

Network Security - CSE 508 - Fall 09

Faculty - Rob Johnson

Friday October 9, 2009

1 Chosen Ciphertext Security

- Alice sends Bob an encrypted message $E_k(m)$
- Eve uses Alice as an Encryption oracle.
- Eve sends a msg. m to Alice and Alice sends back $E_k(m)$ (in the ideal world)
- Eve also uses Alice as a Decryption oracle.
- Eve sends a valid encrypted message, c to Alice and Alice responds back with $D_k(c)$

2 Chosen Ciphertext Secure Encryption

- We build a Chosen Ciphertext Secure Encryption scheme E using an Encryption scheme E' and a secure MAC M . Let E' be a (t, q, ϵ) R-O-R secure encryption scheme and M is a (t, q', q'', ϵ) secure MAC.

Let the Encryption fn., $E(k||k', m) = c||M(k', c)$ where c is $E'(k, m)$

And the Decryption fn., $D(k||k', c||t) = D'(k, c)$ if $t = M(k', c)$ or \perp otherwise

Then E is IND-CCA2 $(t - O(q, q', q''), \min(q, q'), q'', \epsilon)$ secure encryption scheme

- Definition: An Encryption scheme is (t, q, q', ϵ) IND-CCA secure if

$$Adv_A = |Pr[A^{E_k D_k} = 1] - Pr[A^{E_k o D_k} = 1]| \leq \epsilon$$

$\forall A$ running in time $\leq t$ and making at most q Encryption queries and q' Decryption queries and only making valid queries.

2.1 Proof

- Proof by Contrapositive: Suppose A breaks E ,

Observation: If A ever makes successful decryption queries, then A has forged a MAC. This happens with probability $\epsilon' \rightarrow Bad$

$$\begin{aligned}
\text{Then, } Adv A &= (AdvA|Bad)P(Bad) + (AdvA|\neg Bad)P(\neg Bad) \\
&\leq (1)(P(Bad)) + (AdvA|\neg Bad)(1) \\
&\leq \varepsilon' + \varepsilon
\end{aligned}$$

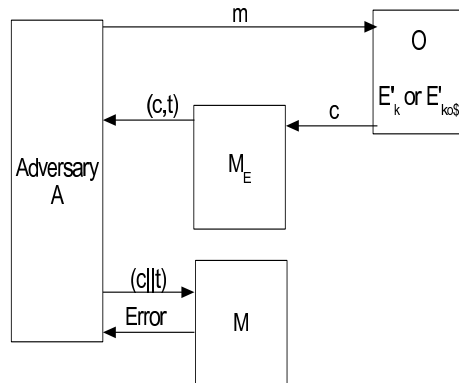


Figure 1: Chosen Ciphertext Secure Encryption

Summary: The security of the above Encryption scheme mainly depends on the adversary being able to forge a MAC query. But the MAC verification oracle is always a NULL decryption oracle as we assume it is secure. Assuming that the MAC can be forged, we can take the example of CTR mode encryption where the adversary can flip a bit in the encrypted message and adjust the MAC in such a way that the MAC verification oracle returns a ‘True’. If this happens, then the Adversary is able to tell whether he is in the Real or the Ideal world and hence the security of the scheme is broken. Since we assume that the MAC is (q, t, t', ε) secure, the probability of this is very low.

This is an example of a ‘Encrypt then MAC’ which is a good scheme.

Alternatively, we can also have a ‘MAC then encrypt’, $(E_k(m || mac(k', m)))$ or a ‘Encrypt and MAC’, $E_k(m) || mac_k(m)$ which are not so secure schemes. Hence this is a good chosen ciphertext scheme.