International Journal of Cryptology Research 10(2): 23 - 37 (2020)

Security Analysis of the Key Encapsulation Mechanism based on Rabin-p Encryption Scheme

Ji-Jian Chin[1] and **Moesfa Soeheila Mohamad**[*2]

[1] *Faculty of Engineering, Multimedia University, Cyberjaya.*
[2] *Information Security Lab, MIMOS Berhad, Kuala Lumpur.*

E-mail: soeheila.mohamad@mimos.my
[*] *Corresponding author*

ABSTRACT

The Rabin-p key encapsulation mechanism (KEM) was proposed by Asyraf et al in 2019 for the MySEAL New Cryptographic Algorithm (AKBA) initiative. The KEM was built upon their earlier proposal of a variant of the Rabin cryptosystem in that the modulus is multiprime and the private key consists of only one prime. The scheme is deterministic and does not achieve indistinguishability against chosen-plaintext attacks. Therefore the authors conducted a Dent transform to convert it into a KEM that is indistinguishably-secure against chosen ciphertext attacks in the random oracle model. However the authors only provide some statements claiming to satisfy the IND-CCA2 requirements. This work provides the formal treatment for the KEM scheme with regards to the security proof.

Keywords: key encapsulation mechanism, public key encryption, Rabin encryption

[3] This work was first published in CRYPTOLOGY2020.

1 INTRODUCTION

In 2015, CyberSecurity Malaysia Berhad brought together cryptographers from all around Malaysia under the MySEAL initiative to provide a rigorous study on cryptographic algorithms that are deemed 'safe' to be deployed by the Malaysian government. The first list of trusted cryptographic algorithms chosen from standards and other nations' recommended list, AKSA, was published in November 2017 on the MySEAL website (MySEAL, 2019). The AKSA list consists of twelve symmetric block ciphers, three symmetric stream ciphers, three digital signatures, six public key encryption schemes, two key agreement schemes, twenty hash functions and its variants, three prime number generators and nine deterministic random bit generators.

Following that, a call for proposals for new algorithms by Malaysian cryptographers was initiated. Upon receiving numerous proposals and completion of two rounds of rigorous analysis, algorithms that did not fulfill the AKBA proposal's criteria were eliminated. The outcome of the AKBA exercise yielded two remaining algorithms. The Rabin-p key encapsulation mechanism (KEM) is one of the finalists.

The Rabin-p KEM (Asbullah et al., 2019a) is constructed from the Rabin-p public key encryption (PKE) scheme by Asbullah and Ariffin (2016). Its security is based on the hardness of factoring, similar to the original Rabin encryption scheme by Rabin (1979). This variation is developed to eliminate the decryption error of the original Rabin encryption scheme.

Whilst it is known that the Rabin-p cryptosystem does not satisfy indistinguishability, the designers of the scheme claim that the scheme satisfies one-wayness. Using this property, the designers then proceeded to reinvent the Rabin-p encryption scheme into a KEM following the transformation proposed by Dent (2003). Initially claiming the KEM to be secure against indistinguishable adaptive chosen-ciphertext attacks (IND-CCA2), the designers then downplayed the security claims to only satisfy indistinguishability under chosen-plaintext attacks (IND-CPA) due to the work of Paillier and Villar (2006). To the best of our knowledge, there exists no proof to the designers' claims that their KEM satisfies IND-CPA or IND-CCA2.

2 RELATED WORKS

Public key cryptosystems were invented to overcome the symmetric key distribution problem by enabling secure key agreement protocols and key transport protocols. As for data encryption, public key encryption is efficient only for short messages. For messages with lengths being multiple of the encryption algorithm block size, the symmetric encryption is recommended.

Consequently, hybrid encryption is deployed in practice. Hybrid encryption is an encryption scheme which uses both public key encryption and symmetric key encryption. First, a secret key is generated and used with a symmetric encryption on the message. Then the secret key is encrypted using a public key encryption method. Finally, both ciphertexts are sent to the receiver. The receiver must first decrypt the encrypted secret key, and then use the secret key to recover the message. Fujisaki and Okamoto (1999) proposed a generic hybrid encryption scheme construction. The construction transforms a public key encryption scheme achieving one-wayness and a symmetric encryption scheme achieving indistinguishability against eavesdroppers, with additional requirements, into a hybrid encryption achieving indistinguishability under chosen plaintext attack(IND-CPA).

