PGP利用における公開鍵の配送について*

1J－1

○森　隆之　　松山　実　　横井　利彰
武蔵工業大学

1　はじめに

現在ネットワーク社会が到来しつつあり，電子通貨等が実用化されるに従って，オンライン上のデータの保護が必要になってきた．インターネットでは見ず知らずの人が管理者を務める中継ネットワークをデータが通過するので，いつどこで改竄されるか分からない．電子メールなどの個人のプライバシーの保護も大切であるが，現在は組織的にデータを保護するのが難しく，従って個人でプライバシーを守る必要がある．個人でプライバシーを守る一方法としてPGP (Pretty Good Privacy: プライバシー機能実現メール)が注目されている．

本報告では，PGPで用いる公開鍵の配送をメールのやり取りのみで行う場合，ゼロ知識対話証明で用いた乱数を最後に配送した方が，直接鍵を配送するよりも安全性を確保しやすいことを述べる．

2　PGP

PGPとは共通鍵と公開鍵を併用した暗号システムで，ファイル及び電子メールの暗号化，ファイルなどへの電子署名が個人レベルで可能である．[1]

PGPでは公開鍵の配送をメールで行うか，直接手渡すのが基本である．しかし，メールで配送する場合，途中で改竄される可能性があるので，鍵の指紋(fingerprint)を電話等でいちいち確認しなければならないのが面倒である．

*Public key distribution on PGP
Takayuki Mori,Minoru Matsuyama,Toshiaki Yokoi
Musashi Institute of Technology

3　ゼロ知識対話証明

ゼロ知識対話証明は，自分の持っている秘密情報を漏らさずに，その秘密情報を持っていることを相手に納得させる方法である．

ここでは，上記の鍵の指紋の信憑性を，ゼロ知識対話証明を用いて検証する．

4　適用

ここでは，ゼロ知識対話証明の一実現方法としてFiat-Shamir法を用いる．[2]

公開鍵を公開する人を証明者とし，受け取る人を検証者と呼ぶことにする．証明者は2つの素数$p, q (p > q)$を生成して，$N(= p \times q)$を公開する．秘密情報s（これに，鍵の指紋を割り当てる）に対して$I = s^2 \bmod N$を満たすIを計算し公開する．証明者は，この$I = s^2 \bmod N$を満たすs（鍵の指紋）を持っていること，すなわち検証者の持っているものと同一であることをゼロ知識対話証明で検証者に証明する．

ステップは以下のようになる．

Step 1 証明者は乱数rを選び，$X = r^2 \bmod N$なるXを計算して，検証者に送信する．

Step 2 検証者は2進数$e \in \{0, 1\}$をランダムに生成して，証明者に送信する．

Step 3 証明者はeを受信し，$Y = r \cdot s^e \bmod N$を計算して，検証者に送信する．

Step 4 検証者は$Y^2 \equiv X \cdot I^e \pmod N$が成り立つことを検証する．これで検証者は，証明者が確かに鍵を保持していることが検証できる．

Step 5 証明者は乱数rを検証者に送信し，検証者側で追試する．これで検証者は，証明者と同一の鍵を持っていることが検証できる．

公開鍵が改竄されていても発見できない確率（なりすませる確率）は1回の検査で2^{-1}なので，以上の手順をl回繰り返すとその確率は2^{-l}になる．また，1回しか繰り返さなくても，秘密情報をk個にすれば，同様になりすませる確率は2^{-k}になる．また，以上の方法では1回の検査のために4回の情報交換が必要なので，計64回の対話が必要になる．(乱数は検証後まとめて送る．) しかし，16回分の検査を同時実行してまとめて送信すれば，計4回の対話で証明が完了する [3].

5 鍵の配送

1回の検査の処理の流れは以下のようになる．(この場合は，改竄者と送受信者が同等の (計算) 能力を持っている．)

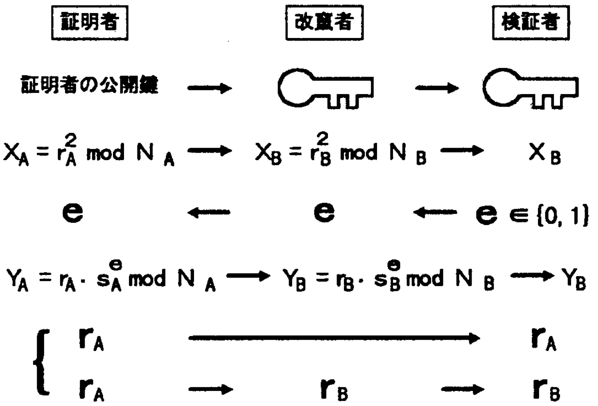

図 1: 情報の流れ

ここでは最後に送信する乱数rについて考える．公開鍵の配布であるから，その情報が盗聴されてもかまわない．しかし，Step 5 の鍵の検証に用いる乱数rまでもが改竄されると，それに気付かない場合がある．従って，Step 1〜4 で情報が改変された場合でも，乱数rは改竄されないものとしなければならない．

但し，ここでは乱数が改竄されても，それに気付けばなりすましを発見できるので，検証者が受け取った情報が改竄されていて，かつそれに気付かない場合を望ましくない状況と考える．[4]

送受信者と改竄者の行える (計算) 能力が同じだとすると，改竄者は完全になりすますことができるので，改竄者より送受信者の方が (計算) 能力が大きくなくては安全な送信はできない．そこで，1回の処理 (Step 1〜5) で改竄者がなりすませる確率をn^{-1}とする．m回目以降 ($m \geq 2$) は，$m-1$回目の処理で用いた乱数rをゼロ知識対話証明の秘密情報として繰り返し処理を行う．

以上をc回繰り返すと，最終的に検証者が受け取る情報が正しい確率 (なりすましを発見できる確率) は，$1 - \frac{1}{n^c}$ となる．検査に用いる乱数rが毎回の処理ごとに同じだとStep5までに改竄者に解読されてしまう．秘密情報sが処理ごとに違えば，乱数は漏れても良いと考えられるが，この検査において，秘密情報sは秘密ではなくなるので，やはり乱数についても毎回違う値を使用しなくては，最後まで乱数を改竄者に秘密にできるというメリットがなくなってしまう．(秘密情報はあらかじめ公開し，乱数はStep5まで秘密であるため．) 検査に用いる情報を並列に処理出来ないので，トラフィックは増大することになる．

6 おわりに

PGPという一般的になりつつある暗号化システムの公開鍵の配送について，ゼロ知識対話証明を適用した．鍵を直接配送するより，ゼロ知識対話証明で用いた乱数を最後に配送した方が，安全性を確保しやすいということを，改竄者と送受信者の計算能力の違いを基に示した．今後は，実際の処理の流れに適用できる関数を考え，安全性が確保できることを示す．その上で，繰り返し処理においても，トラフィックを増大させずに検査できるか考えたい．

参考文献

[1] Bruce Schneier,(力武健次, 道下宣博 訳):「E-mail セキュリティ」, オーム社 (1995)

[2] 岡本龍明, 太田和夫 (共編):「暗号・ゼロ知識証明・数論」, 共立出版 (1995)

[3] 小林信博, 岡本隆司, 桜井幸一:「零知識証明のコンピュータ間認証への適用」, 情報処理学会第44回全国大会,4,pp.265-266(1992)

[4] 坂本直志:「情報を意図的に改変する可能性のある通信路における安全な通信について」, 信学論 (D-I),J79-D-I,pp.621-630(1993)