Lecture 9b: February 23, 2004

Lecturer: David Wagner *Scribe: Marco Barreno*

Lecture 9, Part 2: More on MACs

What if Alice uses her key twice, as in Figure 9.1?

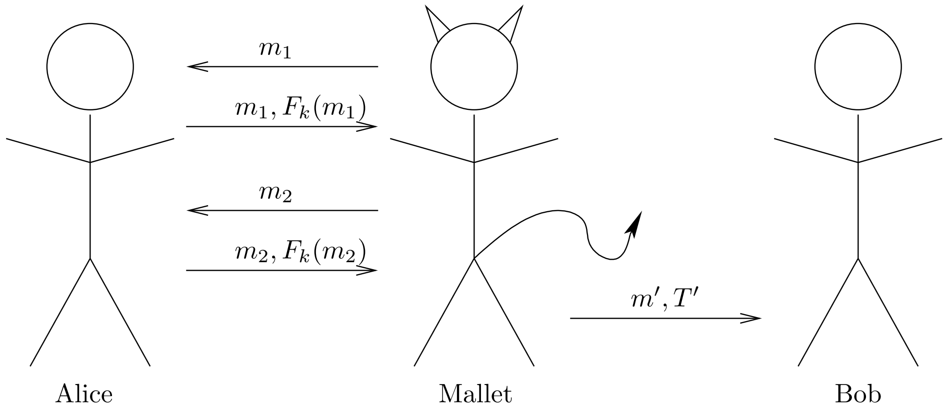

Figure 9.1: Alice reuses key k

In this case, we're still okay if we use a 3-universal hash (meaning triplets are independent), and we use a 4-universal hash if we want to use the key three times, etc. But what about an unbounded number of messages?

Insight: a random function is "as many universals as you want!" Unfortunately, the entire function (codebook) must be known to both Alice and Bob, which is impractical. But we can use a PRF. We will now proceed to show that this does result in a secure MAC. Note that q_t is the number of chosen-plaintext queries the attacker makes and q_v is the number of verification queries.

Lemma 9.1 *If $R : X \rightarrow Y$ is a random function, it is a $(\infty, q_t, q_v, \frac{q_v}{|Y|})$-MAC.*

Proof: For $q_v = 1$: let A be an attacker. We can assume A makes all q_t chosen-plaintext queries first, then the verification query.

$$\begin{aligned} \text{Adv } A &= \Pr_R[A^{R,V[R]} \text{ forges}] && (9.1)\\ &= \Pr_R[(m', T') \leftarrow A^R; R(m') = T' \text{ and m' is new}] && (9.2)\\ &= \frac{1}{|Y|} && (9.3) \end{aligned}$$

Note that this probability could be less if the attacker is stupid and outputs an old m!

Since A can make q_v verification queries and each one has probability $\frac{1}{|Y|}$ of succeeding, the overall probability of success is $\frac{q_v}{|Y|}$. ■

Theorem 9.2 *F is a $(t, q_t + q_v, \epsilon)$-PRF $\Rightarrow$ F is a $(t - O(q_t + q_v), q_t, q_v, \epsilon + \frac{q_v}{|Y|})$-MAC.*

Proof: Let A be an attack against F as a MAC. Define B, attacking F as a PRF, by

B^g :

1. Run $A^{g,V[g]}$.

   Queries to A's first oracle are sent to g, and queries to A's second oracle require simulating $V[g]$; this accounts for the $O(q_t + q_v)$ in F's time restriction.

2. If A forges, output 1, else output 0.

$$\begin{aligned} \mathrm{Adv}^{prf}\ B &= \Pr_k[B^{F_k} = 1] - \Pr[B^R = 1] && (9.4)\\ &\geq \mathrm{Adv}^{mac}\ A - \frac{q_v}{|Y|} \text{ (from lemma)} && (9.5)\\ \mathrm{Adv}^{mac}\ A &\leq \mathrm{Adv}^{prf}\ B + \frac{q_v}{|Y|} && (9.6) \end{aligned}$$

■

A practical consideration: we want arbitrary-length messages. Block ciphers such as AES are good PRFs, but they work only on fixed-size blocks. To get around this limitation, we use the trick illustrated in Figure 9.2. We will show that this composition creates not only a good hash, but also a good PRF (almost 2-universal).

