Analysis on Aigis-Enc: asymmetrical and symmetrical *

Yupu Hu[1[0000−0002−1977−0959]], Siyue Dong[1[0000−0001−9756−5742]], and Xingting Dong[1[0000−0001−8666−7209]]

Xidian University, Shaanxi Xi'an, China
yphu@mail.xidian.edu.cn
https://www.xidian.edu.cn
359442088@qq.com

Abstract. Aigis-Enc is an encryption algorithm based on asymmetrical LWE. In this algorithm, the compression process is utilized during both key generation and encryption (which is equivalent to add some LWR noise). Then encapsulation is realized by FO transformation. It is well known that FO transformation is not considered for discussing CPA security. On the other hand, since the security reduction of LWR is hard to proceed, it is not considered for discussing the CPA security of Aigis-Enc. But compression must be put into consideration when we discuss decryption failure probability. In other words, when we discuss the CPA security of Aigis-Enc, the compression and FO transformation are ignored. But when decryption failure probability is discussed, compression should be taken into consideration while FO transformation remains ignored.

According to the assumptions above, Aigis-Enc designers claim that the CPA security of Aigis-Enc is approximately equal to that of the symmetrical LWE scheme in the same scale, and the decryption failure probability of Aigis-Enc is far below that of the symmetrical LWE scheme in the same scale.

In this paper, we make a thorough comparison between Aigis-Enc (with the recommended parameters) and the symmetrical LWE encryption scheme in the same scale. Our conclusion is as followed:

(1) The comparison on CPA security. The former's is 160.898, and the latter's is 161.836.

(2) The comparison on computation complexity. In key generation phase, the ratio of the former and the latter on sampling amount of distribution $\begin{bmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ is 5:4; In encryption phase, that ratio is 19:14. The other computations remain the same.

(3) The comparison on decryption failure probability. The former's is $2^{-128.699}$, the latter's is $2^{-67.0582}$. The comparison seems to be dramatic. But in fact, we can slightly increase some traffic to keep failure

* This work was supported by the National Key R&D Program of China under Grants(No. 2017YFB0802000), National Natural Science Foundations of China(No. 61672412, No.61972457), National Cryptography Development Fund under Grant(No. MMJJ20170104).

probability unchanged. In other words, by compressing less to keep decryption failure probability unchanged. In specific: we change the parameters (d_1, d_2, d_3) from $(9, 9, 4)$ to $(10, 10, 4)$, which means a large part of the public key remains the same, the small part of the public key changes from 9 bits per entry into 10bits. A large part of the ciphertext changes from 9 bits per entry into 10 bits, the small part of the ciphertext remains the same. As thus, the communication traffic increases less than $\frac{1}{9}$, while the decryption failure probability is lower than $2^{-128.699}$.

We generalize those attacks presented by designers of Aigis-Enc, including primal attacks and dual attacks. More detailedly, our attacks are more extensive, simpler, and clearer. With them, we obtain the optimal attacks and "the optimal-optimal attack" on Aigis-Enc and the symmetrical LWE scheme in the same scale.

Keywords: LWE-based cryptosystem · primal attack · dual attack.

1 Preliminaries

LWE[1] is a quality cryptography primitive. The parameters of public key algorithm based on LWE are {modulus, noise size, compression ratio, number of rows, number of columns}, the optimization of these parameters will optimize the performance of an algorithm. That is, make the optimal balance of {calculated amount, security strength, decryption failure probability, communication traffic}.

Aigis-Enc[2] is an encryption algorithm based on asymmetrical LWE. In this algorithm, the compression process is utilized during both key generation and encryption (which is equivalent to add some LWR noise). Then encapsulation is realized by FO transformation[3,4]. It is well known that FO transformation is not considered for discussing CPA security. On the other hand, since the security reduction of LWR is hard to proceed, it is not considered for discussing the CPA security of Aigis-Enc. But compression must be put into consideration when we discuss decryption failure probability. In other words, when we discuss the CPA security of Aigis-Enc, the compression and FO transformation are ignored. But when decryption failure probability is discussed, compression should be taken into consideration while FO transformation remains ignored.

According to the assumptions above, Aigis-Enc designers claim that the CPA security of Aigis-Enc is approximately equal to that of the symmetrical LWE scheme in the same scale[5,6], and the decryption failure probability of Aigis-Enc is far below that of the symmetrical LWE scheme in the same scale.

In this paper, we make a thorough comparison between Aigis-Enc (with the recommended parameters) and the symmetrical LWE encryption scheme in the same scale. Our conclusion is as followed:

(1) The comparison on CPA security. The former's is 160.898, and the latter's is 161.836.

(2) The comparison on computation complexity. In key generation phase, the ratio of the former and the latter on sampling amount of distribution $\begin{bmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ is

5:4; In encryption phase, that ratio is 19:14. The other computations remain the same.

(3) The comparison on decryption failure probability. The former's is $2^{-128.699}$, the latter's is $2^{-67.0582}$. The comparison seems to be dramatic. But in fact, we can slightly increase some traffic to keep failure probability unchanged. In other words, by compressing less to keep decryption failure probability unchanged. In specific: we change the parameters (d_1, d_2, d_3) from $(9, 9, 4)$ to $(10, 10, 4)$, which means a large part of the public key remains the same, the small part of the public key changes from 9 bits per entry into 10bits. A large part of the ciphertext changes from 9 bits per entry into 10 bits, the small part of the ciphertext remains the same. As thus, the communication traffic increases less than $\frac{1}{9}$, while the decryption failure probability is lower than $2^{-128.699}$.

