P2P 環境下における動的グループ生成用暗号利用方式の評価

渡邉浩朗[†1] 加藤貴法[†1] 佐々木良一[†1]
江口雄介[†2] 安永洋平[†3] 吉田兼也[†4]

P2P におけるデータの共用は不特定多数の間で実施されてきたが，今後特定の人々の間で選択的にデータを共用することが予想される．ここでは，暗号を利用しグループ鍵を生成することにより復号できる相手を制限する方法を採用し，安全かつ柔軟に動的なグループを生成する方式として 4 つの方式を考案した．予備評価を行い，望ましい 2 つの方式をリストアップするとともに，実際にプログラムを作成し評価を実施したので，その結果を報告する．

Evaluation on Dynamic Group Key Generation Methods under P2P Environment

Hiroaki Watanabe,[†1] Takanori Kato,[†1] Ryoichi Sasaki,[†1]
Yusuke Eguchi,[†2] Yohei Yasunaga[†3] and Kennya Yoshida[†4]

Although common use of the data in P2P has been carried out between many and unspecified persons in near future, it is expected to be to carry out alternatively among specific. Since the method of restricting the partner who can decipher by using a cipher and generating a group key was adopted, preliminary evaluation was performed while proposing four systems as a system which generates a dynamic group safely and flexibly, the result is reported.

1. はじめに

P2P とは，コンピュータどうしを対等な立場で接続し，直接情報のやりとりを行うインターネットの利用形態であり，ファイルや演算能力などの情報資源を共用するシステムである．データ共用においていままでは不特定多数の間でやりとりされてきた．第 1 世代では中央にサーバを構え，データのインデックスやユーザのオンラインオフラインを管理していた．Hybrid P2P と呼ばれており，代表ツールに Napster がある．第 2 世代では，Hybrid P2P 型でサーバが管理していたことをユーザ同士で管理を行うようになり，PureP2P と呼ばれ，代表ツールに Gnutella がある．第 3 世代では構成した仮想ネット内をキャッシュファイルが流れることにより，ファイルのやりとりを意識せずにすむ freenet や winny が登場してきている．今後 P2P でのファイル共用の需要は増すと思われるが，いままでのように不特定多数が相手ではなく，相手を特定し選択的に行われることも多くなると予想される．

本研究では，暗号技術を利用することにより動的なグループを生成し，共用する相手を制限することを目標としている．4 つの方式を提案するとともに予備評価を行い，2 方式について実際にプログラムを作成し評価を実施したので，その結果を報告する．

2. P2P における評価指標

本論文では，P2P システムとして第 2 世代の PureP2P を想定しており，転送するファイルはユーザが指定し転送開始する方法を考えている．

P2P におけるデータ配信を**図 1** に示す．1，2，3 がグループを構成しており，1 から 2，3 に対してデータの共用を行おうとしている．1 がファイルを暗号化し，P2P ツールを使いデータを共用する．

グループメンバではない 4 も，データを入手することはできるが，グループ鍵を用い暗号化されているため，復号することはできないことを示している．

†1 東京電機大学
Tokyo Denki University
†2 東京通信ネットワーク株式会社
TOKYO TELECOMMUNICATION NETWROK CO., INC.
†3 アマノ株式会社
Amano Corporation
†4 株式会社電算
DENSAN, INC.

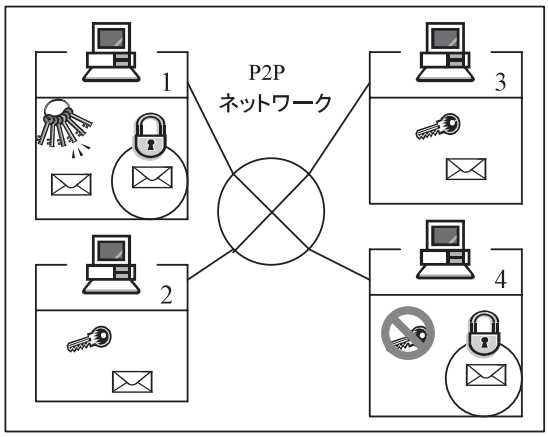

図 1 P2P における選択的情報共用の概念図
Fig. 1 Conceptual figure of alternative information common usage in P2P.

