The Fundamental Lemma of Game Playing

Advanced Topics in ~~Cybersecurity~~Cryptography (7CCSMATC)

Martin R. Albrecht

Outline

Introduction

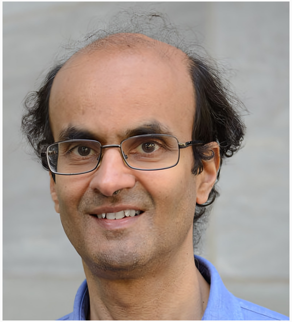
Recap

- We have defined what it means for an encryption scheme to be secure (IND-CPA + INT-CTXT = IND-CCA).
- We have shown that the OTP achieves IND-CPA security, even **unconditionally**.

The One-Time Pad is impractical, we want something more manageable $\Rightarrow$ Pseudorandomness!

Main Reference

Mihir Bellare and Phillip Rogaway. Code-Based Game-Playing Proofs and the Security of Triple Encryption. Cryptology ePrint Archive, Report 2004/331. 2004. URL: https://eprint.iacr.org/2004/331

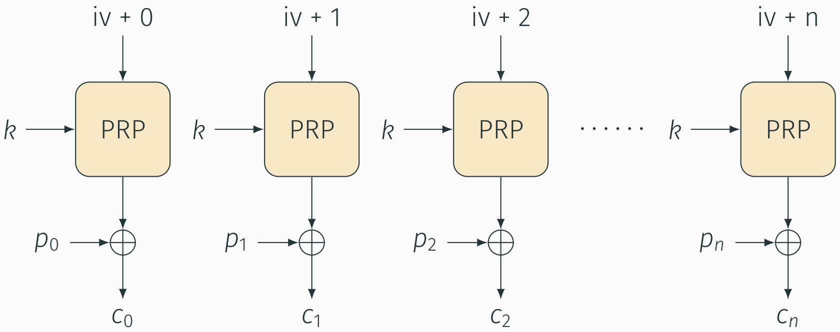


Mihir Bellare is a professor at UCSD

- **2003** RSA Conference's Sixth Annual Award
- **2013** Fellow of the Association for Computing Machinery.
- **2019** Levchin Prize for Real-World Cryptography

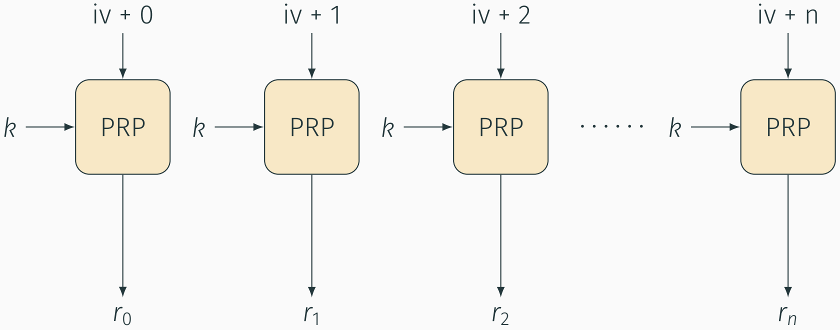
CTR Mode

CTR Mode



Picture credit: `https://www.iacr.org/authors/tikz/`

CTR Mode Stream



$r_i \in \{0,1\}^\lambda$

Want: $n+1$ Pseudorandom Strings of length λ

Definition (PRF)

A PRF is a keyed function $F_k : \{0,1\}^\lambda \to \{0,1\}^N$ where N depends on λ and for $k \leftarrow\$ \mathcal{K}$.
We say F_k is (t, ε)-secure **PRF** if for Game_0 and Game_1 defined below we have:

$$\forall \mathcal{D} \in t \text{ steps: } \mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{D}) = \left|\Pr[\mathcal{D}^{\mathsf{Game}_1} = 1] - \Pr[\mathcal{D}^{\mathsf{Game}_0} = 1]\right| < \varepsilon$$

Game_0

1: $f \leftarrow \emptyset$
2: **return** $\mathcal{D}^{\mathsf{F}}$

Game_1

1: $f \leftarrow \emptyset;\ k \leftarrow\$ \mathcal{K}$
2: **return** $\mathcal{D}^{\mathsf{F}}$

