Applied Cryptography
Spring Semester 2023
Lecture 7

Kenny Paterson (@kennyog)

Applied Cryptography Group

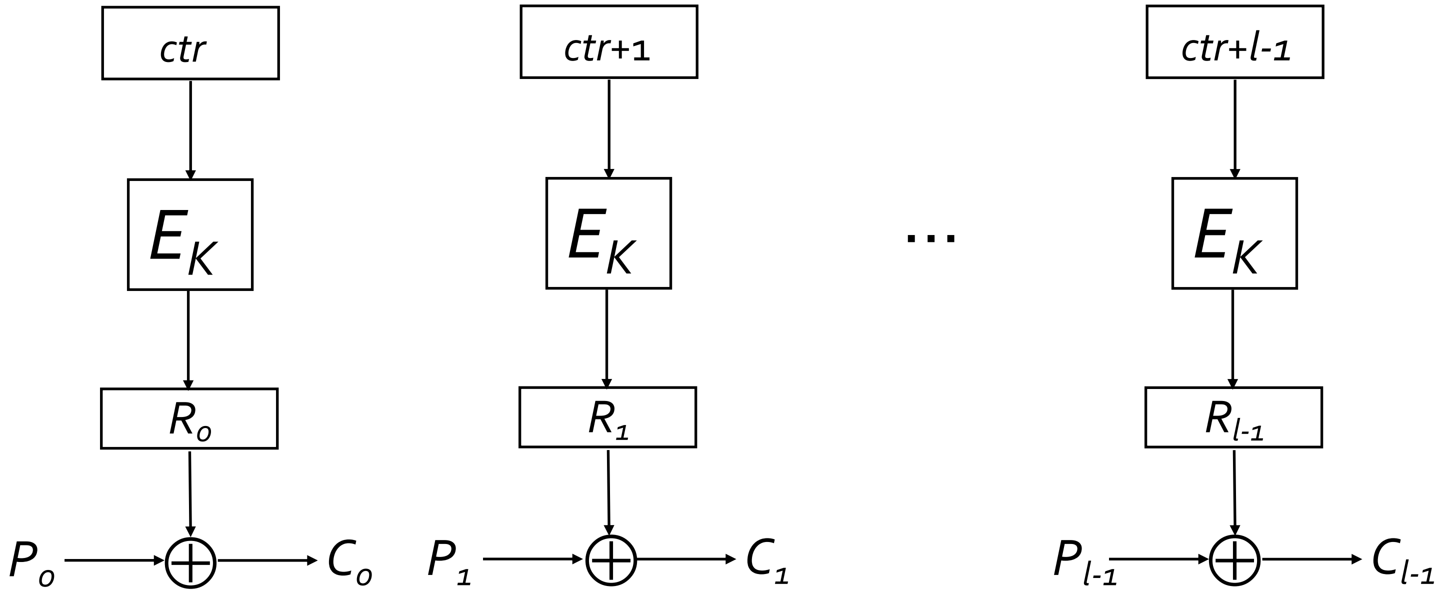
https://appliedcrypto.ethz.ch/

Overview of Lecture 7

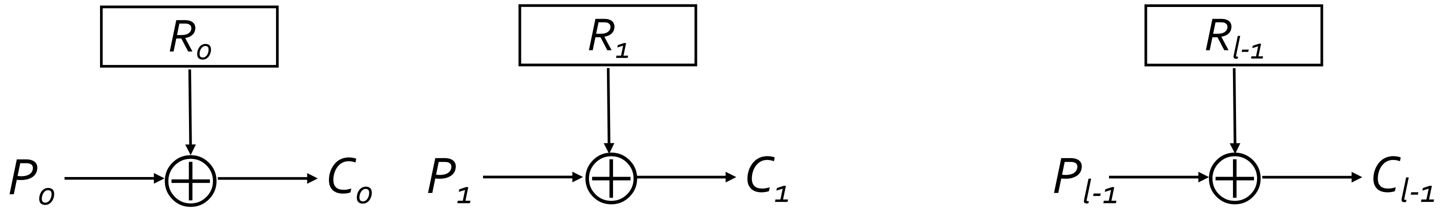
- Proof of security for (simplified) CTR mode