We generalize those attacks presented by designers of Aigis-Enc, including primal attacks and dual attacks. More detailedly, our attacks are more extensive, simpler, and clearer. With them, we obtain the optimal attacks and "the optimal-optimal attack" on Aigis-Enc and the symmetrical LWE scheme in the same scale.

2 Aigis-Enc and symmetrical LWE scheme in the same scale: with the recommended parameters without FO transformation

2.1 Conventions and some special notations

Due to the MLWE[7,8] structure Aigis-Enc has, we use some special notations to simplify our expression.

We name the square matrix $\begin{bmatrix} a_0 & a_1 & \cdots & a_{255} \\ -a_{255} & a_0 & \cdots & a_{254} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{bmatrix}$ a 256×256 rotation matrix.

For a 256-dimension vector $\mathbf{v} = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{255} \end{pmatrix}$, we denote a 256×256 square matrix $\mathbf{T}(\mathbf{v}) = \begin{bmatrix} v_0 & -v_{255} & \cdots & -v_1 \\ v_1 & v_0 & \cdots & -v_2 \\ \vdots & \vdots & \ddots & \vdots \\ v_{255} & v_{254} & \cdots & v_0 \end{bmatrix}$, and name it the transpose of vector $\mathbf{v}$.

For a 768-dimension vector $\mathbf{v} = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{767} \end{pmatrix}$, we denote a 256×768 matrix $\mathbf{T}(\mathbf{v}) = \left[\mathbf{T}\begin{pmatrix} v_0 \\ \vdots \\ v_{255} \end{pmatrix}, \mathbf{T}\begin{pmatrix} v_{256} \\ \vdots \\ v_{511} \end{pmatrix}, \mathbf{T}\begin{pmatrix} v_{512} \\ \vdots \\ v_{767} \end{pmatrix} \right]$, and name it the transpose of vector $\mathbf{v}$.

It is easy to see that, if $\mathbf{u}, \mathbf{v}$ are two 256-dimension or two 768-dimension column vectors, $\mathbf{T}(\mathbf{u}) \cdot \mathbf{v} = \mathbf{T}(\mathbf{v}) \cdot \mathbf{u}$.

Probability distribution $\boldsymbol{b}_\eta$ is a centered binomial distribution with parameter η. In particular $\boldsymbol{b}_1$ is the probability distribution $\begin{bmatrix} -1 & 0 & 1 \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \end{bmatrix}$.

Modulus $q = 7681$.

2.2 Aigis-Enc with the recommended parameters: without compression

Key generation: Set $\{\eta_1, \eta_2\} = \{1, 4\}$. A $\in \mathbb{Z}_q^{768 \times 768}$ is a special matrix which generated from 9 256×256 rotation matrices arranged in order.

Let $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, where $\mathbf{s} \stackrel{\$}{\longleftarrow} \boldsymbol{b}_{\eta_1}^{768}$, $\mathbf{e} \stackrel{\$}{\longleftarrow} \boldsymbol{b}_{\eta_2}^{768}$. The public key is $(\mathbf{A}, \mathbf{b})$, and the secret key is $(\mathbf{s}, \mathbf{A}, \mathbf{b})$.

Encryption: First, transform matrix $\mathbf{A}$ to $\mathbf{A}^T$, where $\mathbf{A}^T$ is the "transpose matrix" of $\mathbf{A}$ with respect to the 256×256 rotation sub-matrices (rather than with repect to entries).

Given a plaintext column vector $\mu = \begin{pmatrix} \mu_0 \\ \vdots \\ \mu_{255} \end{pmatrix}$, calculate the ciphertext $\{\mathbf{c_1}, \mathbf{c_2}\}$,

$$\begin{cases} \mathbf{c}_1 = \mathbf{A}^T \mathbf{r} + \mathbf{x}_1 \\ \mathbf{c}_2 = [\mathbf{T}(\mathbf{b})] \cdot \mathbf{r} + \mathbf{x}_2 + \mu \cdot \lceil \frac{q}{2} \rceil \end{cases}$$

where $\mathbf{r} \stackrel{\$}{\longleftarrow} \boldsymbol{b}_{\eta_1}^{768}$, $\mathbf{x}_1 \stackrel{\$}{\longleftarrow} \boldsymbol{b}_{\eta_2}^{768}$, $\mathbf{x}_2 \stackrel{\$}{\longleftarrow} \boldsymbol{b}_{\eta_2}^{256}$.

Decryption: Calculate

$$\begin{aligned} \mathbf{c} &= \begin{pmatrix} c_0 \\ \vdots \\ c_{255} \end{pmatrix} \\ &= \mathbf{c_2} - [\mathbf{T}(\mathbf{s})] \cdot \mathbf{c_1} \\ &= \mu \left\lceil \frac{q}{2} \right\rceil + \mathbf{x_2} + [\mathbf{T}(\mathbf{e})] \cdot \mathbf{r} - [\mathbf{T}(\mathbf{s})] \cdot \mathbf{x_1} \end{aligned}$$

Obtain $\mu_i = \begin{cases} 0 \ |c_i| \le \frac{q}{4} \\ 1 \ |c_i| > \frac{q}{4} \end{cases}$.

