

Measuring AI Adoption – Without Seeing Company Data

BIS Workshop on Data Security and Privacy
September 14, 2026



DEVELOPMENT
DATA PARTNERSHIP

Context

The World Bank, IMF and OECD are collaborating with the Frontier AI Labs to measure global AI adoption, by aggregating AI usage statistics.

Each Frontier AI Lab (Partner) is willing to contribute to the aggregate, provided their **individual, commercially sensitive contribution is not disclosed to any other Partner, to the Development Banks, or the public.**



Problem

How do you aggregate statistics from Partners without anyone — including the aggregator — being able to learn the individual inputs?



Solution

Masked Submission with Pairwise Noise Cancellation

Each Partner disguises their real number by adding or subtracting a shared, secret "noise" value before submitting it.

When all submissions are summed, the noise values cancel each other out, leaving only the true total.



Masked Submission with Pairwise Noise Cancellation

Paired partners add or subtract a shared noise value

Pair	Shared Noise	Who Adds It	Who Subtracts It
PartnerA ↔ PartnerB	150,000	PartnerA (+150,000)	PartnerB (-150,000)
PartnerA ↔ PartnerC	80,000	PartnerA (+80,000)	PartnerC (-80,000)
PartnerB ↔ PartnerC	45,000	PartnerB (+45,000)	PartnerC (-45,000)

Partner	Actual Value	Noise	Submission
Partner A	1,000,000	+230,000	1,230,000
Partner B	500,000	-105,000	395,000
Partner C	200,000	-125,000	75,000
Total	1,700,000	0	1,700,000 ✓

The aggregator sees only this



Masked Submission with Pairwise Noise Cancellation

Paired partners add or subtract a shared noise value

Partner	Actual Value	Noise	Submission
Partner A	1,000,000	+230,000	1,230,000
Partner B	500,000	-105,000	395,000
Partner C	200,000	-125,000	75,000
Total	1,700,000	0	1,700,000 ✓

- Noise is a shared random number
- When it is added to or subtracted, it masks the actual value
- This masking is done on the Partners side ensuring the aggregator cannot see the real value.
- Every Partner knows their value and can know their pairwise noise.
- In a 3-party system with no colluding players, no Partner can identify the value of another Partner.



Masked Submission with Pairwise Noise Cancellation

Paired partners add or subtract a very large, shared noise value

- This noise is generated using a uniform distribution.
- Noise is generated per agreed dimension, time
- minNoise1_000_000_000_000 (1T)
- maxNoise1_000_000_000_000_000 (1Q)
- **The Noise would be much larger than the anticipated token value**

Partner	Actual Value	Noise	Submission
Partner A	300,000,000,000,000	+23,000,000,000,000	323,000,000,000,000
Partner B	80,000,000,000,000	-10,500,000,000,000	69,500,000,000,000
Partner C	40,000,000,000,000	-125,000,000,000,000	-85,000,000,000,000



Shared Noise Generation

Shared noise is created by sharing a secret key between Partner Pairs



Every Partner generates a key pair

A key-pair comprises an encapsulation and a decapsulation key. Encapsulation key is used to generate the **shared secret** and a cipher text.



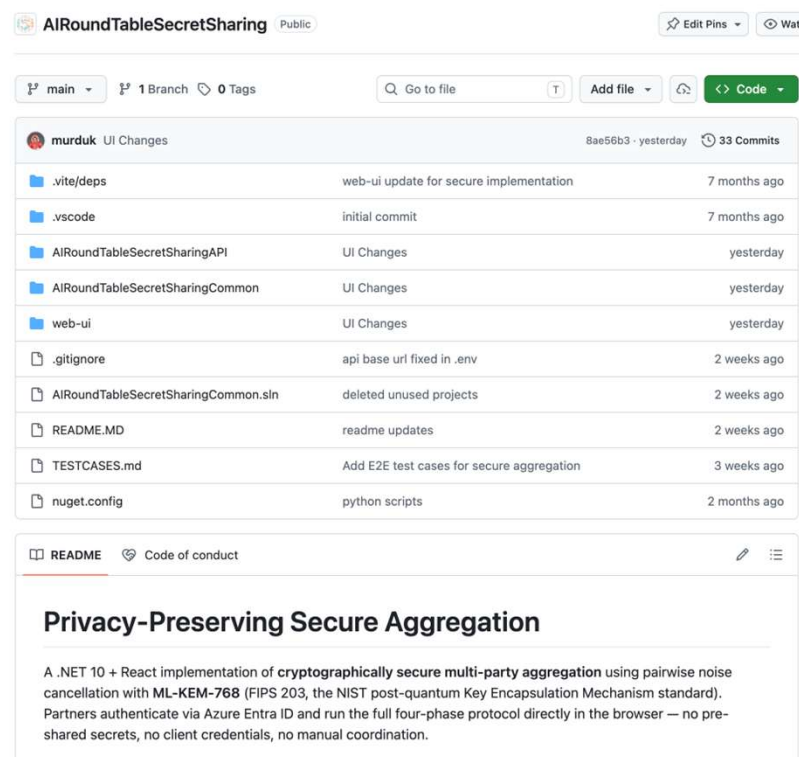
Aggregator facilitates encapsulation key and cipher text sharing

World Bank facilitates the sharing of the encapsulation keys and cipher texts between partners but cannot decapsulate the cipher text.



