

Intellectual Property Statement for the Submission of Rabin- p Key Encapsulation Mechanism to the MySEAL Project

I, Muhammad Asyraf bin Asbullah, of Institute for Mathematical Research, Universiti Putra Malaysia, do hereby declare that the cryptosystems that I have submitted, known as Rabin- p Key Encapsulation Mechanism, are my own original works, or if submitted jointly with others, are the original work of the joint submitters.

I further declare that both the Rabin- p Key Encapsulation Mechanism are properties of Universiti Putra Malaysia (UPM). It has been filed for copyright as according to Universiti Putra Malaysia (Research) Rules 2012. Their copyright application reference are belonged to the thesis of Muhammad Asyraf bin Asbullah entitled 'Cryptanalysis on the Modulus $N = p^2q$ and Design of Rabin-like Cryptosystem without Decryption Failure'. UPM hopes that all parties interested with Rabin- p Key Encapsulation Mechanism will endeavor to communicate with the owners as well as to cite this document in all future works regarding Rabin- p Key Encapsulation Mechanism.

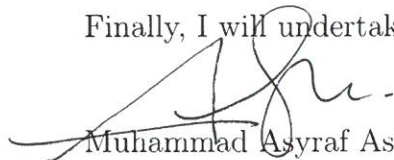
In addition, I do hereby declare that the cryptosystems that I have submitted, known as Rabin- p Key Encapsulation Mechanism, are already in publications prior to this proposal submission, as follows;

1. M A Asbullah & M R K Ariffin. Algebraic Analysis of a Rabin-Like Cryptosystem and Its Countermeasures. 2017. Indian Journal of Science and Technology, 10(1), 1-5.



2. M A Asbullah & M R K Ariffin. Design of Rabin-like Cryptosystem Without Decryption Failure. 2016. Malaysian Journal of Mathematical Science, 10(S), 1-18.
3. M A Asbullah, M R K Ariffin & Z Mahad. Analysis on the Rabin- p cryptosystem. AIP Conference Proceedings 1787, 080012 (2016)
4. M A Asbullah & M R K Ariffin. Provably Secure Rabin- p Cryptosystem in Hybrid Setting. AIP Conference Proceedings 1739, 020001 (2016)
5. M A Asbullah, Z Mahad & M R K Ariffin, Efficient Programming Deployment Strategy for Rabin- p Cryptosystem in C/C++, MyIPO Copyright Filing No. LY2018004528, 27 September 2018.
6. M A Asbullah, Z Mahad & M R K Ariffin, Efficient Programming Deployment Strategy for Rabin- p Cryptosystem in Java, MyIPO Copyright Filing No. LY2018004528, 27 September 2018.

Finally, I will undertake to update the MySEAL project when necessary.



Muhammad Asyraf Asbullah (Inventor)

10 January 2019

DR. MUHAMMAD ASYRAF ASBULLAH
Pensyarah (Unit Matematik)
Pusat Asasi Sains Pertanian
Universiti Putra Malaysia
43400 UPM Serdang

