III

INTERNAL EXPLANATIONS

Dream Revision Protocol @ July 25

Hi Viktor.

This is my **internal** report what I did to address the April 25 reviewer comments.

It consists of the email of the editor to you with my explanations inline.

All reviewer and editor comments are answered. There is one open question.

A similar document is the (IV) official 'Response Note,' which is for submission.

Below is the April editor's response to your initial application of the dream paper that included the comments of the reviewers the editor let us know by way of this email.

Green marks the reviewer comments. The editor summarized them first,

Blue are my explanations **to you** of what I did in response.

The Overleaf history and review highlights provide additional detail where needed: https://www.overleaf.com/project/5efeadc275d71b00014b2ea8.

Red is the one open question – the re-use of the one-time pad.

In reaction to the reviewer comments, I added two new sections to the paper: one "Synopsis" as 3.1, its purpose being to more slowly lead the reader into the formula-heavier parts of the paper and to give a feel for the formulas in advance in a high-level overview that in simple language describes only the core network traffic and the OTP creation (as opposed to your other overview-like paragraphs in the paper that stay either non-technical or look at the resulting functionality). This is meant as the main response to the blanket criticism of reviewer 1 that the paper was 'not understandable,' which echoed "batman's" review comment from April in Overleaf, who gave up at around the place where the "Synopsis" has now been inserted.

I also added language to the Conclusion that is both in answer to the requests of reviewer 1 and especially to the concrete proposals by reviewer 2. E.g., it uses the comments of reviewer 2 (as seen below) where he lists who in his opinion would benefit from the paper to create what.

The original email with my inline comments follows.

From: ryenwhite@gmail.com

To: viktor.tron@gmail.com

CC: tweb@acm.org, viktor.tron@gmail.com, hd@lexon.org

Subject: Transactions on the Web - Decision on Manuscript ID TWEB-25-0111

Body: 31-May-2025

Dear Mr. Tron:

Manuscript ID TWEB-25-0111 entitled "A Dream Come True: Deletable Content in Immutable Storage." which you submitted to the Transactions on the Web, has been reviewed. The comments of the reviewers are included at the bottom of this letter.

The reviewers have several suggestions for revising your manuscript.

Therefore, I invite you to respond to the reviewers' comments and revise your manuscript for further review.

Done. See Overleaf "for-submission.tex".

Please address the comments below in your revised version and create a file or note indicating how you have addressed them.

Done. File "Dream - (IV) June 2025 Response Note to Reviewer Comments"

When you resubmit your paper, the Manuscript Central paper submission system will give you instructions for uploading this information.

To submit your revised manuscript, log into https://mc.manuscriptcentral.com/tweb and enter your Author Center, where you will find your manuscript title listed under "Manuscripts with Decisions." Under "Actions," click on "Create a Revision." Your manuscript number has been appended to denote a revision.

IMPORTANT: Your original files are available to you when you upload your revised manuscript. Please delete any redundant files before completing the submission.

TODO for you.

Would you be able to send us your revised submission within 3 months? Please confirm by responding to tweb@acm.org.

Done: confirmed we will do so to Mr. White.

Once again, thank you for submitting your manuscript to the Transactions on

the Web, and I look forward to receiving your revision.

Sincerely,
Dr. Ryen White
Editor-in-Chief, Transactions on the Web

Associate Editor's Comments to Author:

Associate Editor: Guest Editors, Advanced Technologies in the Decentraliz

Comments to the Author:

Thanks for submitting your work to TWEB SI on decentralized web.

We recommend a revise and resubmit before the manuscript can be considered for publication. The paper presents a novel and structured protocol, but both reviewers raise critical concerns that must be addressed.

All concerns are addressed in the revised paper and explained in the prepared note they ask for.

File “Dream - (IV) June 2025 Response Note to Reviewer Comments”

Reviewer 1 questions the claim of censorship resistance, noting that uploader-controlled revocation implies centralization.

Non-sensical. Added explanatory text and footnotes -- see below.

Additionally, the misuse of the "one-time pad" contradicts its security guarantees, leading to potential information leakage.

The OTP reuse is an open question -- see below.

Reviewer 2 highlights the lack of discussion on real-world deployment constraints

Added -- see below.

and recommends clarifying complex constructs with examples or diagrams.

Added diagrams -- see below.

Both suggest strengthening the conclusion

Added text to conclusion -- see below.

–Reviewer 1 urges addressing data deletion

Not a correct summary of the reviewer's concern.

No action.

and Reviewer 2 recommends outlining future directions.

Added to section 5 -- see below.

Minor issues such as spelling errors also need correction.

Done and changed all to British English.