この方式において望ましいと思われる鍵配送システムの評価指標をあげた．システム全般として，通常用いられる以下の 4 つの指標を採用した．

① 安全性の高いこと．
② 保存すべきデータ量が少ないこと．
③ 鍵数が少なく，管理が容易なこと．
④ 暗復号の計算時間が少ないこと．

P2P に関しては，このほかに

⑤ PureP2P がそうであるように，常時アクセスしなければならないサーバを必要としないこと，
⑥ 現在主流のクライアントサーバ型のシステムより導入コストが少なくて済む，

があげられると思われる．

3. 動的グループ鍵生成法の候補

グループを生成する方法として以下のようなものが考えられる．

3.1 個別鍵利用方式

共通鍵の暗号を用いてファイルを共通化したい相手ごとに暗復号を行う．この鍵の暗号化に公開鍵暗号方式を用いる．暗号化したデータを対応する相手に取得させ，ユーザは自分が持っている鍵でデータを復号化する方式である．

3.2 グループペア鍵利用方式

自分が所属しうるグループすべての共通鍵を持ち，共用する相手ごとで暗号化する方式である．自分が含まれるグループすべての共通鍵を持っているので，たとえば A は自分だけが暗号化できる鍵 K_A，B と 2 人だけで共用できる共通鍵 K_{AB}，C と 2 人だけで共用できる共通鍵 K_{AC}，B と C の 3 人で共用できる共通鍵 K_{ABC} の 4 種類を持つことになる．仮に B とだけで共用する場合，共通鍵 K_{AB} を使用すれば，C がそのデータを入手したとしても復号することはできない．

3.3 IC カード利用方式

この方式は，IC カード内に格納されているシステム固有のマスタ鍵と宛先リストからグループ鍵を生成し，その鍵を用いて情報を暗号化する．

宛先リストとは，情報の開示先となるユーザ名およびグループ名のリストである．復号化処理には，権限チェックプログラムが暗号化情報のヘッダから宛先リストを読み出し，復号化を試みるユーザの ID 情報が宛先リストに含まれるか否かを確認する．このとき，含まれていればグループ鍵生成プログラムがグループ鍵を生成し，含まれなければ生成しない．なお，暗号方法は共通鍵暗号方式である．

IC カード利用方式では暗復号化処理時に鍵を動的に生成するものであり，ユーザがいくつもの鍵をつねに所持しておく必要がないという特徴がある．この方式は文献 1) に示す方式と同じである．

3.4 公開鍵利用方式

発信者は，ファイルを共用したいユーザの公開鍵を入手しグループ鍵，セッション鍵を生成する．セッション鍵で情報を暗号化し，その後セッション鍵をグループ鍵で暗号化する．この 2 つのファイルを両方入手することで，ユーザは自分の秘密鍵を用いてセッション鍵を取り出し，取り出したセッション鍵を用いて情報を復号化する．なおグループ鍵は公開鍵暗号方式であり，セッション鍵は共通鍵暗号方式である．グループ鍵をユーザの公開鍵より生成するため自分の所有する秘密鍵で復号することができる．発信者自身がユーザを選択することができるため，管理者を必要としない．管理する鍵は公開鍵と秘密鍵の 2 つとなるが，グループ鍵やセッション鍵は動的に生成するため，管理する必要がないというメリットがある．この方式は文献 2) に示す方法と同じである．

3.5 比較・検討

以上を評価指標①〜③において予備評価した結果を**表 1** に示す．暗号化前のデータを M，暗号化後のデータを K(M)，暗号化するグループの人数を N，暗号化情報に付加されるヘッダを H，グループ鍵を G とする．いずれの方式も①の安全性は問題ないと思われる．また表 1 より以下のことがいえる．

(1) 個別鍵利用方式では，暗号化されたデータを人数分用意しなければならず，データ量が多くなる．暗号に使う鍵数も同様である．
(2) グループペア鍵利用方式は，グループ数が増え

表 1 グループ鍵方式の比較
Table 1 Comparison of group key system.

