cisco Live!

Let's go

#CiscoLive

The bridge to possible

Data Protection

with Homomorphic Encryption and Multiparty Computing

Frank Michaud Principal Engineer
@fmiche76

BRKETI-2004

Cisco Webex App

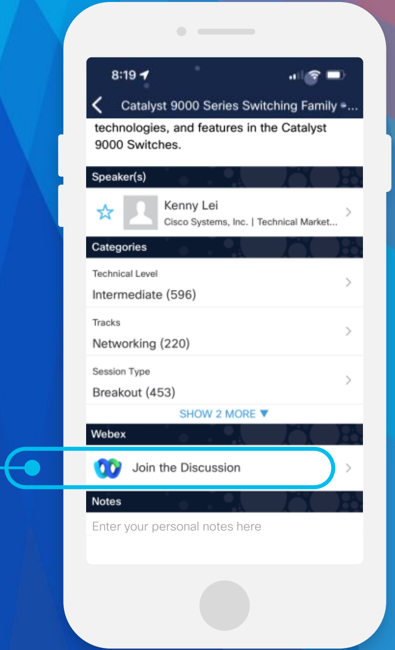
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

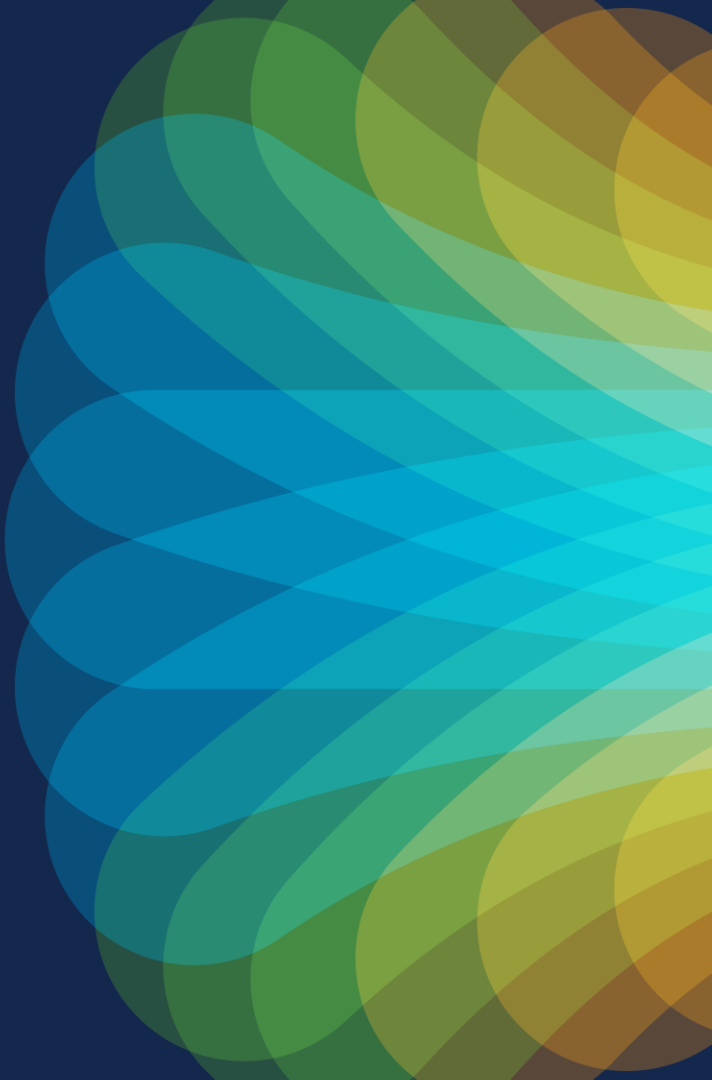
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKETI-2004

Agenda

- Introduction
- Data Protection
- Introducing Homomorphic Encryption and Multi-Party Computing
- Some Use Cases
- Summary and Key Takeaways

Introduction

to data protection



Data today

110 110
1011 1011
010 010

Data
the new crown jewels of enterprise

Data risks today

Data
the new crown jewels of enterprise

Therefore,

Raises the interest of
hackers and regulations

Data Protection

today

Data protection

Trends and reality today

Regulations

Sovereign

Breaches
time to detection

Challenges for organization today

aaS transformation

mobility

Challenges for organization today

aaS transformation

mobility

CISO

Solution

Avoid complexity

Solution

Avoid complexity

Simple concepts: “keep the data where you can protect it”

