



SDI Review Form 1.6

Journal Name:	British Journal of Mathematics & Computer Science
Manuscript Number:	2014_BJMCS_14321
Title of the Manuscript:	Modified Matrix Modular Cryptosystems
Type of the Article	Original Research Article

General guideline for Peer Review process:

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty**', provided the manuscript is scientifically robust and technically sound.

To know the complete guideline for Peer Review process, reviewers are requested to visit this link:

(<http://www.sciencedomain.org/page.php?id=sdi-general-editorial-policy#Peer-Review-Guideline>)



SDI Review Form 1.6

PART 1: Review Comments

	Reviewer's comment	Author's comment (if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)
Compulsory REVISION comments	(1) In Abstract, authors stated that the aim of this article is to decrease the number of these exponentiations and consequently to accelerate the execution of encryption algorithm. However, authors only discussed the security of their improved schemes and didn't analyze the efficiency. Authors should analyze the efficiency of three schemes, i.e., BMMC, MMMC1 and MMMC2 in terms of time complexity and experimental values. (2) In Abstract, the Basic Matrix Modular Cryptosystem (BMMC) is a public-key cryptosystem. Generally speaking, the security of public-key cryptosystems always bases on some difficult mathematical problems . For example, RSA is the Integer Factorization Problem, ECC (Elliptic curve cryptosystem) is the Elliptic Curve Discrete Logarithm Problem. What is the difficult mathematical problem for BMMC? (3) In Abstract, authors stated that the level of security is high enough for an appropriate choice of parameters of the cryptosystems. What is meaning of appropriate choice of parameters? Or how to judge a parameter is appropriate or not? (4) Authors proposed two improved scheme of BMMC. Authors should make comparisons among these three schemes, i.e., BMMC, MMMC1 and MMMC2 in terms of security and efficiency.	From this observation, I agree, but to implement it in this article is not possible, since all of these comparisons will be examined in a separate article, including a comparison BMMC with RSA and ELGamal. The answer to this question is added in the Introduction. How to be added to the abstract and conclusions, the lower bound for the security of the modified matrix modular cryptosystems is a 40-bit modulus n of the residue ring $\mathbf{Z}_n$. See response to comment (1)



SDI Review Form 1.6

<u>Minor</u> REVISION comments	(5) The paper structure should be described in Section Introduction. (6) For the self-contain of this paper and easy understanding for readers, BMMC should be described in brief . Authors also should emphasize the differences among the improved schemes and BMMC. (7) What is the meaning of r in Section 3(2.1)? Therefore, all the mathematical signals should be explained when they first appear in the paper.	Description of the structure of article added to the Introduction. Brief description of BMMC added in the article and executed as a section 3. Differences between BMMC and its modifications are obvious and need no comments. The parameter r is not secret and may be any integer greater than or equal to 2, but how to be added to the description of the modifications it is preferable to choose the value of 2 in case of an expected bit length $2m$ of modulus n, then a prime number p is selected so that there has been a bit length m.
<u>Optional/General</u> comments	(8) Generally speaking, Section Conclusions should not include any reference. Therefore, the sentences are suggested to put in Section Introduction. "In the most important case for the use of public-key cryptosystems, namely, key exchange protocols for symmetric ciphers, such as AES, the key length is usually equal to 256 bits. Protocol using BMMC was developed for the key exchange in [2]." (9) Section References is too weak. (10) There are some typos.	The said proposal added to the Introduction. Section References expanded to 13 items.