L-019

# 携帯電話網を用いた公開鍵交換システム

Public Key Exchange System by means of Mobile Phone Network

坂本千鶴[*1] G. De Marco[*1] 多々内允晴[*1]
Chizuru Sakamoto Masaharu Tadauchi

## １．はじめに

現在，ネットワークにおける情報システムセキュリティのための取り組みが数多くなされている．その中でも，公開鍵暗号方式を用いた暗号化と電子署名は非常に有効な方法であり，これにより情報の秘匿性と完全性，および送受信者の認証が満足できる．しかしこの方式では，公開鍵が偽の鍵とすり返られると大きな問題となる．インターネット上では相手を認証することが難しいという問題から，証明されていない鍵は信頼性が低い．このため，信頼の輪やPKI，IBE などの方法がとられているが，個人がこれらの方法を利用して各々の鍵を持ち，日常的に E メールなどを暗号化することはまだ少ない．これはユーザのセキュリティへの意識の低さのためだけではなく，第三者に証明してもらうには手間や費用がかかることが利用の妨げとなっているためである．

そこで本論文では，このような問題を解決するために，携帯電話網を用いた公開鍵交換システムを提案する．携帯電話網はインターネット網と比較して認証性が非常に高く，良く知る者の間における鍵交換ならば，鍵証明のための特別な第三者機関が無くても信頼できる鍵を入手することができる．

さらに実際の利用に際し，複数の鍵を要求するときには，コストや利便性を考えると，すべての相手にそれぞれ要求信号を送るよりも，数人の信頼できる相手から，持っている鍵をまとめて受け取り，検索する方が良いことを，シミュレーションにより示す．

## ２．既存システム

公開鍵証明における多くの方法の中で，典型的なものを 3 つ挙げる．

a) 信頼の輪 (PGP)

ユーザ間で鍵を証明し合う方法で，証明書に公開鍵と所有者情報を含め，他のユーザがその証明書に電子的に署名をすることにより信頼性を与える．例えば，ある程度信頼できる推薦人が何人か署名をしていたら，その鍵を信頼する．あるいは，一人の完全に信頼できる推薦人が署名をしていたら，それだけで鍵を信頼する．この方法は柔軟性があり，実施しやすいが，輪が広がりすぎると証明書の信頼性が落ちるという欠点がある．

b) PKI (Public Key Infrastructure)

認証局(CA)が電子証明書に署名をすることで，公開鍵と所有者の正当性を証明する方法．PKI では CA の信頼性や証明書失効リストの管理が問題となる[1]．また申請手続きの手間や費用が利用の妨げになっている．

c) IBE (Identity Based Encryption)[2]

ユーザ固有の情報が公開鍵として使えるシステムで，例えばE メールアドレスを公開鍵としてそのまま使うことができる．これにより，証明書が不要となる．また PKG(Private Key Generator)サーバが公開鍵と一致する秘密鍵を作り，サーバ上で秘密鍵を管理するため，ユーザは鍵の管理から開放される．しかし，インターネットのような匿名性の高いシステムでは確実な認証は難しく，成りすましによって秘密鍵が盗まれる危険性が高い．さらにサーバに欠陥が生じた場合のリスクが大きいことも問題である．

## ３．提案システム

### 3.1 記号定義

| | |
|---|---|
| M | メッセージ |
| $Pk_A$ | A の公開鍵 |
| $\{M\}_A$ | A の公開鍵による M の暗号化 |
| $[M]_A$ | A の秘密鍵による M の復号または電子署名 |
| $(M)_K$ | セッション鍵 K による M の暗号化 |
| S | 公開鍵要求信号（シングルクエリ） |
| $S_M$ | 公開鍵要求信号（グループクエリ） |
| A → B : S | A が B に信号 S を送る |
| $P_A$ | A が保持している鍵の集合 |
| $G_A$ | A の接続グループまたは接続リスト |
| $T_A$ | A の電話番号 |
| $ID_A$ | A の ID |
| PMN | 携帯電話網 (Public Mobile Network) |

