CSA E0 235: Cryptography 2nd February, 2016

Chalk & Talk Session 1

Instructor: Arpita Patra *Submitted by: Pranav Nuti and Sayantan Khan*

1 Showing the equivalence of three notions of perfect security

1.1 Defining the notions

We'll start by first defining the notions in precise terms, and then motivating those definitions, if they're not sufficiently motivated.

Definition 1(Perfect Secrecy) An encryption scheme (Gen, Enc_k, Dec_k) is said to be perfectly secure if for all messages m in the message space, and for all ciphertexts c in the ciphertext space, the following holds true:

$$\mathbb{P}[M = m \mid C = c] = \mathbb{P}[M = m]$$

$\diamondsuit$

This definition makes sense because of the way we define the break model. One does not want the adversary to get any more information from the ciphertext than he/she already had before the ciphertext was intercepted.

Definition 2 (Perfect ciphertext indistinguishability) An encryption scheme (Gen, Enc_k, Dec_k) is said to possess ciphertext indistinguishability if for all pairs of messages m_1 and m_2 in the message space, and for all ciphertexts c in the ciphertext space, the following holds true:

$$\mathbb{P}[C = c \mid M = m_1] = \mathbb{P}[C = c \mid M = m_2]$$

$\diamondsuit$

This definition is also motivated rather naturally. In more informal terms, it just means that the probability that a given ciphertext c came from a message m_1 should be no different than the probability that the ciphertext came from another message m_2.

Since the third definition is a little involved, here's a more informal description of the description. This definition is modelled in the form of a game or an experiment with two parties: the adversary and the verifier. The games goes as follows:

1. The adversary picks any two messages m_0 and m_1 of his/her choice from the message space. He/She then gives the two messages to the verifier.

2. The verifier samples a random bit which is equally likely to be 0 or 1. Call the result of the sampling b. The verifier chooses to encrypt the message m_b. He/She generates a key using the Gen algorithm and encrypts the message using Enc_k algorithm. Call the ciphertext obtained c. He/She then sends c to the adversary.

3. Given the ciphertext c, the adversary has to guess which one of the messages did the verifier encrypt. The adversary makes a guess b'. If $b' = b$, the adversary wins, otherwise the verifier wins.

Ideally, one would like the adversary to never win, i.e. $\mathbb{P}[b' = b] = 0$, but that is a very unrealistic expectation because the adversary can always output b' by randomly sampling a bit. That will increase the winning chances to $\frac{1}{2}$. So now we change our expectation to $\mathbb{P}[b' = b] \leq \frac{1}{2}$. But that is also unrealistic, because for every adversary who wins the probability less than $\frac{1}{2}$, there exists another adversary, who uses the same strategy as the original adversary, but flips the output bit at the end, and hence wins with a probability greater than $\frac{1}{2}$. Hence, the only reasonable expectation is $\mathbb{P}[b' = b] = \frac{1}{2}$.

For a given adversary A and a given scheme Π, we define a random variable $\text{Priv}^{\text{coa}}_{A,\Pi}$ which is 1 if the the adversary wins, otherwise 0. Now we can give a formal definition.

Definition 3 (Perfect Adversarial Indistinguishability) An encryption scheme Π is said to have Perfect Adversarial Indistinguishability if for all adversaries A,

$$\mathbb{P}[\text{Priv}^{\text{coa}}_{A,\Pi}] = \frac{1}{2}$$

$\diamondsuit$

Now we come to why we have such a convoluted definition. Even though this seems unwieldy now, the power of this kind of definition lies in the fact that one can chain multiple adversaries and verifiers in this manner and construct proofs rather neatly. Reduction proofs like this are somewhat of a norm in computer science in general. A later proof will show exactly how this definition is rather elegant.

1.2 Proofs of equivalence

We'll begin by proving definition 1 and definition 2 are equivalent.

Claim 1 *If an encryption scheme (Gen, Enc_k, Dec_k) is perfectly secret, it also possesses perfect ciphertext indistinguishability.*

Proof If the scheme is perfectly secret, then for all messages m and all ciphertexts c,

$$\mathbb{P}[M = m \mid C = c] = \mathbb{P}[M = m]$$

Using Bayes theorem, we can write $\mathbb{P}[M = m \mid C = c]$ as $\frac{\mathbb{P}[C=c \mid M=m] \cdot \mathbb{P}[M=m]}{\mathbb{P}[C=c]}$. Plugging that into the original equation, we get,

$$\frac{\mathbb{P}[C = c \mid M = m] \cdot \mathbb{P}[M = m]}{\mathbb{P}[C = c]} = \mathbb{P}[M = m] \tag{1}$$

$$\iff \mathbb{P}[C = c \mid M = m] = \mathbb{P}[C = c] \tag{2}$$

Note that (1) holds true for all m and all c and all m. In particular, it holds for any pair m_1 and m_2 of messages, and for any ciphertext. We get

$$\mathbb{P}[C = c \mid M = m_1] = \mathbb{P}[C = c] = \mathbb{P}[C = c \mid M = m_2] \tag{3}$$

This completes the proof. ■

Now we'll prove the converse.

