Analysis on Aigis-Enc: Asymmetrical and symmetrical

Yupu Hu | Siyue Dong | Xingting Dong

Xidian University, X’ian, Shaanxi, China

Correspondence
Yupu Hu, Xidian University, X’ian, Shaanxi, China.
Email: yphu@mail.xidian.edu.cn

Abstract
Aigis-Enc is an encryption algorithm based on asymmetrical learning with errors (LWE). A thorough comparison between Aigis-Enc (with the recommended parameters) and a symmetrical LWE encryption scheme on the same scale (the sampling parameters are \( \eta_1, \eta_2 = \{2, 2\} \) instead of \( \{1, 4\} \)) on Chosen-plaintext attack (CPA) security, computation complexity and decryption failure probability is made. In particular, the authors ascertain that the CPA security of Aigis-Enc is 160.895, and that of the symmetrical LWE encryption scheme on the same scale is 161.834. The ratio of computation complexity on the sampling amount of the former and the latter is 5:4 in the key generation phase and 19:14 in the encryption phase. The decryption failure probability of the former is \( 2^{-128.699} \) and that of the latter is \( 2^{-67.0582} \), then the authors show how to reduce the decryption failure probability of the latter significantly by increasing some traffic. Furthermore, those attacks presented by designers of Aigis-Enc, including primal attacks and dual attacks are generalised. Our attacks are more extensive, simpler, and clearer. With them, the optimal attacks and the ‘optimal-optimal attacks’ on Aigis-Enc and the symmetrical LWE scheme on the same scale are obtained.

1 | INTRODUCTION

Learning with errors (LWE) [1] is an excellent cryptographic primitive. Currently, most of the state-of-the-art lattice cryptosystems are based on the LWE problems and small integer solutions problems [2,3]. 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 optimise the performance of an algorithm. In other words, the goal is to make the optimal balance of (calculated amount, security strength, decryption failure probability, communication traffic).

Aigis-Enc [4,5] is an encryption algorithm based on asymmetrical LWE (ALWE), that is, the secret key \( s \) and noise \( e \) are sampled from different distributions. The designers of Aigis-Enc indicate that the framework design of Aigis-Enc is inspired from the works Bos et al. and Cheon et al. [6,7]. The security foundation of the ALWE problem comes from previous works [8–10].

Compression process is utilised in both key generation and encryption phases of Aigis-Enc (which is equivalent to add some learning with rounding (LWR) noise). Then encapsulation is realised by Fujisaki-Okamoto (FO) transformation [11,12]. It is well known that FO transformation is not considered when we discuss Chosen-plaintext attack (CPA) security. On the other hand, since the security reduction of LWR is hard to proceed, compression is not considered when we discuss 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, 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 above assumptions, Aigis-Enc designers claim that the CPA security of Aigis-Enc is approximately equal to that of the symmetrical LWE scheme on the same scale, and the decryption failure probability of Aigis-Enc is far below that of the symmetrical LWE scheme on the same scale.

We make a thorough comparison between Aigis-Enc (with the recommended parameters) and the symmetrical LWE encryption scheme on the same scale. Our conclusion is as follows:

1) The comparison on CPA security. The former's is 160.895, and the latter's is 161.834.
2) The comparison on computation complexity. In the key generation phase, the ratio of the former and the latter on
Due to the module learning with errors structure Aigis-Enc has, we use some special notations to simplify our expressions.

We name the square matrix 
\[
\begin{bmatrix}
  0 & 1 \\
  1 & 1 \\
  2 & 2
\end{bmatrix}
\]

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

(3) The comparison on decryption failure probability. The former's is \(2^{-128.609}\), 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 particular, we change the compression 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 10 bits. A large part of the ciphertext changes from 9 bits per entry into 10 bits, the small part of the ciphertext remains the same. Thus, the communication traffic increases less than \(\frac{1}{9}\); while the decryption failure probability is lower than \(2^{-128.609}\).