2.3 Aigis-Enc with the recommended parameters: with compression

Set $\{d_1,d_2,d_3\} = \{9,9,4\}$.

Key generation: Set $\{\eta_1,\eta_2\} = \{1,4\}$. A $\in \mathbb{Z}_q^{768\times 768}$ is a special matrix which generated from 9 256×256 rotation matrices arranged in order.

Let $\mathbf{b} = \mathbf{As} + \mathbf{e} + \overline{\mathbf{e}}$, where $\mathbf{s} \xleftarrow{\$} \boldsymbol{b}_{\eta_1}^{768}$, $\mathbf{e} \xleftarrow{\$} \boldsymbol{b}_{\eta_2}^{768}$,

$\overline{\mathbf{e}} = -(\mathbf{Ar} + \mathbf{e}(\text{mod}q))(\text{mod}2^{d_1})$. The public key is $(\mathbf{A},\mathbf{b})$, and the secret key is $(\mathbf{s},\mathbf{A},\mathbf{b})$.

Encryption: Transform matrix $\mathbf{A}$ to $\mathbf{A}^T$.

Given a plaintext column vector $\mu = \begin{pmatrix} \mu_0 \\ \vdots \\ \mu_{255} \end{pmatrix}$, calculate the ciphertext $\{\mathbf{c_1},\mathbf{c_2}\}$,

$$\begin{cases} \mathbf{c}_1 = \mathbf{A}^T\mathbf{r} + \mathbf{x}_1 + \overline{\mathbf{x}}_1 \\ \mathbf{c}_2 = [\mathbf{T}(\mathbf{b})] \cdot \mathbf{r} + \mathbf{x}_2 + \overline{\mathbf{x}}_2 + \mu \cdot \lceil \frac{q}{2} \rceil \end{cases}$$

where $\mathbf{r} \xleftarrow{\$} \boldsymbol{b}_{\eta_1}^{768}$, $\mathbf{x}_1 \xleftarrow{\$} \boldsymbol{b}_{\eta_2}^{768}$, $\mathbf{x}_2 \xleftarrow{\$} \boldsymbol{b}_{\eta_2}^{256}$, $\overline{\mathbf{x}}_1 = -(\mathbf{Ar} + \mathbf{x_1}(\text{mod}q))(\text{mod}2^{d_2})$, $\overline{\mathbf{x}}_2 = -([\mathbf{T}(\mathbf{b})] \cdot \mathbf{r} + \mathbf{x}_2(\bmod q))(\bmod 2^{d_3})$.

Decryption: Calculate

$$\begin{aligned} \mathbf{c} &= \begin{pmatrix} c_0 \\ \vdots \\ c_{255} \end{pmatrix} \\ &= \mathbf{c_2} - [\mathbf{T}(\mathbf{s})] \cdot \mathbf{c_1} \\ &= \mu \left\lceil \frac{q}{2} \right\rceil + \mathbf{x_2} + \overline{\mathbf{x}}_\mathbf{2} + [\mathbf{T}(\mathbf{e}) + \mathbf{T}(\overline{\mathbf{e}})] \cdot \mathbf{r} - [\mathbf{T}(\mathbf{s})] \cdot (\mathbf{x_1} + \overline{\mathbf{x}}_\mathbf{1}) \end{aligned}$$

Obtain $\mu_i = \begin{cases} 0 \ |c_i| \le \frac{q}{4} \\ 1 \ |c_i| > \frac{q}{4} \end{cases}$.

2.4 Symmetrical LWE scheme in the same scale: with and without compression

The scheme is almost the same as Aigis-Enc. The only difference is the sampling parameters $\{\eta_1,\eta_2\} = \{2,2\}$ instead of $\{1,4\}$.

3 Attack scenarios and resource (without compression)

3.1 Scenario 1 and resource

We randomly choose two plaintexts $\mu^{(1)}$ and $\mu^{(2)}$ and send them to the Oracle. The Oracle randomly chooses one to encrypt and return the ciphertext to us. Then we guess in $\{\mu^{(1)},\mu^{(2)}\}$ which plaintext is encrypted. When we obtain the returned ciphertext $\{\mathbf{c_1},\mathbf{c_2}\}$, correct guess on the value of $\mu^{(i)}$ enables us to acquire 1024 LWE samples:

$$\begin{pmatrix} \mathbf{c_1} \\ \mathbf{c_2} - \mu^{(i)} \cdot \lceil \frac{q}{2} \rceil \end{pmatrix} = \begin{bmatrix} \mathbf{A}^T \\ \mathbf{T}(\mathbf{b}) \end{bmatrix} \mathbf{r} + \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \end{pmatrix},$$

in the equation every component of the secret vector $\mathbf{r}$ obeys the probability distribution $\boldsymbol{b}_{\eta_1}$, every component of the noise vector $\begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \end{pmatrix}$ obeys the probability distribution $\boldsymbol{b}_{\eta_2}$.

3.2 Scenario 2 and resource

When we capture a random ciphertext $\{\mathbf{c_1}, \mathbf{c_2}\}$, we acquire 1024 LWE samples:

$$\begin{pmatrix} \mathbf{c_1} \\ 2\mathbf{c_2} \end{pmatrix} = \begin{bmatrix} \mathbf{A}^T \\ 2\mathbf{T}(\mathbf{b}) \end{bmatrix} \mathbf{r} + \begin{pmatrix} \mathbf{x_1} \\ 2\mathbf{x_2}+\mu \end{pmatrix},$$

in the equation every component of the secret vector $\mathbf{r}$ obeys the probability distribution $\boldsymbol{b}_{\eta_1}$, every component of $\mathbf{x_1}$ obeys the probability distribution $\boldsymbol{b}_{\eta_2}$, every component of $2\mathbf{x_2}+\mu$ has the standard deviation larger than $\sqrt{2}$ times of the standard deviation of $\boldsymbol{b}_{\eta_2}$.

