暗号技術を用いたセキュアグループチャットの提案

棚田　慎也[†*]，鈴木　秀和[†]，内藤　克浩[‡]，渡邊　晃[†] ([†] 名城大学，[‡] 愛知工業大学)

Proposal of Secure Group Chat using Encryption Technology

Shinya Tanada[†], Hidekazu Suzuki[†], Katsuhiro Naito[‡], Akira Watanabe[†] ([†]Meijo University, [‡]Aichi Institute of Technology)

1　はじめに

ネットワーク技術の発展により, インターネットを介したセキュアなチャット通信に関心が高まっている. これを実現するためグループでの情報共有の際にはグループ鍵と呼ばれる共通鍵を用いて暗号化する方法が用いられる. しかし, 現存する方式では管理者やグループ退会者から情報が漏えいする懸念があった. 本稿では,2 通りの鍵からグループ鍵を生成することによりセキュリティを向上したセキュアグループチャットを提案する.

2　現状のセキュアチャットシステム

グループ鍵を用いてチャット通信を行う場合,1 対 1 の通信に比べて一般的に方式が複雑になる. 特に, メンバの参加や退会といった動きがある点を考慮すべきである. チャットにおけるグループ鍵共有方式はいくつか存在するが, 万全のセキュリティを備えた方式はまだ存在しない. 例えば, 鍵を配布する管理者が鍵を所持していると, グループの通信内容を盗聴することができる. またグループを退会したメンバがグループ鍵を所有しているとそこから情報が漏えいしてしまう.

3　提案方式

<3・1 > 概要　管理者にも盗聴することができないセキュリティを実現するために, エンド端末間で共有する共通鍵 (以下 CK1) と鍵管理サーバ (Key Management Server:以下 KMS) から配布する共通鍵 (以下 CK2) を利用し, 新たなグループ共通鍵 (以下 GK) を生成する. 共通鍵の配布では, エンド端末と KMS に公開鍵証明書を持たせ, 双方向認証を確実に行う. なお, 公開鍵は RSA(鍵長 1024 ビット以上), 共通鍵は AES(鍵長 128 ビット以上) を利用し, 暗号化アルゴリズム上はセキュリティの課題がないことを前提とする.

<3・2 > グループ鍵共有方式　Fig. 1 に提案するグループ鍵共有方式を示す.KMS はグループ名とメンバの管理を行う.CK1 はユーザがグループを作成する際に生成する. 新たにメンバを招待するときに公開鍵証明書を用いてエンド端末間で直接認証を行い, その公開鍵を用いて CK1 を共有する.CK2 は KMS がユーザからグループ作成通知を受けた際に生成し, 招待されたメンバへ配布を行う. 一定の更新期間を設け KMS が定期的に CK2 を生成し更新を行う. またメンバが退会したタイミングでは KMS から新しい CK2 をグループメンバに配布し更新する. エンド端末は [CK1|CK2|GroupName] のハッシュ値をグループ暗号鍵 GK として生成する. 同一の GK を保持しているユーザのみが正式メンバとなり相互通信を行える.

KMS 管理者は CK1 を所持しないので, グループ通信の内容はわからない. またグループ退会者は新たな CK2 を入手できないので, やはり通信内容を盗聴することができない. このためグループメンバのみによるセキュアなグループチャットを行うことができる.

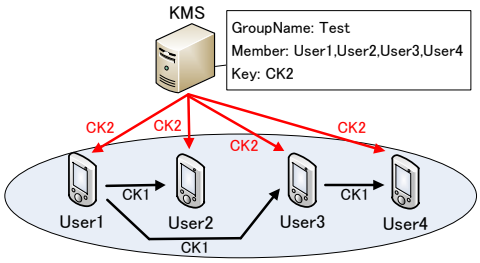


Fig. 1　proposal of group key sharing method.

Table 1　comparison of chat applications.

	項目 (1)	項目 (2)	項目 (3)	項目 (4)
LINE	○	×	×	×
Skype	○	×	×	×
ChatSecure	○	○	○	-
提案方式	○	○	○	○

4　評価

Table 1 にチャットアプリケーションの比較を示す. 項目 (1)~(3) は電子フロンティア財団 (Electronic Frontier Foundation:以下 EFF)[1] により提示されたチャットアプリケーションのセキュリティ評価項目であり, 項目 (4) は独自に追加した評価項目である. 評価項目の内容は以下のとおりである.

(1) 通信経路が暗号化されている.
(2) 管理者が読めないように暗号化されている.
(3) 暗号鍵が盗まれても過去の通信内容が安全である.
(4) 退会したメンバが通信内容を盗聴できない.

比較対象は LINE,Skype,ChatSecure とした.LINE,Skype はセキュリティがぜい弱であることがわかる.ChatSecure は EFF による評価項目を全て満たしているが,1 対 1 のチャットでありグループチャットはできない. 項目 (2) において提案方式では CK1 と CK2 の 2 つの鍵から GK を生成するため KMS の管理者でさえ通信内容がわからない. 項目 (3) において提案方式では定期またはメンバ退会時に CK2 を更新しているため暗号鍵が盗まれたとしても過去の通信内容は安全である. 但し, 退会したユーザは過去の内容を閲覧できる. 項目 (4) では提案方式では退会時に CK2 を更新するため退会したメンバは盗聴できない.

5　まとめ

本稿では, 通信端末に公開鍵証明書を持たせ, 異なるルートで 2 つの鍵を共有し, その 2 つの鍵で新たに生成するグループ鍵によるセキュアなグループチャットを提案した. 今後は実装や再評価を行う予定である.

文　献

[1] Electronic Frontier Foundation : Secure Messaging Scorecard, available from <https://www.eff.org/secure-messaging-scorecard> (accessed 2015-07-10)

暗号技術を用いた
セキュアグループチャットの提案

棚田 慎也† 鈴木 秀和† 内藤 克浩‡ 渡邊 晃†

†名城大学 理工学部
‡愛知工業大学 情報科学部

Watanabe Lab.

