CS.202: Intro to Cryptography Friday, 11/18/2016

Homework 5

Due Wednesday, 11/30/2016, at the beginning of the class

1 Combining Encryption and Authentication

Recall section 4.5 in [KL], on obtaining privacy and message authentication at the same time, and the three basic methods of combining CPA-secure encryption and MACs.

1. Can the encrypt-and-authenticate method result in secure *authenticated encryption* if the MAC scheme has unique tags? (*Hint: Think of the properties of the encryption...*)
2. Show that a CCA-secure symmetric-key encryption does not have to be an authenticated encryption. *Hint: What you need is that the adversary can create some valid ciphertexts without endangering the CCA security of the encryption...*

2 PKE with Multiple Keys

Assume $\Pi = (KG, Enc, Dec)$ is a CPA secure PKE and let $\Pi' = (KG', Enc', Dec')$ be a "multiple-key version" of Π in the following sense: $KG'(1^\tau)$ runs $KG(1^\tau)$ n times, collects the generated public keys as $pk' = (pk_1, ..., pk_n)$ and the corresponding private keys as $sk' = (sk_1, ..., sk_n)$. Then $Enc'((pk_1, ..., pk_n), m) = (Enc(pk_1, m), ..., Enc(pk_n, m))$ while $Dec'((sk_1, ..., sk_n), (c_1, ..., c_n))$ output $Dec(sk_i, c_i)$ for any i (doesn't matter which).

Is Π' CPA PKE if Π is CPA PKE? Argue why or why not.

What real-world situation is modeled by (KG, Enc, Dec)?

3 TDF with Multiple Keys

Assume $\Pi = (Gen, Samp, Eval, Inv)$ is a TDF family which is "domain uniform" in the sense that for every τ there exists D_τ s.t. for every (I, td) generated by $Gen(\tau)$ the domain of function f_I is D_τ. In other words, all TDF's f_I generated for some security parameter τ share the same domain D_τ. Consider the following construction of a "multi-key version" of this TDF, denoted $\Pi' = (Gen', Samp', Eval', Inv')$: $Gen'(1^\tau)$ runs $Gen(1^\tau)$ n times, generating (I_1, td_1),...,(I_n, td_n), and outputs $I' = (I_1, ..., I_n)$ and $td' = (td_1, ..., td_n)$. Let $f'_{(I_1,...,I_n)}$ be defined on the same domain D_τ as $f'_{(I_1,...,I_n)}(x) = (f_{I_1}(x), ..., f_{I_n}(x))$. Clearly, algorithm $Eval'$ can run $Eval$ on (I_i, x) for $i = 1, ..., n$ to compute $f'_{(I_1,...,I_n)}$, and Inv' can invert f' using just one computation of Inv, for any td_i in td'.

Show that Π' is not a TDF given any TDF Π by instantiating Π with an RSA TDP, slightly modified to assure "domain uniformity". In other words, assume that the domain of each RSA TDF generated on security parameter τ is $D_\tau = \{0, 1\}^{p(\tau)-1}$ for some fixed polynomial p.[1] Look at the various attacks on the "textbook RSA" encryption in [KL,

[1]In the case of RSA TDP (for some fixed e) the domain of $F((N, e), \cdot)$ for each N generated by RSA TDP generator Gen_e on security parameter τ is Z_N^* where N is an RSA composite of bitlenght $p(\tau)$. Therefore

section 10.4], and recall that "textbook RSA" is exactly the RSA TDF (mis)used as a public key encryption. One of the attacks gives an answer to this question...

3.1 Bonus Question

If someone tried to prove the opposite, i.e. that Π' is a TDF for any domain-uniform TDF Π, and if they tried to use a hybrid argument, where exactly would this argument break? (It must break at some point because the statement is not true.)

4 Trapdoor Functions and Public Key Encryption

Assume that (G, F, F^{-1}) is a TDF s.t. for all security parameters τ, for all (pk, td) generated by $G(\tau)$, $F(pk, \cdot)$ is a function from $\{0,1\}^\tau$ to $\{0,1\}^\tau$. Consider the following attempts at creating a PKE (G, E, D) on message space $\{0,1\}^\tau$, where the key generation algorithm G is the generation algorithm of the TDF, except that the trapdoor output td will now be called a secret key $sk = td$. In each case state whether the PKE scheme is CPA secure given any TDF (G, F, F^{-1}), and explain why or why not.

(a) $E(pk, m) = F(pk, m)$

(b) $E(pk, m) = (r, F(pk, r) \oplus m)$ for r random in $\{0,1\}^\tau$.

(c) $E(pk, m) = (F(pk, r), r \oplus m)$ for r random in $\{0,1\}^\tau$.

(d) $E(pk, m) = (F(pk, r), H(r) \oplus m)$ for r random in $\{0,1\}^\tau$, where H is a Random Oracle hash onto $\{0,1\}^\tau$.

if N_1 and N_2 are output by two runs of $Gen_e(1^\tau)$ we have that $|N_1| = |N_2| = p(\tau)$, but $Z^*_{N_1}$ and $Z^*_{N_2}$ are two different groups, so this TDF doesn't exactly fit the restriction that all F's generated on the same security parameter must share the same domain. However, we can easily restrict each of these RSA TDF to $D_\tau = \{0,1\}^{p(\tau)-1}$, i.e. all integers between 0 and $2^{p(\tau)-1}$. Note that $D_\tau \subseteq Z^*_N$ for each N generated by $Gen_e(1^\tau)$ (except for elements which are not co-prime with N, but if anyone finds these then they can factor n so we can ignore them). The reason why one can restrict each RSA TDF to just D_τ is that for each N generated by $Gen_e(1^\tau)$ we have that $|D_\tau| > \frac{1}{2} \cdot |Z^*_N|$, i.e. D_τ is a very significant subset of Z^*_N, and therefore if a function is One-Way on domain Z^*_N then it must also be One-Way on the D_τ subset of its domain.