Paths to Technical Standards for Modern Homomorphic Encryption Schemes

Ro Cammarota

AI System Privacy and Trustworthiness Guy

Intel AI Research

Agenda

- Outreach
- Standards Recognition
- Proposed Next Steps

Outreach

- Goal: Find adoption beyond the stakeholders, enthusiasts and niche markets
  - Software and semiconductor industry pay attention to privacy, startups proliferate
  - Privacy-preserving technologies can be architected as a solution (e.g., HE, MPC, TEE)
  - Go beyond proofs of concept requires wider recognition (e.g., by standards bodies.)

- How: Leverage this venues' participant positions into standards bodies, being mindful of the different bodies mindsets
  - E.g., IEEE, ISO, TG – to define technologies.
  - E.g., IETF, WFA – to implement technologies.

Standards Recognition

- ISO:
  - Seek acknowledgment of a broader community with starting a study period in JTC1 SC27.
  - Follow up with gathering experts input for next steps, e.g., amendments - ISO/ IEC FDIS 18033-6, new standards.
  - https://www.iec.ch/members_experts/refdocs/iec/JTC1-Supplement-2017.pdf

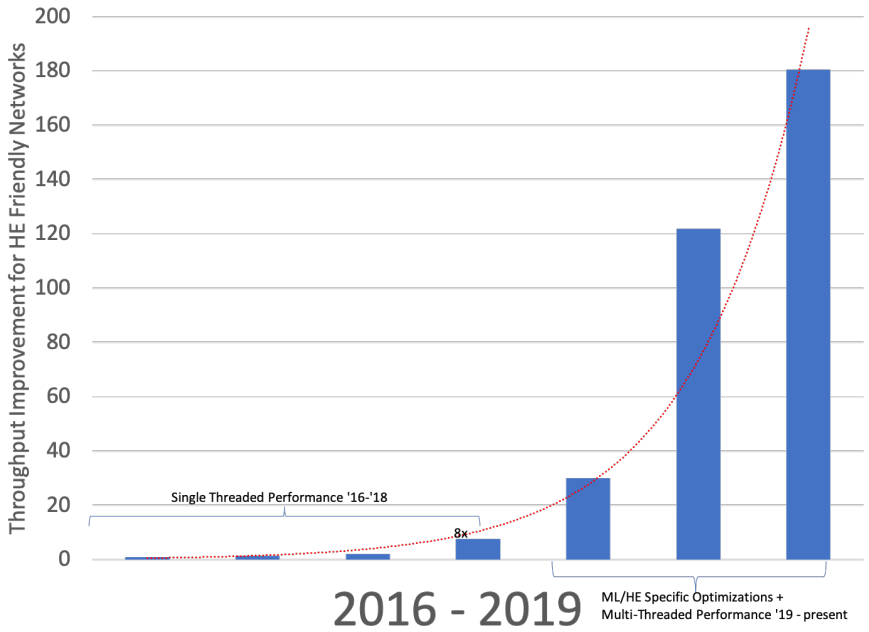
- IEEE:
  - Start a study group, e.g., in P1363, to develop a PAR for "Recommended Practices on the use of HE schemes in applications."
  - For a working group and develop the standards upon PAR approval.
  - https://standards.ieee.org/faqs/pars.html

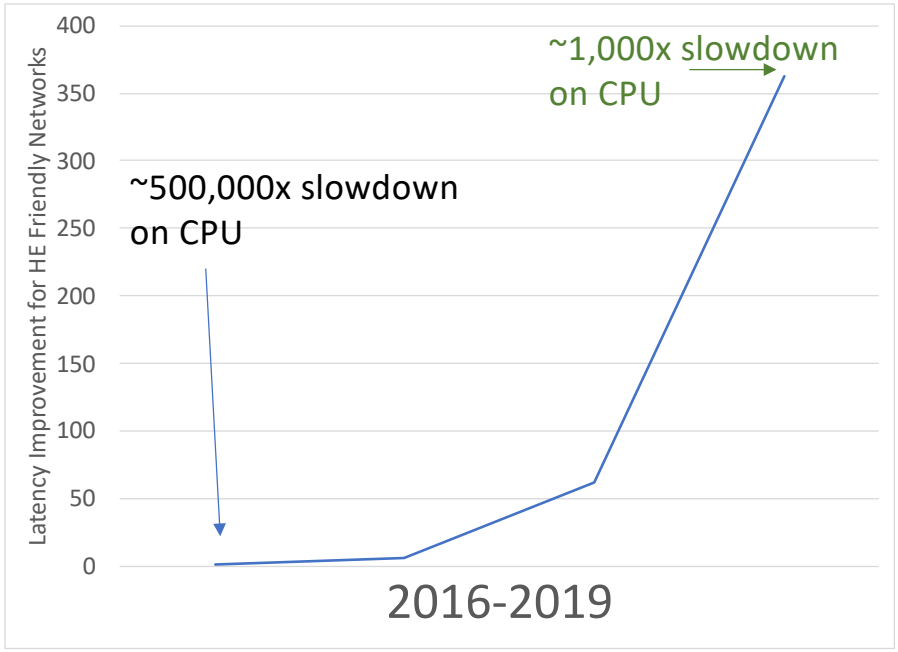
- IETF:
  - Option 1: Prepare (improve the technical writing of current documents) and submit to Area Director as Standards Track RFC.
  - Option 2: Informational RFC – fastest but not recommended, as it's not a document vetted by a community of experts.
  - https://www.ietf.org/blog/guidance-area-director-sponsoring-documents/

- Other Bodies in Specific Application Domains (e.g., IEEE 802.x, WFA.)