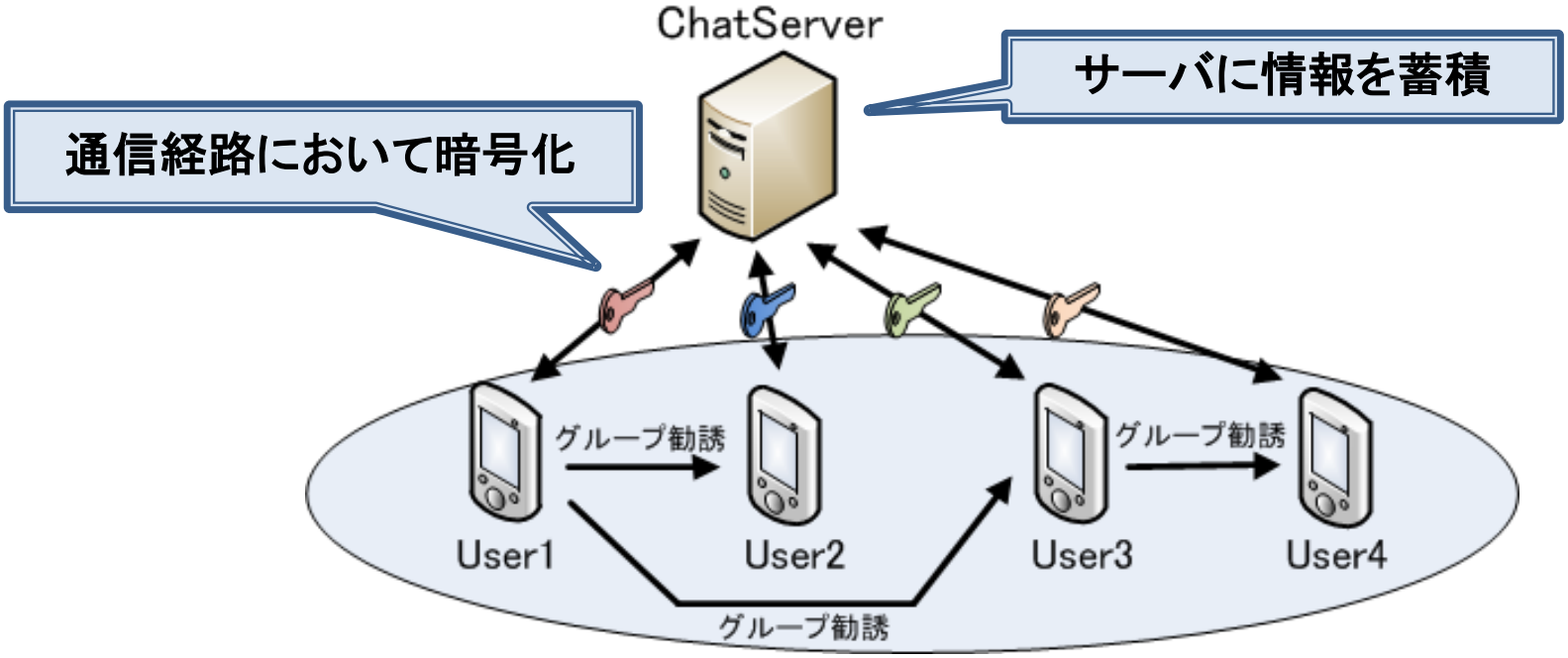
研究背景

- ネットワーク技術の発展
  - インターネットを介した情報共有
- チャットアプリケーションの普及
  - 強力なコミュニケーションツール
  - 業務で用いたいという企業の要望
    ⇒セキュリティが万全ではない

暗号技術を用いたセキュアなグループチャットの提案

現状のグループチャット

- LINEの場合



- グループチャットの問題点

セキュリティが脆弱

提案方式の目的

業務でも利用可能なセキュアグループチャットの実現

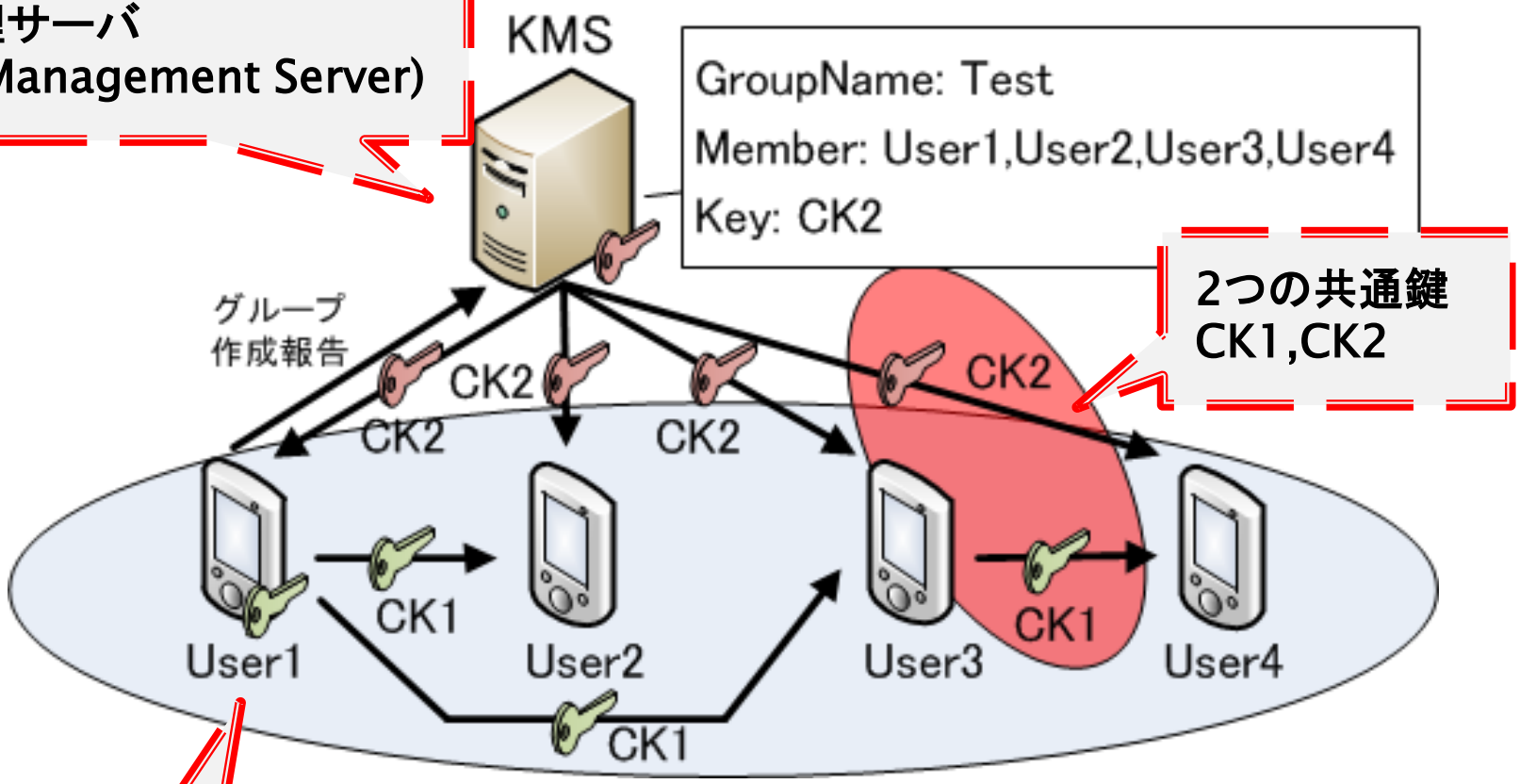
- 考慮すべき点
  - 管理者が盗聴することができない
  - グループ退会者が盗聴することができない