Solution

Avoid complexity

Simple concepts: “keep the data where you can protect it”

Need of new tools

Introducing

homomorphic encryption and multi-party computing

Introducing
Homomorphic Encryption and Multi-Party Computing

introduced

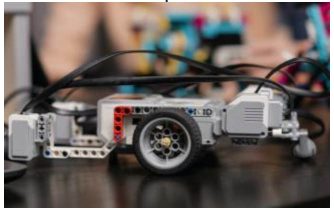
research

3rd FHE generation

Late 70s

2008

2016



1st practical MPC

Let’s see how it works

Homomorphic Encryption

Introducing

Homomorphic encryption

$$message\!: m \xrightarrow{\text{Function: } f} f(m)$$

Introducing
Homomorphic encryption

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, "Enc"'] & f(m) \arrow[d, "Enc"'] \\
Enc(m) \arrow[r, "f"] & Enc(f(m))
\end{tikzcd}$$

Introducing

Homomorphic encryption

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, "Enc"'] & f(m) \arrow[d, "Enc"'] \\
Enc(m) \arrow[r, "f"] & Enc\big(f(m)\big) = F(Enc(m))
\end{tikzcd}$$

Introducing

Homomorphic encryption

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, "Enc"'] & f(m) \arrow[d, "Enc"'] \\
Enc(m) \arrow[r, "f"] & Enc\big(f(m)\big) = F(Enc(m))
\end{tikzcd}$$

Introducing

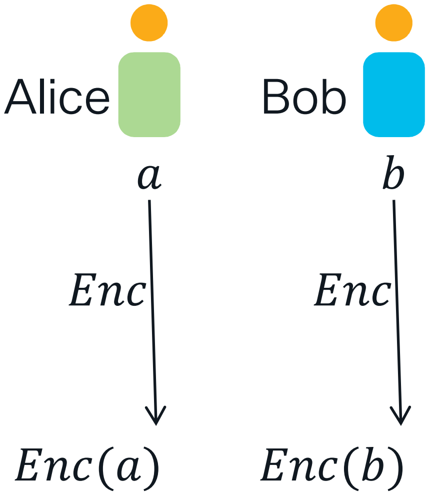
Homomorphic encryption

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, "Enc"'] & f(m) \arrow[d, "Enc"'] \\
Enc(m) \arrow[r, "f"] & F(Enc(m))
\end{tikzcd}$$