	総データ量	鍵数		予備評価
		管理する数	暗号化に必要な数	(①〜③の観点)
個別鍵方式	K(M)×N	1	N	×
グループペア鍵方式	K(M)	$\sum_{i=1}^{N-1} {}_{N-1}C_i + 1$	1	×
IC カード方式	K(M)+H	1	1	○
公開鍵利用方式	G(K)+K(M)+H	1	2	○

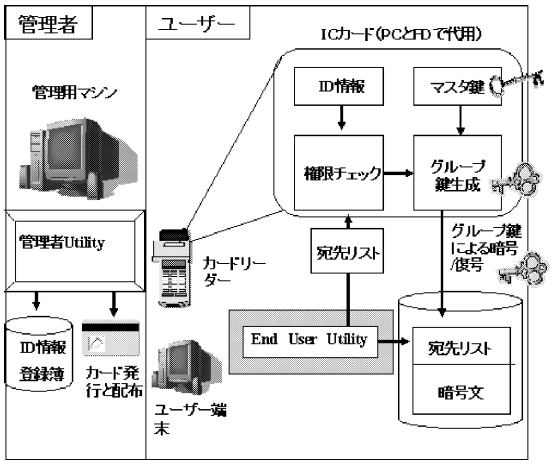

図 2 IC カード利用方式の構成図
Fig. 2 Structure of integrated circuit card usage system.

ると管理する鍵数が表 1 で示したとおり多くなる．仮に 10 人でグループを構成すると鍵数は 512 個に．20 人だと 52 万 4,288 個，30 人だと 5 億 3,687 万 912 個となってしまう．

以上により個別鍵利用方式とグループペア方式は適していないと判断し，IC カード利用方式と公開鍵利用方式を実装し，評価指標④〜⑥の面から評価することにした．

4. IC カード利用方式の実装と評価

4.1 システム構成と処理手順

システム構成を**図 2** に示す．管理者は，管理者ユーティリティを用いてグループ固有のマスタ鍵を生成し，管理者マシンへ登録する．ユーザから発行要求があった場合，登録した ID 情報とマスタ鍵を IC カードに入れユーザに渡す．ユーザは発効された IC カードとエンドユーザユーティリティを用いグループ鍵を生成し，ファイルを暗復号化する．

以下にこの方式の暗号化の流れを示す．

① マスタ鍵を事前に IC カードに入力する．
② データを公開する人がデータを見る権利のある人を示す宛先リストを作成する．
③ メンバが同じ場合，同じ値ができてしまうのを回避するために，その宛先リストに乱数を付加する．
④ 乱数付宛先リストのハッシュ値を取得する．
⑤ ハッシュ値を IC カード内でマスタ鍵を用いてグループ鍵を生成し，それを出力する．
⑥ 生成したグループ鍵を用い，情報を PC 内で暗号化する．
⑦ 宛先リストに暗号を付加したものと暗号文を一緒にして公開する．

復号化の場合は以下のとおりである．

① データに付加している乱数付宛先リストを読み込む．
② IC カード内の ID 情報が宛先リストに入るかどうかにより権限チェックを行い，復号できるユーザかどうかを確認する．
③ 乱数付宛先リストよりハッシュ値を取得する．
④ ハッシュ値とマスタ鍵を用いることによりグループ鍵を生成する．
⑤ グループ鍵を用い情報の対象となっているファイルの復号化を行う．

本方式において，仮に宛先リストが改竄された場合でも，権限チェックプログラムは通過されるが，グループ鍵は宛先リスト情報のハッシュを利用して生成しており，暗号時に生成したグループ鍵と同じ鍵を生成することはできない．よって，復号化されてデータを盗み見されることはない．