We generalise 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-attacker’ on Aigis-Enc and the symmetrical LWE scheme on the same scale.

2 AIGIS-ENC AND SYMMETRICAL LWE SCHEME ON THE SAME SCALE: WITH THE RECOMMENDED PARAMETERS WITHOUT FOURIER TRANSFORMATION

2.1 Conventions and some special notations

Due to the module learning with errors structure Aigis-Enc has, we use some special notations to simplify our expression.

We name the square matrix 
\[
\begin{bmatrix}
  a_0 & a_1 & \cdots & a_{255} \\
  -a_{255} & a_0 & \cdots & a_{254} \\
  \vdots & \vdots & \ddots & \vdots \\
  -a_1 & -a_2 & \cdots & a_0
\end{bmatrix}
\]

256 \times 256 rotation matrix.

For a 256-dimensional vector \(\mathbf{v} = \left(\begin{array}{c}
\varphi_0 \\
\varphi_1 \\
\vdots \\
\varphi_{254} \\
\varphi_{255}
\end{array}\right)\), we denote a 256 \times 256 matrix 
\[
\mathbf{T}(\mathbf{v}) = \left[\begin{array}{c}
\varphi_0 \\
\varphi_1 \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{511} \\
\varphi_{512} \\
\varphi_{513} \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{255} \\
\varphi_{256}
\end{array}\right],
\]

and name it the transpose of vector \(\mathbf{v}\).

For a 768-dimensional vector \(\mathbf{v} = \left(\begin{array}{c}
\varphi_0 \\
\varphi_1 \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{511} \\
\varphi_{512} \\
\varphi_{513} \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{255} \\
\varphi_{256}
\end{array}\right)\), we denote a 256 \times 768 matrix 
\[
\mathbf{T}(\mathbf{v}) = \left[\begin{array}{c}
\varphi_0 \\
\varphi_1 \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{511} \\
\varphi_{512} \\
\varphi_{513} \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{255} \\
\varphi_{256} \\
\vdots \\
\varphi_{255} \\
\varphi_{256}
\end{array}\right],
\]

and name it the transpose of vector \(\mathbf{v}\).

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

Probability distribution \(\mathbf{b}_j\) is a centred binomial distribution with parameter \(\eta\). In particular \(\mathbf{b}_j\) is the probability distribution 
\[
\begin{bmatrix}
1 & 1 & 1 \\
4 & 2 & 4
\end{bmatrix}
\]

Modulus \(q = 7681\).

2.2 Aigis-Enc with the recommended parameters: Without compression

Key generation: Set \(\{\eta_1, \eta_2\} = \{1, 4\}\). \(A \in \mathbb{Z}^{768 \times 768}_{256}\) is a special matrix which is generated from nine 256 \times 256 rotation matrices arranged in a 3 \times 3 way with arbitrary order.

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

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 \times 256 rotation sub-matrices (rather than with respect to entries).

Given a plaintext column vector \(\mu = \left(\begin{array}{c}
\mu_0 \\
\vdots \\
\mu_{255}
\end{array}\right)\), calculate the ciphertext \(\{\mathbf{c}_1, \mathbf{c}_2\}\),

\[
\begin{align*}
\mathbf{c}_1 &= \mathbf{A}^T \mathbf{r} + \mathbf{x}_1 \\
\mathbf{c}_2 &= [\mathbf{T}(\mathbf{b})] \cdot \mathbf{r} + \mathbf{x}_2 + \mu \cdot \left(\frac{q}{2}\right)
\end{align*}
\]  

(1)

where \(r \sim \mathbf{b}_{\eta_1}^{768}, \mathbf{x}_1 \sim \mathbf{b}_{\eta_2}^{768}, \mathbf{x}_2 \sim \mathbf{b}_{\eta_2}^{256}\).

