ゼロ知識証明とは

2013/12/11

(数物･電子情報系学科･情報工学EP3年)

・調査背景（なぜこのキーワードを選んだか）

「ゼロ知識証明」という言葉の意味が知りたかった。
また、それがどのように暗号理論に応用されるのかを調べるため。

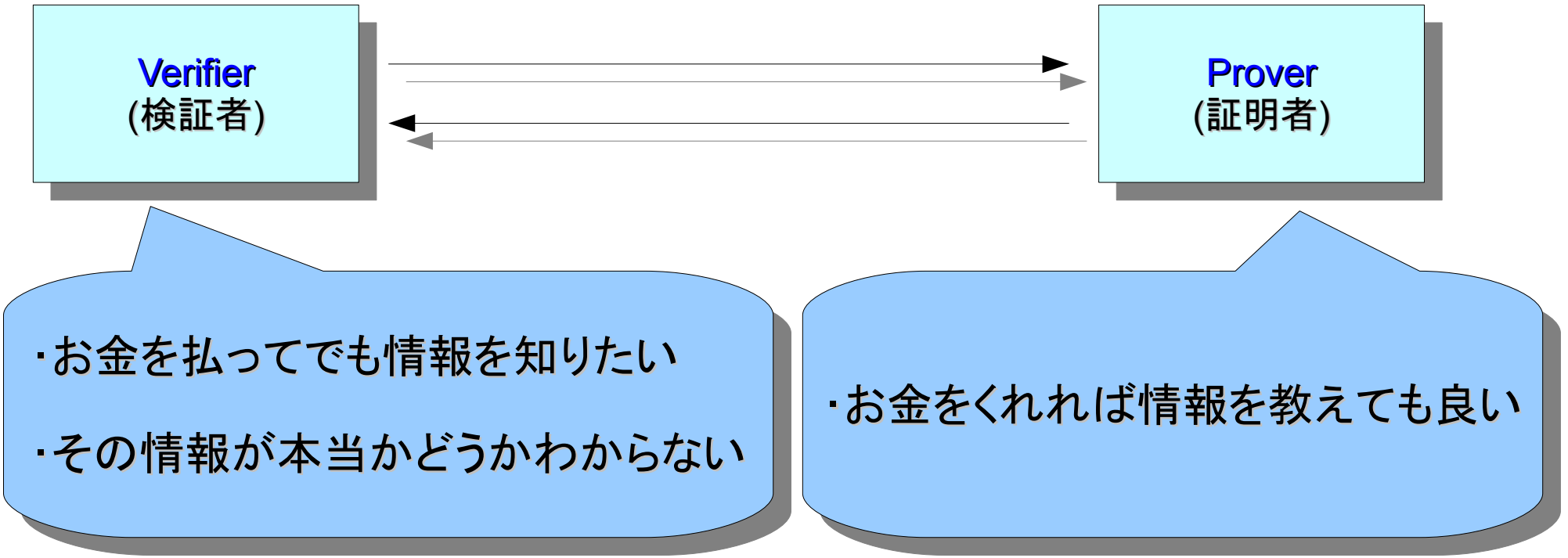
⇒”0”の知識を”証明”するとは？
⇒”ゼロ知識”とは？

・発表の流れ

1.ゼロ知識証明とは
2.具体例
3.応用例

ゼロ知識証明

ZKIP（Zero Knowledge Interactive Proof）



Prover(証明者)はVerifier(検証者)に

「正しい情報を知っていること」**のみ**を教えたい

⇒情報の中身は教えたくない

ゼロ知識証明

ZKIP（Zero Knowledge Interactive Proof）

ゼロ知識証明が満たすべき3つの条件

完全性:

真であることを確認する側（検証者）は、証明する側（証明者）の持っている命題が真であるならば、真であることが必ずわかること。

健全性:

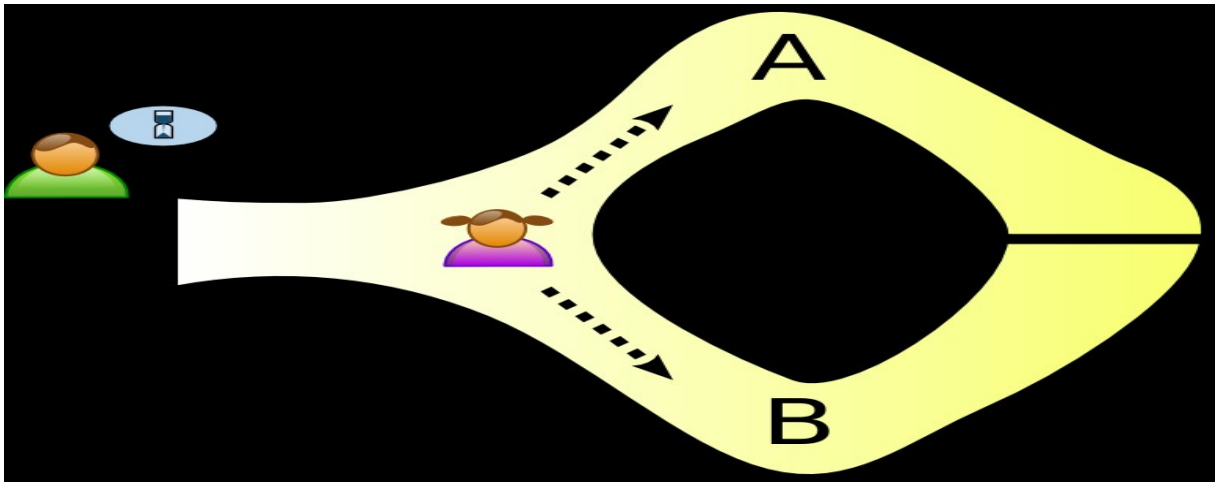
証明者の持つ命題が偽であるなら、検証者は高い確率でそれが偽であると見抜けること。

