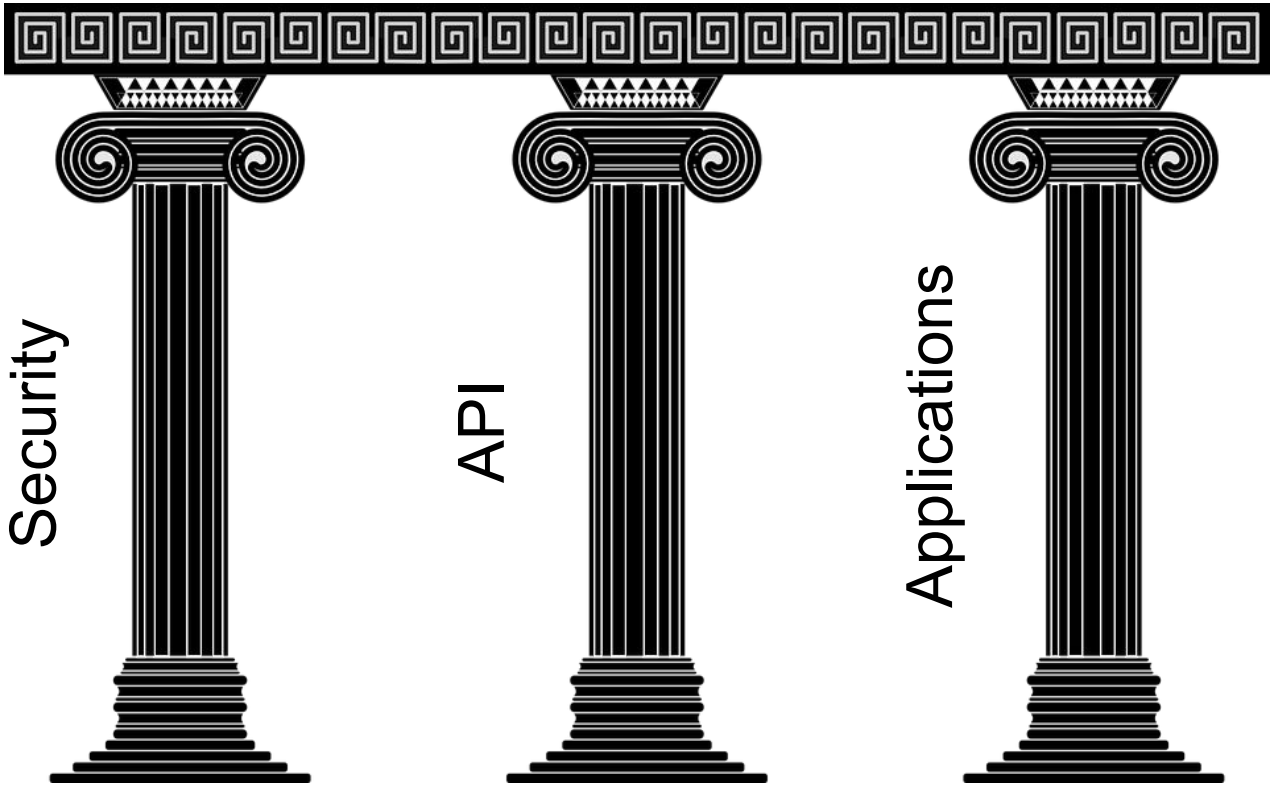
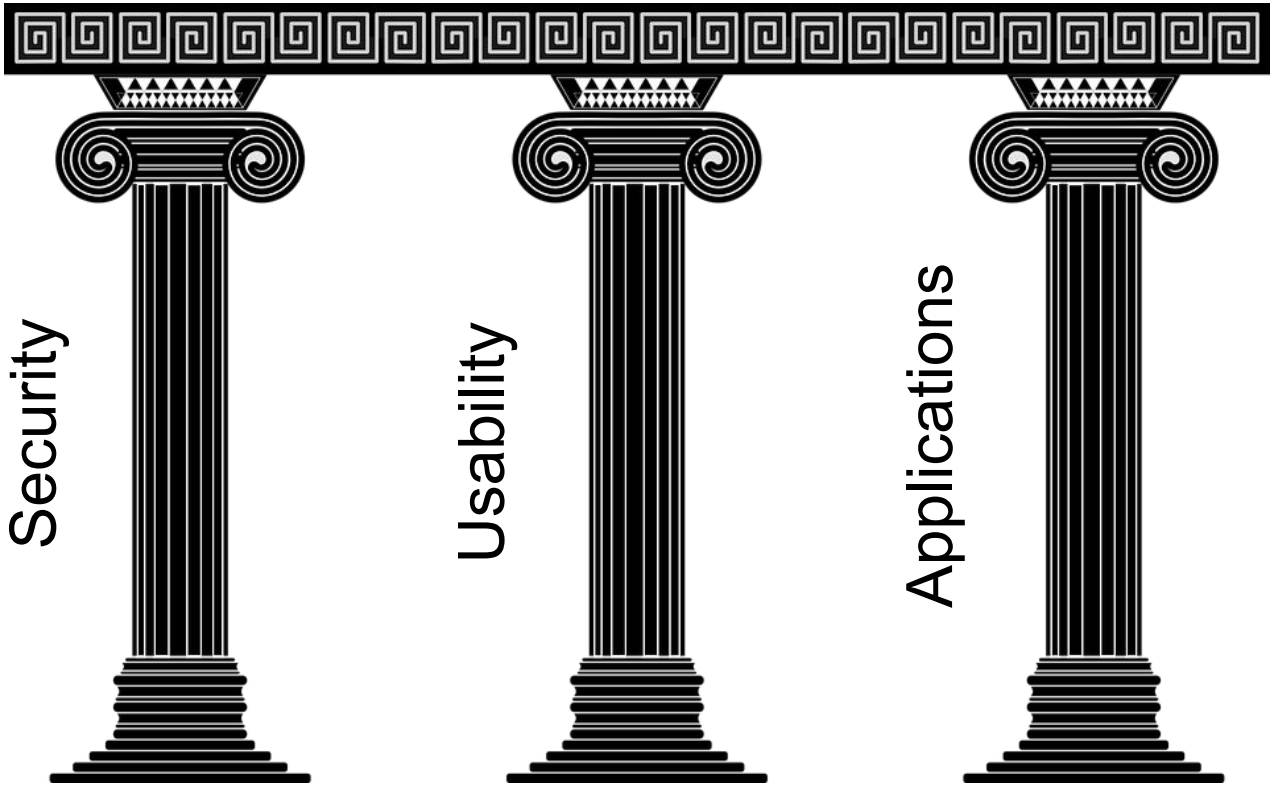
Updates from the Standardization Community

