On Hiding Message Length in Symmetric-key Cryptography

Cihangir Tezcan

School of Computer and Communication Sciences

Semester Project

January 2011

Responsible
Prof. Serge Vaudenay
EPFL / LASEC

Supervisor
Prof. Serge Vaudenay
EPFL / LASEC

LASEC

Chapter 1

Introduction

Although an encryption process makes a plaintext unreadable to adversaries, the resulting ciphertext may still leak some privacy. For example, the length of a plaintext may give some information away and it may be obtained from the ciphertext. For instance, the lengths of a plaintext and the corresponding ciphertext are identical or differ by a small number when the encryption is done by a stream or a block cipher. One way of hiding the plaintext size is to use *random padding* before the encryption which appends a padding of random length in $[0, n)$. In this work, we investigate the information leakage when random padding is used.

In order to see the information leakage in random padding, we first modify the indistinguishability under chosen-plaintext attack ($IND-CPA$) game to define two new games $E-IND-CPA$ and $\Delta-IND-CPA$. In $E-IND-CPA$ game, the two chosen plaintexts have different lengths and in $\Delta-IND-CPA$ game, the difference of the lengths of the two chosen plaintexts is less than or equal to some positive integer Δ. Hence, in these games the adversary selects two plaintexts of different lengths and sends them to the challenger. The challenger selects one of them, uses random padding, encrypts it, and then sends the ciphertext back to the adversary. Since the lengths of the plaintexts are different, the adversary has nonzero advantage. Our aim is to find the best distribution for the length of the random padding so that the advantage of the adversary is minimized.

In this study, we assume that the distribution used for the length of the random padding is independent from the plaintext and we investigate the security of the $\Delta-IND-CPA$ game. When n is divisible by Δ, we solve the problem of finding the best distribution and for this solution we show that the winning chance of the best adversary is $\frac{1}{2}+\frac{\Delta}{2n}$. We also show that when n is not divisible by Δ, for the best distribution the winning chance of the best adversary is upper bounded by $\frac{1}{2}+\frac{\Delta}{2n}$ and lower bounded by $\frac{1}{2}+\frac{1}{2\left\lceil\frac{n}{\Delta}\right\rceil}$.

Moreover, for the case when n is not divisible by Δ, the winning chance of the best adversary is $\frac{1}{2} + \frac{n}{n^2+1}$ for the best distribution when $\Delta = 2$.

Chapter 2

Games, Advantage, and Security Analysis

2.1 Games

In all of the following games, we assume that the challenger pads a random bit string of length i to the plaintext before the encryption. The following assumptions can be made to define the behavior of the random padding:

A_1: i depends only on $|P|$ and independent random coins

A_2: i is independent from P

A_3: $\Pr[i \leq n-1] = 1$

Note that the assumption A_2 is stronger than the assumption A_1. Throughout this work, we assume that the padded bit string of length i is independent from P and $\Pr[i \leq n-1] = 1$ (i.e. We assume that A_2 and A_3 holds). Hence, if c is the ciphertext for the plaintext p, we have $|c| = |p| + i$ where $i \in [0, n-1]$.

We define the extended indistinguishability under chosen-plaintext attack game ($E - IND - CPA$) as follows:

Game 1. *$[E - IND - CPA]$*

1: *Challenger selects a key at random*

2: *Adversary selects plaintexts p_0 and p_1*

3: *Challenger selects a bit b, encrypts $p_b \rightarrow c$ and sends c back to the adversary*

4: *Adversary guesses b' and wins if $b' = b$*

The difference with the standard $IND - CPA$ game is that we do not restrict to $|p_0| = |p_1|$ in the $E - IND - CPA$ game. We define the $\Delta - IND - CPA$ game as follows:

Game 2. *[$\Delta - IND - CPA$]*

1: *Challenger selects a key at random*

2: *Adversary selects plaintexts p_0 and p_1 where $||p_0| - |p_1|| \leq \Delta$*

3: *Challenger selects a bit b, encrypts $p_b \rightarrow c$ and sends c back to the adversary*

4: *Adversary guesses $b^{'}$ and wins if $b^{'} = b$*

In this study, we aim to find the optimal distribution that defines the length of the random padding for the $\Delta - IND - CPA$ game with the assumptions A_2 and A_3.

