1outof2

RSA: N, e →

random x_0, x_1 →

pick b, random k

← $v = x_b + k^e$

$k_0 = (v - x_0)^d, k_1 = (v - x_1)^d$

$m'_0 = m_0 + k_0, m'_1 = m_1 + k_1$ →

$m_b = m'_b - k$

3ballot

Alice ○	Alice ○	Alice ○
Bob ○	Bob ○	Bob ○
Charlie○	Charlie○	Charlie○
ID2902	ID2076	ID3384

Empty ballots

Alice ○	Alice ○	Alice ●
Bob ●	Bob ●	Bob ○
Charlie○	Charlie●	Charlie○
ID6232	ID1602	ID7614

Vote for Bob

3parties-DHKE

C

(1) g^b (2) g^{bc} (1) g^c (2) g^{ac}

A (1) g^a (2) g^{ca} B

3parties-JOUX

C

cP aP bP cP

A aP bP B

CBC-MAC

m_1 m_2 m_3

0^n → ⊕ → F_k → ⊕ → F_k → ⊕ → F_k → t

CBC-small

m_1 m_2 m_3

IV → ⊕ → F_k → ⊕ → F_k → ⊕ → F_k

IV c_1 c_2 c_3

CBC

m_1 m_2 m_3

IV → ⊕ → F_k → ⊕ → F_k → ⊕ → F_k

IV IV c_1 c_2 c_3

CCA-PKCS

pk — $[c' = (2^r)^e \cdot c]$ → sk

← [Yes/No: $MSB(m') = {}'1'$] —

Client   Server

CCA

k_1, k_2 → Gen' → k_1, k_2

m → Enc' — $\langle c, t \rangle$ → Dec' → m

Alice   Bob

Adversary   ⊥

CMAC

m_1 m_2 m_3

0^n → ⊕ → F_k → ⊕ → F_k → ⊕ → F_k ← k_1 or k_2 → t

CTR

ctr   ctr + 1   ctr + 2   ctr + 3

F_k F_k F_k

m_1 → ⊕ m_2 → ⊕ m_3 → ⊕

ctr c_1 c_2 c_3

DESkey

56-bit key

28-bit	28-bit
L-Shift	L-Shift
L PC	R PC

48-bit sub-key

56-bit key

DHkey

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}$

$x \leftarrow \mathbb{Z}_q$

$h_1 := g^x$ $\mathbb{G}, q, g, h_1$ →

$y \leftarrow \mathbb{Z}_q$

← h_2 $h_2 := g^y$

$k_A := h_2^x$ $k_B := h_1^y$

Davies-Meyer

m_i

h_{i-1} → F → ⊕ → h_i

ECB

m_1 m_2 m_3

F_k F_k F_k

c_1 c_2 c_3

ElGamal

$\mathbb{G}, q, g$

g^x, g^y

D $pk = \langle \mathbb{G}, q, g, g^x \rangle$

m_1, m_2

$g_3 = g^z$ or g^{xy}

$b \leftarrow \{0, 1\}$ $(g^y, g_3 \cdot m_b)$ $\mathcal{A}$

1 if $b' = b$ b'

HMAC

$k \oplus ipad$, m_1, $\cdots$, $|m|$, IV, $k \oplus opad$

$IV \rightarrow h^s \rightarrow h^s \rightarrow \cdots \rightarrow h^s \rightarrow h^s \rightarrow h^s \rightarrow t$

IBE

KGC

generate KGC pk and sk;
generate Bob's sk_B from
sk and "Bob"

ask for Bob

Alice $\xrightarrow{E_{pk_B}(m)}$ Bob

generate Bob's pk_B from
KGC's pk and "Bob"

KDC

KDC

I want to talk to Bob

$E_{Alice}(k), E_{Bob}(k)$

Alice $\xrightarrow{\text{Let's talk, } E_{Bob}(k)}$ Bob

MDtransform

x_1, x_2, $\cdots$, x_B, L

$IV \rightarrow h^s \rightarrow h^s \rightarrow \cdots \rightarrow h^s \rightarrow h^s \rightarrow H^s(x)$