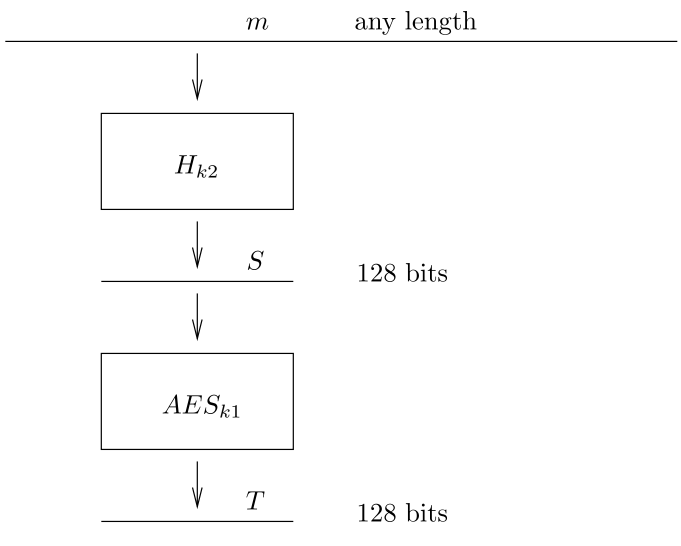

Figure 9.2: The trick we use to use a fixed-length block cipher with a message of any length.

Definition 9.3 *H is ϵ-almost 2-universal if*

$$\Pr_k[H_k(m) = H_k(m')] \leq \epsilon \qquad \forall m, m'(m \neq m'). \tag{9.7}$$

Theorem 9.4 *Given:*

- $E : K_E \times \{0,1\}^{128} \to \{0,1\}^{128}$ *is a* (t, q, ϵ_E)*-PRF (e.g. AES)*
- $H : K_H \times \{0,1\}^* \to \{0,1\}^{128}$ *is* ϵ_H*-almost 2-universal*
- $F : (K_H \times K_E) \times \{0,1\}^* \to \{0,1\}^{128}$ *such that* $F_{k1,k2}(m) = E_{k1}(H_{k2}(m))$

then F *is a* $(t - O(q), q, \epsilon_E + \binom{q}{2}\epsilon_H)$*-PRF.*

Proof: Let A be an attack on F. Define B on E by

B^g :

1. Pick $k_2 \leftarrow k_H$
2. Let $b \leftarrow A^{g \circ H_{k2}}$
3. Output b

When B gets AES, it runs A on AES. When B gets random, it runs A on random (almost): taking the hash of the input and then putting it through a random function results in random output when there are no collisions in the hash function. We will see how to deal with collisions in a moment.

Let $R : \{0,1\}^{128} \to \{0,1\}^{128}$ be a random function on 128 bits (to 128 bits) and $R' : \{0,1\}^* \to \{0,1\}^{128}$ be a random function on any number of bits (to 128 bits). Note also that $k1$ and $k2$ must be independent here.

$$\begin{aligned}
\text{Adv } B &= \Pr_k[B^{E_k} = 1] - \Pr_R[B^R = 1] && (9.8)\\
&= \Pr_{k1,k2}[A^{F_{k1,k2}} = 1] - \Pr_{R,k2}[A^{R \circ H_{k2}} = 1] && (9.9)\\
&= \Pr[A^{F_{k1,k2}} = 1] - \Pr[A^{R'} = 1] + \Pr[A^{R'} = 1] - \Pr[A^{R \circ H_{k2}} = 1] && (9.10)\\
&= \text{Adv } A + \Pr[A^{R'} = 1] - \Pr[A^{R \circ H_{k2}} = 1 | \text{coll}] \Pr[\text{coll}] - \Pr[A^{R \circ H_{k2}} = 1 | \overline{\text{coll}}] \Pr[\overline{\text{coll}}] && (9.11)\\
&\geq \text{Adv } A + \Pr[A^{R'} = 1] - \Pr[\text{coll}] - \Pr[A^{R \circ H_{k2}} = 1 | \overline{\text{coll}}] && (9.12)\\
&\geq \text{Adv } A - \binom{q}{2}\epsilon_H && (9.13)
\end{aligned}$$

Equation 9.11 follows because $\Pr[A] = \Pr[A \cap B] + \Pr[A \cap \overline{B}]$ and $\Pr[A \cap B] = \Pr[A|B]\Pr[B]$. Equation 9.12 follows because when there is a collision we bound the probability of guessing the output by 1. Equation 9.13 follows because we said earlier (intuitively) that if there are no collisions, then the output of a random function applied to a hash looks random. ■