COM S 6830 - Cryptography October 16, 2009

Lecture 14: Trapdoor permutations and Zero-knowledge introduction

Instructor: Rafael Pass *Scribe: Srivatsan Ravi*

1 Public key encryption-Review

Definition 1. (Public key encryption scheme) *{Gen,Enc,Dec} is a public key encryption scheme if the following hold*

1. *Gen is a PPT algorithm : pk,sk* $\leftarrow$ *Gen*(1^k)
2. *Enc is a PPT algorithm :* $c \leftarrow Enc_{\mathrm{pk}}(m)$
3. *Dec is a PPT algorithm :* $m \leftarrow Dec_{\mathrm{sk}}(c)$
4. $\forall m \in \{0,1\}^*$, $Pr[pk,sk \leftarrow Gen(1^{|m|}: Dec_{\mathrm{sk}}(Enc_{\mathrm{pk}}(m))=m]=1$

Definition 2. (Secure Public key encryption scheme) *{Gen,Enc,Dec} is said to be single message secure if* $\forall$ *non-uniform PPT machines D, there exists a negligible function* ε *such that* $\forall n \in \mathbb{N}$ *and* $m_0, m_1 \in \{0,1\}^n$, *D distinguishes the following distributions with probability* $\leqslant \varepsilon(n)$

$\{pk,sk \leftarrow Gen(1^n):(pk,Enc_{\mathrm{pk}}(m_0))\}$

$\{pk,sk \leftarrow Gen(1^n):(pk,Enc_{\mathrm{pk}}(m_0))\}$

The definitions of CPA/CCA1/CCA2 security can extended to public key cryptosystems
If an encryption scheme is single-message secure, then it is also multi-message secure
An encryption scheme with a deterministic algorithm (even with state) would not be secure because an adversary can simply encrypt the message m_0 with pk and compare the encryption of m_0 with the challenge ciphertext (which is the encryption of either m_0 or m_1).

2 RSA Example

Definition 3. *(RSA Collection) Define the RSA cryptosystem as follows*

1. *G*(1^k) *corresponds to the following algorithm: (p,q)* $\in$ *PRIMES and are k-bits each. Let* $n=pq$, $e \leftarrow \mathbb{Z}^*_{\varphi(n)}$, $d=e^{-1} \bmod \varphi(n)$,$M_k = \mathbb{Z}^*_n$. $pk=(n,e),sk=(d,n)$
   $\varphi(n)$ *is Euler's Totient function defined as the number of positive integers less than n that are coprime to n*
2. $c=E_{\mathrm{pk}}(m)=m^e \bmod n$
3. $D_{\mathrm{sk}}(c)=c^d \bmod n$

2.1 What is RSA?

Consider the scenario if factoring was easy i.e (p,q) can be easily obtained and knowing that φ(n)=(p-1)(q-1) when n=pq, inverting the RSA function becomes easy.Assuming factoring is hard,the RSA function is one-way. We can generalize this as RSA belonging to a collection of one-way permutations with the additional property that the inverse is easy to obtain with the knowledge of this function(a trapdoor) which allows its possesor to efficiently invert it at any point in the domain of its choosing.

2.2 RSA assumption

Definition 4. *Let* $n=pq$; $(p,q) \in$ *PRIMES and* $|p|=|q|=k$. *Then for every PPT machine A and negligible function* ε, $Pr[A(n,e,RSA_{n,e}(x))=x] < \epsilon(k)$

Under the RSA assumption,the RSA family of trapdoor permutations forms a secure public key encryption scheme with security parameter $\mathbb{k}$ since inverting Enc is hard for an adversary that knows the public key,but not the secret key.

3 Trapdoor functions and collections

A collection of one-way permutations with the additional property that the inverse is easy to obtain with some special information is called a collection of trapdoor permutations.