Decryption: calculate

\[
\mathbf{c} = \left(\begin{array}{c}
\mathbf{c}_0 \\
\vdots \\
\mathbf{c}_{255}
\end{array}\right)
\]

\[
\mathbf{c}_2 - [\mathbf{T}(\mathbf{s})] \cdot \mathbf{c}_1
\]

\[
\mathbf{\mu}_1 = \begin{cases}
0 & |c_i| \leq \frac{q}{4} \\
1 & |c_i| > \frac{q}{4}
\end{cases}
\]
2.3 | Aigis-Enc with the recommended parameters: With compression

Set the compression parameters \{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 is generated from nine 256 \times 256 rotation matrices arranged in a 3 \times 3 way with arbitrary order.

Let \(b = As + e + \varepsilon\), where \(s \sim b_{\eta_1}^768\), \(e \sim b_{\eta_2}^768\), \(\varepsilon = -(A(\overline{r}) + e(\text{mod } q))(\text{mod } 2^{d_i})\). The public key is \((A, b)\), and the secret key is \(s\).

Encryption: transform matrix \(A\) to \(A^T\). Given a plaintext column vector \(\mu = \begin{pmatrix} \mu_0 \\ \vdots \\ \mu_{255} \end{pmatrix}\), calculate the ciphertext \(\{c_1, c_2\}\),

\[
\begin{align*}
    c_1 &= A^T r + x_1 + \overline{x}_1 \\
    c_2 &= [T(b)] \cdot r + x_2 + \overline{x}_2 + \mu \cdot \left\lceil \frac{q}{2} \right\rceil
\end{align*}
\]

where \(r \sim b_{\eta_1}^768\), \(x_1 \sim b_{\eta_1}^768\), \(x_2 \sim b_{\eta_2}^{256}\), \(x_1 = -(A^{\Gamma} + x_1(\text{mod } q)) \text{ (mod } 2^{d_i})\), \(x_2 = -(T(b)) \cdot r + x_2(\text{mod } q)(\text{mod } 2^{d_i})\).

Decryption: calculate

\[
c = \begin{pmatrix} c_0 \\ \vdots \\ c_{255} \end{pmatrix}
\]

\[
c = c_2 - [T(s)] \cdot c_1
\]

\[
= \mu \lceil \frac{q}{2} \rceil + x_2 + \overline{x}_2 + [T(e) + T(\varepsilon)] \cdot r - [T(s)] \cdot (x_1 + \overline{x}_1)
\]

Obtain \(\mu_i\) as

\[
\mu_i = \begin{cases} 
0 & |c_i| \leq \frac{q}{4} \\
1 & |c_i| > \frac{q}{4}
\end{cases}
\]

2.4 | Symmetrical LWE scheme on 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 \(\{c_1, c_2\}\), correct guess on the value of \(\mu^{(i)}\) enables us to acquire 1024 LWE samples:

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

in Equation (6) every component of the secret vector \(r\) obeys the probability distribution \(b_{\eta_1}\), every component of the noise \(2x_2 + \mu\) has the SD larger than \(\sqrt{2}\) times of the SD of \(b_{\eta_1}\).

3.2 | Scenario 2 and resource

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

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

in Equation (6) every component of the secret vector \(r\) obeys the probability distribution \(b_{\eta_1}\), every component of \(2x_2 + \mu\) has the SD larger than \(\sqrt{2}\) times of the SD of \(b_{\eta_1}\).

3.3 | Scenario 3 and resource

From public key we obtain the following 768 LWE samples:

\[
b = As + e,
\]

in Equation (7) every component of the secret vector \(s\) obeys the probability distribution \(b_{\eta_1}\), every component of \(e\) obeys the probability distribution \(b_{\eta_2}\).