$\mathsf{F}(x)$

1: **if** $x \notin f.\mathrm{keys}$ **then** $f[x] \leftarrow\$ \{0,1\}^N$
2: $y \leftarrow f[x]$
3: $y \leftarrow F_k(x)$ //Game_1
4: **return** y

Have: $n+1$ calls to Pseudorandom Permutation of length λ

Definition (PRP)

A PRP is a keyed permutation $E_k : \{0,1\}^\lambda \to \{0,1\}^\lambda$ for $k \leftarrow\$ \mathcal{K}$. We say E is (t,ε)-secure **PRP** if for Game_0 and Game_1 defined below we have:

$$\forall \mathcal{D} \in t \text{ steps: } \mathrm{Adv}_E^{\mathrm{prp}}(\mathcal{D}) = \left|\Pr[\mathcal{D}^{\text{Game}_1} = 1] - \Pr[\mathcal{D}^{\text{Game}_0} = 1]\right| < \varepsilon$$

Game_0	$\mathrm{P}(x)$
$f \leftarrow \emptyset$	**if** $x \notin f.\mathrm{keys}$ **then** $f[x] \leftarrow\$ \{0,1\}^\lambda \setminus f.\mathrm{values}$
return $\mathcal{D}^{\mathrm{P}}$	$y \leftarrow f[x]$
Game_1	$y \leftarrow E_k(x)$ //Game_1
$f \leftarrow \emptyset;\ k \leftarrow\$ \mathcal{K}$	**return** y
return $\mathcal{D}^{\mathrm{P}}$	

The Gap

Game_0

$f \leftarrow \emptyset$

return $\mathcal{D}^{\mathsf{F}}$

Game_1

$f \leftarrow \emptyset;$

return $\mathcal{D}^{\mathsf{F}}$

$\mathsf{F}(x)$

if $x \in f.\mathrm{keys}$ **then**

  $y \leftarrow f[x]$

else

  $y \leftarrow\!\!\$\ \{0,1\}^{\lambda} \setminus f.\mathrm{values}$

  $y \leftarrow\!\!\$\ \{0,1\}^{\lambda}$ $//\mathsf{Game}_1$

$f[x] \leftarrow y$

return y

PRP-PRF Switching Lemma

Lemma

*Let π be a random **permutation** from $\{0,1\}^\lambda \to \{0,1\}^\lambda$; let ρ be a random **function** from $\{0,1\}^\lambda \to \{0,1\}^\lambda$. Let $\mathcal{A}$ be an adversary making at most q queries to its oracle, then:*

$$|\Pr[\mathcal{A}^\pi] - \Pr[\mathcal{A}^\rho]| \leq \frac{q \cdot (q-1)}{2^{\lambda+1}}.$$

PRP-PRF Switching Lemma I

Consider the following games:

Game_0

$\pi \leftarrow \emptyset$

$\textbf{return } \mathcal{A}^{\mathsf{P}}$

Game_1

$\pi \leftarrow \emptyset$

$\textbf{return } \mathcal{A}^{\mathsf{P}}$

$\mathsf{P}(x)$

$\textbf{if } x \in \pi.\mathsf{keys} \textbf{ then return } \pi[x]$

$y \leftarrow\!\!\$ \{0,1\}^{\lambda}$

$\textbf{if } y \in \pi.\mathsf{values} \textbf{ then}$

$\quad \mathsf{bad} \leftarrow \textbf{true}$

$\quad y \leftarrow\!\!\$ \{0,1\}^{\lambda} \setminus \pi.\mathsf{values}$ // Game_1

$\pi[x] \leftarrow y$

$\textbf{return } y$

PRP-PRF Switching Lemma II

$$
\begin{aligned}
\left|\Pr[\mathcal{A}^{\pi}] - \Pr[\mathcal{A}^{\rho}]\right| &= \left|\Pr[\mathcal{A}^{\mathrm{Game}_0}] - \Pr[\mathcal{A}^{\mathrm{Game}_1}]\right| && (1)\\
&\leq \Pr[\mathcal{A}^{\mathrm{Game}_0}] \text{ sets bad} && (2)\\
&\leq q \cdot (q+1)/2^{\lambda+1} && (3)
\end{aligned}
$$