4.2 グループ鍵生成プログラム

この方式を CryptoAPI を用いて開発した．言語は Microsoft VisualC++，ステップ数約 800 ステップ，マシンスペックは，CPU Celeron 733 MHz，メモリ 192 MB である．ここでは本来 IC カード内で実施すべきことも PC 内で実施している．

本実験システムでは，CryptoAPI を用いて開発しているため，関数の仕様上そのまま実現するのは困難であった．そのため，次のような方法で実現した．

CryptoAPI の関数で，与えたデータのハッシュ値から鍵を生成するものがある．ここに宛先リストを与える．また，このときハッシュをとるアルゴリズムを

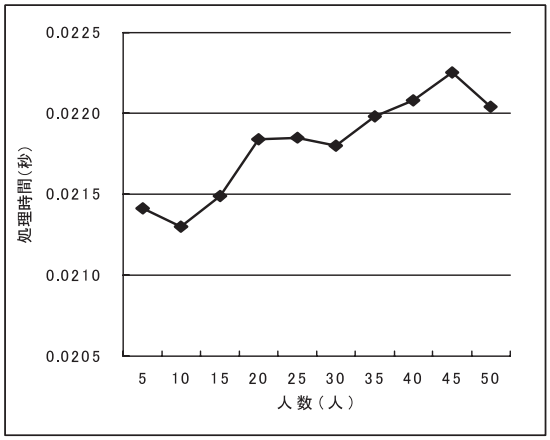

図 3 人数変化における処理時間
Fig. 3 Processing time related to number change.

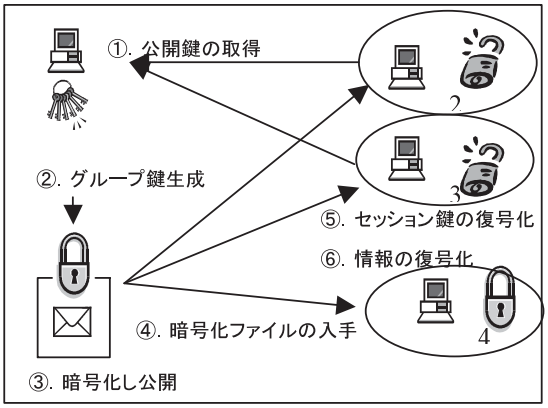

図 4 公開鍵利用方式のシステム全体図
Fig. 4 System structure of public key usage system.

指定できるので，ここに鍵付きのハッシュアルゴリズムを指定する．ハッシュの鍵にマスタ鍵を用いることで，宛先リストとマスタ鍵とから鍵が生成され，これがグループ鍵となる．暗号には RC2，ハッシュには MD5 ベースのものを用いた．

4.3 処理時間の計測

図 3 にグループ鍵を生成し，暗号化するまでの処理時間を示す．共用する人数を 5 人から 50 人まで 5 人ずつ増やし，それぞれの場合に，宛先リスト情報をランダムに与え処理時間を求めた．人数が 5 人から 50 人に増えても処理時間は 1 ms 程度の差であり，1,000 人のグループであれば，50 ms 程度で暗号化することができ，人数増加の処理時間への影響は非常に小さいと予想される．人数増加に逆らい処理時間が減少している点があるが，与える宛先リストのデータ量の影響と思われる．

なお，ここでは本来 IC カードで実施すべき部分を PC で実施している．IC カードのクロック数は 5 MHz 程度，今回使用した CPU は 733 MHz なので，約 150 倍近い差があり，処理時間も今回計測した値の 150 倍ほどかかると思われる[4]．

本システムは IC カードの耐タンパ性が保たれる限りは安全であると思われる．またつねにアクセスしなければならないサーバはなく，評価指標⑤に適していると思われる．しかしサーバ運用者は，