2.2 Advantage

Definition 1. *We say that a cryptosystem is $\Delta - IND - CPA$ ϵ-secure if the winning chances of every adversary is less than or equal to $\frac{1}{2} + \frac{\epsilon}{2}$.*

Definition 2 (Advantage)**.** *Let a and b be non-negative integers with $a < b$. For a set A of integers, we define $D_A(X) = 1_{X \in A}$ and we use D_A to distinguish $a + N$ from $b + N$ where N is a random variable. The advantage we obtain is*

$$Adv_{D_A}(a, b) = \Pr[a + N \in A] - \Pr[b + N \in A].$$

Thus, our aim is to find the optimal distribution that defines the length of the random padding which minimizes $\max_{|b-a| \leq \Delta} \max_A Adv_{D_A}(a, b)$ for the $\Delta - IND - CPA$ game.

2.3 Security Analysis

Lemma 1. *We have $\Pr[N < b - a] \leq \max_A Adv_{D_A}(a, b)$ and equality holds if and only if $\Pr[N = x + b - a] \leq \Pr[N = x]$ for all $x \geq 0$.*

Proof. Let $\epsilon = \max_A Adv_{D_A}(a, b)$. Then we have

$$\begin{aligned}
\epsilon &= \max_A (\Pr[a + N \in A] - \Pr[b + N \in A]) \\
&= \max_A \sum_{x \in A} (\Pr[N = x - a] - \Pr[N = x - b]) \\
&= \sum_{x : \Pr[N = x - a] \geq \Pr[N = x - b]} (\Pr[N = x - a] - \Pr[N = x - b]) \\
&\geq \sum_{x : x < b} \Pr[N = x - a] \\
&= \Pr[N < b - a]
\end{aligned}$$

Since the optimal A is the set of all x's such that $\Pr[N = x - a] > \Pr[N = x - b]$, we have $\epsilon \geq \Pr[N < b - a]$ and equality holds if and only if $\Pr[N = x + b - a] \leq \Pr[N = x]$ for all $x \geq 0$. □

Theorem 1. *If $b - a = 1$, then $\max_A Adv_{D_A}(a, b) \geq \frac{1}{n}$ and equality holds if and only if N is uniform.*

Proof. Let $\epsilon = \max_A Adv_{D_A}(a, b)$.

Case 1: Assume $\Pr[N = 0] > \frac{1}{n}$. Then for $A = \{a\}$ we have $Adv_{D_A}(a, b) = \Pr[N = 0]$. Hence, $\epsilon \geq \Pr[N = 0] > \frac{1}{n}$.

Case 2: Assume $\Pr[N = 0] = \frac{1}{n}$. If there exists an integer $j \neq a$ with $\Pr[N = j - a] > \Pr[N = j - b]$, then $A = \{a, j\}$ makes $\epsilon \geq Adv_{D_A}(a, b) = \Pr[N = 0] + \Pr[N = j - a] - \Pr[N = j - b] > \frac{1}{n}$.

If such a j does not exist, then $\Pr[N = x + b - a] \leq \Pr[N = x]$ for all $x \geq 0$ and by Lemma 1 we obtain $\epsilon = \Pr[N = 0] = \frac{1}{n}$. When $\Pr[N = x + b - a] = \Pr[N = x]$ for all $x \geq 0$, N becomes uniform and $\epsilon = \frac{1}{n}$. Note that we cannot have $\Pr[N = x + 1] < \Pr[N = x]$ for some x because this would make $\sum_{i=0}^{n-1} \Pr[N = i] < 1$, which contradicts the fact that N is a random variable.

