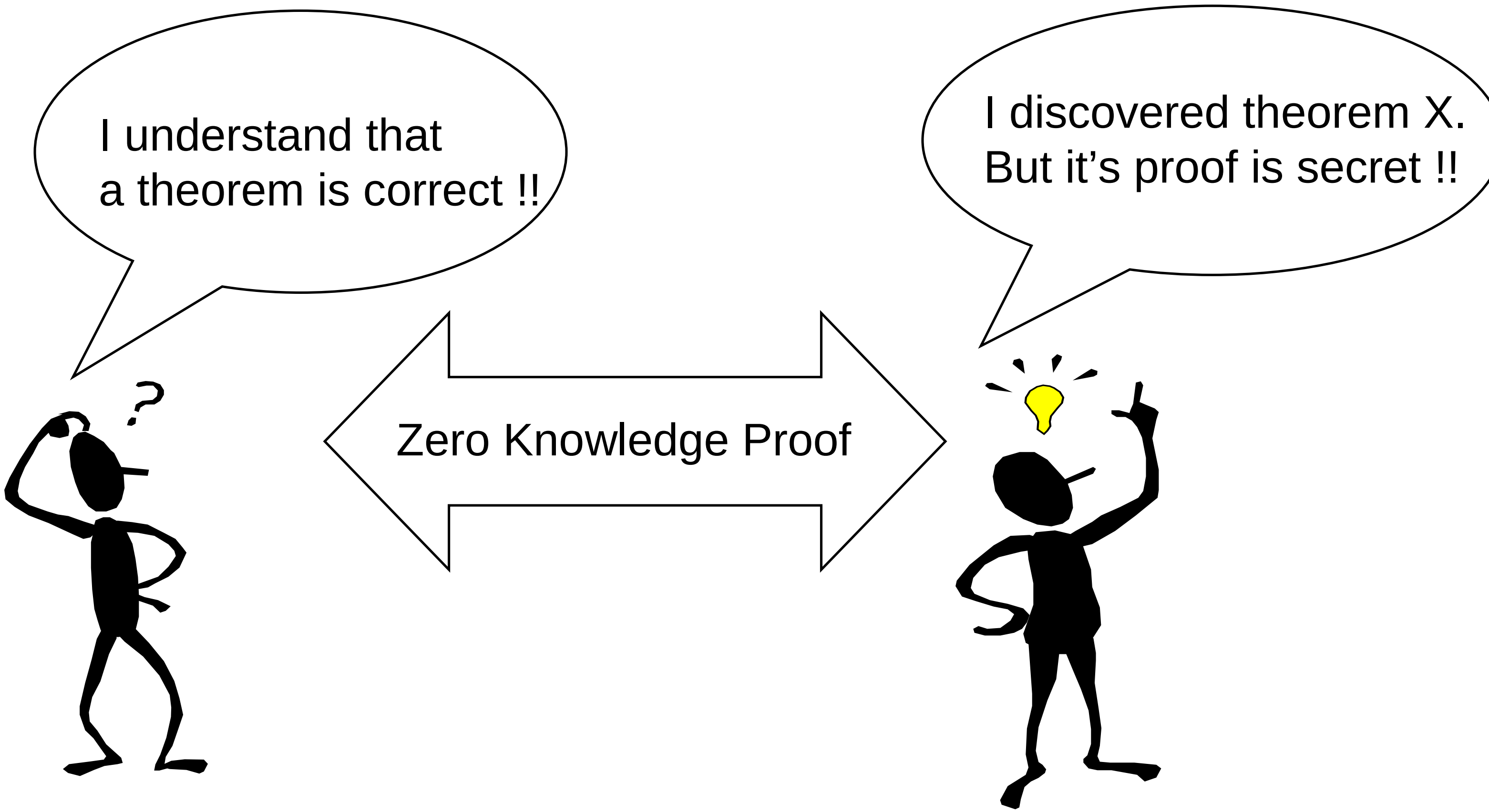
Cryptographic Protocols(I)

- 1976 : Birth of concepts of PKC
- 1978 : Birth of RSA
  - New applications compared to traditional concepts
    - ✓ Digital Signature
    - ✓ Coin Flipping
    - ✓ Mental Poker
    - ✓ Contract Signing
    - ✓ Electronic Voting
    - ✓ Comparison of Richness

Cryptographic Protocols(II)

- 1978 - 1984
  - A variety of PKCs
  - Research on various cryptographic protocols
- 1985
  - ZKIP (Zero Knowledge Interactive Proof)
  - Authentication
  - Multiparty Protocol
  - Proof of NP-complete problem

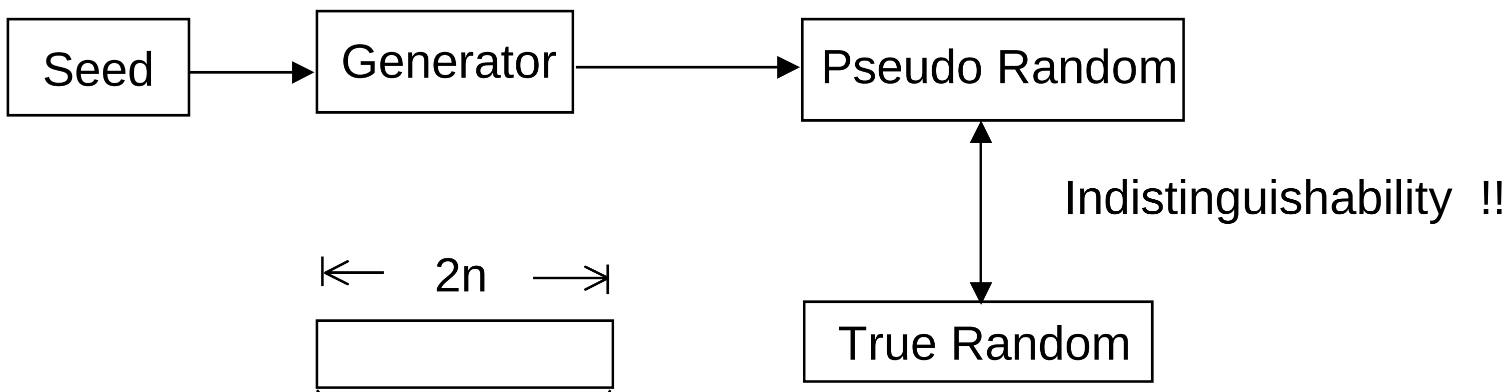
Cryptographic Protocols(III)

