CSE5014: Cryptography and Network Security

2024 Spring Semester Summary notes

One-sentence definition of *Cryptography*: "Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries." – R.L. Rivest

Milestone papers:

[1] C.E. Shannon, Communication theory of secrecy systems, *The Bell system technical journal*, 28(4): 656-715, 1949.

[2] W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, 22(6): 29-40, 1976.

[3] R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 21(2): 120-126, 1978.

and many others ...

Three principles of modern cryptography:

1. **Formal definitions**: precise, mathematical model and definition of what security means.
2. **Precise assumptions**: should be clearly stated and unambiguous.
3. **Proofs of security**: make it possible to move away from "design-break-tweak".

A typical cryptographic definition contains two parts: security guarantee/goal, and threat model. The former means what we want to achieve and/or what we want to prevent the attacker from achieving, and the latter means what (real-world) capabilities the attacher is assumed to have.

Definition 1. *A* private-key encryption *scheme is defined by a message space $\mathcal{M}$ and three algorithms (Gen, Enc, Dec):*

- *Gen (key-generation algorithm): generates the private key k;*
- *Enc (encryption algorithm): takes key k and message $m \in \mathcal{M}$ as input; outputs ciphertext c: $c \leftarrow Enc_k(m)$;*
- *Dec (decryption algorithm): takes key k and ciphertext c as input; outputs m': $m' = Dec_k(c)$.*

Probability review: A *random variable* (r.v.) is a variable that takes on (discrete) values with certain probabilities. For an r.v., a *probability distribution* is the distribution of probabilities that are specified to all possible values of the r.v. such that each probability must be between 0 and 1, and the probabilities must sum to 1. An *event* is a particular occurrence in some experiment, and $\Pr[E]$ denotes the probability that the event E occurs. The *conditional probability* is the probability that one event occurs given that some other event occurred, and the corresponding formula is

$$\Pr[A|B] = \Pr[A \text{ and } B]/\Pr[B].$$

Two r.v.'s X and Y are called *independent* if for all possible values x, y, it holds that

$$\Pr[X = x|Y = y] = \Pr[X = x].$$

By the formula for the conditional probability, an equivalent condition of independence of two r.v.'s is

$$\Pr[X = x \text{ and } Y = y] = \Pr[X = x] \cdot \Pr[Y = y].$$

Given that $E_1, E_2, \ldots, E_n$ are a partition of all possibilities. Then for any event A, it holds that

$$\Pr[A] = \sum_i \Pr[A \text{ and } E_i] = \sum_i \Pr[A|E_i] \cdot \Pr[E_i].$$

This is called the *law of total probability*. For a private-key encryption scheme, the key K can be viewed as the r.v. that ranges over the key space $\mathcal{K}$, and the plaintext M is the r.v. that ranges over the plaintext space $\mathcal{M}$. Note that the two random variables M and K are *independent*, i.e., the message that a party sends does NOT depend on the key used to encrypt the message.

Fix an encryption scheme (Gen, Enc, Dec), and some distribution for M. Consider the following randomized experiment:

1. Choose a message m according to the given distribution
2. Generate a key k using the algorithm Gen
3. Compute $c \leftarrow Enc_k(m)$

Then this defines a distribution on the ciphertext. Let C be an r.v. denoting the value of the ciphertext in this experiment. Thereby, the set of all possible values of the ciphertext constitutes the ciphertext space $\mathcal{C}$

Suppose that $k \in \{0,1\}^n$, $m \in \{0,1\}^\ell$, and $c \in \{0,1\}^L$. With this setting above, how can we define what it means for an encryption scheme (Gen, Enc, Dec) over the plaintext space $\mathcal{M}$ to be *secure* against a (single) ciphertext-only attack?

The definition of *perfect secrecy* is the following, which means that by observing the ciphertext, the attacker's knowledge about the distribution of M should not be changed.

Definition 2 (Definition 1.5)**.** *An encryption scheme (Gen, Enc, Dec) with the message space $\mathcal{M}$ and the ciphertext space $\mathcal{C}$ is* perfectly secure *if for every distribution over $\mathcal{M}$, for every message $m \in \mathcal{M}$, and every $c \in \mathcal{C}$ with $\Pr[C = c] > 0$, it holds that*

$$\Pr[M = m | C = c] = \Pr[M = m].$$

Essentially, perfect secrecy means that the ciphertext c reveals *zero additional information* about the plaintext m. An equivalent version of the definition above is the following.

Definition 3 (Definition 1.5')**.** *For every set $M \subseteq \{0,1\}^\ell$ of plaintexts, and for every strategy used by Eve, if we choose at random $x \in M$ and a random key $k \in \{0,1\}^n$, then the probability that Eve guesses x correctly after seeing $Enc_k(x)$ is* at most $1/|M|$*, i.e.,*

$$\Pr[Eve(Enc_k(x)) = x] \leq 1/|M|.$$

There are another two equivalent versions of the definition of perfect secrecy.