On Eq. (1): Game_0 perfectly simulates a random function ρ and Game_1 perfectly simulates a random permutation π, by the **principle of lazy sampling**. Thus, we have

$$\Pr[\mathcal{A}^{\rho}] = \Pr[\mathcal{A}^{\mathrm{Game}_0}] \text{ and } \Pr[\mathcal{A}^{\mathrm{Game}_1}] = \Pr[\mathcal{A}^{\pi}].$$

On Eq. (2): we will appeal to the **fundamental lemma of game playing**.

On Eq. (3): by the union bound the probability that $y \in \pi.\mathrm{values}$, is at most

$$\frac{(1+2+\cdots+(q-1))}{2^{\lambda}} = \frac{q \cdot (q-1)}{2^{\lambda+1}}.$$

Fundamental Lemma of Game Playing

We say Game_0 and Game_1 are "identical-until-bad" if they are … identical until some flag bad is set.

Fundamental Lemma of Game Playing

Lemma (Fundamental Lemma of Game Playing)

Let Game_0, Game_1 *be identical-until-bad games and* $\mathcal{A}$ *be an adversary. Then*

$$\left|\Pr[\mathcal{A}^{\mathsf{Game}_0}] - \Pr[\mathcal{A}^{\mathsf{Game}_1}]\right| \leq \Pr[\mathcal{A}^{\mathsf{Game}_0} \textit{ sets bad}].$$

Proof of the Fundamental Lemma of Game Playing

Proof Reference

We follow

Mike Rosulek. The Joy of Cryptography. `https://joyofcryptography.com`. self published, 2021, Proof of Lemma 4.8

Conditional Probabilities

- If Y is some event, then we write $\bar{Y}$ to denote the complement event i.e~the event that Y does not happen. For all events Y, we have

$$\Pr[Y] + \Pr[\bar{Y}] = 1$$

- We write $\Pr[X \mid Y]$ to denote the probability of X, conditioned on the event Y. Conditional probability is defined as:

$$\Pr[X \mid Y] = \Pr[X \wedge Y] / \Pr[Y]$$

- It satisfies the important identity for all events X and Y :

$$\Pr[X] = \Pr[X \mid Y] \Pr[Y] + \Pr[X \mid \bar{Y}] \Pr[\bar{Y}].$$

Proof I

- Let B_0 be the event that bad is set in Game_0
- Let B_1 be the event that bad is set in Game_1
- We can write:

$$\Pr[\mathcal{A}^{\mathsf{Game}_0}] = \Pr[\mathcal{A}^{\mathsf{Game}_0} \mid B_0] \cdot \Pr[B_0] + \Pr[\mathcal{A}^{\mathsf{Game}_0} \mid \bar{B}_0] \cdot \Pr[\bar{B}_0]$$
$$\Pr[\mathcal{A}^{\mathsf{Game}_1}] = \Pr[\mathcal{A}^{\mathsf{Game}_1} \mid B_1] \cdot \Pr[B_1] + \Pr[\mathcal{A}^{\mathsf{Game}_1} \mid \bar{B}_1] \cdot \Pr[\bar{B}_1]$$

- We have $\alpha := \Pr[B_0] = \Pr[B_1]$ because the two games are identical-until-bad.
- We have $\beta := \Pr[\mathcal{A}^{\mathsf{Game}_0} \mid \bar{B}_0] = \Pr[\mathcal{A}^{\mathsf{Game}_1} \mid \bar{B}_1]$ because the two games only differ when bad is set.

