CS6222 Cryptography

Topic: Chosen Plaintext Attack
Lecturer: Wei-Kai Lin (TA: Arup Sarker)

Date: September 17, 2024
Scriber: Chase Fickes

1 Secure Encryption Schemes

As opposed to our definition of perfect secrecy which assumes that the adversary receives only the ciphertext, we can create models based on more practical scenarios in which the adversary may have more information.

Definition 1 (Chosen Plaintext Attack (CPA))**.** Let $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ and define an experiment $\mathbf{Expr}_b^{\Pi,A}(1^n)$, where $n \in \mathbb{N}$, $b \in \{0,1\}$, and A is an NUPPT adversary, as follows:

Experiment $\mathbf{Expr}_b^{\Pi,A}$:

1. $k \leftarrow \mathbf{Gen}(1^n)$
2. $(m_0, m_1, \mathbf{states}) \leftarrow A^{\mathbf{Enc}_k(\cdot)}(1^n)$
3. $c_b \leftarrow \mathbf{Enc}_k(m_b)$
4. $b' \leftarrow A^{\mathbf{Enc}_k(\cdot)}(c, \mathbf{state})$

Then Π is a CPA if, for all NUPPT A,

$$\{\mathbf{Expr}_0^{\Pi,A}\}_n \approx_c \{\mathbf{Expr}_1^{\Pi,A}\}_n.$$

The idea here is that the adversary is able to do more than eavesdrop: they are able to ask an oracle for encryptions as well. For an encyption scheme to be secure, it should stand that the encryption of any two messages should be computationally indistinguishable [KL21].

Theorem 2 (CPA-secure Encryption from PRF)**.** *If there exists a family of PRF such that* $\boldsymbol{PRF} = \{f_s \mid \{0,1\}^{|s|} \to \{0,1\}^{|s|}\}_{s\in\{0,1\}^*}$*, then there must also exist CPA-secure encryption* $(\boldsymbol{Gen}, \boldsymbol{Enc}, \boldsymbol{Dec})$ *such that*

- $\boldsymbol{Gen}(1^n)$*:* $k \leftarrow \{0,1\}^n$
- $\boldsymbol{Enc}_k(m; r)$*: given* $r \leftarrow \{0,1\}^n$*,* $c := (m \oplus f_k(r); r)$
- $\boldsymbol{Dec}(c)$*: given* $c = (c'; r)$*,* $m' := c' \oplus f_k(r)$

We will show why this is the case.

Proof. We want to show that $\mathbf{Expr}_0^{\Pi,A} \approx_c \mathbf{Expr}_1^{\Pi,A}$. To do this, we will define hybrid experiments H_b^A as follows:

Hybrid H_b^A:

1. $R \leftarrow RF_n$

2. $(m_0, m_1, \textbf{state}) \leftarrow A^{O(\cdot)}(1^n)$, where O is an oracle such that $O(m; r) := (m \oplus R(r); r)$
3. $c \leftarrow O(m_b)$
4. $b' \leftarrow A^{O(\cdot)}(c, \textbf{state})$

By oracle indistinguishability, we get that $\textbf{Expr}_0^{\Pi,A} \approx_c H_0^A$ and $\textbf{Expr}_1^{\Pi,A} \approx_c H_1^A$. With this, it should suffice to show that $H_0^A \approx_c H_1^A$ to complete the proof. To do this, we will define a set $S := \{r \in \{0,1\}^n \mid R(r) \text{ is queried by } A^{O(\cdot)}\}$ and we now want to show that $|\Pr[H_0^A = 1] - \Pr[H_1^A = 1]|$ is negligible for all NUPPT A.

$$\begin{aligned} \Pr[H_0^A = 1] &= \Pr[H_0^A = 1 \cap r* \in S] + \Pr[H_0^A = 1 \cap r* \notin S] \\ &\leq \Pr[r* \in S] + \Pr[H_0^A \mid r* \notin S] \cdot \Pr[r* \notin S] \\ &= \beta + \Pr[H_0^A = 1 \mid r* \notin S](1 - \beta) \end{aligned} \tag{1}$$

Where $\beta = |S|/2^n$. We also know that $\Pr[H_0^A = 1 \mid r* \notin S] = \Pr[H_1^A = 1 \mid r* \notin S]$, so we can substitute into the last step by writing

$$\begin{aligned} \Pr[H_0^A = 1] &\leq \beta + \Pr[H_1^A = 1 \mid r* \notin S](1 - \beta) \\ &\leq \beta + Pr[H_1^A = 1 \cap r* \notin S] \end{aligned} \tag{2}$$

Since β is negligible, this gives us that $|\Pr[H_0^A = 1] - \Pr[H_1^A = 1]| \leq \beta$, thus concluding that $\textbf{Expr}_0^{\Pi,A} \approx_c \textbf{Expr}_1^{\Pi,A}$.

□

References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography.* CRC Press, 2021.