{XM\langle 3,3\rangle XM\langle 3,4\rangle} \bmod p)$

[0073] 以上の新鍵共有処理(72)が完了すると、次にキャプテンは、共有した新しい鍵を、部分木の他のメンバに配布する新鍵配布処理(73)を新鍵配布部(15)によって行う。

メンバ加入の際は、新しい鍵を加入以前の古い鍵を使って暗号化し、部分木のメンバに配布する。

[0074] 図4では、部分木を代表するM<3,0>(52)とM<3,4>(53)がそれぞれ、新しい鍵K'<1,0>、K'<0,0>を古い鍵K<1,0>, K<0,0>で暗号化して各部分木に配布する。すなわち、

$M\langle 3,0\rangle \rightarrow T\langle 1,0\rangle : E(K\langle 1,0\rangle, K'\langle 1,0\rangle)$

$M\langle 3,4\rangle \rightarrow T\langle 0,0\rangle : E(K\langle 0,0\rangle, K'\langle 0,0\rangle)$

ここで、E(K,X)とは共通鍵暗号の鍵KによるデータXの暗号文を表す。

新鍵が配布されると、グループの各メンバは新しい鍵を復号し、該当するノードに割り当てて全てのサブグループ鍵及びグループ鍵を更新する。

グループ内の通信では新しいグループ鍵により暗号化が行われる。

[0075] 以上の加入プロトコルを一般化した処理流れ図を図8に示す。図8において、1ー6はl＝1の場合、7ー13はlが2以上の場合であり、2及び8では木構造データの更新(70)、3及び9がキャプテンの選択(71)、4及び10が新鍵の共有(72)、5ー6及び11ー13が新鍵の配布(73)の各処理である。

実施例 3

[0076] メンバ加入時の新鍵共有処理(72)及び新鍵配布処理(73)の別実施例を次に示す。(本方式をFDLKHのdistributed方式と呼ぶ。)

まず、新鍵共有処理(72)において、実施例2のように加入メンバM<3,3>(50)が各キャプテンM<3,2>, M<3,0>, M<3,4>と鍵の共有を行うのではなく、加入メンバM<3,3>(50)は最下位のキャプテンM<3,2>(51)と新鍵を共有し、次いでそのキャプテンM<3,2>(51)とM<3,0>(52)、M<3,0>(52)とM<3,4>(53)が順次新鍵を共有する。

[0077] すなわち、

M<3,3>←→ M<3,2> : K'<2,1>

M<3,2>←→ M<3,0> : K'<1,0>

M<3,0>←→ M<3,4> : K'<0,0>

(←→は共有を示す)

のように、各メンバ間でサブグループ鍵、グループ鍵を共有する。

[0078] そして、新鍵配布処理(73)では、実施例2と同様に、

M<3,0>→ T<1,0> : E(K<1,0>,K'<1,0>)

M<3,4>→ T<0,0> : E(K<0,0>,K'<0,0>)

としてキャプテンが部分木に新鍵を配布する。

また、本実施例の新鍵共有処理(72)では、加入メンバM<3,3>はK'<2,1>だけを受け取っているため、メンバM<3,2>(51)及びM<3,0>(52)が1つ上位の新鍵を下位の鍵で暗号化し、順次送信するように構成する。すなわち、

M<3,2>→ M<3,3>: E(K'<2,1>,K'<1,0>)

M<3,0>→ M<3,3>: E(K'<1,0>,K'<0,0>)

の処理を新鍵配布処理(73)で合わせて行う。以上により、加入メンバ(50)にも全てのサブグループ鍵及びグループ鍵が配布され、各メンバは鍵の更新を行うことが

できる。

[0079] 以上の加入プロトコルを一般化した処理流れ図を図9に示す。図9において、1ー6はl＝1の場合、7ー15はlが2以上の場合であり、2及び8では木構造データの更新(70)、3及び9がキャプテンの選択(71)、4及び10ー11が新鍵の共有(72)、5ー6及び12ー15が新鍵の配布(73)の各処理である。

実施例 4

[0080] 次に、実施例2に対応するメンバが脱退する際の処理(dedicated方式)を説述する。図7はメンバが脱退する場合の脱退プロトコルである。

上述した通り、メンバ(60)が脱退する場合、加入脱退検知部(11)で検知すると、キャプテン当否判定部(13)の処理を各メンバが行うことにより、木構造におけるキャプテンが選択(80)される。

[0081] そして、新鍵共有処理(81)に進む。ここで、新鍵の生成・変更にはDH鍵共有を用いる。メンバ加入の際には加入メンバと各キャプテンがDH鍵共有を行う。各キャプテンは、DH鍵共有で共有した値を暗号学的に安全な一方向性ハッシュ関数hに入力し、その結果得られた出力を部分木の根ノードに割り当てる共通鍵暗号の鍵とする。

[0082] 図5のメンバ脱退の例では、部分木T<2,0>のキャプテンとして選択されたM<3,1>(61)と、それ以外のキャプテンとして選択されたM<3,3>(62), M<2,3>(63)が前述の数1の結果を以下のように送信する。

$M\langle 3,1\rangle \rightarrow [M\langle 3,3\rangle, M\langle 2,3\rangle] : Y_{M\langle 3,1\rangle}$

$M\langle 3,3\rangle \rightarrow M\langle 3,1\rangle : Y_{M\langle 3,3\rangle}$

$M\langle 2,3\rangle \rightarrow M\langle 3,1\rangle : Y_{M\langle 2,3\rangle}$

[0083] 各メンバにおいて、新鍵共有部(14)において数1の結果を受信すると、DH鍵共有のベキ乗剰余演算を行い、その結果の値をハッシュ関数hに入力して演算する。これにより、M<3,1>と、M<3,3>、M<2,3>とは、それぞれ以下の鍵を共有することができる。

$K'\langle 1,0\rangle = h(g^{XM\langle 3,1\rangle XM\langle 3,3\rangle} \bmod p)$

$K'\langle 0,0\rangle = h(g^{XM\langle 3,1\rangle XM\langle 2,3\rangle} \bmod p)$

[0084] 次いで、新鍵配布処理(82)を新鍵配布部(15)で行う。メンバ脱退の際は、部分木の根ノードから1つ下層のノードの鍵を使って新しい鍵を暗号化し、部分木のメンバ

に配布する。さらにこの配布された新しい鍵を使って、脱退メンバの親ノードを根とする部分木のキャプテンが、各部分木に不足している鍵を暗号化して配布する。

[0085] 図5では、M<3,3>とM<2,3>がそれぞれ、新しい鍵K'<1,0>, K'<0,0>を、鍵K<2,1>, K<1,

1>で暗号化して各部分木に配布する。すなわち、

M<3,3>→ T<2,1> : E(K<2,1>,K'<1,0>)

M<2,3>→ T<1,1> : E(K<1,1>,K'<0,0>)

そしてM<3,1>が部分木T<1,0>に不足している鍵K'<0,0>を、先に配布されたK'<1,0>を使って暗号化し配布する。すなわち、

M<3,1>→ T<1,0> : E(K'<1,0>,K'<0,0>)

のように配布する。

[0086] そして、鍵配布の後、グループの各メンバは新しい鍵を復号し、該当するノードに割り当てて鍵更新する。

さらに各メンバは木構造データ更新部(12)により木構造データの更新処理(83)を行い、脱退処理を完了する。

[0087] 以上の脱退プロトコルを一般化した処理流れ図を図10に示す。図10において、1ー3はl＝1の場合、4ー10はl＝2の場合、11ー18はlが3以上の場合である。そして、l＝1の場合には根ノードを削除して部分木の名前を更新する処理であり、その他の場合には、5及び12がキャプテンの選択(80)、6及び13が新鍵の共有(81)、7ー9及び14ー17が新鍵の配布(82)、10及び18が木構造データの更新(83)の各処理である。

実施例 5

[0088] メンバが脱退する場合の別プロトコル(distributed方式)として、次のように構成することもできる。これは実施例3に示す加入プロトコルに対応する方法である。

実施例4において、新鍵共有部(14)がM<3,1>(61)と、M<3,3>(62)、M<2,3>(63)とが鍵をK'<1,0>及びK'<0,0>を共有したが、本実施例では、M<3,1>(61)とM<3,3>(62)がK'<1,0>を、M<3,3>(62)とM<2,3>(63)とがK'<0,0>を共有する。

