# ゼロ知識証明を用いたユーザ登録方式の設計

2G−4

佐藤　信　　千葉　則茂*
岩手大学工学部情報工学科

## 1　はじめに

インターネットおよびイントラネットなどの相互接続型ネットワークは，独立したネットワークを組み合わせることにより柔軟にネットワークを構成できる．このような相互接続型ネットワークにおいてセキュリティを確保するために，公開鍵暗号を基本にしたプロトコルが使用される．この公開鍵を配布する方式として，認証局を使用する方式が研究開発されている[1]．本稿では，認証局を使用せずに，安全に公開鍵を配布しユーザ登録をおこなうプロトコルの設計について述べる．本プロトコルは，知識の所有のゼロ知識個人認証プロトコルであるFiat-Shamir法[2]を基本としたメッセージ認証プロトコル[3]を応用したものである．本プロトコルにより，相互接続型ネットワークで，認証局を使用せずに柔軟，容易そして安全にユーザ登録することが可能となる．

## 2　プロトコルの設計方針

秘密鍵の所有者が，認証局を使用せずに直接公開鍵を配布する方式と比較すると，認証局を使用した公開鍵配布方式の特徴はつぎの点である．

1）認証局を使用して，通信相手の公開鍵を効率良く入手することが可能である．いっぽうそれぞれの認証局および公開鍵の信頼のレベルを考慮する必要がある．
2）認証局と通信不可能な場合は，公開鍵キャシュに格納されている公開鍵を使用可能である．しかし，認証局と通信可能な場合と比較して，よりいっそう公開鍵の有効期限を考慮する必要がある．
3）公開鍵を配布される者は，認証局から公開鍵を入手する段階で，公開鍵に対応する秘密鍵の所有者に，公開鍵の正当制を確認できない．

本稿で提案する，秘密鍵の所有者が，直接公開鍵を配布する方式の特徴はつぎの点である．

1）公開鍵を配布される者は，その公開鍵に対応する秘密鍵の所有者に，直接，公開鍵の正当性を確認できる．
2）認証局を使用しないので，公開鍵を配布される者と，その公開鍵に対応する秘密鍵の所有者が通信可能であれば，公開鍵を配布可能である．
3）公開鍵を配布される者は，公開鍵を使用する前に公開鍵の正当性を確認できる．
4）人間同士のコミュニケーションに近い，認証方式である．

本稿で提案するプロトコルのポイントは，つぎの点である．

1）公開鍵の安全性のみを仮定して，公開鍵を配布される者（検証者）と，その公開鍵に対応する秘密鍵の所有者（証明者）の間に，セキュリティチャネルを構成可能である．
2）証明者と検証者が認証のために使用したユーザ認証のための通信データを，再使用することが不可能である．

セキュリティチャネルを構成するための従来のプロトコルでは，メッセージ認証のための通信データの再使用を回避するために，暫定数またはタイムスタンプをする[4]．ユーザ登録する以前に，証明者と検証者が使用するそれぞれのコンピュータが，暫定数，タイムスタンプを使用するための準備をおこなっていない場合でも，ユーザ登録可能なように，提案のプロトコルでは，暫定数またはタイムスタンプを使用しない．また，提案のプロトコルでは，通信相手が正当であるかどうかを確認するために，お互いの画像データおよび音声データを送信してユーザ認証のための会話をおこなう．このときのユーザ認証のための通信データは，第三者はもちろん検証者でも再使用不可能である．

---

*Design of User Registration Protocol Using Zero-Knowledge Interactive Proof, Makoto Satoh, Norishige Chiba,Iwate University, Department of Computer and Information Science 4-3-5 Ueda,Morioka,Iwate 020-8551,Japan