Hybrid encryption becomes modular by the introduction of the KEM-DEM framework. Shoup (2001) proposes the framework during the development of the first ISO public key encryption standard. In the framework, the KEM may be designed and analysed separately from the Data Encryption Method (DEM). The proposal provides the notion of KEM security and an experiment to define indistinguishability against chosen ciphertext attack (IND-CCA) for KEM. An analysis of the security requirements on the underlying PKE was specified too.

From the experiment proposed by Shoup (2001), Dent (2003) defines KEM security precisely from the complexity perspective. The KEM is said to achieve indistinguishability against adaptive chosen ciphertext attack (IND-CCA2) if any adversary can distinguish the generated key from a random bitstring in the challenge encapsulated key-pair with an insignificant advantage in terms of the security parameter. In addition, Dent (2003) proposes generic KEM constructions from deterministic and probabilistic public key encryption schemes.

By his constructions, an OW-CPA-secure public key encryption is transformed into an IND-CCA2 KEM.

Further relaxation of requirements on PKE with corresponding secure KEM construction and improvements on KEM security are proposed by Kurosawa and Desmedt (2004) and Liu and Paterson (2015), among others. While Javier-Herranz et al. (2010) analysed the requirements on both PKE for KEM and symmetric encryption for DEM to achieve IND-CCA on the resulting hybrid encryption.

In recent years, with the active research to develop post-quantum public key cryptosystems, hybrid encryption in such setting has been considered. Generic constructions upon quantum-safe public key encryption schemes have been proposed by Hofheinz et al. (2017), Targhi and Unruh (2016). The security is defined against quantum adversary and security defined under quantum-oracle model (Boneh et al., 2011). We do not consider such adversary in this work because Rabin-p encryption scheme is based on integer factorization problem; which is not a post-quantum primitive candidate.

Our Contribution This work aims to provide the formal treatment to the security of Rabin-p KEM. In this work, we show that the Rabin-p KEM does indeed satisfy IND-CCA2 under the random oracle model, following Dent's transformation. This is notwithstanding the claims of the designers that the Rabin-p KEM achieves only IND-CPA security due to Paillier and Villar (2006) which only show the impossibility of single private key encryption schemes (such as the Rabin cryptosystem) to achieve IND-CCA2 security. However, since the Rabin-p KEM is not an encryption scheme but a KEM, this result does not apply. Therefore, here we instantiate the proof from (Dent, 2003, Appendix B) to tailor to Rabin-p KEM, showing concrete security bounds of an IND-CCA2 adversary's advantage against Rabin-p KEM.

The rest of the paper is as follows: We begin by providing notations and a review of PKEs and KEMs in Section 3, then review the Rabin-p PKE and KEM in Section 4. The main contribution of this work can be found in Section 5 where we provide the proof of security for the Rabin-p KEM. We also share some insight on recommended key lengths for Rabin-p KEM in order to achieve similar security level to that of 128-bit AES in Section 6. Finally we conclude in Section 7.

3 PRELIMINARIES

Here are the notations and general definition and security of cryptographic primitives which will be used in the rest of the paper.

We denote $\{0,1\}^*$ as the set of all bit strings and $\mathbb{Z}_p$ as the set of positive integers modulo p, where p is a large prime number. The notation $a \overset{\$}{\leftarrow} S$ denotes sampling a random element a uniformly from a finite set S, therefore $x \overset{\$}{\leftarrow} \{0,1\}^n$ shows randomly sampling a bitstring of length n whereas $b \overset{\$}{\leftarrow} \mathbb{Z}_p$ shows randomly sampling an integer b from the set of $\mathbb{Z}_p$.

We denote a function $\mathsf{negl}(n)$ as negligible if for all polynomials p there is a constant N_{p} where for any $n \geq N_{\mathsf{p}}$, $\mathsf{negl}(n) \leq \frac{1}{\mathsf{p}(n)}$.