Definition 4 (Definition 1.6)**.** *An encryption scheme (Gen, Enc, Dec) with the message space $\mathcal{M}$ and the ciphertext space $\mathcal{C}$ is* perfectly secure *if and only if for every two distinct plaintexts $\{x_0, x_1\} \in \mathcal{M}$, and for every strategy used by Eve, if we choose at random $b \in \{0,1\}$ and a random key $k \in \{0,1\}^n$, then the probability that Eve guesses x_b correctly after seeing the ciphertext $c = Enc_k(x_b)$ is at most $1/2$.*

Definition 5 (Definition 1.7)**.** *An encryption scheme (Gen, Enc, Dec) is* perfectly secure *if and only if for every pair of plaintexts $x_0, x_1 \in \mathcal{M}$, it holds that*

$$Enc_{k \leftarrow U_n \mathcal{K}}(x_0) \equiv Enc_{k \leftarrow U_n \mathcal{K}}(x_1).$$

Recall that two probability distributions X, Y over $\{0,1\}^\ell$ are identical, denoted by $X \equiv Y$, if for every $y \in \{0,1\}^\ell$, it holds that $\Pr[X = y] = \Pr[Y = y]$.

The following theorem proves the equivalence of Definition 1.5' and Definition 1.6.

Theorem 1 (Theorem 1.8)**.** *An encryption scheme* (Gen, Enc, Dec) *is* perfectly secure *if and only if for each* $b \in \{0,1\}$*,*

$$\Pr[Eve(Enc_k(x_b)) = x_b] \leq 1/2.$$

Proof. "only if" part: this is the special case that $|M| = 2$ in Definition 1.5'.

"if" part: Suppose that the encryption scheme (Gen, Enc, Dec) is NOT perfectly secure, by Definition 1.5', this means that there exists some set M and some strategy for Eve to guess a plaintext chosen from M with probability larger than $1/|M|$. We need prove that there is also some set M' of size 2, and there exists some strategy Eve' for Eve to guess a plaintext chosen from M' with probability larger than $1/2$.

Fix $x_0 = 0^\ell$ and pick x at random from M. Then it holds that for random key k and message $x_1 \in M$,

$$\Pr_{k \leftarrow \{0,1\}^n,\ x \leftarrow M}[Eve(Enc_k(x)) = x] \geq 1/|M|.$$

On the other hand, for very choice of k, $x' = Eve(Enc_k(x_0))$ is a fixed string independent on the choice of x. So if we pick x at random from M, the probability that $x = x'$ is at most $1/|M|$, i.e.,

$$\Pr_{k \leftarrow \{0,1\}^n,\ x \leftarrow M}[Eve(Enc_k(x_0)) = x] \leq 1/|M|.$$

Due to the linearity of expectation, there exists some x_1 satisfying

$$\Pr[Eve(Enc_k(x_1)) = x_1] > \Pr[Eve(Enc_k(x_0)) = x_1]. \text{ (Why?)}$$

We now define a new attacker Eve' as :

$$Eve'(c) = \begin{cases} x_1, & \text{if } Eve(c) = x_1, \\ x_i,\ i \in \{0,1\} \text{ at random}, & \text{otherwise.} \end{cases}$$

Then the probability that $Eve'(Enc_k(x_b)) = x_b$ is larger than $1/2$ (Why?).

□

One-time Pad. The XOR operation is defined as the addition mod 2, i.e., $a \oplus b = a + b \bmod 2$. For a message x and a key k with $n = |k| = |x|$, the

encryption algorithm $Enc : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is $Enc_k(x) = x \oplus k$, and the decryption algorithm is $Dec_k(y) = y \oplus k$, where $\oplus$ denotes the bitwise XOR operation.

Theorem 2 (Theorem 1.9)**.** *One-time pad is* perfectly secure*.*

Proof. By Definition 1.7, it suffices to prove that for every $x \in \{0,1\}^n$, the distribution $Y_x = Enc_{U_n}(x)$ is uniformly distributed.

Let $y \in \{0,1\}^n$, we need show that

$$\Pr_{k \leftarrow_R \{0,1\}^n}[x \oplus k - y] = 2^{-n}.$$

Since there is a unique single value of $k = x \oplus y$, the probability that the equation is true is 2^{-n}. □

Proof. [Alternative proof] By Definition 1.5, it suffices to prove $\Pr[M = m|C = c] = \Pr[C = c]$ for arbitrary distribution over $\mathcal{M} = \{0,1\}^n$ and arbitrary $m, c \in \{0,1\}^n$.