Kim Laine, Microsoft
Organizing Committee

Three Pillars (2017)



Three Pillars (2019)



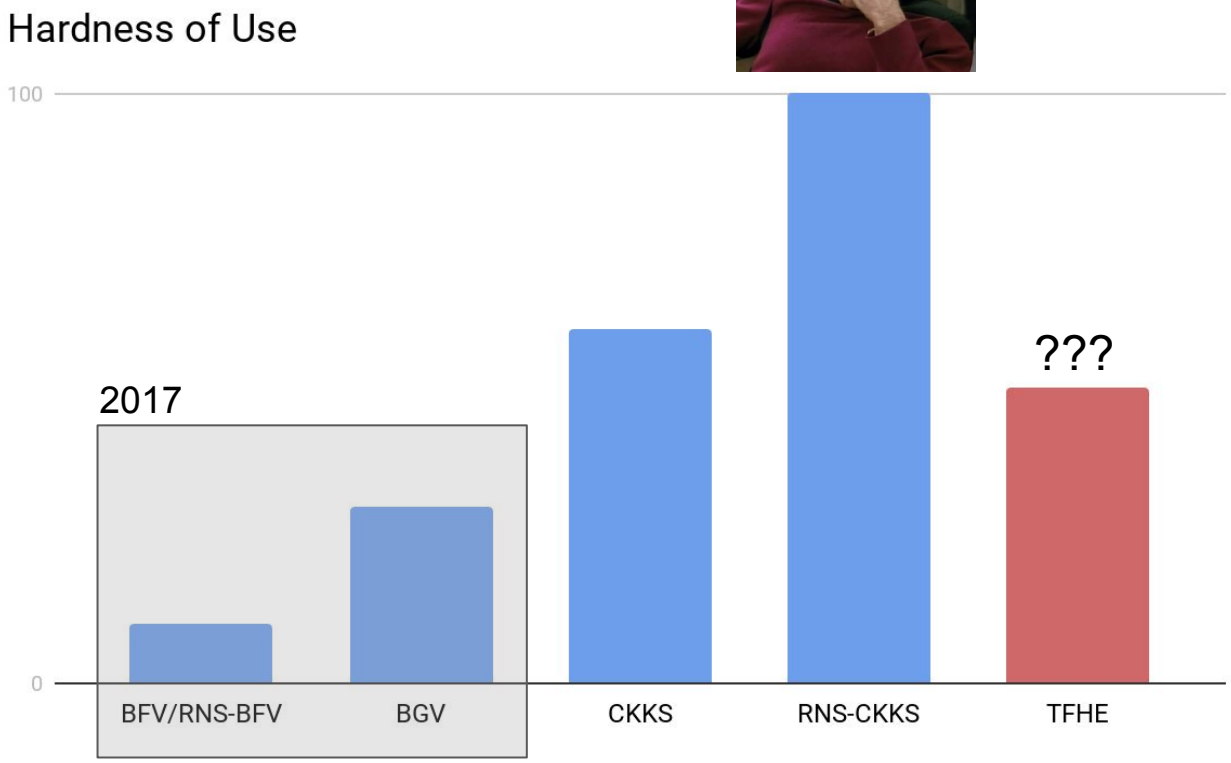
Security

First version of security standard approved at MIT workshop

Polishing and minor improvements since then

Adoption rate?
New attacks?
Next steps?

Popular Schemes



Applications (2017)

The following table presents some key attributes of the different applications discussed in this document:

Domain	Genomics	Health	National Security	Education
Topic	Match Maker	Billing and Reporting	Smart Grid (Municipal Service)	School Dropouts
Data Owner	Medical Institutions	Small Hospital, Clinic	Nodes and Network	School, Hospital, Welfare
Latency of Service	Hours	Hours	Quasi-Real Time	Week
Data volume (size x no)	DB O(1000X1MB) Query O(1KB)	O(10M) x O(1M)	O(1M) x O(1M)	O(1K) x O(1M)
Data persistency	Add Only	Add Only	Add Only	Add Only
Technical Issues	Comparison, Sorting Auditing Privacy	Tabulation, Linear Algebra	Comparison	Comparison Matrix Analysis
When is possible	1 years	2-3 years	Now	2-3 years
Why HE?	HIPAA	Cyber insurance	Privacy	FERPA
Who pays?	Health Insurance	Hospital	Energy Company	DoE

Applications (2019)

What to say?