### 3.2 本システムにおける携帯電話網と公開鍵の役割

ここで言う携帯電話網とは，携帯電話における音声通話網のことである．

インターネットでは本人性を認証することが難しく，中間者攻撃や成りすましが容易であり，受け取った公開鍵が本当に相手のものであるか確認できないため，鍵の証明が必要とされる．それに対して携帯電話による通信では，事業者によって通信毎に端末の認証が行われ，且つ 1 台の端末を複数人で使用することは少なく，多くは常に携帯している物なので，端末＝本人と認識することは容易である．したがって，インターネット網や固定電話網を介さず，携帯電話網のみを利用するならば，中間者攻撃や成りすましは容易でない．ただし，クローン携帯が存在する場合や，端末を盗難された場合は例外である．また，現在第 3 世代携帯電話の一部では，KASUMI（霞）という暗号化アルゴリズムが導入されており，基地局‐端末間の無線通信路での盗聴は防止され，改ざんの検出も可能となっている．しかし，全ての携帯電話が KASUMI に対応しているわけではなく，また基地局間の通信は暗号化されているか定かでないため，盗聴の可能性を否定できない．そこで，携帯電話網で交換する鍵は共有鍵ではなく，盗聴されても問題のない公開鍵を用いることで，この問題を解決する．

*1 豊田工業大学大学院先端工学専攻
Graduate School of Tovota Technical Institute

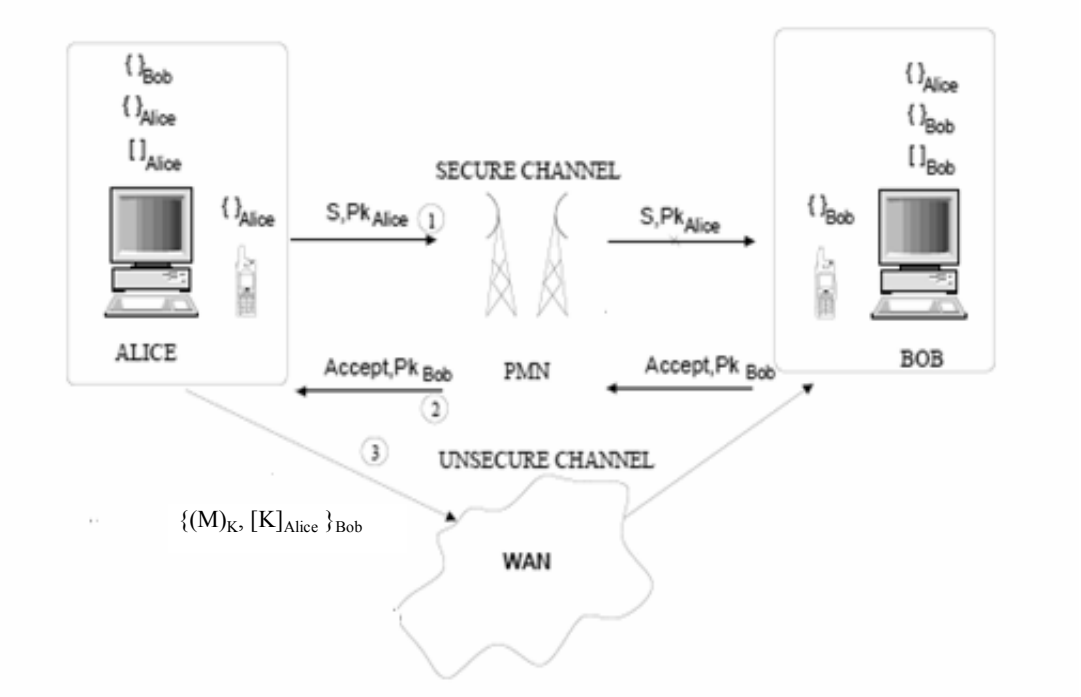



図-1 システム構成図

### 3.3 仮定

本システムは以下の条件のもとに安全性を確保するものである．

a) 通信相手とは面識があり，携帯電話の番号を互いに知っている．
b) すべての通信相手は携帯電話を持っている．また，それらの携帯電話は公開鍵を備え，管理するための専用のソフトウェアがインストールされている．
c) 得られた公開鍵は他の通信に利用するために，ＰＣの特定のファイルに保存する．
d) 秘密鍵は誰にも見られないように保管されている．
e) 携帯電話が鍵の要求信号を受信するために，携帯電話網は特別なメッセージサービスを有する．
f) 鍵要求信号 S を受信した者は送信を拒否することも可能である．
g) 本システムは相手がデータを送りたい場合にいつでも使用できる．

### 3.4 鍵交換の手順と利用方法

鍵交換と鍵の利用方法を簡単に述べる．図-１に，Alice (A) が Bob (B)に安全にデータを送りたい場合を例にして，本システムのプロトコルを示す．

はじめに，A は鍵要求信号Ｓを A の公開鍵 $Pk_A$ を添えて B の携帯電話に送信する(step 1)．もし B の携帯電話が通信可能で，B が A からの信号を許可するなら，B は許可信号(ACCEPT)を B の公開鍵 $Pk_B$ も添えて送信する(step 2)．

