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

1S－2

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に構成できる。しかし，セキュリティレベルが各サイトで異なる，第３者が回線上のデータを比較的簡単に観測可能であるという点を指摘できる。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。そこで，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。そして，このプロトコルを使用できるように telnet プロトコルを変更した。

2　プロトコルの設計方針

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。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。

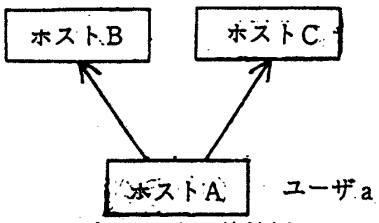

図 1: ホストの接続例

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。このために図１のように，ユーザａがホストＡから管理者の異なるホストＢとホストＣを使用する場合には，同じパスワードを使用してもホストＢとホストＣに格納されているプロトコルで使用するユーザａの公開データは異なるほうがセキュリティ上は好ましい。このため，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

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。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）認証処理は図２のように３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。

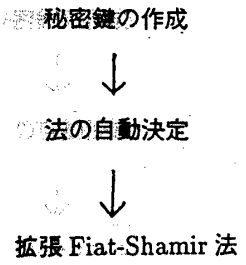

図 2: プロトコルの概要

An 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

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*A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Cをを作成して$E = D * D(mod\ n)$とデータC比較して使用するnを決定する。これらをIとsの最初の1桁についておこなう。
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を計算して,
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,
$2 * (r * s)^3 \geq 0\ (mod\ n)$ならば
$Y = r * s(r + s)\ mod\ n$
$2 * (r * s)^3 < 0\ (mod\ n)$ならば
$Y = r * s(r - s)\ mod\ n$
e=1のとき,
$2 * (r * s)^3 \geq 0\ (mod\ n)$ならば
$Y = r * s(r - s)\ mod\ n$
$2 * (r * s)^3 < 0\ (mod\ n)$ならば
$Y = r * s(r + s)\ mod\ n$
を計算して検証者に送信する。

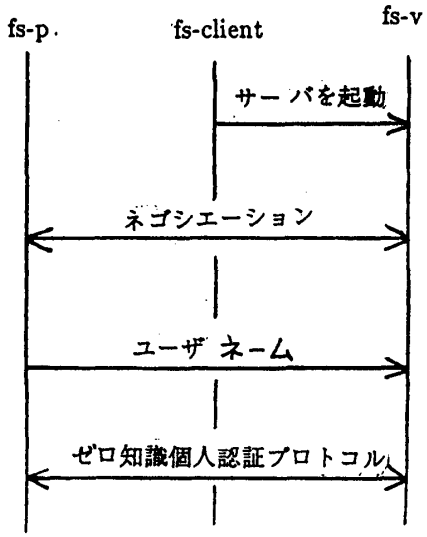

図 3: telnetへの適用

step4: 検証者はe=0のとき,
$Y^2 - X^2 * I - X * I^2 \geq 0\ (mod\ n)$
e=1のとき,
$Y^2 - X^2 * I - X * I^2 < 0\ (mod\ n)$
確認し,
$(Y^2 - X^2 * I - X * I^2)^2 \equiv 4 * (X * I)^3\ (mod\ n)$を確認する。

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する。

4 telnetへの適用

本プロトコルをtelnetで実行するために,telnetクライアントに本プロトコルを実行するサーバを起動する機能と本プロトコルの証明者として動作する機能telnetサーバに本プロトコルの検証者として動作する機能を追加する。それぞれの機能を実行するクライアントをfs-clientとfs-p,サーバをfs-vとする。図3にプロトコルの動作概要を示す。同一のクライアントがfs-clientとfs-p実行してもよいし,異なるクライアントが実行してもよい。これはホストを多重に接続している場合に本プロトコルを実行する区間を選択できようにするためである。証明者と検証者のネゴシエーションにはDATAとしてのエスケープシーケンスを使用している。これはfs-pとfs-vのあいだに本プロトコルをサポートしていないtelnetが存在してもよいようにするためである。

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個人認証をおこなえる。今後は他の通信プロトコルにも本プロトコルをしよう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,携帯用端末に本プロトコルを適用する方法も検討をおこなう予定である。

参考文献
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)