University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Lecture 24

1 Perfectly-Secure Message Authentication

We consider our goal — briefly introduced last time — more carefully now. Recall that we want to construct MACs which are secure against an unbounded adversary. This will have the advantage of achieving secure message authentication *without any unproven assumptions*; note that the use PRFs (as we did in previous constructions) we need to assume that some one-way function exists. We noted last time that full security against an unbounded adversary is not really possible: for one thing, it is impossible to prevent an adversary from succeeding with probability at least $\max\{2^{-k}, 2^{-n}\}$, where k is the key-length and n the tag-length of the scheme. Furthermore, it becomes impractical to achieve security unless we bound the number of queries the adversary can make to the MAC oracle. So, the best we can hope is to achieve the following level of security:

Definition 1 *A message authentication scheme is said to be* ϵ-secure after ℓ uses *if, for any adversary submitting at most* ℓ *messages to its* MAC *oracle, the probability that the adversary can then output a valid tag on a new message is less than* ϵ.

An alternate way of phrasing this definition is to require the following: let s represent a key for the message authentication scheme, and assume without loss of generality that the scheme is deterministic. Let $\mathcal{M} = \{m_1, \ldots, m_\ell\}$ be a set of messages and let $\mathcal{T} = \{\mathsf{tag}_1, \ldots, \mathsf{tag}_\ell\}$ be the corresponding set of tags for these messages (i.e., $\mathsf{tag}_1 = \textsc{mac}_s(m_1)$, etc.). Then for all $\mathcal{M}$ and $\mathcal{T}$, and for any $m \notin \mathcal{M}$ and any tag, we should have:

$$\Pr[\textsc{mac}_s(m) = \mathsf{tag} \mid \mathcal{M}, \mathcal{T}] < \epsilon.$$

Do you see why this is equivalent to Definition 1?

We will give constructions of schemes achieving this level of security. Before doing so, however, we take a brief digression and discuss finite fields.

2 Finite Fields

The notion of a *field* extends the notion of a group, by considering sets for which two types of operations are defined.

Definition 2 *A field* $(F, +, \times)$ *is a set* F *with special elements 0 and 1, along with two operations* $(+, \times)$ *defined on pairs of elements of* F *such that the following conditions hold:*

1. $(F, +)$ *is a commutative group, with identity 0.*

2. *The $\times$ operation is associative; for all $a, b, c \in F$, $a \times (b \times c) = (a \times b) \times c$.*

3. *The $\times$ operation is commutative: for all $a, b \in F$, $a \times b = b \times a$.*

4. *The element 1 is an identity for $\times$; for all $a \in F$, $1 \times a = a \times 1 = a$.*

5. *The* distributive law *is satisfied; for all $a, b, c \in F$, $a \times (b + c) = (a \times b) + (a \times c)$.*

6. *All nonzero elements in F have an inverse under $\times$; for all $a \in F, a \neq 0$, there exists an element $a^{-1} \in F$ such that $a \times a^{-1} = 1$.*

For any field F, we denote by F^* the set of invertible elements of F (note that the usage corresponds to our prior usage for $\mathbb{Z}_N^*$). In the case of a field, F^* is simply all nonzero elements.

Typical example of fields are the real numbers or the complex numbers. These are both examples of infinite fields (i.e., fields with an infinite number of elements). Of interest in cryptography are finite fields. As an example, note that $\mathbb{Z}_5$ is a field under addition and multiplication (modulo 5). We have already seen that $\mathbb{Z}_5$ is a group under addition. Furthermore, we can check that requirements 2–5 are satisfied (since they hold over the set $\{1, \ldots, 5\}$ considered as a subset of the integers). The non-trivial one to check is condition 6, but this can be verified on a case-by-case basis (i.e., the inverse of 2 is 3; 4 is its own inverse). On the other hand, note that $\mathbb{Z}_6$ is *not* a field. For example, 4 has no multiplicative inverse (try to find one!).

In fact, we can state the following lemma showing the existence of many finite fields:

Lemma 1 *Let p be a prime number. Then $\mathbb{Z}_p$ is a field under addition and multiplication modulo p.*

The proof of this is simple. As above, it is clear that $\mathbb{Z}_p$ is a commutative group under addition, and that conditions 2–5 hold. That condition 6 holds is easy to show, using the fact (discussed previously in class) that $\mathbb{Z}_p^*$ is a *cyclic group* under multiplication (for prime p). Recall that this means there exists some generator $g \in \mathbb{Z}_p^*$ for which $\mathbb{Z}_p^* = \{g^0, g^1, \ldots, g^{p-2}\}$ (we may stop here, since $g^{p-1} = 1 = g^0$ and the cycle repeats). Consider any element $a \in \mathbb{Z}_p^*$. We know that we can write a as g^x for some $x \in \{0, \ldots, p-2\}$. But then $g^x g^{p-x-1} = g^{p-1} = 1$ and hence $a^{-1} = g^{p-x-1}$; since a was arbitrary this means that every nonzero element has an inverse and we are done.