First, by Law of total probability, we have

$$\begin{aligned}
&\Pr[C = c] \\
&= \sum_{m'} \Pr[C = c|M = m'] \cdot \Pr[M = m'] \\
&= \sum_{m'} \Pr[K = m' \oplus c] \cdot \Pr[M = m'] \\
&= \sum_{m'} 2^{-n} \cdot \Pr[M = m'] \\
&= 2^{-n}.
\end{aligned}$$

Then we have

$$\begin{aligned}
&\Pr[M = m|C = c] \\
&= \Pr[C = c|M = m] \cdot \Pr[M = m]/\Pr[C = c] \\
&= \Pr[K = m \oplus c] \cdots \Pr[M = m]/2^{-n} \\
&= 2^{-n} \cdot \Pr[M = m]/2^{-n} \\
&= \Pr[M = m].
\end{aligned}$$

Therefore, one-time pad is perfectly secure. □

Now we have a "clean" definition of security, together with a construction of encryption scheme that is perfectly secure. However, this is not the end of cryptography, since several limitations exist: the key length is as the same as the length of plaintexts; one-time pad leaks information if the same key is used for multiple plaintexts; one-time pad can be easily broken by a known-plaintext attack... The following theorem states the first drawback in terms of key length, i.e., for perfectly secure encryption schemes, the key length cannot be shorter than the length of plaintexts by even one bit.

Theorem 3 (Theorem 1.10)**.** *There is* no *perfectly secure encryption schemes* (Gen, Enc, Dec) *with* n*-bit plaintexts and* $(n-1)$*-bit keys.*

Proof. Suppose that (Gen, Enc, Dec) is such an encryption scheme with n-bit plaintexts and $(n-1)$-bit keys. Denote by Y_0 the distribution of $Enc_{U_{n-1}}(0^n)$ and by S_0 the support of Y_0.

Since there are only 2^{n-1} possible keys, we have $|S_0| \leq 2^{n-1}$. Now for every key k the function $Enc_k(\cdot)$ is a one-to-one function and hence the image size of the ciphertexts is $\geq 2^n$. This means that for every k, there must exist an plaintext x such that $Enc_k(x) \notin S_0$. Fix such a key k and the plaintext x, then the distribution $E_{U_{n-1}}(x)$ does not have the same support as Y_0. Therefore, it is not identical to Y_0.

□

To overcome the limitations of perfect secrecy, it is a good idea to examine whether we can relax these assumptions. Namely, we may say that an encryption scheme is ϵ-statistically secure if the probability that Eves guesses correctly which of the two messages was encrypted is at most $1/2 + \epsilon$, with a tiny advantage ϵ.

Definition 6 (Definition 2.1)**.** *Let* X *and* Y *be two distributions over* $\{0,1\}^n$*. The* statistical distance *of* X *and* Y*, denoted by* $\Delta(X, Y)$ *is defined to be*

$$\max_{T \subseteq \{0,1\}^n} |\Pr[X \in T] - \Pr[Y \in T]|.$$

If $\Delta(X, Y) \leq \epsilon$*, we denote that* $X \equiv_\epsilon Y$*.*

The following lemma give a systematic way to determine the statistical distance between two distributions.

Lemma 4 (Lemma 2.3)**.**

$$\Delta(X,Y) = \frac{1}{2} \sum_{w \in Supp(X) \cup Supp(Y)} |\Pr[X = w] - \Pr[Y = w]|,$$

where $Supp(X)$ denotes the support of the distribution X.

Proof. For every set $T \subseteq \{0,1\}^n$, define

$$\Delta_T(X,Y) = |\Pr[X \in T] - \Pr[Y \in T]|.$$

Then by Definition 2.1, we have $\Delta(X,Y) = \max_{T \subseteq \{0,1\}^n} \Delta_T(X,Y)$. Note that since $\Pr[X \in T^c] = 1 - \Pr[X \in T]$, we have $\Delta_{T^c}(X,Y) = \Delta_T(X,Y)$. Let $T = \{w : \Pr[X = w] > \mathrm{Y} = \mathrm{w}\}$, then we have

$$\begin{aligned}
&\frac{1}{2} \sum_{w \in Supp(X) \cup Supp(Y)} |\Pr[X = w] - \Pr[Y = w]| \\
&= \frac{1}{2} \sum_{w \in T} (\Pr[X = w] - \Pr[Y = w]) + \frac{1}{2}(\Pr[Y = w] - \Pr[X = w]) \\
&= \frac{1}{2}(\Delta_T(X,Y) + \Delta_{T^c}(X,Y)) \\
&= \Delta_T(X,Y) \\
&\leq \Delta(X,Y). \qquad (*)
\end{aligned}$$

On the other hand, let S be the set achieving the maximum of $\Delta_S(X,Y)$, i.e., $\Delta(X,Y) = \Delta_S(X,Y)$. Without loss of generality, assume that $\Pr[X \in S] \geq \Pr[Y \in S]$ (otherwise, take the complement of S). Then we have

$$\begin{aligned}
2\Delta(X,Y) &= \Delta_S(X,Y) + \Delta_{S^c}(X,Y) \\
&= \Pr[X \in S] - \Pr[Y \in S] + \Pr[Y \in S^c] - \Pr[X \in S^c] \\
&= \sum_{w \in S} (\Pr[X = w] - \Pr[Y = w]) + \sum_{w \in S^c} (\Pr[Y = w] - \Pr[X = w]) \\
&\leq \sum_{w \in S} |\Pr[X = w] - \Pr[Y = w]| + \sum_{w \in S^c} |\Pr[Y = w] - \Pr[X = w]| \\
&= \sum_{w} |\Pr[X = w] - \Pr[Y = w]|. \qquad (**)
\end{aligned}$$

Therefore, by (*) and (**), the conclusion is proved. □

Note that it is clear that $0 \leq \Delta(X,Y) \leq 1$ and $\Delta(X,Y) = 0$ if $X = Y$. One may try proving that $0 \leq \Delta(X,Y) \leq \Delta(X,Z) + \Delta(Z,Y)$, and further prove that the statistical distance is a *metric*.