提案方式の概要

- 鍵管理サーバKMS(Key Management Server)を設置
  - 共通鍵の配布を行う
- 公開鍵証明書による双方向認証
  - エンド端末とKMSに公開鍵証明書を持たせる
  - 共通鍵共有時に双方向認証を確実にする
- 2つの共通鍵を共有
  - それぞれ別ルートで共有
  - 2つの共通鍵を用いて新たなグループ共通鍵GK生成
- 暗号アルゴリズム上は十分安全であることが前提

提案方式の構成(1)

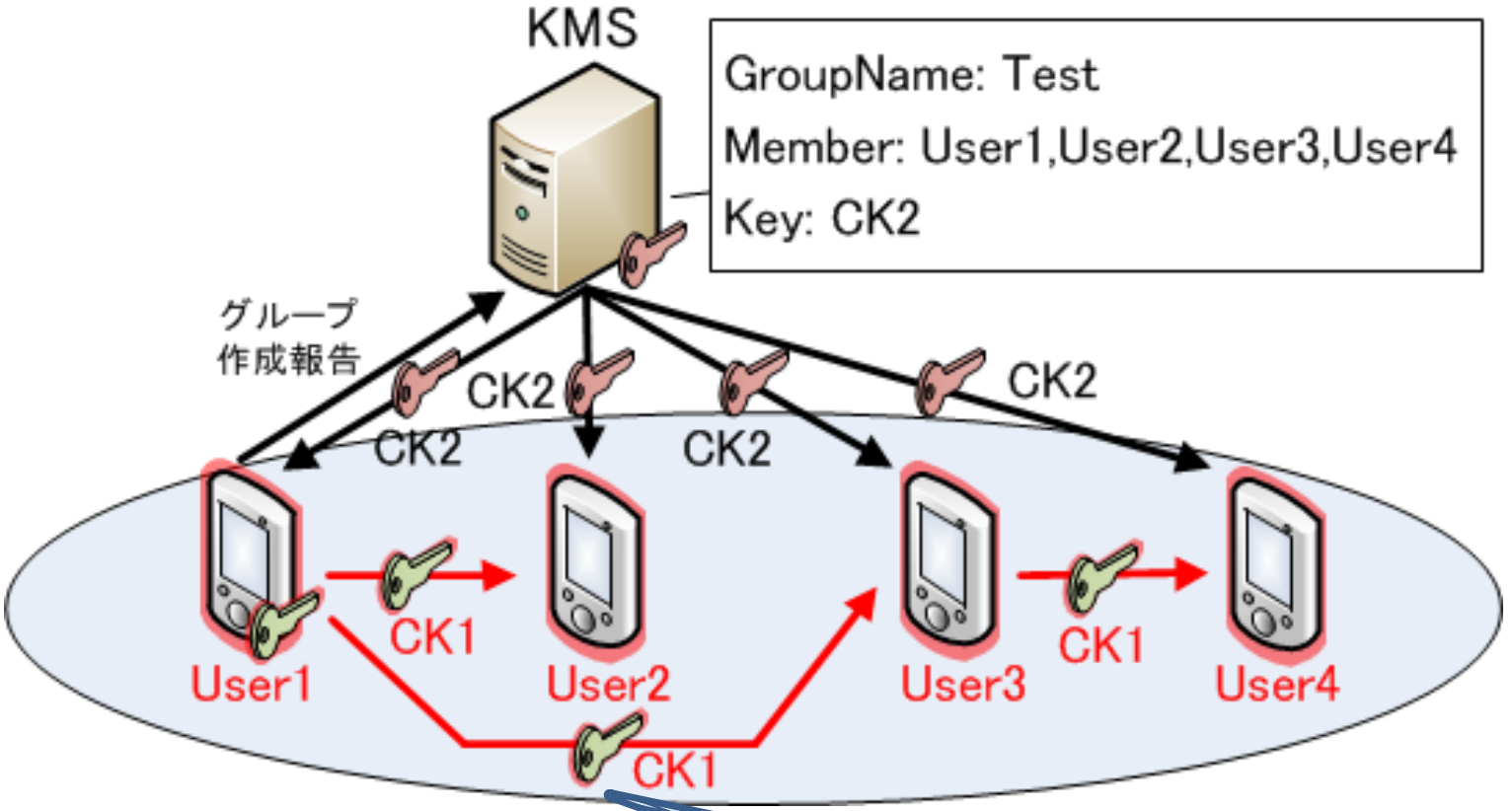
鍵管理サーバ
(Key Management Server)