3.3 Scenario 3 and resource

From public key we obtain the following 768 LWE samples:

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e},$$

in the equation every component of the secret vector $\mathbf{s}$ obeys the probability distribution $\boldsymbol{b}_{\eta_1}$, every component of the noise vector $\mathbf{e}$ obeys the probability distribution $\boldsymbol{b}_{\eta_2}$.

3.4 Advantaged scenario and resource

Because the noise vector in scenario 2 is larger than that in scenario 1, and in scenario 3 we obtain fewer LWE samples than in scenario 1, we believe scenario 1 is the advantaged attack scenario.

4 The security strength comparison under primal attacks

4.1 Traditional primal attack

$d \in \{770, 771, \ldots, 1025\}$, we consider the d-dimension lattice generated by the column vectors of the below matrix $\mathbf{B}$.

$$\mathbf{B} = \begin{bmatrix} c\mathbf{I}_{768} & 0 & c(\mathbf{A}^T)^{-1}\mathbf{c}_1 \\ -\mathbf{T}(\mathbf{b})^*(\mathbf{A}^T)^{-1} & q\mathbf{I}_{d-769} & \left(\mathbf{c}_2 - \mu^{(i)} \lceil \frac{q}{2} \rceil - \mathbf{T}(\mathbf{b})(\mathbf{A}^T)^{-1} \cdot \mathbf{c}_1\right)^* \\ 0 & 0 & t \end{bmatrix}$$

In the equation $\mathbf{T}(\mathbf{b})^*$ is the matrix constructed from $d-769$ rows of $\mathbf{T}(\mathbf{b})$, $\left(\mathbf{c}_2 - \mu^{(i)}\left\lceil \frac{q}{2}\right\rceil - \mathbf{T}(\mathbf{b})(\mathbf{A}^T)^{-1}\cdot \mathbf{c}_1\right)^*$ is the vector constructed from the corresponding $d-769$ components of $\mathbf{c}_2 - \mu^{(i)}\left\lceil \frac{q}{2}\right\rceil - \mathbf{T}(\mathbf{b})(\mathbf{A}^T)^{-1}\cdot \mathbf{c}_1$, $\mu^{(i)}$ is the correct plaintext. $c>0$, $t>0$, (c,t) are the tunable parameters. We also know $\left(c\cdot \mathbf{r}^T, \mathbf{x}_2^{*T}, t\right)^T$ is a small vector of the regarding lattice, where $\mathbf{x}_2^*$ is the vector constructed from $d-769$ components of the encryption noise vector $\mathbf{x}_2$. The size of the small vector is $\sqrt{c^2\times 768\times \frac{\eta_1}{2} + (d-769)\times\frac{\eta_2}{2} + t^2}$ approximately. The aim of the attack is to find the small vector. It isn't difficult to see "the traditional primal attack"[9,10,11] the designers of Aigis-Enc proposed is included in our traditional primal attack.

4.2 Transformed primal attack

$d\in\{770, 771, \ldots, 1793\}$, we consider the lattice generated by the column vectors of the below matrix $\mathbf{B}$.

$$\mathbf{B}=\begin{bmatrix} c\mathbf{I}_{768} & 0 & 0 \\ \begin{bmatrix}\mathbf{A}^T\\ \mathbf{T}(\mathbf{b})\end{bmatrix}^* & q\mathbf{I}_{d-769} & \begin{pmatrix}\mathbf{c}_1\\ \mathbf{c}_2\end{pmatrix}^* \\ 0 & 0 & t\end{bmatrix}$$

In the equation $\begin{bmatrix}\mathbf{A}^T\\ \mathbf{T}(\mathbf{b})\end{bmatrix}^*$ is the matrix constructed from $d-769$ rows of $\begin{bmatrix}\mathbf{A}^T\\ \mathbf{T}(\mathbf{b})\end{bmatrix}$, $\begin{pmatrix}\mathbf{c}_1\\ \mathbf{c}_2\end{pmatrix}^*$ is the vector constructed from the corresponding $d-769$ components of $\begin{pmatrix}\mathbf{c}_1\\ \mathbf{c}_2\end{pmatrix}$. $c>0$, $t>0$, (c,t) are the tunable parameters. We also know $\left(c\cdot\mathbf{r}^T, \mathbf{x}^{*T}, t\right)^T$ is the small vector of the regarding lattice, where $\mathbf{x}^*$ is the vector constructed from $d-769$ corresponding components of the encryption noise vector $\begin{pmatrix}\mathbf{x}_1\\ \mathbf{x}_2\end{pmatrix}$. The size of the small vector $\ell = \sqrt{c^2\times 768\times\frac{\eta_1}{2} + (d-769)\times\frac{\eta_2}{2} + t^2}$. The aim of the attack is to find the small vector. It isn't difficult to see "the transformed primal attack 1" and "the transformed primal attack 2"[12,13] the designers of Aigis-Enc proposed are included in our transformed primal attack.

