Lecture 11 for CS276, Spring 2004

Jayanthkumar Kannan
(Instructor: David Wagner)

Mar 1, 2004

1 Combining Encryption with Authentication

As we saw in the previous lecture, since some IND-CPA-secure encryption algorithms are *malleable*, it is necessary to include authentication along with encryption. Otherwise, it is possible for the adversary to introduce controlled changes in the message. In this lecture, we will consider ways of doing that, and prove their (in)security.

Given an encryption scheme (E_k, D_k) that is IND-CPA, and an message authentication scheme $(S_{k'}, R_{k'})$ that is INT-CTXT, three potential candidates for an IND-CCA2 encryption scheme are as follows:

1. Encrypt-and-Authenticate: E&A: $E_{k,k'}(m) = (E_k(m), S_{k'}(m))$ (used in SSH)
2. Encrypt-then-Authenticate: EtA: $E_{k,k'}(m) = S_{k'}(E_k(m))$ (used in SSL)
3. Authenticate-then-Encrypt: AtE: $E_{k,k'}(m) = E_k(S_{k'}(m))$ (used in IPSEC)

The decryption algorithms $D_{k,k'}$ can be defined accordingly: decrypt and verify. Of the three reasonable looking candidates above, only EtA is IND-CCA2-secure (proved in [1] as late as 2000). We will first prove the other two insecure, then prove EtA secure.

Claim 1
E&A is susceptible to a CPA (i.e. it is not IND-CPA secure).

Proof: This proof is similar to the proof that a deterministic, stateless encryption scheme cannot be IND-CPA secure. Firstly, it is clear that encryption schemes of the form $E_{k,k'}(m) = (E_k(m), m, S_{k'}(m))$ are ruled out, since confidentiality is broken. For schemes for the form $E_{k,k'}(m) = (E_k(m), S_{k'}(m))$, it is easy to construct an adversary A that can RoR-CPA-break $E_{k,k'}$ with advantage close to 1. Attacker A can distinguish between the oracles $E_{k,k'}$ and $E_{k,k'} \circ \$ \circ len$ as follows. It simply queries its oracle on the same input message M twice, and let the outputs of its oracle be $o_1 = (e_1, h_1), o_2 = (e_2, h_2)$. If $h_1 \neq h_2$, then A knows it has the oracle $E_{k,k'} \circ \$ \circ len$, otherwise, with high probability, A has been given the oracle $E_{k,k'}$. Thus, $Adv_{RoR-CPA} \approx 1$ with $O(1)$ computation. Basically, the attack works since the INT-CTXT requirement for the MAC scheme $(S_{k'}, R_{k'})$ does not imply that it is stateful or randomized. □

Claim 2
AtE is not IND-CCA2 secure.

Proof: To prove this statement, it suffices to demonstrate an IND-CPA-secure (E_k, D_k) and an INT-CTXT-secure MAC $(S_{k'}, R_{k'})$ such that the AtE construction is not IND-CPA secure (although it is possible that this construction is secure for specific instances of (E_k, D_k) and $(S_{k'}, R_{k'})$).

Consider the following definitions (assume that the message is a single bit). Define an encoding as follows: $encode(0) = 00$, and $encode(1)$ is either 11 or 00 with probability $= 1/2$. Now, define an OTP scheme as follows: $E_k(m) = k \oplus encode(m)$ where the key k is a 2-*bit* OTP. Define, $D_k(m) = decode(m \oplus k)$ where $decode(00) = 0$, $decode(11/10) = 1$, and $decode(01) = \perp$. Consider any arbitrary $(S_{k'}, R_{k'})$ that is INT-CTXT secure.

