CSA E0 235: Cryptography 11/2/2016

Scribe for Lecture 9

Instructor: Arpita Patra *Submitted by: Tapesh Yadav*

Review

We started with classical ways of encrypting message to be sent over communication channel. Due to some major flaws in the methods used in classical crypto we introduced the field of modern crypto and tried to solve the problem of message privacy through modern crypto. In previous discussions we have shown that if ppt adversary is given power of eavesdropping (coa) or to ask encryption oracle to provide cipher text to the messages of his choice (cpa), then also our scheme is computationally secure. But as and when adversary is given the power of chosen cipher text attack, where adversary can get decrypted messages of his choice, our definitions of security fell down. And the main reason we found for failure of the current security definition was malleability of the scheme. Where we defined malleability as the power of adversary to easily change the cypher text which itself correspond to a valid message and change in the cypher text is directly related to the change in message. For our message to be non malleable, we first need the decrypted message to be the same as that of the encrypted message (messsage integrity) and then the message should be sent to the same person as was intended (message authenticity). We can clearly see that we reached a completely different domain of modern cryptography where we are no more concerned about the secrecy of the message but we want our message to be sent to the desired destination and without any change in the message during its propagation. In this regard we defined security for message authentication code (MAC) and formulated message space, key space and tag space.

Topics to be Covered

- Security Definition of MAC and construction from PRF
- MAC for variable length message
- Authenticated Encryption (AE) - Definition, security and construction.

1 Security for MAC

1.1 Threat and Break

Threat model remains the same as of SKE i.e adversary is randomized and ppt powerful but break definition is different and comes in two versions as-

- Chosen Message Attack (CMA) It is not possible to come up with (m,t) if no tag on m is seen before.

- **Chosen Message and Verification Attack (CMVA)** It is not possible to come up with (m,t) if (m,t) has not been seen before.

We will be concerned mostly with CMA security as CMVA is relatively new and still an active field of research.

1.2 CMA Security for MAC

Let $\prod = (Gen, Mac, Vrfy), n$ be the scheme. Then the message authentication experiment $Mac - forge_{A;\prod}(n)$ will be-

1. A random key $k \leftarrow \{0,1\}^n$ is chosen.

2. The adversary A is given oracle access to $Mac_k(.)$ and outputs a pair (m; t). Formally, (m; t) $\leftarrow A^{Mac_k(.)}(1^n)$. Let Q denote the queries asked by A during the execution.

3. The output of the experiment is defined to be 1 if and only if $m \notin Q$ and $Vrfy_k(m,t) = 1$.

DEFINITION 1 A message authentication code Π = (Gen, Mac, Vrfy) is existentially unforgeable under an adaptive chosen-message attack, or just secure, if for all probabilistic polynomial-time adversaries A, there exists a negligible function negl such that:

$$Pr[Mac - forge_{A;\Pi}(n) = 1] \leq negl(n)$$

Message will be strong CMA secure if in the above experiment instead of saying m does not belongs to Q, we say (m,t) does not belongs to Q.

1.3 Replay Attack and MAC

Consider the following scenario: a user Alice sends her bank an order to transfer $1,000 from her account to Bob's account. Alice is the legitimate user, and so she also applies a message authentication code to the message so that the bank knows that it is authentic. Bob is unable to intercept the message and change the sum to $10,000 because this would involve forging the MAC scheme. However, nothing prevents Bob from intercepting Alice's message and forwarding it ten times repeatedly to the bank. If the bank accepts all of these messages, then $10,000 will be transferred to Bob's account, and not $1,000. Such an attack is called a replay attack and the MAC mechanism within itself does not prevent it. Rather, the application using the MAC is responsible for preventing replays. The reason for this is that the legitimacy or illegitimacy of replays depends on the application. Furthermore, it cannot be solved by considering a single isolated message; rather the context and history must be taken into account. It is thus left to the higher-level application.

1.4 Fixed Length MAC from PRF

Theorem 1 Assume that the function F used in Construction 1 is a pseudorandom function. Then, Construction 1 is a fixed length message authentication code with length parameter l(n) = n that is existentially unforgeable under chosen message attacks.