Dealing with possible Headwinds with Benchmarks

~60x slowdown
on CPU with HE + MPC





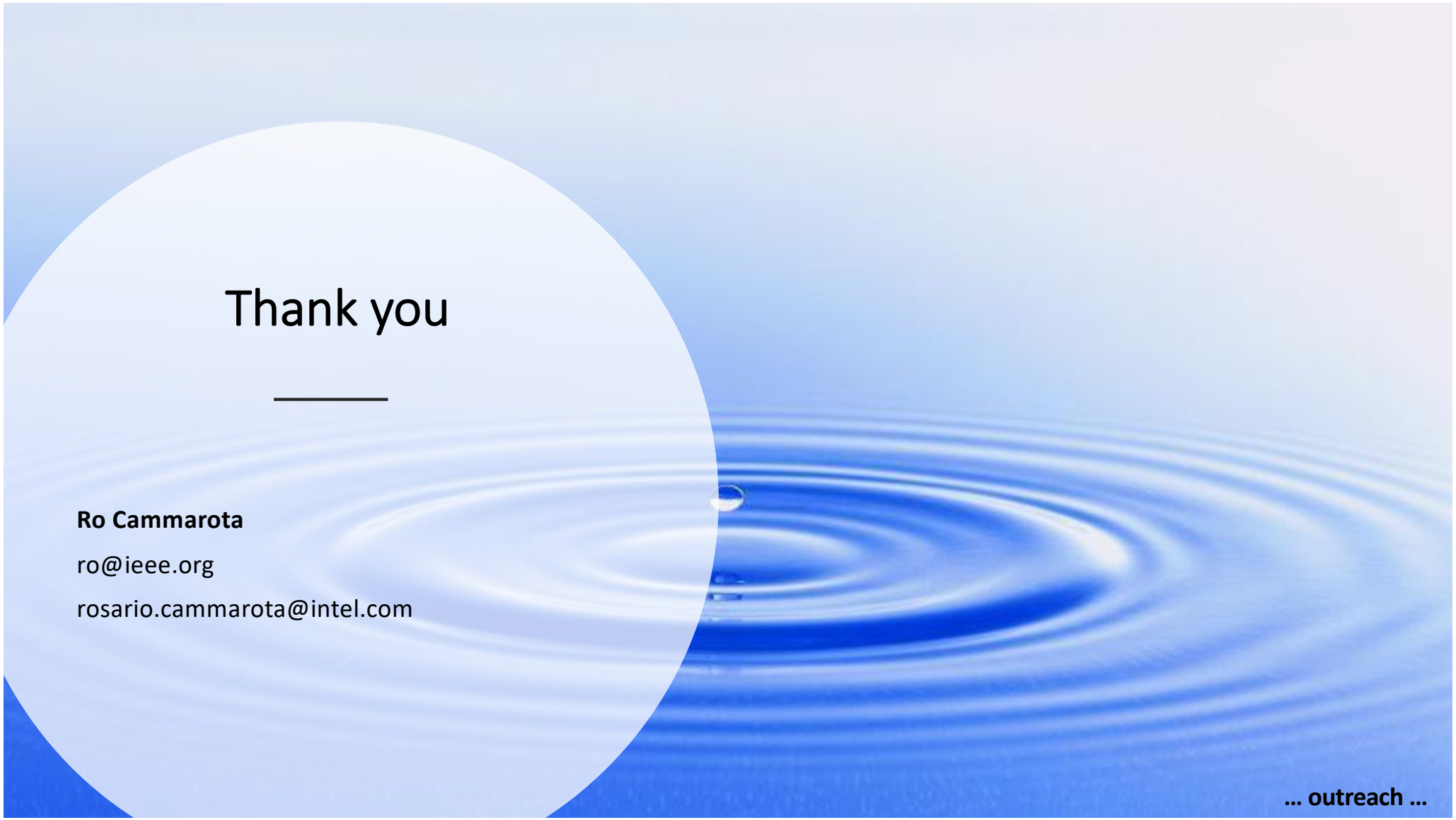
- Performance/ resource utilization never looked better (for digit recognition – figures above.)
- Expected deployment for consumers use cases, such face recognition, preventive health-care, recommendation systems other machine learning services, but also localization.
- More performance improvement possible with leveraging architecture specific optimizations, e.g., avx, blocking, maybe accelerators.

Proposals/ Recommendations

- Proposal 1 – coming ~8-10 weeks: improve technical writing
  - Derive new documents to the highest level of details required (e.g., for IETF submissions)
  - *Decide on the standards document type.*
  - *Add Implementable Procedures.*
  - *Add Test Vector*.
  - Decide on one scheme to begin with, e.g., BFV, but leave space to expand.

- Proposal 2 – coming ~1-2Qr: create a new document with benchmarks and both quantitative/ qualitative assessments.
  - Decide on the benchmarks and benchmark setup.
  - Create and open the benchmark to the public.

- Recommendations: Strategy and Tactics – ~2-5 years run.
  - *Produce a draft for IETF standards track – the least it requires executing of proposals 1.*
  - Consider the possibility of study groups at ISO and IETF, or IETF and find adoption in IEEE application standards – *requires executing of proposal 2*
  - A third alternative is IEEE – *requires executing proposal 1 and 2.*



Ro Cammarota

ro@ieee.org

rosario.cammarota@intel.com