Consider the following $IND-CCA2$ adversary A who breaks the confidentiality of $E_{k,k'}$ as follows. Let A be given the encryption $c = E_{k,k'}(b)$ of a message bit b. Then A obtains c' by flipping the second bit of c and queries $D_{k,k'}(c')$. If it obtains $\perp$, then $b = 0$, else $b = 1$. It is easy to see that A deciphers any ciphertext c correctly using this techique. From this description, it is easy to construct a $RoR-CCA2$ adversary B that breaks $E_{k,k'}$. Let B be given the oracle f (where $f = E_{k,k'}$ *or* $E_{k,k'} \circ \$ \circ len$). B obtains $c = f(b)$ on the fixed message bit, say $b = 0$. It then obtains $m = D_{k,k'}(c)$ (by using the method outline before). If $m = 0$, then B declares that its oracle is "real", otherwise "random". Clearly, B can repeat this process, say n times, to obtain an advantage of $1 - (1/2)^n$. □

In order to prove that EtA is IND-CCA2 secure, first we prove the following lemma:

Claim 3
$(S_{k'}, R_{k'})$ INT-CTXT-secure $\Rightarrow$ $(E_{k,k'}, D_{k,k'})$ is INT-CTXT-secure

Proof: This is easy to see since if an adversary A that INT-CTXT-breaks $(E_{k,k'}, D_{k,k'})$ can INT-CTXT break $(S_{k'}, R_{k'})$ by simply encrypting its input to the oracle using the scheme (E_k, D_k) using a randomly chosen key k. □

Theorem 4
If (E_k, D_k) is (t, q_p, q_c, ϵ)-LoR-CPA-secure, and $(S_{k'}, R_{k'})$ is (t, q_p, q_c, ϵ)-INT-CTXT-secure, then EtA defined as:

$$\begin{aligned} \epsilon_{k,k'}(m) &= S_{k'} \circ E_k \\ D_{k,k'}(m) &= \perp \quad if\ R_{k'}(c) = 1\ or\ D_k(R_{k'}(c)) = 1 \\ &= D_k(R_{k'}(c)) \quad o.w \end{aligned}$$

is $(t - O(q_p + q_c), q_p, q_c, \epsilon + \epsilon')$-IND-CCA2 secure.

Proof: Let A be an LoR-CCA2 attack that $(t - O(q_p + q_c), q_p, q_c, \epsilon + \epsilon')$-breaks ϵ.
$Adv(A) = \Pr[A^{E_{k,k'} \circ g_0, D_{k,k'}} = 1] - \Pr[A^{E_{k,k'} \circ g_1, D_{k,k'}} = 1] \geq \epsilon + \epsilon'$
Define B^g, a LoR-CPA attack against E as follows:

1. Pick a random key k'.
2. Run $A^{f,g}$ where:

$$\begin{aligned} f(x) &= S_{k'}(g(x)) \\ g(x) &= \text{``}halt\ and\ die\text{''}\ if\ R_{k'}(y) = 1 \\ &= \perp\ (o.w.) \end{aligned}$$

3. Output A's output.

Define a BAD event as the event that B "halts and dies". Then, $\Pr[BAD] \leq \Pr[Aforges] \leq \epsilon'$, since if A makes a successful query to $R_{k'}$, then it has successfully made a forgery. Also, $Adv(B)|\overline{BAD} = Adv(A)|\overline{BAD}$ since if A does not forge, then B is a perfect simulator of A. Also notice that:

$$\begin{aligned}
\epsilon + \epsilon' \quad \leq Adv(A) \quad &= \Pr[\overline{BAD}]\ Adv(A)|\overline{BAD} + \Pr[BAD]\ Adv(A)|BAD \\
&\leq \Pr[\overline{BAD}]\ Adv(A)|\overline{BAD} + \Pr[BAD] \\
&= \Pr[\overline{BAD}]\ Adv(B)|\overline{BAD} + \Pr[BAD] \\
&\leq Adv(B) + \epsilon' \\
&\Rightarrow \epsilon \leq Adv(B)
\end{aligned}$$

□

Thus, in conclusion, the EtA construction is the easiest secure way to combine a generic IND-CPA encryption scheme and a generic INT-CTXT MAC into a IND-CCA2 encryption scheme.

References

[1] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm", Advances in Cryptology, ASIACRYPT '00. Lecture Notes in Computer Science, Vol. 1976.