Ｂの公開鍵を受信した A は，セッション鍵Ｋを使ってメッセージ M を暗号化し(Perfect Forward Secrecy のため)，K を A の秘密鍵で電子署名をすることで A からのメッセージであることを証明する．これらを B の公開鍵で暗号化することで，対応する秘密鍵を持つ B だけがメッセージを読めるようにする（$\{(M)_K, [K]_A\}_B$ ）．

## ４．解析

多数の人の鍵が一度に必要な場合でも，一人一人に要求する方が当然鍵の信頼性は高いが，コストや利便性を考慮すると，複数の鍵を一度に入手する方法も有効である．したがって，ここでは複数の公開鍵を要求する場合についてコストの解析を行う．

### 4.1 記号定義

| | |
|---|---|
| N | ネットワーク内のノード数 |
| $k_i$ | ノード i が持つエッジ数（アドレス登録数） |
| p | ネットワークのリンク率 |
| d | ネットワークの平均リンク数 |
| S | シングルクエリ |
| $S_M$ | グループクエリ |
| $U_S$ | S によるコスト関数 |
| $U_M$ | $U_S$ によるコスト関数 |
| $T_h$ | 1 パケットのサイズ |
| $\gamma_i$ | $S_M$ の数で，ノード i は $\gamma_i$ 人に鍵を要求する |
| $p_S$ | 希望する鍵集合がすべて得られる成功確率 |
| $N_\gamma^i$ | ノード i が $S_M$ を $\gamma_i$ 人に送るときのその集合 |

### 4.2 ネットワークの定義

知人関係のネットワークにおいては，自分（A）と知人（B)のどちらも知っている共通の知人が一人もいないという状況は少ない．したがって，ここでは人の関係性を，クラスタ性を持つグラフＧ(V,E)を用いてモデル化する．V は頂点集合，E はエッジ集合である．２つの u, v∈Ｖ の間のエッジは u と v が携帯電話番号を互いに知っていることを意味する．

シミュレーションは，A が以下の 2 通りの方法のいずれかで，すべての知人の鍵を要求する場合について行う．

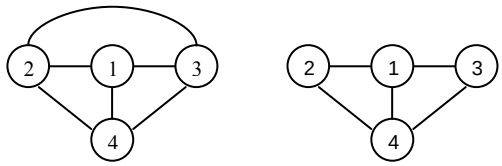
(1) ひとりひとりにシングルクエリＳを送る．
(2) 一部のグループＲ⊂$G_A$にグループクエリ $S_M$ を送る．

後者ではAが要求する複数の鍵を，知人 B がすべて持っている場合，一回の要求で複数の鍵を入手できる．ここでは，上記 3.3 の操作を行う場合には，完全に信頼できる鍵を得ることができるものとしてシミュレーションしているが，実際にはひとりひとりと直接鍵交換を行わなければ，鍵の信頼性は十分でない．したがって，A は必要な信頼性に応じて 2 つの方法を選択する必要がある．

グループクエリを送る場合，その人の知人ネットワークが広いほど，要求するすべての公開鍵を得られる確率は高くなる．この確率はクラスタ係数から見て取ることができる．ここでノード i ∈V のクラスタ係数$C_i$とネットワークのクラスタ係数 C は，式(1)で定義される．

$$C \equiv \frac{1}{N}\sum_{i=1}^{N} Ci\ ,\quad C_i = \frac{2E_i}{k_i(k_i-1)} \qquad (1)$$

ただし，$E_i$ はクラスタ数である．あるノードがすべてのノードとリンクしていればクラスタ係数は 1 となり，誰か一人にグループクエリを送信すれば，すべての人の鍵が手に入る．したがって，図-2 の $C_I$= 1 のグラフと $C_I$= 2/3 のグラフを比較すると，C=1 のグラフならば， 一人へ鍵を要求すれば，残りの人の鍵もすべて受け取ることができる．