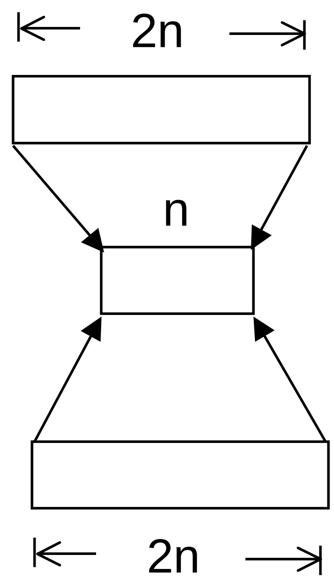


Cryptographic Protocols(IV)

- 1987 NIZK(Non-interactive ZK)
  - RSA
    - ✓ Strong against direct attack
    - ✓ But weak in chosen ciphertext attack
- Application of NIZK
  - Strong PKC against CCA
  - Digital signature against CPA

Application of PKC

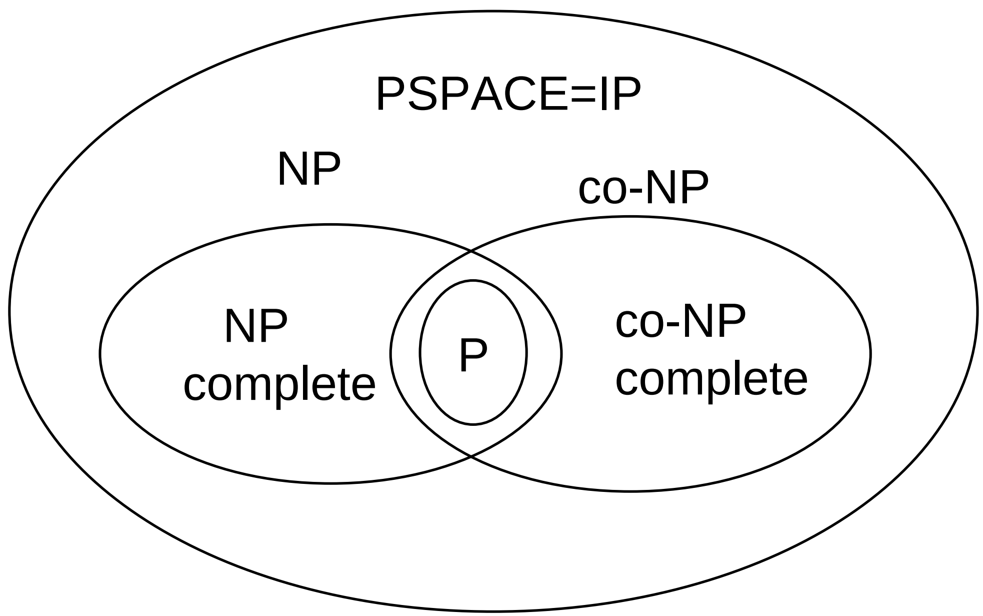




Hash ft that deriving collision pair is impossible.

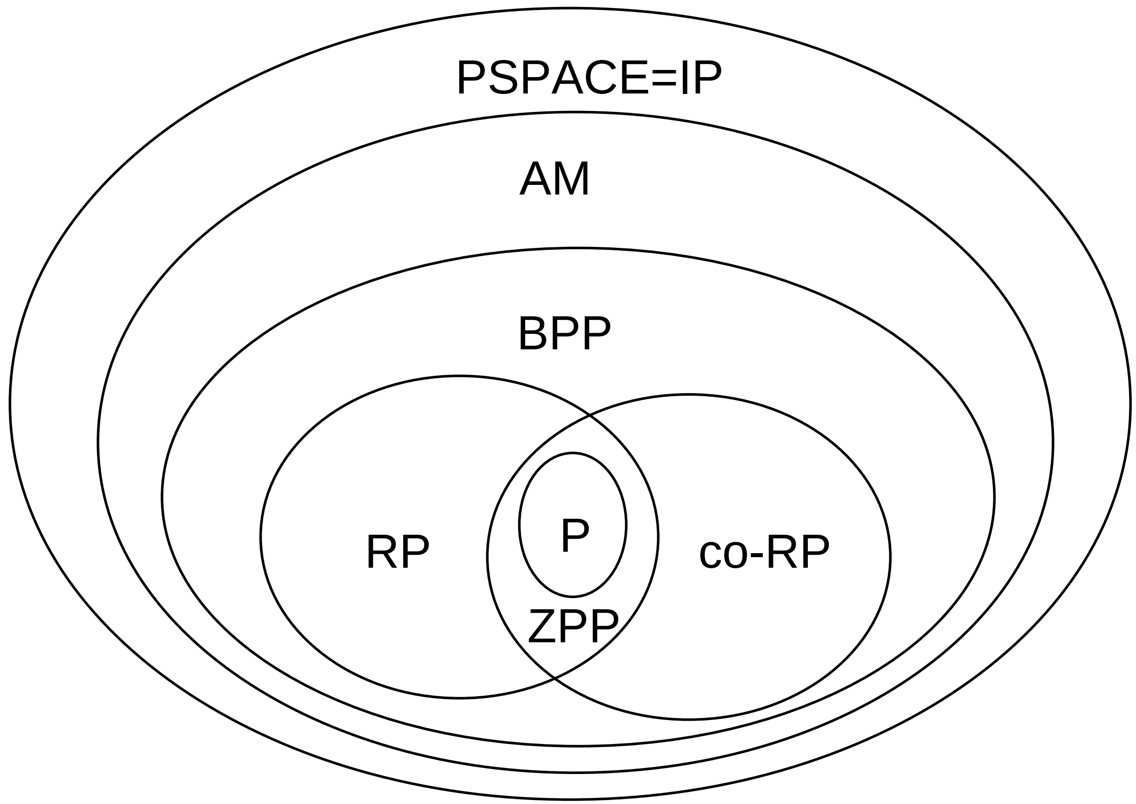
Complexity Class(I)

Language L={0,1}*: infinite set of elements with various input size
Uniform Model : Turing Machine (computer algorithm)
Non-uniform Model : Circuit model (VLSI)
P : Deterministic poly, NP : Non deterministic Poly

