

Take-home question for midterm  
CIS-6930: Adv. Topics in Crypt. and Network Security

Department of Computer Science  
Florida State University

Breno de Medeiros

Spring 2006

**Definition of Left-Middle-or-Right experiment**

- A symmetric scheme  $\mathcal{SE}$  is given by its key generation  $\mathcal{K}$ , encryption  $\mathcal{E}$ , and decryption  $\mathcal{D}$  algorithms. At the beginning of each experiment, the simulator chooses a random value  $b \in \{0, 1, 2\}$ .  $\mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-}b}$ , where  $\text{atk}$  is one of  $\text{cpa}$  or  $\text{cca}$ , is defined as follows.
- The simulator generates a new symmetric key  $K$  according to algorithm  $\mathcal{K}$ , then instantiates the encryption oracle  $\mathcal{O}^{\text{LMR}, b, K}(\cdot)$  to respond to queries  $(m_0^i, m_1^i, m_2^i)$  by returning the encryption of  $m_b^i$  under  $K$ :  $\mathcal{O}^{\text{LMR}, b, K}(m_0^i, m_1^i, m_2^i) = \mathcal{E}(K, m_b^i)$ . If  $\text{atk} = \text{cca}$ , the decryption oracle  $\mathcal{O}^{K^{-1}}(\cdot)$  is instantiated, and decrypts queried ciphertexts—though refuses to decrypt values returned as replies to encryption queries.
- At the end of the simulation, the adversary guesses  $b' \in \{0, 1, 2\}$ —trying to match the value  $b$  used by the simulator.

**Definition of LMR security**

- A  $(\epsilon, t, q, \mu, k)$ -LMR adversary for a symmetric scheme  $\mathcal{SE}$  is a probabilistic algorithm that:
  - on instances of security parameter  $k$ ;
  - using at most  $q$  queries to the oracles;
  - receiving at most  $\mu$  bits total in the answers to its queries;
  - taking at most  $t$  computational steps;

– Achieves advantage  $\mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk}}$  at least  $\epsilon$ , where

$$\mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk}} := \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-0}} = 0 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-1}} = 1 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-2}} = 2 \right] - 1.$$

- Naturally, a symmetric scheme  $\mathcal{SE}$  is  $(\epsilon, t, q, \mu, k)$ -LMR secure if no  $(\epsilon, t, q, \mu, k)$ -LMR adversaries exist against it.

**Statement of Question** Show concrete-security relationships between LMR and left-or-right security. In particular, show that, given an adversary  $\mathcal{A}$  of LMR attacks you can build an adversary  $\mathcal{B}$  to LoR and vice-versa. Work out the relationship between the advantages  $\epsilon_{\text{LoR}}$  and  $\epsilon_{\text{LMR}}$  in each case. Use the example for LoR and RoR (real-or-random) in the studied paper for guidance.

**Answer:** Let  $\mathcal{A}$  be an adversary for LMR. We wish to show how to generate an adversary  $\mathcal{B}$  for LoR. At the beginning of the simulation,  $\mathcal{B}$  will choose a value  $c$  at random from  $\{0, 1, 2\}$ . This value will remain constant for that simulation.

Then  $\mathcal{B}$  activates  $\mathcal{A}$  as a subroutine, and  $\mathcal{A}$  will at times generate encryption queries, which consist of a triple of messages  $(m_0^i, m_1^i, m_2^i)$ . Now,  $\mathcal{B}$  will forward either  $(m_0^i, m_1^i)$ ,  $(m_1^i, m_2^i)$ , or  $(m_2^i, m_0^i)$ , according to whether  $c = 0, 1$ , and  $2$ , respectively. There are several cases:

$c = 0$ : If  $\mathcal{A}$  guesses  $b' = 0$  or  $b' = 1$ ,  $\mathcal{B}$  forwards it as its guess. On the other hand, if  $\mathcal{A}$  guesses  $b' = 2$ —which is not consistent with  $\mathcal{B}$ 's options— $\mathcal{B}$  throws a random coin and answers with  $b' = 0$  or  $b' = 1$  with equal probability.

$c = 1$ : If  $\mathcal{A}$  guesses  $b' = 1$  or  $b' = 2$ ,  $\mathcal{B}$  forwards  $b' = 0$  or  $b' = 1$ , respectively. On the other hand, if  $\mathcal{A}$  guesses  $b' = 0$ , this is not consistent with  $\mathcal{B}$ 's strategy. So,  $\mathcal{B}$  chooses to answer  $b' = 0$  or  $b' = 1$  at random.

