Pairing-Friendly Curves

Yumi Sakemi

3rd November 2025

Montréal, Canada

What is Pairing?

■ Pairing

- Pairings are used to realize advanced cryptographic primitives such as BLS signatures, zk-SNARKs, IBE, etc.
- Their security depends critically on the chosen pairing curve and parameters

■ History of Pairing draft

- Our draft proposed the recommended parameters and they were passed expert crypto panel review
- CFRG RG item, two RGLCs started (2021)
- Now, our activity stopped later

Problem and Our Goal in Our Draft

■ Problem

- Is Kim et al.'s attack presented in CRYPTO 2016 (exTNFS) and it reduced security of curves like BN254
- Yet legacy pairing parameters are still in use, even though their security is no longer strong enough

■ Goal

- provide a clear, practical list of pairing-friendly curves and parameters with post-exTNFS security levels
  - e.g., ~128 / 192 / 256 bits

Why the Draft Status Got Stuck

GMO CONNECT

- the pairing parameters are not cause – those had **broad consensus**

- Disagreement on **scope** of the document
  - Authors:
    focus on **standardizing parameters**
  - Some reviewers:
    add **textbook-level tutorial** explaining the whole background of pairings

- Current Status
  - Because of this difference, we could not find a good agreement with the reviewers.

- Current Opinion
  - We believe a full tutorial belongs in a separate document,
    not in this parameter-focused I-D
    - We believe detailed explanations of pairing algorithms involve **many implementation choices** – for example, how to define finite fields, or which pairing algorithm to use and they are not standardized in CFRG
    - These topics should be discussed in a **separate standardization effort.**
    - Writing a full textbook section would require **a large effort** but bring **little benefit** for implementers.

Restart Activities on Pairing's I-D

GMO CONNECT

- We would like to restart this work, and authors are ready to move forward
  - Motivation
    - Our draft is bottleneck for other drafts such as BBS signature scheme
  - Proposed scope:
    - The authors would like to focus on only the essential information for standardizing pairing parameters, aiming for an early RFC publication.
      - leave tutorial / survey content to a separate document, if needed
  - If CFRG members would like to add textbook-level writing
    - Writing a full textbook section requires **a large effort, we need volunteers**

- Next steps
  - Team rebuilding
  - Re-check / update recommended parameters and Security Considerations, if needed
  - Confirm this parameter-focused scope
  - Feedback from implementers and protocol designers on what information is most useful

Please feedback through CFRG ML or talk to us after IETF124 CFRG session ☺

References

- Internet-draft
  - https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/

Internet for Everyone

GMO