① 使用する IC カード内容の初期設定，
② 無効となった IC カードの回収，

を行う必要がある．

5. 公開鍵利用方式の実装と評価

5.1 システムの要件

P2P 上で公開鍵暗号を用い動的にグループを構成し共用する方式上での条件の検討を以下のように行った．

(1) 各個人の公開鍵を利用し，グループ鍵を生成する際，マスタ鍵の管理やユーザを登録するなどといった作業が発生せず，また復号時に必要となる秘密鍵の配布を必要としない．
(2) ユーザのための秘密鍵を生成しそれらを配信するディーラが必要な方式と不要な方式があるが，ここではできるだけセンタ的な仕組みを持たないディーラなしのほうを採用することにした．
(3) また暗号文を受け取りグループ内の複数人が承知して初めて復号できるようにしたい場合もあるので，復号しきい値のある方式を採用することにした．

公開鍵暗号を利用し動的にグループ鍵を生成する方式はいろいろ提案されているが以上の条件を満たすものとして 5.2 節に示す方式[2]を採用し，プログラム開発を行った．

5.2 グループ鍵生成

システム全体図を**図 4** に，暗号化の処理の流れの概要を以下に示す．

① ユーザは各自公開鍵と秘密鍵を生成する．
② 情報を発信したいユーザはグループに加えたいユーザの公開鍵を入手し，グループ鍵を生成する．
③ セッション鍵を用い情報を暗号化し，セッション鍵を先に作ったグループ鍵を用い暗号化し，暗号化されたセッション鍵と情報を公開する．

次に復号の処理の流れの概要を以下に示す．

④ 暗号化された情報を入手する．

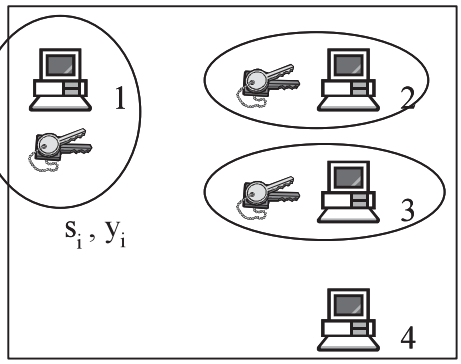

図 5 公開鍵と秘密鍵の生成
Fig. 5 Generation of public key and private key.

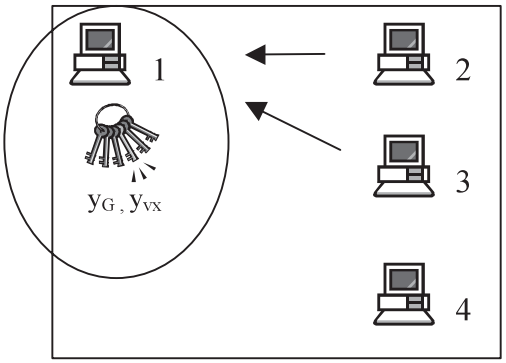

図 6 グループ鍵の生成
Fig. 6 Generation of group key.

⑤ 自分の秘密鍵を用いセッション鍵を復号する．
⑥ セッション鍵を用い情報を復号する．

以下に，もう少し詳しく説明を追加する．

① ユーザは各自秘密鍵 s_i と公開鍵 $y_i = g^{si} \bmod p$ を生成する（**図 5**）．

② ここでは，秘密分散法を用いて処理を行う．すなわち，まず，発信者はグループユーザの公開鍵を使い，以下のようにグループ公開鍵 y_G を作成する．p は大きな素数，q は $p-1$ を割り切る素数，g は q 以下の p の原始根，n はグループのユーザ数，m は復号時に協力すべき人数であるしきい値，GID はその ID の集合である．

$$y_G = \prod_{i \in GID} y_i^{\lambda_i(0)} (\bmod p) \tag{1}$$

$$\lambda_i(0) = \prod_{j \in GID, j \neq i} (-j)(i-j)^{-1} (\bmod q) \tag{2}$$

次に $n-m$ 個の仮想点の集合 $V = \{v_1, \ldots, v_n\}$ を他のユーザ ID と重ならないように選び，公開鍵 y_{vx} を以下のように計算する（**図 6**）．

$$y_{\nu_x} = \prod_{j \in GID} y_i^{\lambda_i(\nu_x)} (\bmod p) \tag{3}$$

$$\lambda_i(\nu_x) = \prod_{j=GID, j \neq i} (\nu_x - j)(i-j)^{-1} (\bmod q) \tag{4}$$