Definition 5. *A collection of trapdoor permutations is a set* $F=\{f_i : D_i \rightarrow D_i\}_{i\epsilon I}$ *where I is a set of finite indices and* f_i *is a permutation* $\forall i \epsilon I$ *s.t*

1. *(Easy to sample function) : There exists a PPT Gen which on input* 1^n *outputs* (i,t_i) *where* t_i *is the trapdoor of i*
2. *(Easy to sample domain) : There exists a PPT which on input* $i \epsilon I$ *outputs* $x \epsilon D_i$
3. *(Easy to evaluate function) : There exists a PPT A which on inputs* $i \epsilon I$ *and* $x \epsilon D_i$, *computes* $A(i,x)=f_i(x)$
4. *(Hard to invert) : For every PPT A and large enough k,* $\exists$ *negligible function* ε *s.t*
$$Pr[\, f_i(z)=y : i \leftarrow I : x \leftarrow D_i : y \leftarrow f_i(x) \; ; \; z \leftarrow A(i,y)] \leqslant \varepsilon(k)$$
5. *(Easy to invert when trapdoor is known) : There exists a PPT B s.t* $B(i,t_i,f_i(x))=x$

It is easy to see that RSA defines a collection trapdoor permutations with index set (n,e);t being (n,d) over the domain $\mathbb{Z}_n^*$ s.t ed=1modφ(n)

Lemma 6. *(Trapdoor predicate)For the RSA scheme,there exists a PPT algorithm A and a negligible function* ε *such that*
$Pr[A(n,e,x^e mod\ n)=LSB(x^e mod\ n)] \leqslant 1/2 + \varepsilon(k)$
i.e given $n,e,x^e mod\ n$ *; it is hard to guess the hardcore bit with non-negligibly larger probability than 1/2*

Definition 7. *Pick a random* $X \epsilon \{0,1\}^n$ *and* $b \epsilon \{0,1\}$.
Then $\{Gen,Enc'=\{X^e mod\ n, b \oplus P(X)\}, Dec'=\{c \oplus P(c^d mod\ n)\}\}$ *is single bit secure encryption scheme where P is the trapdoor predicate for RSA(The LSB bit)*

Proof outline:

Assume this encryption scheme is not secure.Then for some PPT algorithm A and a negligible function ε, P the trapdoor predicate for RSA ,
$\Pr_{b\epsilon\{0,1\}}[A(Enc_{pk}(x),b \oplus P(x),pk)=b] > 1/2 + \varepsilon(n)$
Consider the algorithm $A'(y,pk)$ which for random $c \epsilon \{0,1\}$ returns $c \oplus A(y,c,pk)$
$\Pr[A'(Enc_{pk}(x),pk)=P(x,pk)]$
$=\Pr[A(Enc_{pk}(x),c,pk)=c \oplus P(x,pk)]$
$=\Pr_{b\epsilon\{0,1\}}[A(Enc_{pk}(x),b \oplus P(x,pk),pk)=b] > 1/2 + \varepsilon(n)$
which is a contradiction
$\Rightarrow$ The encryption scheme must be secure

4 Zero knowledge

4.1 Introduction

Goal of this topic is to redefine encryption schemes using knowledge based approaches
What is knowledge?It is a behavioral approach,knowing is the ability to perform a task

Definition 8. *Zero knowledge(Informal): Consider a Prover who knows the proof for a problem P and a Verifier who needs to be convinced of the proof. A ZK proof convinces the Verifier of the existence of the proof, but does not reveal any new information about the proof*

Consider the following example: A Journalist wants to know more information about a murder that was commited. All the Police reveal is that someone has been murdered when the journalist queries the Police. Thus, no new information has been revealed to the journalist, but the Police has confirmed that a murder has occured.

A variant of the same would be when a journalist calls up the Police to query about the murder. The police flips a fair coin and hangs up or says 'someone has been murdered' with equal probability. Again, the journalist has obtained no new information that he himself could not have inferred by flipping a coin

Axiom 9. *Knowledge assumptions:*
1. *Randomness is free*
2. *Polytime computation is free*

Definition 10. *(ZK encryption){Gen,Enc,Dec} is said to be (comp)ZK encryption if* $\exists$ *PPT simulator S and* $\forall$ *nuPPT's D, there exists a negligible function* ε *s.t D distinguishes* $\{Enc_k(m) : k \leftarrow Gen(1^n)\}$ *and* $S(1^n)$ *with utmost* $\varepsilon(n)$ *probability*

Theorem 11. *(equivalence of secure and ZK encryption) {Gen,Enc,Dec} is a secure encryption scheme iff it is a ZK encryption as well*