Case 3: Let us assume that $\Pr[N = 0] < \frac{1}{n}$. Then $\frac{1}{n} - \Pr[N = 0] = \delta$ for some $\delta > 0$. Let $\sum_{i=1}^{n-1} (\Pr[N = i] - \Pr[N = i - 1]) \leq \delta$. Then $\Pr[N = i] \leq \frac{1}{n} - \delta + \delta$ for all $i \in [1, n-1]$. Therefore, $\sum_{i=0}^{n-1} \Pr[n = i] \leq \frac{1}{n} - \delta + (n-1)\frac{1}{n} = 1 - \delta$ which is not possible. So we must have $\sum_{i=1}^{n-1} (\Pr[N = i] - \Pr[N = i - 1]) > \delta$. Since $\Pr[N = 0] = \frac{1}{n} - \delta$, we get $\epsilon > \frac{1}{n}$.

Thus, in all of the cases $\epsilon \geq \frac{1}{n}$ and equality holds if and only if N is uniform.

□

Theorem 2. *If $b - a = \Delta$ and n is divisible by Δ, then $\max_A Adv_{D_A}(a, b) \geq \frac{\Delta}{n}$ and equality holds if and only if $\Pr[N < b - a] = \frac{\Delta}{n}$ and $\Pr[N = i]$ is periodic over $[0, \ldots, n - 1]$ with period Δ.*

Proof. Let $\epsilon = \max_A Adv_{D_A}(a, b)$.

Case 1: Assume $\Pr[N < \Delta] > \frac{\Delta}{n}$. Then for $A = \{a, a+1, \ldots, a+\Delta-1\}$, we have $\epsilon \geq Adv_{D_A}(a,b) = \Pr[N < \Delta] > \frac{\Delta}{n}$.

Case 2: Assume $\Pr[N < \Delta] = \frac{\Delta}{n}$. If there exists an integer $j > a+\Delta-1$ with $\Pr[N = j-a] > \Pr[N = j-b]$, then $A = \{a, a+1, \ldots, a+\Delta-1, j\}$ makes $\epsilon \geq Adv_{D_A}(a,b) = \Pr[N < \Delta] + \Pr[N = j-a] - \Pr[N = j-b] > \frac{\Delta}{n}$.

If such a j does not exist, then we have $\Pr[N = x+\Delta] \leq \Pr[N = x]$ for all $x \geq 0$. Note that when $\Pr[N = x+\Delta] = \Pr[N = x]$ for all $x \in [0, n-\Delta-1]$, by Lemma 1 we obtain $\epsilon = \frac{\Delta}{n}$ and $\Pr[N = i]$ becomes periodic over $[0, \ldots, n-1]$ with period Δ. Since n is divisible by Δ, we get $\Pr[j\Delta \leq N < (j+1)\Delta] \leq \frac{\Delta}{n}$ for all $j \in [0, \ldots, \frac{n}{\Delta}]$. Therefore, we have $1 = \sum_{i=0}^{n-1} \Pr[N = i] \leq \frac{n}{\Delta} \cdot \frac{\Delta}{n} = 1$. Thus, we cannot have $\Pr[N = x+\Delta] < \Pr[N = x]$ for any x.

Case 3: Assume $\Pr[N < \Delta] < \frac{\Delta}{n}$. Then $\frac{\Delta}{n} - \Pr[N < \Delta] = \delta$ for some $\delta > 0$. Since $\sum_{j=0}^{\frac{n}{\Delta}-1} \sum_{i=j\Delta}^{(j+1)\Delta-1} \Pr[N = i] = 1$ and $\sum_{i=0}^{\Delta-1} \Pr[N = i] = \frac{\Delta}{n} - \delta$, there must exist an integer j such that $\sum_{i=j\Delta}^{(j+1)\Delta-1} \Pr[N = i] > \frac{\Delta}{n} + \delta$. Thus, if we set $A = \{a, a+1, \ldots, a+(j+1)\Delta-1\}$, we obtain $\epsilon \geq Adv_{D_A}(a,b) > \frac{\Delta}{n}$.

Thus in all cases $\epsilon \geq \frac{\Delta}{n}$ and equality holds if and only if $\Pr[N < \Delta] = \frac{\Delta}{n}$ and $\Pr[N = i]$ is periodic over $[0, \ldots, n-1]$ with period Δ.

