ElGamal Encryption (1982)

PKE from D-H.

Ingredients: G: FCG of order q w/gen $g \in G$.

(E_s, D_s): sym. cipher over (K, M, C)

$H: G^2 \to K$: hash fn.

Scheme:

Gen: $\alpha \xleftarrow{R} \mathbb{Z}_q$, $h := g^\alpha$, $[sk := \alpha,\ pk := h \in G]$

$E(pk, m)$: $\beta \xleftarrow{R} \mathbb{Z}_q$, $u := g^\beta$, $v := h^\beta = g^{\alpha\beta}$

(pk = $h \in G$)

$K := H(u, v) \in K$ ← derived from D-H secret v

$c := E_s(k, m)$

output (u, c)

$D(sk, (u, c))$: (sk = α)

$v = u^\alpha = g^{\alpha\beta}$

$k = H(u, v) \in K$

$m = D_s(k, c)$

output m

Performance: enc: 2 exp in G

1 sym enc

dec: 1 exp in G

1 sym dec

As a standard: ECIES (ell. curve. enc. system)

Security.

Thm. 1. (Gen, E, D) is semsec (eavesdropping)

assuming (1) CDH holds in (G, g)

(2) (E_s, D_s) is semsec

(3) H is a secure key derivation fn (preserves entropy in v)

Thm. 2. (Gen, E, D) is CCA secure.

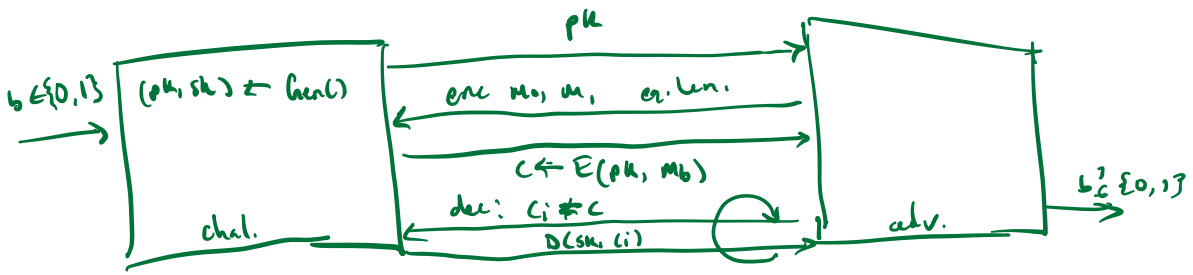
↑ tampering

assuming (1) Interactive D-H assumption holds (stronger than CDH)

(2) (E_s, D_s) provides $A_0 E$.

(3) H is a "random oracle" (ideal hash fn)

CCA security



Trapdoor functions (TDF)

Def. Tuple of eff. algs (Gen, F, F^{-1})

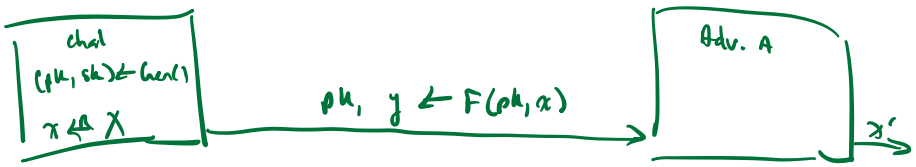
Gen: rand. alg outputs key pair (pk, sk)

$F(pk, \cdot)$ det. alg that defines an fn $X \to Y$

$F^{-1}(sk, \cdot)$ defines a fn $Y \to X$ that inverts $F(pk, \cdot)$

$\forall (pk, sk)$ def by Gen, $\forall x \in X$: $F^{-1}(sk, F(pk, x)) = x$

Security. (Gen, F, F^{-1}) is secure if it is a one-way fn:
can be evaluated, but not inverted w/o sk



Def. $Gen(F, F^{-1})$ is secure if for all eff. A:

$$Adv_{OW}[A, F] = Pr[x = x'] < \text{negligible}.$$

PKE from TDF.

$\ell(Gen, F, F^{-1})$: secure TDF $X \to Y$

(E_s, D_s) sym. auth. enc. over (K, M, C)

H: $X \to K$ hash fn

$\Rightarrow (Gen, E, D)$:

Gen: same as TDF Gen

$E(pk, m)$: $x \xleftarrow{R} X$, $y \leftarrow F(pk, x)$
$k \leftarrow H(x)$, $c \leftarrow E_s(k, m)$
output (y, c)

$D(sk, (y, c))$

$x \leftarrow F^{-1}(sk, y)$

$k \leftarrow H(x)$, $m \leftarrow D_s(k, c)$

output m

Thm. If (Gen, F, F^{-1}) is a secure TDF, (E_s, D_s) provides AE, $H: X \to K$ is a random oracle, then it is CCA-secure.

RSA

Trapdoor permutation

Let $N = pq$ where p, q prime

$Gen()$: choose random distinct primes $p, q \approx 1024$ bits

set $N = pq$

choose ints e, d s.t. $ed = 1 \pmod{\varphi(N)}$

output $pk = (N, e)$, $sk = (N, d)$

$F: Z_N^* \to Z_N^*$; $RSA(x) = x^e$ in Z_N

$F^{-1}(sk, y) = y^d$; $y^d = RSA(x)^d = x^{ed} = x^{k\varphi(N)+1} = (x^{\varphi(N)})^k x = x$

RSA$_c$ Assumption

RSA w/exp e is a one-way permutation

for all eff. algs A:

$$Pr[A(N, e, y) = y^{1/e}] < \text{negligible}$$

where $p, q \xleftarrow{R}$ n-bit primes, $N \leftarrow pq$, $y \xleftarrow{R} Z_N^*$

PKE

(E_s, D_s): sym. enc. scheme providing AE

$H: \mathbb{Z}_n \to K$ where K is key space of (E_s, D_s)

Gen(): generate RSA params $pk = (N, e)$, $sk = (N, d)$

$E(pk, m)$: 1. choose random x in $\mathbb{Z}_n^*$

2. $y \leftarrow RSA(x) = x^e$, $k \leftarrow H(x)$

3. output $(y, E_s(k, m))$

$D(sk, (y, c))$: output $D_s(H(RSA^{-1}(y)), c)$