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

\(d \in \{770, 771, ..., 1025\}\), we consider the \(d\)-dimension lattice generated by the column vectors of the below matrix \(B\).
\[
B = \begin{bmatrix}
\phi_{768} & 0 & (\mathbf{A}^T)^{-1} \mathbf{c}_1 \\
-\mathbf{T}(\mathbf{b})^*(\mathbf{A}^T)^{-1} q \mathbf{I}_{d-769} & (\mathbf{c}_1)^* \\
0 & 0 & t
\end{bmatrix}
\] (8)

In Equation (8), \(\mathbf{T}(\mathbf{b})^*\) is the matrix constructed from \(d - 769\) rows of \(\mathbf{T}(\mathbf{b})\),
\[
\mathbf{c}_3 = \mathbf{c}_2 - \mu^{(j)} \left[ \frac{T}{2} \right] - \mathbf{T}(\mathbf{b}) (\mathbf{A}^T)^{-1} \cdot \mathbf{c}_1,
\] (9)

\((\mathbf{c}_3)^*\) is the vector constructed from the corresponding \(d - 769\) components of \(\mathbf{c}_3\), \(\mu^{(j)}\) is the correct plaintext. Note that the \(d - 769\) rows of the matrix chosen can be arbitrary as long as these rows are linearly independent. But the following \(d - 769\) rows from other matrices are chosen corresponding to which rows we chose in the first matrix. \(c > 0\), \(t > 0\), \((c, t)\) are the tunable parameters. We also know \((c \cdot \mathbf{r}^T, x^*^T, t)^T\) is a small vector of the regarding lattice, where \(x^*_2\) is the vector constructed from \(d - 769\) components of the encryption noise vector \(\mathbf{x}_2\). The size of the small vector is \(\sqrt{c^2 \times 768 \times \frac{t}{2} + (d - 769) \times \frac{t}{2} + t^2}\) approximately. The aim of the attack is to find the small vector. It isn’t difficult to see ‘the traditional primal attack’ [15–17] 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 \(\mathbf{B}\).

\[
\mathbf{B} = \begin{bmatrix}
\phi_{768} & 0 & 0 \\
\mathbf{A}^T & (\mathbf{c}_1)^* \\
\mathbf{T}(\mathbf{b})^* & (\mathbf{c}_1)^* \\
0 & 0
\end{bmatrix}
\] (10)

In Equation (10), \([\mathbf{A}^T, \mathbf{T}(\mathbf{b})]^*\) is the matrix constructed from \(d - 769\) rows of \([\mathbf{A}^T, \mathbf{T}(\mathbf{b})]\), \((\mathbf{c}_1)^*\) is the vector constructed from the corresponding \(d - 769\) components of \((\mathbf{c}_1)^*\) \(c > 0\), \(t > 0\), \((c, t)\) are the tunable parameters. We also know \((c \cdot \mathbf{r}^T, x^*_2^T, t)^T\) is the small vector of the regarding lattice, where \(x^*_2^T\) is the vector constructed from \(d - 769\) corresponding components of the encryption noise vector \((\mathbf{x}_1, \mathbf{x}_2)^T\). The size of the small vector \(\ell = \sqrt{c^2 \times 768 \times \frac{t}{2} + (d - 769) \times \frac{t}{2} + t^2}\). The aim of the attack is to find the small vector. It isn’t difficult to see ‘the transformed primal attack’ [18,19] 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 \(2^{0.209b}\) (the quantum complexity is \(2^{0.263b}\)), the parameter \(b\) is as small as possible, while satisfying \(b \in [100, d]\) and

\[
\left( \frac{b}{d} \right)^{\frac{1}{3}} \cdot \left( \frac{\pi b}{2 \pi c} \right)^{\frac{1}{2}} \leq \left( \det(\mathbf{B}) \right)^{\frac{1}{2}}
\] (11)

The above inequality comes from the work of previous contributors [4,20], we no longer take time to verify its rationality. Notice the following five facts:

1. The left part of Equation (11) is independent of the tunable parameters \((c, t)\)
2. The left part of Equation (11) 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 Equation (11) has the same expression \(f(c, t)\), and

\[
f(c, t) = \frac{c^2 \cdot \frac{\delta_3}{\delta_2} \cdot \frac{\delta_2}{\delta_3} \cdot \frac{1}{\delta_2}}{\sqrt{c^2 \times 768 \times \frac{t}{2} + (d - 769) \times \frac{t}{2} + t^2}}
\] (12)

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 \(c > 0\), \(\lim_{t \to 0} f(c, t) = 0\), \(\lim_{t \to +\infty} f(c, t) = 0\).