[0089] そして、新鍵配布処理(82)ではM<3,3>(62)が部分木T<2,1>にK<2,1>で暗号化し

た新鍵K'<1,0>を、M<2,3>(63)が部分木T<1,1>にK<1,1>で暗号化した新鍵K'<0,0>をそれぞれ送信する。

さらに、M<3,3>(62)は新鍵K'<0,0>をK'<1,0>で暗号化して部分木T<1,0>に送信する。

[0090] 以上の脱退プロトコルを一般化した処理流れ図を図11に示す。図11において、1ー3はl＝1の場合、4ー10はl＝2の場合、11ー18はlが3以上の場合である。そして、l＝1の場合には根ノードを削除して部分木の名前を更新する処理であり、その他の場合には、5及び12がキャプテンの選択(80)、6及び13が新鍵の共有(81)、7ー9及び14ー17が新鍵の配布(82)、10及び18が木構造データの更新(83)の各処理である。

評価実験

[0091] 次に本発明に係るFDLKHの評価実験結果を示す。実験として、鍵の数、およびメンバ加入・脱退時のグループ鍵更新にかかるコスト(DH鍵共有の回数、共通鍵暗号による暗号化・復号の回数)を比較する。

比較対象として鍵を集中管理する鍵管理サーバを用いた2つの鍵管理方式(Flat, LKH)のコストを併せて示す。ここで、Flatは鍵管理サーバとメンバの間で個別の共通鍵(以下、個別鍵と呼ぶ。)を共有し、その他の階層的な鍵の割り当てを行わないスター型のnaive な方式を指し、LKHは同じく鍵管理サーバとメンバの間で個別鍵を共有し、さらにグループ鍵更新のための鍵を木構造で管理する従来の技術として示した方式を指す。

[0092] なお評価の簡単化のため、LKHで用いる鍵の木の度数(各ノードが持つ子の数)は2とし、LKH、FDLKHともにメンバの加入後もしくは脱退前のメンバ数nは2のベキ数、鍵の木は完全2分木とする。

このとき、加入・脱退メンバをM<l,m>とすると$l = \log_2 n$が成り立つ。

[0093] 表1は、Flat、LKH、FDLKHの3方式におけるシステム全体の鍵の総種類数と、1メンバが保持する鍵の数を示している。FDLKHは鍵管理サーバを用いず、ゆえにメンバ毎の個別鍵も存在しないため、1メンバあたりの鍵の数はLKHよりも1つ少なく、鍵の総種類数はLKHの約半分となっている。

[0094] [表1]

	鍵の全体数	1メンバ当たりの鍵の数
Flat	n+1	2
LKH	2n-1	l+1
FDLKH	n-1	l

[0095] 次に、メンバが加入する際のコストを表2に示す。なお、表2のRegular membersは、キャプテンと加入メンバを除いたその他のメンバを示し、回数はそれぞれ1ノード当たりで表している。

M<l,m>がグループに加入する際、加入メンバ(newcomer)が個別鍵でl 回の復号を行うLKH に対し、FDLKHでは加入メンバと各キャプテンが延べl 回のDH鍵共有を行う。

本発明に係るFDLKHでは鍵管理サーバを必要としない方式であり、サーバレスである代わりに、加入メンバの計算量はLKHに比べて増加する。ただし、FlatやLKHでは鍵管理サーバ(Key server)とメンバ(Members)との間の個別鍵共有のコストが別途必要であり、全体としてのコストはFDLKHが低くなる。

また、distributed方式は、dedicated方式に比して、1メンバに偏っていた加入・脱退プロトコルの際の処理を、さらに分散化させた方式であることが示されている。

[0096] [表2]

	ノード	DH鍵共有回数	暗号化回数	復号化回数
Flat	Newcomer			1
	Member			1
	Key server		2	
LKH	Newcomer			1
	Member			2
	Key server		21	
FDLKH (dedicated)	Newcomer	1		
	Regular member			2
	Captain	1	1	(l-1)/2
FDLKH (distributed)	Newcomer	1		l-1
	Regular member			2
	Captain	(2l-1)/2	(2l-2)/2	(l-1)(l-2)/2l

[0097] メンバの復号回数はLKHでは平均2回以下である。FDLKHでも同様にキャプテン

や加入・

脱退メンバ以外の一般メンバ(regular members)の復号回数は平均2 回以下である。LKHでは鍵管理サーバの暗号化回数は2l回であり、このうち半数は部分木への鍵配布のための暗号化である。

FDLKH(dedicated方式)ではこの鍵配布のための暗号化を各キャプテンが1回ずつ(延べl-1回)行う。また、キャプテンの平均復号回数は(0+1+・・・+l-1)/l=(l-1)/2である。

図12はFDLKH(dedicated方式)の、図13はFDLKH(distributed方式)の、それぞれメンバ加入において、メンバ数に対する共通鍵暗号系のコスト(暗号化回数と復号回数の和)の変化を示している。

[0098] 次に、メンバ脱退時のコストを検討する。M<l,m>がグループから脱退する際には表3に示すようにFlat 方式では、鍵管理サーバが脱退メンバ(seceder)以外のn-1個の個別鍵で新しいグループ鍵を暗号化して各メンバに配布する必要があり、スケーラビリティは低い。

LKHでは鍵管理に木構造を導入し、鍵管理サーバの暗号化回数を2l 回に抑えている。

[0099] FDLKH では脱退メンバの親ノードを根とする部分木のキャプテン(generous captain)がl-1回のDH鍵共有とl-2回の鍵配布のための暗号化を行う。それ以外の各キャプテンは1回のDH鍵共有と、1回の暗号化(延べl-1回)を行う。キャプテンの平均復号回数は(0+1+・・・+l-2)/(l-1)=(l-2)/2である。

図14はFDLKH(dedicated方式)の、図15はFDLKH(distributed方式)の、メンバ脱退において、メンバ数に対する共通鍵暗号系のコストの変化を示している。また、Buddy captainは、脱退メンバに最も近い(実施例5におけるM<3,1>(61))キャプテンを示している。

[0100] [表3]

		回数		
Flat	Seceder			
	Member			1
	Key server		n-1	
LKH	Seceder			
	Member			2
	Key server		21	
FDLKH (dedicated)	Seceder			
	Regular member			2
	Captain	1	1	(1-2)/2
	Buddy Captain	1-1	1-2	
FDLKH (distributed)	Seceder			
	Regular member			2
	Captain	(21-2)/1	(21-3)/1	(1-1)(1-2)/21

請求の範囲

[1] 通信ネットワーク中で複数のメンバが加入可能なグループを組織し、該グループ内で通信データの暗号化もしくは認証に用いるグループ鍵を共有するとともに、グループ鍵を最上位の根に割り当て、サブグループ鍵を枝の分岐点であるノードに割り当て、各メンバを最下位の部分木の先端である葉に割り当てて、各メンバはグループ鍵及びグループ鍵から自己に至るまでの全てのサブグループ鍵を保持して通信を行う通信方法であって、

あらかじめグループに属する各メンバにはグループ全体の木構造データ及び、グループ鍵、全てのサブグループ鍵を記憶させておき、

新しいメンバの加入を各メンバが加入脱退検知手段により検知すると、

各メンバが、木構造データ更新手段により、加入メンバを所定の規則に従って木構造の葉に割り当て、自己の記憶する木構造データを更新する木構造データ更新ステップ、

各メンバが、キャプテン当否判定手段により、新しい木構造データから所定の規則に従って自己が部分木のキャプテンとなるか否かを判定するキャプテン当否判定ステップ、

該キャプテンが、新鍵生成配布手段により、少なくとも自己の部分木の各メンバとの間で新鍵を生成し配布する新鍵生成配布ステップ

の各ステップを含むことを特徴とする非集中型鍵管理方式を用いた通信方法。

[2] 前記通信方法における新鍵生成配布ステップが、

該加入メンバと各キャプテンとが、新鍵共有手段により、互いに新しいグループ鍵又はサブグループ鍵の生成情報を通信し、新鍵を生成して共有する新鍵共有ステップ、

各キャプテンが、新鍵配布手段により、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布する新鍵配布ステップ

の各ステップからなることを特徴とする

請求項1に記載の非集中型鍵管理方式を用いた通信方法。

[3] 前記通信方法における新鍵生成配布ステップが、

加入メンバと最下位のキャプテンが新鍵を共有すると共に、順次下位のキャプテンが1階層上位のキャプテンと新鍵を共有する新鍵共有ステップ、

各キャプテンが、新鍵配布手段により、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、下位のキャプテンから順次に、該キャプテンが属する部分木の新鍵で1階層上位の新鍵を暗号化して加入メンバに送信する新鍵配布ステップ

