5 L − 2

相互接続型ネットワークでのゼロ知識相互個人認証プロトコルの統計的識別不可能性

佐藤 信　　阿部 芳彦 *
岩手大学工学部情報工学科

1 はじめに

本稿では，相互接続型ネットワークのためのゼロ知識相互個人認証プロトコルの通信データのプロトコルデータを剰余計算するのに使用する法の統計的識別不可能性について述べる。相互接続型ネットワークは柔軟なネットワークを構成できる。しかし，セキュリティ上の問題として，データの盗聴，改ざんそしてなりすましを指摘できる。そこで，ゼロ知識個人認証プロトコルである Fiat-Shamir 法 [1] を拡張してこのネットワークで柔軟，容易そして安全に相互個人認証するプロトコルを設計した [2]。このプロトコルは知識の所有のゼロ知識証明であり，さらに通信データから法と公開鍵を推定しにくくしている。そこでこれを利用して，検証者が公開鍵を所有していることを証明者に知識の所有のゼロ知識証明をすることにより検証者の正当性の確認をおこなっている。このプロトコルを改良してその通信データがプロトコルデータを剰余計算するのに使用する法に対して統計的識別不可能であることを示す。

2 プロトコルの概要

（前処理）証明者は剰余計算に使用する素数 $p,q > N$ の合成数 $n = p*q$ を決定する。素数環 p,q の原始根を p_g, q_g，平方剰余を p_s, q_s とする。中国人の剰余定理により環 n での (p_g,q_g)，(p_g,q_s)，(q_g,p_s) に対応する数を $ns[0]$，$ns[1]$，$ns[2]$ とする。
パスワードを変換鍵 k でインボルーションして秘密鍵 s を作成してこれより公開鍵 $I = s*s(modn)$ を作成する。証明者は n, N, k, I を検証者に知らせる。
（認証処理）認証処理は 4 段階で構成される。

秘密鍵の作成

検証者は証明者に変換鍵 k を送信する。証明者はパスワードを変換鍵 k でインボルーションして秘密鍵 s を作成する。

法の自動決定

検証者は $I*I$ から $n < A < n*N$ のビットパターン A を作成するためのデータ B を作成して $C = A(mod\ n)$ を計算する。検証者は B,C を証明者に送信する。証明者は $s*s*s*s$，複数所有している n とデータ B からビットパターン D をを作成して $E = D(mod\ n)$ とデータ C 比較して使用する n を決定する。検証者は認証者と共有する乱数系列 t のシード $seed$ を発生して $expand(seed) \otimes expand(I)$ を認証者に送信する。

拡張 Fiat-Shamir 法

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。
乱数ビット $t \in \{0,1\}$ を生成して
$t = 1$ であり，そのカウントが偶数で
ないならば，均等に $i \in \{0,1,2\}$ を使用して，
$X = ns[i]*X(mod\ n)$ を計算する。
$t = 0$ ならば，
$X = expand(X) \otimes (\neg expand(I))$
$t = 1$ ならば，
$X = expand(X) \otimes expand(I)$
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，
$Y = r\ (mod\ n)$
$e = 1$ のとき，
$Y = r*s\ (mod\ n)$
を計算して
$t = 0$ ならば，
$Y = expand(Y) \otimes (\neg expand(I))$
$t = 1$ ならば，
$Y = expand(Y) \otimes expand(I)$
を検証者に送信する。

step4: 検証者は，
乱数ビット $t \in \{0,1\}$ を生成して
$t = 1$ であり，そのカウントが偶数ならば，
$reduce(Y \otimes expand(I))^2 \equiv$

*Statistical Indistinguishability of a Mutual Identification Protocol Using Zero-Knowledge Proofs in Interconnected Network, Makoto Satoh, Yoshihiko Abe ,Iwate University, Department of Computer and Information Science 4-3-5 Ueda,Morioka,Iwate 020,Japan

