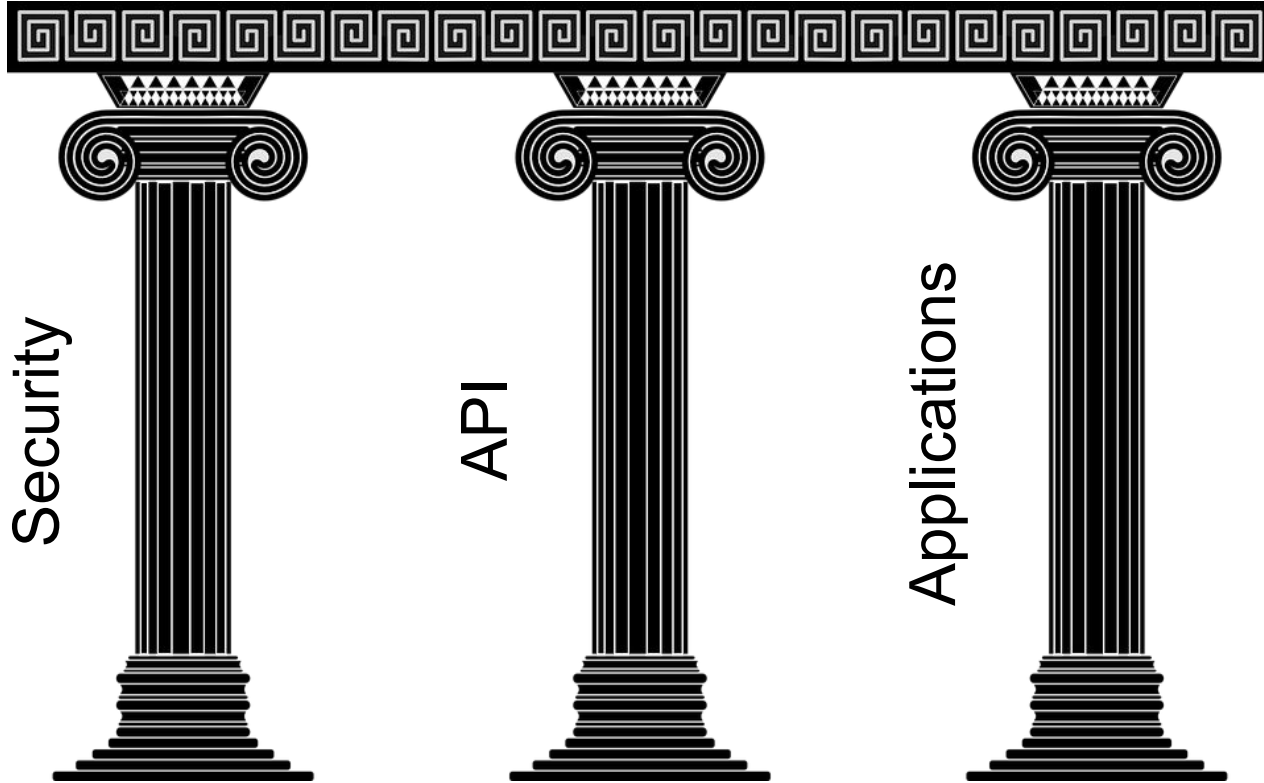


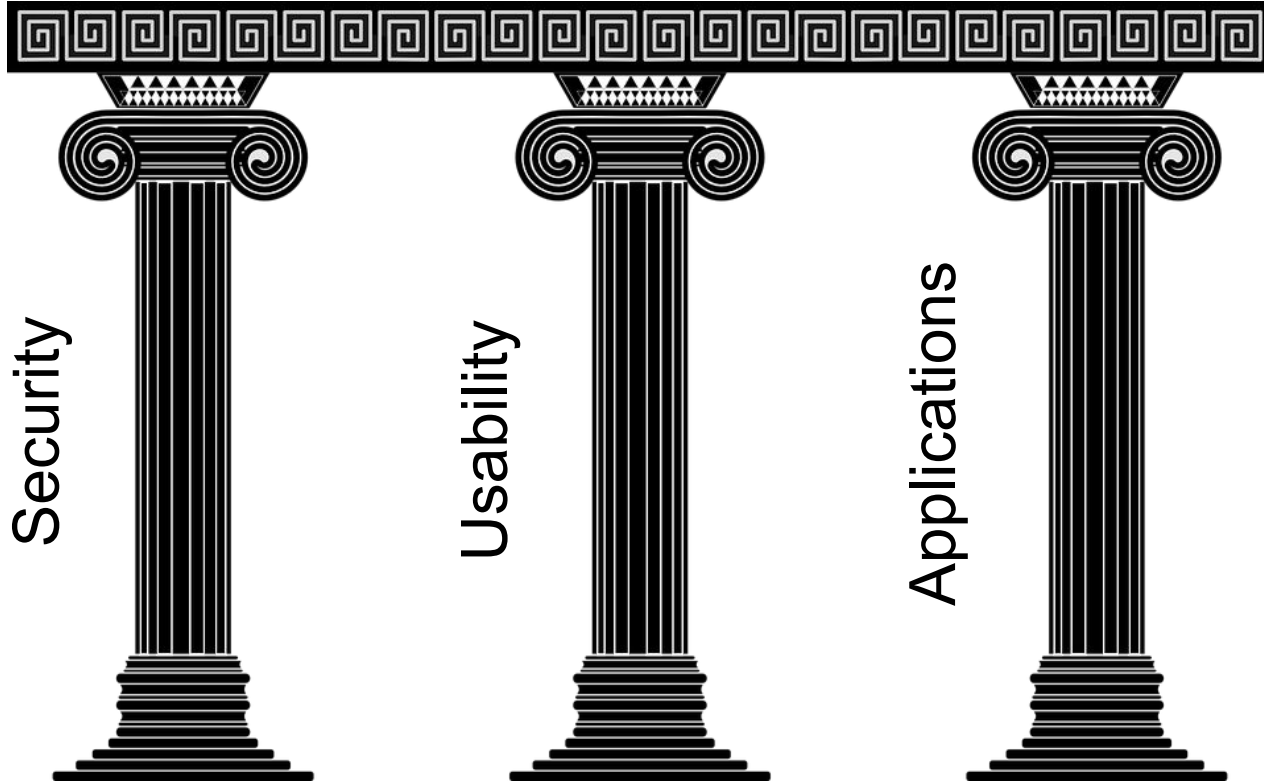
# Updates from the Standardization Community

