1outof2

RSA: N, e

random x_0, x_1

random b, k

$v = x_b + k^e$

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

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

$m_b = m'_b - k$

3parties-DHKE

C

(1) g^c

(2) g^{bc}

(1) g^a

(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

$0^n \rightarrow \oplus$

F_k F_k F_k

t

CBC-small

m_1 m_2 m_3

$IV \rightarrow \oplus$

F_k F_k F_k

IV

c_1 c_2 c_3

CBC

m_1 m_2 m_3

$IV \rightarrow \oplus$

F_k F_k F_k

IV

c_1 c_2 c_3

CCA-PKCS

pk sk

$[c' = (2^r)^e \cdot c]$

$[\text{Yes/No: } MSB(m') = \text{'}1\text{'}]$

Client Server

CCA

k_1, k_2 Gen' k_1, k_2

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

Alice Bob

Adversary $\perp$

CMAC

m_1 m_2 m_3

$0^n \rightarrow \oplus$ $\oplus$ $\oplus \leftarrow k_1$ or k_2

F_k F_k F_k

t

CTR

ctr $\text{ctr} + 1$ $\text{ctr} + 2$ $\text{ctr} + 3$

F_k F_k F_k

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

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

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

$x \leftarrow \mathbb{Z}_q$

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

$y \leftarrow \mathbb{Z}_q$

h_2 $\quad h_2 := g^y$

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

Davies-Meyer

m_i

$h_{i-1} \rightarrow F \rightarrow \oplus \rightarrow h_i$

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

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

m_1, m_2

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

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

1 if $b' = b$ $\quad b'$

HMAC

$k \oplus ipad$ $\boxed{m_1}$ $\cdots$ $|m|$ IV $k \oplus opad$

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

KDC

KDC

I want to talk to Bob

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

Let's talk, $E_{Bob}(k)$

Alice   Bob

MDtransform

| x_1 | x_2 | $\cdots$ | x_B | L |

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

MS-PPTP

k $\qquad$ k

$[m_1\|m_2\|m_3] \oplus PRG(k) \longrightarrow$

$\longleftarrow [s_1\|s_2\|s_3] \oplus PRG(k)$

Client   Server

Miyaguchi-Preneel

h_{i-1}

$m \rightarrow F \oplus \rightarrow h_i$

NMAC

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

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

OAEP-plus

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

$\oplus \quad G$

$H \quad \oplus$

| $\hat{m}_1$ | $\hat{m}$ |

OAEP

| m | $00\cdots0$ | r |

$\oplus \quad G$

$H \quad \oplus$

| $\hat{m}_1$ | $\hat{m}$ |

OFB

IV

$F_k \quad F_k \quad F_k$

$m_1 \rightarrow \oplus \quad m_2 \rightarrow \oplus \quad m_3 \rightarrow \oplus$

$IV \quad c_1 \quad c_2 \quad c_3$

OWF

easy

$x \qquad f(x)$

hard

SAEP-plus

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

$\oplus \quad H$

| $\hat{m}_1$ | $\hat{m}$ |

SIV-CTR

$SIV \quad SIV+1 \quad SIV+2 \quad SIV+3$

$F_{k_1} \quad F_{k_2} \quad F_{k_2} \quad F_{k_2}$

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

$t := SIV \quad c_1 \quad c_2 \quad c_3$

TDES

$k_1 \quad k_2 \quad k_3$

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

VCBC-MAC

$|m| \quad m_1 \quad m_2 \quad m_3$

$F_k \quad \oplus \quad F_k \quad \oplus \quad F_k \quad \oplus \quad F_k$

$\rightarrow t$

attack-spn

K_1

$S_{1,1} \quad S_{1,2} \quad S_{1,3} \quad S_{1,4}$

K_2

$S_{2,1} \quad S_{2,2} \quad S_{2,3} \quad S_{2,4}$

● 20 bits known
● 20 bits unknown
● 4 bits compared

authentication

$k \leftarrow$ Gen $\rightarrow k$

Enc $\cdots$ Dec $\rightarrow m'$

Alice   Bob

Adversary

c'

baby-giant

$g^{k \cdot t}$

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

$y \quad y \cdot g^t \quad y \cdot g^t$

birthdayattack

x_0 I J i $2i$

blindsignature

Signer
$pk = e,\ sk = d$
$m' \equiv mr^e$
$s \equiv m'^d$
$s \equiv s'r^{-1}$
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

Charlie
Certificate Authority (CA)
Alice trusts Charlie and knows pk_C.
Bob trusts Charlie.
Charlie trusts Bob.
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

$b \leftarrow \{H, T\}$
a random r
$m = b\|r$
$h = \mathsf{Hash}(m)$
$b' \in \{H, T\}$
m
$h \overset{?}{=} \mathsf{Hash}(m)$
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
$\oplus$
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
$x \to \oplus \to F \to \oplus \to y$