Taking all the above five facts into consideration, it was found 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

\[
(c_0, t_0) = \begin{cases}
(2, \sqrt{2}) \\
(1, 1), \quad \text{when } \eta_1 = 1, \eta_2 = 4
\end{cases}
\] (13)

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 on the same scale are \((c, t) = (1, 1)\)
4.4 The comparison of the complexity of the optimal primal attack and ‘the optimal-optimal primal attack’

For each \( d \in \{1022, \ldots, 1793\} \), we can compute a corresponding \( b \) with Equations (11)–(13). Therefore, as is shown in Figure 1, with the data we obtain, we can draw a line graph in which the \( x \)-axis is the dimension \( d \), and the \( y \)-axis is the classic complexity of the optimal primal attack. Note that the scale on the \( y \)-axis is the exponent part of the complexity (e.g. 165 on the \( y \)-axis represent the complexity of \( 2^{165} \)). The minimum points on the curves are marked. In order to make the result more intuitively, we choose 13 sets of data in Table 1. Under 13 different values of \( d \), we list the classic complexity of the optimal primal attack on Aigis-Enc and the symmetrical LWE scheme on the same scale.

The so-called optimal-optimal primal attack is the optimal primal attack with a further optimised dimension \( d \). It can be observed in Table 1 and Figure 1 that the complexity of the ‘optimal-optimal primal attack’ on Aigis-Enc is \( 2^{162.54} \), that on the symmetrical LWE scheme on the same scale is \( 2^{163.436} \).

5 THE SECURITY STRENGTH COMPARISON UNDER DUAL ATTACKS

5.1 Our dual attack

We consider the following 768 ‘trivial LWE samples’:

\[
o = - I_{768} r + r, \tag{14} \]

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

\[
\begin{pmatrix}
o \\
c_1 \\
c_2 - \mu^{(i)} \frac{q}{2}
\end{pmatrix} = \begin{pmatrix}-I_{768} \\
A_{768}^T \\
T(b)
\end{pmatrix} r + \begin{pmatrix}r \\
x_1 \\
x_2
\end{pmatrix}. \tag{15}
\]

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

\[
\begin{pmatrix}
o \\
c_1 \\
c_2 - \mu^{(i)} \frac{q}{2}
\end{pmatrix} = \begin{pmatrix}-I_{768} \\
A_{768}^T \\
T(b)
\end{pmatrix} r + \begin{pmatrix}r \\
x_1 \\
x_2
\end{pmatrix}, \tag{16}
\]

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. \( [\begin{pmatrix}A^{*} & c I_{d-768} \end{pmatrix} \mod q] \) is a matrix which entries are all 0s.

2. We have the following Equation (17):

\[
[\begin{pmatrix}A^{*} & c I_{d-768} \end{pmatrix}] \begin{pmatrix}
o \\
c_1 \\
c_2 - \mu^{(i)} \frac{q}{2}
\end{pmatrix} \mod q = \begin{pmatrix}r \\
x_1 \\
x_2
\end{pmatrix}. \tag{17}
\]

We consider the lattice generated by the row vectors of the below matrix (B):

\[
B = \begin{bmatrix}q I_{768} & 0 \\
A^{*} & c I_{d-768}
\end{bmatrix}. \tag{18}
\]

