12.4

Zero-Knowledge Proof

$P: \{0,1\}^* \longrightarrow \{0,1\}$

P solvable
x

Prover

Verifier
poly time

NP

IP: Interactive Proof

IP = PSPACE

若 $P_1 \rightleftarrows V$

$P_2 \rightleftarrows V$

MIP: Multi-prover IP = NEXP

Language L

Claim:
$x \in L$

prover $\rightleftarrows$ Verifier (poly-time)

IP: if $x \in L$, $\Pr[\langle P(x), V(x) \rangle = 1] = 1$

if $x \notin L$, $\forall P^*$, $\Pr[\langle P^*, V(x) \rangle = 1] \leq \frac{1}{2}$

Alice claim: (N, e) is valid RSA pk （不能发 p, q）

claim: a is a QR_N

b is a QNR_N

Example of ZKP

图 G

Alice claim: s 和 t 点 连通

$\xrightarrow{r \xleftarrow{\$} G,\ (s,r) \text{连通}}$

$\xleftarrow{b \xleftarrow{\$} \{0,1\}}$

$\longrightarrow$

path $s \to r$ if $b=0$

path $r \to t$ if $b=1$

claim: $a \in QR_N$ （$a = x^2$）只有 Alice 知道

$\xrightarrow{r = y^2,\ y \xleftarrow{\$}}$

Prover $\xleftarrow{b \xleftarrow{\$} \{0,1\}}$ Verify

$\longrightarrow$

y if $b=0$

$\frac{x}{y}$ if $b=1$

ZKP Protocol: ppt algo P, V

Completeness: $\forall x \in L$, $\Pr[\langle P(x,w), V(x) \rangle \to 1] = 1$

Soundness: $\forall x \notin L$, $\forall P^*$

$$\Pr[\langle P^*, V(x) \rangle \to 1] < \frac{1}{2}$$

Honest Zero Knowledge (perfect): $\exists$ ppt Simulator S

$\forall x \in L, \forall w$, $\{S(x)\} \underset{\text{identical}}{=} \{View_V(\langle P(x,w), V(x) \rangle)\}$

QR_N protocol Simulator S:

$b \xleftarrow{\$} \{0,1\}$

if $b=0$, $y \xleftarrow{\$}$, $r=y^2$

if $b=1$, $z \xleftarrow{\$}$, $r=\frac{a}{z^2}$

Graph Isomorphism: $(G_0, G_1) \in L$ iff $\exists$ permutation π, s.t. $\pi(G_0)=G_1$

Prover: sample τ

$\xrightarrow{G_2 = \tau \circ G_0}$

$b \xleftarrow{\$} \{0,1\}$

$\xleftarrow{\quad}$

$\xrightarrow{\quad}$

proof $G_b \cong G_2$

$\begin{cases} \tau & b=0 \\ \tau\circ\pi^{-1} & b=1 \end{cases}$

Completness, Soundness 显然

Simulator, $b \xleftarrow{\$} \{0,1\}$

若 $b=0$, sample τ

若 $b=1$, sample $\tau\circ\pi^{-1}$

都是 Honest Verifier

Malicious Verifier Zero-Knowledge:

$\forall_{ppt} V^*$, $\exists$ p.p.t S

$\forall x \in L$, $\forall$ witness w

$$\{S(x)\} \xleftrightarrow{id} \{View_V(\langle P(x,w), V^*(x)\rangle)\}$$

QR_N malicious Simulator S:

sample rt, $b \xleftarrow{\$} \{0,1\}$

$$r = \begin{cases} \text{———} \\ \text{———} \end{cases}$$

$$b' \longleftarrow V^*(x, rt)$$

若 $b'=b$, output View

若 $b' \neq b$, rewind

$$View = \{S(x)\}$$

Graph Non Isomorphism 需prover无限算力

QNR ZK:

$$\xleftarrow{u^2 \text{ 或 } v^2 \cdot a}$$

$$\xrightarrow{v^2 a \notin QR}$$

$$\{S(x)\} \approx_c \{View_V(\langle P(x,w), V(x)\rangle)\}$$

claim: Graph G is 3-colorable

Commitment

Commit: Prover Verifier

Open get m

Completeness Open(Commit(m))=m

Hiding: "Verifier learns nothing before open 不可能同时perfect

Binding: "After commiting, cannot change"