Proof of Security for CTR mode

Recap: Counter (CTR) mode encryption



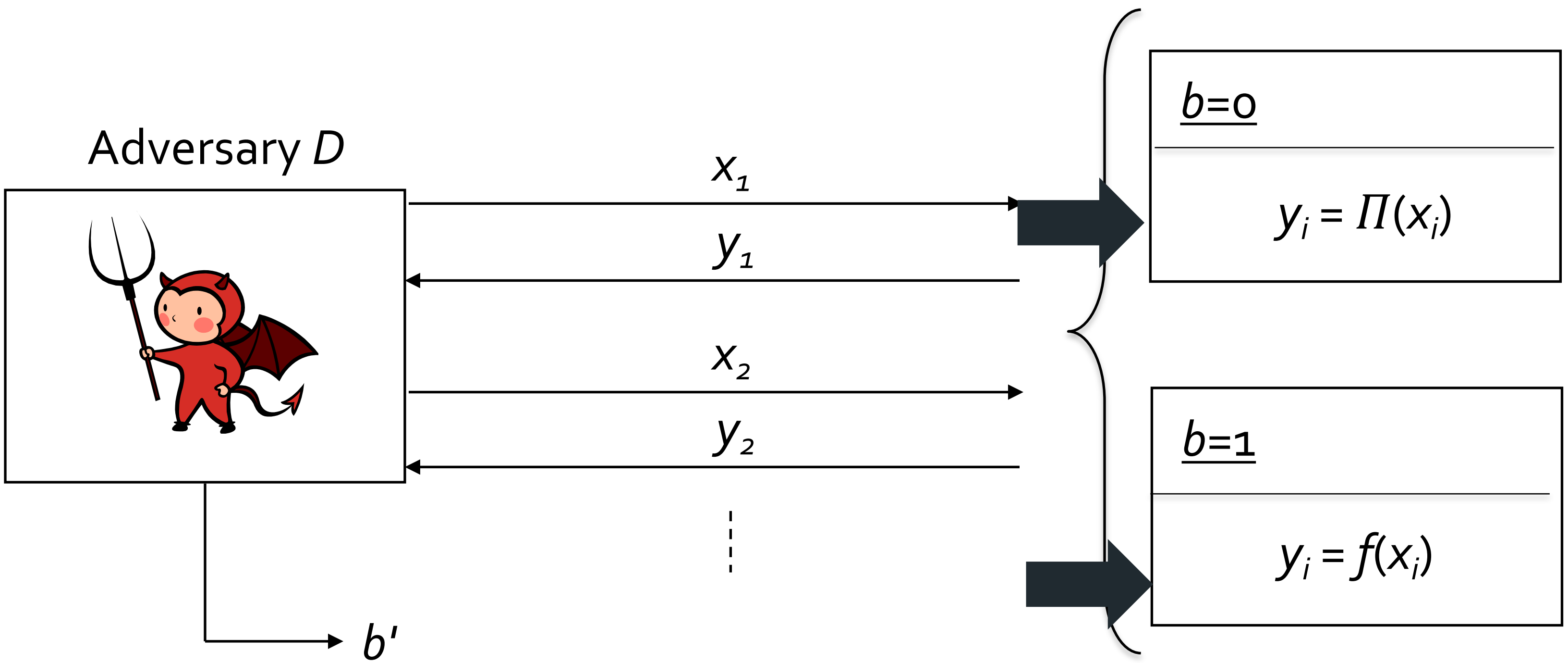
Recap: One time pad



- R_i are independent random values.
- Then C_i are independent of P_i (in the probabilistic sense).
- Hence advantage of any IND-CPA adversary (even unbounded) against OTP is zero.