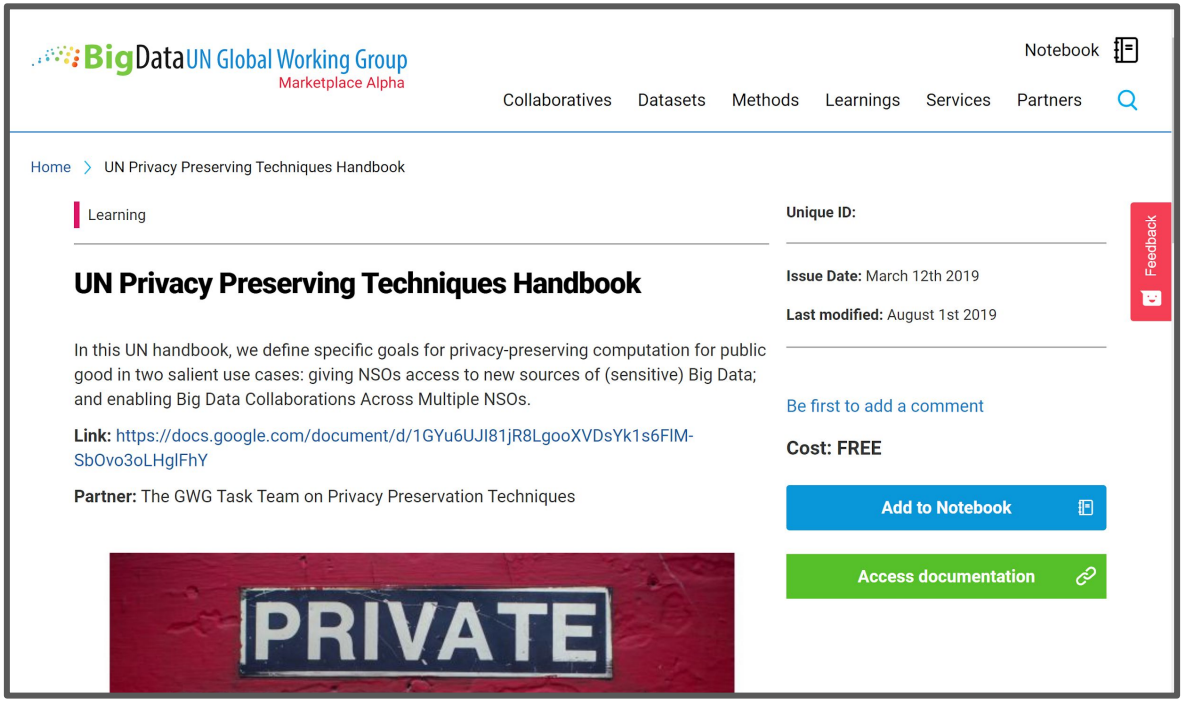
- ❏ Improved understanding of realistic application domains

- ❏ Private inference
- ❏ Private learning
- ❏ Medical applications
- ❏ Financial applications

- ❏ iDASH competition
- ❏ Private Set Intersection
- ❏ Building block for hybrid protocols
- ❏ Multiple start-ups

What should the standards community do, if anything?

Applications (2019)



https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook

Applications (2019)

Financial Conduct Authority (UK)
Week-long hackathon

Financial crime detection by enabling cross-bank collaboration on detection on anomalous customer behavior

Cross-disciplinary teams

HE, MPC used

Main challenge is not the PET but understanding legal/regulatory framework and incentives

https://www.fca.org.uk/events/techsprints/aml-financial-crime-international-techsprint

Agenda for Today

Time	
8:00-9:00	**Registration and networking breakfast / Poster set-up**
9:00-9:15	**Intro and welcome**; Casimir Wierzynski (Intel)
9:15-10:15	**Status updates of the standards community**; Kim Laine (Microsoft), Tancrede Lepoint (Google), Jung Hee Cheon (Seoul National University), Ro Cammarota (Intel)
10:15-11:15	**Usability for application developers**; Flavio Bergamaschi (IBM Research), Fabian Boemer (Intel), Kurt Rohloff(Duality), Axel Schröpfer (SAP); moderated by Shai Halevi (Algorand)
11:15-11:30	**Poster preview;** (1 min no-slide announcement per poster.)
11:30-12:30	**Lunch / Posters**
12:30-13:00	**Applications**; Kurt Rohloff (Duality), Juan Troncoso-Pastoriza (EPFL)
13:00-13:30	**Update from Libraries mailing list**; Kim Laine (Microsoft), Yuriy Polyakov (NJIT), Mariya Georgieva (Inpher)
13:30-14:00	**Break / Posters**
14:00-15:30	**Security standard discussion**; Kristin Lauter (Microsoft), Daniele Micciancio (UCSD), Rachel Player (RHUL), Ben Curtis (RHUL)
15:30-15:45	**Break / Posters**
15:45-16:30	**Governance**; Yaron Sheffer (Intuit), Bastiaan Quast (ITU)
16:30-17:00	**Going forward and conclusion;** Straw poll on next workshop

Poster Preview

Poster presenters have an **exactly** 1 min slot to give an elevator pitch for their poster! The elevator pitch can be shorter too.

Great opportunity to get the audience excited about your work and practice your skills in summarizing complex topics.

No slides.