Construction from OWP

P($m\in\{0,1\}$)

sample r

Commit: $\xrightarrow{OWP(r),\ HCB(r)\oplus m}$

Open: $\xrightarrow{r,m}$

3-colorable

commit(染色) $\longrightarrow$

$\xleftarrow{看一条边}$ Soundness error $\leq 1-\frac{1}{|E|}$

open边 $\longrightarrow$

Simulator: 随机染色, commit

Boost Soundness Error

sequential simulator

parallel：不一定安全

Sol1: Random Oracle

$P \xrightarrow{a} V \quad RO(a)$

$\xleftarrow{b}$

$\xrightarrow{z}$

$\vdots$

不安全 P把自己当 simulator

$P \xrightarrow{a^1} \xrightarrow{a^2} \cdots \quad V$

$\xleftarrow{b^1} \xleftarrow{b^2} \quad (b^1 b^2 \ldots b^T) = RO(a_0, a_1, a^1 a^2, \ldots)$

$\xrightarrow{z^1} \xrightarrow{z^2} \cdots$

Zero knowledge < proof / argument (ppt prover) (of knowledge)

(non-interactive) → perfect / statistic / computational

Proof of knowledge: Prover without witness cannot convince the Verifier, ∃ppt Extractor E

$\forall x, \forall \text{ppt } P^*$, 若 $\Pr[\langle P^*, V(x)\rangle \to 1] \geq \frac{2}{3}$

$E(P^*) \to w$, s.t. w 是 witness

Zero-Knowledge Proof

Boost Soundness Error:

Sequential repeat。安全

Parallel repeat：

Simulator: 先 sample $b_1, b_2, ..., b_\lambda$，再调用 V^* 代码看是否猜中所有 b_i，以 $\frac{1}{2^\lambda}$ 概率全猜对。无法 poly-time simulate 出原分布，不一定安全。

Non-interactive ZKP：

Sol1: 用 Random Oracle

Graph-Isomorphism 问题，认为 sample b 是一个 Random Oracle。b_i 也由 Prover 发给 Verifier

若 Sequential 重复：若 $(G_0, G_1) \in GRAPH_ISOMORPHISM$，可类似 simulator rewind 的过程，若某个 G_i，Prover 会的问题不是 $RO(G^i)$，则重新随机 G^i。期望 2 次可获得会的 b。则不满足 Soundness。

若 Parallel 重复。当命题为假时，$(b_1, b_2, ..., b_\lambda) = RO(G^1, G^2, ..., G^\lambda)$，只有 $\frac{1}{2^\lambda}$ 概率随机到，Prover 难以生成错误证明。则 Soundness 满足。

Zero-Knowledge: Simulator: 可随机 $(G^1, G^2, ..., G^\lambda)$，令 $RO(G^1, G^2, ..., G^\lambda)$ 为每个 G^i 会做的那个问题。

Non-interactive computationally ZKP 证明 NPC 语言：

Sol2:Common Random String

Prover 和 Verifier 共享一个 random string。将其视为若干个 $\mathbb{Z}_n$ 中的元素。

(1).

Claim: N 至多有 2 种不同质因数，即 $N = p^c q^d, p, q \in Prime$。（此方法并不能证明 $N = pq$）

Protocol: CRS 看作 $r_1, r_2, ..., r_\lambda$。

首先忽略所有 $\left(\frac{r_i}{N}\right) \neq 1$ 的 r_i，c 和 d 不全是偶数时大概丢弃一半，Verifier 也可以验证。对于剩下的满足 $\left(\frac{r_i}{N}\right) = 1$ 的 $r_1, r_2, ..., r_\lambda$：

对所有 $r_i \in \mathbb{QR}_N$，将 $\sqrt{r_i}$ 发给 Verifier。由分布大概 $\frac{1}{2}$ 的数是二次剩余。既可以发送大约 $\frac{\lambda}{4}$ 个数。

对于 c 和 d 都是偶数的情况，所有数 jacobi 符号都是 1，那么随机丢弃一半的数，依然符合分布。

Completeness: 显然。

Soundness: 多于 2 个不同质因数的 N，$\mathbb{Z}_n^*$ 中有至多 $\frac{1}{8}$ 是二次剩余。

Zero-Knowledge: Simulator：每个位置以 $\frac{1}{4}$ 概率，sample 一个 y，令 $r_i = y^2 mod N$。以 $\frac{3}{4}$ 概率 r_i 从 $\mathbb{Z}_N^*$ 中 sample。

(2).

