CS 276: Cryptography
Lecture Notes

Todd Kosloff

February 18, 2004
First Half

Last time, we talked about definitions of security for symmetric key cryptosystems. We can use these definitions to prove that various modes of operation are secure. These kinds of proofs are very similar, so one example should be enough. We will prove that counter mode is IND-CPA. Well, a simplified counter mode, anyway, where we assume messages are only one block long. First, we need the definition of counter mode.

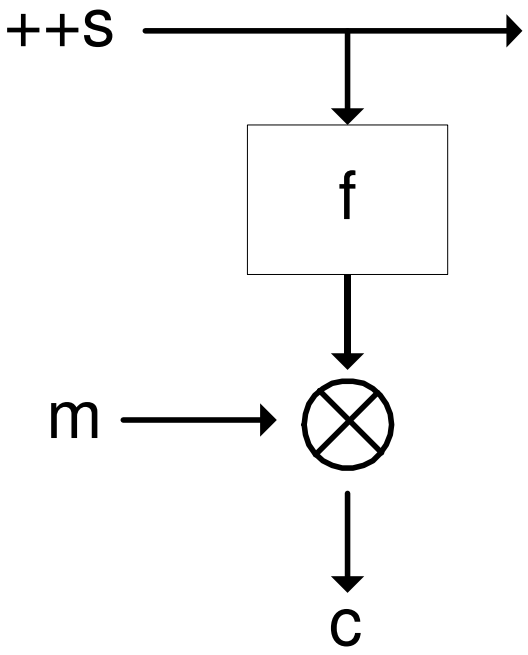

Figure 1: Counter Mode

int S = 0;

$CTR[f] \cdot E(m) : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$
$f : N \rightarrow \{0,1\}^{128}$ where N is the space of integers that fit within 128 bits.

To encrypt: output $(++S, f(S) \oplus m)$

$CTR[f] \cdot D(c) : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$

To decrypt:
1. Parse c as (t, y)
2. Output $f(t) \oplus y$

Note that while encryption is stateful, the decryption is not. To use counter mode, we have to plug in some block cypher, e.g. $CTR[AES_K]$. With the definition in hand, we can now prove that counder mode is IND-CPA. First, some intuition. CTR only uses f as a subroutine. If we choose truly random encryption instead of AES, then counter mode becomes a one time pad.

Lemma: $CTR[R_{Random}]$ is $(\infty, \infty, 0)$-LR-secure. That is, countermode on random functions is unconditionally secure.
Proof:

Adv A = Pr $[A^{CTR[R] \cdot E \circ \oint_0} = 1] - [A^{CTR[R] \cdot E \circ \oint_1} = 1]$ in the LR scheme.

Consider the left world, A makes the query (m_0, m_1). Oracle returns $(++S, R(S) \oplus m_0)$, which has the same distribution as $(++S, Uniform)$.

In the right world, A makes the query (m_0, m_1). Oracle returns $(++S, R(S) \oplus m_1)$, which also is close to $(++S, Uniform)$.

So the response from the oracle is the same distribution in both the left world and the right world, so Adv A = 0.

Now we use that lemma to prove that counter mode is IND-CPA.

Claim: If F is a (t, q, ε)-PRF running in time t', then $CTR[F]$ is $(t - t', q, 2\varepsilon)$-LR-secure.
Proof:

Intuition: If we can attack F, we can attack $CTR[F]$. Suppose A is a LR-attack against $CTR[F]$ with Adv A $> 2\varepsilon$. Note: we could run A against $CTR[R]$ with advantage 0. Define B which is an attack against f. B^f must tell whether f is F, or rather, is f R. Use A to do this, run A and "see if it succeeded". But how? This is tricky! A picture might help.