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

\[
v \begin{pmatrix}-I_{768} \\
A^{*} \\
1/c
\end{pmatrix} \mod q = (0, \ldots, 0). \tag{19}
\]
Searching for a small vector $\mathbf{v}$ (row vector) on the lattice. From Lemma 1 (2), we can calculate

$$
\mathbf{v} \begin{pmatrix}
1 \\
\frac{1}{c} \\
\frac{\mathbf{x}_1}{c} \\
\frac{\mathbf{x}_2}{c}
\end{pmatrix}^* \pmod{q}
$$

The aim of our attack is to distinguish

$$
\mathbf{v} \begin{pmatrix}
1 \\
\frac{1}{c} \\
\frac{\mathbf{x}_1}{c} \\
\frac{\mathbf{x}_2}{c}
\end{pmatrix}^* \pmod{q}
$$

from some uniform value. Our attack includes all the dual attacks the designers of Aigis-Enc proposed, including ‘the traditional dual attack’ [21], ‘the transformed dual attack 1’, ‘the transformed dual attack 2’, [19] and ‘the transformed dual attack 3’ [22]. 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 $c = 1$.
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

In the work of previous contributors [4], the researchers use the complexity of solving $b$-dimension sub-lattice shortest vector problem to estimate the complexity of finding the shortest vector in the $d$-dimension lattice conservatively. With the model they construct, the researchers conclude that the complexity of the dual attack is

$$
\max \left\{ \frac{\exp \left(4\pi^2 \tau^2\right)}{2^d \cdot 20 \cdot 3075 \cdot b \cdot 16} \right\} 2^{0.202b},
$$

where $\tau = \frac{\mu \ell}{\sqrt{d} \cdot q}$, $\ell$ is the size of the small vector $\mathbf{v}$ on the lattice.

$\ell'$ is the size of the small vector operating inner product with $\mathbf{v}$ on the lattice. The small vector is

$$
\begin{pmatrix}
\mathbf{r} \\
\frac{1}{c} \\
\frac{\mathbf{x}_1}{c} \\
\frac{\mathbf{x}_2}{c}
\end{pmatrix}^*,
$$

and the size of it is

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

The size of the small vector $\mathbf{v}$ on the lattice is estimated to be $\ell = \left( \frac{\pi b}{2e} \right)^{\frac{d}{2}} \cdot (\det(B))^{\frac{1}{2}}$. Therefore, we have:
\[ \ell \cdot \ell' = \left( (\pi b)^2 \cdot \frac{b}{2\pi} \right)^{\frac{d+1}{2d}} \cdot q^2 \cdot c^{-\ell} \cdot \sqrt{c^2 \times 768 \times \frac{\eta_1}{2} + (d - 768) \times \frac{\eta_2}{2}} \]  

(23)

For any fixed \((d, b), 0 < b < d\), it satisfies \(\lim \ell \cdot \ell' = +\infty\), \(\lim \ell \cdot \ell' = +\infty\). 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 ref. [19], 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 \(b \leq d\), the value of \(b\) is hard to be determined. Therefore, we make a conservative estimation, its classic complexity is

\[ \min_{100 \leq b \leq d} \left\{ \max \left\{ 1, \frac{\exp(4\pi^2 r_1^2)}{20.20756 \cdot 16} \right\} \cdot 2^{0.292b} \right\} \]  

(24)

### 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

\[ \min_{100 \leq b \leq d} \left\{ \max \left\{ 1, \frac{\exp(4\pi^2 r_1^2)}{20.20756 \cdot 16} \right\} \cdot 2^{0.292b} \right\} \]  

(25)

where

\[ r_1^2 = \left( (\pi b)^2 \cdot \frac{b}{2\pi} \right)^{\frac{d}{d+1}} \cdot 768 \cdot \frac{1500 - \frac{d}{2}}{\pi} \cdot 2^{\frac{d-1536}{d}} \]  

(26)

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

\[ \min_{100 \leq b \leq d} \left\{ \max \left\{ 1, \frac{\exp(4\pi^2 r_2^2)}{20.20756 \cdot 16} \right\} \cdot 2^{0.292b} \right\} \]  

(27)

where

\[ r_2^2 = \left( (\pi b)^2 \cdot \frac{b}{2\pi} \right)^{\frac{d}{d+1}} \cdot 768 \cdot \frac{1500 - \frac{d}{2}}{\pi} \cdot 2^{\frac{d-1536}{d}} \]  

(28)

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 on 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 on the same scale.