4.3 Optimal primal attack

The classic complexity of our primal attack is $2^{0.292b}$ (The quantum complexity is $2^{0.265b}$), the parameter b is as small as possible, while satisfying $b\in[100,d]$, and

$$\left(\frac{b}{d}\right)^{\frac{1}{2}}\cdot\left((\pi b)^{\frac{1}{b}}\cdot\frac{b}{2\pi e}\right)^{\frac{d^2-2bd+d}{2(b-1)(d-1)}} \le \frac{(\det(\mathbf{B}))^{\frac{1}{d}}}{\ell}$$

The above inequality comes from the work of previous contributors[14], we no longer take time to verify its rationality. Notice the following five facts:

(1) The left part of the above inequality is independent of the tunable parameters (c, t);

(2) The left part of the above inequality is a decreasing function of b when $b \in [100, d]$;

(3) No matter in the traditional or the transformed primal attack scenario, the right part of the above inequality has the same expression $f(c, t)$, and

$$f(c,t) = \frac{c^{\frac{768}{d}} \cdot q^{\frac{d-769}{d}} \cdot t^{\frac{1}{d}}}{\sqrt{c^2 \times 768 \times \frac{\eta_1}{2} + (d-769) \times \frac{\eta_2}{2} + t^2}};$$

(4) For any fixed $t > 0$, $\lim_{c \to 0^+} f(c,t) = 0$, $\lim_{c \to +\infty} f(c,t) = 0$;

(5) For any fixed $c > 0$, $\lim_{t \to 0^+} f(c,t) = 0$, $\lim_{t \to +\infty} f(c,t) = 0$.

Take all the five facts above into consideration, we know that if $f(c, t)$ has a single stationary point (c_0, t_0) in $\{c > 0, t > 0\}$, it must be the global maximum point of $f(c, t)$. Put (c_0, t_0) into the above inequality we can acquire the minimum point of b. In other words, the primal attack using (c_0, t_0) as parameters is the optimal primal attack. Fortunately, $f(c, t)$ does have a single stationary point (c_0, t_0) in $\{c > 0, t > 0\}$, where

$$(c_0, t_0) = \begin{cases} (2, \sqrt{2}), & \text{when } \eta_1 = 1, \eta_2 = 4 \\ (1, \quad 1), & \text{when } \eta_1 = \eta_2 = 2 \end{cases}$$

Notice that the stationary point (c_0, t_0) is independent of dimension d. Therefore, we obtain Proposition 1:

Proposition 1. *For any fixed dimension $d \in \{770, \ldots, 1793\}$,*

(1) *The parameters of the optimal primal attack on Aigis-Enc are $(c, t) = (2, \sqrt{2})$.*

(2) *The parameters of the optimal primal attack on the symmetrical LWE scheme in the same scale are $(c, t) = (2, \sqrt{2})$.*

4.4 The comparison of the complexity of the optimal primal attack and "the optimal-optimal primal attack"

We provide 13 sets of data in Table 1, under 13 different value of d, we list the classic complexity of the optimal attack on Aigis-Enc and the symmetrical LWE scheme in the same scale.

The so-called "the optimal-optimal primal attack" is the optimal attack with a further optimized dimension d. It can be observed in Table 1 that the complexity of the "the optimal-optimal primal attack" on Aigis-Enc is $2^{162.542}$, that on the symmetrical LWE scheme in the same scale is $2^{163.443}$.

5 The security strength comparison under dual attacks

5.1 Our dual attack

We consider the following 768 "trivial LWE samples":

$$\mathbf{o} = -\mathbf{I}_{768}\mathbf{r} + \mathbf{r},$$

Table 1. The classic complexity of the optimal primal attack

d	on Aigis-Enc	on the symmetrical LWE scheme in the same scale
1022	$2^{194.977}$	$2^{209.027}$
1025	$2^{194.226}$	$2^{208.03}$
1175	$2^{171.152}$	$2^{177.275}$
1325	$2^{163.538}$	$2^{166.178}$
1369	$2^{162.808}$	$2^{164.757}$
1395	$2^{162.601}$	$2^{164.186}$
1415	$\underline{\mathbf{2^{162.542}}}$	$2^{163.866}$
1440	$2^{162.579}$	$2^{163.596}$
1490	$2^{162.98}$	$\underline{\mathbf{2^{163.443}}}$
1519	$2^{163.388}$	$2^{163.56}$
1540	$2^{163.755}$	$2^{163.728}$
1619	$2^{165.604}$	$2^{164.899}$
1793	$2^{171.659}$	$2^{169.751}$

where $\mathbf{o} \in \mathbb{Z}_q^{768}$ is a column vector which components are all 0s. Therefore, we have the following 1792 LWE samples in total:

$$\begin{pmatrix} \mathbf{o} \\ \mathbf{c}_1 \\ \mathbf{c}_2 - \mu^{(i)} \left\lceil \frac{q}{2} \right\rceil \end{pmatrix} = \begin{bmatrix} -\mathbf{I}_{768} \\ \mathbf{A}^T \\ \mathbf{T}(\mathbf{b}) \end{bmatrix} \mathbf{r} + \begin{pmatrix} \mathbf{r} \\ \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix}.$$