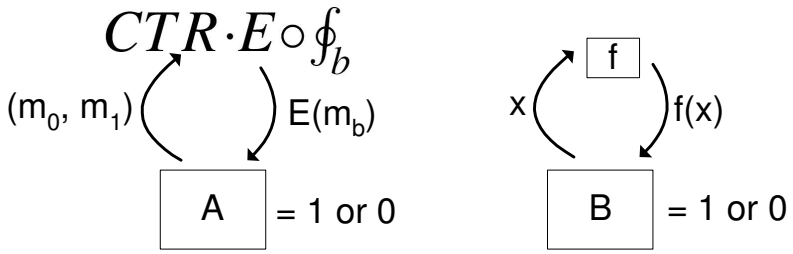

Figure 2: A and B

Given A, given f, we must instantiate A by supplying it with an oracle. We might refer to f as g to avoid getting f confused with F.

"X is a single query to B's oracle"

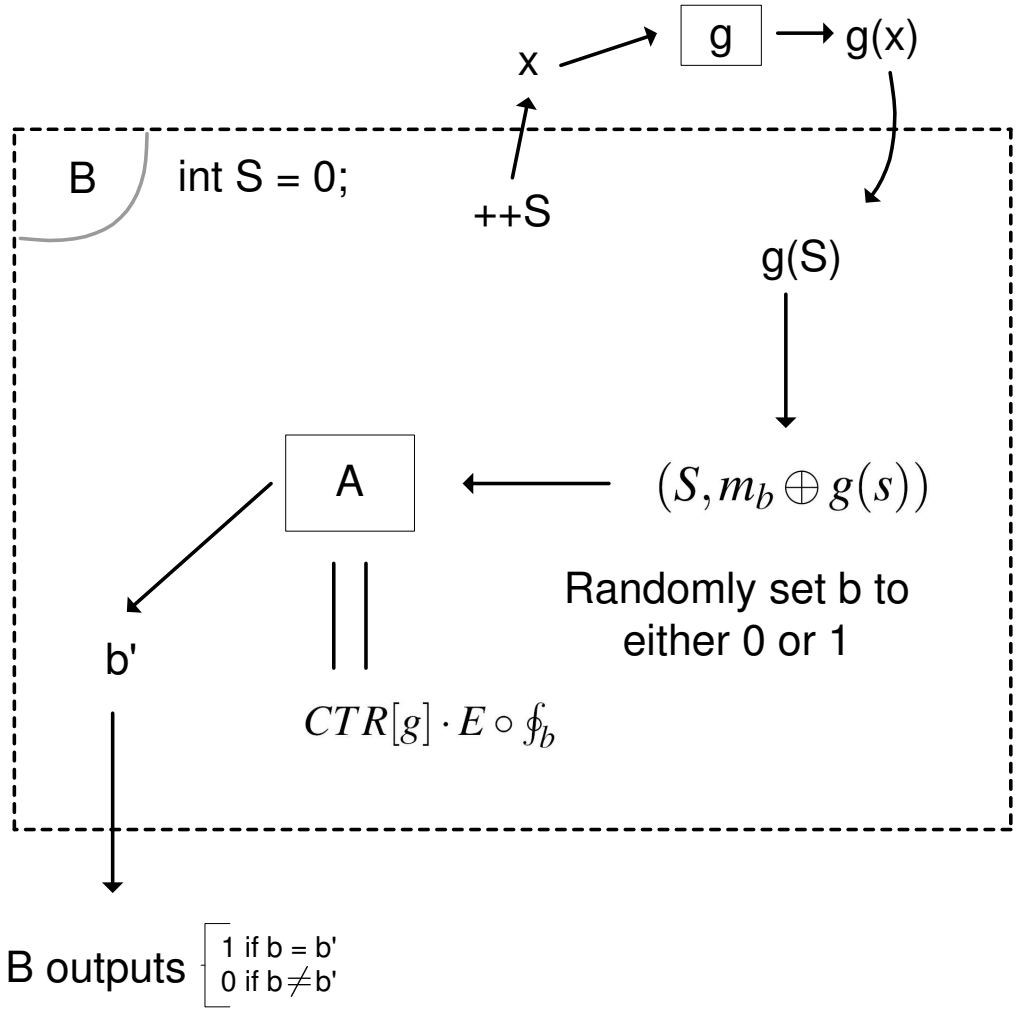

Figure 3: The inner-workings of B

When $b = 0$, $B^{F_K} = A$ run in left world on $CTR[F_K]$, but $B^R = A$ run in left world on $CTR[R]$. When $b = 1$, $B^{F_K} = A$ run in right world on $CTR[F_K]$, but $B^R = A$ run in right world on $CTR[R]$. Hmm... still tricky, Let's simulate the whole LR game, rather than just counter mode. Pick b to randomly be 0 or 1. A outputs b'. B outputs 1 if $b = b'$, 0 if $b \neq b'$. Now we see where this is going!!! So B is slightly more likely to pick 1 given F^K Therefore, we are now equipped with good intuition. Time to formalize it.

Formal:
B^g: 1. Randomly set b either to 0 or 1.
2. If $A^{CTR[g]\circ f_b} = b$, output 1, else 0
Claim: Adv B $> \varepsilon$
Proof:
Adv B = $\Pr[B^{F_K} = 1] - \Pr[B^R = 1]$.
Now plug in our knowledge of the internal structure of B.
Adv B = $\Pr[A^{CTR[F_K]\cdot E\circ f_b} = b] - \Pr[A^{CTR[R]\cdot E\circ f_b} = b]$ By the Lemma...