ゼロ知識性(これが一番重要):

証明者の持つ命題が真であるなら、検証者が不正して証明者から知識を盗もうとしても「命題が真である」以外の何の知識も得られないこと。

(例)パスワードを盗もうとしても、「正しいパスワードを入力すれば、ログインができる」以外の情報が得られない⇒パスワード自体についてはわからない

具体例
(洞窟の問題)

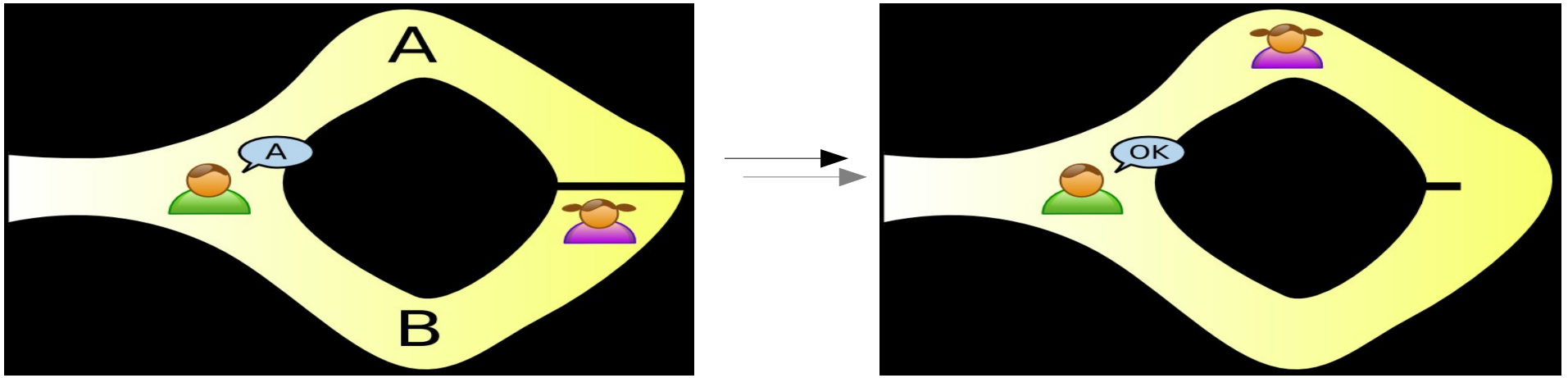


- 洞窟の一番奥に、ある合言葉で開く魔法の扉があり、洞窟は途中で分かれて奥でつながっていて、魔法の扉で仕切られている。
- Pさんは洞窟の奥にある魔法の扉を開く合言葉を手に入れた。
- Vさんは合言葉をお金を払ってでも知りたいが、Pさんが本当の合言葉を知っているかどうかを確認したい。
- Pさんは合言葉を教えても良いが、Vさんがお金を払うまで教えたくない。

⇒合言葉そのものを教えることなく

「Pさんは合言葉を知っている」という事実のみを証明したい。

具体例
(洞窟の問題)



(証明方法)