の各ステップからなることを特徴とする

請求項1に記載の非集中型鍵管理方式を用いた通信方法。

[4] 前記木構造データ更新ステップにおいて、加入メンバを葉に割り当てる所定の規則が、

木構造全体の最下位でかつ最右側のノードにおける最左側の葉、又は最下位でかつ最左側のノードにおける最右側の葉として割り当てる

請求項1ないし3に記載の非集中型鍵管理方式を用いた通信方法。

[5] 前記キャプテン当否判定ステップにおいて、キャプテンとなるか否かを判定する所定の規則が、

ある部分木におけるキャプテンとなるメンバは、その部分木の上位側からみて加入メンバがいる側の枝と反対側の枝の葉のメンバから選択する

請求項1ないし4に記載の非集中型鍵管理方式を用いた通信方法。

[6] 前記木構造が2分木である

請求項1ないし3に記載の非集中型鍵管理方式を用いた通信方法。

[7] 通信ネットワーク中で複数のメンバが加入可能なグループを組織し、該グループ内で通信データの暗号化もしくは認証に用いるグループ鍵を共有するとともに、グループ鍵を最上位の根に割り当て、サブグループ鍵を枝の分岐点であるノードに割り当て、各メンバを最下位の部分木の先端である葉に割り当てて、各メンバはグループ鍵及びグループ鍵から自己に至るまでの全てのサブグループ鍵を保持して通信を行う通信方法であって、

あらかじめグループに属する各メンバにはグループ全体の木構造データ及び、グループ鍵、全てのサブグループ鍵を記憶させておき、

メンバの脱退を各メンバが加入脱退検知手段により検知すると、

各メンバが、キャプテン当否判定手段により、脱退メンバを除いた木構造データから所定の規則に従って自己が部分木のキャプテンとなるか否かを判定するキャプテン当否判定ステップ、

該キャプテンが、新鍵生成配布手段により、少なくとも自己の部分木のメンバ及び他のキャプテンとの間で新鍵を生成し配布する新鍵生成配布ステップ

各メンバが、木構造データ更新手段により、所定の規則に従って脱退メンバの属する部分木のメンバを葉として再割り当てし、自己の記憶する木構造データを更新する木構造データ更新ステップ

の各ステップを含むことを特徴とする非集中型鍵管理方式を用いた通信方法。

[8] 前記通信方法における新鍵生成配布ステップが、

脱退メンバの生じた最下位の部分木のキャプテンと、脱退メンバの属する部分木のその他全てのキャプテンとが、新鍵共有手段により、互いに新しいグループ鍵又はサブグループ鍵の生成情報を通信し、新鍵を生成して共有する新鍵共有ステップ、

各キャプテンが、新鍵配布手段により、生成された新鍵を1階層下位の従前のサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、脱退メンバの生じた最下位の部分木のキャプテンが、新鍵配布手段により、不足している新鍵をその部分木の従前のサブグループ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布ステップ

の各ステップからなることを特徴とする

請求項7に記載の非集中型鍵管理方式を用いた通信方法。

[9] 前記通信方法における新鍵生成配布ステップが、

脱退メンバの生じた最下位の部分木のキャプテンから順次に、下位のキャプテンが1階層上位のキャプテンと新鍵を共有する新鍵共有ステップ、

各キャプテンが、新鍵配布手段により、自己の部分木の各メンバに新鍵を配布すると共に、脱退メンバの生じた部分木のキャプテンが、新鍵配布手段により、不足している新鍵をその部分木の従前のサブグループ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布ステップ

の各ステップからなることを特徴とする

請求項7に記載の非集中型鍵管理方式を用いた通信方法。

[10] 前記キャプテン当否判定ステップにおいて、キャプテンとなるか否かを判定する所定の規則が、

ある部分木におけるキャプテンとなるメンバは、その部分木の上位側からみて加入メンバがいる側の枝と反対側の枝の葉のメンバから選択する

請求項7ないし9に記載の非集中型鍵管理方式を用いた通信方法。

[11] 前記木構造が2分木である

請求項7ないし10に記載の非集中型鍵管理方式を用いた通信方法。

[12] 通信ネットワーク中で複数のメンバが加入可能なグループを組織し、該グループ内で通信データの暗号化もしくは認証に用いるグループ鍵を共有するとともに、グループ鍵を最上位の根に割り当て、サブグループ鍵を枝の分岐点であるノードに割り当て、各メンバを最下位の部分木の先端である葉に割り当てて、各メンバはグループ鍵及びグループ鍵から自己に至るまでの全てのサブグループ鍵を保持して通信を行う通信システムであって、

各メンバとなる端末装置に、

グループ全体の木構造データ及び、グループ鍵、全てのサブグループ鍵を記憶する記憶手段と、

新しいメンバの加入又はメンバの脱退を検知する加入脱退検知手段と、

加入メンバを所定の規則に従って木構造の葉に割り当て、自己の記憶する木構造データを更新するか、又は所定の規則に従って脱退メンバの属する部分木のメンバを葉として再割り当てし、自己の記憶する木構造データを更新するかの少なくともいずれかの処理を行う木構造データ更新手段と、

木構造データから所定の規則に従って自己が部分木のキャプテンとなるか否かを判定するキャプテン当否判定手段と、

キャプテンとなった場合に、少なくとも自己の部分木のメンバとの間で新鍵を生成し配布する新鍵生成配布手段と

を備えて構成することを特徴とする

非集中型鍵管理方式を用いた通信システム。

[13] 前記通信システムにおける端末装置の新鍵生成配布手段が、

該加入メンバ及びキャプテン間で、互いに新しいグループ鍵又はサブグループ鍵の生成情報を通信し、新鍵を生成して共有する新鍵共有手段と、

キャプテンの時に、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布する新鍵配布手段と

からなる請求項12に記載の非集中型鍵管理方式を用いた通信システム。

[14] 前記通信システムにおける端末装置の新鍵生成配布手段が、

加入メンバと最下位のキャプテンが新鍵を共有すると共に、順次下位のキャプテンが1階層上位のキャプテンと新鍵を共有する新鍵共有手段と、

キャプテンの時に、新鍵を対応する従前のグループ鍵又はサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、下位のキャプテンから順次に、該キャプテンが属する部分木の新鍵で1階層上位の新鍵を暗号化して加入メンバに送信する新鍵配布手段と

からなる請求項12に記載の非集中型鍵管理方式を用いた通信システム。

[15] 前記通信システムにおける端末装置の新鍵生成配布手段が、

脱退メンバの生じた最下位の部分木のキャプテンと、脱退メンバの属する部分木のその他全てのキャプテンとが、互いに新しいグループ鍵又はサブグループ鍵の生体情報を通信し、新鍵を生成して共有する新鍵共有手段と、

キャプテンの時に、生成された新鍵を1階層下位の従前のサブグループ鍵で暗号化して部分木の各メンバに配布すると共に、脱退メンバの生じた最下位の部分木のキャプテンが、不足している新鍵をその部分木の従前のサブグループ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布手段と

からなる請求項12に記載の非集中型鍵管理方式を用いた通信システム。

[16] 前記通信システムにおける端末装置の新鍵生成配布手段が、

脱退メンバの生じた最下位の部分木のキャプテンから順次に、下位のキャプテンが1階層上位のキャプテンと新鍵を共有する新鍵共有手段と、

キャプテンの時に、新鍵配布手段により、自己の部分木の各メンバに新鍵を配布す

ると共に、脱退メンバの生じた部分木のキャプテンが、不足している新鍵をその部分木の従前のサブグループ鍵で暗号化して、当該部分木の各メンバに配布する新鍵配布手段と

からなる請求項12に記載の非集中型鍵管理方式を用いた通信システム。

[17] 前記木構造データ更新手段で用いる加入メンバを葉に割り当てる所定の規則が、

木構造全体の最下位でかつ最右側のノードにおける最左側の葉、又は最下位でかつ最左側のノードにおける最右側の葉として割り当てる

請求項12ないし16に記載の非集中型鍵管理方式を用いた通信システム。

[18] 前記キャプテン当否判定手段で用いるキャプテンとなるか否かを判定する所定の規則が、

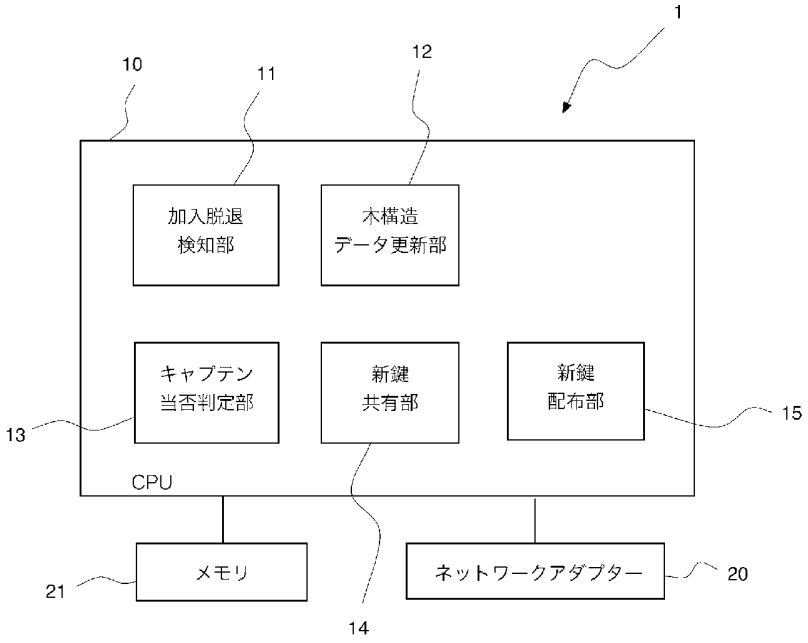
ある部分木におけるキャプテンとなるメンバは、その部分木の上位側からみて加入メンバがいる側の枝と反対側の枝の葉のメンバから選択する