3.1 Public Key Encryption (PKE)

Let $\mathcal{M}_E$ be the message space and $\mathcal{C}_E$ be the ciphertext space of a public key encryption (PKE) scheme E. A PKE scheme E consists of three algorithms:

1. $E.\mathsf{KGen}(1^n) \rightarrow (pk, sk)$: The key generation algorithm that takes in the security parameter and outputs a public/private key pair.
2. $E.\mathsf{Enc}(m, pk) \rightarrow C$: the encrypt function that takes in a user's public key pk and a message $m \in \mathcal{M}_E$ and outputs a ciphertext $C \in \mathcal{C}_E$.
3. $E.\mathsf{Dec}(C, sk) \rightarrow m$: the decrypt function that takes in a user's corresponding private key sk and a ciphertext $C \in \mathcal{C}_E$ and recovers the message $m \in \mathcal{M}_E$.

It is required for correctness that $E.\mathsf{Dec}(E.\mathsf{Enc}(pk, m), sk) = m$.

The security game for E against one-way chosen plaintext attacks (OW-CPA) is defined as the advantage of adversary $\mathcal{A}$ winning the following OW-CPA experiment, shown in Figure 1.

```
$Exp_{E,\mathcal{A}}^{OW-CPA}(1^n)$
$(pk, sk) \xleftarrow{\$} \mathsf{KGen}(1^n)$
$(state) \xleftarrow{\$} \mathcal{A}(1^n, pk)$
$m \xleftarrow{\$} \mathcal{M}$
$c \xleftarrow{\$} \mathsf{Enc}(pk, m)$
$m' \xleftarrow{\$} \mathcal{A}(1^n, pk, c, state)$
if $m^* = m'$ then
    return $1$
 else
    return $0$
```

Figure 1: OW-CPA experiment against E.

The security of E is then defined as advantage of the adversary $\mathcal{A}$ as follows:

$$Adv_{E,\mathcal{A}}^{OW-CPA}(1^n) = \Pr\left[Exp_{E,\mathcal{A}}^{OW-CPA}(1^n) = 1\right]$$

3.2 Key Encapsulation Mechanism (KEM)

Let $\mathcal{K}_{KEM}$ be the key space and $\mathcal{C}_{KEM}$ be the ciphertext space. A key encapsulation mechanism KEM consists of three algorithms:

1. $KEM.\mathsf{KGen}(1^n) \rightarrow (pk, sk)$: The key generation algorithm that takes in the security parameter and outputs a public-private key pair.

2. $KEM.\mathsf{Encap}(pk) \rightarrow (K, C)$: the key encapsulation function that takes in a user's public key pk and outputs a ciphertext $C \in \mathcal{C}_{KEM}$ and a key $K \in \mathcal{K}_{KEM}$ using its random coins.

3. $KEM.\mathsf{Decap}(C, sk) \rightarrow K$: the decrypt function that takes in a user's

corresponding private key sk and a ciphertext $C \in \mathcal{C}_{KEM}$ and recovers the key $K \in \mathcal{K}_{KEM}$.

The security game for KEM against indistinguishable chosen ciphertext attacks (IND-CCA2) is defined as the advantage of adversary $\mathcal{B}$ winning the following IND-CCA2 experiment, shown in Figure 2. The security of KEM is then defined as advantage of the adversary $\mathcal{B}$ as follows:

$$Adv_{KEM,\mathcal{B}}^{\text{IND-CCA2}}(1^n) = \left| \Pr\left[Exp_{KEM,\mathcal{B}}^{\text{IND-CCA2}}(1^n) = 1\right] - \frac{1}{2} \right|$$

```
$Exp_{KEM,\mathcal{B}}^{\text{IND-CCA2}}(1^n)$
$(pk, sk) \xleftarrow{\$} KEM.\mathsf{KGen}(1^n)$
$(\mathsf{state}) \xleftarrow{\$} \mathcal{A}^{KEM.\mathsf{Decap}(sk,.)}(1^n, pk)$
$(K_0^*, C^*) \xleftarrow{\$} KEM.\mathsf{Encap}(pk)$
$(K_1^*) \xleftarrow{\$} \mathcal{K}_{KEM}$
$b \xleftarrow{\$} \{0, 1\}$
$b' \xleftarrow{\$} \mathcal{A}^{KEM.\mathsf{Decap}(sk,.)}(1^n, pk, K_b^*, C^*, \mathsf{state})$
if $b = b'$ then
    return $1$
else
    return $0$
fi
```

Figure 2: IND-CCA experiment against KEM

4 THE RABIN-P PKE AND KEM

In this section we review the Rabin-p public key encryption (PKE) scheme (Asbullah and Ariffin, 2016) and the derived KEM (Asbullah et al., 2019a,b).

