



SDI Review Form 1.6

Journal Name:	Journal of Advances in Mathematics and Computer Science
Manuscript Number:	Ms_JAMCS_37301
Title of the Manuscript:	Triple-Protocol – a New Direction of Elliptic-Curve Cryptography
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>)

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)
<u>Compulsory</u> REVISION comments	- Line No. 90, Is it exponentiation? If then, what is the time complexity? - Line No. 96; Logic operation HOR? - Line No. 150; How are the values of R1, R2 and R3 made available to Subscriber B? - Line No. 135; Where are the errors being corrected? - Line 146-156: These lines of user B, uses the symbol of XOR. Is it same as this ^ symbol, as used by the User A. - Lines 158-164: Who is checking for a successful transmission from user A to user B? - Is Table 2 values made available to User B for the successful decryption? - References are not up-to-date. Are there no advances in this work in 6 years? - Is Messi-Omura protocol being proposed by the authors? There is no clarity about the algorithm. - Conclusion is missing in the paper.	
<u>Minor</u> REVISION comments		
<u>Optional/General</u> comments		

Reviewer Details:

Name:	S. AKhila
Department, University & Country	Department of Electronics and Communication, BMS College of Engineering, India