Set $d \in \{769, \ldots, 1792\}$, and we only consider the d LWE samples below:

$$\begin{pmatrix} \mathbf{o} \\ \begin{pmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 - \mu^{(i)} \left\lceil \frac{q}{2} \right\rceil \end{pmatrix}^* \end{pmatrix} = \begin{bmatrix} -\mathbf{I}_{768} \\ \begin{bmatrix} \mathbf{A}^T \\ \mathbf{T}(\mathbf{b}) \end{bmatrix}^* \end{bmatrix} \mathbf{r} + \begin{pmatrix} \mathbf{r} \\ \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix}^* \end{pmatrix},$$

we denote $\mathbf{A}^* = \begin{bmatrix} \mathbf{A}^T \\ \mathbf{T}(\mathbf{b}) \end{bmatrix}^* \in \mathbb{Z}_q^{(d-768)\times 768}$, then we have

$$\begin{bmatrix} \mathbf{A}^* \ \mathbf{I}_{d-768} \end{bmatrix} \begin{bmatrix} -\mathbf{I}_{768} \\ \mathbf{A}^* \end{bmatrix} (\mathrm{mod} q)$$

is a matrix which entries are all 0s. Now the rationality of Lemma 1 is obvious.

Lemma 1. *For any real number $c > 0$,*

(1) $\begin{bmatrix} \mathbf{A}^* & c\mathbf{I}_{d-768} \end{bmatrix} \begin{bmatrix} -\mathbf{I}_{768} \\ \frac{1}{c}\mathbf{A}^* \end{bmatrix} (\bmod q)$ *is a matrix which entries are all 0s.*

(2) $$\begin{bmatrix} \mathbf{A}^* & c\mathbf{I}_{d-768} \end{bmatrix} \begin{pmatrix} \mathbf{o} \\ \frac{1}{c}\begin{pmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 - \mu^{(i)} \left\lceil \frac{q}{2} \right\rceil \end{pmatrix}^* \end{pmatrix} (\bmod q)$$
$$= \begin{bmatrix} \mathbf{A}^* & c\mathbf{I}_{d-768} \end{bmatrix} \begin{pmatrix} \mathbf{r} \\ \frac{1}{c}\begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix}^* \end{pmatrix} (\bmod q).$$

We consider the lattice generated by the row vectors of the below matrix $\mathbf{B}$:

$$\mathbf{B} = \begin{bmatrix} q\mathbf{I}_{768} & 0 \\ \mathbf{A}^* & c\mathbf{I}_{d-768} \end{bmatrix}$$

where $c > 0$ is a tunable parameter. From Lemma 1 (1), this lattice is the entire set of row vectors $\mathbf{v}$ which satisfy

$$\mathbf{v} \begin{bmatrix} -\mathbf{I}_{768} \\ \frac{1}{c}\mathbf{A}^* \end{bmatrix} (\bmod q) = (0, \ldots, 0)$$

Searching for a small vector $\mathbf{v}$ (row vector) on the lattice. From Lemma 1 (2), we can calculate

$$\mathbf{v} \begin{pmatrix} \mathbf{o} \\ \frac{1}{c}\begin{pmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 - \mu^{(i)} \left\lceil \frac{q}{2} \right\rceil \end{pmatrix}^* \end{pmatrix} (\bmod q) = \mathbf{v} \begin{pmatrix} \mathbf{r} \\ \frac{1}{c}\begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix}^* \end{pmatrix} (\bmod q)$$

The aim of our attack is to distinguish $\mathbf{v} \begin{pmatrix} \mathbf{r} \\ \frac{1}{c}\begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix}^* \end{pmatrix} (\bmod q)$ from some uniform value. Our attack includes all the dual attacks the designers of Aigis-Enc proposed, including "the traditional dual attack"[15], "the transformed dual attack 1", "the transformed dual attack 2"[13] and "the transformed dual attack 3"[16]. To be more specific:

(1) "The traditional dual attack" and "the transformed dual attack 1" the designers of Aigis-Enc proposed is equivalent to our dual attack when $c = 1$; "The transformed dual attack 3" the designers of Aigis-Enc proposed is equivalent to our dual attack when $c = 2^{\frac{\sqrt{d-768}}{\sqrt{768}}}$. And we can prove: for any $d \in \{769, \ldots, 1792\}$, the parameter of the optimal dual attack on Aigis-Enc is $c = 2$ rather than $c = 1$ or $c = 2^{\frac{\sqrt{d-768}}{\sqrt{768}}}$.

(2) "The transformed dual attack 2" the designers of Aigis-Enc proposed is equivalent to our dual attack when $c = 2$. Although it indeed is the optimal dual attack on Aigis-Enc, but they only declare the attack is superior to the attack when $c = 1$.

5.2 Optimal dual attack

From the work of the previous contributors, the complexity of dual attack is

$$\max\left\{1, \frac{\exp(4\pi^2\tau^2)}{2^{0.2075\cdot b}\cdot 16}\right\} e^{0.292b},$$

where $\tau = \frac{\ell\cdot\ell'}{\sqrt{d\cdot q}}$, ℓ is the size of the small vector $\mathbf{v}$ on the lattice. ℓ' is the size of the small vector operating inner product with $\mathbf{v}$ on the lattice. The small vector is $\begin{pmatrix} \mathbf{r} \\ \frac{1}{c}\begin{pmatrix}\mathbf{x}_1 \\ \mathbf{x}_2\end{pmatrix}^* \end{pmatrix}$, and the size of it is

$$\ell' = \frac{1}{c}\sqrt{c^2\times 768\times\frac{\eta_1}{2} + (d-768)\times\frac{\eta_2}{2}}.$$