4.1 Rabin-p PKE

Rabin-p PKE is a variation of the Rabin encryption scheme in which decryption is always correct. The changes includes the public key from $N = pq$ to $N = p^2q$ and using only p as the private key.

Let $msg \xleftarrow{\$} \{0, 1\}^*$ and $\mathsf{Parse}(\cdot)$ be a function that maps bitstrings to elements in $\mathcal{M} = \left\{0, 2^{2n-1}\right\}$. The Rabin-p PKE scheme E consists of three algorithms as described in Figure 3.

```
$E.\mathsf{KGen}(1^n) \rightarrow (pk = N, sk = p)$
    $p, q \xleftarrow{\$} \mathbb{Z}_l$ :
        $2^n < l < 2^{(n+1)}, p, q \equiv 3(\mathrm{mod} 4)$
    $N = p^2q$
    return $(N, p)$
```

```
$E.\mathsf{Enc}(m, pk = N) \rightarrow C$
    $m = \mathsf{Parse}(msg)$ :
        $0 < m < 2^{2n-1} \mathsf{and} gcd(m, N) = 1$
    $C = m^2(\mathrm{mod} N)$
    return $(C)$
```

```
$E.\mathsf{Dec}(C, sk = p) \rightarrow m$
    $w \equiv C(\mathrm{mod} p)$
    $m_p \equiv w^{\frac{p+1}{4}}(\mathrm{mod} p)$
    $i = \frac{c - m_p^2}{p}$
    $j \equiv \frac{i}{2m_p}(\mathrm{mod} p)$
    $m_1 = m_p + jp$
    if $m_1 < 2^{2n-1}$ then
        return $m = m_1$
    else
        return $m = p^2 - m_1$
```

Figure 3: Rabin-p PKE

Rabin-p encryption scheme has been proven to achieve OW-CPA. Breaking the onewayness of the scheme was shown as equivalent to factoring the modulus $N = p^2q$ (Asbullah et al., 2019a, Theorem3.2).

4.2 Rabin-p KEM

Let $\mathcal{K} = \{0, 1\}^{keylen}$ and $\mathcal{C}_{KEM} = \{0, N\}$. Furthermore, define KDF to be a pseudorandom function and H to be a hash function. The Rabin-p KEM

```
$KEM$.KGen$(1^n) \rightarrow (pk = N, sk = p)$
$p, q \xleftarrow{\$} \mathbb{Z}_l : 2^n < l < 2^{(n+1)},$
        $p, q \equiv 3(\bmod 4)$
$N = p^2 q$
Select $KDF : \mathbb{Z}_{2^{2n-1}} \rightarrow \mathcal{K}$
Select $H : \mathbb{Z}_{2^{2n-1}} \rightarrow \mathcal{C}$
return $(N, p, KDF, H)$
```

```
$KEM$.Encap$(pk = N) \rightarrow (K, C)$
$x \xleftarrow{\$} \mathbb{Z}_l : 2^{3n/2} < l < 2^{2n-1}$
$C_1 = x^2(\bmod N)$
$C_2 = H(x)$
$C = (C_1, C_2)$
$K = KDF(x)$
return $(K, C)$
```

```
$KEM$.Decap$(C, sk = p) \rightarrow K$
Parse $C = (C_1, C_2)$
$w \equiv C_1(\bmod p)$
$x_p \equiv w^{\frac{p+1}{4}}(\bmod p)$
$i = \frac{C_1 - x_p^2}{p}$
$j \equiv \frac{i}{2x_p}(\bmod p)$
$x_1 = x_p + jp$
if $x_1 < 2^{2n-1}$ then
    $x = x_1$
else
    $x = p^2 - x_1$
if $C_2 \neq H(x)$ return $\perp$
$K = KDF(x)$
return $K$
```

Figure 4: Rabin-p KEM

consists of three algorithms as described in Figure 4.

5 SECURITY ANALYSIS

We provide the IND-CCA2 proof for the Rabin-p KEM in this section.