2つの共通鍵
CK1,CK2

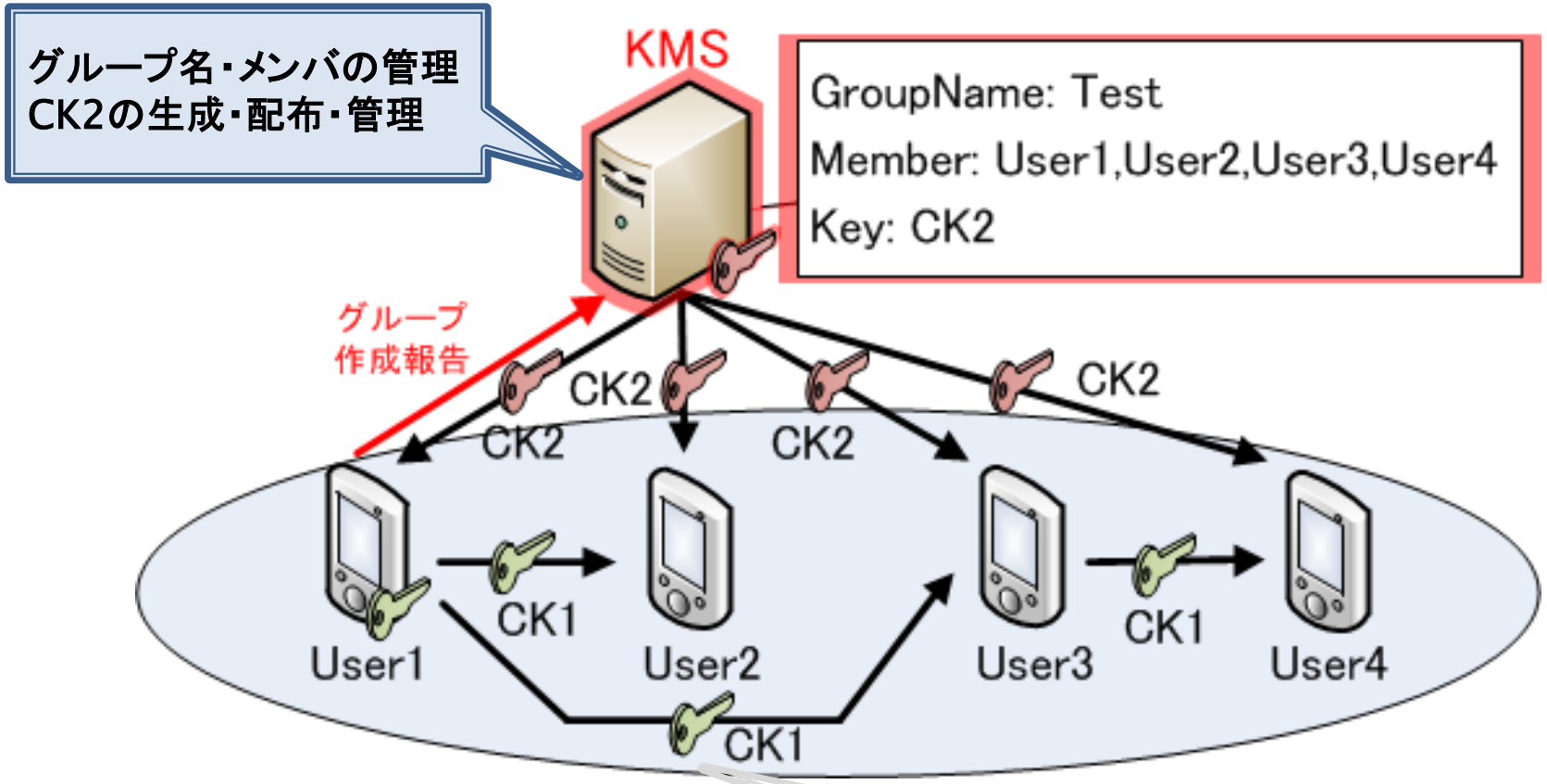
エンド端末
2つの共通鍵でグループ鍵生成

提案方式の構成(2)



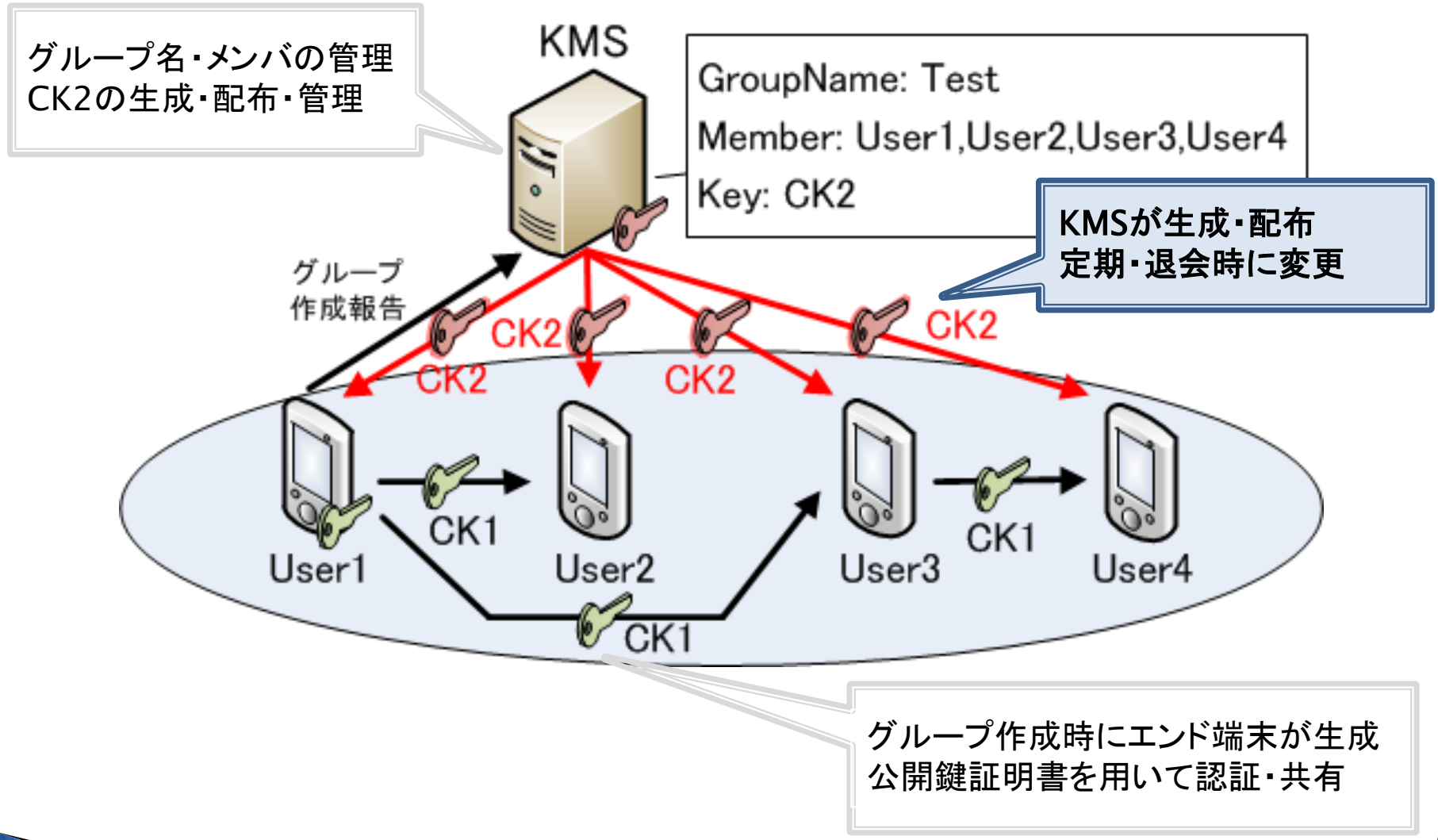
グループ作成時にエンド端末が生成
公開鍵証明書を用いて認証・共有

提案方式の構成(3)