PRP/PRF security game/definition: Pictorial definition

$b \leftarrow\!\$ \{0,1\}$
b=0: $\Pi \leftarrow\!\$$ Perms[$\{0,1\}^n$]
b=1: $f \leftarrow\!\$$ Funcs[$\{0,1\}^n$, $\{0,1\}^n$]



$\mathrm{Adv}^{\mathrm{PRP/PRF}}(D) := 2|\Pr[b'=b] - ½|.$

PRP/PRF security game/definition: Pictorial definition

$b \leftarrow_\$ \{0,1\}$
b=0: $\Pi \leftarrow_\$ \text{Perms}[\{0,1\}^n]$
b=1: $f \leftarrow_\$ \text{Funcs}[\{0,1\}^n, \{0,1\}^n]$

Upon receiving the i-th query x_i from A do:
If $x_i = x_j$ for some $j < i$
    then $y_i \leftarrow y_j$
else
    $y_i \leftarrow_\$ \{0,1\}^n \setminus \{y_0, \dots, y_{i-1}\}$
Return y_i.

b=0

$y_i = \Pi(x_i)$

Adversary D

x_2

y_2

Upon receiving the i-th query x_i from A do:
If $x_i = x_j$ for some $j < i$
    then $y_i \leftarrow y_j$
else
    $y_i \leftarrow_\$ \{0,1\}^n$
Return y_i.

b=1

$y_i = f(x_i)$

b'

$\text{Adv}^{\text{PRP/PRF}}(D) := 2|\Pr[b'=b] - ½|$.

A bound on PRP/PRF security

The b=0 and b=1 cases are identical unless a repeated value occurs amongst the y_i.

- Let Z denote the event that a repeated value **does** occur.
- As in lecture 6, Pr[Z] $\leq q^2/2^{n+1}$.

Let W_1 be the event that b′ = 1 (i.e. D outputs "1") conditioned on b=0.

Let W_2 be the event that b′ = 1 (i.e. D outputs "1") conditioned on b=1.

We have: event $W_1 \wedge \neg Z$ occurs if and only if event $W_2 \wedge \neg Z$ occurs.

Then:

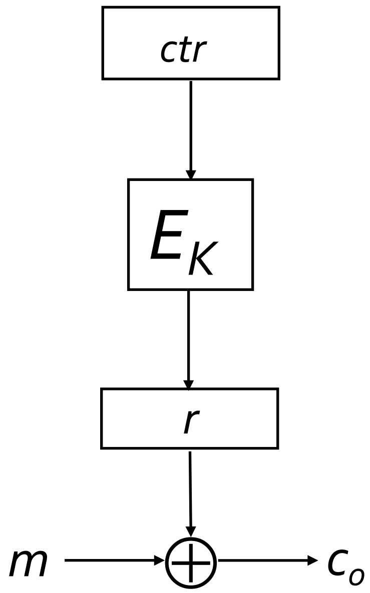
$$\begin{aligned} \mathrm{Adv}^{\mathrm{PRP/PRF}}(D) &= |\Pr[b' = 1 \mid b=1] - \Pr[b' = 1 \mid b=0]| \\ &= |\Pr[W_2] - \Pr[W_1]| \\ &\leq \Pr[Z] \\ &\leq q^2/2^{n+1}. \end{aligned}$$

Advantage rewriting

Apply difference lemma

NB this analysis depends only on the number of queries q made by D and is independent of D's running time!

Our object of analysis: Simplified CTR mode



- We assume for simplicity that all messages consist of exactly one block, so $m \in \mathcal{M} = \{0, 1\}^n$.
- We analyse the case where *ctr* is chosen uniformly at random for each encryption.
- Pseudo-code for CTR mode encryption:

<u>$\mathrm{Enc}_K(m)$:</u> // *m* is just a single block of *n* bits

1. $ctr \leftarrow\$ \{0,1\}^n$
2. $r = E_K(ctr)$
3. $c_o = m \oplus r$
4. return (ctr, c_o)

- Everything can be adapted to the case of multi-block messages and messages in which the last block is not full for some messages.
- Things just get a bit messier!

IND-CPA security for CTR mode: G_0

Adversary A

Challenger

$b \leftarrow\$ \{0,1\}$

$K \leftarrow\$ \mathrm{KGen}$

LoR oracle

1. $ctr \leftarrow\$ \{0,1\}^n$
2. $r = E_K(ctr)$
3. $c_0 = m_b \oplus r$
4. return $c = (ctr, c_0)$

(m_0, m_1)

c

b'

$$\mathrm{Adv}^{G_0}_{\mathrm{CTR}}(A) := \mathrm{Adv}^{\text{IND-CPA}}_{\mathrm{CTR}}(A) = 2|\Pr[b'=b] - \tfrac{1}{2}|.$$