Reviewer(s)' Comments to Author:

Reviewer: 1

Recommendation: Revise & Resubmit

Comments:

1.In the first page, the statement "The approach preserves the censorship resistance of..." . If the uploader has the ability to revoke access rights from all users, this essentially constitutes a form of **centralized control**, which I believe violates the very definition of **"censorship resistance."**

Misunderstanding.

Added multiple clarifying phrases and footnotes in relevant places.

2. In Section 3.1, under point **D**, the manuscript claims to use a **"one-time pad"**, but it allows the pad to be reused. This directly contradicts the requirements of **information-theoretic security**.

If an attacker obtains two different plaintexts encrypted with the same key, this would lead to **complete information leakage**, as the attacker can simply XOR the two ciphertexts to recover the XOR of the plaintexts, which can then be exploited to fully reconstruct the original messages.

Added multiple clarifications throughout the text to make the re-use of the OTP for deniability more careful.

However, the OTP re-use for deniability remains an open question.

See file "Dream - (II) July 2025 Questions and Rationales" #4, pg. 3.

I think it MIGHT be best addressed by asymmetrical encrypting C and A before XORing them with the OTP.

For an example of the exploit see the images I shared in our Telegram direct messages.

Re double OTP use, see:

https://incoherency.co.uk/blog/stories/otp-key-reuse.html

3. In the conclusion section, it is recommended to address the critical issue of controlling and deleting already distributed data replicas.

Misunderstanding.

Made minor changes to be yet clearer in the paragraph that is already stating explicitly that this cannot be addressed and is never expected, i.e., in section 2, now reading:

"It is obvious that any party that is privileged to access such information could store, re-code, and potentially disseminate it, so that the content can be made accessible by them at a later point in time to anyone they wish, which would of course frustrate any process that could qualify as deletion (or removal of access) at the original download source. However, as there is no protection possible against such adversity, any legally and socially useful notion of deletion (e.g. revocation of access) therefore, invariably defines a narrower case: taking away the viability to replay the same access method at a lower cost than at least the full cost of storing the content." [underline added here]

Also added two sentences in appropriate places explicating that the OTP itself is larger than the content so that also storing the key as part of a new reference <r,k> makes no sense vs. just storing the content.

4. There are multiple spelling mistakes, e.g., 'impsossible' → 'impossible', 'feasable' → 'feasible'.

Corrected.

Also made consistent change of entire document to British English and doubled checked all spell checker highlights. Added multiple legal but rare words to the Overleaf dictionary.

Additional Questions:

Is the paper in the expected journal style?: Yes

If not, please note what key sections or components are missing (abstract, related work, evaluation, references, etc).:

Are the references comprehensive and appropriate?: Yes

If key references are missing, please list them. If there are too many self-citations, please suggest alternatives.:

Relative to the subject material, is the paper understandable without requiring too much effort on the part of the reader?: No

Three main courses of action:

- Added Synopsis as section 2.1 (as mentioned above) to narrate the core technical functionality on a high-level before the formulas spell out the details.
- Added appropriate variable names throughout the main text when a relevant word is first used in a paragraph, or, vice versa, adding the words to the variable names (e.g., 'dream pad k').
- Added graphics on dream path and update function – see below.

Please rate the relevance of the paper to TWEB from 1 to 5, 1 being the lowest/poorest score.: 3

Is there enough new content in this paper to distinguish it from other works?

In answering this question, you can use the Manuscript Central capabilities for external searches on both the authors and title as well as the "Search for a Companion Paper" feature. If significant parts of the paper have been previously published, authors are supposed to indicate this with their submission. Unfortunately, not all authors do this.: Yes

If the paper is an extended version of a conference paper, does the submission provide enough new material for journal publication?: Yes

If the answer to either of these questions is no, please explain.:

Manuscripts submitted to TWEB should not be concurrently under review for publication in another conference or journal. If you suspect that the same paper is simultaneously being considered for publication elsewhere, the editor should be notified.:

Is the work primarily theoretical, practical or is it a survey?: T

Is the content technically sound?: Yes

Please explain if not or if you are unsure.:

Rate the level of originality and innovation of the work reported from 1 to 5, 1 being the lowest/poorest score.: 3

Describe how the submission advances the state of the art in the field.:

Rate the impact of this work on the research community, 1 being the lowest/poorest score.: 3

Suggest beneficiaries from the work.:

Rate the impact of this work on the wider community, 1 being the lowest/poorest score.: 3

Suggest beneficiaries from the work.:

Please help ACM create a more efficient time-to-publication process: Using your best judgment, what amount of copy editing do you think this paper needs?: Moderate

Addressed (see above and below).