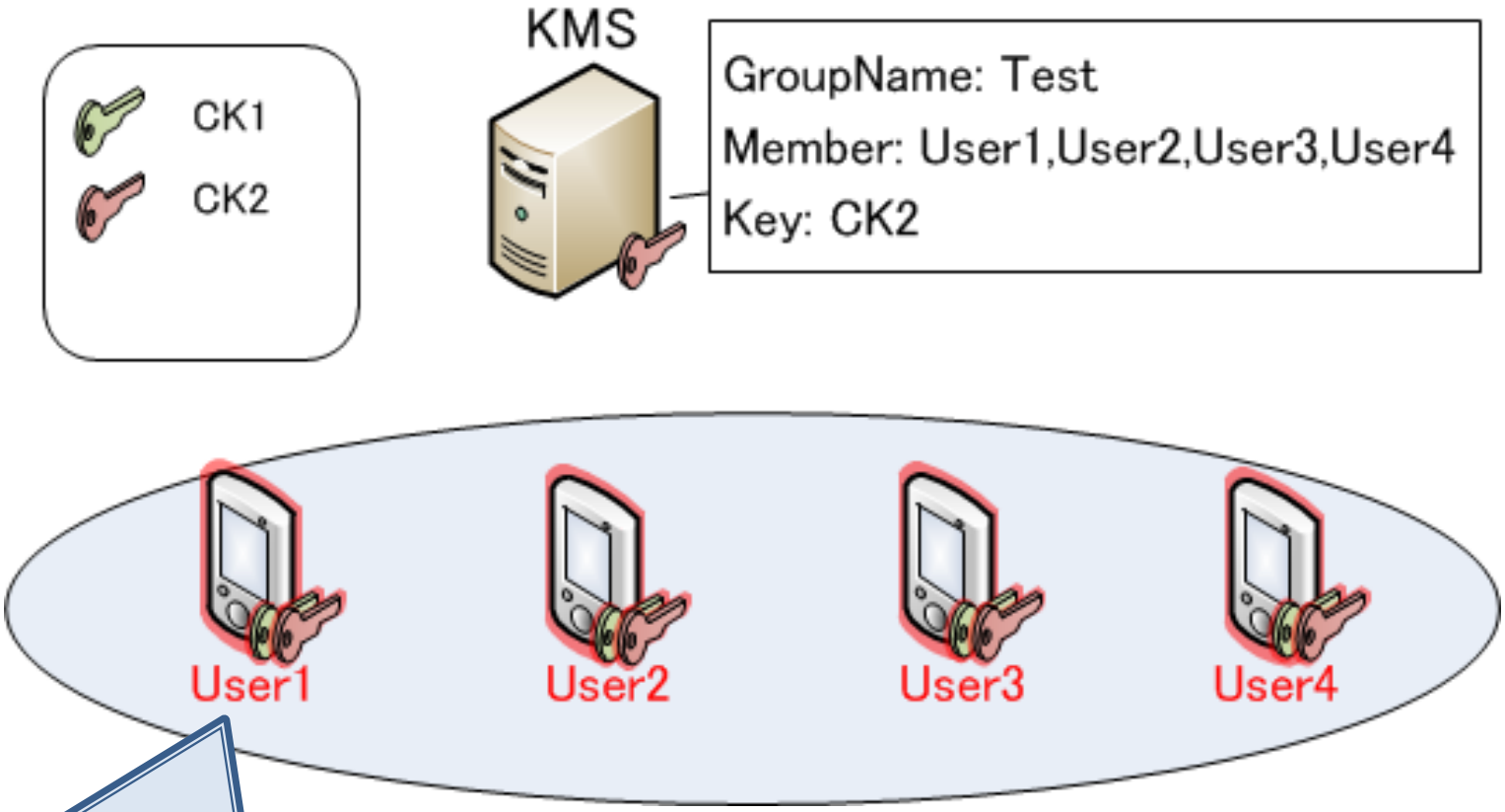


グループ作成時にエンド端末が生成
公開鍵証明書を用いて認証・共有

提案方式の構成(4)

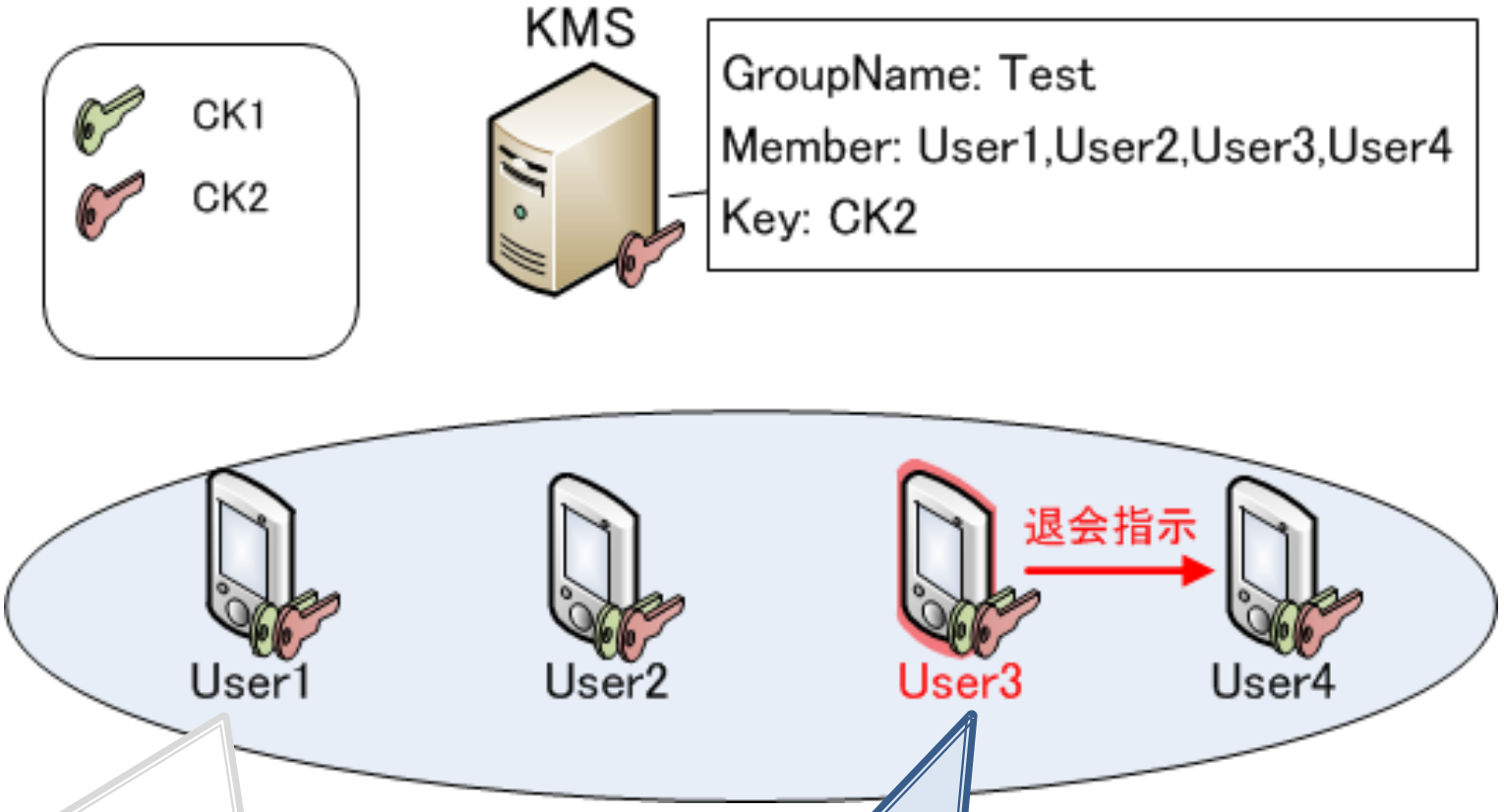

グループ名・メンバの管理
CK2の生成・配布・管理
KMS
GroupName: Test
Member: User1,User2,User3,User4
Key: CK2
KMSが生成・配布
定期・退会時に変更
グループ
作成報告
CK2
CK2
CK2
CK2
CK1
CK1
CK1
User1
User2
User3
User4
グループ作成時にエンド端末が生成
公開鍵証明書を用いて認証・共有

提案方式の構成(5)