Adv B = $(\frac{1}{2} + \frac{\text{Adv A}}{2}) - (\frac{1}{2} + \frac{0}{2}) \Rightarrow \frac{\text{Adv A}}{2} > \varepsilon \Rightarrow$ Adv B $> 2\varepsilon$ While figuring out this proof might have looked messy, it is, in fact, easy! You can almost do it in your head. No insight is required, just symbol pushing.
Note: the time bound we gave earlier is bogus. $CTR[F]$ is, in fact, $(t - qt' - O(1), q, t\varepsilon)$... or something like that.
And that concludes our proof that counter mode is IND-CPA. Next we present some intuition for CBC, and we sketch a similar proof.
A reminder, what is CBC?

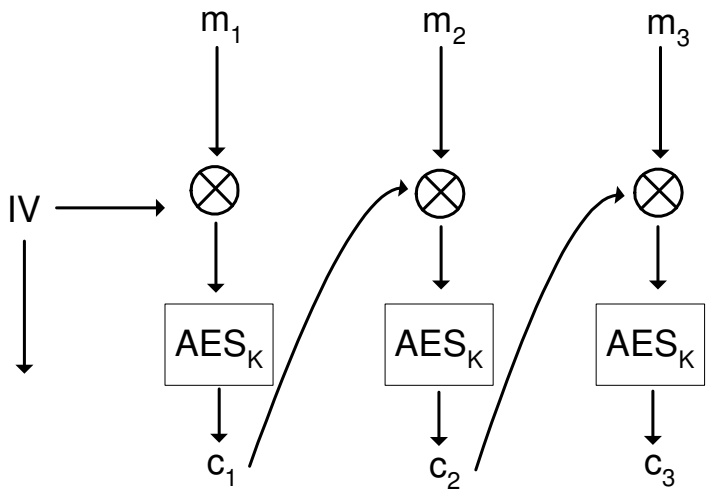

Figure 4: Cypher-Block-Chaining (CBC)

Note: To do this kind of proof, CBC must not use K except in order to use AES_K as a subroutine. Basically, CBC is secure "If inputs never repeat". Well, CAN inputs ever repeat? Here we mean inputs as in the thing that we are xor-ing with the block. Well, given random IV's, that probability is 2^{-128}, at least considering the first block. Now what about later blocks down the chain?
It turns out that we are OK, because:

(1) "Input" is random
(2) AES_K is a PRF
(3) (1) $\oplus$ (2) gives something random, uniform distinct.

Thus, chances of repeat "input" are low. Thus, if we work out the details (which we will not do), we will discover that CBC is secure. This concludes our discussion of symmetric key encryption.