$c = 2$ : If  $\mathcal{A}$  guesses  $b' = 2$  or  $b' = 0$ ,  $\mathcal{B}$  forwards  $b' = 0$  or  $b' = 1$ , respectively, as its guess. On the other hand, if  $\mathcal{A}$  guesses  $b' = 1$ , then  $\mathcal{B}$  answers with  $b' = 0$  or  $b' = 1$  at random.

We now estimate  $\mathcal{B}$ 's success probability:

$$\begin{aligned} \mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk}} &= -1 + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-0}} = 0 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-1}} = 1 \right] \\ &= -1 + \frac{1}{3} \left\{ \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-0}} = 0 | c = 0 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-1}} = 1 | c = 0 \right] \right. \\ &\quad + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-0}} = 0 | c = 1 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-1}} = 1 | c = 1 \right] \\ &\quad \left. + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-0}} = 0 | c = 2 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-1}} = 1 | c = 2 \right] \right\} \end{aligned} \tag{1}$$

We compute each term:

$$\begin{aligned}
& \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-0}} = 0 \mid c = 0 \right] = \\
& \qquad \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-0}} = 0 \right] + \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-0}} = 2 \right] \\
& \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-1}} = 1 \mid c = 0 \right] = \\
& \qquad \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-1}} = 1 \right] + \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-1}} = 2 \right] \\
& \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-0}} = 0 \mid c = 1 \right] = \\
& \qquad \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-1}} = 1 \right] + \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-1}} = 0 \right] \\
& \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-1}} = 1 \mid c = 1 \right] = \\
& \qquad \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-2}} = 2 \right] + \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-2}} = 0 \right] \\
& \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-0}} = 0 \mid c = 2 \right] = \\
& \qquad \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-2}} = 2 \right] + \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-2}} = 1 \right] \\
& \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-1}} = 1 \mid c = 2 \right] = \\
& \qquad \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-0}} = 0 \right] + \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-0}} = 1 \right]
\end{aligned}$$

To be able to argue about the above equations, label the terms in equation  $i$  such that  $eq_i : LHS_i = P_i + \frac{1}{2}Q_i$ . We need to add all the  $LHS_i$  terms. First, note that the  $P_i$  terms are those that appear in the definition of  $\mathcal{A}$ 's advantage, and each appear twice. So  $P_1 + \dots + P_6 = 2X$ , where

$$X = \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-0}} = 0 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-1}} = 1 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-2}} = 2 \right].$$

Now, note that  $P_1, Q_1$ , and  $Q_2$  are probability values of complementary events, i.e.,  $Q_1 + Q_2 = 1 - P_1$ , and similarly  $Q_3 + Q_4 = 1 - P_3$ ,  $Q_5 + Q_6 = 1 - P_5$ . Therefore,  $Q_1 + \dots + Q_6 = 3 - X$ .

Putting it all together, we get that  $\sum_{i=1}^6 LHS_i = \frac{3}{2}(X + 1)$ . Substituting it into Equation 1, we get that

$$\mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk}} = -1 + \frac{1}{3} \left\{ \frac{3}{2}(X + 1) \right\} = \frac{1}{2}(-1 + X) = \frac{1}{2} \mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk}}.$$

For the converse reduction, now let  $\mathcal{A}$  be an adversary for LoR. We wish to show how to generate an adversary  $\mathcal{B}$  against LMR. Note that  $\mathcal{B}$  will activate  $\mathcal{A}$  as a subroutine, and at times,  $\mathcal{A}$  will submit encryption queries, which consist of a pair of messages  $(m_0^i, m_1^i)$ .  $\mathcal{B}$  will forward the query  $(m_0^i, m_0^i, m_1^i)$  as its query. If  $\mathcal{A}$  then guesses  $b' = 1$ ,  $\mathcal{B}$  forwards  $b' = 2$  as its guess. However, if  $\mathcal{A}$  guesses  $b' = 0$ , then  $\mathcal{B}$  guesses  $b' = 0$  or  $b' = 1$  at random.

By definition, we have that  $\mathcal{B}$ 's advantage is:

$$\mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk}} = -1 + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-0}} = 0 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-1}} = 1 \right] + \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-2}} = 2 \right].$$

We compute each probability:

$$\text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-}0} = 0 \right] = \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-}0} = 0 \right],$$

$$\text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-}1} = 1 \right] = \frac{1}{2} \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-}0} = 0 \right],$$

and

$$\text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk-}2} = 2 \right] = \text{Prob} \left[ \mathbf{Exp}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk-}1} = 1 \right],$$

So, it is clear that, in this reduction  $\mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk}} = \mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk}}$ .

To summarize, we get that, for attacks that require the same number of queries, and receive answers of same length:

$$2\mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk}} \geq \mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lmr-atk}} \geq \mathbf{Adv}_{\mathcal{SE}, \mathcal{A}_{\text{atk}}}^{\text{lor-atk}}.$$