Theorem 5.1. *Given a OW-CPA secure Rabin-p PKE scheme, a pseudorandom key derivation function KDF and a hash function H, the Rabin-p KEM is secure against IND-CCA2 attacks with the following advantage:*

$$Adv_{KEM,\mathcal{B}}^{IND-CCA2}(n) \leq Adv_{PKE,\mathcal{A}}^{OW-CPA}(n) + \frac{q_D}{2^{Hashlen}} + \frac{q_D}{2^{2n-1}}$$

where q_D is the number of decapsulation queries made by $\mathcal{A}$ and $Hashlen$ is the length of the output of H.

Proof. We model the security of IND-CCA2 Rabin-p KEM as a game where $\mathcal{A}$ breaks the OW-CPA Rabin-p PKE scheme using an adversary $\mathcal{B}$ that breaks IND-CCA2 of Rabin-p KEM. During initiation, $\mathcal{A}$ receives the public key $pk = N = p^2q$ and a challenge ciphertext C^* of which it must invert (i.e. produce x^* such that $C^* = (x^*)^2(\mathrm{mod} N)$ using the help of $\mathcal{B}$.

$\mathcal{A}$ maintains two lists for its KDF and H oracles, $KDF - list$ and $H - list$ respectively. $\mathcal{A}$ passes $pk = N$ to $\mathcal{B}$, stores C^* aside for the challenge phase, and simulates KDF and H as random oracles. Upon each KDF or H query, on input of x_i from $\mathcal{B}$, $\mathcal{A}$ checks if $C_1^* = E.\mathsf{Enc}(x_i, pk)$. If true, $\mathcal{A}$ ends the game and returns x_i as the solution m^* to the challenge C^*. Otherwise, $\mathcal{A}$ provides the following oracles for $\mathcal{B}$ to query adaptively:

1. KDF queries: $\mathcal{A}$ checks if $(x_i, K_i) \in \{KDF - list\}$. If the entry is not found, $\mathcal{A}$ samples $K_i \overset{\$}{\leftarrow} \mathcal{K}_{KEM}$, stores $(x_i, K_i) \in \{KDF - list\}$ and returns K_i to $\mathcal{B}$.
2. H queries: $\mathcal{A}$ checks if $(x_i, H(x_i)) \in \{H - list\}$. If the entry is not found, $\mathcal{A}$ samples $H(x_i) \overset{\$}{\leftarrow} \{0,1\}^{Hashlen}$, stores $(x_i, H(x_i)) \in \{H - list\}$ and returns $H(x_i)$ to $\mathcal{B}$.
3. Decap queries: On input of $(C_i = (C_{(1,i)}, C_{(2,i)}))$ from $\mathcal{B}$, one of the following two scenarios will cause $\mathcal{A}$ to abort the game:
   (a) if $C_{(1,i)} = C^*$.
   (b) if $(x_i, C_{(2,i)}) \in \{H - list\}$ such that $C^* = E.\mathsf{Enc}(x_i, pk)$.

   Otherwise, $\mathcal{A}$ generates or retrieves the corresponding x_i to $C_{(2,i)}$ from $\{H - list\}$, generates or retrieves K_i from $(x_i, K_i) \in \{KDF - list\}$ and returns K_i to $\mathcal{B}$.

Once $\mathcal{B}$ completes the training phase and outputs a state to be challenged on, $\mathcal{A}$ produces $K_0^* \overset{\$}{\leftarrow} KEM.\mathsf{Encap}(pk)$ and $K_1^* \overset{\$}{\leftarrow} \mathcal{K}_{KEM}$. Next, $\mathcal{A}$ flips a bit $b \overset{\$}{\leftarrow} \{0,1\}$ and passes K_b^* and $C_{KEM}^* = (C^*, C_2^*)$ to $\mathcal{B}$. After receiving this challenge, $\mathcal{B}$ can continue querying oracles with the exception of decapsulation query on C^*. Finally, $\mathcal{B}$ must output a guess b'.

If $\mathcal{A}$ has not ended the game at this point, it then samples $x^* \overset{\$}{\leftarrow} \{0, 2^{2n-1}\}$ and outputs x^* as its solution.

It remains to calculate the probability of $\mathcal{B}$ running to completion and the abort scenarios.