$C_I$ = 1　　$C_I$ = 2 / 3

図-2　クラスタ係数

また，ネットワークのリンク率 p は，実際のリンク数 L と完全グラフにおけるリンクの数の比で表される．ノードが N 個の完全グラフにおけるリンク数は

$${}_N C_2 = \frac{N(N-1)}{2}$$

であるから

$$p = \frac{2L}{N(N-1)} \qquad (2)$$

となる．したがって，グラフ G(V, E)は Erdos-Renyi ランダムグラフ G(p, N)となる．

### 4.3 コスト関数の定義

多数の S を送信する場合と，いくつかの $S_M$ を送信する場合のコストを単純に比較するために，自分の携帯電話のアドレスに登録されている人全員の鍵を要求する場合について考える．ここでは信号と鍵をそれぞれ 1 パケット以下とする．

まずシングルクエリ S を用いる場合，ノード i がアドレスに登録している人全員に S を一回ずつ送信し，各々から鍵が返信されるため，コスト関数は次のように定義される．

$$U_S^i(k_i) = 2k_i \qquad (3)$$

次にグループクエリ $S_M$ を用いる場合，$S_M$ を受け取ったノード j は，アドレスに登録されているすべての人の鍵 $k_j$ 個を返信する．このときのコストは，

$$\gamma_i + \sum_{j\in N_\gamma^i}\left\lceil \frac{k_j}{T_h}\right\rceil$$

である．一方，グループクエリを送っても，返信された鍵集合の中に，ノード i が必要とするすべての鍵が含まれていなければ，残りの( $k_i$ − $\gamma_i$ )人にシングルクエリ S を送るとする（図-3）．

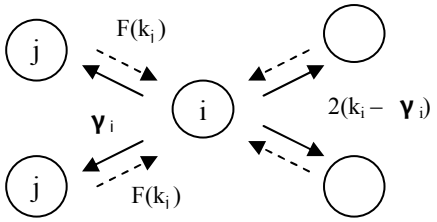



図-3　グループクエリの場合のコスト

このコストは，

$$\gamma_i + \sum_{j\in N_\gamma^i}\left\lceil \frac{k_j}{T_h}\right\rceil + 2(k_i-\gamma_i)$$

である．前者は確率 $p_S$ ，後者は確率(1 - $p_S$ )で起こるので，グループクエリのコスト関数は次のように定義される．

$$U_M^i(k_i) = p_s\left[\gamma_i + \sum_{j\in N_\gamma^i}\left\lceil \frac{k_j}{T_h}\right\rceil\right] + (1-p_s)\left[\gamma_i + \sum_{j\in N_\gamma^i}\left\lceil \frac{k_j}{T_h}\right\rceil + 2(k_i-\gamma_i)\right]$$

$$U_M^i(k_i) = \gamma_i p_s + \sum_{j\in N_\gamma^i}\left\lceil \frac{k_j}{T_h}\right\rceil + (1-p_s)(2k_i-\gamma_i) \qquad (4)$$

ただし，$\gamma_i$ は k をパラメータとして次のように決める．

$$\gamma_i \overset{\Delta}{=} \left\lceil \frac{k_j}{k}\right\rceil \qquad (5)$$

ネットワーク全体の平均は，Jensen の不等式を用いて以下のようになる．

$$\overline{U_S}(d) = 2d \qquad (6)$$

$$\overline{U_M}(d) \le \gamma p_s + \frac{\gamma d}{T_h} + (1-p_s)(2d-\gamma) \qquad (7)$$

