ゼロ知識証明入門

土井洋(情報セキュリティ大学院大学)

今回の入門講義では，ゼロ知識証明とはどんな技術か，そのからくりはどうなっているか，またなぜ知識を示さないのに証明といえるのか，解説を行う．

効率のよいゼロ知識証明では，数学の一分野である整数論が利用される場合が多い．本講義では例として整数のべき乗演算と密接に関係がある離散対数問題を取り上げ，ゼロ知識証明の解説を行う．最終的にはゼロ知識証明を利用した電子署名の構成例を示す．

離散対数問題

- 離散対数とは
  $G=(Z/pZ)^*$, g：位数がq(素数)の元
  $y=g^x \bmod p$ に対してxをyのgに対する離散対数とよぶ
- 離散対数問題
  (p,q,g,y)が与えられた時，xを求める問題
- 離散対数問題は，|p|，|q|が十分大きい場合は，困難な問題であると考えられている．
  - |p|=1024以上，|q|=160以上
- 離散対数は指数と呼ばれる場合もある．

今回の講義では，離散対数問題をターゲットとする

離散対数問題と暗号

- 公開鍵暗号系を構築するための2大数論問題
  - 素因数分解問題
    - RSA暗号で利用される(1978)
      - 公開鍵暗号方式の現在の標準
  - 離散対数問題
    - DH鍵配送方式で利用される(1976)
    - ElGamal暗号で利用される(1985)

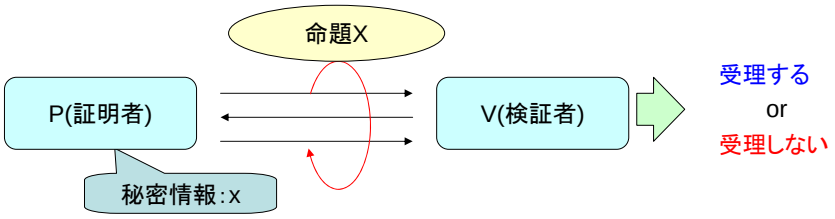
ゼロ知識対話証明

- 1985年に概念が提案された
  - Goldwasser, Micali, Rackoff, ”The knowledge complexity of interactive proof-systems”
- 特徴
  - 対話証明
  - ゼロ知識
  - 確率的

今回の講義で扱う命題Xは，「公開された情報yに対する秘密情報xを知っていること」に限定する．

対話証明とは(直感的)

- (通常の)証明の拡張
  - 証明者Pと検証者Vが存在する.
  - PとVでデータのやり取り(対話)をする.
  - 対話のあと，Vは，Pの主張(命題Xが真であること)が正しいと(非常に高い確率で)確信する(=受理する).



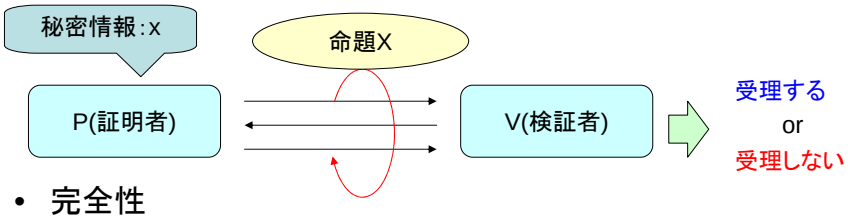
ゼロ知識とは(直感的)

- 証明したいこと(Pの主張(命題Xが真であること)が正しいこと)以外の情報がVに漏れない

[命題X]
(p,q,g,y)が与えられた時，$y \equiv g^x \pmod p$ となるxを知っている.

[ゼロ知識対話証明後]
検証者Vは，(証明者Pが) $y \equiv g^x \pmod p$ となるxを知っているに違いないと確信する．しかしながら，検証者Vはxに関する情報を得ることができない.

ゼロ知識対話証明



- 完全性
  - 命題Xが真の場合，(P,Vがプロトコルに従えば)Vは高確率で受理する.
- 健全性
  - 命題Xが偽の場合，(P*がどのように振舞っても)Vが受理する確率は無視できるほど小さい.
- ゼロ知識性
  - PとVの対話証明で得られるデータは，(Pなしでも)模倣できる.