MS-PPTP

k, k

$\xleftarrow{[m_1 \| m_2 \| m_3] \oplus PRG(k)}$

$\xleftarrow{[s_1 \| s_2 \| s_3] \oplus PRG(k)}$

Client, Server

Miyaguchi-Preneel

h_{i-1}

$m \rightarrow F \rightarrow \oplus \rightarrow h_i$

NMAC

m_1, m_2, $\cdots$, $|m|$, k_1

$k_2 \rightarrow h^s \rightarrow h^s \rightarrow \cdots \rightarrow h^s \rightarrow h^s \rightarrow t$

OAEP-plus

m, $W(m,r)$, r

G, H

$\hat{m}_1$, $\hat{m}$

OAEP

m, $00 \cdots 0$, r

G, H

s, t

OFB

IV

F_k, F_k, F_k

$m_1 \rightarrow \oplus$, $m_2 \rightarrow \oplus$, $m_3 \rightarrow \oplus$

IV, c_1, c_2, c_3

OWF

easy

x, $f(x)$

hard

SAEP-plus

m, $W(m,r)$, r

H

$\hat{m}_1$, $\hat{m}$

SIV-CTR

SIV, $SIV+1$, $SIV+2$, $SIV+3$

F_{k_1}, F_{k_2}, F_{k_2}, F_{k_2}

m, $m_1 \rightarrow \oplus$, $m_2 \rightarrow \oplus$, $m_3 \rightarrow \oplus$

$t := SIV$, c_1, c_2, c_3

TDES

k_1, k_2, k_3

$x \rightarrow F \rightarrow F^{-1} \rightarrow F \rightarrow y$

VCBC-MAC

$|m|$, m_1, m_2, m_3

F_k, F_k, F_k, F_k

t

alice

attack-spn

- 20 bits known
- 20 bits unknown
- 4 bits compared

authentication

$k \leftarrow$ Gen $\rightarrow k$

Alice — Enc $\cdots$ Dec $\rightarrow m'$ Bob

Adversary c'

baby-giant

$t = \lfloor\sqrt{q}\rfloor$

$g^{k \cdot t}$

y $y \cdot g^i$ $y \cdot g^t$

bilinear-map

G_1 P abP aP bP

mapping e

G_2 $e(P,P)^{ab}$

birthdayattack

I J

x_0

i $2i$

blindsignature

Signer

$pk = e,\ sk = d$

$m' \equiv mr^e$

$s' \equiv m'^d$

$s \equiv s'r^{-1}$

Generate a random r

cPRF

k

$G_0(k)$ $G_1(k)$

$G_0(G_0(k))$ $G_1(G_0(k))$ $G_0(G_1(k))$ $G_1(G_1(k))$

$F_k(011) = G_1(G_1(G_0(k)))$

certificates

CA

Alice trusts Charlie and knows pk_C.

Bob trusts Charlie. Charlie knows pk_B.

$cert_{C \to B}$

$pk_B, cert_{C \to B}$

Alice Bob

chain-sig

pk_1 m_1 pk_2 m_2 pk_3 $\cdots$ pk_i m_i pk_{i+1}

sk_1 σ_1 sk_2 σ_2 sk_3 $\cdots$ sk_i σ_i sk_{i+1}

cipher-stealing

m_{l-1} F c_{l-1} c_l

m_l F c_l c_{l-1}

coinflipping

$b \leftarrow \{H,T\}$

$m = b\|r, r$ is random

$h = \mathsf{Hash}(m)$

$b' \in \{H,T\}$

$m \longrightarrow$ $h \overset{?}{=} \mathsf{Hash}(m)$

Win if $b = b'$

collision

X Y X Y X Y

Collision Resistance 2nd Pre-image Resistance Pre-image Resistance

combination

Enc Mac   Enc Mac   Mac Enc

compute-sec

Pr. of break: ε

Break!

Brute force

Security Zone

Time: t

constructD

$w \in \{0,1\}^{\ell(n)}$

n from $\ell(n)$

$\mathcal{D}$ $b \leftarrow \{0,1\}$ n

$m_0, m_1 \in \{0,1\}^{\ell(n)}$

$c := w \oplus m_b$

$\mathcal{A}$

1 if $b' = b$

b'

des

32-bit input 48-bit sub-key

Expansion

48-bits

48-bits (8×6-bits)

s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8

32-bits (8×4-bits)