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?

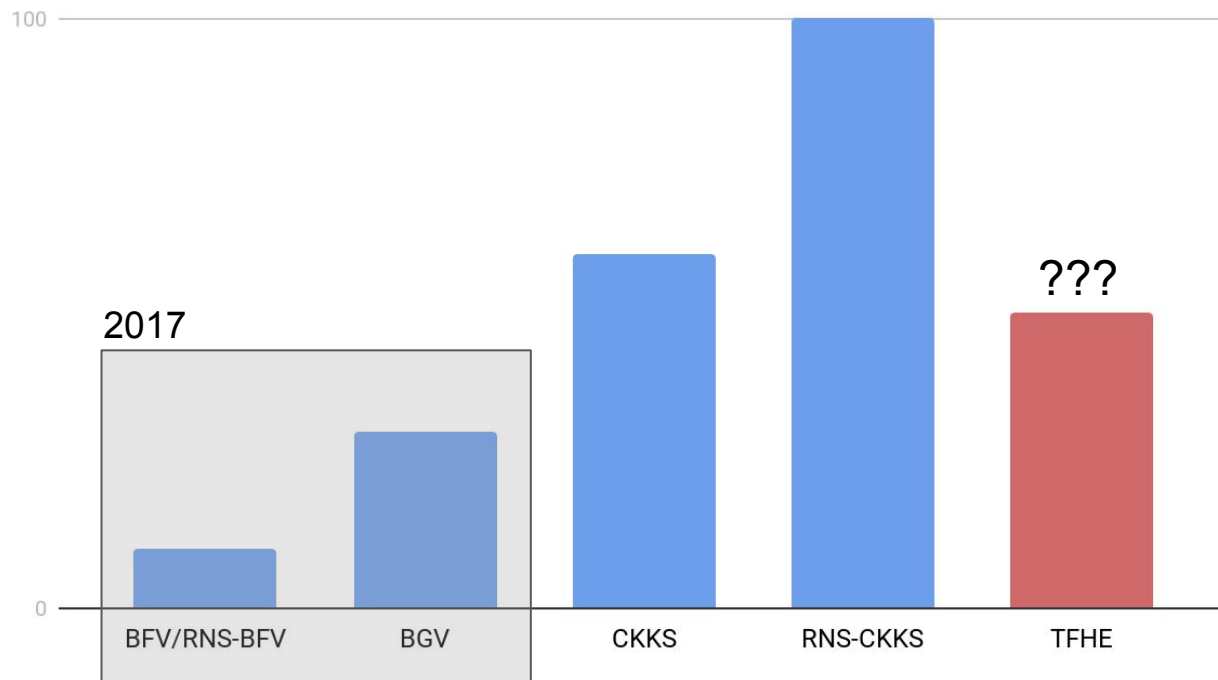
New attacks?

Next steps?



# Popular Schemes

Hardness of Use



# 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)

The screenshot shows the 'Big Data UN Global Working Group Marketplace Alpha' interface. The header includes the logo and navigation links: Collaboratives, Datasets, Methods, Learnings, Services, Partners, and a search icon. A 'Notebook' icon is also present. The breadcrumb trail indicates the location: Home > UN Privacy Preserving Techniques Handbook. The main content area features a 'Learning' tab, the title 'UN Privacy Preserving Techniques Handbook', a description of the handbook's goals, a link to the document, and the partner information. On the right, there is a sidebar with fields for 'Unique ID', 'Issue Date', and 'Last modified', a 'Feedback' button, and a 'Be first to add a comment' link. At the bottom of the sidebar are two buttons: 'Add to Notebook' and 'Access documentation'. A large 'PRIVATE' stamp is visible at the bottom of the main content area.

Big Data UN Global Working Group  
Marketplace Alpha

Notebook

Collaboratives Datasets Methods Learnings Services Partners

Home > UN Privacy Preserving Techniques Handbook

Learning

## UN Privacy Preserving Techniques Handbook

In this UN handbook, we define specific goals for privacy-preserving computation for public good in two salient use cases: giving NSOs access to new sources of (sensitive) Big Data; and enabling Big Data Collaborations Across Multiple NSOs.

**Link:** <https://docs.google.com/document/d/1GYu6UJI81jR8LgooXVDsYk1s6FIM-SbOvo3oLHglFhY>

**Partner:** The GWG Task Team on Privacy Preservation Techniques

Unique ID:

Issue Date: March 12th 2019

Last modified: August 1st 2019

Be first to add a comment

Cost: FREE

Add to Notebook

Access documentation

Feedback

PRIVATE

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