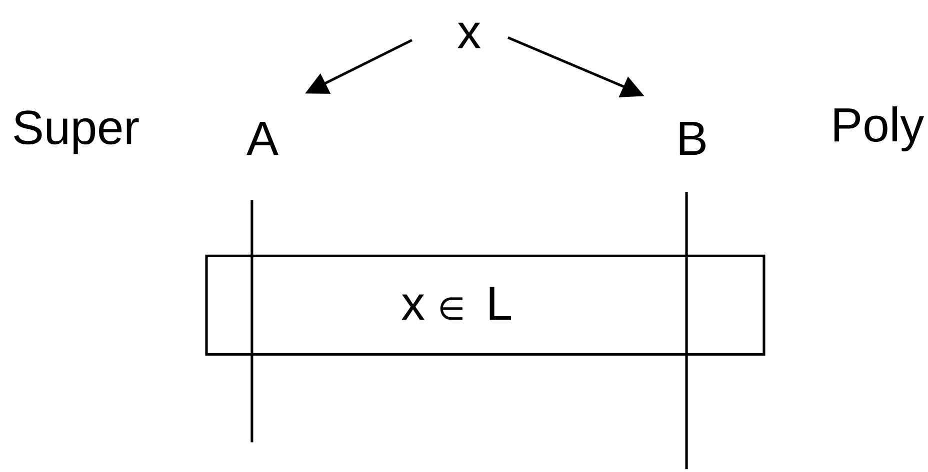


Complexity Class(II)

Allows random coin -> error



Computation & Proof(I)



For B

no help : P, BPP

1-way proof : NP

interactive proof : IP

+

zero knowledge = ZKIP

Computation & Proof(II)

$L \in P$

$$x \longrightarrow \boxed{TM} \longrightarrow \begin{cases} x \in L \\ x \notin L \end{cases}$$

Prob. of error =0

$L \in BPP$

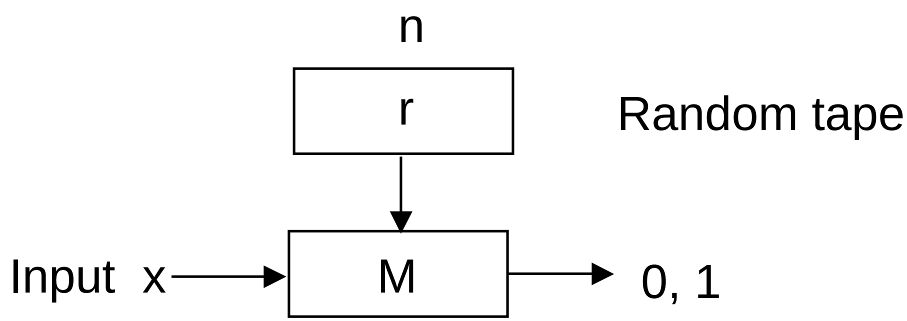
Poly-time

Random tape

$$x \longrightarrow \boxed{TM} \longrightarrow \begin{cases} 1, & x \in L \\ 0, & x \notin L \end{cases}$$

Completeness	$x \in L$	Prob(TM(x)=1) $\geq$ 2/3
Soundness	$x \notin L$	Prob(TM(x)=0) $\geq$ 2/3

BPP(I)



r	r_1	...	r_k	r_{k+1}	...	r_{2^n}
$M(x,r)$	1	…	1	0	…	0

$$\mathrm{Prob}(M(x) = 1) = k/2^n \begin{cases} > 1 - \varepsilon & \text{if } x \in L \\ < \varepsilon & \text{if } x \notin L \end{cases}$$

$$\mathrm{Prob}(M(x)=0) = (2^n - k) / 2^n$$

$M(x)$: random variable

BPP(II)

❑ Example of BPP

L = { p | p = prime }

Probabilistic prime test by Solovay-Strassen

- ✓ gcd (a,p) =1 (1)
- ✓ (a/p) = $a^{(p-1/2)}$ mod p (2)

If $p \in$ L, eqs (1) and (2) are always true.

If $p \notin$ L, eq.(1) or eq.(2) is false with over pr. 1/2

Check on a_1, …, a_k :

If eqs (1) and (2) are true for all a_i,

then p is prime greater than with pr. $(1 - 1/2^k)$

BPP (III)

$\Pr[M(x) = 1] \geq 2/3$ if $x \in L$

$\Pr[M(x) = 0] \geq 2/3$ if $x \notin L$

$$\Updownarrow$$

$\Pr[M(x) = 1] \geq 1/2 + |x|^{-c}$ if $x \in L$

$\Pr[M(x) = 0] \geq 1/2 + |x|^{-c}$ if $x \notin L$

$$\Updownarrow$$

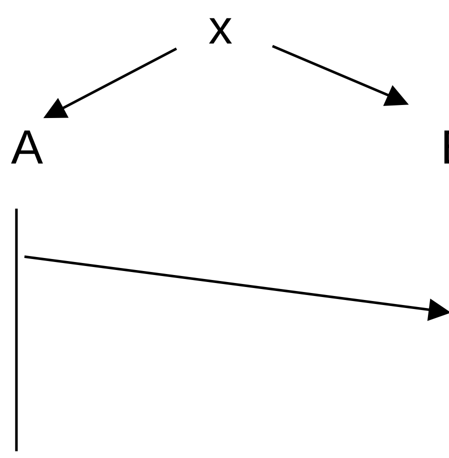
$\Pr[M(x) = 1] \geq 1 - 2^{-|x|}$ if $x \in L$

$\Pr[M(x) = 0] \geq 1 - 2^{-|x|}$ if $x \notin L$

Computation & Proof (III)

$L \in NP$

Superman



Poly-time

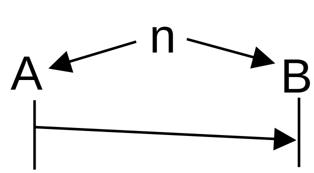
w
(witness)

$f(x,w)$ = accept or reject

Completeness : if $x \in L$, $f(x, \exists w)$ = accept
Soundness : if $x \notin L$, $f(x, \forall w)$ = reject