請求項12ないし17に記載の非集中型鍵管理方式を用いた通信システム。

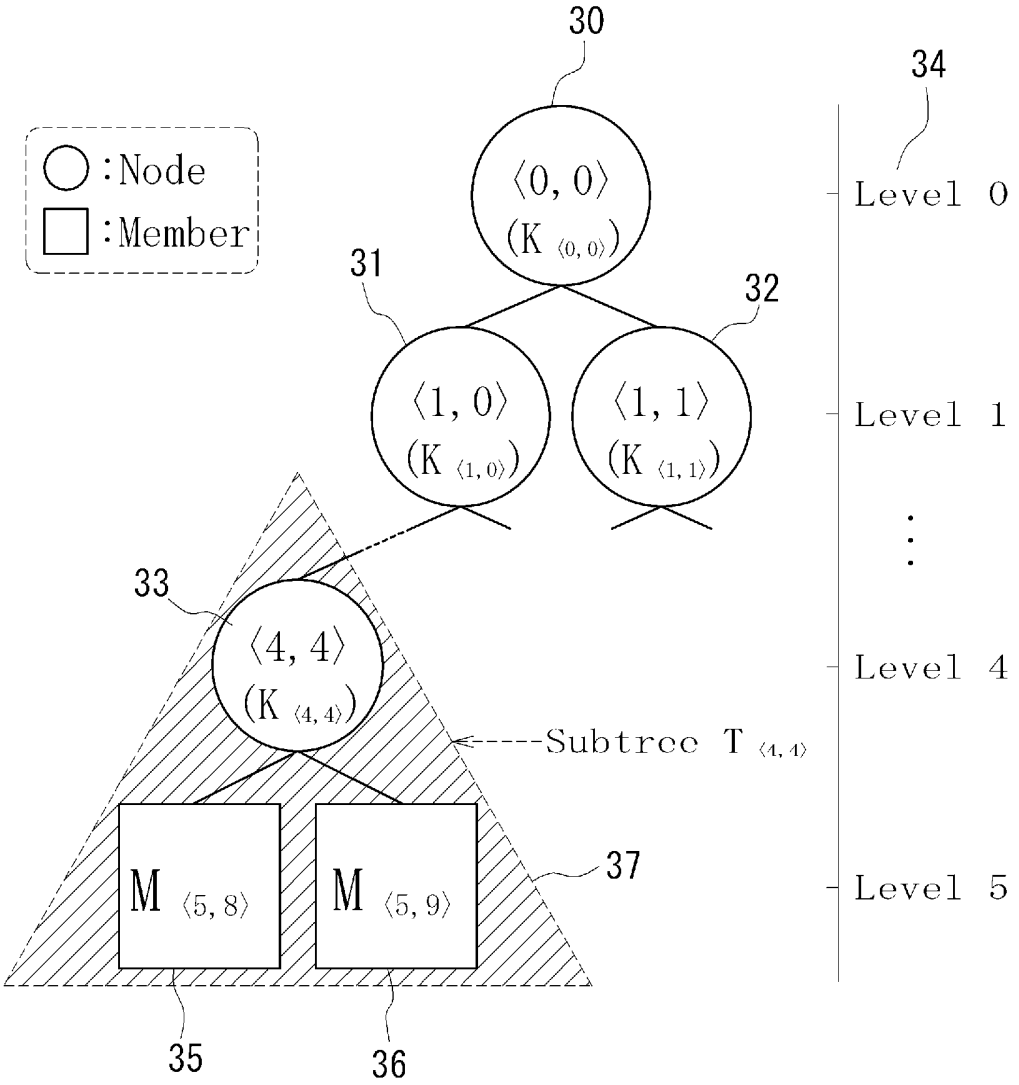
[19] 前記木構造が2分木である

請求項12ないし18に記載の非集中型鍵管理方式を用いた通信システム。

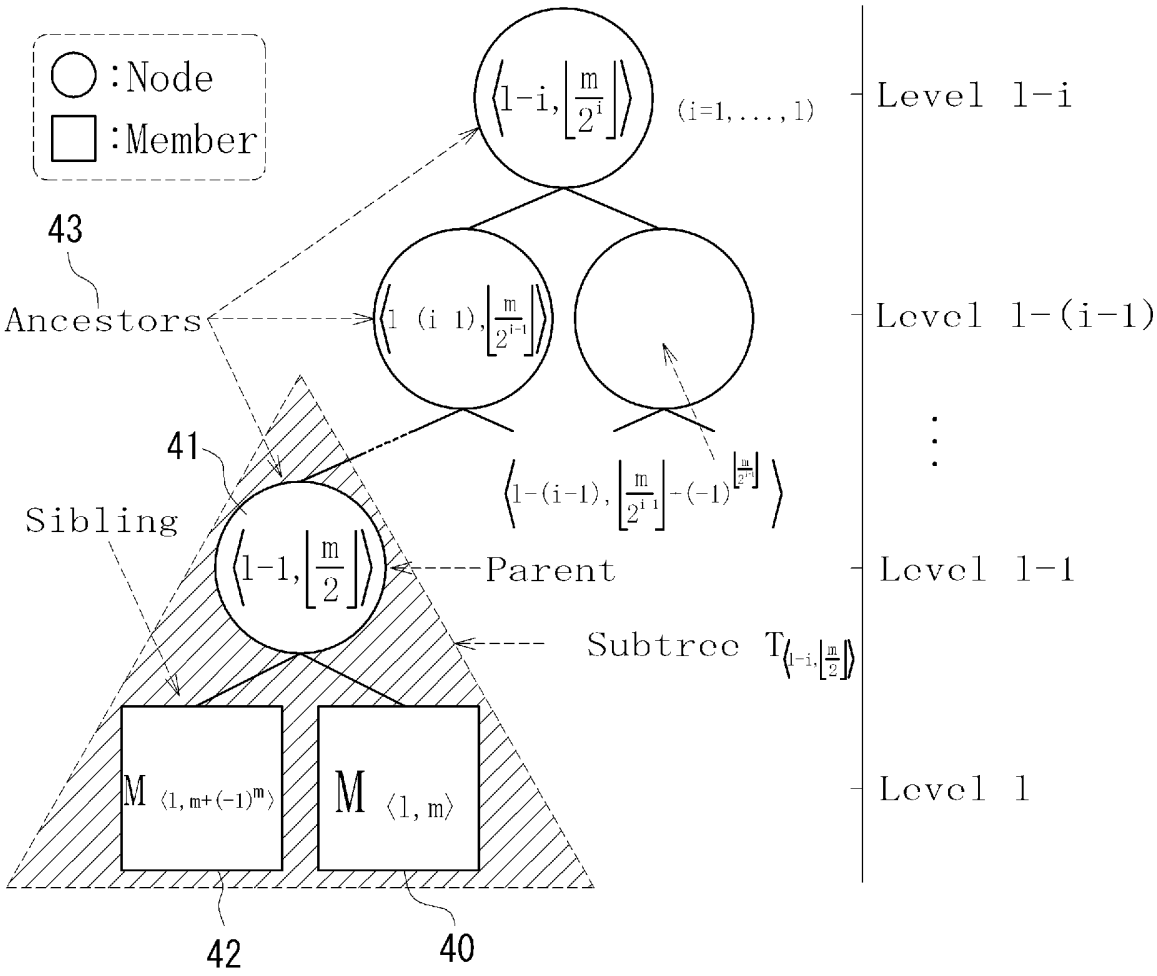
[図1]


1
10
11
12
加入脱退
検知部
木構造
データ更新部
キャプテン
当否判定部
新鍵
共有部
新鍵
配布部
13
15
CPU
メモリ
ネットワークアダプター
21
20
14