## 3　メッセージ認証プロトコル

**（前処理）** 証明者は剰余計算に使用する素数$p,q$の合成数$n=p*q$を決定する．秘密鍵$s$を作成してこれより公開鍵$I=s*s(mod\ n)$を作成する。証明者は$n,I$を検証者に知らせる．

**（認証処理）** 以下の手順を$O(|n|)$回繰り返す．

step1: 証明者は乱数を生成して，
$X=r*r(mod\ n)$を計算する．
証明者は$X$を検証者に送信する．

step2: 検証者は乱数ビット$e\in\{0,1\}$を
生成して，これを証明者に送信する．

step3: 証明者は$e=0$のとき，$Y=r$,
$e=1$のとき，
$Y=r*s*\mathrm{t}*(\mathrm{r}*\mathrm{s}+\mathrm{t})\ (mod\ n)$
を計算して検証者に送信する．
$t$はメッセージである．
証明者は，繰り返しの最後で，
$T=t*t(mod\ n)$を計算し，
$T$を検証者に送信する．

step4: 検証者は$e=0$のとき，
$X\equiv Y*Y\ (mod\ n)$を確認する．
繰り返しの最後で，$e=1$のときの
それぞれの$X,Y$，$I$と$T$から
$P\equiv r*s*t\ (mod\ n)$を計算し，
$P*P\equiv\ (X*I*T)^2(mod\ n)$を確認する．
$t=Y*(X*I+P)^{-1}(mod\ n)$
を計算する．

すべての，検査に合格したら，証明者は公開鍵$I$に対する秘密鍵$s$を所有していることを確認できる．このとき，メッセージ$t$が全て同じならばメッセージ認証も知識の所有の対話証明と同程度の健全性である．

## 4　ユーザ登録方式

ゼロ知識証明を用いたユーザ登録方式について説明する．ユーザ登録を要求する者（証明者）と要求されるもの（検証者）の通信には３節のゼロ知識個人認証を用いたメッセージ認証を使用する．また，メッセージとして証明者と検証者の画像と音声を送信する．画像には，埋め込み情報を取り出すのに必要な情報を公開可能な電子透かしを埋め込む[5].

Step1: 証明者は，メッセージ認証に使用する合成数$n_p$および秘密鍵$s_p$を決定し，公開鍵$I_p$を作成する．証明者は$n_p$および$I_p$を検証者に送信する．

Step2: 検証者は，メッセージ認証に使用する合成数$n_v$および秘密鍵$s_v$を決定し，公開鍵$I_v$を作成する．検証者は$n_v$および$I_v$を証明者に送信する．

Step3: 証明者と検証者は，それぞれがこれから送信する画像の電子透かしの埋め込み情報を取り出すのに必要な情報を，メッセージ認証を使用してお互いに送信する．

Step4: 証明者と検証者は，メッセージ認証を使用してお互いの画像と音声を送信して，会話をおこなう．検証者は，証明者がユーザとして妥当であると判断したら，システムに登録する．このとき，画像の電子透かしの埋め込み情報としては，メッセージの送信者の公開鍵を使用する．メッセージの受信者は，受信画像の，電子透かしの埋め込み情報を取り出す．そして，取り出した情報が，送信者のメッセージを受信者が認証するための公開鍵に等しいことを確認する．

## 5　おわりに

提案のプロトコルにより，相互接続型ネットワークで認証局を使用しないで柔軟，容易そして安全に知識の所有のゼロ知識証明を用いたユーザ認証をおこなえる。認証局を使用した公開鍵配布方式の機能を補完するために，提案の方式を使用することもできる．たとえば，認証局への公開鍵の登録時，または，何らかの原因により認証局を使用できないときの通信方式として提案の方式を使用できる．今後は，本プロトコルをグループ認証プロトコルに拡張する予定である．

参考文献


1）Menezes, van Oorschot, Vanstone : HANDBOOK of APPLIED CRYPTOGRAPHY, CRC press(1997)

2）太田，藤岡：ゼロ知識証明の応用，情報処理　Vol.32 N0.6, pp.654-662(1991)

3）佐藤，阿部：ゼロ知識個人認証を用いたメッセージ認証プロトコルの設計，情報処理学会第５８回全国大会論文集（第１分冊），pp.339-340(1999)

4）GEORGE COULOURIS 他：分散システム，電気書院，pp.859-888

5）岩村，山口，今井，公開抽出情報を用いる電子透かし手法の提案，コンピュータセキュリティシンポジウム'98 論文集，pp33-38(1998)