Construction 1

Let F : $\{0,1\}^* \times \{0,1\}^* \longrightarrow \{0,1\}^*$ be a function such that for every k, $F_k(.)$ maps n-bit strings to n-bit strings. Define a fixed-length MAC as follows:

- $Gen(1^n)$: upon input 1^n, choose k $\leftarrow \{0,1\}^n$
- $Mac_k(m)$: upon input key k$\in$ $\{0,1\}^n$ and message m$\in$ $\{0,1\}^n$, compute t = $F_k(m)$tg. (If $| m | \neq | k |$ then output $\perp$.)
- $Vrfy_k(m;t)$: upon input key $k \in \{0,1\}^n$, message m $\in \{0,1\}^n$ and tag t$\in$ $\{0,1\}^n$, output 1 if and only if t = F$_k$(m). (If the lengths are incorrect, then output 0.)

Actual proof of the theorem 1 is left to the reader. Here is the hint:

1. Show that if Π is not cma-secure then F is not a PRF by designing a distinguisher for F.

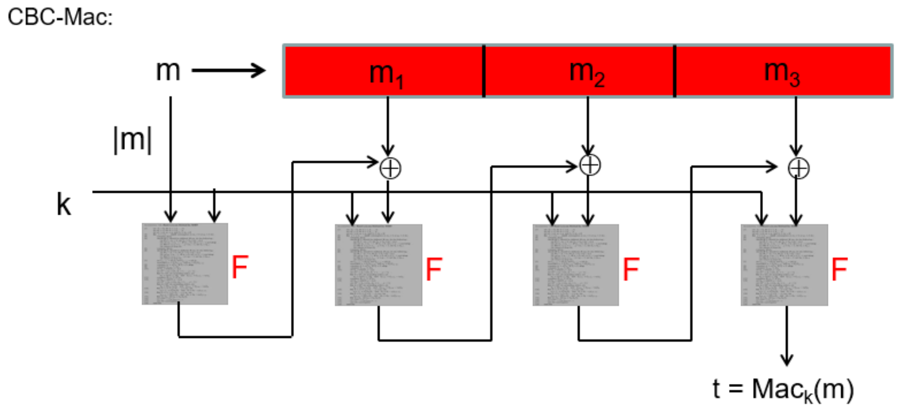
2. If instead a TRF f was used to compute tag then an attacker can guess f(m) for a new m with probability at most 2^{-n}.

3. The same should hold even if a PRF is used (as key is unknown).

1.5 Domain Extension

Domain extension for MAC is not the same as domain extension of SKE where we can encrypt individual blocks of messages and concatenate them to get the resulting cypher text. Thus cypher text created this way has a larger length then message. But it is not the case with MAC. We can preserve tag length irrespective of the input message length. For the process to be efficient, we use various constructions like CBC-MAC, C-MAC, Hash and Map, HMAP.

1.5.1 CBC-MAC



- Let F: $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF, whose key k is agreed between S and R

- Let S has a message m with $| \, m \, |$ = dn, where d is some polynomial in n
- Length of m (i.e. $| \, m \, |$) need to be prepended, not appended — otherwise insecure
- For Higher Efficiency-
    1. The tag consists of only n bits
    2. Only d invocations of PRF

2 Authenticated Encryption (AE)

Till now we have separately studied SKE and MAC both having complementary properties. Where SKE provides privacy but don't care about message authenticity and integrity, MAC provides authenticity and integrity but do not care about privacy of message. But if we combine both of these in a single definition then our message will remain hidden from adversary and will reach to the right person in the right form. Such a security is termed as Authenticated Encryption and is clearly the best possible security we have seen so far.

2.1 Definition

Let Π = (Gen, Enc, Dec) be a symmetric-key cipher. Intuitively we demand the following secrecy and integrity property to be satisfied by Π to qualify it as an AE scheme :

- For secrecy, we demand CPA security: no PPT attacker should be able to non-negligibly distinguish between encryption of two messages of its choice, even if it has access to encryption oracle service.
- For integrity/authentication, we demand something similar to strong cma-security for MAC. No PPT attacker can come up with a valid ciphertext for ANY message). Implies if receiver has received a valid ciphertext that it is THE ciphertext sent by the sender.

