THE ONRAMP SUBMISSIONS

In response to NIST's call for additional digital signatures

SCOPE

- NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.

- NIST may also be interested in signature schemes that have short signatures and fast verification.

- Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.

TIMELINE

- July 2022 - Call for Additional Signatures announced
- August 2022 – Submission requirements and evaluation criteria published
- March 1, 2023 – Preliminary submission deadline for early review
    - March 31, 2023 – Feedback given back to submitters
- June 1, 2023 – Final deadline for submission
- ~ July 1 ?, 2023 – Accepted submissions will be posted on NIST's webpage

SUBMISSION NUMBERS

- 17 Preliminary submissions

- 50 submissions received by the final deadline
  - These are being checked for submissions requirements
  - There were 23 signatures (and 59 KEMs) submitted in 2017

- 262 distinct submitters
  - There are 4 submitters who each have 4 submissions
  - There are 6 submitters who each have 3 submissions
  - There were 278 distinct submitters back in 2017
  - 45 people submitted in 2017 and 2023

GEOGRAPHY

- In 2017, we had submitters from
  - 6 continents and 26 countries

- In 2023, we have submitters from
  - 5 continents and 28 countries

Australia
Austria
Belgium
Canada
China
Denmark
Finland
France
Germany
India
Israel
Japan
Malaysia
Mexico
Netherlands
Norway
Portugal
Senegal
Singapore
Slovakia
South Korea
Spain
Sweden
Switzerland
Taiwan
United Arab Emirates
United Kingdom
United States

CATEGORIES

Type	Number
Lattice	8
Code-based	5
Multivariate	11
MPC in the head	7
Symmetric	6
Isogeny	1
Other	12
Total	50