Permutation

desx

k_1 k_2 k_3

$x \longrightarrow \oplus \longrightarrow F \longrightarrow \oplus \longrightarrow y$

differential

$\Delta P = [0000\ 1011\ 0000\ 0000]$

K_1

$S_{1,1}$ $S_{1,2}$ $S_{1,3}$ $S_{1,4}$ $S_{1,2}:\ \Delta X = B \to \Delta Y = 4$

K_2

$S_{2,1}$ $S_{2,3}$ $S_{2,4}$ $S_{2,2}:\ \Delta X = 4 \to \Delta Y = 5$

K_3

$u_{3,6}$ $u_{3,14}$

$S_{3,1}$ $S_{3,2}$ $S_{3,3}$ $S_{3,4}$ $\Delta U = [0000\ 0100\ 0000\ 0100]$

K_4 $k_{4,2\cdot i}$ Guess $k_{4,2\cdot i}$

digitalsignature

$sk \longleftarrow$ Gen $\longrightarrow pk$

Alice m Enc $\cdots\ c\ \cdots$ Dec m Bob

m Sign $\longrightarrow \sigma \longrightarrow$ Vrfy b

dining

doubleE

k_1 k_2

$x \longrightarrow F \longrightarrow F \longrightarrow y$

ePRG

s_0 $f^0(s)$

s_1 $f^1(s)$ hc_0

s_2 $f^2(s)$ hc_1 hc_0

s_3 $f^3(s)$ hc_2 hc_1 hc_0

elgamal-con

y m

g^y h^y $\cdot$

c_1 c_2

encryptionwithpf

r

$k \longrightarrow F$

Pad

$m \longrightarrow \oplus \longrightarrow c$

encryptionwithpg

k

G

Pad

$m \longrightarrow \oplus \longrightarrow c$

feistel-prp

L_0 R_0

$\oplus$ F_{k_1}

$\oplus$ F_{k_2}

$\oplus$ F_{k_3}

$\oplus$ F_{k_4}

L_4 R_4

feistel

L_0 R_0

$\oplus$ f_1

$\oplus$ f_2

$\oplus$ f_3

$\oplus$ f_4

L_4 R_4

feistel2

L_0 R_0

$\oplus$ f_1

L_1 $\oplus$ f_2 R_1

L_2 R_2

feistel3

L_0 R_0

$\oplus$ f_1

L_1 $\oplus$ f_2 R_1

L_2 $\oplus$ f_3 R_2

L_3 R_3

hash

Gen $\to s$

m H h

hcp

easy

x $f(x)$

hc(x)

easy   hard

hs-reduce-1

s

$\mathcal{C}$ $pk' = \langle pk, s \rangle$

m_i

$\sigma_i \leftarrow \mathsf{Sign}_{sk}(H^s(m_i))$ $\mathcal{A}'$

(m, m_i) if $\exists i$ (m, σ)

$H^s(m) = H^s(m_i)$

hs-reduce-2

$$pk \quad \mathcal{A} \quad pk' = \langle pk, s\rangle$$
$$\hat{m}_i := H^s(m_i) \qquad m_i$$
$$\sigma_i \text{ on } \hat{m}_i \qquad \sigma_i$$
$$\mathcal{A}'$$
$$(H^s(m), \sigma) \qquad (m, \sigma)$$

hybrid-enc-proof

$$\langle pk, \mathsf{Enc}_{pk}(k), \mathsf{Enc}'_k(m_0)\rangle \xleftrightarrow{\text{(by transitivity)}} \langle pk, \mathsf{Enc}_{pk}(k), \mathsf{Enc}'_k(m_1)\rangle$$

(by security of Π) \qquad (by security of Π)

$$\langle pk, \mathsf{Enc}_{pk}(0^n), \mathsf{Enc}'_k(m_0)\rangle \longleftarrow \langle pk, \mathsf{Enc}_{pk}(0^n), \mathsf{Enc}'_k(m_1)\rangle$$