Claim 2 *If an encryption scheme (Gen, Enc_k, Dec_k) has perfect ciphertext indistinguishability, then it is perfectly secret.*

Proof Since $\mathbb{P}[C = c \mid M = m_1] = \mathbb{P}[C = c \mid M = m_2]$ is equal for all m_1 and m_2, call the quantity k_c. We'll show that $\mathbb{P}[C = c] = k_c$. By the law of total probability

$$\mathbb{P}[C = c] = \sum_{m \in M} \mathbb{P}[C = c \mid M = m] \cdot \mathbb{P}[M = m] \tag{4}$$

$$= k_c \sum_{m \in M} \mathbb{P}[M = m] \tag{5}$$

$$= k_c \tag{6}$$

Also, by Bayes theorem,

$$\mathbb{P}[M = m \mid C = c] = \frac{\mathbb{P}[C = c \mid M = m] \cdot \mathbb{P}[M = m]}{\mathbb{P}[C = c]} \tag{7}$$

$$= \frac{k_c \cdot \mathbb{P}[M = m]}{k_c} \tag{8}$$

$$= \mathbb{P}[M = m] \tag{9}$$

This proves the claim. ■

We have managed to show that definition 1 and definition 2 are equivalent. Now we need to show that definition 3 is equivalent to either one of them. First we'll show that definition 1 implies definition 3 and then we'll show that definition 3 implies definition 2.

Claim 3 *If a scheme* Π *is perfectly secret, then it has the adversarial indistinguishability property.*

Proof Let $\Pi = (Gen, Enc_k, Dec_k)$ be a perfectly secret encryption scheme. We need to show for all adversaries A, $\mathbb{P}[\mathrm{Priv}^{\mathrm{coa}}_{A,\Pi}] = \frac{1}{2}$.

Since A is an adversary who can use randomness in his/her attack, we'll assume that the source of that randomness is Y, a random variable which is completely independent of every other random variable in the system. For any adversary, the guessing algorithm is some function of the randomness Y and the challenge ciphertext c. In more formal terms, $b' = f(c, Y)$, where b' is the adversary's guess to the message sent.

But, because the scheme has perfect secrecy, by equation 2, C is independent of M. That means $f(c, Y)$ must be a random variable completely independent from b. That means b are b' are independent and $\mathbb{P}[b = b'] = \frac{1}{2}$. This shows that $\mathbb{P}[\mathrm{Priv}^{\mathrm{coa}}_{A,\Pi}] = \frac{1}{2}$ for all A. ■

Now all that is left is to show that definition 3 implies definition 2. This can be shown by proving the contrapositive of the claim.

Claim 4 *If* Π *is a scheme such that there exist* m_0, m_1 *and* c *for which* $\mathbb{P}[C = c \mid M = m_0] \neq \mathbb{P}[C = c \mid M = m_1]$, *then there exists an adversary* A *for which* $\mathbb{P}[\mathrm{Priv}^{\mathrm{coa}}_{A,\Pi}] > \frac{1}{2}$.

Proof Without loss of generality, assume

$$\mathbb{P}[C = c \mid M = m_0] > \mathbb{P}[C = c \mid M = m_1] \tag{10}$$

Now consider an adversary with the following strategy. He/She picks m_0 and m_1 and gives those to the verifier. After that, the adversary receives a challenge ciphertext c'. If $c' = c$, the adversary outputs 0, otherwise if $c \neq c'$, the adversary outputs a bit at random. What is the probability that the adversary wins the game.

$$\begin{aligned}
\mathbb{P}[b = b'] &= \mathbb{P}[b = b' \mid c = c'] \cdot \mathbb{P}[c = c'] + \mathbb{P}[b = b' \mid c \neq c'] \cdot \mathbb{P}[c \neq c'] && (11)\\
&= \mathbb{P}[b = 0 \mid c = c'] \cdot \mathbb{P}[c = c'] + \mathbb{P}[b = b' \mid c \neq c'] \cdot \mathbb{P}[c \neq c'] && (12)
\end{aligned}$$

But we know that $\mathbb{P}[b = b' \mid c \neq c'] = \frac{1}{2}$, because both b and b' are bits chosen uniformly at random. Now we'll show that $\mathbb{P}[b = 0] > \frac{1}{2}$. For equation 10, we have

$$\begin{aligned}
&\mathbb{P}[C = c \mid M = m_0] > \mathbb{P}[C = c \mid M = m_1] && (13)\\
\iff &\frac{\mathbb{P}[M = m_0 \mid C = c] \cdot \mathbb{P}[C = c]}{\mathbb{P}[M = m_0]} > \frac{\mathbb{P}[M = m_1 \mid C = c] \cdot \mathbb{P}[C = c]}{\mathbb{P}[M = m_1]} && (14)\\
\iff &\mathbb{P}[M = m_0 \mid C = c] > \mathbb{P}[M = m_1 \mid C = c] && (15)\\
\iff &\mathbb{P}[b = 0 \mid c = c'] > \mathbb{P}[b = 1 \mid c = c'] && (16)
\end{aligned}$$

But we also know that

$$\mathbb{P}[b = 0 \mid c = c'] + \mathbb{P}[b = 1 \mid c = c'] = 1 \tag{17}$$

This implies $\mathbb{P}[b = 0 \mid c = c'] > \frac{1}{2}$.
Plugging that into equation 12, we get

$$\mathbb{P}[b = b'] > \frac{1}{2}\mathbb{P}[c = c'] + \frac{1}{2}\mathbb{P}[c \neq c'] = \frac{1}{2} \tag{18}$$

We have shown an adversary who can win with a probability greater than $\frac{1}{2}$, and that completes the proof ■