IND-CPA security for CTR mode: G_1

Adversary A

(m_0, m_1) →

← c

b'

Challenger

$b \leftarrow\$ \{0,1\}$

$\Pi \leftarrow\$ \text{Perms}[\{0,1\}^n]$

LoR oracle

1. $ctr \leftarrow\$ \{0,1\}^n$
2. $r = \Pi(ctr)$
3. $c_0 = m_b \oplus r$
4. return $c = (ctr, c_0)$

$$\text{Adv}^{G_1}_{\text{CTR}}(A) := 2|\Pr[b'=b] - ½|.$$

IND-CPA security for CTR mode: G_2

Adversary A

(m_0, m_1) →

← c

→ b'

Challenger

$b \leftarrow\$ \{0,1\}$

$f \leftarrow\$ \text{Funcs}[\{0,1\}^n, \{0,1\}^n]$

LoR oracle

1. $ctr \leftarrow\$ \{0,1\}^n$
2. $r = f(ctr)$
3. $c_0 = m_b \oplus r$
4. return $c = (ctr, c_0)$

$$\text{Adv}^{G_2}_{\text{CTR}}(A) := 2|\Pr[b'=b] - ½|.$$

IND-CPA security for CTR mode: G_3

Adversary A

Challenger

$b \leftarrow_\$ \{0,1\}$

$f \leftarrow_\$ \text{Funcs}[\{0,1\}^n, [\{0,1\}^n]$

(m_0, m_1)

c

LoR oracle

1. $ctr \leftarrow \$ \{0,1\}^n$
2. $r \leftarrow \$ \{0,1\}^n$
3. $c_0 = m_b \oplus r$
4. return $c = (ctr, c_0)$

b'

$\text{Adv}^{G_3}_{\text{CTR}}(A) := 2|\Pr[b'=b] - ½| = 0.$

IND-CPA security for CTR mode: Intuition

- The proof involves a sequence of games $G_0, \ldots, G_3$.
- Each game is played between a fixed IND-CPA adversary *A* and a challenger (in the picture; just part of the game in the pseudo-code version).
- We change the operation of the challenger slightly as we transition between different pairs of games.
- In G_0, the challenger is just the normal IND-CPA challenger for CTR mode.
- In G_3, the challenger uses one-time pad encryption, so *A*'s advantage there is zero (see slide 5).
- We show that in each transition, *A*'s advantage cannot change much.
- Since *A*'s advantage is zero in G_3, the advantage in G_0 must be small.
- We will formalise this intuition and be concrete about "small".

IND-CPA security for CTR mode: Notation

- The proof involves a sequence of games $G_0, \dots, G_3$.
- Let X_i denote the event that $b' = b$ in game G_i (i.e. A wins in game G_i).
- Let $q_i = \Pr[X_i]$.
- So:

$$\mathrm{Adv}^{G_0}_{CTR}(A) = \mathrm{Adv}^{IND\text{-}CPA}_{CTR}(A) = 2|q_0 - ½|.$$

- And:

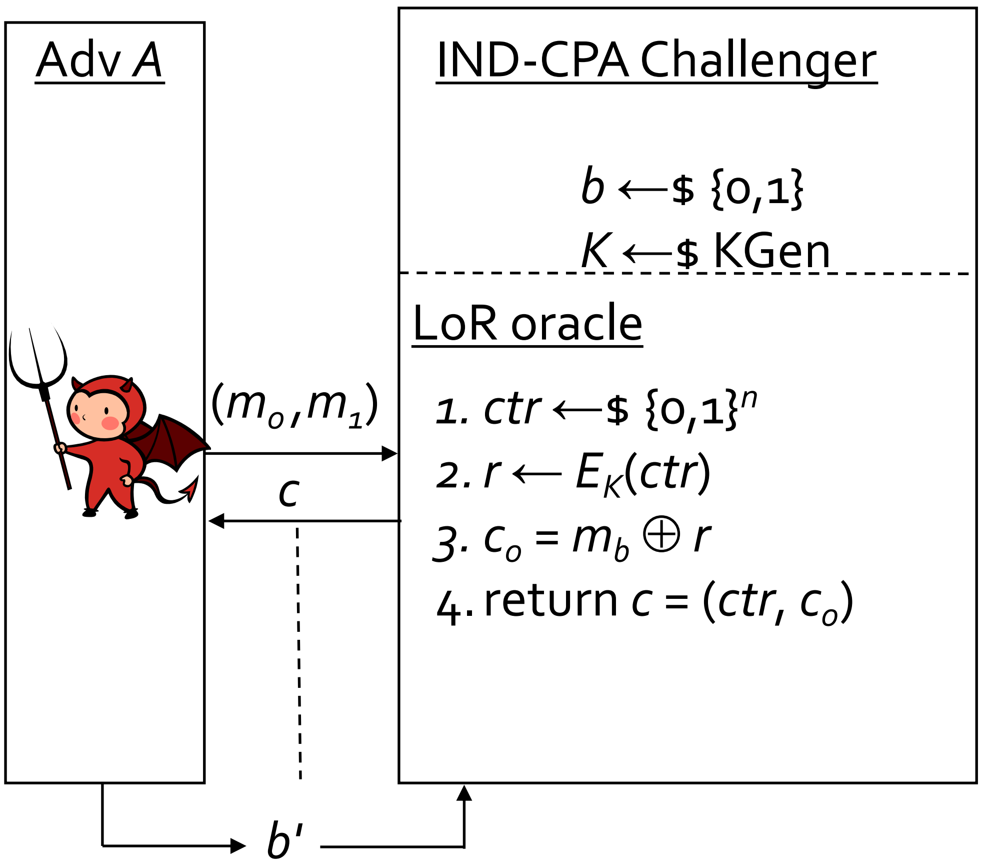
$$\begin{aligned} |q_0 - ½| &= |(q_0 - q_1) + (q_1 - q_2) + (q_2 - q_3) + (q_3 - ½)| \\ &\leq |q_0 - q_1| + |q_1 - q_2| + |q_2 - q_3| + |q_3 - ½| \\ &= |q_0 - q_1| + |q_1 - q_2| + |q_2 - q_3| \end{aligned}$$

This term is zero because of OTP encryption in G_3!

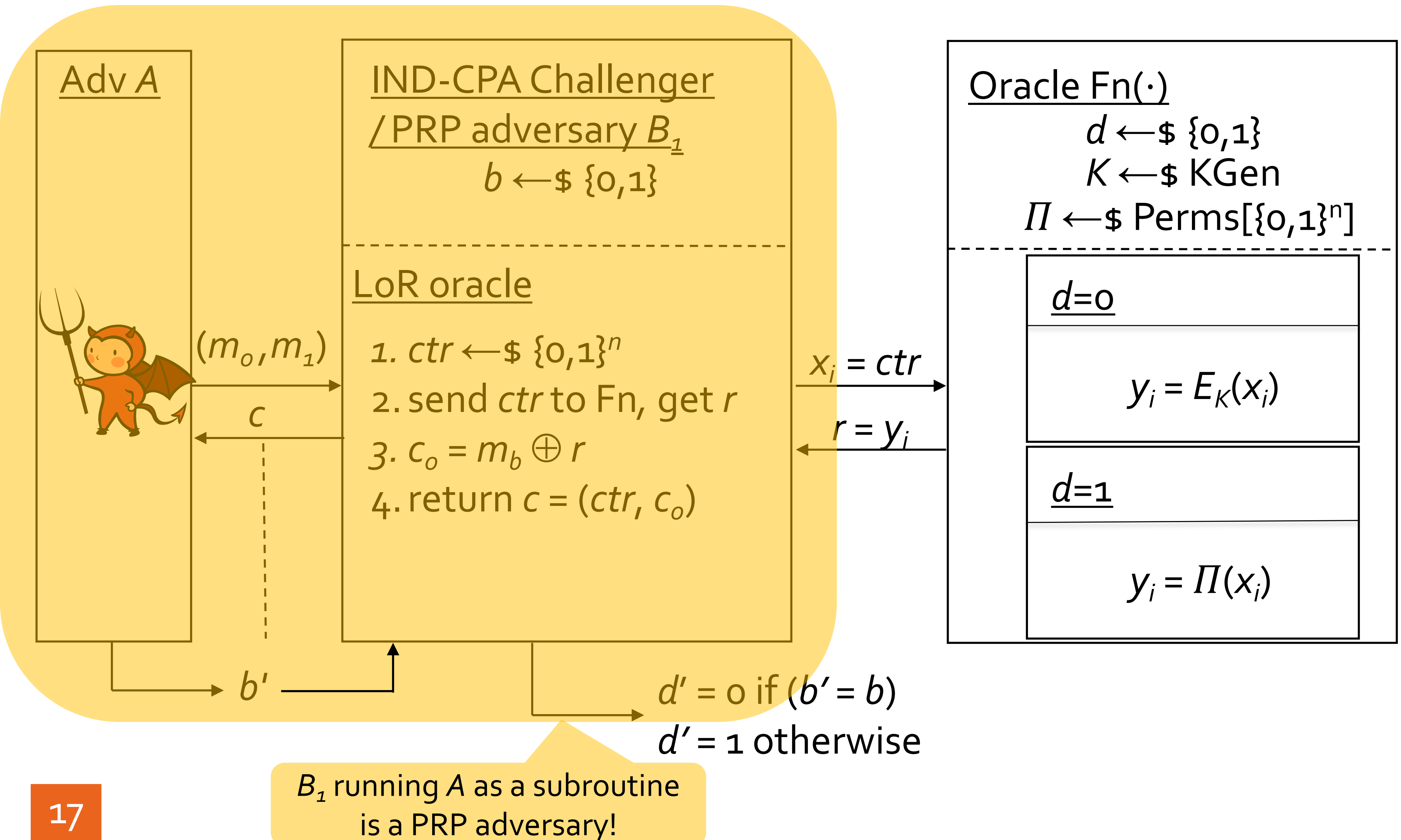
Sum of differences of winning probabilities.