ML-KEM-768 is used for key exchange

This is a post-quantum, NIST-standardized key encapsulation mechanism that allows for secret sharing.



Encrypted Secret Sharing & Shared Noise Generation

1

Key Generation

Each Partner generates an encapsulation and decapsulation key locally. The Encapsulation key is shared with the Aggregator (World Bank)

2

Encapsulation

Each partner uses the other partners' Encapsulation keys to generate a shared secret and a cipher text. Cipher text is shared through the aggregator. The aggregator cannot read the shared secret inside the cipher text.

3

Decapsulation

Each partner retrieves the cipher texts addressed to them and uses their decapsulation key (which never leaves their system) to recover the shared secret from the cipher text.

4

Masked Submission

Each partner uses the shared secret to compute noise, applies it to their real value, and submits only the masked value to the aggregator.



Pros and Cons of this Approach

- The aggregator learns **only the total** never any individual partner's value.
- Partners **do not communicate directly** with each other.
- **No pre-shared secrets** are needed
- The system is secure against **quantum computers** (post-quantum standard).
- Partner identity is verified through **Azure Entra ID** no separate credentials to manage.

- **All partners** in a group (called an "epoch") **must submit** before the aggregate is available.
- If $n-1$ partners deliberately collude, they could theoretically deduce the last partner's value. This is a feature not a bug.
- A partner who drops out midway through the protocol (after generating keys but before submitting) will block the aggregate for that epoch.
- The aggregator **cannot verify** that partners submitted **honest values**



Implementation

To implement this data sharing mechanism, all Partners need to adopt **Pairwise Noise Cancellation (PNC) using ML-KEM-768 key exchange (the solution)**.

Adoption of the solution can be done in two ways

- 1. Machine-to-Machine Solution:** Each Partner will implement and deploy the solution based on the agreed, shared protocol.
- 2. Human-to-Machine Solution:** World Bank will implement and deploy the solution on a web interface that can be used directly by Partners.

Proposal currently under discussions with Frontier AI Labs: Implement **human to machine approach first**, which is more controlled and feasible with agreed timeline, **followed by machine-to-machine approach**, which is more sustainable.





THANK YOU

Contact points:

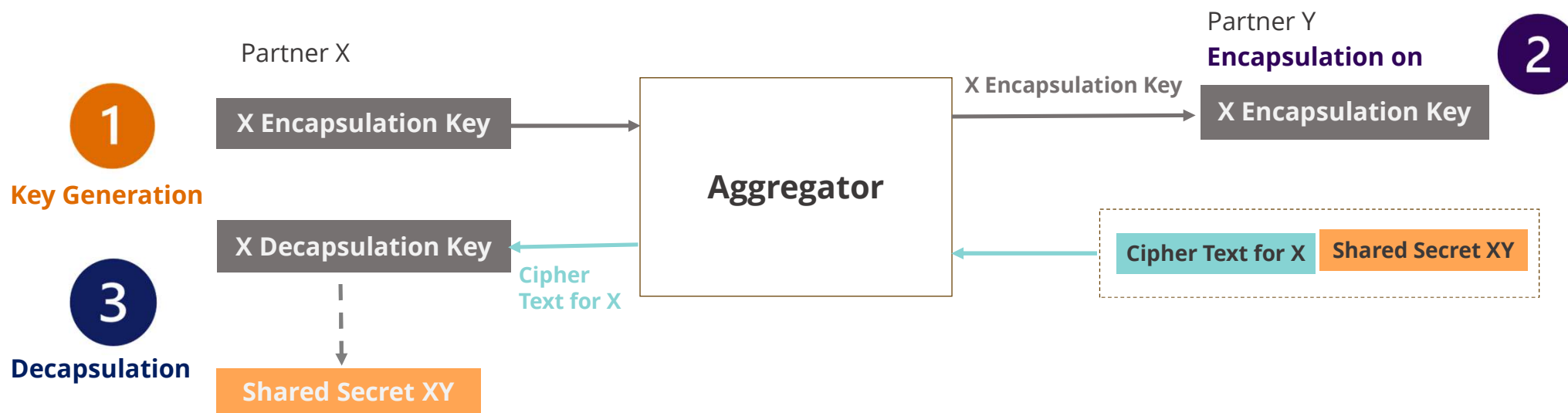
Marco Marini (IMF, mmarini@imf.org)

Mert Ozdag (World Bank, mozdag@worldbankgroup.org)

datapartnership.org

Annex - Encrypted Secret Sharing

A secret key is shared through quantum proof encryption



Annex contd.- Shared Noise Generation

Shared noise is created by sharing a secret key between Partner Pairs