Most ACM journal papers are researcher-oriented. Is this paper of potential interest to developers and engineers?: Yes

---

Reviewer: 2

Recommendation: Revise & Resubmit

Comments:

1. While the paper presents a well-structured protocol, it lacks discussion on the **practical deployment constraints** of DREAM—such as Swarm's **current adoption level, network size,** and **availability assumptions**. It would be helpful to include a short section or paragraph discussing the applicability boundaries and operational prerequisites. [emphasis added]

Added section 5, "Implementation Constraints" that discusses these topics.

2. Section 3 introduces several complex constructs (e.g., **dream path Π**, **update function Δ**) using mathematical formalism. To enhance readability

for a broader audience, it is recommended to include a high-level illustrative example or a simplified diagram that shows the end-to-end dream protocol in action. [emphasis added]

Added two explanatory diagrams as proposed (**dream path**, now fig. 2, and **delta function,** now fig. 3) that illustrate the variables that appear in the formulas. In their visuals as well as captions they add sequence descriptions specifically of how the dream path Π and the update function Δ work.

The reviewer seemed to explicitly ask for more detail than what was already given in the graphics of the dream protocol (now fig. 4).

3. The conclusion could be strengthened by outlining potential **future directions**, such as integrating DREAM with more granular **access control** schemes, resilience against **active adversarial interference**, or combining the mechanism with **off-chain computation** and **zero-knowledge proofs** for enhanced privacy. [emphasis added]

Added some points in section 5 as follows, but not all the topics seem sensical:

- Access control is already addressed in Addressability. Added two references in appropriate places throughout the text.
- Active Interference was already addressed in section 'Security.'
- Off-chain Computation is addressed by adding thoughts on offline mining.
- Zero-knowledge proofs seem out of place. One could make a comparison in how the key is stored and used in a way that is removed from the grantee but it seems to not quite fit.

Additional Questions:
Is the paper in the expected journal style?: Yes

If not, please note what key sections or components are missing (abstract, related work, evaluation, references, etc).:

Are the references comprehensive and appropriate?: Yes

If key references are missing, please list them. If there are too many self-citations, please suggest alternatives.:

Relative to the subject material, is the paper understandable without requiring too much effort on the part of the reader?: Yes

Please rate the relevance of the paper to TWEB from 1 to 5, 1 being the lowest/poorest score.: 4

Is there enough new content in this paper to distinguish it from other works?

In answering this question, you can use the Manuscript Central capabilities for external searches on both the authors and title as well as the "Search for a Companion Paper" feature. If significant parts of the paper have been previously published, authors are supposed to indicate this with their submission. Unfortunately, not all authors do this.: Yes

If the paper is an extended version of a conference paper, does the submission provide enough new material for journal publication?: Yes

If the answer to either of these questions is no, please explain.:

Manuscripts submitted to TWEB should not be concurrently under review for publication in another conference or journal. If you suspect that the same paper is simultaneously being considered for publication elsewhere, the editor should be notified.:

Is the work primarily theoretical, practical or is it a survey?: T

Is the content technically sound?: Yes

Please explain if not or if you are unsure.:

Rate the level of originality and innovation of the work reported from 1 to 5, 1 being the lowest/poorest score.: 4

Describe how the submission advances the state of the art in the field.: The paper presents an original approach to enabling deletable content in immutable, decentralized storage systems by redefining deletion as revocation of access. Its design of the DREAM protocol—based on a distributed one-time pad mechanism and leveraging Swarm's network features—offers a technically novel yet practical solution.

Utilized the above snippet in text added to the conclusion.

Rate the impact of this work on the research community, 1 being the lowest/poorest score.: 4

Suggest beneficiaries from the work.: Web3 infrastructure researchers exploring privacy-preserving decentralized systems.

Protocol designers working on Swarm, IPFS, or Filecoin who need access control mechanisms.

Legal tech and compliance researchers addressing "right to be forgotten" in blockchain-based storage.

Utilized in conclusion (rephrased).

Rate the impact of this work on the wider community, 1 being the lowest/poorest score.: 3

Suggest beneficiaries from the work.: Privacy-conscious users in decentralized platforms who want control over their shared data.

Policymakers and legal advocates seeking technological pathways for enforcing data removal rights.

Developers of censorship-resistant publishing tools, who may incorporate DREAM as a privacy-respecting access control mechanism.

Utilized in conclusion (rephrased).

Please help ACM create a more efficient time-to-publication process: Using your best judgment, what amount of copy editing do you think this paper needs?: Moderate

Addressed -- see all of the above.

Most ACM journal papers are researcher-oriented. Is this paper of potential interest to developers and engineers?: Maybe

Date Sent: 31-May-2025