(by security of Π')

hybrid-encrypt

$$k \qquad m$$
$$pk \to \boxed{\mathsf{Enc}_{pk}} \quad \boxed{\mathsf{Enc}'_k}$$
$$c_1 \qquad c_2$$

hybrideg

$$pk \qquad \mathcal{A}' \qquad pk$$
$$m_0^2, m_1^2 \qquad (m_0^1, m_0^2), (m_1^1, m_1^2)$$
$$c_b^2 \qquad (c_0^1, c_b^2)$$
$$\mathcal{A}$$
$$b' \qquad b'$$

hybridproof

$$pk \qquad \mathcal{A}' \quad i \leftarrow \{1, \ldots, t\} \qquad pk$$
$$m_0^i, m_1^i \qquad \vec{M}_0, \vec{M}_1$$
$$c_b^i \qquad \vec{C}^{(i-b)}$$
$$\mathcal{A}$$
$$b' \qquad b'$$

identification-schnorr

Prover (x) \qquad Verifier $(\mathbb{G}, q, g, y)$

$$k \leftarrow \mathbb{Z}_q; \ I := g^k \xrightarrow{\ I\ }$$
$$\xleftarrow{\ r\ } \quad r \leftarrow \mathbb{Z}_q$$
$$s := [rx + k \mod q] \xrightarrow{\ s\ }$$
$$g^s \cdot y^{-r} \stackrel{?}{=} I$$

identification

Prover (sk) \qquad Verifier (pk)

$$(I, \mathsf{st}) \leftarrow \mathcal{P}_1(sk) \xrightarrow{\ I\ }$$
$$\xleftarrow{\ r\ } \quad r \leftarrow \Omega_{pk}$$
$$s := \mathcal{P}_2(sk, \mathsf{st}, r) \xrightarrow{\ s\ }$$
$$\mathcal{V}(pk, r, s) \stackrel{?}{=} I$$

integrity

$$k \xleftrightarrow{} \boxed{\mathsf{Gen}} \xrightarrow{} k$$
$$\text{Alice} \xrightarrow{m} \boxed{\mathsf{Enc}} \qquad \boxed{\mathsf{Dec}} \xrightarrow{m'} \text{Bob}$$
$$c \qquad c'$$
$$\text{Adversary}$$

interlock

$$pk_A$$
$$pk_B$$
$$c_A = \mathsf{Enc}_{pk_B}(m_A) \qquad c_B = \mathsf{Enc}_{pk_A}(m_B)$$
$$(c_{A1}\|c_{A2}) = c_A \qquad (c_{B1}\|c_{B2}) = c_B$$
$$c_{A1}$$
$$c_{B1}$$
$$c_{A2}$$
$$c_{B2}$$
$$c_B = (c_{B1}\|c_{B2}) \qquad c_A = (c_{A1}\|c_{A2})$$
$$m_B = \mathsf{Dec}_{pk_A}(c_B) \qquad m_A = \mathsf{Dec}_{pk_B}(c_A)$$

keyed-func

$$K \quad X \quad Y \qquad X \quad Y \qquad X \quad Y$$

$$F: K \times X \to Y \qquad F_k(x) \stackrel{\text{def}}{=} F(k, x) \qquad f: X \to Y$$
2D function \qquad Keyed function \qquad Look-up table

linear

$$p_5 \quad p_7 p_8$$
$$k_{1,5} k_{1,7} \quad k_{1,8}$$
$$S_{1,1} \quad S_{1,2} \quad S_{1,3} \quad S_{1,4} \qquad S_{1,2}: x_1 \oplus x_3 \oplus x_4 = y_2$$
$$k_{2,6} \quad K_2$$
$$S_{2,1} \quad S_{2,2} \quad S_{2,3} \quad S_{2,4} \qquad S_{2,2}: x_2 = y_2 \oplus y_4$$
$$k_{3,6} \quad K_3 \quad k_{3,14}$$
$$u_{3,6} \qquad u_{3,14}$$
$$S_{3,1} \quad S_{3,2} \quad S_{3,3} \quad S_{3,4} \qquad u_{3,6} \oplus u_{3,14} \oplus p_5 \oplus p_7 \oplus p_8 = 0$$
$$K_4 \quad k_{4,2 \cdot i} \qquad \text{Guess } k_{4,2 \cdot i}$$

mac

$$k \xleftrightarrow{} \boxed{\mathsf{Gen}} \xrightarrow{} k$$
$$\text{Alice} \xrightarrow{m} \boxed{\mathsf{Enc}} \xrightarrow{c} \boxed{\mathsf{Dec}} \xrightarrow{m} \text{Bob}$$
$$m \to \boxed{\mathsf{Mac}} \xrightarrow{t} \boxed{\mathsf{Vrfy}} \xrightarrow{b}$$