The size of the small vector $\mathbf{v}$ on the lattice is estimated to be $\ell = \left((\pi b)^{\frac{1}{b}}\cdot\frac{b}{2\pi e}\right)^{\frac{d}{2(b-1)}}\cdot (\det(\mathbf{B}))^{\frac{1}{d}}$. Therefore, we have:

$$\ell\cdot\ell' = \left((\pi b)^{\frac{1}{b}}\cdot\frac{b}{2\pi e}\right)^{\frac{d}{2(b-1)}}\cdot q^{\frac{768}{d}}\cdot c^{\frac{-768}{d}}\cdot\sqrt{c^2\times 768\times\frac{\eta_1}{2} + (d-768)\times\frac{\eta_2}{2}}.$$

For any fixed (d,b), $0<b<d$, it satisfies $\lim\limits_{c\to 0^+}\ell\cdot\ell' = +\infty$, $\lim\limits_{c\to+\infty}\ell\cdot\ell' = +\infty$. Therefore, if a single stationary point of $\ell\cdot\ell'$ in $c>0$ exists, it will be the global minimum point where the classic complexity of dual attack is the lowest. In [13], the contributor indicates that when $\eta_1 = \eta_2$, the single stationary point is $c=1$, that means the parameter of the optimal dual attack is $c=1$. The designers of Aigis-Enc indicate that when $(\eta_1,\eta_2) = (1,4)$, the dual attack can be more effective if we choose $c=2$ rather than $c=1$. Our conclusion is the following Proposition 2.

Proposition 2. *For any $d\in\{769,\ldots,1024,1537,\ldots,1792\}$, the parameter of the optimal dual attack on Aigis-Enc is $c=2$.*

The value of c is determined, it is time to determine the value of b. Since we only have $b\le d$, the value of b is hard to be determined. Therefore, we make a conservative estimation, its classic complexity is

$$\min_{100\le b\le d}\left\{\max\left\{1, \frac{\exp\left(4\pi^2\tau^2\right)}{2^{0.2075b}\cdot 16}\right\}\cdot 2^{0.292b}\right\}.$$

5.3 The comparison of the complexity of the optimal dual attack and "the optimal-optimal dual attack"

It is trivial to obtain that the classic complexity of the optimal dual attack on Aigis-Enc is

$$\min_{100\le b\le d}\left\{\max\left\{1, \frac{\exp\left(4\pi^2\left((\pi b)^{\frac{1}{b}}\cdot\frac{b}{2\pi e}\right)^{\frac{d}{b-1}}\cdot 7681^{\frac{1536-2d}{d}}\cdot 2^{\frac{d-1536}{d}}\right)}{2^{0.2075b}\cdot 16}\right\}\cdot 2^{0.292b}\right\},$$

and that on the symmetrical LWE scheme in the same scale is

$$\min_{100\le b\le d}\left\{\max\left\{1, \frac{\exp\left(4\pi^2\left((\pi b)^{\frac{1}{b}}\cdot\frac{b}{2\pi e}\right)^{\frac{d}{b-1}}\cdot 7681^{\frac{1536-2d}{d}}\right)}{2^{0.2075b}\cdot 16}\right\}\cdot 2^{0.292b}\right\}.$$

Therefore, the rationality of below Proposition 3 is obvious.

Proposition 3. *When dimension $d < 1536$, the classic complexity of the optimal dual attack on Aigis is no higher than that on the symmetrical LWE scheme in the same scale; when dimension $d \geq 1536$, the classic complexity of the optimal dual attack on Aigis is no lower than that on the symmetrical LWE scheme in the same scale.*

We provide 13 sets of data in Table 2, under 13 different value of d, we list the classic complexity of the dual attack on Aigis-Enc and the symmetrical LWE scheme in the same scale.

It can be observed in Table 2 that the complexity of the "the optimal-optimal dual attack" on Aigis-Enc is $2^{160.898}$, that on the symmetrical LWE scheme in the same scale is $2^{161.836}$.

5.4 Comparison on the CPA classic security strength (without compression)

Combine the content of section 4 and sub-sections 5.1∼5.3, the CPA classic security strength of Aigis-Enc is 160.898, the CPA classic security strength of the symmetrical LWE scheme is 161.836.

6 Comparison on calculated amout

A basic calculation is the sampling of probability distribution $\chi = \begin{bmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$.

In the key generation phase, χ is sampled $(8+2)\times 768 = 7680$ times in Aigis, and $(4+4)\times 768 = 6144$ times in the symmetrical LWE scheme in the same scale, the former is the $\frac{5}{4}$ times of the latter. Certainly, sampling of χ may be

Table 2. The classic complexity of the optimal dual attack

d	on Aigis-Enc	on the symmetrical LWE scheme in the same scale
1022	$2^{192.102}$	$2^{205.835}$
1300	$2^{162.385}$	$2^{165.408}$
1354	$2^{162.275}$	$2^{163.406}$
1380	$2^{161.013}$	$2^{162.767}$
1400	$2^{160.914}$	$2^{162.4}$
1420	$\underline{\mathbf{2^{160.898}}}$	$2^{162.131}$
1480	$2^{161.285}$	$\underline{\mathbf{2^{161.836}}}$
1500	$2^{161.542}$	$2^{161.888}$
1520	$2^{161.855}$	$2^{162.005}$
1535	$2^{162.125}$	$2^{162.134}$
1544	$2^{162.3}$	$2^{162.227}$
1600	$2^{163.602}$	$2^{163.049}$
1649	$2^{165.004}$	$2^{164.071}$

not accounted for the main calculated amount in key generation phase, because the public key matrix is also sampled uniformly.