□

Remark 1. *If $b-a = \Delta$ and n is not divisible by Δ, ϵ can be less than $\frac{\Delta}{n}$.*

Example 1. *Let $b-a = \Delta = 2$ and $n = 5$. We define N as follows:*

$\Pr[N = 0] = \Pr[N = 2] = \Pr[N = 4] = 0.22$
$\Pr[N = 1] = \Pr[N = 3] = 0.17$

Thus, $\epsilon = \Pr[N = 0] + \Pr[N = 1] = 0.39$ which is less than $\frac{2}{5}$. However, if we keep this N and reduce Δ to 1, we get $\epsilon = \Pr[N = 0] + \Pr[N = 2] + \Pr[N = 4] - \Pr[N = 1] - \Pr[N = 3] = 0.32$. Thus, for $\Delta = 1$ and $\Delta = 2$, we have $\epsilon = 0.32$ and $\epsilon = 0.39$, respectively. Note that when N is uniform, for $\Delta = 1$ and $\Delta = 2$ we have $\epsilon = 0.2$ and $\epsilon = 0.4$, respectively.

Corollary 1. *If $b-a = \Delta$, then*

$$\max_A Adv_{D_A}(a,b) \geq \frac{1}{\lceil \frac{n}{\Delta} \rceil}.$$

Proof. Let $\epsilon = \max_A Adv_{D_A}(a,b)$.

Case 1: Assume $\Pr[N < \Delta] > \frac{1}{\lceil \frac{n}{\Delta} \rceil}$. Then for $A = \{a, a+1, \ldots, a+\Delta-1\}$, we have $\epsilon \geq Adv_{D_A}(a,b) = \Pr[N < \Delta] > \frac{1}{\lceil \frac{n}{\Delta} \rceil}$.

Case 2: Assume $\Pr[N < \Delta] = \frac{1}{\lceil \frac{n}{\Delta} \rceil}$. If there exists an integer $j > a + \Delta - 1$ with $\Pr[N = j-a] > \Pr[N = j-b]$, then $A = \{a, a+1, \ldots, a+\Delta-1, j\}$ makes $\epsilon \geq Adv_{D_A}(a,b) = \Pr[N < \Delta] + \Pr[N = j-a] - \Pr[N = j-b] > \frac{1}{\lceil \frac{n}{\Delta} \rceil}$.

If such a j does not exist, then we have $\Pr[N = x + \Delta] \leq \Pr[N = x]$ for all $x \geq 0$. Note that when $\Pr[N = x + \Delta] = \Pr[N = x]$ for all $x \in [0, n - \Delta - 1]$, by Lemma 1 we have $\epsilon = \frac{1}{\lceil \frac{n}{\Delta} \rceil}$ and $\Pr[N = i]$ becomes periodic over $[0, \ldots, n-1]$ with period Δ. Note that the periodicity of Δ divides $\Pr[N = i]$ into $\lceil \frac{n}{\Delta} \rceil$ intervals and when the sum of the probabilities in every interval is $\frac{1}{\lceil \frac{n}{\Delta} \rceil}$, we have $\sum_{i=0}^{n-1} \Pr[N = i] = \left\lceil \frac{n}{\Delta} \right\rceil \cdot \frac{1}{\lceil \frac{n}{\Delta} \rceil} = 1$. This property gives the restriction that $\Pr[N = \Delta - 1 - t] = \ldots = \Pr[N = \Delta - 1] = 0$ where t is the remainder of the division of n by Δ.