$$\gamma = \frac{d}{k} \qquad d = \bar{k}_i = p(N-1) \qquad (8)$$

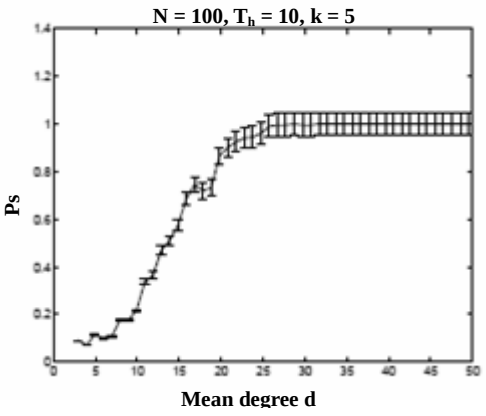
これらのコストはあくまでも最悪の場合を想定した場合のものである．

## ５．シミュレーション

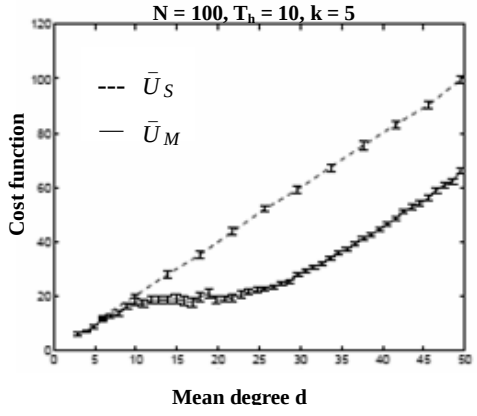
式(6),(7)のコスト関数を計算するために，モンテカルロシミュレーションを行う．MATLAB でユーザ数N= |V| = 100 のランダムグラフG（p, N）をシミュレーションする．成功確率 $p_s$ は 0.003 から 0.5 の値を取るとし，200 回の計算の平均を求めることで，ネットワーク全体の平均成功確率および平均コストを算出する．これらの評価指標を計算するために，ランダムにノード i と $\gamma_i$ を選択する．図-4(a)(b)では，平均リンク数 d に対する成功確率 $p_s$ と平均コスト $\bar{U}_S$，$\bar{U}_M$ をそれぞれ示す．

成功確率 $p_s$ はネットワークの平均リンク数 d が多くなるほど高くなり，d > 25 で 1 に収束する．コストはリンク数が d < 10 なら，$S_M$ を送る場合も S を送る場合もほとんど変わらないが，それ以降は $\bar{U}_M < \bar{U}_S$ になる．したがって，関係性の小さなネットワークでは，S より $S_M$ を使用する方がよいことがわかる．

また，これらは $T_h$ = 10 で計算しているが，図-5 では，$T_h$ = 1 の場合の結果を示す．このように携帯電話網のコストが高い場合には，S を送るほうがよいことがわかる．




(a)




(b)

図-4　シミュレーション結果

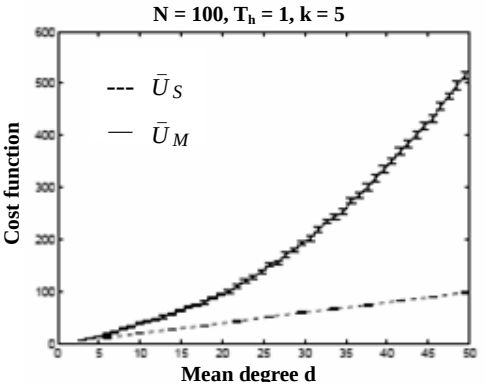



図-5　$T_h$ = 1 の場合

## ６．提案システムの問題点

提案システムの脆弱性としては 2 つ考えられる．まず，携帯電話を直接第三者に操作される，またはコンピュータウイルスに感染することによって公開鍵が書き換えられる恐れがあることである．これにより A の公開鍵が B のものとすり返られ，B がインターネット上で A を装い重要なデータを得ることができてしまう．今のところ携帯電話内のデータを直接書き換えられるようなウイルスは存在していないが，今後更なる携帯電話の高機能化に伴い，このようなウイルスが出現することも予想される．

2 つ目として，クローン携帯による成りすましの問題である．A のクローン携帯を B が入手できれば，B の公開鍵を A の公開鍵として相手に信用させることができてしまう．現在，事業者はクローン携帯の存在を否定しているが，可能性はありうる．

## ７．まとめ

本論文では，鍵サーバや特別な機関を利用しなくても，手軽に信頼性の高い公開鍵を入手するために，携帯電話システムを利用した交換方法を提案した．提案システムはユーザが互いに信頼し合っていることを前提にしているので，信頼の輪のシステムと類似している．しかし本システムでは，既存の信頼の輪のようにインターネットを介するのではなく，携帯電話網の認証性の高さを利用することで，信頼性の高い鍵を交換できる．

また，公開鍵の要求にグループクエリを使う場合の解析をランダムグラフ上で行い，複数人の鍵を要求する場合には，コストの観点からグループクエリを送る方がよいことを示した．ただし，信頼性を考慮すると，シングルクエリでひとりひとりと鍵を交換する方がよいことは言うまでもない．信頼性とコストはトレードオフの関係にある．

## ８．参考文献

[1] K. Bicakci, B. Crispo, and A. S. Tanenbaum. How to incorporate revocation status information into the trust metrics for public-key certification. *International Journal for Infonomics Special Issue Selected papers of the ACM SAC 2005 TRECK Track*, pages 1-10, 2005

[2] Dan Boneh, Matthew Franklin. Identity-Based Encryption from the Weil Pairing. *The Proceedings of Crypto 2001*, volume 2139 of Lecture Notes in Computer Science, pages 213-229, Springer-Verlag, 2001