For completeness we note that other finite fields exist; however, we will not use these in this class.

3 Constructing a Perfect MAC

Armed with the machinery of finite fields, we can now give a construction of a message authentication scheme that is ϵ-secure after 1 use. We will extend this below to give schemes secure after ℓ uses, for arbitrary ℓ.

Assume our message space is a finite field F (of course, all we really need is to be able to efficiently map messages — in a one-to-one manner — to elements of F). The sender and receiver share a key of the form a, b, where a and b are randomly chosen in F. The authentication tag on a message m will be $\mathtt{tag} = am + b$. (Note that it is easy for the receiver to verify correctness of a given tag on a given message.)

Lemma 2 *The message authentication scheme above is* $1/|F|$*-secure after 1 use.*

Proof Using the reformulation of Definition 1, we show that for any m and any tag t, and for any $m' \neq m$ and any tag t', we have $\Pr[\mathrm{MAC}_{a,b}(m') = t' \mid \mathrm{MAC}_{a,b}(m) = t] < 1/|F|$. Note that:

$$\Pr[\mathrm{MAC}_{a,b}(m') = t' \mid \mathrm{MAC}_{a,b}(m) = t] = \frac{\Pr[\mathrm{MAC}_{a,b}(m') = t' \wedge \mathrm{MAC}_{a,b}(m) = t]}{\Pr[\mathrm{MAC}_{a,b}(m) = t]}.$$

Let us first count the number of possible keys. Since $a, b \in F$, the total number of keys is $|F|^2$. Of these keys, we claim that exactly F satisfy $\mathrm{MAC}_{a,b}(m) = t$. Indeed, this is equivalent to requiring that $am + b = t$, or $b = t - am$. So, plugging in any value for a yields a possible solution for b; since there are $|F|$ choices for a, this means that there are $|F|$ solutions in total. We have just shown that $\Pr[\mathrm{MAC}_{a,b}(m) = t] = |F|/|F|^2 = 1/|F|$ (note that this holds for arbitrary m, t).

We claim further that for any $m' \neq m$ and any t', exactly one key satisfies $\mathrm{MAC}_{a,b}(m') = t' \wedge \mathrm{MAC}_{a,b}(m) = t$. Note that this is equivalent to requiring that $am+b = t$ and $am'+b = t'$. Solving these equations gives $a = (t-t')(m-m')^{-1}$ and $b = t-ma$ (note it is crucial here that $m' \neq m$ — otherwise, $(m-m')$ does not have an inverse!). Thus there is exactly one solution to this equation, and we have shown that $\Pr[\mathrm{MAC}_{a,b}(m') = t' \wedge \mathrm{MAC}_{a,b}(m) = t] = 1/|F|^2$.

Plugging in to the equation above shows that $\Pr[\mathrm{MAC}_{a,b}(m') = t' \mid \mathrm{MAC}_{a,b}(m) = t] = 1/|F|$, and we are done. ■

So, given a particular message space with M messages (representing all possible messages we might send), we can efficiently authenticate these as follows: Pick a prime p such that $p \geq M$. This will define a field $\mathbb{Z}_p$ in which we can embed our message space.[1] The scheme above then achieves $1/p$-security after one use.

This is all well and good...but what if our message space is small? Does this mean that we are then restricted to achieving security $1/p \approx 1/2M$ (which might not be acceptable if M is too small)??? Not at all. We can choose p as large as we like (subject to $p \geq M$) and then *embed* our (small) message space within the (larger) field $\mathbb{Z}_p$. In this way we obtain security $1/p$ and, by setting p large enough, can achieve whatever level of security we desire.

3.1 Achieving security after ℓ uses

The scheme above used a degree-1 (i.e., linear) polynomial $am + b$ to achieve security after one use. This suggests the following extension of the scheme for security after ℓ uses: Let F be a finite field. The sender and receiver share $\ell + 1$ random elements $a_0, \ldots, a_\ell \in F$. To authenticate a message $m \in F$, the sender computes $\mathtt{tag} = a_0 + a_1 m + a_2 m^2 + \cdots a_\ell m^\ell$. We leave it to the reader to verify that this gives a scheme which is $1/|F|$-secure after ℓ uses (the proof proceeds as above, and uses the fact that a degree-ℓ polynomial over a field is uniquely defined by its values on any $\ell + 1$ distinct points).

[1]Note also that we will not have to pick a p too large — a theorem from number theory states that for all M there exists a prime in the interval $[M, 2M]$.