Definition 7 (Definition 2.2 ϵ-statistical security)**.** *An encryption scheme* (Gen, Enc, Dec) *is* ϵ-statically secure *if and only if for every pair of plaintexts* m, m'*, it holds that* $Enc_{U_n}(m) \equiv_\epsilon Enc_{U_n}(m')$*.*

Lemma 5 (Lemma 2.4)**.** *Eve has at most* $1/2 + \epsilon$ *success probability if and only if for every pair of* m_1, m_2*, it holds that*

$$\Delta(Enc_{U_n}(m_1), Enc_{U_n}(m_2)) \leq 2\epsilon.$$

Proof. Suppose that Eve has $1/2 + \epsilon$ success probability with the two messages m_1, m_2. Let $p_{i,j} = \Pr[Eve(Enc_{U_n}(m_i)) = j]$. Then we have

$$\begin{aligned} p_{1,1} + p_{1,2} &= 1 \\ p_{2,1} + p_{2,2} &= 1 \\ (1/2)p_{1,1} + (1/2)p_{2,2} &\leq 1/2 + \epsilon. \end{aligned}$$

The last two together imply that

$$p_{1,1} - p_{2,1} \leq 2\epsilon,$$

which means that if we let T be the set $\{c : \ Eve(c) = 1\}$, then T demonstrates that $\Delta(Enc_{U_n}(m_1), Enc_{U_n}(m_2)) \leq 2\epsilon$.

Similarly, if we have such a set T, we can define an attacker from it that succeeds with probability $1/2 + \epsilon$.

□

Similar to Theorem 1.10, the following result demonstrates that the limitation still exists if we consider ϵ-statistical security instead of perfect security.

Theorem 6 (Theorem 2.5)**.** *Let* (Gen, Enc, Dec) *be a valid encryption scheme with the encryption algorithm* $Enc : \{0,1\}^n \times \{0,1\}^{n+1} \to \{0,1\}^*$*. Then there exist plaintexts* m_1, m_2 *such that* $\Delta(Enc_{U_n}(m_1), Enc_{U_n}(m_2)) > 1/2$*.*

Proof. **Fact**. For a r.v. Y, if $E[Y] \leq \mu$, then $\Pr[Y \leq \mu] > 0$.

Let $m_1 = 0^{n+1}$, and let $S = Supp(Enc_{U_n}(m_1))$, then $|S| \leq 2^n$.

We choose a random message $m \leftarrow_R \{0,1\}^{n+1}$ and define the following 2^n random variables for every k:

$$T_k(m) = \begin{cases} 1, & \text{if } Enc_k(m) \in S, \\ 0, & \text{otherwise.} \end{cases}$$

Since for every k, the encryption function $Enc_k(\cdot)$ is a one-to-one function, we have $\Pr[T_k = 1] \leq 1/2$. Define $T = \sum_{k \in \{0,1\}^n} T_k$, then

$$E[T] = E[\sum_k T_k] = \sum_k E[T_k] \leq 2^n/2.$$

This means that the probability $\Pr[T \leq 2^n/2] > 0$. In other words, there exists an m such that $\sum_k T_k(m) \leq 2^n/2$. For such an m, at most half of the keys k satisfy $Enc_K(m) \in S$, i.e.,

$$\Pr[Enc_{U_n}(m) \in S] \leq 1/2.$$

Since $\Pr[Enc_{U_n}(0^{n+1}) \in S] = 1$, we then have

$$\Delta(Enc_{U_n}(0^{n+1}), Enc_{U_n}(m)) \geq 1/2.$$

□

Now we consider a standard form of security definition: we formulate an experiment on the basis of Definition 1.6.

Let $\Pi = (Gen, Enc, Dec)$ be an encryption scheme with message space $\mathcal{M}$, and A an adversary. Define a *randomized* experiment $PrivK_{A,\Pi}$:

1. A outputs $m_0, m_1 \in \mathcal{M}$
2. $k \leftarrow Gen$, $b \leftarrow \{0,1\}$, $c \leftarrow Enc_k(m_b)$
3. $b' \leftarrow A(c)$

Adversary A succeeds if $b = b'$, and we say the experiment *evaluates to* 1 ($PrivK_{A,\Pi} = 1$) in this case.

If we define Π is *perfectly indistinguishable* if for *all* attackers (algorithm) A, it holds that

$$\Pr[PrivK_{A,\Pi} = 1] \leq 1/2.$$

Then we have exactly the definition of perfect security in the form of $PrivK_{A,\Pi}$.

Claim. Π is *perfectly indistinguishable* if and only if Π is *perfectly secure*.

