

Cryptographically Privileged State Estimation With Gaussian Keystreams

Response to Reviewers' Comments - Submission L-CSS 21-0154

Marko Ristic

Benjamin Noack

Uwe D. Hanebeck

May 25, 2021

Dear Dr. Ji-Feng Zhang,
Dear Reviewers,

We would like to thank you all for your responses and agreement on accepting our manuscript. As specified in the Author's Checklist, we list the changes made to the accepted manuscript here. The changes consist of switching to the final version template and minor wording and spelling changes. Throughout this response, reviewers' comments are in blue.

Sincerely,
Marko Ristic, Benjamin Noack, and Uwe D. Hanebeck

Response to the Editor's Report

E.1 All the Reviewers are fine with the revised version. Accordingly, I am glad to recommend the paper publication.

One reviewer pointed out a possible small typo in a reference. I have checked that: the reference given by the authors is correct. I guess the reviewer found the draft of the book in http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf which does not correspond exactly with the published version.

We are happy to hear of your decision, thank you. Regarding the reference, we have left it as it was submitted in the accepted version.

Response to the Comments of Reviewer 1 (46379)

R1.1 The authors have answered all my earlier concerns.

We are glad to hear this, thank you.

Response to the Comments of Reviewer 2 (46381)

R2.1 The authors have addressed my comments

We are happy we could address them all, thank you.

Response to the Comments of Reviewer 3 (44309)

R3.1 The reviewer only have the following one more suggestion.

1. Could the author explain more about the negligible function η in Definition 2.3. and make a definition of this function in this paper? The reviewer cannot find the definition 3.4. in ref [8] which may be a different version.

We're sorry to hear that the reference was not easier to find. The editor has indicated that the reference was correct and differs from the book draft that can be found online, so we have left it unchanged. We're glad we could address your remaining suggestions.