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
$S_{2,1}$ $S_{2,2}$ $S_{2,3}$ $S_{2,4}$ $S_{2,2}: \Delta X = 4 \to \Delta Y = 5$
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 Gen pk
Alice
m Enc c Dec m
m Sign σ Vrfy b Bob

dining

①

k_1 k_2

$x \rightarrow F \rightarrow F \rightarrow y$

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

y m

g^y h^y $\cdot$

c_1 c_2

P_3
P_4
P_2
P_1
$y^2 = x^3 - x + 1$
$-P_3$

r

$k \rightarrow F$

Pad

$m \rightarrow \oplus \rightarrow c$

k

G

Pad

$m \rightarrow \oplus \rightarrow c$

L_0 | R_0
F_{k_1}
F_{k_2}
F_{k_3}
F_{k_4}
L_4 | R_4

L_0 | R_0
f_1
f_2
f_3
f_4
L_4 | R_4

L_0 | R_0
f_1
L_1 | R_1
f_2
L_2 | R_2

L_0 | R_0
f_1
L_1 | R_1
f_2
L_2 | R_2
f_3
L_4 | R_3

Gen $\rightarrow s$

m H h

easy

x $f(x)$

easy hard

$hc(x)$

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 $\exists i$

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

pk

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

$\hat{m}_i := H^s(m_i)$ m_i

σ_i on $\hat{m}_i$ σ_i $\mathcal{A}'$

$(H^s(m), \sigma)$ (m, σ)

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

(by security of Π) (by security of Π)

$\langle pk, \mathsf{Enc}_{pk}(0^n), \mathsf{Enc}'_k(m_0) \rangle$ $\xleftarrow{\text{(by security of } \Pi')}$ $\langle pk, \mathsf{Enc}_{pk}(0^n), \mathsf{Enc}'_k(m_1) \rangle$

k m

$pk \rightarrow \mathsf{Enc}_{pk}$ Enc'_k

c_1 c_2

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

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

Alice ; m ; Enc ; c ; Gen ; k ; k ; Dec ; c' ; m' ; Bob ; Adversary

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

K ; X ; Y ; X ; Y ; X ; Y

$F : K \times X \to Y$
2D function

$F_k(x) \stackrel{\text{def}}{=} F(k, x)$
Keyed function

$f : X \to Y$
Look-up table

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

Alice ; m ; Enc ; c ; Gen ; k ; k ; Dec ; m ; Bob ; m ; m ; b ; Mac ; t ; Vrfy ; m

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

m ; k ; F ; t

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

x ; F ; z_2 ; z_1 ; z_0 ; z_3 ; k_1' ; k_1 ; k_2'' ; k_2 ; k_2''' ; F^{-1} ; y

$\vec{M}_0, \vec{M}_1$; Gen b, k ; $\vec{C} = (c^i \leftarrow \mathsf{Enc}_k(m_b^i))$; b' ; Win if $b = b'$

$\mathcal{D}$; 1^n ; Gen ; $\mathcal{R}$; $\mathcal{D}_I$; Samp ; I ; $\mathcal{R}_I$; x ; f_I ; y

PRG ; HCP ; PRF ; OWF ; PRP ; PrivK

CAPTCHA Server ; (2) $Enc_k(w)$; (3) Image of w or error ; (0) shared key k ; (1) $Enc_k(w)$; (4) w ; User ; Web Server

$\mathcal{O} : F_k$ or f ; 1^n ; $\mathcal{D}$; $b \leftarrow \{0, 1\}$; n ; $m_0, m_1 \in \{0, 1\}^n$; $s' = \mathcal{O}(r), r \leftarrow \{0, 1\}^n$; $c := \langle r, s' \oplus m_b \rangle$; $\mathcal{A}$; 1 if $b' = b$; b'

pgfMAC

$\mathcal{O} : F_k$ or f

1^n

$\mathcal{D}$

n

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

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

$\mathcal{A}$

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

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

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

$\text{Enc}_k(\cdot)$

m_0, m_1

Gen b

$\text{Enc}_k(m_b)$

b'

Win if $b = b'$

pri-eav-exp

m_0, m_1

Gen b, k

$\text{Enc}_k(m_b)$

b'

Win if $b = b'$

private-key

k — Gen — k

m — Enc — c — Dec — m

Alice

Adversary

Bob

public-key

pk — Gen — sk

m — Enc — c — Dec — m

Alice

Adversary

Bob

qr-qnr

$\mathbb{Z}_p^*$

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

$\mathbb{Z}_N^*$

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

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

$\mathcal{QNR}_N$

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

rabinOT

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

a random x

$x^2 \bmod N$

the square root y of x^2

$y \stackrel{?}{=} \pm x$

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 $c \leftarrow \{0,1\}$

$s = r + cx$

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

spn

P_1 **Plaintext** 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

$E_{pk}(\text{premaster secret } s)$

Hash of previous msgs

Hash of previous msgs

session keys from (a, b, s) session keys from (a, b, s)

synchronizedmode

G

K

Part 1 | Part 2 | Part 3

$m_1 \oplus c_1$ $m_2 \oplus c_2$ $m_3 \oplus c_3$

Synchronized Mode

K

G — Part 1 — G — Part 2 — G — Part 3

IV_1 $m_1 \oplus c_1$ IV_2 $m_2 \oplus c_2$ IV_3 $m_3 \oplus c_3$

Unsynchronized Mode

tdp-cca1

r

m

pk — f_I — H — E

c_1

c_2

tdp-cca2

r

m

pk — f_I — H — $\oplus$ — G

c_1

c_2 c_3

tdp-cpa

tdp-pk

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

threepass

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

transmission

Alice $\quad$ Adversary $\quad$ Bob

trapdoor

tree-sig

$m = 011$

worldofpk

Private-Key Encryption $\qquad$ Message Authentication Codes

Pseudorandom Functions

Block Ciphers $\qquad$ Pseudorandom Generators

One-Way Function

RSA, Discrete Log, Factoring

zkp-rsa

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

zkp