In the encryption phase, χ is sampled $2 \times 768 + 8 \times 1024 = 9728$ times in Aigis, and $4 \times 768 + 4 \times 1024 = 7168$ times in the symmetrical LWE scheme in the same scale, the former is the $\frac{19}{14}$ times of the latter. More importantly, sampling of χ is accounted for a significant part of the calculated amount in encryption phase.

As for other calculated amount, there is no difference bewteen Aigis and the symmetrical LWE scheme in the same scale.

7 Comparison on decryption failure probability (with compression)

The decryption error vector is $\mathbf{x_2} + \overline{\mathbf{x}}_\mathbf{2} + (\mathbf{T}(\mathbf{e}) + \mathbf{T}(\overline{\mathbf{e}})) \cdot \mathbf{r} + \mathbf{T}(\mathbf{s}) \cdot (\mathbf{x_1} + \overline{\mathbf{x}}_\mathbf{1})$, the decryption failure probability is identical to the probability of the random event below:

$$\frac{4}{q} \left| \mathbf{x_2} + \overline{\mathbf{x}}_\mathbf{2} + (\mathbf{T}(\mathbf{e}) + \mathbf{T}(\overline{\mathbf{e}})) \cdot \mathbf{r} + \mathbf{T}(\mathbf{s}) \cdot (\mathbf{x_1} + \overline{\mathbf{x}}_\mathbf{1}) \right| \geq 1$$

The probability distribution of $\frac{4}{q}\left(\mathbf{x_2}+\left(\mathbf{T}\left(\mathbf{e}\right)+\mathbf{T}\left(\overline{\mathbf{e}}\right)\right)\cdot\mathbf{r}+\mathbf{T}\left(\mathbf{s}\right)\cdot\left(\mathbf{x_1}+\overline{\mathbf{x}}_\mathbf{1}\right)\right)$ can be regarded as normal distribution, but that of $\frac{4}{q}\cdot\overline{\mathbf{x}}_\mathbf{2}$ can only be regarded as uniform distribution. Therefore, we need to find in the probability of the event, where the sum of a normal variable and uniform variable is no lower than 1. Our simplified method is to approximate the uniform variable to a variable which has equal probabilities on 41 points. The result of our approximate calculation is as followed:

The decryption failure probability of Aigis-Enc is $2^{-128.699}$,

The decryption failure probability of the symmetrical LWE scheme in the same scale is $2^{-67.0582}$. The comparison seems to be dramatic. But in fact, we can slightly increase some traffic to keep the decryption failure probability unchanged. In other words, by compressing less to keep the decryption failure probability unchanged. In specific: we change the parameters (d_1, d_2, d_3) from $(9, 9, 4)$ to $(10, 10, 4)$, which means a large part of the public key remains the same, the small part of the public key changes from 9 bits per entry to 10 bits, a large part of the ciphertext changes from 9 bits per entry to 10 bits, the small part of the ciphertext remains the same. As thus, the communication traffic increases less than $\frac{1}{9}$, while the decryption failure probability is lower than $2^{-128.699}$.

References

1. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.
2. Jiang Zhang and Yu Yu and Shuqin Fan and Zhenfeng Zhang and Kang Yang. Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: KEMs and Signatures of Smaller Sizes. IACR Cryptology ePrint Archive report 2019/510, 2019. https://eprint.iacr.org/2019/510.
3. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, *CRYPTO 1999*, volume 1666 of *LNCS*, pages 537–554. Springer, 1999.
4. Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the fujisaki-okamoto transformation. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography – TCC 2017*, volume 10677 of *LNCS*, pages 341–371. Springer International Publishing, 2017.
5. J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle. Crystals - kyber: A cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 353–367, April 2018.
6. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. In Aggelos Kiayias, editor, *Topics in Cryptology – CT-RSA 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer Berlin Heidelberg, 2011.
7. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. Fully homomorphic encryption without bootstrapping. *Innovations in Theoretical Computer Science, ITCS*, pages 309–325, 2012.
8. Damien Stehlé Adeline Langlois. Worst-case toaverage-casereductions for module-lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

9. Ravi Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, 12(3):415–440, 1987.
10. Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving usvp and applications to lwe. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 297–322, Cham, 2017. Springer International Publishing.
11. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. In Aggelos Kiayias, editor, *Topics in Cryptology – CT-RSA 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer Berlin Heidelberg, 2011.
12. Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary lwe. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy*, pages 322–337, Cham, 2014. Springer International Publishing.
13. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange— a new hope. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 327–343, Austin, TX, 2016. USENIX Association.
14. Yuanmi Chen. Lattice reduction and concrete security of fully homomorphic encryption. *Dept. Informatique, ENS, Paris, France, PhD thesis*, 2013.
15. Daniele Micciancio and Oded Regev. Lattice-based cryptography. In DanielJ. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*, pages 147–191. Springer Berlin Heidelberg, 2009.
16. Martin R. Albrecht. On dual lattice attacks against small-secret lwe and parameter choices in helib and seal. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 103–129, Cham, 2017. Springer International Publishing.