safe area

An example

Homomorphic encryption



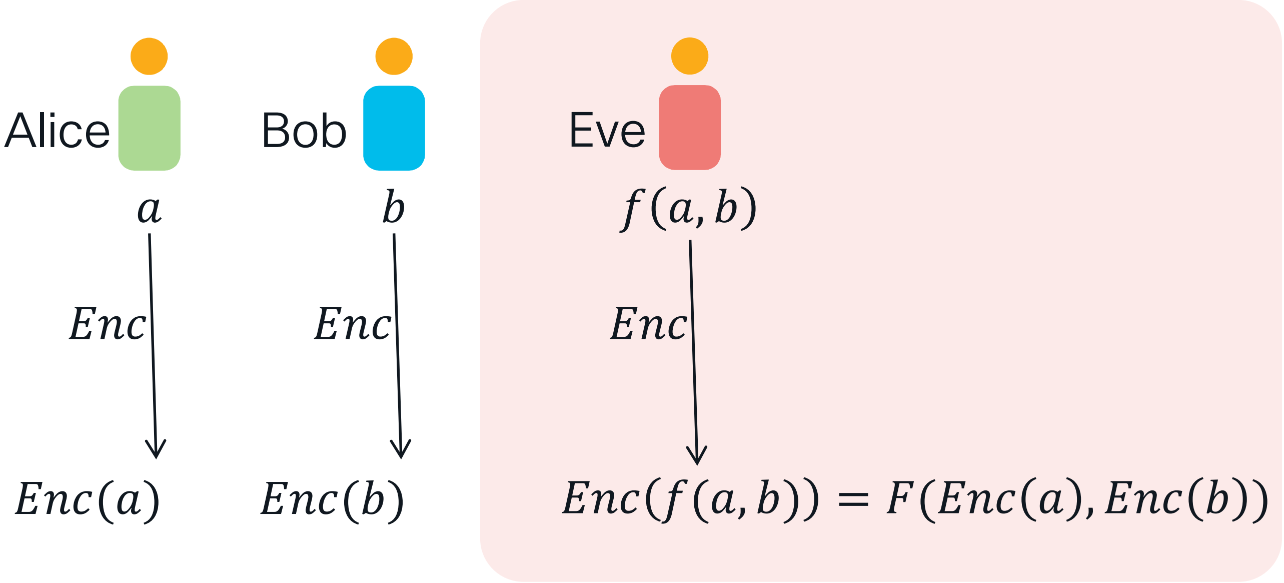
Alice

Bob

$$\begin{tikzcd}
a \arrow[d, "Enc"'] & b \arrow[d, "Enc"'] \\
Enc(a) & Enc(b)
\end{tikzcd}$$