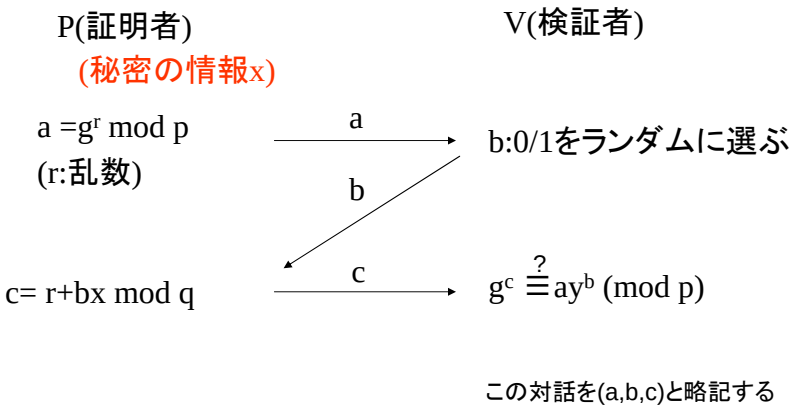
模倣=simulation

模倣とは?

- 本物の対話により得られる対話データと識別できない対話データを(秘密情報xを用いずに)作成すること.
- 模倣のレベル
  - 確率分布の差異が重要
    - PとVのデータのやり取り･･･確率変数
    - 模倣･･･確率変数
  - 模倣が完全であるとは･･･
    - 上記2つの確率変数の分布が同一

例1

(p,q,g,y)が与えられた時$y \equiv g^x \pmod p$となるxを知っている



この対話を(a,b,c)と略記する

攻撃1(例1への攻撃)

- xを知らない証明者P^*がVに受理させる方法
  1. bをランダムに選ぶ
  2. cもランダムに選ぶ
  3. $a=g^c y^{-b} \bmod p$を計算する.

---

4. aをVに送り，Vの返事を待つ.

5-1 もし，Vがbを返してきたら，cをVに送る. (攻撃成功)

5-2 もし，Vがbを返してこなかったら，中止. (攻撃失敗)

考察(攻撃1の成功確率)

- 攻撃1の成功確率=1/2
  - P*がランダムに選んだbを，たまたまVが選べばVは受理してしまう. ｝攻撃成功確率=1/2
  - P*が選ばなかったb’対して，P*がc’を送ることができるか?⇒できない ｝攻撃失敗確率=1/2

攻撃方法に依存しない議論

Pが$(a,0,c_0),(a,1,c_1)$を生成できるとせよ.
検証式$g^{c_0} \equiv a \bmod p, g^{c_1} \equiv ay \bmod p$が成立するので
$g^{c_1-c_0} \equiv y \bmod p$が成り立つ．つまり，離散対数
$x = c_1 - c_0 \bmod q$をPが計算できたことになる.
これはPがxを知らないということに反する.

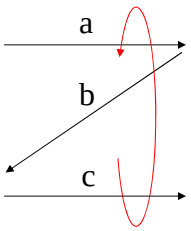
例2(例1の繰り返し)

(p,q,g,y)が与えられた時$y \equiv g^x \pmod p$となるxを知っている

P(証明者)　　V(検証者)

(秘密の情報x)

$a = g^r \bmod p$
(r:乱数)



b:0/1をランダムに選ぶ

$c = r + bx \bmod q$

$g^c \stackrel{?}{\equiv} ay^b \pmod p$

20回繰り返せばどうなるか?

考察(例2への攻撃1の成功確率)

- 攻撃1の成功確率=1/2
- 20回繰り返すとどうなるか?
  - 成功確率は$1/2^{20}=0.000001$
- Vの視点
  - Pがxを知らないのなら，20回繰り返せば，1回くらいは失敗するはず(確率0.999999で1回は失敗するはず).

例2の評価(繰り返し回数=20回)

- 完全性
  - Pが$y \equiv g^x \pmod p$となるxを知っていたら，Vは必ず受理する.
- 健全性
  - P^*が$y \equiv g^x \pmod p$となるxを知らない場合，20回連続してVが受理する確率は$1/2^{20} \fallingdotseq 0.000001$，逆にVが受理しない確率は$1-1/2^{20} \fallingdotseq 0.999999$
- ゼロ知識性
  - 対話を模倣可能(攻撃1を繰り返せばよい)

攻撃1が成功したら終了．外れたら，その回だけやり直し．
20回分の対話の模倣には40回程度試行する必要がある．

本来の対話回数の2倍程度

対話回数削減

- HVZKIP
  - Honest Verifier Zero Knowledge Interactive Proof の略
  - 検証者は正しく乱数を生成するというモデル.
- このモデルだと，対話回数を減らすことができる.
  - ただし，健全性，ゼロ知識性の定義を若干変更する必要がある.
- 電子署名などへの拡張も可能
  - これには，「非対話化」を行う必要がある.
    - 理想的なランダム関数を利用する.
    - 現実世界では，ハッシュ関数を「理想的なランダム関数」の代替として利用している.