- The rest of the proof consists of showing that each of these differences is small.

IND-CPA security for CTR mode: Bounding $| q_0 - q_1 |$



IND-CPA security for CTR mode: Bounding $| q_0 - q_1 |$



IND-CPA security for CTR mode: Bounding $|q_0 - q_1|$

- We construct from IND-CPA adversary A a PRP adversary B_1 against E.
- B_1 runs A as a subroutine, acting as a challenger to A, and uses A's output to estimate the hidden bit d in its own PRP security game.
- We show that any difference in A's output in G_0 / G_1 can be "converted" by B_1 into an advantage in its PRP security game.
- When $d = 0$, A is playing in G_0, which is just the normal IND-CPA game.
- When $d = 1$, A is playing in G_1, the game where E_K is replaced with Π.
- So:

$$q_0 = \Pr[b'=b \text{ in } G_0] = \Pr[b'=b \mid d=0] = \Pr[d'=0 \mid d=0];$$

$$q_1 = \Pr[b'=b \text{ in } G_1] = \Pr[b'=b \mid d=1] = \Pr[d'=0 \mid d=1].$$

Advantage rewriting

- And so:

$$|q_0 - q_1| = |\Pr[d'=0 \mid d=0] - \Pr[d'=0 \mid d=1]| = \mathrm{Adv}_E^{PRP}(B_1).$$

IND-CPA security for CTR mode: Bounding $| q_0 - q_1 |$

- We have shown that B_1, acting as a PRP adversary against E, is such that:

$$| q_0 - q_1 | = \mathrm{Adv}_E^{PRP}(B_1).$$

- Formally B_1 runs A, and answers its encryption queries by using its own oracle Fn(·).

- Then the running time of B_1 is essentially that of A, and if A makes q queries to its encryption oracle, then B_1 makes q queries to its PRP oracle.

- But if E is a good PRP, then B_1's advantage must be small, and so $| q_0 - q_1 |$ must be small too.