Case 3: Assume $\Pr[N < \Delta] < \frac{1}{\lceil \frac{n}{\Delta} \rceil}$. Then $\frac{1}{\lceil \frac{n}{\Delta} \rceil} - \Pr[N < \Delta] = \delta$ for some $\delta > 0$. Let $\sum_{i=\Delta}^{n-1} (\Pr[N = i] - \Pr[N = i - \Delta]) \leq \delta$. Then $\sum_{i=j\Delta}^{(j+1)\Delta-1} \Pr[N = i] \leq \frac{1}{\lceil \frac{n}{\Delta} \rceil} - \delta + \delta$ for all $j \in [1, \ldots, \frac{n}{\Delta} - 1]$. Therefore, $\sum_{i=1}^{n-1} \Pr[n = i] \leq \frac{1}{\lceil \frac{n}{\Delta} \rceil} - \delta + (\left\lceil \frac{n}{\Delta} \right\rceil - 1) \cdot \frac{1}{\lceil \frac{n}{\Delta} \rceil} = 1 - \delta$ which is not possible. So we must have $\sum_{i=\Delta}^{n-1} (\Pr[N = i] - \Pr[N = i - \Delta]) > \delta$. Since $\Pr[N < \Delta] = \frac{1}{\lceil \frac{n}{\Delta} \rceil} - \delta$, we get $\epsilon > \frac{1}{\lceil \frac{n}{\Delta} \rceil}$.

Thus in all cases $\epsilon \geq \frac{1}{\lceil \frac{n}{\Delta} \rceil}$ and equality holds if and only if $\Pr[N < \Delta] = \frac{1}{\lceil \frac{n}{\Delta} \rceil}$, $\Pr[N = i]$ is periodic over $[0, \ldots, n-1]$ with period Δ and $\Pr[N = \Delta - 1 - t] = \ldots = \Pr[N = \Delta - 1] = 0$ where t is the remainder of the division of n by Δ.

□

Example 2. *For any given n and Δ, note that the following distribution always satisfies the minimum advantage $\frac{1}{\lceil \frac{n}{\Delta} \rceil}$ that is given in Corollary 1.*

Let $\Pr[N = 0] = \frac{1}{\lceil \frac{n}{\Delta} \rceil}$, $\Pr[N = 1] = \ldots = \Pr[N = \Delta - 1] = 0$ *and let* $\Pr[N = i]$ *be periodic over* $[0, \ldots, n-1]$ *with period* Δ. *Then* $\sum_{i=0}^{n-1} \Pr[N = i] = \left\lceil \frac{n}{\Delta} \right\rceil \cdot \frac{1}{\lceil \frac{n}{\Delta} \rceil} = 1$ *and* $\max_A Adv_{D_A}(a, b) = \Pr[N = 0] = \frac{1}{\lceil \frac{n}{\Delta} \rceil}$.

However, $\max_{|b-a|=1} \max_A Adv_{D_A}(a, b) = 1$ *for this construction because of* $A = \{a, a + \Delta, a + 2\Delta \ldots\}$. *Therefore, Corollary 1 provides the lower bound* $\frac{1}{\lceil \frac{n}{\Delta} \rceil}$ *for* $\max_{|b-a| \leq \Delta} \max_A Adv_{D_A}(a, b)$ *but this lower bound may not be achievable.*

Theorem 3. *For* $b - a \leq \Delta$, *if* n *is divisible by* Δ *then for the optimal distribution* $\max_{|b-a| \leq \Delta} \max_A Adv_{D_A}(a, b) = \frac{\Delta}{n}$. *Otherwise*

$$\frac{\Delta}{n} \geq \max_{|b-a| \leq \Delta} \max_A Adv_{D_A}(a, b) \geq \frac{1}{\lceil \frac{n}{\Delta} \rceil}.$$

Proof. Let $\epsilon = \max_{|b-a| \leq \Delta} \max_A Adv_{D_A}(a, b)$.

Case 1: When n is divisible by Δ, by Theorem 2 we obtain $\epsilon \geq \frac{\Delta}{n}$ and it is clear that the uniform distribution satisfies the equality. Thus, $\epsilon = \frac{\Delta}{n}$ for the optimal distribution.

Case 2: When n is not divisible by Δ, by Corollary 1 we obtain $\epsilon \geq \frac{1}{\lceil \frac{n}{\Delta} \rceil}$ but this lower bound may not be achievable. Moreover, if we select N as the uniform distribution, then we obtain $\epsilon = \Pr[N < \Delta] = \frac{\Delta}{n}$.