The game ends when $\mathcal{A}$ wins. This corresponds to the advantage of $\mathcal{A}$: $Adv^{OW-CPA}_{PKE,\mathcal{A}}(n)$. This happens on the event that $C^*_1 = E.\mathsf{Enc}(x_i, pk)$ occurs during KDF and H queries. $\mathcal{A}$ wins when it returns x_i as the solution to the challenge ciphertext C^*.

The game also ends following two scenarios that happen during decapsulation queries that cause $\mathcal{A}$ to abort. This is reviewed below together with their corresponding probabilities:

1. if $(C_{(1,i)}) = C^*$, this means $\mathcal{B}$ issued a decapsulation query on the challenge ciphertext. This might happen before $\mathcal{B}$ wishes to switch to challenge phase and happens with an upper-bound probability of $\frac{1}{2^{2n-1}}$ as a random x_i is sampled each time from $\mathbb{Z}_l$ where $2^{3n/2} < l < 2^{2n-1}$. With q_D queries, the probability of this happening throughout the game is $\frac{q_D}{2^{2n-1}}$.
2. if $(x_i, C_{2,i}) \in \{H - list\}$ such that $C^* = E.\mathsf{Enc}(x_i, pk)$, $\mathcal{B}$ has caused a collision in the random oracle query. This happens with probability $\frac{1}{2^{HashLen}}$. With q_D queries, the probability of this happening throughout the game is $\frac{q_D}{2^{HashLen}}$.

Putting them together, the chances of $\mathcal{B}$ running to completion and winning the game is given as in Theorem 5.1:

$$Adv^{IND-CCA2}_{KEM,\mathcal{B}}(n) \leq Adv^{OW-CPA}_{PKE,\mathcal{A}}(n) + \frac{q_D}{2^{Hashlen}} + \frac{q_D}{2^{2n-1}}$$

□

However, we do note a few points of contention that may raise further concerns. The first issue is that the existence of a mapping protocol $parse$ that maps from bitstrings of variable length to elements in $\mathcal{M}_E = \{0, 2^{2n-1}\}$ seems like folklore. However, this very function is used to map inputs for the Rabin-p PKE's encryption algorithm from bitstrings to integers with the condition that $\gcd(m, N) = 1$. The designers make no note of what will happen when $\gcd(m, N) \neq 1$, whether the message will be remapped, or the encryption simply aborts. This additional control may potentially leak information to an adversary.

Secondly this proof does not take into account the generation of prime numbers, nor the range of safe primes within the encapsulation algorithm. That analysis is beyond the scope of this paper. Although the authors did provide some ad hoc analysis of the Rabin-p PKE with regards to attack vectors from Coppersmith, Novak, and other mathematical analysis, it remains uncertain whether whether the exhaustive list of algebraic attacks is made known.

6 RECOMMENDED KEY LENGTHS

Since the proof of security is tight and the added advantage of the IND-CCA2 adversary is only linear to the advantage of the OW-CPA adversary, we affirm that the keylength of 3072-bits for the modulus N is sufficient to provide security at 128-bit AES security level. Table 1 lists the recommended security parameter lengths for Rabin-p KEM.

This is done by instantiating the advantage equation from Theorem 5.1 to the security parameter of $k = 1024$ corresponding to the prime number size, selecting SHA3-512 as the hash function with $Hashlen = 512$, and bounding decapsulation queries $q_D = 2^{30}$ following Coron's example Coron (2000). Thus we have:

$$\begin{aligned} Adv_{KEM,\mathcal{A}}^{IND-CCA2}(n) &\leq Adv_{PKE,\mathcal{A}}^{OW-CPA}(n) + \frac{q_D}{2^{Hashlen}} + \frac{q_D}{|\mathcal{M}|} \\ &\leq Adv_{PKE,\mathcal{A}}^{OW-CPA}(n) + 2^{30-512} + 2^{30-1024} \\ &\leq Adv_{PKE,\mathcal{A}}^{OW-CPA}(n) + 2^{-482} + 2^{-994} \end{aligned}$$

Since the addition of the terms from the decapsulation queries are linear, if $Adv_{PKE,\mathcal{A}}^{OW-CPA}(n)$ is a negligible function $\mathsf{negl}(n)$ then $Adv_{KEM,\mathcal{A}}^{IND-CCA2}(n)$ remains $\mathsf{negl}(n)$. Hence, NIST guidelines can still be followed to assume 3076-bits for factoring to provide the equivalence to 128-bit security as published on keylength.com (BlueKrypt, 2019).