(예) L = { n | n = composite}, $n = n_1 n_2$

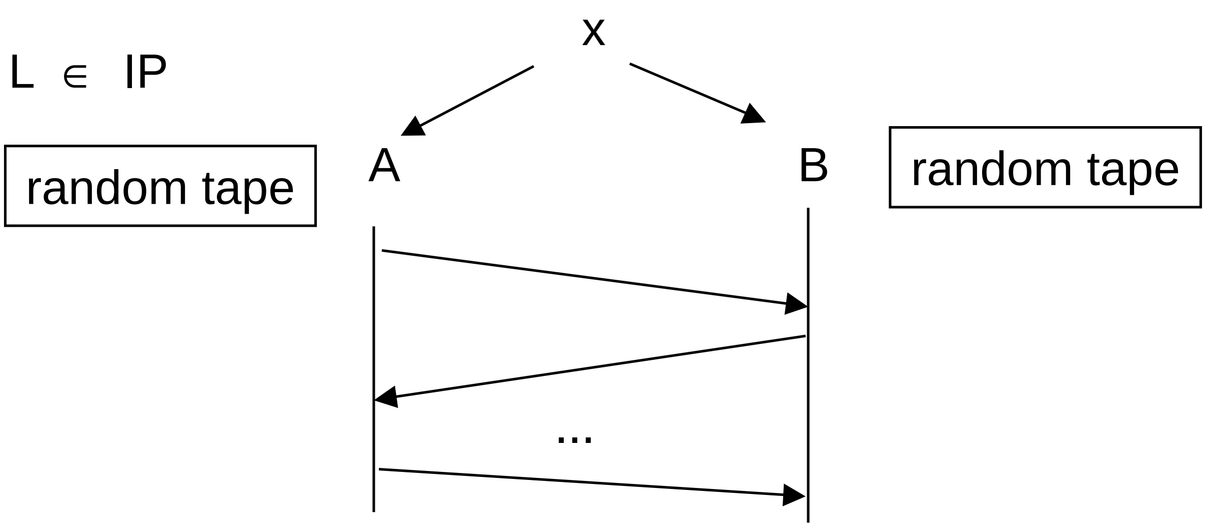
n_1



n_1 is a factor of n ?

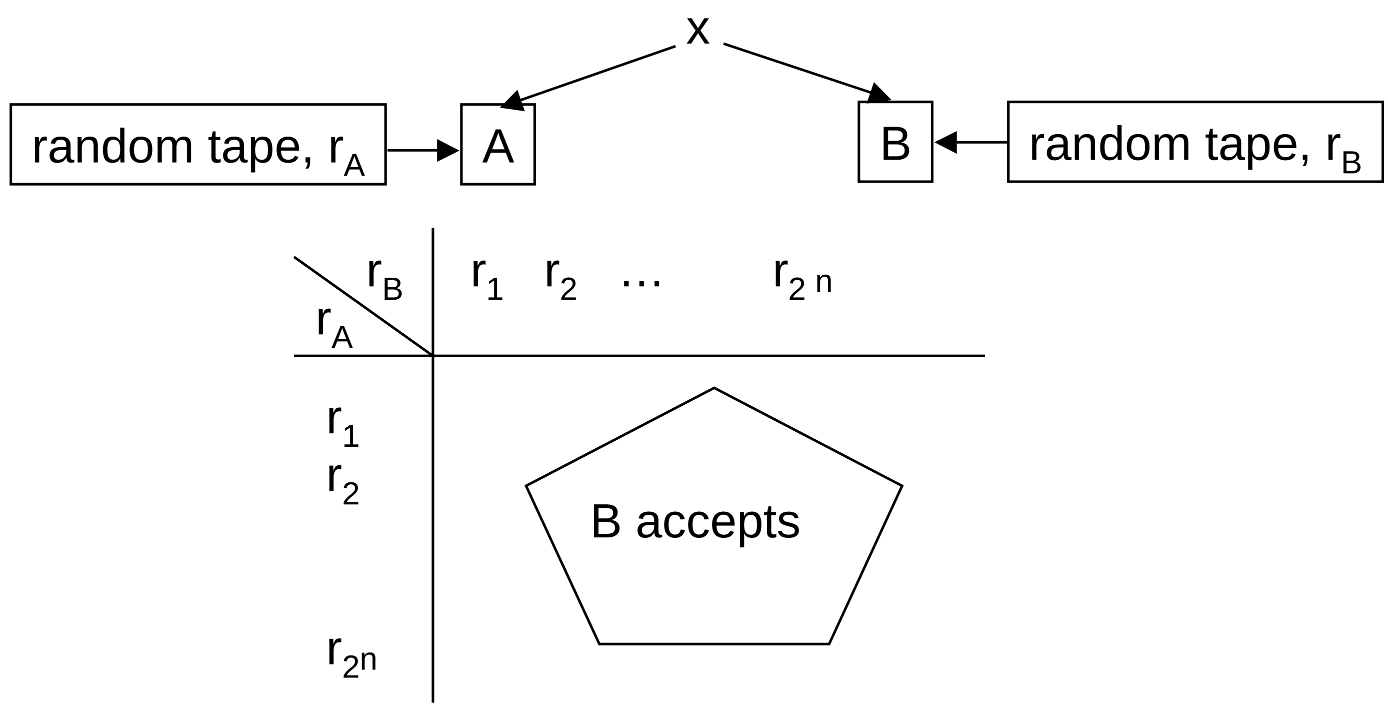
Computation & Proof (IV)

$L \in IP$



Completeness if $x \in L$, prob[B accepts x] $\geq 1 - \varepsilon$
Soundness if $x \notin L$, prob[B rejects x for $\forall$A] $\geq 1 - \varepsilon$

Meaning of Probability (IP)



Prob(B accepts) $\equiv$ Area that B accept / Total area

$$\begin{cases} 1 - \varepsilon & \text{if } x \in L \\ < \varepsilon & \text{if } x \notin L \text{ for } \forall A \end{cases}$$