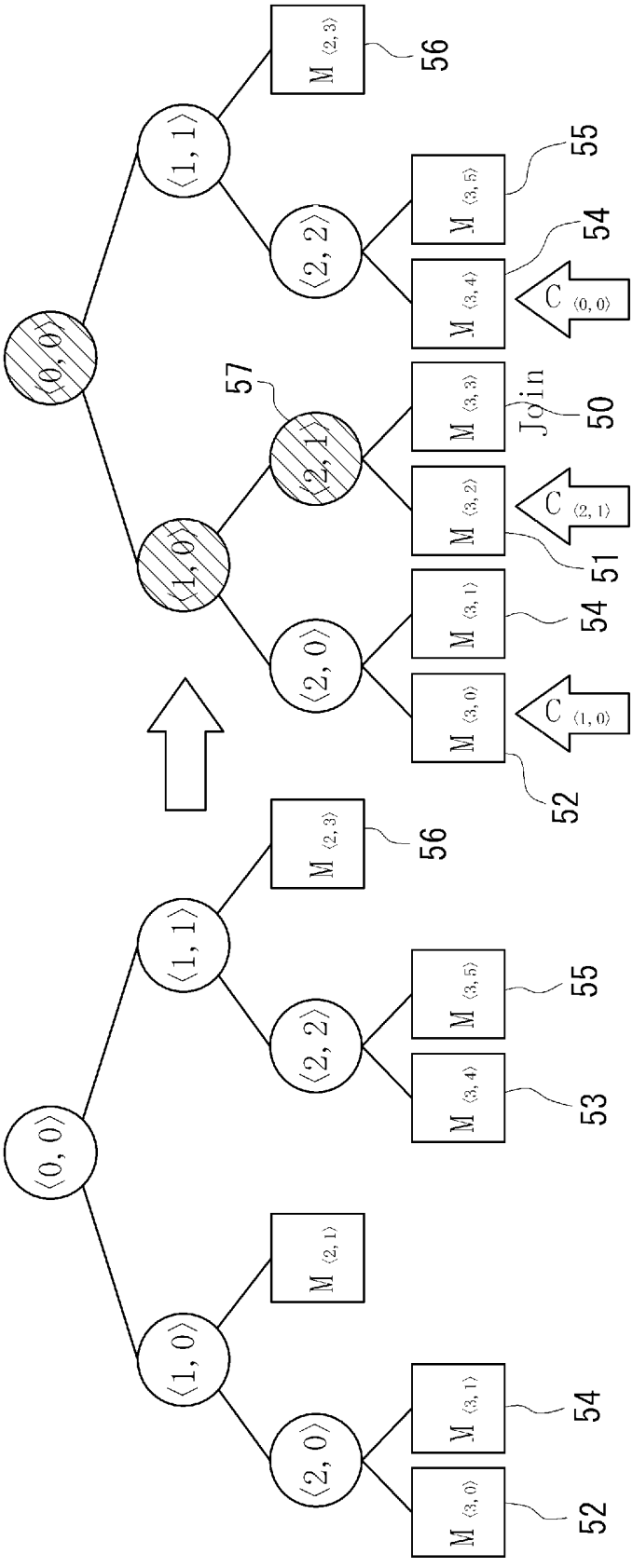
[図2]


30
34
:Node
:Member
⟨0, 0⟩
(K ⟨0, 0⟩)
Level 0
31
32
⟨1, 0⟩
(K ⟨1, 0⟩)
⟨1, 1⟩
(K ⟨1, 1⟩)
Level 1
33
⟨4, 4⟩
(K ⟨4, 4⟩)
Level 4
Subtree T ⟨4, 4⟩
M ⟨5, 8⟩
M ⟨5, 9⟩
37
Level 5
35
36

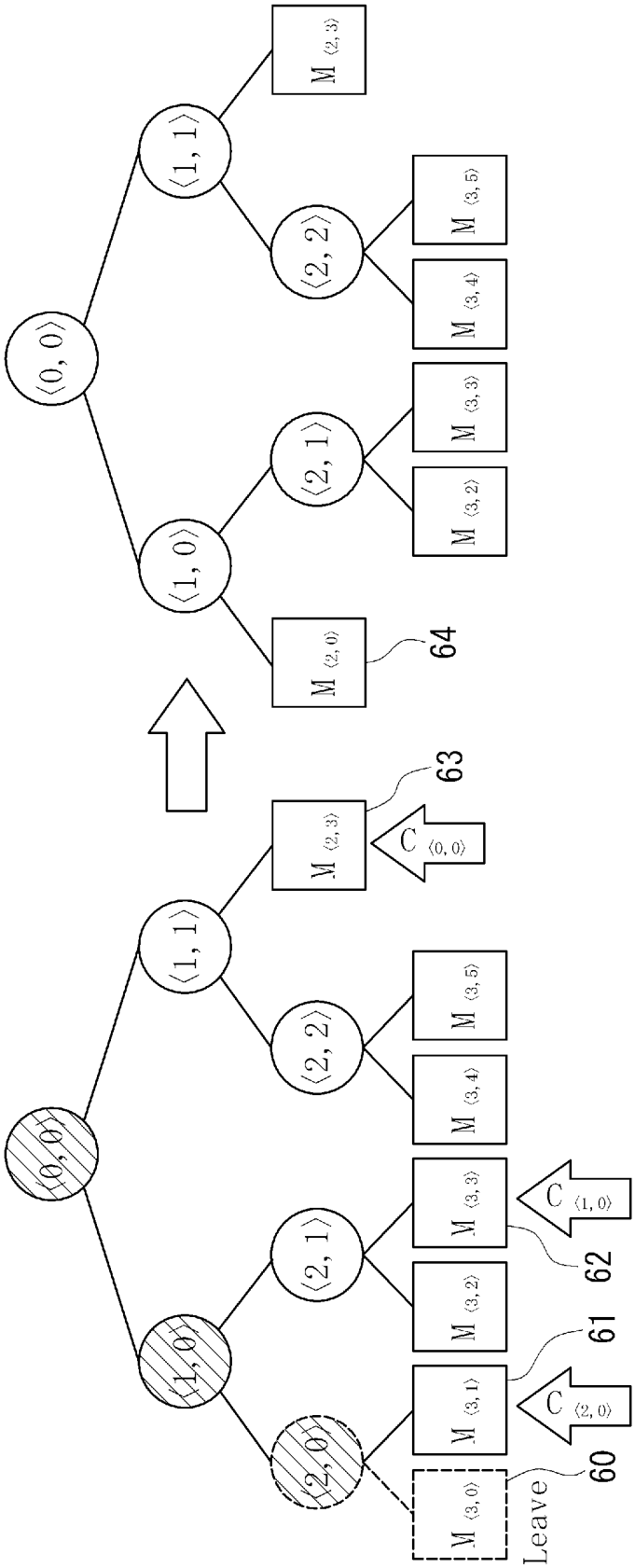
[図3]


:Node
:Member
43
Ancestors
41
Sibling
Parent
Subtree
Level l-i
Level l-(i-1)
Level l-1
Level l
42
40

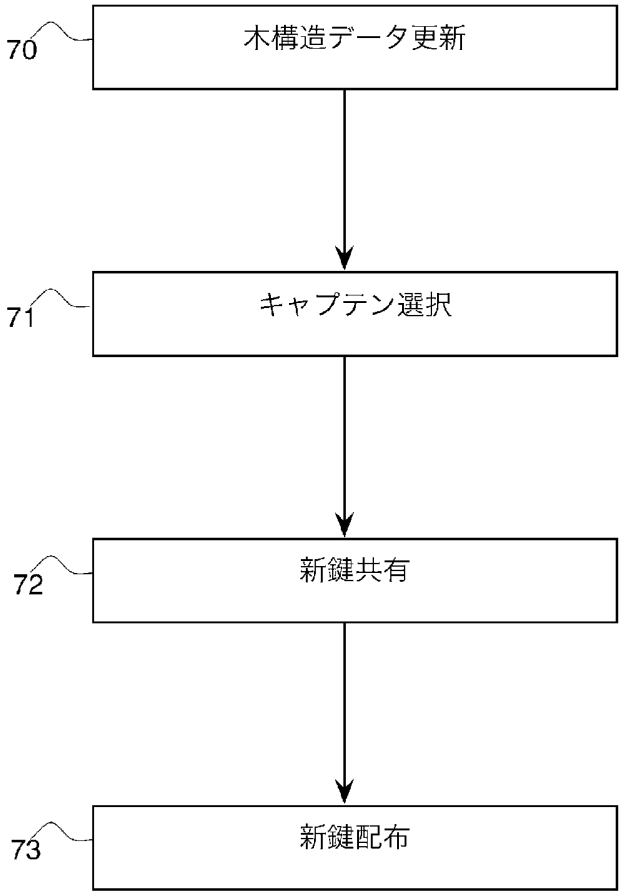
[図4]


