**From:** Moody, Dustin (Fed)
**To:** Apon, Daniel C. (Fed)
**Subject:** RE: 1st Round Report: Picnic, minor
**Date:** Wednesday, December 12, 2018 11:12:00 AM

---

Got it. Thanks.

---

**From:** Apon, Daniel C. (Fed)
**Sent:** Wednesday, December 12, 2018 11:09 AM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
**Subject:** 1st Round Report: Picnic, minor

Hi,

After examining the new Picnic changes yesterday, I wanted to suggest a small change to the final paragraph of the summary:

Current:
"There is a multi-target attack reported on the Picnic submission, and the Picnic team has proposed a countermeasure in addition to a number of other modifications to improve efficiency. Being a novel scheme, Picnic would benefit from much more scrutiny and analysis."

Proposed change:
"There is a multi-target attack reported on the Picnic submission, and the Picnic team has proposed a countermeasure in addition to a number of other modifications to improve efficiency, as well as a new, tight security proof that avoids the forking lemma. However, being a novel scheme, Picnic would still benefit from much more scrutiny and analysis."

--Daniel