IPS

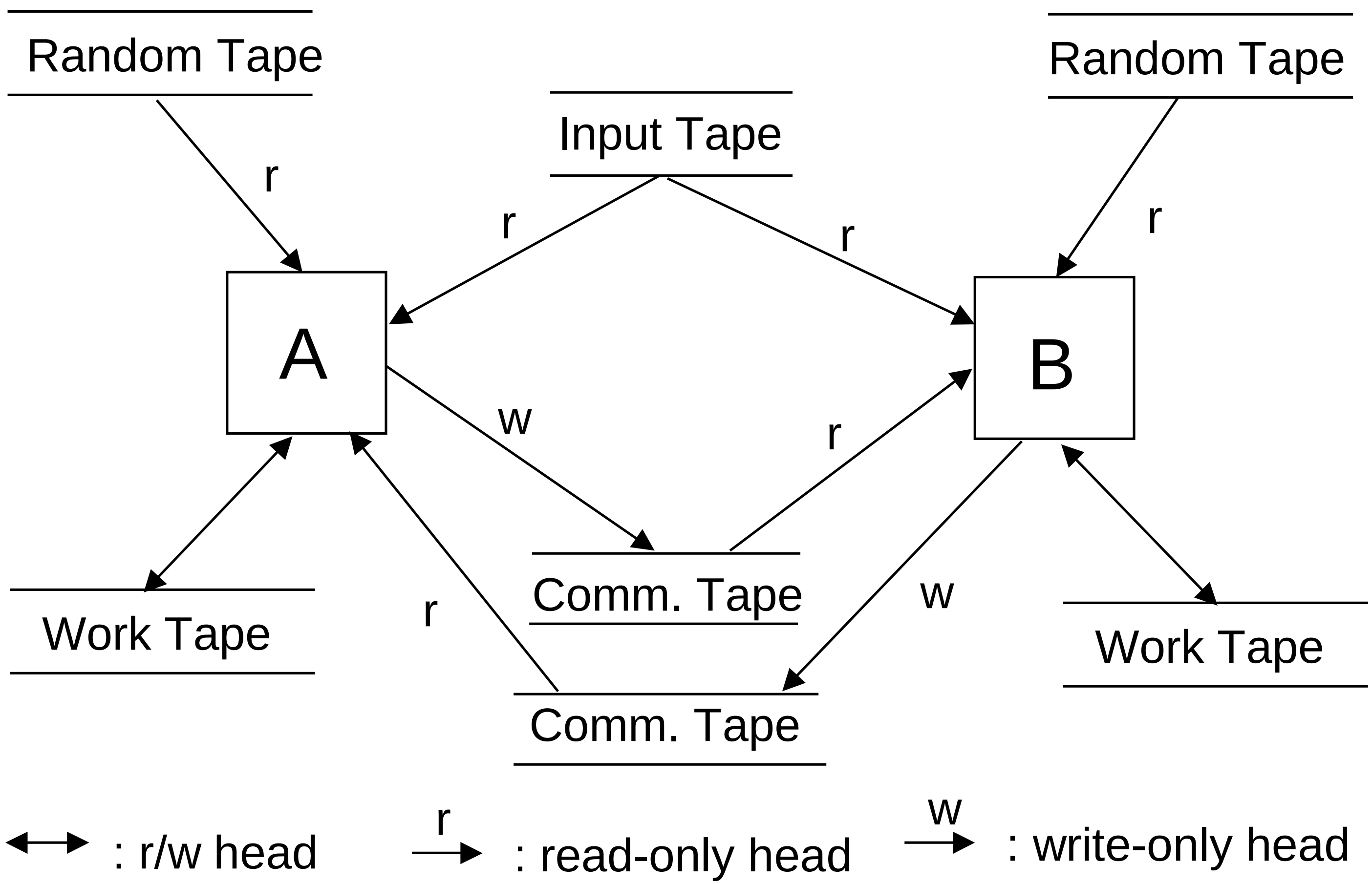
- Protocol : a pair of algorithm (A,B)
- Interactive Proof System : Protocol (A,B) satisfying completeness and soundness
- If L $\in$ IP (Interactive Poly-time), L has an IPS (Interactive Proof System).

ZKIP

- GMR(Goldwasser, Micali, Rackoff)
  ; Proposed at first in 1985

- ZKIP (Zero Knowledge Interactive Proof) : Between P and V,
  - Completeness : Only true P can prove V.
  - Soundness : False P' can't prove V.
  - 0-Knowledge : No knowledge transfer to V.

Turing Machine Model



Concepts of ZKIP

By Quisquater and Guillou

P knows the secret, but he doesn't want to reveal his secret.

1. V stands at point A.

2. P walks all the way into the cave, either C or D.

3. After P disappeared into the cave, V walks to point B.

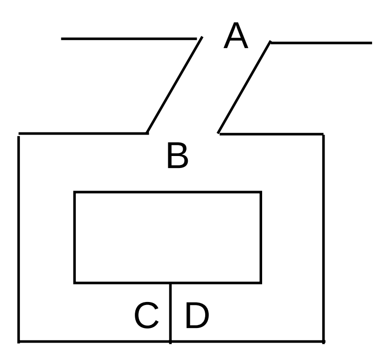
4. V shouts to P asking him either to:

(a) come out of the left passage or (b) come out of the right passage

5. P complies, using the magic words to open secret door if he has to.

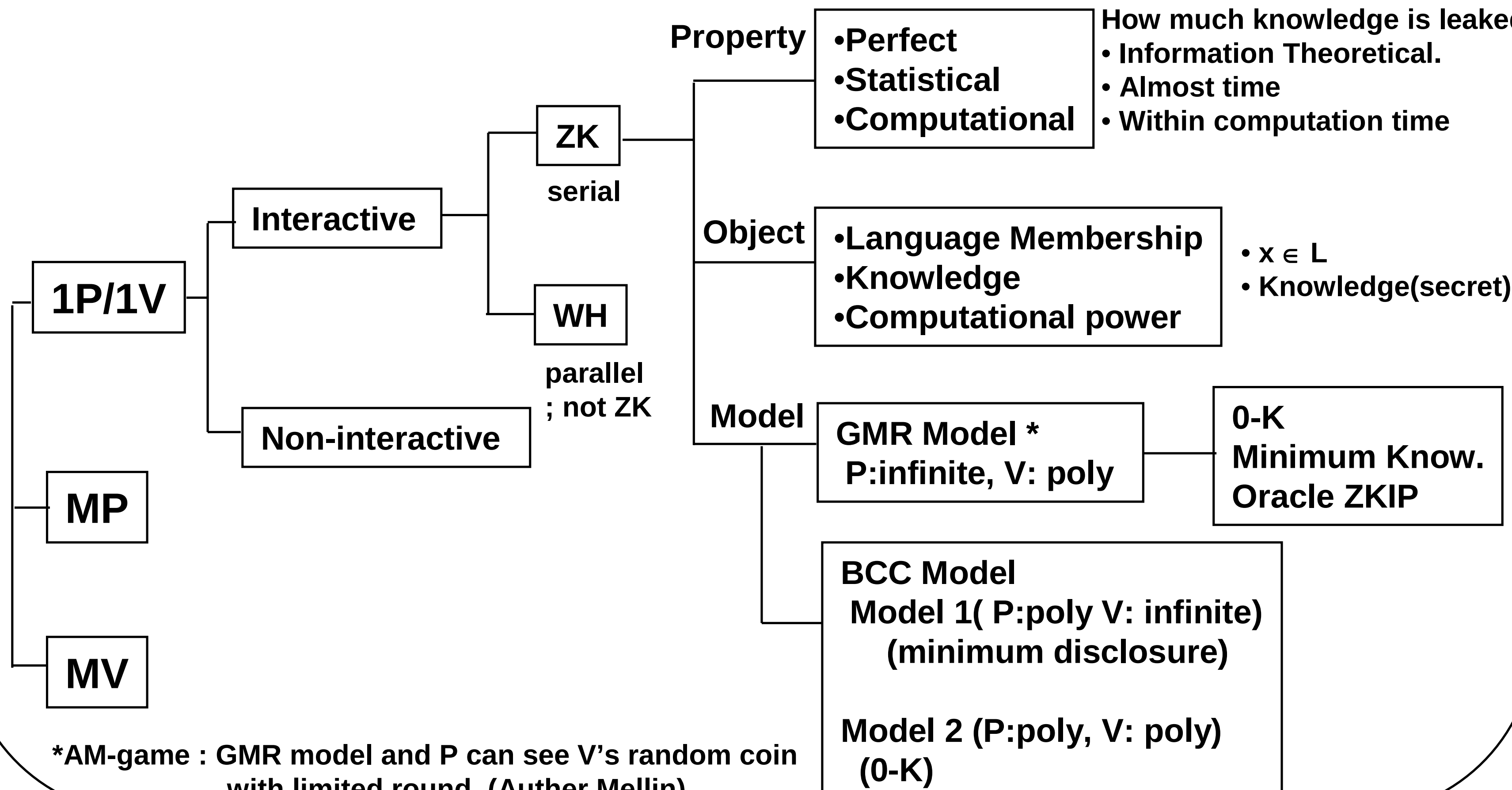
6. P and V repeat step (1) -(5) *t* times

*** P knows the magic words (secret) to open the secret door between C and D.**



0-knowledge cave

Classification of ZKPS



*AM-game : GMR model and P can see V's random coin with limited round, (Auther Mellin)

Indistinguishability (I)

- Family of r.v., U ={U(x)} where *x* is from L, a particular set of $\{0,1\}^*$, all r.v. are taken from $\{0,1\}^*$, U and V are r.v.
- Verdict who can tell a bit from U or V is limited to
  - infinite time and space : perfect
  - infinite time and polysize space : statistical
  - polysize time and space : computational

Indistinguishability (II)

- **L : Language**
- **{U(x)}, {V(x)} : family of random variable**

- **(Perfect) If for all x $\in$ L, U(x) = V(x) (where "= " means "equal as random variables") , {U(x)} and {V(x)} are <u>perfectly indistinguishable</u> for L.**
- **(Statistical) If $\Sigma_{\alpha \in \{0,1\}^*}$ |Pr[U(x)=α] - Pr[V(x)= α]| < ε (|x|), {U(x)} and {V(x)} are <u>statistically indistinguishable</u> for L.**
- **(Computational) For all circuit C (distinguisher) with polynomial size of |x| , if |Pr[C(U(x))=1] - Pr[C(V(x))= 1]| < ε , {U(x)} and {V(x)} are <u>computational indistinguishable</u> for L.**

Way of proofing

There are many ways to prove the truth of a proposition like “I know the modular square root of V” (or any other PSPACE problem):

1. To give the proof (i.e., to tell the square root to the verifier)
2. Zero-knowledge proof : to convince the verifier that the claim holds without giving him any information on the proof (and thus he cannot compute the square root).

ZKIPs are used in identification scheme, in which a user (called the prover) proves to the verifier that he knows a certain secret, without revealing the secret, or any information on the secret.

F-S Identification(I)

- **(Preparation)**

(1) Unlike in RSA, a trusted center can generate a universal *n*, used by everyone as long as none knows the factorization.

(2) P has an RSA modulo $n=pq$ whose factorization is secret.

(3) secret key : P chooses random value *S*, s.t. gcd(S,n)=1.($1 < S < n$)

public key : P computes $I=S^2$ mod *n*, and publishes (I,n) as public

F-S Identification(II)

(Goal)

P has to convince V that he knows secret key *S* corresponding public key (*I*,*n*) (i.e., to prove that he knows a modular square root of *I* mod *n*), without revealing *S*.

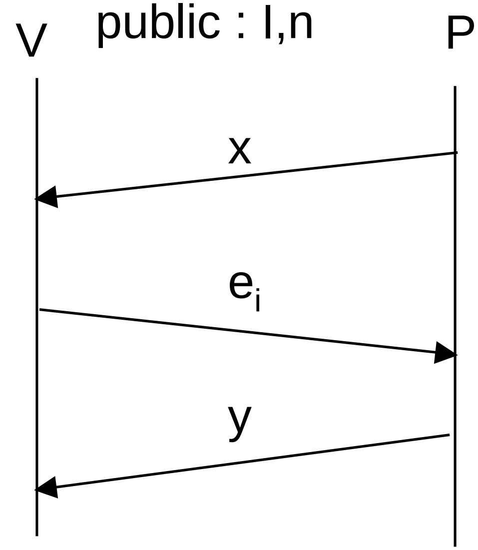
F-S Identification(III)

1. P chooses random value r ($1<r<n$) and computes $x=r^2 \bmod n$. then sends x to V.
2. V requests from P one of the following request at random
   (a) r or (b) rS mod n
3. P sends the requested information to V.
4. V verifies that he received the right answer by checking whether
   (a) $r^2 = x \bmod n$ or (b) $(rS)^2 = xI \bmod n$
5. If verification fails, V concludes that P does not know S, and thus he is not the claimed party.
6. This protocol is repeated t (usually 20 or 30) times, and if in all of them the verification succeeds, V concludes that P is the claimed party.