Proof II

- Substituting in, we obtain

$$
\begin{aligned}
\Pr[\mathcal{A}^{\mathrm{Game}_0}] &= \Pr[\mathcal{A}^{\mathrm{Game}_0} \mid B_0] \cdot \alpha + \beta \cdot (1 - \alpha) \\
\Pr[\mathcal{A}^{\mathrm{Game}_1}] &= \Pr[\mathcal{A}^{\mathrm{Game}_1} \mid B_1] \cdot \alpha + \beta \cdot (1 - \alpha)
\end{aligned}
$$

- We can calculate the advantage

$$
\begin{aligned}
\left|\Pr[\mathcal{A}^{\mathrm{Game}_0}] - \Pr[\mathcal{A}^{\mathrm{Game}_1}]\right| &= \left| \begin{array}{r} \Pr[\mathcal{A}^{\mathrm{Game}_0} \mid B_0] \cdot \alpha + \beta \cdot (1 - \alpha) \\ - \Pr[\mathcal{A}^{\mathrm{Game}_1} \mid B_1] \cdot \alpha + \beta \cdot (1 - \alpha) \end{array} \right| \\
&= \left| \left(\Pr[\mathcal{A}^{\mathrm{Game}_0} \mid B_0] - \Pr[\mathcal{A}^{\mathrm{Game}_1} \mid B_1] \right) \cdot \alpha \right| \\
&= \left| \Pr[\mathcal{A}^{\mathrm{Game}_0} \mid B_0] - \Pr[\mathcal{A}^{\mathrm{Game}_1} \mid B_1] \right| \cdot \alpha \\
&\le \alpha = \Pr[B_0] = \Pr[\mathcal{A}^{\mathrm{Game}_0} \text{ sets bad}].
\end{aligned}
$$

where the last step follows from $0 \le \left| \Pr[\mathcal{A}^{\mathrm{Game}_0} \mid B_0] - \Pr[\mathcal{A}^{\mathrm{Game}_1} \mid B_1] \right| \le 1$.

Closing

Matching Attack

- Call $\sqrt{2^\lambda} = 2^{\lambda/2}$ times and check if any answer repeats.
- By the birthday bound this happens with constant probability

Memory-less Attack

Read about the Pollard-rho attack to learn how to make this attack use poly(λ) memory instead of $2^{\lambda/2}$.

Fin

We want to approximate the one-time pad

If we have a PRF, this is straight-forward

If we "only" have a PRP, an ideal primitive, this breaks down after $q = \sqrt{2^\lambda}$ queries, e.g. 2^{64} for $\lambda = 128$ (AES-128).

Next: How do we get a PRP?

[BR04] Mihir Bellare and Phillip Rogaway. Code-Based Game-Playing Proofs and the Security of Triple Encryption. Cryptology ePrint Archive, Report 2004/331. 2004. URL: https://eprint.iacr.org/2004/331.

[Ros21] Mike Rosulek. The Joy of Cryptography. https://joyofcryptography.com. self published, 2021.

Proof of the Fundamental Lemma of Game Playing as in [BR04] I

We require that both the adversary and the game always terminate in finite time.

- For any adversary $\mathcal{A}$ there must exist an integer T such that $\mathcal{A}$ always halts within T steps (regardless of the random choices $\mathcal{A}$ makes and the answers it receives to its oracle queries).
- For any game Game there must exist an integer T such that Game always halts within T steps (regardless of the random choices made).

Proof of the Fundamental Lemma of Game Playing as in [BR04] II

Since $\mathcal{A}$ and Game terminate in finite time,

- there must be an integer T such that they each execute at most T random-assignment statements, and
- there must be an integer B such that the size of the set $\mathcal{S}$ in any random-assignment statement $s \leftarrow\$ \mathcal{S}$ executed by the adversary or the game is at most B.

$\Rightarrow$ The execution of Game with $\mathcal{A}$ uses finite randomness, meaning Game and $\mathcal{A}$ are underlain by a finite sample space Ω.

Punchline

Probabilities are well-defined and we can talk about the probabilities of various events in the execution.

Proof of the Fundamental Lemma of Game Playing as in [BR04] III

- This means that there exists an integer z such that the execution of Game_0 with $\mathcal{A}$ and the execution of Game_1 with $\mathcal{A}$ perform no more than z random-assignment statements, each of these sampling from a set of size at most z.