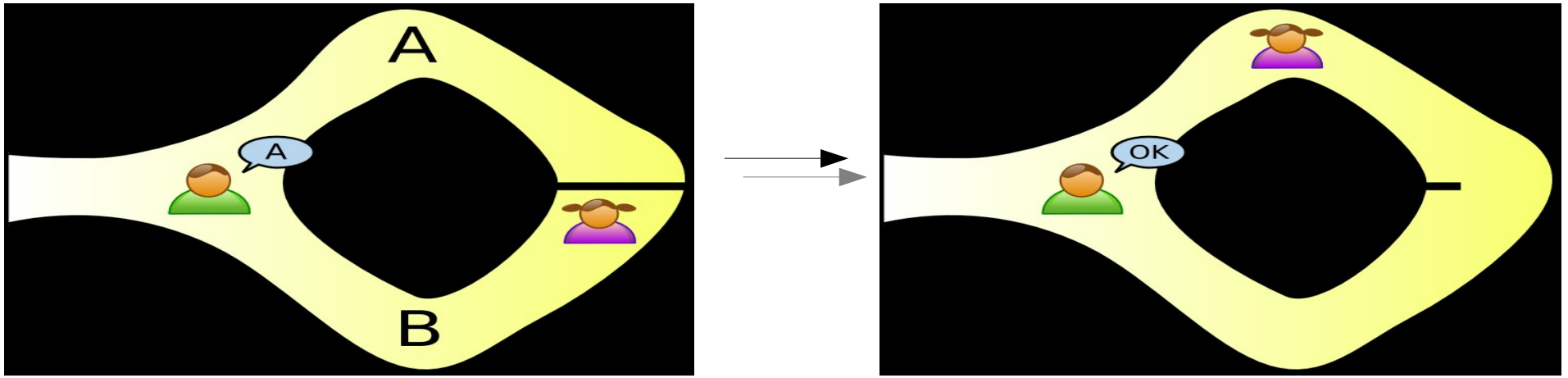
まず、Vさんは洞窟の外で待ち、Pさんだけ入る。

左右の分かれ道をそれぞれA,Bと呼ぶことにすると、PさんはAかBどちらかの分かれ道をランダムに選んで奥に入ることになる。

次にVさんは分かれ道の入り口まで行き、どちらかの道をランダムに選ぶ。そしてPさんに、ランダムに選んだその道から出てきてほしいと大声で伝える。

Pさんが合い言葉を知っているならそれに答えるのは簡単である。もし反対側なら魔法の扉を開けて通るだけでよい。VさんはPさんがどちらから入ったのかは知らないという点に留意。

具体例
(洞窟の問題)



Q:Pさんに「Aから入ってBから出て欲しい」というだけではダメなのか？

⇒確かに**証明はできる**が、Vさんがこっそりpさんの跡をつけて合言葉を盗める可能性がでてくる。**(※ゼロ知識性を満たしていない)**

Q:PさんがAから入って、VさんがAから出てきた場合、証明ができないのでは？

⇒Pさんが合言葉を知らなかった場合、正答率は50%だが**繰り返すことで0%に限りなく近づけることができる。(※健全性の保証)**

これが、**ゼロ知識証明のメカニズム**である。

暗号分野のゼロ知識証明

もう一つ例を挙げる。mを法とした平方根を求めるのが困難だという前提のもと、整数Z,mが与えられたとき、証明者が

$$Z \equiv T^2 \bmod m$$

(Z･･･Tを2乗してmで割った時の余り)

となるTを知っていることを確かめる。

つまり、Tを教えることなく、Tを知っていることを証明できればよい。

※ちなみに、mはできるだけ大きな素数の積⇒素因数分解問題に準拠

暗号分野のゼロ知識証明
Z ≡ T^2 mod m

1.証明者は乱数Rを生成し X≡R^2 (mod m)を検証者に送る。

2.検証者は b=0or1をランダムに選び証明者に送る。

3.証明者は Y≡(T^b)･R (mod m)を検証者に送る。

4.検証者は (Z^b)･X≡y^2 (mod m)を確かめる。

＊証明者が本当にTを知っていれば、4.は常に成立する。

＊証明者がTを知らなかった場合･･･
もしb=1となることが事前にわかっていた場合、Xの値を適切な数値にすることで4.を常に成立させることができ、b=0となることが既に分かっていれば、Rをやりとりするだけなので常に成立する。

＊実際にはbの値が事前にわからないため、騙せる確率は50%。
⇒繰り返すことで0%に限りなく近づく。

暗号分野のゼロ知識証明
16 ≡ 18^2 mod 77

証明者:
R=4としX=4^2 mod77=16を送信

検証者:b=1を送信

証明者:Y=(T^b)･R mod77
=18*4 mod77=72を送信

検証者:
(Z^b)･X mod77
=16*9 mod77=25

Y^2 mod77=72^2 mod77=25

洞窟の問題で言うと、Pさんが
A⇒Bと出てくる例。

正しい解を知っていれば成立。

証明者:
R=11としX=11^2mod77=44を送信

検証者:b=0を送信

証明者:Y=(T^b)･R mod77
=11 mod77=11を送信

検証者:
(Z^b)･X mod77
=1*44 mod77=44

Y^2 mod77=11^2 mod77=44

洞窟の問題で言うと、Pさんが
A⇒Aと出てくる例。

乱数のやりとりのみ。常に成立。

これをさらに応用していくと、ゼロ知識対話証明のプロトコルとなる。

(参考文献)

Wikipedia-ゼロ知識証明
http://ja.wikipedia.org/wiki/ゼロ知識証明

Security BOSS-Security事情
http://www.nttpc.co.jp/service/securityboss/news/security/index.html

小山 謙二-ゼロ知識対話証明の原理と課題 (<小特集>ゼロ知識証明とその応用)
http://ci.nii.ac.jp/naid/110002762502

ゼロ知識証明入門
http://lab.iisec.ac.jp/~arita/lecture3.html

ご静聴ありがとうございました。