ここで，発信者はセッション鍵 K を生成し $(A, B) = (g^r, K y_G{}^r)$ と暗号化する．r は $1 \leq r \leq q-1$ の乱数であり，先に計算した仮想点 V はメッセージヘッダとして $MH = \langle (v_1, y_{v1}{}^r) \cdots (v_{m-k}, y_{vn-m}{}^r) \rangle$ を計算し，付加する．生成したセッション鍵 K で全体を暗号化し情報を公開する（**図 7**）．

③ 各ユーザは暗号化されたデータを公開フォルダから持ってくる．

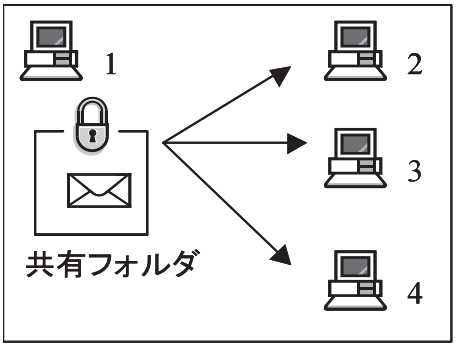

図 7 暗号化しての情報の公開
Fig. 7 Encipher and presentation of informational public presentation.

④ 復号する権利のあるユーザ m 人が A^{si} を以下のように計算し公開することにより，$A^{f(0)}$ を復元することができる．なお 1 人だけで単独に復号できる場合は $m = 1$ となる．

$$A^{f(0)} = \prod_{i \in V} y_i^{\lambda i(0)} \prod_{i \in GID} A^{s_i \lambda_i(0)} (\bmod p) \tag{5}$$

$$\lambda_i(0) = \prod_{j \in GID, j \neq i} (-j)(i-j)^{-1} (\bmod q) \tag{6}$$

ここで，$y_G = g^{f(0)}$ になっているので

$$\frac{B}{A^{f(0)}} = \frac{k_g^{f(0)r}}{g^{rf(0)}} = K (\bmod p) \tag{7}$$

となり，セッション鍵 K が復号できデータを復号することが可能となる．**図 8** は $m = 1$ の場合を示しており，ユーザ 2 とユーザ 3 はセッション鍵 K を取り出すことができ，復号することができるが，ユーザ 4 は鍵を取り出すことができず復号できないことを示している．

⑤ このようにして得られたセッション鍵で，暗号文を復号し，平文を求める．

5.3 処理時間の計測

今回はICカード方式と条件を揃えるためにしきい値 m を1として検討した．すなわち権利のある1人1人が復号したければ1人で復号できるように設定している．公開鍵利用方式における人数変化による鍵生成処理時間の変化を**図9**に示す．1,024 bit長の鍵を用い，5人から50人まで5人ずつ増やして1,000回計測し，その平均をとった．5人ならば，1秒強で鍵を生成することができるが，50人になると2分近くなり，5人のときと比較し100倍近くかかることが分かった．また復号処理時間も計測したので**図10**に示す．5人の場合1秒弱，50人の場合でも14秒弱の処理時間である．200人のグループならば，1分ほどで復号でき，復号処理より鍵の生成に時間がかかることが分かった．