Claim：$g \in \mathbb{QNR}_N$

12.4

Zero-Knowledge Proof

$P: \{0,1\}^* \longrightarrow \{0,1\}$

$\boxed{P \text{ solvable } x}$

Prover Verifier (poly time)

NP

IP: Interactive Proof IP = PSPACE

若 $P_1 \rightleftarrows V$, $P_2 \rightleftarrows V$

MIP: Multi-prover IP = NEXP

Language L

$\boxed{\text{Claim: } x \in L}$

prover $\rightleftarrows$ Verifier (poly-time)

IP: if $x \in L$, $Pr[\langle P(x), V(x)\rangle = 1] = 1$

if $x \notin L$, $\forall P^*$, $Pr[\langle P^*, V(x)\rangle = 1] \leq \frac{1}{2}$

Alice claim: (N, e) is valid RSA pk (不能给 p, q)

claim: a is a QR_N

b is a QNR_N

Example of ZKP

图 G

Alice claim: s 和 t 点连通

$\xrightarrow{r \xleftarrow{\$} G,\ (s,r)\text{连通}}$

$\xleftarrow{b \xleftarrow{\$} \{0,1\}}$

$\longrightarrow$ path $s \to r$ if $b=0$; path $r \to t$ if $b=1$

claim: $a \in QR_N$ ($a = x^2$) 只有Alice知道

Prover $\xrightarrow{r = y^2,\ y \xleftarrow{\$}}$ Verify

$\xleftarrow{b \xleftarrow{\$} \{0,1\}}$

$\longrightarrow$ y if $b=0$; $\frac{x}{y}$ if $b=1$

ZKP Protocol: ppt algo P, V

Completeness: $\forall x \in L$, $Pr[\langle P(x,w), V(x)\rangle \to 1] = 1$

Soundness: $\forall x \notin L$, $\forall P^*$

$Pr[\langle P^*, V(x)\rangle \to 1] < \frac{1}{2}$

Honest Zero-Knowledge (perfect): $\exists$ ppt Simulator S

$\forall x \in L, \forall w$, $\{S(x)\} \xlongequal{\text{identical}} \{View_V(\langle P(x,w), V(x)\rangle)\}$

98

QR protocol Simulator S:

Protocol: 同 (1) 中处理，只考虑 $\left(\frac{s_i}{N}\right)=1$ 的数。

若 $s_i \in \mathbb{QR}_N$，发送 $\sqrt{s_i}$。

否则 $s_i \cdot g \in \mathbb{QR}_N$，发送 $\sqrt{s_i \cdot g}$

大概可发送 $\frac{1}{2}$ 的数。

Completeness：显然。

Soundness: 若 $g \in \mathbb{QR}_N$，则 $s_i \in \mathbb{QNR}_N$ 时无法发送，只能发大约 $\frac{1}{4}$ 的数。

Zero-knowledge: Simulator: 每个位置以 $\frac{1}{2}$ 概率 $s_i \in \mathbb{Z}_N^*$ 均匀 sample。以 $\frac{1}{4}$ 概率，$y \in \mathbb{Z}_N^*$ 均匀 sample，令 $s_i = y^2 modN$。以 $\frac{1}{4}$ 概率，$y \in \mathbb{Z}_N^*$ 均匀 sample，令 $s_i = y^2 \cdot g^{-1} modN$。

(3)

claim：某 $3CNF$ 存在一组合法解。

Protocol: 类似 (1) 中处理，只考虑 $\left(\frac{t_i}{N}\right)=1$ 的所有 t_i。

取 $g \in \mathbb{QNR}_N$，发送证明。每个 $3CNF$ 中变量 x_i，令 $c_i = g^{x_i} \cdot u^2$，u 随机 sample。发送所有 c_i。

对每个分句，证明 $d_{i,1}, d_{i,2}, d_{i,3}$ 至少一个是 QNR。其中若 $c_{i,j}$ 本身出现，$d_{i,j} = c_{i,j}$。若 $c_{i,j}$ 取反命题出现，则 $d_{i,j} = g \cdot c_{i,j}$。

对 CRS 中当前 t_i，根据其是否属于 $\mathbb{QR}_N$ 决定一组 z_1, z_2, z_3，使得 $t_i \cdot d_{i,1} \cdot d_{i,2} \cdot d_{i,3} \in \mathbb{QR}_N$，并发送 z_1, z_2, z_3 和其平方根 π_i。

Completeness 显然

Soundness: 若某个分句每个 literal 都是 0，则当 $t_i \in \mathbb{QNR}_N$ 时，无论怎么选 z，$t_i \cdot d_{i,1} \cdot d_{i,2} \cdot d_{i,3}$ 都不是二次剩余，只能发大约一半的值。

Zero-knowledge: c_i 部分直接 random sample（residual assumption）。

以 $\frac{1}{2}$ 概率，t_i 在 $\mathbb{Z}_N^*$ 中 random sample。

以 $\frac{1}{2}$ 概率，$z_{i,1}, z_{i,2}, z_{i,3}$ 在 $\{0,1\}^3$ 中随机 sample。pi_i 在 $\mathbb{Z}_N^*$ 中随机 sample。$t_i = \pi_i^2 \cdot (c_{i,1}^{z_{i,1}} \cdot c_{i,2}^{z_{i,2}} \cdot c_{i,3}^{z_{i,3}})^{-1}$