- More precisely, we can bound $| q_0 - q_1 |$ by the maximum advantage ε of *any* PRP adversary D against block cipher E that runs in the same time as A and makes the same number of queries as A, i.e.:

$$\max \{ \mathrm{Adv}_E^{PRP}(D) : D \text{ runs in time } t_A \text{ and makes } q_A \text{ queries} \}.$$

IND-CPA security for CTR mode: Bounding $|q_1 - q_2|$

Adv A

(m_0, m_1) →

← c

IND-CPA Challenger / PRP-PRF adversary B_2

$b \leftarrow\$ \{0,1\}$

LoR oracle

1. $ctr \leftarrow\$ \{0,1\}^n$
2. send ctr to Fn, get r
3. $c_0 = m_b \oplus r$
4. return $c = (ctr, c_0)$

$x_i = ctr$ →

← $r = y_i$

Oracle Fn(·)

$d \leftarrow\$ \{0,1\}$

$\Pi \leftarrow\$ \text{Perms}[\{0,1\}^n]$

$f \leftarrow\$ \text{Funcs}[\{0,1\}^n, \{0,1\}^n]$

d=0:

$y_i = \Pi(x_i)$

d=1:

$y_i = f(x_i)$

b'

$d' = 0$ if $(b' = b)$

$d' = 1$ otherwise

IND-CPA security for CTR mode: Bounding $|q_1 - q_2|$

- We construct from IND-CPA adversary A an adversary B_2 distinguishing between a random permutation Π and a random function f.
- B_2 runs A as a subroutine, acting as a challenger to A, and uses A's output to estimate the hidden bit d in its own PRP/PRF security game.
- When $d = 0$, A is playing in G_1, where Π is used to answer B_2's queries.
- When $d = 1$, A is playing in G_2, the game where Π is replaced with f.
- So:

$$q_1 = \Pr[b'=b \text{ in } G_1] = \Pr[b'=b \mid d=0] = \Pr[d'=0 \mid d=0];$$

$$q_2 = \Pr[b'=b \text{ in } G_2] = \Pr[b'=b \mid d=1] = \Pr[d'=0 \mid d=1].$$

Advantage rewriting

- And:

$$|q_1 - q_2| = |\Pr[d'=0 \mid d=0] - \Pr[d'=0 \mid d=1]| = \mathrm{Adv}^{PRP/PRF}(B_2).$$

IND-CPA security for CTR mode: Bounding $|q_1 - q_2|$

- We have shown that B_2, acting as a PRP/PRF adversary, is such that:

$$|q_1 - q_2| = \mathrm{Adv}^{PRP/PRF}(B_2).$$

- Formally B_2 runs A, and answers its encryption queries by using its own oracle Fn(·).
- Then the running time of B_2 is essentially the same as that of A, and if A makes q queries to its encryption oracle, then B_2 makes q queries to its PRP/PRF oracle.
- But we know from slides 6-8 of this lecture that for *any* algorithm D making q queries:

$$\mathrm{Adv}^{PRP/PRF}(D) \leq q^2/2^{n+1}.$$

- Hence we obtain:

$$|q_1 - q_2| \leq q^2/2^{n+1}.$$

IND-CPA security for CTR mode: Bounding $| q_2 - q_3 |$

Adv A

(m_0, m_1) →

← c

b'

IND-CPA Challenger B_3

$b \leftarrow\$ \{0,1\}$

LoR oracle

1. $ctr \leftarrow\$ \{0,1\}^n$
2. send ctr to oracle, get r
3. $c_0 = m_b \oplus r$
4. return $c = (ctr, c_0)$

$x_i = ctr$ →

← $r = y_i$

Rand function or rand values

$d \leftarrow\$ \{0,1\}$

$f \leftarrow\$ \text{Funcs}[\{0,1\}^n, \{0,1\}^n]$

d=0:

$y_i = f(x_i)$

d=1:

$y_i \leftarrow\$ \{0,1\}^n$

IND-CPA security for CTR mode: Bounding $| q_2 - q_3 |$

- B_3 acts as a challenger to A; the oracle here just controls how encryption is done.

  - When $d = 0$, A is playing in G_2, where:

    $$ctr \leftarrow\$ \{0,1\}^n;\ r = f(ctr);\ c_0 = m_b \oplus r.$$

  - When $d = 1$, A is playing in G_3, where:

    $$ctr \leftarrow\$ \{0,1\}^n;\ r \leftarrow\$ \{0,1\}^n;\ c_0 = m_b \oplus r.$$

f is a random function, so these r values are *almost* uniformly random. Why not exactly so?