F-S Identification(IV)

public : I,n

secret, $I=S^2 \bmod n$
$n=pq$



1. generate unique random,r
   $x=r^2 \bmod n$

2.$e_i=\{0,1\}$

3. If $e_i=0$, send $y=r$
   If $e_i=1$, send $y=rS$

4.If $e_i=0$, check $y^2=x \bmod n$?
  If $e_i=1$, check $y^2=xI \bmod n$?

Repeat
t **times**

* commitment-witness-challenge-response-verification and repeat

Security of F-S scheme

(1) It is assumed that computing S is difficult, actually the difficulty is equivalent to that of factoring n.

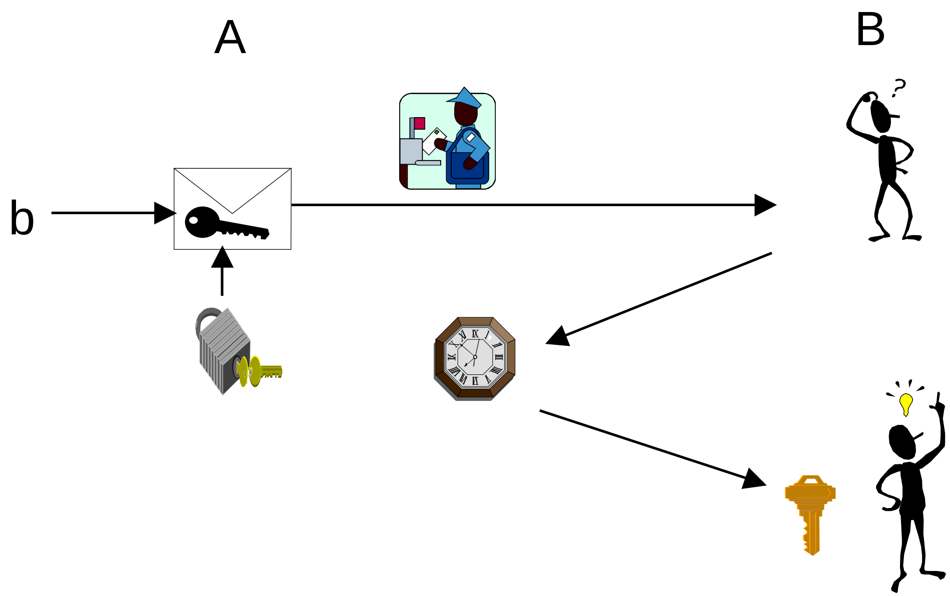
(2) Since P doesn't know in advance (when he chooses r or rS mod n) which question V will ask, he can't choose the required choice. He can succeed in guessing V's question with prob. 1/2 for each question, and thus V can catch him in half of the times, and fails to catch him in half of the times. The protocol is repeated t times,and thus the prob. that V fails to catch P in all the times is only 2^{-t}, which is exponentially reducing with t. (t=20 or 30)

F-S scheme is ZKIP

- The F-S protocol convinces V that P knows the square root of *I*, without revealing any information on *S*. However, V gets <u>one bit</u> of information : <u>he learns that *I* is a quadratic residue</u>

Bit Commitment(I)

- Basic component of many cryptographic protocols
  - Commit stage : A commits B to a bit b, that B has no idea what b is.
  - Revealing stage : B can verify that committed bit is from A.



Bit Commitment(II)

Def) S,V : probabilistic poly time TM

- Commit Phase : S selects b $\in_U$ {0, 1} and sends it to V.
- Reveal Phase : S reveals b to V and V finally accept or rejects.

(1) At commit phase, an adversary A tries to compute b like V, probability to derive *b* is negligible small.

(2) After A did commit phase like S, then revealing b=0 or b=1 at the reveal phase is negligible small even if he has an unlimited power.

(Theorem) We can construct BC for a given 1 –way ft.

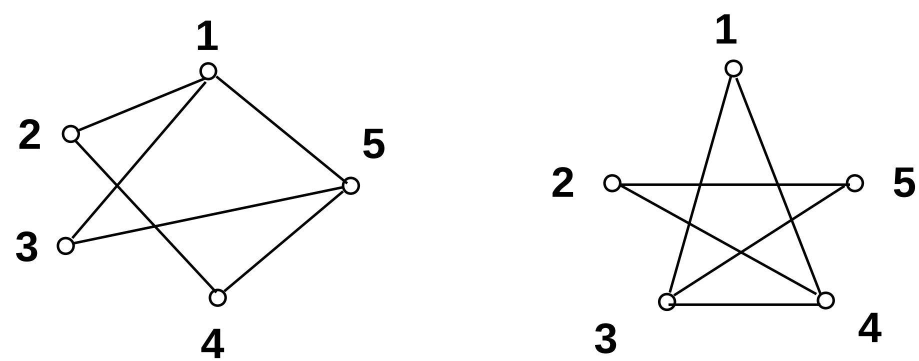
Coin flipping by BC

A		B
$b \in_u \{0,1\}$ $X=BC(b,r)$ where r is random number	$\xrightarrow{X}$	
	$\xleftarrow{c}$	$c \in_u \{0,1\}$
$\alpha = b \oplus c$	$\xrightarrow{(b,r)}$	Verify that $X = BC(b,r)$ If OK, compute $\alpha = b \oplus c$

α: coin flipping result
Each side can't change the value of α at favour.

GI(Graph Isomorphism)

- **(Def) G={V,E}=((1,…,n),({(i,j)})), n vertex**
- **∃ a 1-1 and onto mapping ϕ keeping the incidence relation of Graph G_1 and G_2.**



G_1 G_2

ϕ =(1, 2, 3, 4, 5, $\longrightarrow$
4, 2, 1, 5, 3) $G_2 = \phi\,(G_1)$

GI belongs to NP (Non deterministic Polynomial).

ZKIP using GI (I)

Checks that
P really knows π

G_0, G_1

Knows $G_1=\pi(G_0)$,
but keep π secret.