$reduce(X \otimes expand(I)) * I^e \ (mod\ n)$
を確認する。

ここでexpand(X)は，0からn-1のビットパターンを0から$2^{|n|}$-1にほぼ均等に拡張する。

検証者の正当性の確認

検証者はIを所有していることを証明者に拡張Fiat-Shamir法で証明する。

これらの検査に全部合格したら，検証者は証明者が公開情報(n, N, k, I)に対応するユーザであると判断し，証明者は検証者が正当であると確認する。

3　プロトコルの変更点

プロトコルで使用している関数expandを次のように変更する。

```
expand(X) {
  center = 0
  width = 法の値 + 1
  digit = 法の桁数
  while( width != 2^digit ) {
    if ( X ≥ center ) {
      if ( width == ODD ) {
        width = width + 1
        X = X + ( 2^digit - width ) / 2
        center = center + 2^(digit-1)
        if ( X == center ) {
          乱数ビット e ∈ {0,1}を発生する
          if ( e == 1 ) X = X + 1}
        elseif ( X > center ) X = X + 1 }
      else {
        X = X + ( 2^digit - width ) / 2
        center = center + 2^(digit-1) }
      width = width / 2
      digit = digit - 1 }
    else （同様の処理） }
  return(X)
}
```

関数reduce(X)もこれと対応させて変更する。

4　検討

本プロトコルはshamirらの知識の所有の対話証明の定義（完全性，健全性）を満たしている。また，ゼロ知識証明の条件も満たしている。そして，原始根の性質と中国人の剰余定理とexpandにより任意の通信データをa, bとしてその任意のビットをi, jとすると，

$Prob(a[i] = b[i]) = Prob(a[i] = b[j]) = 1/2$

である。また統計的識別不可能性は次のように定義できる。

定義 $\{U(x)\}, \{V(x)\}$を確率変数の族とする。このとき，

$\forall k > 0 \exists N \forall n > N \forall x[(x, w) \in R \wedge |x| = n]$
$\Pr(x, U, V) < |x|^{-k}$

となるならば，$\{U(x)\}$と$\{V(x)\}$はRに関して統計的に識別不可能であるという。ただし，$\Pr(x, U, V)$は

$\sum_{\alpha \in \sum^*} |\ \Pr\{U(x) = \alpha\} - \Pr\{V(x) = \alpha\}$

で定義されるものとする。

0から$2^n - 1$の範囲に均等に数値を発生させる場合と法$|width| = n$を使用する本プロトコルの通信データを比較すると，

$$Pr(x, U, V) = \frac{(2^n - width)(2 * width - 2^n) * 2}{2^n * width}$$

となる。これは次のようにnが変化しても$width/2^n$にたいして同じ値をとる関数である。上記の定義を満たす区間$[2^{n-1}, 2^{n-1}+a], [2^n-1-b, 2^n-1]$が存在する。ここで，$f(k, n) = a, b$である。

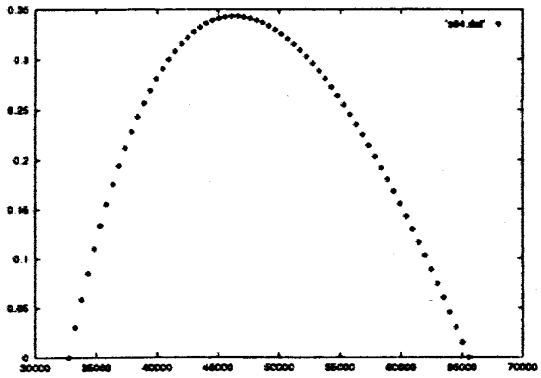

図1: Pr(x,U,V)

5　おわりに

相互接続型ネットワークで柔軟，容易そして安全にゼロ知識相互個人認証をおこなえる。認証局を使用した認証システム[3]と本プロトコルを併用することにより，認証局の負荷を軽減可能であり，プライバシーを重視した通信も可能である。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）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)

2）佐藤，阿部：相互接続型ネットワークでのゼロ知識相互個人認証プロトコル，情報処理学会第54回全国大会，第3分冊 pp509-510

3）Ueli Maurer,Modelling a Public-key Infrastructure,ESORICS96, LNCS1146 Springer pp325-350