1 Related Works

1.1 Message Integrity and Tag Design

Tag

1.1.1 Message Authentication

A common way to protect the integrity of message blocks is utilizing message authentication system. Assume the sender A sends message M to receiver B,the message authentication system is eligible to examine the modification on M. The concept of message authentication system is expressed in Figure 1. The sender uses the message as input to the tag generation system(TG_K(M)) to generate a short information block called tag. The message is concatenated with tag and transmitted to the receiver. Before the receiver accept the message M, M and its tag T are sent to the verification system(VF_K(M,T)). If the output of verification system is 1, that means the M and T are not matched, otherwise the message M is accepted by the receiver.

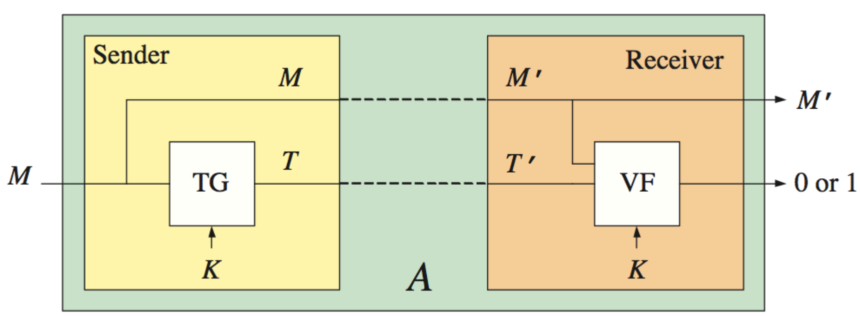

Figure 1: The Concept of Message Authentication System

Common Message Authentication Systems The Message Authentication Code(MAC) is a common message authentication system. The concept of MAC scheme can be seen in Figure 2. In a deterministic MAC scheme, the verification system adopts the same key used in tag generation system. In the verification part of a MAC scheme, the tag T1 of message M is computed and compared with the tag T concatenated with the M. If T1=T then the verification system output 1 and the receiver accepts M, otherwise the verification system output 0. The early designed MAC schemes are deterministic, which means neither the sender nor the receiver needs to maintain a state used in tag generation. Latter some MAC designs adopt a state maintained by the user in the tag generation, such as the GMAC [**?**] and Cost-Effective Tag Design [**?**].

Digital signature is another kind of message authentication system. The signature generation uses a private key while the message verification stage uses public key. The digital signature system can assure non-repudiation of the message protected while MAC schemes can not.

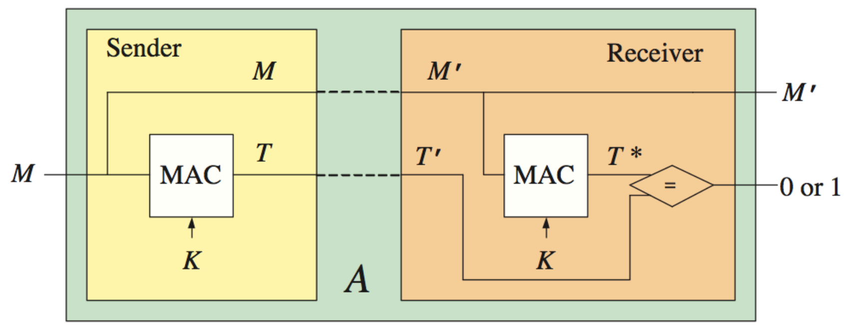

Figure 2: Message Authentication Code(MAC)

1.1.2 The Security of MAC schemes

The forgery attacks When attacking a message authentication system, the adversary try to send a pair(M,T) to the receiver to make VF_k(M,T)=1 while M did not originate with the legal sender. The fake pair(M_f,T_f) that makes VF_k(M_f,T_f)=1 is called a forgery from the adversary. A successful forgery attack indicates that the adversary has made a forgery. The purpose of a message authentication system is preventing the receiver to accept the message from unauthorized senders, such as an adversary. The quantitative property of a secure message authentication system is the low probability for an adversary to make a successful forgery attack with the limited resource.