V

P

H

1. Generate random permutation, ϕ
and commit $H = \phi(G_1)$

repeat, k

2. Generate
random b= {0,1}

b

3. If b=1, $\sigma = \phi$
If b=0, $\sigma = \phi\,\pi$

σ

4. Check
$H = \sigma(G_b)$?

Random Self-reducibility :
average = worst complexity
(*e.g*) GI,DL,QRA

ZKIP using GI(II)

- (Completeness) : If G_0 and G_1 are isomorphism, there exists π and V accepts P with prob. 1.
- (Soundness) : If G_0 and G_1 are not isomorphism, H is not isomorphic to G_0 nor G_1 at step 1. Thus, V selects b at random, the prob. of passing validation step 4 is 1/2. If repeats k times. Prob. of acceptance is $1/2^k$ ($<\varepsilon$ |x|).
- (0-Kness) : Done by Simulator

References(I)

- M.Bellare and O.Goldreich, “On defining proofs of knowledge”, Proc. of Crypto’92, 1992
- M.Bellare, M.Jakosson and M.Yung, “Round-optimal Zero-knowledge arguments based on any one-way function”, Proc. of Eurocrypt’97
- M.Bellare, S.Micali and R.Ostrovsky, “Perfect zero knowledge in constant rounds”, Proc. of 22nd STOC, 1990
- M. Blum, “How to prove a theorem so no one else can claim it”, Proc. of Int’l Congress of Mathematicians, pp.1444-1451, 1986
- M.Blum and S. Micali, “How to generate cryptographically strong sequences of pseudo-random bits”, SIAM J. of Computing, Vol.13, No.4, pp.850-863, 1984
- G. Brassard, D.Chaum and C. Crepeau, “Minumum disclosure proofs of knowledge”, J. of Computer and System Sciences, Vol.37, No.2, pp.156-189, 1988
- G. Brassard, C.Crepeau and M. Yung, “Everything in NP can be argued in perfect zero-knowledge in a bounded number of rounds”, Proc. of 16th ICALP, pp.123-136, 1989
- G.Brassard and C. Crepeau, “Non-transitive transfer of confidence : A perfect zero-knowledge interactive protocol for SAT and beyond”, Proc.of 27th FOCS, 1986
- U.Feige, A.Fiat and A. Shamir, “Zero knowledge proofs of identity”, J. of Cryptology,Vol.1, pp.77-94,1988
- U.Feige and A. Shamir, “Zero knowledge proof of knowledge in two round”, Proc. of Crypto’89, pp.526-544,1989
- O.Goldreich, “A uniform-complexity treatment of encryption and zero-knowledge”, J. of Cryptology, Vol.6, No.1, pp.21-53, 1993
- O.Goldreich and A. Kahan, “On the composition of zero-knowledge proof system”, SIAM J. on Computing, Vol.25, No.1, pp.169-192, 1996
- O.Goldreich, S. Micali and A. Widgerson, “Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof system”, J. of ACM, Vol.38, No.1, pp.691-729, 1991
- S.Goldwasswer, S.Micali and C. Rackoff, “The knowledge complexity of interactive proofs”, Proc. of 17th STOC, pp.291-304, 1985

References(II)

- M.O.Rabin, “Probabilistic algorithm for testing primality”, J. of Number Theory, Vol.12, pp.128-138, 1980.
- R.Solovay and V. Strassen, “ A fast Monte-Carlo test for primality”, SIAM J. on Computing, Vol.6, No.1, pp.84-86, 1977
- M.Tompa and H.Woll, “Random self-reducibility ans zero knowledge interactive proofs of possession of information”, Proc. of 28th FOCS, pp.472-482, 1987
- D.Beaver, “Efficient Multiparty protocols using circuit randomization”, Proc. of Crypto’91, pp.420-432, 1992.
- L.Babai, L.Fortnow, L.Levin and M. Szededi, “Checking computations in poly-logarithmic time”, Proc. of STOC’91
- M.Bellare and O. Goldreich, “On defining proofs of knowledge”, Proc. of Crypto’92, Vol.740, pp.390-420,
- J.Boyar, G. Brassard and P.Peralta, “Subquadratic zero-knowledge”, J. of ACM, Nov. 1995
- M. Ben-Or, O.Goldreich, S. Goldwasser, J. Hastad, J.Killian and S. Micali, “Everything provable is provable in zero-knowledge”, Proc. of Crypto’88, pp.37-56
- J.Benaloh, “ Secret Sharing Homormophisms : keeping shares of a secret secret”, Proc. of Crypto’86, pp.251-260
- R.Cramer and I.Damgard, “Linear Zero-knowledge”, Proc. of STOC’97
- R.Cramer, I.Damgard, U.Mauer, “Span programs and general secure multiparty computations”, BRICS Report series RS-97-27, http://www.brics.dk
- R.Cramer, I.Damgard, B. Schoenmakers, “Proofs of Partial Knowledge and simplified design of witness hiding protocols”, Proc. of Crypto’94, pp.174-187
- E.Fujisaki and T.Okamoto, “Statistical zero-knowledge protocols to prove modular polynomial relations”, Proc. of Crypto’97,
- O.Goldreich, A.Kahan, “How to construct constant-round zero-knowledge proof systems for NP”, J. of Crytology, 1996 (6), 167-189
- G.Gennaro, T.Rabin and M.Rabin, “Simplified VSS and fast-tracking multiparty computation”, Proc. of PODC’98

References(III)

- J.Killian, “Efficient interactive argument”, Proc. of Crypto’95, pp.311-324
- T.Pederson, “Non-interactive and information theoretic secure verifiable secret sharing”, Proc. of Crypto’91, pp.129-140
- A.Shamir, “IP=PSPACE”, J. of ACM, Vol.39, 1992, pp.869-877
- A.Shen, “IP=PSPACE, Simplified Proof”, J. of ACM, Vol.39, 1992, pp.878-880
- A.De Santis, S. Micali, G. Persiano, “Non-interactive zero-knowledge with preprocessing”, Proc. of Crypto’88, 269-282
- M.Bellare and M.Yung, “Certifying permutations : Noninteractive zero-knowledge based on any trapdoor permutations”, J. of Cryptology, 9(3):149-166, 1996
- M.Blum, A. De Santis, S. Micali and G. Persiano, “Noninteractive zero-knowledge”, SIAM J. on Computing, 20(6);1084-1118, 1991
- U.Feige and A. Shamir, “Witness indistingushiability and witness hiding protocols”, Proc. of 22nd STOC, 1990, 416-426
- M.Naor, “Bit commitment using pseudo-randomness”, J. of Cryptology, Vol.4, 1991, pp.151-158
- C.Rackoff and D.Simon, “Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack”, Proc. of Crypto’91, 1992, pp.433-444.