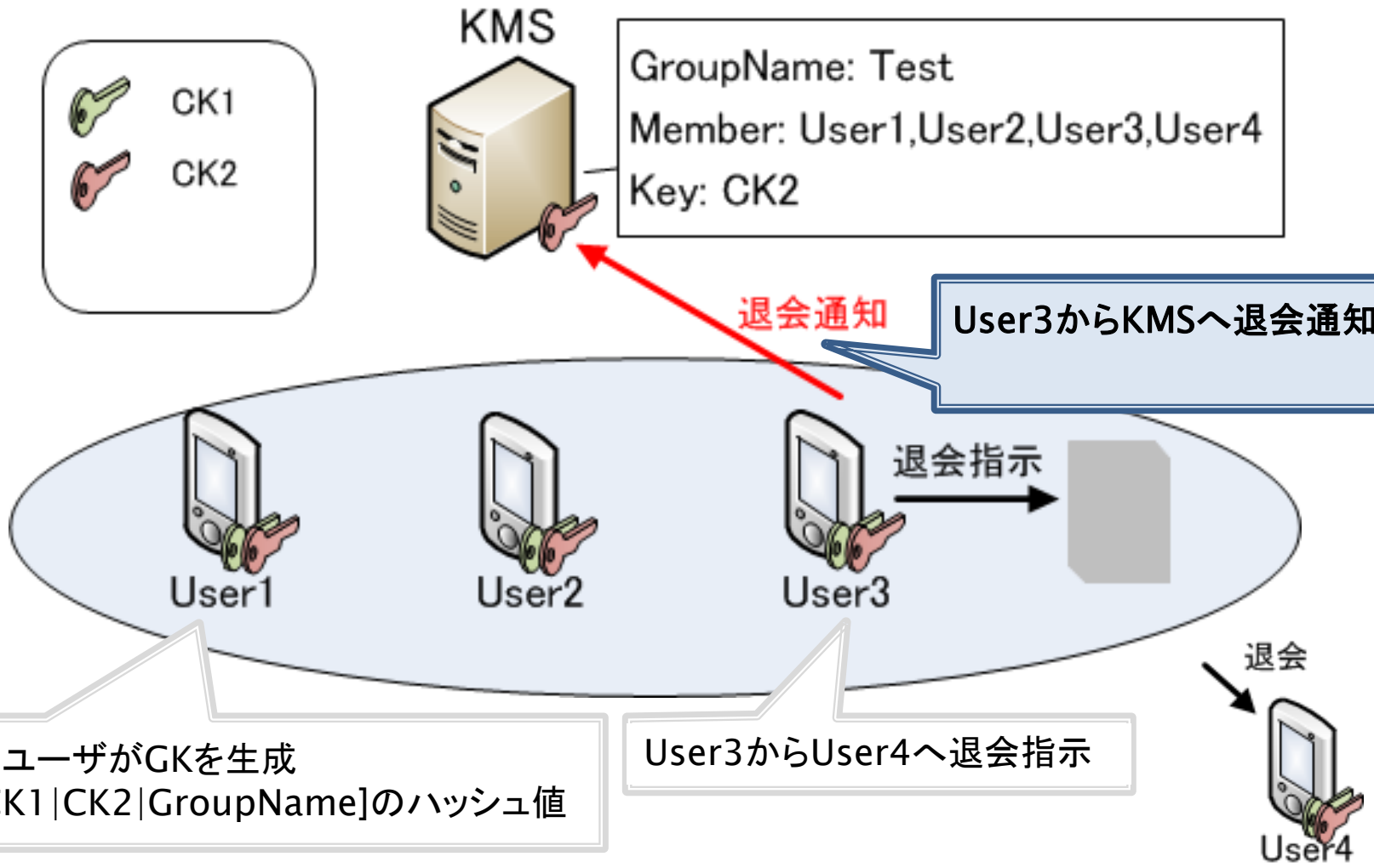


各ユーザがGKを生成
[CK1|CK2|GroupName]のハッシュ値

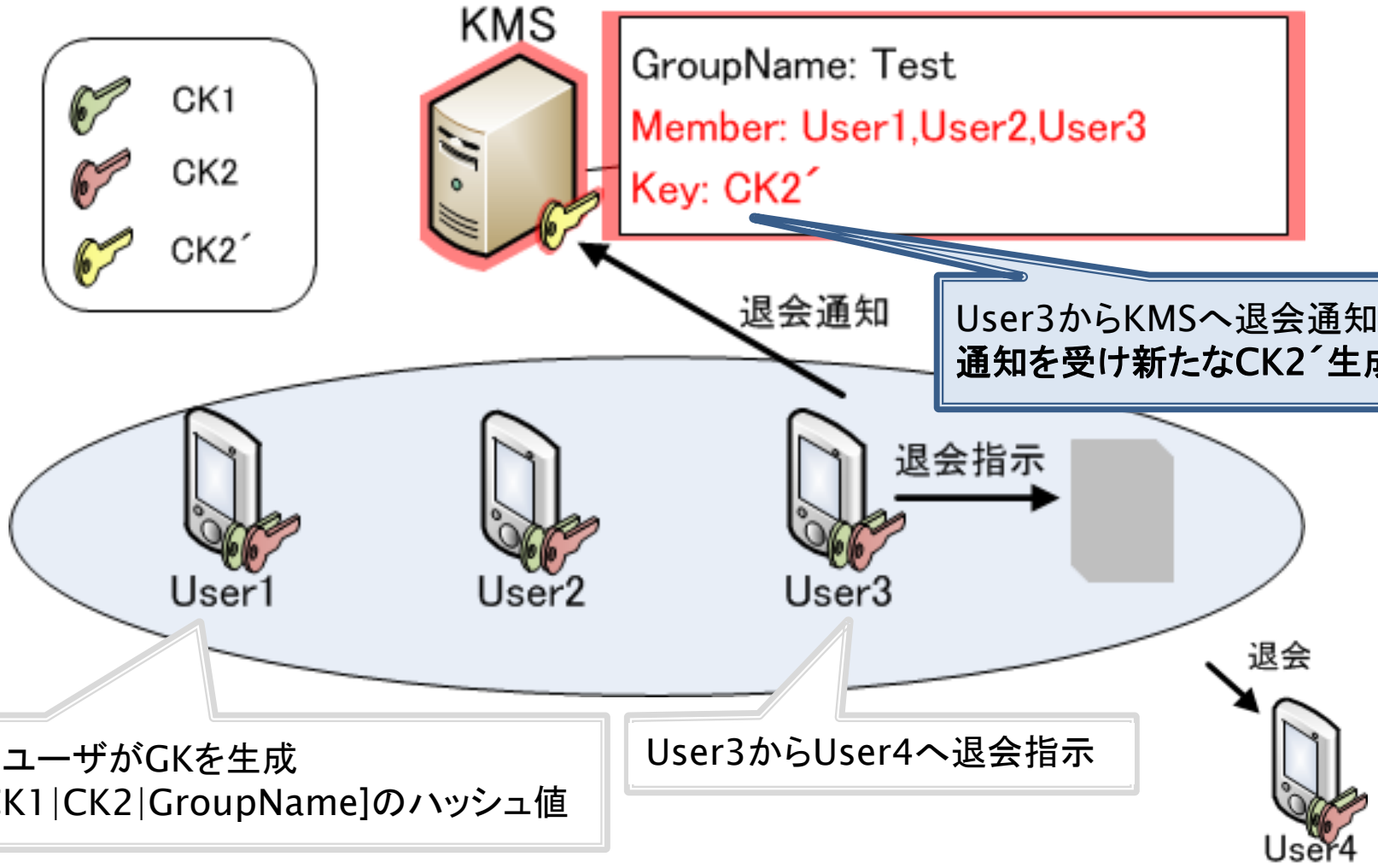
提案方式における鍵の更新処理(1)