⟨0, 0⟩
⟨1, 0⟩
⟨2, 0⟩
⟨2, 1⟩
⟨1, 1⟩
⟨2, 2⟩
M ⟨3, 0⟩
M ⟨3, 1⟩
M ⟨3, 2⟩
M ⟨3, 3⟩
M ⟨3, 4⟩
M ⟨3, 5⟩
M ⟨2, 1⟩
M ⟨2, 3⟩
C ⟨1, 0⟩
C ⟨2, 1⟩
C ⟨0, 0⟩
Join
50
51
52
53
54
55
56
57

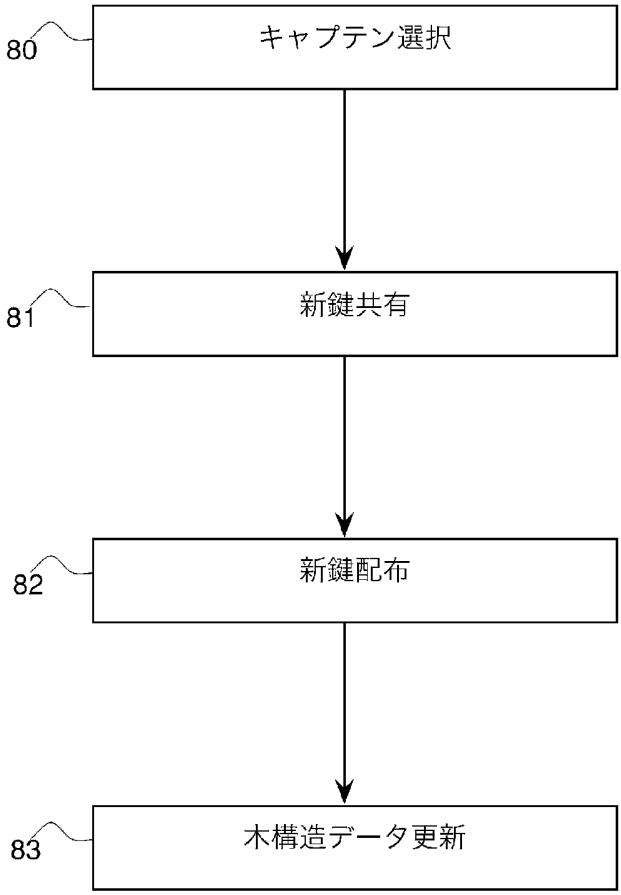
[図5]


⟨0, 0⟩
⟨1, 0⟩
⟨1, 1⟩
⟨2, 0⟩
⟨2, 1⟩
⟨2, 2⟩
M ⟨3, 0⟩
M ⟨3, 1⟩
M ⟨3, 2⟩
M ⟨3, 3⟩
M ⟨3, 4⟩
M ⟨3, 5⟩
M ⟨2, 0⟩
M ⟨2, 3⟩
C ⟨2, 0⟩
C ⟨1, 0⟩
C ⟨0, 0⟩
Leave
60
61
62
63
64

[図6]



[図7]



[図8]

Join Protocol on the Dedicated Strategy

(1) **if** $(l = 1)$
(2) **Update** $\mathrm{T}_{\langle 0,0\rangle}$;
(3) **Select** $\mathrm{C}_{\langle 0,0\rangle}$;
(4) $\mathrm{M}_{\langle 1,1\rangle} \leftrightarrow \mathrm{C}_{\langle 0,0\rangle} : \mathrm{K'}_{\langle 0,0\rangle}$;
(5)* $\mathrm{C}_{\langle 0,0\rangle} \rightarrow \mathrm{T}_{\langle 1,0\rangle} : \mathrm{E}(\mathrm{K}_{\langle 1,0\rangle}, \mathrm{K'}_{\langle 0,0\rangle})$;
(6) $\mathrm{K}_{\langle 0,0\rangle} := \mathrm{K'}_{\langle 0,0\rangle}$;

(7) **else if** $(l \geq 2)$
(8) **Update** $\mathrm{T}_{\langle l-1,\lfloor \frac{m}{2} \rfloor\rangle}$;
(9) **Select** $\mathrm{C}_{\langle l-i,\lfloor \frac{m}{2^i} \rfloor\rangle}$;
(10) $\mathrm{M}_{\langle l,m\rangle} \leftrightarrow \mathrm{C}_{\langle l-i,\lfloor \frac{m}{2^i} \rfloor\rangle} : \mathrm{K'}_{\langle l-i,\lfloor \frac{m}{2^i} \rfloor\rangle}$;
(11) $\mathrm{C}_{\langle l-j,\lfloor \frac{m}{2^j} \rfloor\rangle} \rightarrow \mathrm{T}_{\langle l-j,\lfloor \frac{m}{2^j} \rfloor\rangle} :$
$\mathrm{E}(\mathrm{K}_{\langle l-j,\lfloor \frac{m}{2^j} \rfloor\rangle}, \mathrm{K'}_{\langle l-j,\lfloor \frac{m}{2^j} \rfloor\rangle})$;
(12)* $\mathrm{C}_{\langle l-1,\lfloor \frac{m}{2} \rfloor\rangle} \rightarrow \mathrm{T}_{\langle l,m+(-1)^m\rangle} :$
$\mathrm{E}(\mathrm{K}_{\langle l,m+(-1)^m\rangle}, \mathrm{K'}_{\langle l-1,\lfloor \frac{m}{2} \rfloor\rangle})$;
(13) $\mathrm{K}_{\langle l-i,\lfloor \frac{m}{2^i} \rfloor\rangle} := \mathrm{K'}_{\langle l-i,\lfloor \frac{m}{2^i} \rfloor\rangle}$;

* if needed

[図9]

Join Protocol on the Distributed Strategy

(1) **if** $(l = 1)$

(2)-(6) Similar to the join protocol on the dedicated strategy

(7) **else if** $(l \geq 2)$

(8) **Update** $\mathrm{T}_{\langle l-1, \lfloor \frac{m}{2} \rfloor \rangle}$;

(9) **Select** $\mathrm{C}_{\langle l-i, \lfloor \frac{m}{2^i} \rfloor \rangle}$;

(10) $\mathrm{M}_{\langle l,m \rangle} \leftrightarrow \mathrm{C}_{\langle l-1, \lfloor \frac{m}{2} \rfloor \rangle} : \mathrm{K'}_{\langle l-1, \lfloor \frac{m}{2} \rfloor \rangle}$;

(11) $\mathrm{C}_{\langle l-(j-1), \lfloor \frac{m}{2^{j-1}} \rfloor \rangle} \leftrightarrow \mathrm{C}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle} :$
$\mathrm{K'}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle}$;

(12) $\mathrm{C}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle} \rightarrow \mathrm{T}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle} :$
$\mathrm{E}(\mathrm{K}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle}, \mathrm{K'}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle})$;

(13)* $\mathrm{C}_{\langle l-1, \lfloor \frac{m}{2} \rfloor \rangle} \rightarrow \mathrm{T}_{\langle l, m+(-1)^m \rangle} :$
$\mathrm{E}(\mathrm{K}_{\langle l, m+(-1)^m \rangle}, \mathrm{K'}_{\langle l-1, \lfloor \frac{m}{2} \rfloor \rangle})$;

(14) $\mathrm{C}_{\langle l-(j-1), \lfloor \frac{m}{2^{j-1}} \rfloor \rangle} \rightarrow \mathrm{M}_{\langle l,m \rangle} :$
$\mathrm{E}(\mathrm{K'}_{\langle l-(j-1), \lfloor \frac{m}{2^{j-1}} \rfloor \rangle}, \mathrm{K'}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle})$;

(15) $\mathrm{K}_{\langle l-i, \lfloor \frac{m}{2^i} \rfloor \rangle} := \mathrm{K'}_{\langle l-i, \lfloor \frac{m}{2^i} \rfloor \rangle}$;

$*$ if needed

[図10]

Leave Protocol on the Dedicated Strategy

(1) **if** $(l = 1)$
(2) **Remove** $\langle 0,0\rangle$;
(3) **Update** $\mathrm{T}_{\langle 1,m+(-1)^m\rangle}$;

