Cryptography

Organization:

09. Oct. cancelled
11. Oct. (14:00-17:00) replacement
23. Oct. cancelled

2. Provable Security

One-time pad:

- not practical
- information-theoretically secure
  $\rightarrow$ too strong
- illustrative

Practical cryptosystems

- computationally secure

2.1 Formalization of Encryption

2.1.1 Syntax

Definition:
A symmetric-key cryptosystem Σ consists of 3 algorithms (SKE):
- KeyGen() $\rightarrow$ k , randomized, k $\in$ K
- Enc(k,m) $\rightarrow$ c , m $\in$ M, c $\in$ C (might be randomized)
- Dec(k,c) $\rightarrow$ m , deterministic

Σ = (Σ.KeyGen, Σ.Enc, Σ.Dec, Σ.K, ...)

2.1.2 Correctness

Definition:
A cryptosystem Σ is correct if $\forall$k $\in$ K, $\forall$m $\in$ M:

$$P[Dec(k, Enc(k, m)) = m] = 1$$

Example:
Enc(k, m) $\rightarrow$ m
Dec(k, c) $\rightarrow$ c
$\Rightarrow$ correct but totally insecure

2.1.3 Terminology in distributed systems:

Liveness : correctness

"something good eventually happens"

Safety : security

"nothing bad has happened"

2.1.4 Security

Eavesdrop()-experiment from One-time pad (OTP)
- too specific to OTP

Candidate sec.def. A (attempt 2)

Σ is secure if $\forall$ m $\in$ M, the output of Eavesdrop(m) is a random variable with uniform distribution over C:

Eavesdrop(m $\in$ M):
k $\leftarrow$ KeyGen()
c $\leftarrow$ Enc(k,m)
return c

Candidate sec.def. B (attempt 3)

Σ is secure if $\forall$ m $\in$ M, the following functions produce the same random variable:

"real" Eavesdrop(m $\in$ M):
k $\leftarrow$ KeyGen()
c $\leftarrow$ Enc(k,m)
return c

"ideal/fake" Eavesdrop(m $\in$ M):
c $\leftarrow$ C
return c

Definition B used indistinguishability of distributions
Move towards a definition with an adversary A (distinguishing algorithm)

$$P[A \ \textit{with B-left} \ \to 1] = P[A \ \textit{with B-right} \ \to 1]$$
$$A \ \textit{outputs} \ b \in \{0, 1\}$$

Candidate sec.def. C (attempt 4)

Σ is secure if $\forall$ alg. A, running A With the left or right experiment of Attempt-B outputs 1 is the same.

How secure/useful is this?
K = M = $\{0, 1\}^\lambda$
Enc(k,m) $\to$ m $\oplus$ k || m $\oplus$ k
Dec(k,c) $\to$ c_1 || c_2 = c, return $c_1 \oplus$ k

That example shows that Attempt-C was too strong!

Candidate sec.def. D (attempt 4)

Σ is secure if $\forall$ alg. A and $\forall m_L, m_R \in$ M running with left or right implementation of Eavesdrop, A outputs 1 with equal probability.

Eavesdrop(m_L, m_R)
k $\leftarrow$ KeyGen()
c $\leftarrow$ Enc(k, m_L)
return c

Eavesdrop(m_L, m_R)
k $\leftarrow$ KeyGen()
c $\leftarrow$ Enc(k, m_R)
return c

$\rightsquigarrow$ ***chosen-plaintext attack***

2.2 Defining provable security

Definition:
A Library L is a collection of functions and static (private) variables.
The interface are its functions and their arguments and types.

Definition:
Running a program P with Library L is denoted P $\Diamond$L ("P linked to L").

$$P \to 1$$
$$P \Diamond L \to 1$$

L
s $\leftarrow \{0,1\}^\lambda$
Guess(x):
return x $\stackrel{?}{=}$ s

A:
repeat
x $\leftarrow \{0,1\}^\lambda$
until Guess(x) = True
return x
P[A$\Diamond$L $\rightarrow$ z] $\stackrel{?}{=} 2^{-\lambda}$ for any z $\in \{0,1\}^\lambda$

B:
c $\leftarrow \{0,1\}^\lambda$
return Guess(x)
P[B$\Diamond$L $\rightarrow$ True] $= 2^{-\lambda}$

2.2.1 Two Libraries with same VO behaviour

Definition:
Two Libraries L_L and L_R are exchangeable written:

$$L_L \equiv L_R,$$

if for all distinguishable alg. A:

$$P[A\Diamond L_L \rightarrow 1] = P[A\Diamond L_R \rightarrow 1]$$

Important:
- A interacts with L only via the interface
- No side-channels

2.2.2 Two Libraries $L_{eager} \equiv L_{lazy}$

L_{eager}
for x $\in$ X do
T[x] $\leftarrow \{0,1\}^\lambda$

Get(x)
return T[x]

L_{lazy}
T[$\bullet$] = $\perp$

Get(x)
if T[x] = $\perp$ then
T[x] $\leftarrow \{0,1\}^\lambda$
return T[x]

2.2.3 Security definition using libraries

Definition:
An encription-scheme Σ has uniform ciphertexts if:

$$L_{ots\$-real} \equiv L_{ots\$-rand}$$

$L_{ots\$-real}$
CT × T (m)
k ← KeyGen()
c ← Enc(k,m)
return c

$L_{ots\$-rand}$
CT × T (m)
c ← C
return c

Definition:
An encription-scheme Σ has one-time secrecy if:

$$L_{ots-left} \equiv L_{ots-right}$$

$L_{ots-left}$
Eavesdrop(m_L, m_R)
k ← KeyGen()
c ← Enc(k, m_L)
return c

$L_{ots-right}$
Eavesdrop(m_L, m_R)
k ← KeyGen()
c ← Enc(k, m_R)
return c