An example

Homomorphic encryption



Alice

Bob

Eve

a

b

$f(a,b)$

Enc

Enc

Enc

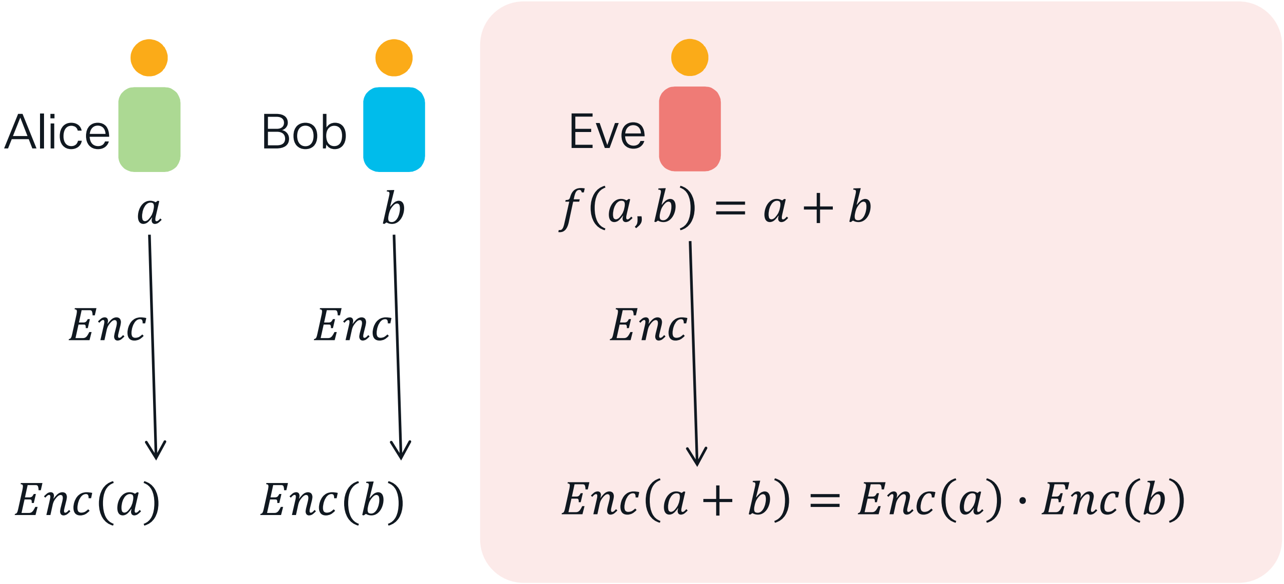
$Enc(a)$

$Enc(b)$

$$Enc(f(a,b)) = F(Enc(a), Enc(b))$$

An example

Homomorphic encryption



Alice a $\xrightarrow{Enc}$ $Enc(a)$

Bob b $\xrightarrow{Enc}$ $Enc(b)$

Eve

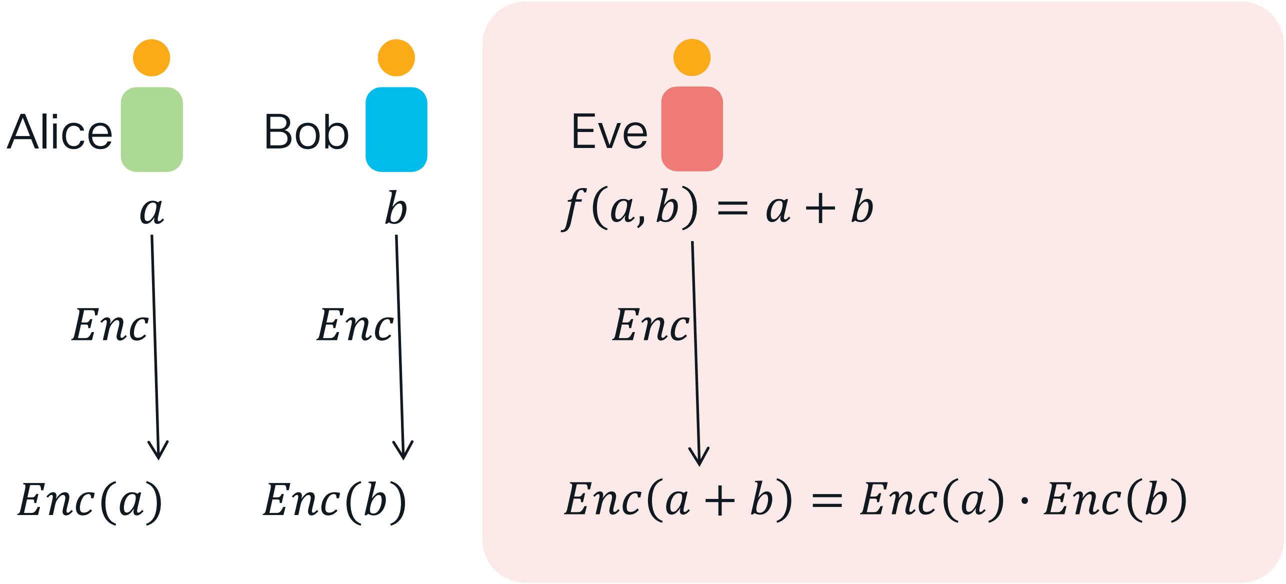
$f(a,b) = a + b$

Enc

$$Enc(a + b) = Enc(a) \cdot Enc(b)$$

An example

Homomorphic encryption