(4) **else if** $(l = 2)$
(5) **Select** $\mathrm{C}_{\langle 1,\lfloor \frac{m}{2}\rfloor\rangle}$ and $\mathrm{C}_{\langle 0,0\rangle}$;
(6) $\mathrm{C}_{\langle 1,\lfloor \frac{m}{2}\rfloor\rangle} \leftrightarrow \mathrm{C}_{\langle 0,0\rangle}$: $\mathrm{K'}_{\langle 0,0\rangle}$;
(7)* $\mathrm{C}_{\langle 0,0\rangle} \rightarrow \mathrm{T}_{\langle 1,\lfloor \frac{m}{2}\rfloor+(-1)^{\lfloor \frac{m}{2}\rfloor}\rangle}$:
$\mathrm{E}(\mathrm{K}_{\langle 1,\lfloor \frac{m}{2}\rfloor+(-1)^{\lfloor \frac{m}{2}\rfloor}\rangle}, \mathrm{K'}_{\langle 0,0\rangle})$;
(8)* $\mathrm{C}_{\langle 1,\lfloor \frac{m}{2}\rfloor\rangle} \rightarrow \mathrm{T}_{\langle 2,m+(-1)^m\rangle}$:
$\mathrm{E}(\mathrm{K}_{\langle 2,m+(-1)^m\rangle}, \mathrm{K'}_{\langle 0,0\rangle})$;
(9) $\mathrm{K}_{\langle 0,0\rangle} := \mathrm{K'}_{\langle 0,0\rangle}$;
(10) **Update** $\mathrm{T}_{\langle 1,\lfloor \frac{m}{2}\rfloor\rangle}$;

(11) **else if** $(l \geq 3)$
(12) **Select** $\mathrm{C}_{\langle l-i,\lfloor \frac{m}{2^i}\rfloor\rangle}$;
(13) $\mathrm{C}_{\langle l-1,\lfloor \frac{m}{2}\rfloor\rangle} \leftrightarrow \mathrm{C}_{\langle l-j,\lfloor \frac{m}{2^j}\rfloor\rangle}$: $\mathrm{K'}_{\langle l-j,\lfloor \frac{m}{2^j}\rfloor\rangle}$;
(14)* $\mathrm{C}_{\langle l-j,\lfloor \frac{m}{2^j}\rfloor\rangle} \rightarrow \mathrm{T}_{\langle l-(j-1),\lfloor \frac{m}{2^{j-1}}\rfloor+(-1)^{\lfloor \frac{m}{2^{j-1}}\rfloor}\rangle}$:
$\mathrm{E}(\mathrm{K}_{\langle l-(j-1),\lfloor \frac{m}{2^{j-1}}\rfloor+(-1)^{\lfloor \frac{m}{2^{j-1}}\rfloor}\rangle}, \mathrm{K'}_{\langle l-j,\lfloor \frac{m}{2^j}\rfloor\rangle})$;
(15)* $\mathrm{C}_{\langle l-1,\lfloor \frac{m}{2}\rfloor\rangle} \rightarrow \mathrm{T}_{\langle l,m+(-1)^m\rangle}$:
$\mathrm{E}(\mathrm{K}_{\langle l,m+(-1)^m\rangle}, \mathrm{K'}_{\langle l-2,\lfloor \frac{m}{2^2}\rfloor\rangle})$;
(16) $\mathrm{C}_{\langle l-1,\lfloor \frac{m}{2}\rfloor\rangle} \rightarrow \mathrm{T}_{\langle l-k,\lfloor \frac{m}{2^k}\rfloor\rangle}$:
$\mathrm{E}(\mathrm{K'}_{\langle l-k,\lfloor \frac{m}{2^k}\rfloor\rangle}, \mathrm{K'}_{\langle l-(k+1),\lfloor \frac{m}{2^{k+1}}\rfloor\rangle})$;
(17) $\mathrm{K}_{\langle l-j,\lfloor \frac{m}{2^j}\rfloor\rangle} := \mathrm{K'}_{\langle l-j,\lfloor \frac{m}{2^j}\rfloor\rangle}$;
(18) **Update** $\mathrm{T}_{\langle l-1,\lfloor \frac{m}{2}\rfloor\rangle}$;

*if needed

[図11]

Leave Protocol on the Distributed Strategy

(1) **if** $(l = 1)$

(2)-(3) Similar to the leave protocol on the dedicated strategy

(4) **else if** $(l = 2)$

(5)-(10) Similar to the leave protocol on the dedicated strategy

(11) **else if** $(l \geq 3)$

(12) **Select** $\mathrm{C}_{\langle l-i, \lfloor \frac{m}{2^i} \rfloor \rangle}$;

(13) $\mathrm{C}_{\langle l-(j-1), \lfloor \frac{m}{2^{j-1}} \rfloor \rangle} \leftrightarrow \mathrm{C}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle} : \mathrm{K}'_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle}$;

(14)$*$ $\mathrm{C}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle} \rightarrow \mathrm{T}_{\langle l-(j-1), \lfloor \frac{m}{2^{j-1}} \rfloor + (-1)^{\lfloor \frac{m}{2^{j-1}} \rfloor} \rangle} :$
$\mathrm{E}(\mathrm{K}_{\langle l-(j-1), \lfloor \frac{m}{2^{j-1}} \rfloor + (-1)^{\lfloor \frac{m}{2^{j-1}} \rfloor} \rangle}, \mathrm{K}'_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle})$;

(15)$*$ $\mathrm{C}_{\langle l-1, \lfloor \frac{m}{2} \rfloor \rangle} \rightarrow \mathrm{T}_{\langle l, m+(-1)^m \rangle} :$
$\mathrm{E}(\mathrm{K}_{\langle l, m+(-1)^m \rangle}, \mathrm{K}'_{\langle l-2, \lfloor \frac{m}{2^2} \rfloor \rangle})$;

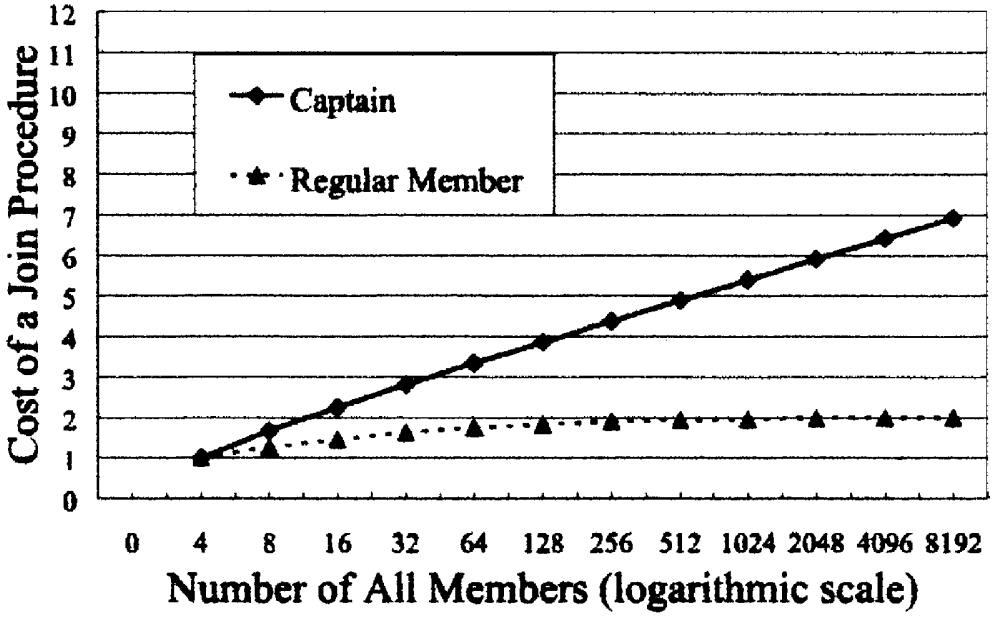
(16) $\mathrm{C}_{\langle l-k, \lfloor \frac{m}{2^k} \rfloor \rangle} \rightarrow \mathrm{T}_{\langle l-k, \lfloor \frac{m}{2^k} \rfloor \rangle} :$
$\mathrm{E}(\mathrm{K}'_{\langle l-k, \lfloor \frac{m}{2^k} \rfloor \rangle}, \mathrm{K}'_{\langle l-(k+1), \lfloor \frac{m}{2^{k+1}} \rfloor \rangle})$;

(17) $\mathrm{K}_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle} := \mathrm{K}'_{\langle l-j, \lfloor \frac{m}{2^j} \rfloor \rangle}$;