macforge-exp

$$\text{Gen } k$$
$$\boxed{\mathsf{Mac}_k(\cdot)}$$
$$(m, t)$$
$$\text{Win if } \mathsf{Vrfy}_k(m, t) = 1 \wedge m \notin \mathcal{Q}$$

macwithprf

$$m$$
$$k \longrightarrow \boxed{F}$$
$$t$$

man-in-middle

$$pk_A \qquad pk_E$$
$$pk_E \qquad pk_B$$
$$c_A = \mathsf{Enc}_{pk_E}(m_A) \qquad c_B = \mathsf{Enc}_{pk_E}(m_B)$$
$$c_A \quad \mathsf{Enc}_{pk_B}(\mathsf{Dec}_{sk_E}(c_A))$$
$$\mathsf{Enc}_{pk_A}(\mathsf{Dec}_{sk_E}(c_B)) \quad c_B$$
$$m_B = \mathsf{Dec}_{pk_A}(c_B) \qquad m_A = \mathsf{Dec}_{pk_B}(c_A)$$

meet-in-middle

$$z_2$$
$$k_1' \quad z_1 \quad k_2''$$
$$x \to \boxed{F} \quad z_0 \quad k_2 \quad \boxed{F^{-1}} \leftarrow y$$
$$k_1 \quad z_3 \quad k_2'''$$

multiple-enc-exp

$\vec{M}_0, \vec{M}_1$

Gen b, k

$\vec{C} = (c^i \leftarrow \mathsf{Enc}_k(m_b^i))$

b'

Win if $b = b'$

owff

$\mathcal{D}$ $1^n \rightarrow$ Gen $\mathcal{R}$

$\mathcal{D}_I$ Samp $\rightarrow I$ $\mathcal{R}_I$

x $f_I \rightarrow$ y

owfover

PRG — HCP — OWF — PrivK — PRP — PRF — PRG

padding-oracle

CAPTCHA server

(0) shared key k

(2) $Enc_k(w)$

(3) Image(w) or error

(1) $Enc_k(w)$

(4) w

User   Web server

pgfD

$\mathcal{O} : F_k$ or f

1^n

$\mathcal{D}$ $b \leftarrow \{0,1\}$ n

$m_0, m_1 \in \{0,1\}^n$

$s' = \mathcal{O}(r), r \leftarrow \{0,1\}^n$

$c := \langle r, s' \oplus m_b \rangle$

b'

1 if $b' = b$

$\mathcal{A}$

pgfMAC

$\mathcal{O} : F_k$ or f

1^n

$\mathcal{D}$ n

$m \in \{0,1\}^n$

$t := \mathcal{O}(m)$

1 if $\hat{t}' = t'$ and new m'

$\hat{t}' = \mathcal{O}(m')$ (m', t')

$\mathcal{A}$

pnp

$\mathcal{NP}$-Hard

$\mathcal{NP}$-Complete

$\mathcal{NP}$

$\mathcal{P}$

$\mathcal{P} \neq \mathcal{NP}$

$\mathcal{NP}$-Hard

$\mathcal{NP}$-Complete $= \mathcal{NP} = \mathcal{P}$

$\mathcal{P} = \mathcal{NP}$

prg-distinguisher

choose a truly random string or generate a pseudorandom one

Distinguisher D

the string

1 or 0

pri-cpa-exp

Gen k $\mathsf{Enc}_k(\cdot)$

m_0, m_1

Gen b

$\mathsf{Enc}_k(m_b)$

b'

Win if $b = b'$

pri-eav-exp

m_0, m_1

Gen b, k

$\mathsf{Enc}_k(m_b)$

b'

Win if $b = b'$

private-key

$k \leftarrow$ Gen $\rightarrow k$

m Enc c Dec m

Alice   Bob

Adversary

public-key

$pk \leftarrow$ Gen $\rightarrow sk$

m Enc c Dec m

Alice   Bob

Adversary

qr-qnr

$\mathbb{Z}_p^*$

$\mathcal{QR}_p$ $\mathcal{QNR}_p$

$\mathbb{Z}_N^*$

$\mathcal{J}_N^{+1}$ $\mathcal{QR}_N$

$\mathcal{QNR}_N^{+1}$ $\mathcal{QNR}_N$ $\mathcal{J}_N^{-1}$

rabinOT

$N, e, m^e \bmod N$

a random x

$x^2 \bmod N$

the square root y of x^2

learn m if $y \neq \pm x$

reduction

Instance x of problem X

Reduction $\mathcal{A}'$

Instance of scheme Π

$\mathcal{A}$

"Break"