Thus, $\frac{\Delta}{n} \geq \epsilon \geq \frac{1}{\lceil \frac{n}{\Delta} \rceil}$ for the optimal distribution and upper bound is achievable when N is uniform.

□

Theorem 4. *If* $b - a \leq 2$ *and* n *is odd, then for the optimal distribution*

$$\max_{|b-a|<2} \max_A Adv_{D_A}(a, b) = \frac{2n}{n^2 + 1}.$$

Proof. Let

$$\epsilon = \max_{|b-a|<2} \max_A Adv_{D_A}(a, b),$$

$$\epsilon_1 = \max_{|b-a|=1} \max_A Adv_{D_A}(a, b),$$

$$\epsilon_2 = \max_{|b-a|=2} \max_A Adv_{D_A}(a, b).$$

Case 1: Assume $\Pr[N=0]$ and $\Pr[N=1]$ are both higher than $\frac{1}{n}$. Then for $A=\{a,a+1\}$ we have $\epsilon \geq Adv_{D_A}(a,b) = \Pr[N<2] > \frac{2}{n}$ which is no better than N being uniform.

Case 2: Assume $\Pr[N=0]$ and $\Pr[N=1]$ are both less than $\frac{1}{n}$. Then $\Pr[N<2] = \frac{2}{n} - \delta$ for some $\delta > 0$. But in this case, in order to have $\sum_{i=0}^{n-1} \Pr[N=i] = 1$, the total increase in the probabilities must be more than δ as shown in case 3 of Theorem 1 and 2 (i.e. $\sum_{i=2}^{n-1}(\Pr[N=i] - \Pr[N=i-2]) > \delta$). Thus, $\epsilon_2 > \frac{2}{n}$.

Case 3: Assume one of $\Pr[N=0]$ and $\Pr[N=1]$ is higher than $\frac{1}{n}$ and the other is less than $\frac{1}{n}$. By Theorem 2 (or 3), we require $\Pr[N=i]$ to be periodic over $[0,\ldots,n-1]$ with period 2 to minimize the advantage. Let $\Pr[N=0] = \frac{1}{n} + \gamma$ and $\Pr[N=1] = \frac{1}{n} - \delta$ for some $\gamma, \delta > 0$.

Since $\sum_{i=0}^{n-1} \Pr[N=i] = 1$ and $\Pr[N=i]$ is periodic, we get $1 - \left(\frac{n-1}{2}\right)\delta + \left(\frac{n+1}{2}\right)\gamma = 1$. Thus, $\delta = \left(\frac{n+1}{n-1}\right)\gamma$.

Hence, $\epsilon_2 = \Pr[N<2] = \frac{2}{n} + \gamma - \delta = \frac{2}{n} - \frac{2\gamma}{n-1}$ and $\epsilon_1 = \Pr[N=0] + \sum_{i=1}^{\frac{n-1}{2}}(\Pr[N=2i] - \Pr[2i-1]) = \frac{1}{n} + \gamma + \left(\frac{n-1}{2}\right)(\gamma+\delta) = \frac{1}{n} + (n+1)\gamma$.

Note that ϵ is minimized when $\epsilon_1 = \epsilon_2$ and this equality is obtained when $\gamma = \frac{n-1}{n^3+n}$. Thus, $\epsilon \geq \frac{2n}{n^2+1}$.

For the final case where $\Pr[N=0] = \frac{1}{n} - \delta$ and $\Pr[N=1] = \frac{1}{n} + \gamma$, the assumption of the periodicity makes $\gamma > \delta$. Hence, for $A=\{a,a+1\}$ we obtain $\epsilon \geq Adv_{D_A}(a,b) = \Pr[N<2] > \frac{2}{n}$.

□

Theorem 4 shows that when $b-a \leq 2$ and n is odd, the lower bound $\frac{1}{\lceil \frac{n}{2} \rceil}$ for the maximum advantage is not achievable. Results of Theorem 3 and 4 for the case when $\Delta = 2$ and n is odd are provided in Table 2.1 for small values of n.