Now that *statistical security* does not allow us to break the impossibility result, namely, the key length should be the same as the length of plaintexts. The idea is that it would be OK if an ecntryption scheme leaked information with *tiny probability* to eavesdroppers with *bounded computational resources*. More precisely, it is allowed that security may fail with tiny probability, and only "efficient" attackers exist. There are two approaches: concrete security and asymptotic security. For concrete (t, ϵ)-indistinguishability, two concrete parameters are involved: security may fail with probability $\leq \epsilon$, and we restrict attention to attackers running in time $\leq t$. However, this concrete setting does *not* lead to a clean theory: this may be sensitive to exact computational model, and Π can be (t, ϵ)-secure for many choices of the parameters t, ϵ.

We focus on asymptotic security, with respect to a *security parameter* n. For now, we view n as the key length, which may be fixed by honest parties at initialization, and assumebly be known by adversary. Then the running time of all parties, and the success probability of the adversary, are both measured by functions in terms of n. For the sake of defining *computational indistinguishability*, it is required that security may fail with probability *negligible* in n, and attackers are assumbed to be running in time (at most) *polynomial* in n.

A function $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ is (at most) *polynomial* if there exists an integer c such that $f(n) < n^c$ for large enough n. A function $f : \mathbb{Z}^+ \to [0, 1]$ is *negligible* if every polynnomial p it holds that $f(n) < 1/p(n)$ for large enough n. A typical example of negligible functions if $f(n) = poly(n) \cdot 2^{-cn}$.

We borrow the concept of "efficient" algorithms from complexity theory as "(probabilistic) polynomial-time (PPT)" algorithms. Two convenient closure properties are useful: $poly * poly = poly$ (poly-many calls to PPT subroutine is still PPT), and $poly * negl = negl$ (poly-many calls to subroutine that fails with negligible probability fails with negligible probability overall).

Now we are ready to define *computational indistinguishability* in terms of the experiment $PrivK_{A,\Pi}(n)$. Let $\Pi = (Gen, Enc, Dec)$ be an encryption scheme with message space $\mathcal{M}$ and A an adversary. Define a randomized experiment $PrivK_{A,\Pi}(n)$:

1. $A(1^n)$ outputs $m_0, m_1 \in \{0, 1\}^*$ of equal length

2. $k \leftarrow Gen(1^n)$, $b \leftarrow \{0,1\}$, $c \leftarrow Enc_k(m_b)$
3. $b' \leftarrow A(c)$

Adversary A succeeds if $b = b'$, and we say the experiment evaluates to 1 ($PrivK_{A,\Pi}(n) = 1$) in this case.

Definition 8 (Definition 3.1)**.** Π *is* computationally indistinguishable *(aka* EAV-secure*) if for all PPT attackers (algorithms) A, there is a negligible function ϵ such that*

$$\Pr[PrivK_{A,\Pi}(n) = 1] \leq 1/2 + \epsilon(n).$$

Example. Consider a scheme where the best attack is brute-force search over the key space (thus the attack algorithm runs in $O(2^n)$), and $Gen(1^n)$ generates a uniform n-bit key. Thus, if A runs in polynomial time $t(n)$, then we have $\Pr[PrivK_{A,\Pi}(n) = 1] \leq 1/2 + O(t(n)/2^n)$. The scheme is EAV-secure: for any polynomial t, the function $t(n)/2^n$ is negligible.

Example. Consider a scheme and a particular attacker A that runs for n^3 minutes and breaks the scheme with probability $2^{40}2^{-n}$. This does not contradict asymptotic security since $2^{40}2^{-n}$ is a negligible function in n. For $n = 40$, A breaks with probability 1 in approximately 6 weeks; $n = 50$, A breaks with probability $1/1000$ in approximately 3 months; $n = 500$, A breaks with probability 2^{-500} in about 200 years. This explains why computational indistinguishability may lead to real-world security with parameters properly chosen.

To build an encryption scheme, we introduce a new cryptographic primitive, *pseudorandom generator* (PRG). To this end, we define pseudorandomness asymptotically.

Definition 9 (Definition 3.2)**.** *Let D_n be a ditribution over $p(n)$-bit strings. $\{D_n\}$ is* pseudorandom *if for all PPT distinguishers A, there is a negligible function ϵ such that*

$$|\Pr_{x \leftarrow D_n}[A(x) = 1] - \Pr_{x \leftarrow U_{p(n)}}[A(x) = 1]| \leq \epsilon(n),$$

where $U_{p(n)}$ denotes the uniform distributio on $p(n)$-bit strings.

Definition. A *PRG* is an efficient, deterministic algorithm that expands a short, *uniform* seed into a longer, *pseudorandom* output. Let G be a deterministic, poly-time algorithm that expands the length of input, i.e.,

$|G(x)| = p(|x|) > |x|$. For all efficient distinguishers A, there is a negligible function ϵ such that

$$|\Pr_{x \leftarrow U_n}[A(G(x)) = 1] - \Pr_{y \leftarrow U_{p(n)}}[A(y) = 1]| \leq \epsilon(n),$$

In other words, no efficient A can distinguish whether it is given $G(x)$ for a uniform x or a uniform string y.