Solution to X

schnorr

a random r

$t = g^r$

a random bit $c \leftarrow \{0,1\}$

$s = r + cx$

$g^s \overset{?}{=} ty^c$

spn

Plaintext P_1 ... P_{16}

sub-key K_1 mixing
S_1 S_2 S_3 S_4
sub-key K_2 mixing
S_1 S_2 S_3 S_4
sub-key K_3 mixing
S_1 S_2 S_3 S_4
sub-key K_4 mixing

ssl

Client   Server

client random a
server random b
certificate of pk
E_{pk}(premaster secret s)
Hash of previous msgs
Hash of previous msgs
session keys from (a, b, s) session keys from (a, b, s)

synchronizedmode

G Part 1 Part 2 Part 3
K $m_1 \to \oplus \to c_1$ $m_2 \to \oplus \to c_2$ $m_3 \to \oplus \to c_3$

Synchronized Mode

K
G Part 1 G Part 2 G Part 3
IV_1 $m_1 \to \oplus \to c_1$ IV_2 $m_2 \to \oplus \to c_2$ IV_3 $m_3 \to \oplus \to c_3$

Unsynchronized Mode

tdp-cca1

r m
$pk \to f_I$ H E
c_1 c_2

tdp-cca2

r m
$pk \to f_I$ H $\oplus$ G
c_1 c_2 c_3

tdp-cpa

r m
$pk \to f_I$ H $\oplus$
c_1 c_2

tdp-pk

I
$y \in \mathcal{D}_I$
$\mathcal{A}_{\mathsf{hc}}$ $pk = I$
$m_0 \neq m_1 \in \{0, 1\}$
$b, z \leftarrow \{0, 1\}$ y, m' $\mathcal{A}$
$m' := m_b \oplus z$ b'
z if $b' = b$
$\overline{z}$ otherwise

threepass

p, e_A, d_A p, e_B, d_B
$c = [m^{e_A} \bmod p]$
$c_1 = [c^{e_B} \bmod p]$
$c_2 = [c_1^{d_A} \bmod p]$
$m = [c_2^{d_B} \bmod p]$

toy-OT

1 \$1M \$2M \$3M \$4M
2 \$1M \$2M \$3M \$4M
3 \$1M \$2M \$3M \$4M   NO NO YES NO
4 \$1M \$2M \$3M \$4M   NO

transmission

k Gen' k
m EncMac' c Dec' m
Alice   Bob
Adversary
$\perp$

trapdoor

easy
easy
x tp $f(x)$
easy
$\mathsf{hc}(x)$ hard
hard

tree-sig

$pk_\varepsilon, sk_\varepsilon$
0   1
pk_0, sk_0 pk_1, sk_1
pk_{00}, sk_{00} pk_{01}, sk_{01} pk_{10}, sk_{10} pk_{11}, sk_{11}
pk_{000} pk_{001} pk_{010} pk_{011} pk_{100} pk_{101} pk_{110} pk_{111}
sk_{000} sk_{001} sk_{010} sk_{011} sk_{100} sk_{101} sk_{110} sk_{111}
$m = 011$

worldofpk

Private-Key Encryption   Message Authentication Codes
Pseudorandom Functions
Block Ciphers   Pseudorandom Generators
One-Way Function
RSA, Discrete Log, Factoring

zkp-commitment

Prover knows sk a random m
$m' = \mathsf{Dec}_{sk}(c)$ c $c \leftarrow \mathsf{Enc}_{pk}(m)$
$h = \mathsf{commit}(m')$ h
m
$m \stackrel{?}{=} m'$
If No, stop;
m' Accept if $m = m'$

zkp-hanmilton

1	2	3	4
3	1	4	2

	2	3	4
1	1	1	0
2		1	1
3			1

	2	3	4
1	1	1	
2			1
3			1

(1) The Graph   (2) A Relabeled Graph   (3) Commited Boxes   (4) Opened Boxes

zkp-rsa

random $k, s > 3$
$ks \equiv e \pmod{N}$
random c
$m = c^d$
$x = m^k$
$x^s \stackrel{?}{=} c$