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

1T－3

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について述べる。このネットワークは独立したネットワークを相互接続することにより柔軟なネットワークを構成できる。しかし，各サイトの管理運営組織が異なる場合，通信をおこなう端点間の経路上のサイトの機能で一定レベル以上のセキュリティを確保するのが困難である。そのため通信をおこなう端点間のプロトコルのみで一定レベルのセキュリティを確保する機能が必要となる。そこで，ゼロ知識個人認証プロトコルであるFiat-Shamir法を拡張してこのネットワークで柔軟，容易そして安全に個人認証するプロトコルを設計した。参考文献2）のプロトコルは対話証明であるがゼロ知識ではないのでこれを改良して参考文献3）を設計した。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が正当であることを確認する相互個人認証プロトコルを設計した。

2　プロトコルの設計方針

個人認証方式を分類するとつぎのようになる。

1)認証者がパスワードそのものを検証者に送信する。
2)使い捨てパスワード方式。認証者が一方向性関数によりパスワードを変換してそれを検証者に送信する。
3)認証者と検証者が知識の所有のゼロ知識対話証明をして認証者がパスワードを所有していることを確認する。

相互接続型ネットワークでは，回線上のデータを第３者が比較的容易に観測可能であるので，１）の方式では充分なセキュリティが得られない。方式２）は不正な検証者に対してセキュリティが充分でない。そこで設計したプロトコルでは知識の所有のゼロ知識対話証明であるFiat-Shamir法を使用している。
Fiat-Shamir法の通信データをある程度観測すると，プロトコルでおこなう剰余計算で使用している法を予測できる。そこで，特定の証明者と検証者が使用している法に対して素因数分解を試行できる。このプロトコルの安全性は法として使用している合成数の素因数分解の困難性と等価であるので，その時点では素因数分解困難な合成数を法として使用する。しかし，計算機の性能向上によりその合成数は安全でなくなる。また，個人認証をおこなう証明者と検証者の組み合わせが多数存在する。このため，Fiat-Shamir法を使用した本プロトコルの設計方針をつぎのようにする。

１）通信データから公開鍵と剰余計算に使用する法を予想しにくくする。この公開鍵を使用して検証者の正当性を確認する。
２）同じパスワードを使用しても同じ公開鍵を使用しない
３）パスワード以外のユーザデータは検証者が所有する

3　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

*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

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。

検証者は認証者と検証者が共有する乱数系列 t のシード $seed$ を発生して $expand(seed) \otimes expand(I)$ 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
$t = 1$ 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。
$X = expand(X) \otimes expand(I)$ 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 $Y = expand(Y) \otimes expand(I)$ 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
$t = 1$ のカウントが偶数ならば,
$reduce(Y \otimes expand(I))^2 \equiv reduce(X \otimes expand(I)) * I^e\ (mod\ n)$
を確認する。

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。

```
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
        乱数ビット e ∈ {0,1}を発生する
        if ( e == 1  X == center )
          X = X + width − 1
        }
      }
      X = X + ( 2^digit − width ) / 2
      width = width / 2
      digit = digit − 1
      center = center + 2^digit
  }
```

reduce(X) はこれと反対の変換をしている。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。

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,
$Prob(a[i] = a[j]) = 1/2$
$Prob(a[i] = b[j]) = 1/2$
である。

5 おわりに

本プロトコルにより, 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。今後は個人認証通信プロトコルにも本プロトコルを使用できるように汎用的に本プロトコルをサポートするソフトウエア・アーキテクチャを設計する予定である。また, 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個人認証プロトコル, 情報処理学会第 52 回全国大会, 第 4 分冊 pp347-348
3）佐藤, 阿部：相互接続型ネットワークでのゼロ知識個人認証プロトコルの設計, 情報処理学会東北支部 1996 年度第 3 回研究会 96-3-14