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
I understand that a theorem is correct!!

I discovered theorem X. But it’s proof is secret!!

Zero Knowledge Proof
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

Seed → Generator → Pseudo Random

Indistinguishability !!!

True Random

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

\[ \text{PSPACE} = \text{IP} \]

![Venn Diagram](image-url)

(c)ICU Kwangjo Kim
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

\[
x \in L
\]
Computation & Proof (II)

$L \in P$

$x \xrightarrow{} \text{TM} \quad \begin{cases} x \in L \\ x \notin L \end{cases} \quad \text{Prob. of error } = 0$

$L \in \text{BPP}$

Poly-time

Random tape

$x \xrightarrow{} \text{TM} \quad \begin{cases} 1, & x \in L \\ 0, & x \notin L \end{cases}$

Completeness $x \in L \quad \text{Prob}(\text{TM}(x)=1) \geq 2/3$

Soundness $x \notin L \quad \text{Prob}(\text{TM}(x)=0) \geq 2/3$
BPP(I)

Input $x$ → $M$ → $0, 1$

Random tape

$M(x, r)$

$r_1 \ldots r_k \ldots r_{k+1} \ldots r_{2n}$

$1 \ldots 1 \ 0 \ldots 0$

$\text{Prob}(M(x) = 1) = \frac{k}{2^n}$

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

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

$M(x) : \text{random variable}$
Example of BPP

$L = \{ p \mid p = \text{prime} \}$

Probabilistic prime test by Solovay-Strassen

1. $\gcd (a,p) = 1$  \hspace{1cm} (1)
2. $\left( a/p \right) = a^{(p-1)/2} \mod p$  \hspace{1cm} (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 $a_1, \ldots, a_k$:

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)

\[
\begin{align*}
\Pr[M(x) = 1] & \geq \frac{2}{3} \quad \text{if } x \in L \\
\Pr[M(x) = 0] & \geq \frac{2}{3} \quad \text{if } x \notin L \\
\Pr[M(x) = 1] & \geq \frac{1}{2} + |x|^{-c} \quad \text{if } x \in L \\
\Pr[M(x) = 0] & \geq \frac{1}{2} + |x|^{-c} \quad \text{if } x \notin L \\
\Pr[M(x) = 1] & \geq 1 - 2^{-|x|} \quad \text{if } x \in L \\
\Pr[M(x) = 0] & \geq 1 - 2^{-|x|} \quad \text{if } x \notin L
\end{align*}
\]
Computation & Proof (III)

$L \in \text{NP}$

Superman

$w$ (witness)

Completeness: if $x \in L$, $f(x, \exists w) = \text{accept}$

Soundness: if $x \not\in L$, $f(x, \forall w) = \text{reject}$

(예) $L = \{ n \mid n \text{ is composite} \}$, $n = n_1 n_2$

$n_1$ is a factor of $n$?
Computation & Proof (IV)

\[ L \in \text{IP} \]

Completeness if \( x \in L, \) \( \Pr[B\text{ accepts } x] \geq 1 - \varepsilon \)

Soundness if \( x \notin L, \) \( \Pr[B\text{ rejects } x \text{ for } \forall A] \geq 1 - \varepsilon \)
Meaning of Probability (IP)

Prob(B accepts) ≡ \frac{\text{Area that B accept}}{\text{Total area}}

\begin{align*}
1 - \varepsilon & \text{ if } x \in L \\
< \varepsilon & \text{ if } x \notin L \text{ for } \forall A
\end{align*}
IPS

- Protocol: a pair of algorithm (A,B)

- Interactive Proof System: Protocol (A,B) satisfying completeness and soundness

- If \( L \in \text{IP (Interactive Poly-time)} \), \( L \) 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

Random Tape

Input Tape

Work Tape

Comm. Tape

Random Tape

Input Tape

Work Tape

Comm. Tape

Comm. Tape

: r/w head

: read-only head

: write-only head

(c)ICU Kwangjo Kim
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.
Classification of ZKPS

Interactive

Non-interactive

1P/1V

MP

MV

ZK

Property

• Perfect
• Statistical
• Computational

How much knowledge is leaked
• Information Theoretical.
• Almost time
• Within computation time

Object

• Language Membership
• Knowledge
• Computational power

Model

GMR Model *
P: infinite, V: poly

BCC Model
Model 1 (P: poly, V: infinite) (minimum disclosure)
Model 2 (P: poly, V: poly) (0-K)

0-K
Minimum Know.
Oracle ZKIP

WH

parallel
; not ZK

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

(c) ICU Kwangjo Kim
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 perfectly indistinguishable for \(L\).

- (Statistical) If \(\sum_{\alpha \in \{0,1\}^*} |Pr[U(x) = \alpha] - Pr[V(x) = \alpha]| < \varepsilon(|x|)\), \{U(x)\} and \{V(x)\} are statistically indistinguishable for \(L\).

- (Computational) For all circuit \(C\) (distinguisher) with polynomial size of \(|x|\), if \(|Pr[C(U(x)) = 1] - Pr[C(V(x)) = 1]| < \varepsilon\), \{U(x)\} and \{V(x)\} are computational indistinguishable 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 $x = r^2 \mod n$. 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) $r^2 = x \mod n$ or (b) $(rS)^2 = xI \mod n$
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 : l,n

secret, l=S^2 mod n
n=pq

1. generate unique random, r
x=r^2 mod n

2. e_i={0,1}

Repeat t times

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

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

* 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 one bit of information: he learns that \( I \) is a quadratic residue.
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 $b \in \{0, 1\}$ 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

\[ b \in \{0,1\} \]
\[ X = BC(b, r) \]
where \( r \) is random number

\[ \alpha = b \oplus c \]

Verify that \( X = BC(b, r) \)
If OK, compute \( \alpha = b \oplus c \)

\( \alpha \): coin flipping result
Each side can’t change the value of \( \alpha \) at favour.
GI (Graph Isomorphism)

- (Def) $G = \{V, E\} = ((1, \ldots, n), \{(i, j)\})$, $n$ vertex
- $\exists$ a 1-1 and onto mapping $\phi$ keeping the incidence relation of Graph $G_1$ and $G_2$.

$\phi = (1, 2, 3, 4, 5, 4, 2, 1, 5, 3)$

$G_2 = \phi(G_1)$

GI belongs to NP (Non deterministic Polynomial).
ZKIP using GI (I)

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

2. Generate random $b = \{0,1\}$

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

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

Checks that $P$ really knows $\pi$

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

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

Repeat, $k$
ZKIP using GI(II)

- (Completeness) : If \( G_0 \) and \( G_1 \) are isomorphism, there exists \( \pi \) 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 \( 1/2^k \) \((< \epsilon |x|)\).

- (0-Kness) : Done by Simulator
References(I)

- 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
References (II)

- M. Ben-Or, O.Goldreich, S. Goldwasser, J. Hastad, J.Killian and S. Micali, “Everything provable is provable in zeroknowledge”, Proc. of Crypto’88, pp.37-56
- E.Fujiyaki and T.Okamoto, “Statistical zero-knowledge protocols to prove modular polynomial relations”, Proc. of Crypto’97,
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