例3

(p,q,g,y)に対して$y=g^x \bmod p$ となるxを知っている

P(証明者) (秘密の情報x)		V(検証者)
$a = g^r \bmod p$ (r:乱数)	a →	
		0≦b<qをランダムに選ぶ
	← b	
$c= r+bx \bmod q$	c →	$g^c \stackrel{?}{\equiv} ay^b \pmod p$

Pが離散対数xを知らない場合，受理される確率は1/q

qを2^{160}程度にすれば健全性はOK

健全性について

- 秘密xを知らないP*は，2通り以上のb,b’に対して，Vが受理するc及びc’を構成できるか?
  ⇒できない

攻撃方法に依存しない議論

$b_0 \neq b_1$である$(a, b_0, c_0), (a, b_1, c_1)$を生成できるとせよ．
検証式$g^{c_0} \equiv a y^{b_0} \bmod p, g^{c_1} \equiv a y^{b_1} \bmod p$が成立するので
$g^{c_1 - c_0} \equiv y^{b_1 - b_0} \bmod p$が成り立つ．つまり，離散対数
$x = c_1 - c_0 / b_1 - b_0 \bmod q$を計算できたことになる．
これはPがxを知らないということに反する．

模倣の方法

- 模倣の手順
  - まず，bをランダムに選ぶ
    - 検証者がbをランダムに選ぶモデルであることに注意
  - 次にcをランダムに選ぶ
  - 最後に，$a=g^c y^{-b} \bmod p$とする．
- 模倣により得られた分布は本物の分布と等しいか?
  - 完全に一致する

ゼロ知識性について

- ゼロ知識性
  - b,c,aの順に生成した対話は，本物の対話と分布が同じ.
  - 本物
    - rはZ_qからランダムに選ばれる元であり，確率は1/q
      - $a=g^r \bmod p$はrから一意に定まる.
    - bはZ_qからランダムに選ばれる元であり，確率は1/q
    - a,bが定まれば，cは一意に定まる.
  - 模倣
    - b,cはZ_qからランダムに選ばれる元であり，確率は各々1/q
    - b,cが定まれば，aは一意に定まる.
  - 本物，模倣の対話データの集合が一致することも確認できる
    - 本物の対話データを(a,b,c)とする.
      - $a=g^r \bmod p$となるr(Z_qの元)が存在することに注意.
    - 模倣で(r,b)がランダムに選ばれた場合，対話データは(a,b,c)となる

例3の評価

- 完全性
  - Pが離散対数xを知っていたら，Vは必ず受理する.
- 健全性
  - Pが離散対数xを知らない場合，Vが受理する確率は1/q.
    - |q|=160の場合，受理する確率は$1/2^{160}$.
- ゼロ知識性
  - Honest Verifier に対するゼロ知識性は有する.

例4a(非対話化)

(p,q,g,y)に対してy=g^x mod pとなるxを知っている

P(証明者)
(秘密の情報x)

V(検証者)

bを証明者であるPが計算するため，
対話不要(送りつけるだけ)

a = g^r (r:乱数)	a →	
b=h(p,q,g,y,a)	b →	①b=h(p,q,g,y,a)を計算
c= r+bx mod q	c →	②$g^c \equiv a y^b \pmod p$が成り立つか検証する

h：理想的なランダム関数(現実世界ではhash関数が用いられる)

Vが生成すべき乱数を，Pが(理想的な)ランダム関数を用いて生成していることに注意

例4b(非対話化・改良版)

(p,q,g,y)に対してy=g^x mod pとなるxを知っている

P(証明者)
(秘密の情報x)

V(検証者)

bを証明者であるPが計算するため，
対話不要(送りつけるだけ)

a = g^r (r:乱数)　aは送る必要なし

b=h(p,q,g,y,a)	b →	①a=g^c/y^b mod pを計算
c= r+bx mod q	c →	②b=h(p,q,g,h,a)が成り立つか検証する

aはb,cから計算できるので，送っていない　} データ長を小さくできる

Vが生成すべき乱数を，Pが(理想的な)ランダム関数を用いて生成していることに注意

例5(知識の署名)

公開鍵簿　Pの公開鍵:y　PはY=g^x mod pとなるxを知っている

P(証明者)　V(検証者)

(秘密の情報x)

a = g^r (r:乱数)

b=h(M,p,q,g,y,a)

c= r+bx mod q

(b,c),M →

①a=g^c/y^b mod p

②c=h(M,p,q,g,h,a)が成り立つか検証する

乱数生成時，Pがメッセージ Mを(理想的な)ランダム関数へ入力している．

Mの値が変わったら，乱数bも変わることに注意．

Schnorr署名と呼ばれる方法とほぼ同じ

まとめ

- ゼロ知識証明についての紹介
  - ゼロ知識証明の概要
  - 基本形(多くの対話が必要な方式)
  - HVZKIP(検証者がHonestなモデルでの方式)
  - 非対話化(ランダム関数の利用)
  - 知識の署名