Chosen-message attacks A strong type of attack that an adversary can conduct on the message authentication system is the adaptive chosen-message attack, marked as uf-cma. When doing uf-cma, the adversary chooses its own input message M and acquires the relative tag T. The adversary try to find the weakness in the design of message authentication system by analyzing the pairs(M,T) of his choice. The uf-cma provides the adversary with the most capability to succeed in the forgery attack. The probability that an adversary conducts a successful forgery attack after limited times of uf-cma is adopted as the basic quantitative security property of a message authentication in cryptography. This fact was also mentioned in [**?**].

The Security Notions of MAC schemes The formalised quantitative notion of the security of a MAC scheme was introduced by Bellare et al. in [**?**]. This notion follows the security notion of digital signature introduced in [**?**]. The successful forgery on a MAC scheme from an adversary A is measured by a experiment called Forgery(MAC,A). In Forgery(MAC,A), the adversary A is provided a black-box access to the tag generation system $\mathrm{TG}_K()$. When $\mathrm{TG}_K()$ takes an input message M_i, it returns tag T_i to A. A conducts uf-cma by keep sending the message queries M_i and observes the relative tag T_i for limited times. On the other hand, A is provided a black-box access to the verification system $\mathrm{VF}_K()$. When A sends a pair(M_j,T_j) to $\mathrm{VF}_K()$, the $\mathrm{VF}_K()$ computes the tag T of M_j and compares T with T_j. If T=T_j then $\mathrm{VF}_K()$=1 otherwise 0. If A sends a pair(M,T) that makes $\mathrm{VF}_K()$ outputs 1 while M has not appeared in the previous queries of uf-cma, then A succeeds a forgery attack and Forgery(MAC,A)=1.

The quantitative security notion of a MAC scheme is forgery probability, expressed as $\mathrm{Forgery}_M AC$=Pr[Forgery(MAC,A)=1].

The Correlation between Security and Randomness Goldreich, Goldwasser, and Micali asserted in [**?**] that any good pseudorandom function(PRF) is a secure MAC scheme under the quantitative security notion. Bellare, Kilian and Rogaway proved this assertion in [**?**] saying that if a system behave like a pseudoranom function, this system is a secure MAC scheme if meeting the requirements on domain and range of MAC schemes. Based on these two reduction of security notion, latter researches on security evaluation of MAC schemes posted their focuses on analyzing whether the MAC scheme evaluated behaves like a PRF.

The Randomness of a MAC scheme The definition of PRF was introduced in [**?**] indicating that PRF could not be distinguished from a ideal random function each bit of whose output was a coin flip. To define how closely a MAC scheme behaves like a PRF, Bellare et al. provided a quantitative notion in [**?**]

named $\text{Adv}_{MAC}^{PRF}()$, which was based on the concept of distinguisher introduced in[**?**].

Let F_0 and F_1 be two function with a common domain D and a common range R. A distinguisher A for F_0 versus F_1 is an adverary A that has access to a black box named oracle f:D-¿R. After accessing the oracle f, A computes a bit. Assume the function stored in the oracle f is X and A guesses that X is in the oracle, then A computes 1 otherwise 0. The the advantage of A in distinguishing F_0 from F_1 is expressed as Adv_{F1}^{F0}=Pr[f$\xleftarrow{R}$F0:A^{F0}=1]-Pr[f$\xleftarrow{R}$F1:A^{F1}=1]. Pr[f$\xleftarrow{R}$F0:A^{F0}=1] means when the content of oracle f is F0, A guesses that F0 is in oracle then output 1.

We can see that if F0 behaves much like F1, it is hard for A to distinguish between F0 and F1 then Adv_{F1}^{F0} is very small. This case is adopted by Bellare et al. in the quantitative notion of randomness of a MAC scheme. If the randomness of a MAC scheme is good, then the MAC scheme behaves like a PRF and $\text{Adv}_{MAC}^{[PRF]}$ is small.

1.2 Implementation of Tag Design

1.2.1 Network and Cloud System

1.2.2 Memory Protection

Single-processor System

Multiple-processor System

1.2.3 Crypto-hardware Design

1.3 Security Evaluation of Tag Design