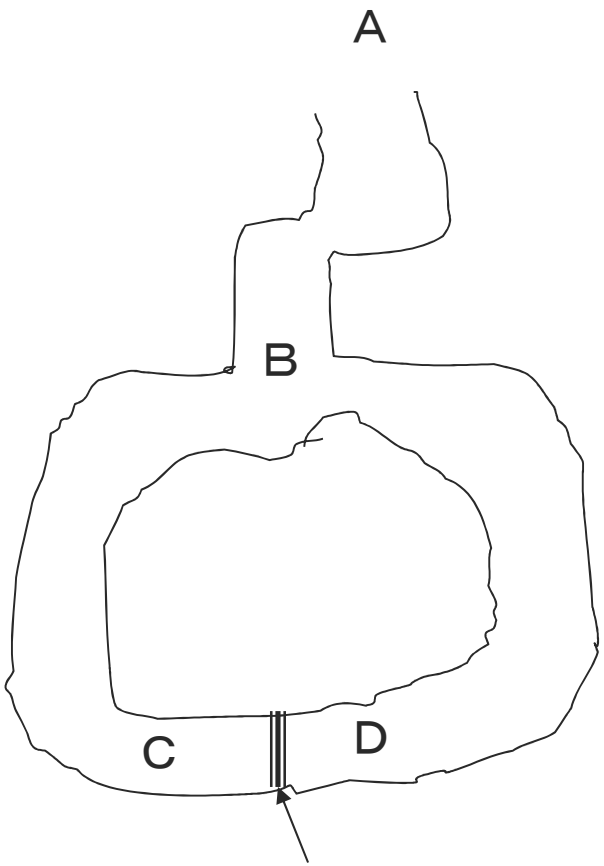
零知識証明(ZKIP)

零知識証明とは

- 自分が持っている秘密を相手に知らせずに秘密を持っていることのみを証明する
- 零知識対話型証明が満たす条件
  - 完全性：検証者は証明者の主張が真であるとき、圧倒的に高い確率で真であると判定できる。
  - 健全性：検証者は証明者の主張が偽であるとき、圧倒的に高い確率で偽であると判定できる。
  - 零知識性：検証者は証明者から何の知識も得られない。

零知識対話型証明の考え方



秘密のドア（呪文を知っていると開く）

1. Ｖ（検証者）はA地点で待つ（B地点は見えない）
2. Ｐ（証明者）はB地点からC地点かD地点のどちらかに進む。
3. VはPがCかDに到着した後にBに進む。
4. VはPに、次のいずれかの指示を出す
   (1)左（Cの側）から出てきてください
   (2)右（Dの側）から出てきてください
5. PはVの指示に従う（必要に応じ呪文を使う）
6. VはPが指示した方から出られなければ、Pは呪文を知らないと判定する。

１～6をk回繰り返すとき、呪文を知らないPがVをだまし通せる確率は、１／2^k

Fiat-Shamir法

- p, qを大きな素数、n=pqとする
- 証明者は秘密sを持っており、$v = s^2 \pmod n$であること（vが平方剰余）であることをsに関する情報を漏らさずに証明したい
- （注）p、qを知っている者はvからsを求められるが、知らない者は（多項式時間では）求められない

Fiat-Shamir法の手順

1. P（証明者）は乱数rを生成し、
   $x=r^2 \pmod n$をV（検証者）に送る。
2. Vは、$e=0$ or 1をランダムに選び、Pに送る。
3. Pは、$y=s^e r \pmod n$を求め、Vに送る。
4. Vは、$y^2=v^e x \pmod n$をチェックする。
   等しくなければ、Pは秘密sを持っていないと判断して終了。
   等しければ、1に戻る。

1～4をk回繰り返し、Step4で終了することがなければ、Pは秘密sを持っていると判定する。

Fiat-Shamir法の手順（不正１）

1. Vはstep2でe=0を送ってくると予想した場合
   Ｐ（証明者）は乱数*r*を生成し、
   $x=r^2 \pmod n$をＶ（検証者）に送る。
2. Ｖは、*e=0* or *1*をランダムに選び、Ｐに送る。
3. Ｐは、$y=s^e r \pmod n$を求め、Ｖに送る。
   e=0ならy=rを送ればよい。e=1の場合は対応できない
4. Ｖは、$y^2=v^e x \pmod n$をチェックする。
   等しくなければ、Ｐは秘密*s*を持っていないと判断して
   終了。等しければ、１に戻る。

１～４を*k*回繰り返し、Step4で終了することがなければ、
Ｐは秘密*s*を持っていると判定する。

Fiat-Shamir法の手順（不正２）

1. Vはstep2でe=1を送ってくると予想した場合
   Ｐ（証明者）は乱数*y*を生成し、
   $x=y^2/v \pmod n$をＶ（検証者）に送る。
2. Ｖは、*e=0* or *1*をランダムに選び、Ｐに送る。
3. Ｐは、~~$y=s^e r \pmod n$を求め、Ｖに送る~~。
   e=1ならyを送ればよい。e=0の場合は対応できない
4. Ｖは、$y^2=v^e x \pmod n$をチェックする。
   等しくなければ、Ｐは秘密*s*を持っていないと判断して
   終了。等しければ、１に戻る。

１～４をｋ回繰り返し、Step4で終了することがなければ、
Ｐは秘密*s*を持っていると判定する。

Fiat-Shamir法の説明

- Pがsを知らないとき:
- (Case1)Vが$e=0$を送ってくると予想

  プロトコル通り$x=r^2$を返せば、$y^2=r^2$, $x=r^2$なので
  パスできる。
- （Case2）Vが$e=1$を送ってくると予想

  yを適当に決め、$x=y^2/v$により求めれば、
  $y^2=vx$を満たせる。

結局、各回毎に1／2の確率でしかVを騙せない