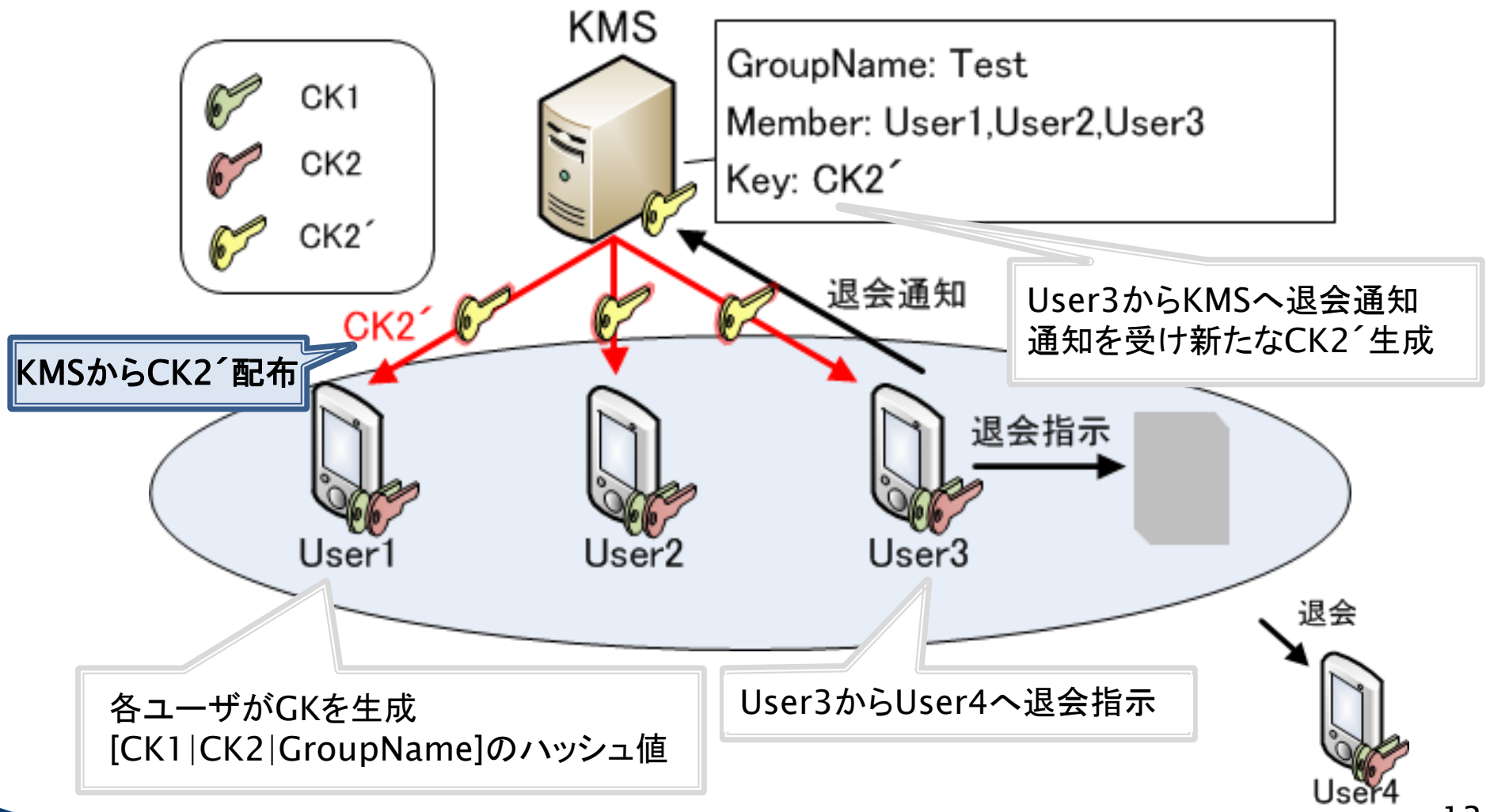
提案方式における鍵の更新処理(2)



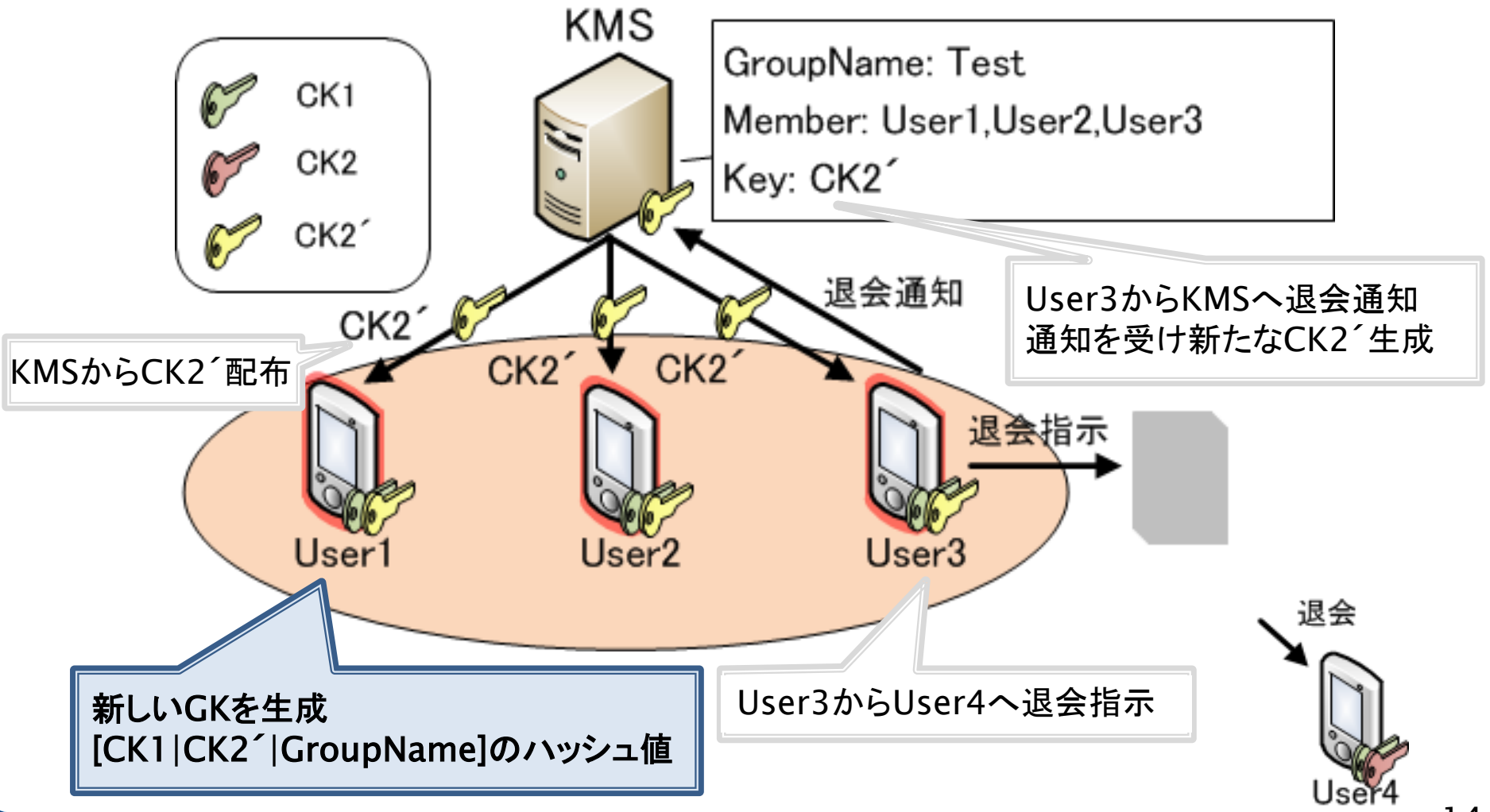
提案方式における鍵の更新処理(3)