この方式もつねにサーバを必要としないので ⑤の条件に適する．

6. 方式の比較・検討

ICカード利用方式と公開鍵利用方式の比較を**表2**に示す．表2より

(1) グループ人数が比較的大きいときは，処理速度の早いICカード利用方式の方が望ましい．公開鍵利用方式は，ICカード利用方式と比較し，10人のときで250倍，50人のときには5,400倍近い処理時間を要する結果となった．ICカード利用方式は今回の実験ではICカードの部分をPCで実現しているので，実際は150倍程度かかるが，それでもICカード方式のほうが短い処理時間ですむ．

(2) 両方式とも，運用時にサーバを必要としない．公開鍵利用方式における公開鍵の正当性は，認証局を用いるほうが望ましいが，PGPで行われ

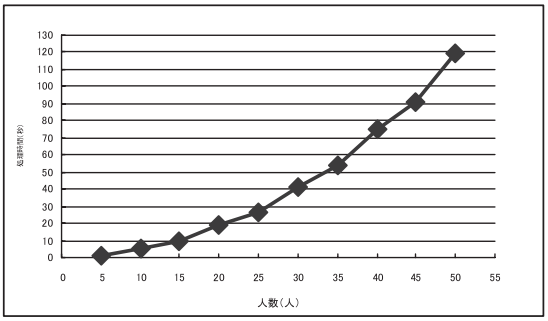

図9 公開鍵利用方式の人数変化による鍵生成処理時間
Fig. 9 Key generation processing time by number change of a public key use system.

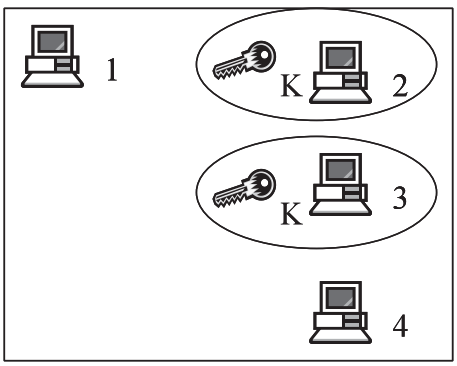

図8 復号鍵の取り出し
Fig. 8 Extraction of decipherment key.

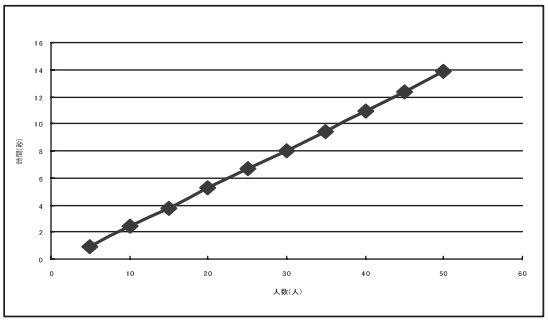

図10 公開鍵利用方式の人数変化による復号化処理時間
Fig. 10 Decryption processing time by number change of a public key use system.

表2 ICカード利用方式と公開鍵利用方式の比較
Table 2 Comparison of integrated circuit card use system and public key use system.

	処理時間			運用中に必要となるサーバの有無	トータルコスト
	10人	30人	50人		
ICカード利用方式 *	0.0213秒	0.0217秒	0.0221秒	○	×
公開鍵利用方式	5.206 秒	41.626秒	119.346秒	○	○

*PCでの処理時間である

ているように，入手した公開鍵より求めた Key fingerprint と，電話やメール，名刺などに記載されている Key fingerprint を比較することにより公開鍵の正当性を認証することができると思われる．鍵の無効化についても，センタを用い CRL などをチェックすることが望ましいが，各個人が自分の信用する人々のリストを逐次更新し，それを各人がチェックすることによりセンタを持たなくても対応可能であると考えられる．

(3) IC カード利用方式では，IC カード自体にタンパ性の問題があり，破壊型解析法のプローブ解析，非破壊解析法の故障利用解析やタイミング解析，電力解析など，さまざまな解析方法がある[3]．IC カード利用者に信頼をおきにくい場合は，システム上の問題が生じる．もしこのような解析方法によりマスタ鍵が盗み出されてしまうと，マスタ鍵の変更が必要になるため，使用している IC カードをすべて回収する必要が出てしまう．また IC カードリーダも使用する PC すべてに付ける必要があり，少なめに見積もっても IC カードリーダ非接触型で 1 台 3,000 円程度，IC カードも 500 円ほどコストがかかる．したがって，ユーザの限られた範囲，学内や社内において利用する P2P に有効な手段と思われ，インターネット利用での P2P 環境下で適するケースは比較的少ないと思われる．

