CS.202: Intro to Cryptography Thursday, 12/1/2016

Take-Home Final

Due Monday, 12/12/2016, noon

1 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 functions f_I generated for some security parameter τ will 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 $f'_{(I_1,...,I_n)}(x) = (f_{I_1}(x), ..., f_{I_n}(x))$. Algorithm $Eval'$ runs $Eval$ 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], 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...

1.1 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.)

2 Trapdoor Functions and Public Key Encryption

Assume that (G, F, F^{-1}) define a TDP s.t. for all security parameters τ, for all (I, td) generated by $G(\tau)$, $F(I, \cdot)$ is a one-way permutation on $\{0,1\}^\tau$, and $F^{-1}(td, \cdot)$ is its inverse which is easy to compute given td. Consider the following attempts at creating a PKE (G, E, D) on message space $\{0,1\}^\tau$, where the key generation algorithm is the generation G algorithm of the TDP, with I playing the role of the public key pk and trapdoor td playing

[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 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.

the role of the secret key sk, i.e. $(pk, sk) = (I, td)$. In each case state whether the PKE scheme is CPA secure given any TDP (G, F, F^{-1}) defined as above, and prove 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 $\{0,1\}^{\tau}$.

3 Is Merkle-Damgard Transform One-Way if the Compression Function is One-Way?

Consider the *Bare* Merkle-Damgard Transform for fixed-size messages of size $B * n$ given a compression function $h : \{0,1\}^{2n} \to \{0,1\}^n$. If we fix the block size of input to B and we fix the IV block, we can denote the bare Merkle-Damgard transform as $H^h_{B,IV}$ which is a function from $\{0,1\}^{B \cdot n} \to \{0,1\}^n$ where $H^h_{B,IV}(x) = z_B$ where $z_0 = IV$, $z_i = h(z_{i-1}|x_i)$ for $i = 1, ..., B$, and x_i is the i-th segment of n bits in x.
We know that if h is collision resistant then $H^h_{B,IV}$ is collision resistant for every (B, IV). But is it also true that if h is a One-Way Function on domain $\{0,1\}^{2n}$ then H is a One-Way Function on domain $\{0,1\}^{Bn}$?
Argue whether the answer is true or false in the usual fashion, i.e. either prove this is true for every h, B, IV satisfying the above constraints, or show that there can exist OWF h s.t. $H^h_{B,IV}$ is not a OWF for some B, IV.
(Hint: Think first about the case $B = 1$, and think about the requirement on the distribution of inputs to h which is considered in the notion that it is a OWF versus the requirement on the distribution of inputs to $H^h_{B,IV}$ which is considered in the notion that it is a OWF.)

4 Public Key Encryption (PKE) for Long Messages

Let G^l be a PRG which stretches a (random) n-bit string to a (pseudorandom) string of length l, for any l polynomial in n. Let E be a public-key encryption which is CPA-secure for message space $M = \{0,1\}^n$ (i.e. E is secure only when restricted to encrypting n-bit strings). Let E' be a public-key encryption whose key generation algorithm is just like that of E, and on input pk and a bitstring m of arbitrary length, $E'(pk, m)$ picks a random n-bit string r, computes $a = E(pk, r)$, $b = G^{|m|}(r) \oplus m$, and outputs $c = (a, b)$. Decide if E' is a CPA-secure public-key encryption for messages of arbitrary length (i.e. for message space $M = \{0,1\}^*$), and prove your answer.

5 Attacks on Key Exchange

Consider two types of attackers on a key exchange (KE) protocol and subsequent communication between the parties which used this KE instance to establish a secure communication key. Attacker Eve eavesdrops on their links, both over the internet and over telephone, while attacker Mallory can stage a man-in-the-middle attack over the internet and he can eavesdrop on the telephone but he cannot fake Alice's and Bob's voices over the telephone. In each case say whether the scheme is secure or not against each attacker type and briefly justify your answer.

(a) Assume two friends Alice and Bob perform a Diffie-Hellman Key Exchange over email, i.e. they pick ther secret exponents resp. a and b at random in $\mathbb{Z}_{p-1}$ for some large prime p, email to each other the corresponding public values $A = g^a \bmod p$ and $B = g^b \bmod p$ for g a generator of $\mathbb{Z}_p^*$, and compute the symmetric key as $k = H(g^{ab} \bmod p)$ where H is a hash which outputs 128-bit strings. After that they communicate using an authenticated encryption using k. Assume the so-called *Hashed Diffie-Hellman* assumption on $\mathbb{Z}_p^*$, which says that given g^a, g^b (all modulo p), value $H(g^{ab})$ is indistinguishable from a random 128-bit string.

(b) What if Alice uses CPA-secure public key encryption scheme to generate a (private,public) key pair, communicates her public key to Bob over email, and Bob chooses a random key k for the authenticated encryption scheme and emails it encrypted under Alice's public key to Alice?

(c) Suppose Alice and Bob do as above but they also hash Alice's public key using a CRH hash H' and read it off to each other over a telephone.

(d) Suppose Alice and Bob do as in (b) but they hash and read off over the telephone Bob's chosen key k instead of Alice's public key? Assume the hash function H' is a true random function, and in particular that for a random 128-bit key k the authenticated encryption using k remains secure even if the adversary learns the $H'(k)$ value.

6 One-time Signature

A one-time signature is a signature scheme where the private key is used to sign only a single message, and then is thrown out and never used again. The security game of a one-time signature is that the adversary A, given a public key pk, can choose a single message m, get a signature $\sigma = S(sk, m)$ on m under the corresponding private key sk, and then A outputs a pair $(m*, \sigma*)$. We say that A wins if $m* \neq m$ and $V(pk, \sigma*, m*) = 1$. A one-time signature is secure if all efficient A's have a negligible probability of winning in this game.

Let f be a One-Way Permutation on domain $D = \{0,1\}^n$. Consider the following signature scheme for messages which are integers from 1 to n, i.e. $M = \{1, ..., n\}$: The key generation picks random x in D, computes $y = f^n(x)$, where $f^i(x)$ for $i \geq 1$ is inductively defined as $f(f^{i-1}(x))$ and $f^0(x) = x$, and outputs the public key y and the private key x. A signature on message m in M is $\sigma = f^{n-m}(x)$. The verification $V(y, \sigma, m)$ outputs 1 if $y = f^m(\sigma)$.

(a) Show that this scheme is not a secure one-time signature. Given a signature on message m, for what other messages can the adversary compute a forgery?

(b) Show how to modify this scheme so that it is secure using two chains of values instead of a single chain. I.e., let $sk = (x, x')$ for x, x' chosen at random in D, and let $pk = (y, y')$ where $y = f^n(x)$ and $y' = f^n(x')$. What should a signature on m in M be, so that this scheme is secure? Argue the security of your construction.