For each \(d \in \{1022, \ldots, 1793\}\), we can compute a corresponding \(b\) with Equations (24)–(28). Therefore, as is shown in Figure 2, with the data we obtain, we can draw a line graphic in which the \(x\) axis is the dimension \(d\), and the \(y\) axis is the classic complexity of the optimal dual attack. The minimums on the curves are marked. In order to make the result more intuitively, we choose 13 sets of data in Table 2. Under 13 different values of \(d\), we list the classic complexity of the optimal dual attack on Aigis-Enc and the symmetrical LWE scheme on the same scale.

It can be observed in Table 2 and Figure 2 that the complexity of the ‘optimal-optimal dual attack’ on Aigis-Enc is \(2^{160.895}\), that on the symmetrical LWE scheme on the same scale is \(2^{161.834}\).

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

Combine the content of Sections 4 and 5.1–5.3, the CPA classic security strength of Aigis-Enc is 160.895, the CPA classic security strength of the symmetrical LWE scheme is 161.834.
6 | COMPARISON ON CALCULATED AMOUNT

A basic calculation is the sampling of probability distribution

\[
\chi = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 2 \end{bmatrix}.
\]

In the key generation phase, \( \chi \) is sampled \((8 + 2) \times 768 = 7680 \) times in Aigis, and \((4 + 4) \times 768 = 6144 \) times in the symmetrical LWE scheme on the same scale, the former is the \( \frac{2}{7} \) times of the latter. Certainly, sampling of \( \chi \) may be not accounted for the main calculated amount in key generation phase, because the public key matrix is also sampled uniformly.

In the encryption phase, \( \chi \) 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 on the same scale, the former is the \( \frac{19}{14} \) times of the latter. More importantly, sampling of \( \chi \) is accounted for a significant part of the calculated amount in encryption phase.

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

7 | COMPARISON ON DECRYPTION FAILURE PROBABILITY (WITH COMPRESSION)

The decryption error vector is \( \bar{x}_2 + \bar{x}_2 + (T(e) + T(\bar{e})) \cdot r + T(s) \cdot (x_1 + x_1) \), the decryption failure probability is identical to the probability of the random event below:

\[
\frac{4}{q} | \bar{x}_2 + \bar{x}_2 + (T(e) + T(\bar{e})) \cdot r + T(s) \cdot (x_1 + x_1) | \geq 1 \quad (29)
\]

The probability distribution of \( \frac{4}{q} (x_2 + (T(e) + T(\bar{e})) \cdot r + T(s) \cdot (x_1 + x_1)) \) can be regarded as normal distribution, but that of \( \frac{4}{q} \bar{x}_2 \) 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 (after several calculation, we find that the choice of 41 points is accurate enough for our approximation). The result is as follows:

The decryption failure probability of Aigis-Enc is \( 2^{-128.699} \).

The decryption failure probability of the symmetrical LWE scheme on 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 particular, 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 \( \frac{1}{3} \), while the decryption failure probability is lower than \( 2^{-128.699} \).

8 | CONCLUSION

The asymmetrical LWE structure makes the attacks on them become much more complicated, and we present our attacks which are more extensive, simpler, and clearer. Our analysis shows that Aigis-Enc has much smaller decryption failure probability than symmetrical LWE encryption scheme on the
same scale (in other words, saving less than $\frac{1}{2}$ communication traffic), by the cost of increasing more than $\frac{1}{2}$ sampling computation, while the CPA security is almost kept the same.