(4) 公開鍵利用方式の場合，ユーザの公開鍵を用いてグループを操作することができる．復号鍵においては公開鍵暗号方式を利用しているため配布する必要がなく，遠距離にいるユーザに関しても容易に加えることができる．基本的に P2P に適していると考えられる．しかし，鍵の生成に関しては処理にかなりの時間がかかり，またグループメンバが変更になった場合，グループ鍵を作り直す必要がある．

7. 終わりに

今回は，グループ鍵生成を P2P において利用するために，IC カード利用方式と公開鍵利用方式における処理速度などの比較を行った．扱えるグループの大きさでは IC カード方式が，トータルコストでは公開鍵利用方式が望ましいことなどが分かった．

今後は公開鍵利用方式をさらに大きなグループにも適用しうるようにするとともに，ユーザ変更の対応や，鍵の失効などの検討を進めたいと考えている．

謝辞 本研究を進めるにあたり，暗号プロトコルに関しご指導くださいました日立製作所システム開発研究所宮崎邦彦氏に深く感謝申し上げます．

参考文献

1) 荒井正人，鍛 忠志，伊藤浩道，手塚 悟，佐々木良一：企業情報向けグループ暗号システム，情報処理学会論文誌，Vol.40, No.12, pp.4378–4388 (1999).
2) 沼尾雅之，渡邊裕治：P2P マルチキャストのための動的グループ鍵生成法，SCIS, pp.405–409 (2002).
3) 平成 11 年度スマートカードの安全性に関する調査調査報告書，情報処理進行事業協会（平成 12 年 2 月 29 日）．http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/SmartCard/index.html
4) 株式会社日立製作所：IC カード用半導体製品カタログ．http://www.hitachisemiconductor.com/sic/jsp/japan/jpn/PRODUCTS/ICCARD/index.html

(平成 14 年 12 月 2 日受付)
(平成 15 年 6 月 3 日採録)

渡邉 浩朗（学生会員）
1975 年 3 月 29 日生．1995 年埼玉工業大学専門学校情報処理科卒業．社会人を経て 1999 年東京電機大学工学部二部情報通信工学科入学．2002 年同大学同学科卒業．現在同大学院工学研究科情報通信工学専攻在籍．

加藤 貴法
1981 年 3 月 7 日生．2003 年東京電機大学工学部二部情報通信工学科卒業．同年株式会社日立コミュニケーションテクノロジー入社．

佐々木良一（正会員）

1971年東京大学卒業．同年日立製作所入所．システム開発研究所にてセキュリティ技術，ネットワーク管理システム等の研究開発に従事．同研究所主管研究長兼セキュリティシステム研究センタ長等を経て現在東京電機大学工学部教授．工学博士（東京大学）．情報処理学会論文賞，電気学会論文賞，著作賞受賞．著書に，「インターネットセキュリティ入門」（岩波新書，1999年）等．情報処理学会フェロー，理事．情報処理学会コンピュータセキュリティ研究会顧問．IFIP TC11日本代表．

江口　雄介

1979年9月9日生．2002年東京電機大学工学部第一部情報通信工学科卒業．同年東京通信ネットワーク株式会社入社．通信設備の建設・保守業務に従事．

安永　洋平

1979年9月21日生．2002年東京電機大学工学部一部情報通信工学科卒業．同年アマノ株式会社入社．ソフトウェア開発に従事．

吉田　兼也

1979年3月17日生．2002年東京電機大学工学部第一部情報通信工学科卒業．同年株式会社電算入社，自治体関連システムの開発に従事．