提案方式における鍵の更新処理(4)



提案方式における鍵の更新処理(5)



提案方式の利点

- KMS管理者はCK1を所持していない
  ⇒グループ鍵GKを生成することができない

- グループ退会者は新しいCK2を所持していない
  ⇒新規の通信内容を盗聴できない
  ⇒ただし過去の通信内容は閲覧できる

グループメンバのみによるセキュアグループチャット

提案方式の評価

- (1)通信経路が暗号化されている
- (2)管理者が読めないように暗号化されている
- (3)暗号鍵が盗まれても過去の通信内容が安全である
- (4)退会したメンバが通信内容を盗聴できない

(1)~(3)・・・Electronic Frontier Foundation※1: EFFによるチャットアプリケーションのセキュリティ評価項目
(4)・・・独自に追加した評価項目

	項目(1)	項目(2)	項目(3)	項目(4)
LINE	○	×	×	○
Skype	○	×	×	○
ChatSecure※2	○	○	○	–
提案方式	○	○	○	○

※1 Electronic Frontier Foundation・・・アメリカに本拠地を置く非営利組織

※2 ChatSecure・・・EFFの調査項目を全て満たしている1対1チャット,グループチャットはできない

まとめ

- セキュアなグループチャットの提案
  - 異なるルートで2つの共通鍵を共有
  - 2つの共通鍵で新たにグループ鍵を生成
    ⇒悪意のある管理者・退会者による盗聴を防止

- 今後の予定
  - 提案方式の詳細設計の検討
  - 実装及び性能評価

補足資料

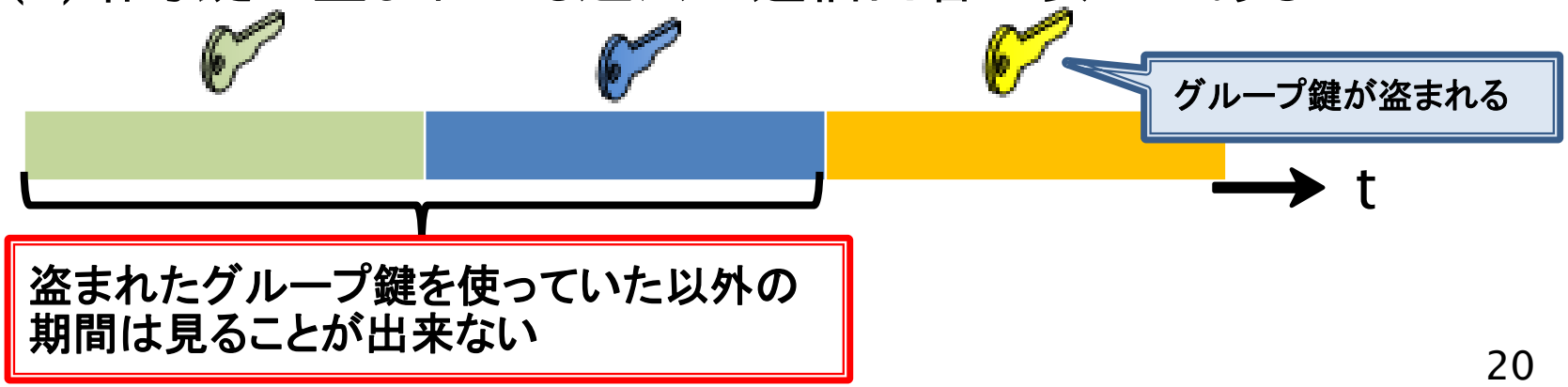
EFFによる Secure Messaging Scorecard

- 1. トランジットで暗号化がされているか?
- 2. プロバイダーが読めないように暗号化されているか?
- 3. 連絡先の確認が可能か?
- 4. 鍵が盗まれても過去の通信内容が安全か?
- 5. コードが公開されていて, 個別の評価が可能か?
- 6. セキュリティの方針は適切に文書化されているか?
- 7. コードは監査を受けているか?

鍵の更新について

- 鍵の更新を行わない場合
  - グループ退会者がGKを所持している
    ⇒退会者が通信内容を盗聴できる
  - グループ鍵が盗まれる
    ⇒過去の全ての通信内容を見ることが出来る

- 提案方式における鍵更新
  - (3)暗号鍵が盗まれても過去の通信内容が安全である



GK作成における検討

- CK1のみの場合
  - エンド端末において鍵の更新,配布が必要
  - CK1が漏えいしてしまうと盗聴可能
    - CK2もあればCK1のみではGKを作ることが出来ない
- CK2のみの場合
  - 管理者が盗聴可能
- CK1・CK2によるGK作成
  - 二重化によるセキュリティ向上
  - CK1では更新などの処理が不要になる

KMSにおける検討

- チャットサーバとは別にKMSを設置
  - 負荷分散
  - KMSはグループ管理,鍵の配布・更新のみ
  - 既存技術への導入が可能

- 課題
  - KMSがCK2の更新・配布を行う
    ⇒利用グループの増加によりKMSへの負荷が大きくなる
    ⇒CK2の更新頻度の検討を行う必要がある