Now we have an encryption scheme, i.e., *pseudo one-time pad*, which can be proved to be EAV-secure.

Let G be a deterministic algorithm with $|G(k)| = p(|k|)$.
$Gen(1^n)$: output uniform n-bit key k. (security parameter n, message space $\{0,1\}^{p(n)}$);
$Enc_k(m)$: output $G(k) \oplus m$;
$Dec_k(c)$: output $G(k) \oplus c$.

Theorem 7 (Theorem 3.3)**.** *If G is a pseudorandom generator (PRG), then the pseudo one-time pad (pseudo-OTP) Π is* EAV-secure.

Proof. We use reduction to prove the result, and the proof idea is: by assuming that there is an efficient attacker A who "breaks" the pseudo-OTP scheme (this means that it is not EAV-secure), we use A as a subroutine to build an efficient D that "breaks" *pseudorandomness* of G. However, by the assumption that G is a PRG, no such a D exists. Thus, no such an A can exist.

Suppose to the contrary that there exists an efficient attacker A such that

$$\Pr[PrivK_{A,\Pi}(n) = 1] > 1/2 + 1/poly(n).$$

(Note that Π is then not EAV-secure.) This means that

$$\Pr[A(Enc_{U_n}(m)) = 1] - \Pr[A(U_{p(n)}) = 1] > 1/poly(n),$$

which further implies that

$$|\Pr[A(G(U_n) \oplus m) = 1] - \Pr[A(U_{p(n)}) = 1]| > 1/poly(n).$$

We define a distinguisher $D : \{0,1\}^{p(n)} \to \{0,1\}$ as $D(y) = A(y \oplus m)$, which means $A(z) = D(z \oplus m)$. Note that D is also efficient. But we have

$$|\Pr[D(G(U_n)) = 1] - \Pr[D(U_{p(n)} \oplus m) = 1]| > 1/poly(n).$$

Since $U_{p(n)} \oplus m \equiv U_{p(n)}$, this contradicts the assumption that G is a PRG.

We may have an alternative form of proof by reduction. The idea is: by assuming that G is a PRG, we fix some arbitrary efficient A attacking the pseudo-OTP scheme, and then use A as a subroutine to build an efficient D attacking G. This thereby relates the distinguishing probability of D to the attacking success probability of A. By assumption of PRG, the distinguishing probability of D must be negligible, and this therefore bounds the success probability of A.

Let $\mu(n) = \Pr[PrivK_{A,\Pi}(n) = 1]$. If the distribution of $y = G(x)$ is pseudo-random, then the view of A is exactly the same as in $PrivK_{A,\Pi}(n)$, i.e.,

$$\Pr_{x \leftarrow U_n}[D(G(x)) = 1] = \mu(n).$$

If the distribution of y is uniform, then A succeeds with probability exactly $1/2$, i.e.,

$$\Pr_{y \leftarrow U_{p(n)}}[D(y) = 1] = 1/2.$$

Since G is a PRG, we have

$$|\mu(n) - 1/2| \leq negl(n),$$

and it then follows that

$$\Pr[PrivK_{A,\Pi}(n) = 1] \leq 1/2 + negl(n).$$

Therefore, the encryption scheme Π is EAV-secure.

□

By Theorem 3.3, the pseudo-OTP is EAV-secure, and has a key shorter than the message, but still has the second limitation that key can only be used once. We will keep the security goal the same, but strengthen the threat model, by defining multiple-message indistinguishability.

Let $\Pi = (Gen, Enc, Dec)$ be an encryption scheme and A an adversary. Define a randomized experiment $PrivK^{mult}_{A,\Pi}(n)$:

1. $A(1^n)$ outputs two vectors $(m_{0,1}, \ldots, m_{0,t})$ and $(m_{1,1}, \ldots, m_{1,t})$. It is required that $|m_{0,i}| = |m_{1,i}|$ for all i.
2. $k \leftarrow Gen(1^n)$, $b \leftarrow \{0, 1\}$, and for all i, $c_i \leftarrow Enc_k(m_{b,i})$.
3. $b' \leftarrow A(c_1, \ldots, c_t)$.

Adversary A succeeds if $b = b'$, and the experiment evaluates to 1 in this case.

Definition 10 (Definition 3.4)**.** Π *is* multiple-message indistinguishable *if for all PPT attackers A, there is a negligible function ϵ such that*

$$\Pr[PrivK^{mult}_{A,\Pi}(n) = 1] \leq 1/2 + \epsilon(n).$$

Question: Show that the pseudo-OTP scheme is not multiple-message indistinguishable.

Instead of working with multiple-message security, we define a stronger notion of *CPA-security*, i.e., security against chosen-plaintext attacks. This is nowadays the minimal notion of security that an encryption scheme should satisfy. In practice, there are many ways an attacker can influence what gets encrypted, and chosen-plaintext attacks encompass such influences.