Security Level	Modulus Size (bits)	Prime Size (bits)
128	3072	1024
192	7608	2560
256	15360	5120

Table 1: Rabin-p KEM recommended modulus length for 2016-2030 & beyond

7 CONCLUSION

In this work, we have shown that the Rabin-p KEM is IND-CCA2 secure assuming the Rabin-p PKE achieves OW-CPA with more concrete bounds in regards to the number of decapsulation queries, hash length and KEM message space. We also affirm that the proposed key lengths to achieve equivalent 128-bit AES security is sufficient.

REFERENCES

Asbullah, M. A. and Ariffin, M. R. K. (2016). Design of Rabin-like cryptosystem without decryption failure. *MJMS*, 10(S):1–18.

Asbullah, M. A., Ariffin, M. R. K., and Mahad, Z. (2019a). Design and analysis of Rabin-p key encapsulation mechanism for CyberSecurity Malaysia MySEAL initiative. *IJCR*, 9(1):19–51.

Asbullah, M. A., Ariffin, M. R. K., and Mahad, Z. (2019b). Rabin-p encapsulation mechanism. AKBA MySEAL, Rabin-p KEM Proposal. `https://myseal.cybersecurity.my/en/akba.html`.

BlueKrypt (2019). Cryptographic key length recommendation. `https://www.keylength.com/`.

Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., and Zhandry, M. (2011). Random oracles in a quantum world. In Lee, D. H. and Wang, X., editors, *Advances in Cryptology – ASIACRYPT 2011*, pages 41–69, Berlin, Heidelberg. Springer Berlin Heidelberg.

Coron, J. (2000). On the exact security of full domain hash. In Bellare, M., editor, *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *LNCS*, pages 229–235. Springer, Heidelberg.

Dent, A. (2003). A designer's guide to KEMs. In Paterson, K., editor, *IMA International Conference on Cryptography and Coding 2003*, volume 2898 of *LNCS*, pages 133–151. Springer, Heidelberg.

Fujisaki, E. and Okamoto, T. (1999). Secure integration of asymmetric and symmetric encryption schemes. In Wiener, M., editor, *Advances in Cryptology — CRYPTO' 99*, pages 537–554, Berlin, Heidelberg. Springer Berlin Heidelberg.

Hofheinz, D., Hövelmanns, K., and Kiltz, E. (2017). A modular analysis of the Fujisaki-Okamoto transformation. In Kalai, Y. and Reyzin, L., editors, *Theory of Cryptography*, pages 341–371, Cham. Springer International Publishing.

JavierHerranz, DennisHofheinz, and EikeKiltz (2010). Some (in)sufficient conditions for secure hybrid encryption. *Information and Computation*, 208(11):1243–1257.

Kurosawa, K. and Desmedt, Y. (2004). A new paradigm of hybrid encryption scheme. In Franklin, M., editor, *Advances in Cryptology – CRYPTO 2004*, pages 426–442. Springer Berlin Heidelberg.

Liu, S. and Paterson, K. G. (2015). Simulation-based selective opening CCA security for PKE from key encapsulation mechanisms. In Katz, J., editor, *Public-Key Cryptography – PKC 2015*, volume 9020 of *LNCS*, pages 3–26. Springer, Berlin, Heidelberg.

MySEAL (2019). MySEAL homepage. `https://myseal.cybersecurity.my/en/index.html`.

Paillier, P. and Villar, J. L. (2006). Trading one-wayness against chosen-ciphertext security in factoring-based encryption. In Lai, X. and Chen, K., editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 252–266. Springer, Heidelberg.

Rabin, M. (1979). Digitalized signatures and public-key functions as intractable as factorization. Computing Science Technical Report TR-212, MIT Laboratory for Computer Science.

Shoup, V. (2001). A proposal for the ISO standard for public-key encryption (version 2.1). `https://shoup.net/iso/`.

Targhi, E. E. and Unruh, D. (2016). Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In Hirt, M. and Smith, A., editors, *Theory of Cryptography*, pages 192–216, Berlin, Heidelberg. Springer Berlin Heidelberg.