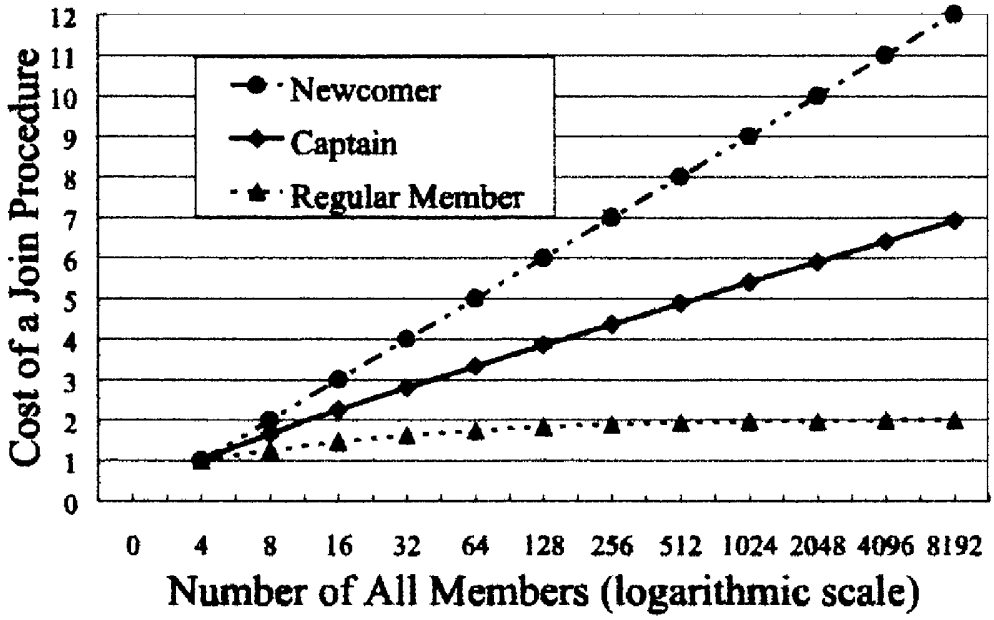
(18) **Update** $\mathrm{T}_{\langle l-1, \lfloor \frac{m}{2} \rfloor \rangle}$;

$*$if needed

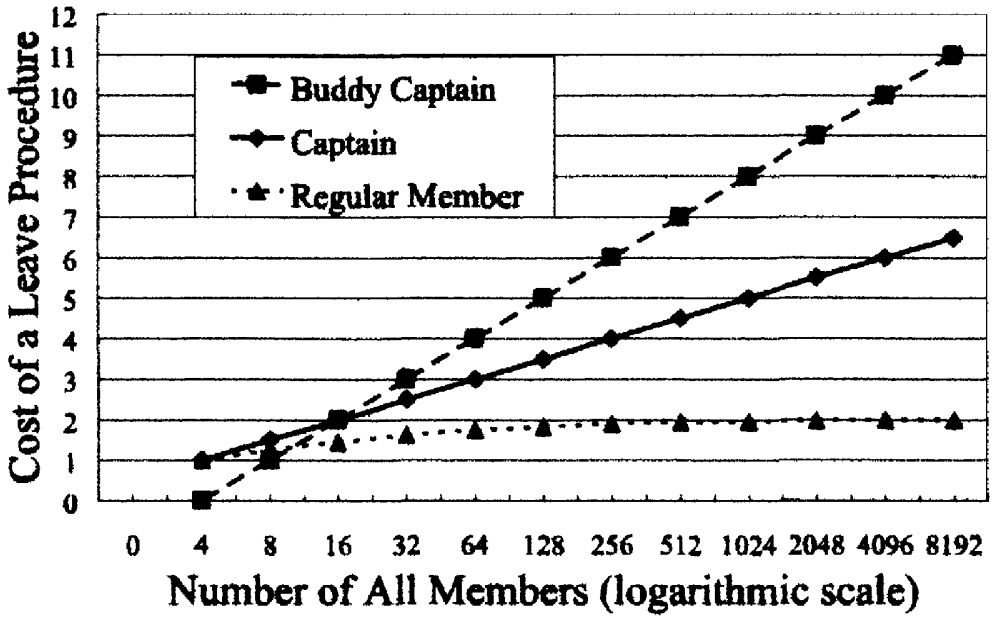
[図12]


Cost of a Join Procedure
0
1
2
3
4
5
6
7
8
9
10
11
12
Captain
Regular Member
0
4
8
16
32
64
128
256
512
1024
2048
4096
8192
Number of All Members (logarithmic scale)

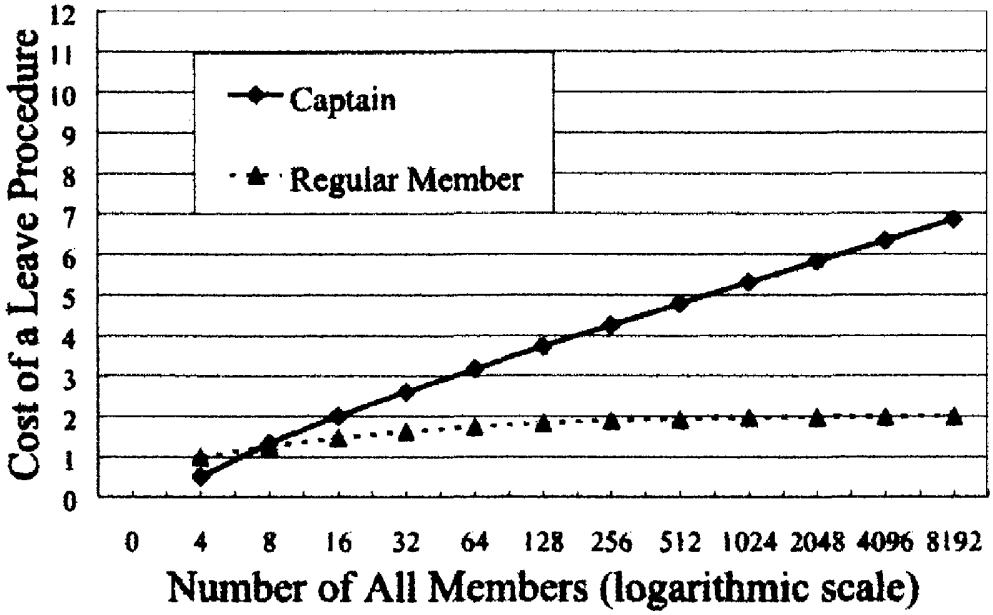
[図13]


Cost of a Join Procedure
0
1
2
3
4
5
6
7
8
9
10
11
12
Newcomer
Captain
Regular Member
0
4
8
16
32
64
128
256
512
1024
2048
4096
8192
Number of All Members (logarithmic scale)

[図14]


Cost of a Leave Procedure
0
1
2
3
4
5
6
7
8
9
10
11
12
Buddy Captain
Captain
Regular Member
0
4
8
16
32
64
128
256
512
1024
2048
4096
8192
Number of All Members (logarithmic scale)

[図15]


Cost of a Leave Procedure
0
1
2
3
4
5
6
7
8
9
10
11
12
Captain
Regular Member
0
4
8
16
32
64
128
256
512
1024
2048
4096
8192
Number of All Members (logarithmic scale)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/019633

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	Daisuke INOUE, Masahiro KURODA, "LKH o Mochiita Hishuchugata Kagi Kanri Hoshiki", 2004 Nen Ango to Joho Security Symposium Yokoshu, Vol. I of II, pages 401 to 406, 27 January, 2004 (27.01.04), particularly, refer to 2 Hishuchugata Kagi Kanri Hoshiki	1,2,4-8, 10-13,15-19 3,9,14
A	KIM, Y., PERRIG, A., TSUDIK, G., Tree-Based Group Key Agreement, ACM Transactions on Information and System Security, Vol.7, No.1, pages 60 to 96, 2004. 02 especially 4. NOTATION AND DEFINITIONS, 5. TGDH PROTOCOLS	1-19

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 28 July, 2005 (28.07.05)	Date of mailing of the international search report 16 August, 2005 (16.08.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１９６３３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L9/08

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	井上大介，黒田正博，ＬＫＨを用いた非集中型鍵管理方式，2004年暗号と情報セキュリティシンポジウム予稿集，Volume I of II，p. 401-406，2004.01.27 特に２ 非集中型鍵管理方式を参照	1, 2, 4-8, 10-13, 15-19
A		3, 9, 14
A	KIM, Y., PERRIG, A., TSUDIK, G., Tree-Based Group Key Agreement, ACM Transactions on Information and System Security, Vol.7, No.1, p. 60-96, 2004.02 especially 4. NOTATION AND DEFINITIONS, 5. TGDH PROTOCOLS	1-19

☐ Ｃ欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２８．０７．２００５	国際調査報告の発送日　16.8.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９３６４ 中里　裕正 電話番号　０３－３５８１－１１０１　内線　３５４６