Let $\Pi = (Gen, Enc, Dec)$ be an encryption scheme and A an adversary. Define a randomized experiment $PrivKCPA_{A,\Pi}(n)$:

1. $k \leftarrow Gen(1^n)$.
2. $A(1^n)$ interacts with an *encryption oracle* $Enc_k(\cdot)$, and then outputs m_0, m_1 of the same length.
3. $b \leftarrow \{0,1\}$, $c \leftarrow Enc_k(m_b)$, give c to A.
4. A can continue to interact with $Enc_k(\cdot)$.
5. A outputs b'.

Adversary A succeeds if $b = b'$, and the experiment evaluates to 1 in this case.

Definition 11 (Definition 4.1)**.** Π *is* secure against chosen-plaintext attacks *(CPA-secure) if for all PPT attackers A, there is a negligible function ϵ such that*

$$\Pr[PrivKCPA_{A,\Pi}(n) = 1] \leq 1/2 + \epsilon(n).$$

At the first glance, this definition of security seems impossible. Consider the following attacker A: use a chosen-plaintext attack to get $c_0 = Enc_k(m_0)$ and $c_1 = Enc_k(m_1)$. Output m_0, m_1, and get the challenge ciphertext c. If $c = c_0$, output 0, and output 1 if $c = c_1$. Then A succeeds with probability 1?

Note that this attack only works if encryption is deterministic. Thus, to achieve CPA-security, randomized encryption must be used! To build an encryption scheme that is CPA-secure, we introduce another cryptographic primitive called *pseudorandom function* (PRF).

Informally, a *pseudorandom function* looks like a random function uniformly picked from the set $Func_n$ of all functions from $\{0,1\}^n$ to $\{0,1\}^n$. By a counting argument, $|Func_n| = 2^{n \cdot 2^n}$. Uniformly choosing a function $f \in Func_n$ is equivalent to choosing $f(x)$ uniformly in $\{0,1\}^n$ for each $x \in \{0,1\}^n$, i.e., filling up the function table with uniform bits for the $n \cdot 2^n$ blanks. It does not make sense to talk about any fixed function being *pseudorandom*. We look instead at keyed functions: by choosing uniformly the key, the keyed function looks like random.

Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient deterministic algorithm. Define $F_k(x) = F(k,x)$, where the first input is called the *key*. Then choosing a uniform $f \in \{0,1\}^n$ is equivalent to choosing the function $F_k : \{0,1\}^n \to \{0,1\}^n$, i.e., the algorithm F defines a distribution over functions in $Func_n$. The number of functions in $\{F_k\}_{k \in \{0,1\}^n}$ is at most 2^n.

Definition 12 (Definition 4.2)**.** *F is a* pseudorandom function *(PRF) if F_k, for uniform $k \in \{0,1\}^n$ is* indistinguishable *from a uniform function $f \in Func_n$. Formally, for all PPT distinguishers D, it holds that*

$$|\Pr_{k \leftarrow \{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow Func_n}[D^{f(\cdot)}(1^n) = 1]| \leq \epsilon(n).$$

A relevant cryptographic primitive is *pseudorandom permutation* (PRP), which defines a keyed function F_k that is indistinguishable from a random permutation from $f \in Perm_n \subset Func_n$. F is a keyed permutation if F_k is a permutation for every k and F_k^{-1} is efficiently computable, where $F_k^{-1}(F_k(x)) = x$.

Definition 13 (Definition 4.3)**.** *F is a* pseudorandom permutation *(PRP) if F_k, for uniform key $k \in \{0,1\}^n$, is indistinguishable from a uniform permutation $f \in Perm_n$.*

Since for large enough n, a random permutation is indistinguishable from a random function, in practice, PRPs are also good PRFs. In fact, bock ciphers are considered as PRPs. PRFs/PRPs are viewed as a stronger primitive than PRGs, since a PRF/PRP can be viewed as a PRG with random access to exponentially long output: $F_k = F_k(0 \ldots 0) | \ldots | F_k(1 \ldots 1)$, which has an output of length $n \cdot 2^n$ bits. On the other hand, a PRF/PRP F

immediately implies a PRG G: simply define $G(k) = F_k(0\ldots0)|F_k(0\ldots1)$, or $G(k) = F_k(\langle 0\rangle)|F_k(\langle 1\rangle)|F_k(\langle 2\rangle)\ldots$ as needed, where $\langle i\rangle$ denotes the n-bit encoding of i.

By employing PRFs/PRPs, we are able to build an encryption scheme which can be prove to be CPA-secure. Let F be a length-preserving, keyed function.
$Gen(1^n)$: choose a uniform key $k \in \{0,1\}^n$.
$Enc_k(m)$: for $|m| = |k|$, choose a uniform $r \in \{0,1\}^n$ (called *nonce* or *initialization vector*), and output the ciphertext $c = \langle c_1, c_2\rangle = \langle r, F_k(r) \oplus m\rangle$.
$Dec_k(c)$: output $c_2 \oplus F_k(c_1)$.