**REFERENCES**

1. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, STOC’05, New York, NY, USA, pp. 84–93 (2005)
2. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, STOC’96, New York, NY, USA, pp. 99–108 (1996)
3. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. Foundations of Computer Science, 2004. Proceedings 45th Annual IEEE Symposium, pp. 372–381 (2004)
4. Zhang, J., et al.: Aegis: a family of signatures and key encapsulation mechanisms from asymmetric (M)LWE and (M)SIS (in Chinese). Technical report, Chinese Association for Cryptologic Research (CACR). https://sfjs.cacr.net.org.cn/site/content/407.html (2019)
5. Zhang, J., et al.: Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: KEMs and Signatures of Smaller Sizes. IACR Cryptology ePrint Archive report 2019/510. https://eprint.iacr.org/2019/510 (2019)
6. Bos, J., et al.: Crystals - lybeer: a cca-secure module-lattice-based kem. 2018 IEEE European Symposium on Security and Privacy (EuroS P), pp. 353–367 (2018)
7. Cheon, J.H., et al.: Cut off the tail! a practical post-quantum public-key encryption from lwe to lwr. Security and Cryptography for Networks, Springer International Publishing, Cham, pp. 160–177 (2018)
8. Goldwasser, S., et al.: Robustness of the learning with errors assumption. Proceedings of the Innovations in Computer Science 2010. Tsinghua University Press, pp. 230–240 (2010)
9. Brakerski, Z., et al.: Classical hardness of learning with errors. Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing, STOC’13, New York, NY, USA, pp. 575–584 (2013)
10. Micciancio, D.: On the hardness of learning with errors with binary secrets. Theor. Comput. 14(13), 1–17 (2018)
11. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes[C]. Annual International Cryptology Conference. Springer, Berlin, Heidelberg, pp. 80–101 (2013)
12. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the fujisaki-okamoto transformation. Theory of Cryptography - TCC 2017, volume 10677 of LNCS, Springer International Publishing, pp. 341–371 (2017)
13. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: Fully homomorphic encryption without bootstrapping. Innovations in Theoretical Computer Science, ITCS, pp. 309–325 (2012)
14. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs Codes Cryptography. 75(3), 565–599 (2015)
15. Kannan, R.: Minkowski’s convex body theorem and integer programming. Math. Oper. Res. 12(3), 415–440 (1987)
16. Albrecht, M.R., et al.: Revisiting the expected cost of solving usvp and applications to lwe. Advances in Cryptology - ASIACRYPT 2017, Springer International Publishing, Cham, pp. 297–327 (2017)
17. Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based cryptography. Topics in Cryptology - CT-RSA 2011, volume 6558 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp. 319–339 (2011)
18. Bai, S., Galbraith, S.D.: Lattice decoding attacks on binary lwe. Information Security and Privacy, Springer International Publishing, Cham, pp. 322–337 (2014)
19. Alkim, E., et al.: Post-quantum key exchange— a new hope. 25th USENIX Security Symposium (USENIX Security 16), USENIX Association, Austin, TX, pp. 327–345 (2016)
20. Chen, Y.M.: Lattice reduction and concrete security of fully homomorphic encryption. Dept. Informatique, ENS, Paris, France, PhD thesis (2013)
21. Micciancio, D., Regev, O.: Lattice-based cryptography. Post-Quantum Cryptography, Springer Berlin Heidelberg, pp. 147–191 (2009)
22. Albrecht, M.R.: On dual lattice attacks against small-secret lwe and parameter choices in helib and seal. Advances in Cryptology - EUROCRYPT 2017, Springer International Publishing, Cham, pp. 103–129 (2017)

How to cite this article: Hu Y, Dong S, Dong X. Analysis on Aigis-Enc: Asymmetrical and symmetrical. *IET Inf. Secur.* 2021;15:147–155. https://doi.org/10.1049/isc2.12009