This definition is modeled by a new experiment- Cyphertext integrity (CiIn) which is similar in spirit to MAC-sforge. Π is an authenticated encryption scheme if no PPT attacker is able to non-negligibly win the CPA-experiment and CiIn experiment with respect to Π

2.2 Cyphertext Integrity experiment

Let $\prod = (Gen, Enc, Dec), n$ be the scheme. Then the cypher text integrity experiment $CiIn_{A;\prod}(n)$ will be-

1. A random key $k \leftarrow \{0,1\}^n$ is chosen.
2. The adversary A is given access to encryption oracle and outputs c. Let Q denote the queries asked by A during the execution.
3. The output of the experiment is defined to be 1 if and only if $c \notin Q$ and $Dec_k(c) = m \neq \perp$.

DEFINITION 2 Π has ciphertext intigrity if for every PPT A:

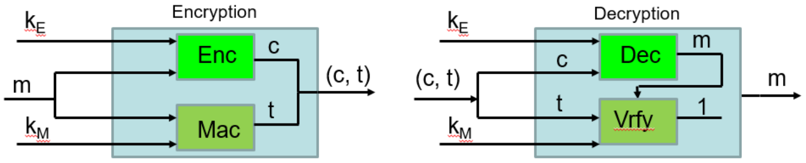
$$Pr[CiIn_{A;\Pi}(n) = 1] \leq negl(n)$$

2.3 Authenticated Encryption- Construction

We have to combine cpa-secure SKE and scma-secure MAC to construct a scheme which follows Authenticated encryption. We will try various ways of combining them and see which one of them is AE secure.

2.3.1 Attempt 1 (Encrypt and Authenticate)

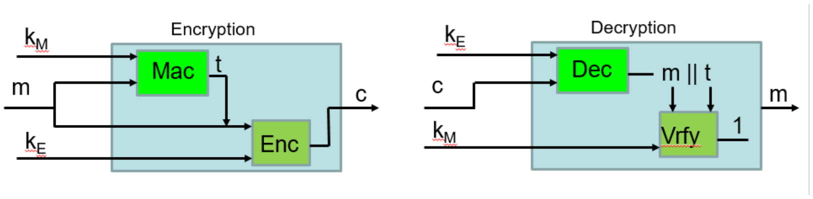
Let Π_E = (Enc, Dec) be a cpa-secure SKE and Π_M = (Mac, Vrfy) be a scma-secure MAC. Algorithm Gen in both Π_E and Π_M selects a random key from the respectively domain independently.



This approach is used in SSH. But it does not guarantee authenticated encryption as a secure MAC not necessarily preserves the privacy of m. Ex: a MAC may always output the first two bits of m as the first two bits of MAC tag

2.3.2 Attempt 2 (Authenticate-then-Encrypt)

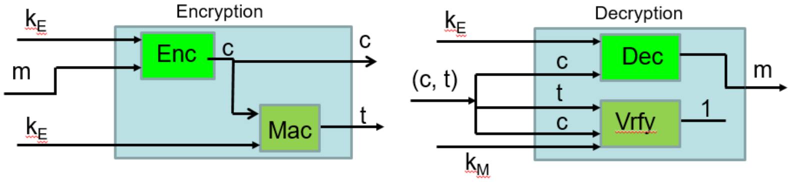
Let Π_E = (Enc, Dec) be a cpa-secure SKE and Π_M = (Mac, Vrfy) be a scma-secure MAC. Algorithm Gen in both Π_E and Π_M selects a random key from the respectively domain independently.



This approach is used in SSL. Unfortunately the above approach does not always lead to an authenticated cipher. There exists an instantiation of Π_E which is cpa-secure and which when combined with any MAC using the above approach does not lead to an authenticated cipher. Ex: CBC-mode of encryption + MAC using above approach $\not\longrightarrow$ authenticated encryption. This way Security of this approach depends upon the underlying instantiation of Π_E.

2.3.3 Attempt 3 (Authenticate-then-Encrypt)

Let $\Pi_E = (\text{Enc}, \text{Dec})$ be a cpa-secure SKE and $\Pi_M = (\text{Mac}, \text{Vrfy})$ be a scma-secure MAC. Algorithm Gen in both Π_E and Π_M selects a random key from the respectively domain independently.



This approach is used in IPSec. Fortunately this approach always lead to an AE, irrespective of how Π_E and Π_M are instantiated.