Theorem 8 (Theorem 5.1)**.** *If F is a pseudorandom function (PRF), then this encryption scheme is CPA-secure.*

Proof. Let $\widetilde{\Pi} = (\widetilde{Gen}, \widetilde{Enc}, \widetilde{Dec})$ denote the encryption scheme using $f \in Func_n$, a random function, and $\Pi = (Gen, Enc, Dec)$ denote the encryption scheme using F_k, a PRF. Fix an arbitrary PPT adversary A and let $q(n)$ be the number of queries that $A(1^n)$ makes to its encryption oracle $Enc_k(\cdot)$ (note that $q(n)$ is bounded by some polynomial).

Step 1: prove that

$$|\Pr[PrivKCPA_{A,\Pi}(n) = 1] - \Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1]| \leq negl(n). \qquad (*)$$

We prove this by reduction, i.e., we use A to construct a distinguisher D for the function F, whether F is "pseudorandom" (equal to F_k for a random $k \in \{0,1\}^n$) or "random" (equal to f for a random $f \in Func_n$) and then demonstrate that A succeeds implies that D succeeds.

Distinguisher D:
D is given input 1^n and gets access to an oracle $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$.

1. Run $A(1^n)$. Whenever A queries its encryption oracle on a message $m \in \{0,1\}^n$, answer this query in the following way:
   (a) choose uniform $r \in \{0,1\}^n$
   (b) query $\mathcal{O}(r)$ and obtain response y
   (c) return the ciphertext $\langle r, y \oplus m\rangle$ to A.
2. When A outputs messages $m_0, m_1 \in \{0,1\}^n$, choose a uniform bit $b \in \{0,1\}$, then do the following:
   (a) choose uniform $r \in \{0,1\}^n$

(b) query $\mathcal{O}(r)$ and obtain response y

(c) return the ciphertext $\langle r, y \oplus m \rangle$ to A.

3. Continue answering encryption oracle queries of A as before until A outputs a bit b'. Output 1 if $b = b'$, and otherwise 0.

Note that D is polynomial-time since A is so. Then we have

$$\begin{aligned} \Pr_{k \leftarrow \{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 1] &= \Pr[PrivKCPA_{A,\Pi}(n) = 1] \\ \Pr_{f \leftarrow Func_n}[D^{f(\cdot)}(1^n) = 1] &= \Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1]. \end{aligned}$$

By the definition of PRFs, we get the equation $(*)$.

Step 2: we prove that

$$\Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1] \leq 1/2 + q(n)/2^n.$$

Let r^* denote the random string used when generating the challenging ciphertext $\langle r^*, f(r^*) \oplus m_b \rangle$. Denote by *Repeat* the event that r^* is used by the encryption oracle when answering at least one of A's queries.

1. r^* is never used when answering any of A's queries.
   $f(r^*)$ is uniformly distributed and is independent of the rest of the experiment, then we have

   $$\Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1] = 1/2 \text{ as one-time pad.}$$

2. r^* is used when answering at least one of A's queries.
   However, since A makes at most $q(n)$ queries to its encryption oracle, and since r^* is chosen uniformly from $\{0,1\}^n$, we have

   $$\Pr[Repeat] \leq q(n)/2^n.$$

Therefore, we have

$$\begin{aligned} &\Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1] \\ &= \Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1 \wedge Repeat] + \Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1 \wedge \neg Repeat] \\ &\leq \Pr[Repeat] + \Pr[PrivKCPA_{A,\widetilde{\Pi}}(n) = 1 | \neg Repeat] \\ &\leq q(n)/2^n + 1/2. \end{aligned}$$

By combining Steps 1 and 2, we prove that

$$\Pr[PrivKCPA_{A,\Pi}(n) = 1] \leq 1 + q(n)/2^n + negl(n) = 1/2 + negl'(n).$$

□

Another key assumption is that the nonce r should be uniformly chosen. Otherwise, there may exist attacks using this bias in real world. Now that we have a CPA-secure encryption scheme based on PRFs. However, there exist two drawbacks: a 1-block plaintext results in a 2-block ciphertext; this is only defined for encryption of n-bit messages.

It is noted that CPA-security is a stronger notion than security for encryption of multiple messages. Thus, to overcome the first drawback, it is straightforward to encrypt long messages block by block, and the encryption is still CPA-secure. To overcome the second drawback, we can do better by using block-cipher modes of operation: both CTR (Counter) mode and CBC (Cipher Block Chaining) mode may lead to more efficient CPA-secure encryption schemes.

CTR mode. Choose $ctr \leftarrow \{0,1\}^n$, set $c_0 = ctr$; For $i = 1$ to t, $c_i = m_i \oplus F_k(ctr + i)$; Output $c_0, c_1, \ldots, c_t$. The ciphertext expansion is just 1 block.

Theorem 9 (Theorem 5.2)**.** *If F is a PRF, then CTR mode is CPA-secure.*

CBC mode. Choose $c_0 \leftarrow \{0,1\}^n$ (also called IV); For $i = 1$ to t, $c_i = F_k(m_i \oplus c_{i-1})$; Output $c_0, c_1, \ldots, c_t$. The ciphertext expansion is also just 1 block.

Theorem 10 (Theorem 5.3)**.** *If F is a PRF, then CBC mode is CPA-secure.*