Table 2.1: Results of the Theorem 3 and 4 when $\Delta = 2$ and n is odd

n	Upper bound (Thm. 3)	Best Achievable (Thm. 4)	Lower Bound (Thm. 3)
3	0.666666666666667	0.6	0.5
5	0.4	0.384615384615385	0.333333333333333
7	0.285714285714286	0.28	0.25
9	0.222222222222222	0.219512195121951	0.2
11	0.181818181818182	0.180327868852459	0.166666666666667
13	0.153846153846154	0.152941176470588	0.142857142857143
15	0.133333333333333	0.132743362831858	0.125
17	0.117647058823529	0.117241379310345	0.111111111111111
19	0.105263157894737	0.104972375690608	0.1
21	0.0952380952380952	0.0950226244343891	0.0909090909090909
23	0.0869565217391304	0.0867924528301887	0.0833333333333333
25	0.08	0.0798722044728434	0.0769230769230769
27	0.0740740740740741	0.073972602739726	0.0714285714285714
29	0.0689655172413793	0.0688836104513064	0.0666666666666667
31	0.0645161290322581	0.0644490644490645	0.0625
33	0.0606060606060606	0.0605504587155963	0.0588235294117647
35	0.0571428571428571	0.0570962479608483	0.0555555555555556
37	0.0540540540540541	0.054014598540146	0.0526315789473684
39	0.0512820512820513	0.0512483574244415	0.05
41	0.0487804878048781	0.0487514863258026	0.0476190476190476
43	0.0465116279069767	0.0464864864864865	0.0454545454545455
45	0.0444444444444444	0.044225074037512	0.0434782608695652
47	0.0425531914893617	0.0425339366515837	0.0416666666666667
49	0.0408163265306122	0.0407993338884263	0.04
51	0.0392156862745098	0.0392006149116065	0.0384615384615385
53	0.0377358490566038	0.0377224199288256	0.037037037037037
55	0.0363636363636364	0.0363516192994052	0.0357142857142857
57	0.0350877192982456	0.0350769230769231	0.0344827586206897
59	0.0338983050847458	0.0338885697874785	0.0333333333333333
61	0.0327868852459016	0.0327780763030629	0.032258064516129
63	0.0317460317460317	0.0317380352644836	0.03125
65	0.0307692307692308	0.0307619498343587	0.0303030303030303
67	0.0298507462686567	0.0298440979955457	0.0294117647058824
69	0.0289855072463768	0.0289794204115918	0.0285714285714286
71	0.028169014084507	0.028163427211424	0.0277777777777778
73	0.0273972602739726	0.0273921200750469	0.027027027027027
75	0.0266666666666667	0.0266619267685745	0.0263157894736842
77	0.025974025974026	0.0259696458684654	0.0256410256410256
79	0.0253164556962025	0.025312399871836	0.025

Chapter 3

Results and Future Work

3.1 Results

We investigated the security of the $\Delta - IND - CPA$ game under the assumptions A_2 and A_3 and showed that when the maximum padding length n is divisible by Δ, the best security we can have is $\epsilon = \frac{\Delta}{n}$. Moreover, we showed that this ϵ-security can be obtained when the random variable N that defines the padding length is chosen as the uniform distribution.

Furthermore, when n is not divisible by Δ, we showed that for the optimal distribution the game is ϵ-secure where $\frac{\Delta}{n} \geq \epsilon \geq \frac{1}{\lceil \frac{n}{\Delta} \rceil}$. The upper bound can always be achieved by selecting N as the uniform distribution but it may not be possible to obtain the lower bound.

Finally, for $\Delta = 2$ and n is odd, we showed that $\epsilon = \frac{2n}{n^2+1}$ which also shows that the lower bound $\frac{1}{\lceil \frac{n}{\Delta} \rceil}$ is unachievable for this case.

3.2 Future Work

Although we found tight bounds for the case when n is not divisible by Δ, we do not know the optimal distribution and the corresponding best achievable advantage for this case.

Moreover, we assumed that the assumption A_2 holds throughout this work and A_2 is stronger than the assumption A_1. Hence, one can minimize the maximum advantage by replacing the assumption A_2 with A_1.