Profiles

- What should a profile look like?
  - Risk disclaimer?
  - General vs. specific?
- Which metrics?

Profile <*profile name*>	
Primitive	*Type of primitive*
Physical characteristics	*Name physical characteristic(s), and provide acceptable range(s) (e.g., 64 to 128 bytes of RAM)*
Performance characteristics	*Name performance characteristic(s), and provide acceptable range(s) (e.g., latency of no more than 5 ns)*
Security characteristics	*Minimum security strength, relevant attack models, side channel resistance requirements, etc.*
Design goals	*List design goals.*

Gathering Information

- How can we make it easier for stakeholders to share profile info with us?
- Is there anything missing from the questionnaire?

Standard Development

- Is a 30-day public comment period long enough to review draft profiles?
- How much information about the use cases does NIST need to provide reviewers in order to evaluate the profiles during the public comment period?

Security and Validation

- Security strength: Is 112 bits too high?
  - How well will weaker algorithms age?
- Validation concerns?
- What validation concerns do vendors have for lightweight portfolio?

Selecting Algorithms

- What criteria should NIST use for considering algorithms?
- How many algorithms?
- Fewer algorithms, many modes?

More Discussion

- Other questions?

- Comments on NISTIR 8114 due **October 31, 2016**
- Mailing List: lwc-forum@nist.gov
- https://www.nist.gov/programs-projects/lightweight-cryptography