IND-CPA security for CTR mode: Bounding $| q_2 - q_3 |$

- Let Z denote the event that the randomly chosen values of *ctr* used by B_3 are not all distinct.
  - A standard analysis as before shows that $\Pr[Z] \leq q^2/2^{n+1}$.
  - G_2 and G_3 are identical unless event Z occurs, because f is a random function whose outputs on distinct inputs are just uniformly random values.
  - Recall that X_i denotes the event that $b' = b$ in game G_i (i.e. A wins in game G_i) and we defined $q_i = \Pr[X_i]$.
  - So we have: $(X_2 \wedge \neg Z)$ occurs if and only if $(X_3 \wedge \neg Z)$ occurs.

Now we apply the difference lemma to obtain:

$$| q_2 - q_3 | = |\Pr[X_2] - \Pr[X_3]| \leq \Pr[Z] \leq q^2/2^{n+1}.$$

IND-CPA security for CTR mode: Combining everything

- Recall:

$$\begin{aligned}
\mathrm{Adv}_{\mathrm{CTR}}^{\text{IND-CPA}}(A) = 2|\,q_0 - \tfrac{1}{2}\,| &\leq 2|\,q_0 - q_1\,| + 2|\,q_1 - q_2\,| + 2|\,q_2 - q_3\,| \\
&\leq 2\mathrm{Adv}_E^{PRP}(B_1) + 2q^2/2^{n+1} + 2q^2/2^{n+1} \\
&= 2\mathrm{Adv}_E^{PRP}(B_1) + q^2/2^{n-1}
\end{aligned}$$

- B_1 is constructed from A and runs in (roughly) the same time as A.
- B_1 is a specific adversary against the PRP security of block cipher E making q queries to its oracle.
- Then the term $\mathrm{Adv}_E^{PRP}(B_1)$ is bounded by the advantage of *any* PRP adversary B against E making at most q queries to its oracle and running in time $t = t_A$.
- But A was an arbitrary IND-CPA adversary, so the same holds for all A.
- Interpreting the bound:
  - If A was a high-advantage adversary against CTR mode, then we could construct from A a high advantage PRP adversary B_1 against E.
  - Hence if our block cipher E is secure (as a PRP), no such A can exist.

IND-CPA security for CTR mode: Combining everything

- For any IND-CPA adversary A, there exists a PRP adversary B_1 such that:

$$\mathrm{Adv}_{\mathrm{CTR}}^{\text{IND-CPA}}(A) \leq 2\mathrm{Adv}_{E}^{PRP}(B_1) + q^2/2^{n-1}$$

- From this we can show something more *concrete*:

  If E is (q, t, ε)-PRP-secure, then the (simplified) CTR mode SE scheme based on E is $(q, t, 2\varepsilon + q^2/2^{n-1})$-IND-CPA-secure.

- To see why:
  - From any (q, t, σ) adversary A against IND-CPA security of CTR, we can construct a (q, t, γ) adversary B_1 against PRP-security of E such that $\sigma \leq 2\gamma + q^2/2^{n-1}$.
  - If E is (q, t, ε)-PRP-secure, then we must have $\gamma \leq \varepsilon$, hence

$$\sigma \leq 2\gamma + q^2/2^{n-1} \leq 2\varepsilon + q^2/2^{n-1}$$

  - Hence CTR mode based on E must be $(q, t, 2\varepsilon + q^2/2^{n-1})$-IND-CPA-secure.
- So we obtain a **concrete** relationship between IND-CPA security of CTR mode and the PRP-security of the block cipher used in its construction.

IND-CPA security for CTR mode: Combining everything

We have shown:

> If E is (q, t, ε)-PRP-secure, then the (simplified) CTR mode SE scheme based on E is $(q, t, 2\varepsilon + q^2/2^{n-1})$-IND-CPA-secure.

- Note how the security of CTR mode based on E is slightly degraded compared to that of E as a PRP.
- The bound becomes meaningless when q is large compared to $2^{n/2}$.
- There are IND-CPA attacks against CTR mode with advantage that more or less matches the security bound:
  - Probability of a repeated counter is about $q^2/2^{n-1}$.
  - A repeated counter means reuse of "one-time pad" $r = E_K(ctr)$.
  - Exercise: work out the details of an IND-CPA attack here.

Homework

- **Action:** try to extend the analysis to CTR mode with longer messages – main challenge is to bound collision probabilities for the counter values.
- **Action:** start exercise sheet 3 and prepare for lab 3.