Proof of the Fundamental Lemma of Game Playing as in [BR04] IV

- Let $\mathcal{C} := \mathrm{Coins}(\mathcal{A}, \mathrm{Game}_0, \mathrm{Game}_1) = [1 \ldots z!]^z$ be the set of z-tuples of numbers, each number between 1 and $z!$.

```
z = 2
R = IntegerModRing(factorial(z)); offset = vector(R, z, [1]*z).lift()
Coins = [coin.lift() + offset for coin in FreeModule(R, z)]
print(Coins)
```

- For $\mathbf{c} = (c_0, \ldots, c_{z-1}) \in \mathcal{C}$, the execution of Game with $\mathcal{A}$ on coins c is defined as follows:
  - On the i-th random-assignment statement, call it $x \leftarrow\!\$\, \mathcal{U}(\mathcal{S})$, where $\mathcal{S} := \{s_i\}_{0 \le i < m}$, if $\mathcal{S} \neq \emptyset$, return $s_{c_i \bmod |\mathcal{S}|}$, otherwise return $\perp$.
- This way to perform random-assignment statements is done regardless of whether it is $\mathcal{A}$ or one of the procedures from Game that is is performing the random-assignment statement.

Proof of the Fundamental Lemma of Game Playing as in [BR04] V

- Note that $m = |\mathcal{S}|$ satisfies $m|z!$ so if $\mathbf{c}$ is chosen at random from $\mathcal{C}$ then the mechanism above will return a point x drawn uniformly from $\mathcal{S}$, and also the values for each random-assignment statement are independent.

- For $\mathbf{c} \in \mathcal{C}$ we let $\mathrm{Game_0}^{\mathcal{A}}(\mathbf{c})$ denote the output of $\mathrm{Game_0}$ when $\mathrm{Game_0}$ is executed with $\mathcal{A}$ on coins $\mathbf{c}$. Same for $\mathrm{Game_1}$.
- Write $\mathcal{C}_{i,\mathrm{one}} := \{\mathbf{c} \in \mathcal{C} : \mathrm{Game_i}^{\mathcal{A}}(\mathbf{c}) \Rightarrow 1\}$
- Write $\mathcal{C}_i^{bad} \subseteq \mathcal{C}$ for the coins that result in *bad* being set to **true** when running $\mathrm{Game_i}^{\mathcal{A}}$.
- Partition $\mathcal{C}_{i,\mathrm{one}}$ into $\mathcal{C}_{i,\mathrm{one}}^{bad}$ and $\mathcal{C}_{i,\mathrm{one}}^{good}$ depending on whether bad was set or not in game $\mathrm{Game_i}$.
- Because games $\mathrm{Game_0}$ and $\mathrm{Game_1}$ are identical-until-bad, an element $\mathbf{c} \in \mathcal{C}$ is in $\mathcal{C}_{0,\mathrm{one}}^{good}$ if and only if it is in $\mathcal{C}_{1,\mathrm{one}}^{good}$.
    - Bad is never set so the sets are same and in particular have the same size.

We then get:

$$\begin{aligned}
\Pr[\mathsf{Game}_0{}^{\mathcal{A}}] - \Pr[\mathsf{Game}_1{}^{\mathcal{A}}] &= \frac{\mathcal{C}_{0,\mathrm{one}}}{\mathcal{C}} - \frac{\mathcal{C}_{1,\mathrm{one}}}{\mathcal{C}} \\
&= \frac{\mathcal{C}_{0,\mathrm{one}}^{good} + \mathcal{C}_{0,\mathrm{one}}^{bad}}{\mathcal{C}} - \frac{\mathcal{C}_{1,\mathrm{one}}^{good} + \mathcal{C}_{1,\mathrm{one}}^{bad}}{\mathcal{C}} \\
&= \frac{\mathcal{C}_{0,\mathrm{one}}^{bad}}{\mathcal{C}} - \frac{\mathcal{C}_{1,\mathrm{one}}^{bad}}{\mathcal{C}} \\
&\leq \frac{\mathcal{C}_{0,\mathrm{one}}^{bad}}{\mathcal{C}} \\
&\leq \frac{\mathcal{C}_{0}^{bad}}{\mathcal{C}} \\
&= \Pr[\mathsf{Game}_0{}^{\mathcal{A}} \text{ sets bad}].
\end{aligned}$$