Alice

Bob

Eve

a

b

$f(a, b) = a + b$

Enc

Enc

Enc

$Enc(a)$

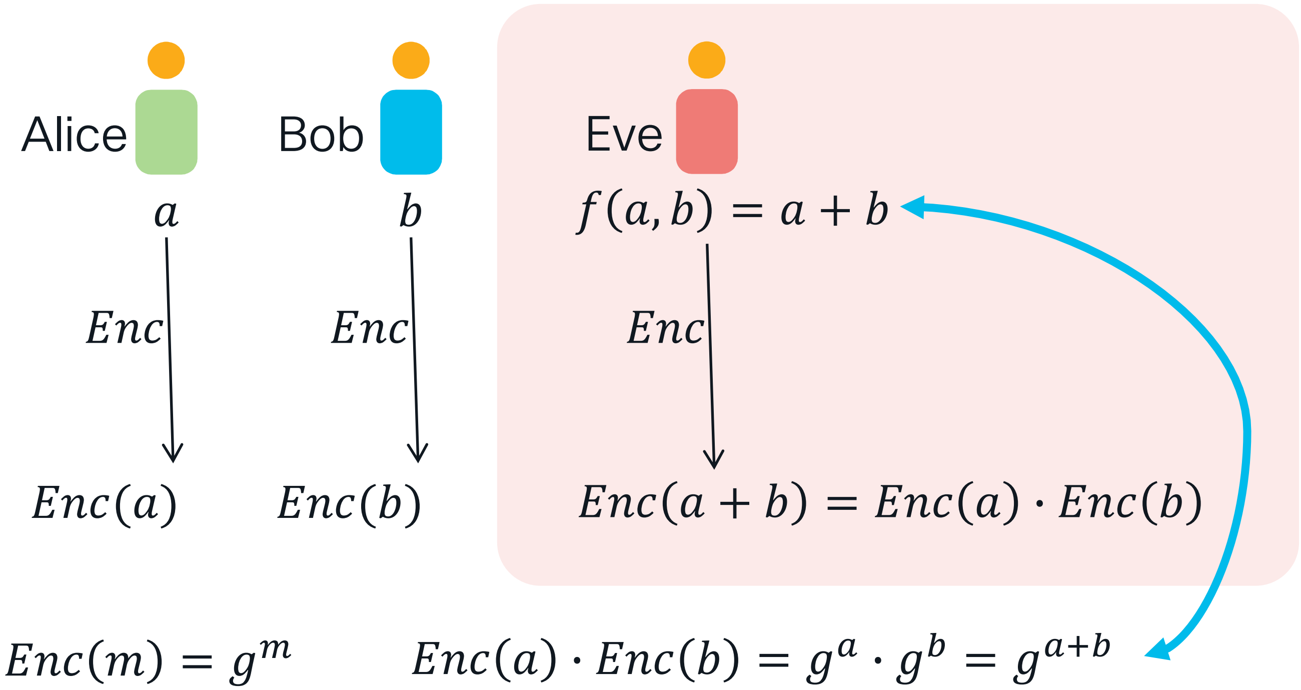
$Enc(b)$

$Enc(a + b) = Enc(a) \cdot Enc(b)$

$$Enc(m) = g^m \qquad Enc(a) \cdot Enc(b) = g^a \cdot g^b = g^{a+b}$$

An example

Homomorphic encryption



Alice

Bob

Eve

a

b

$f(a,b) = a + b$

Enc

Enc

Enc

$Enc(a)$

$Enc(b)$

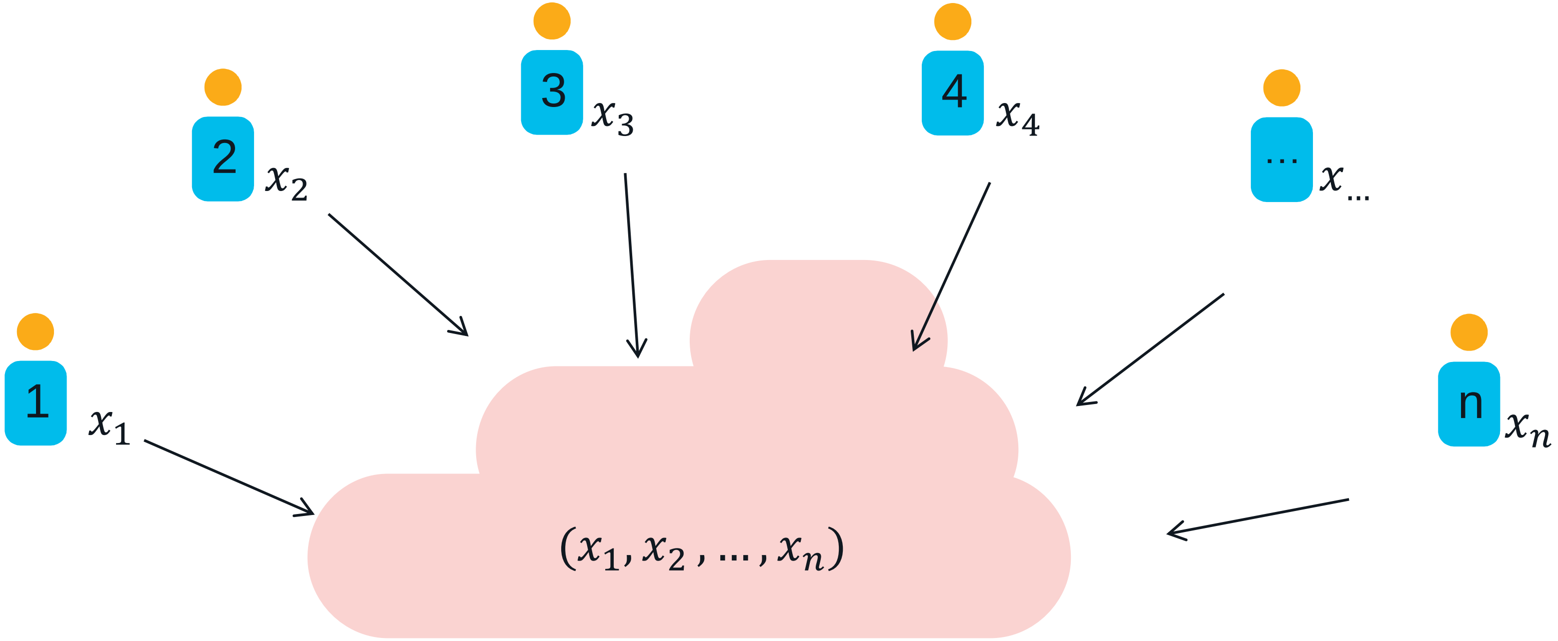
$Enc(a+b) = Enc(a) \cdot Enc(b)$

$$Enc(m) = g^m$$

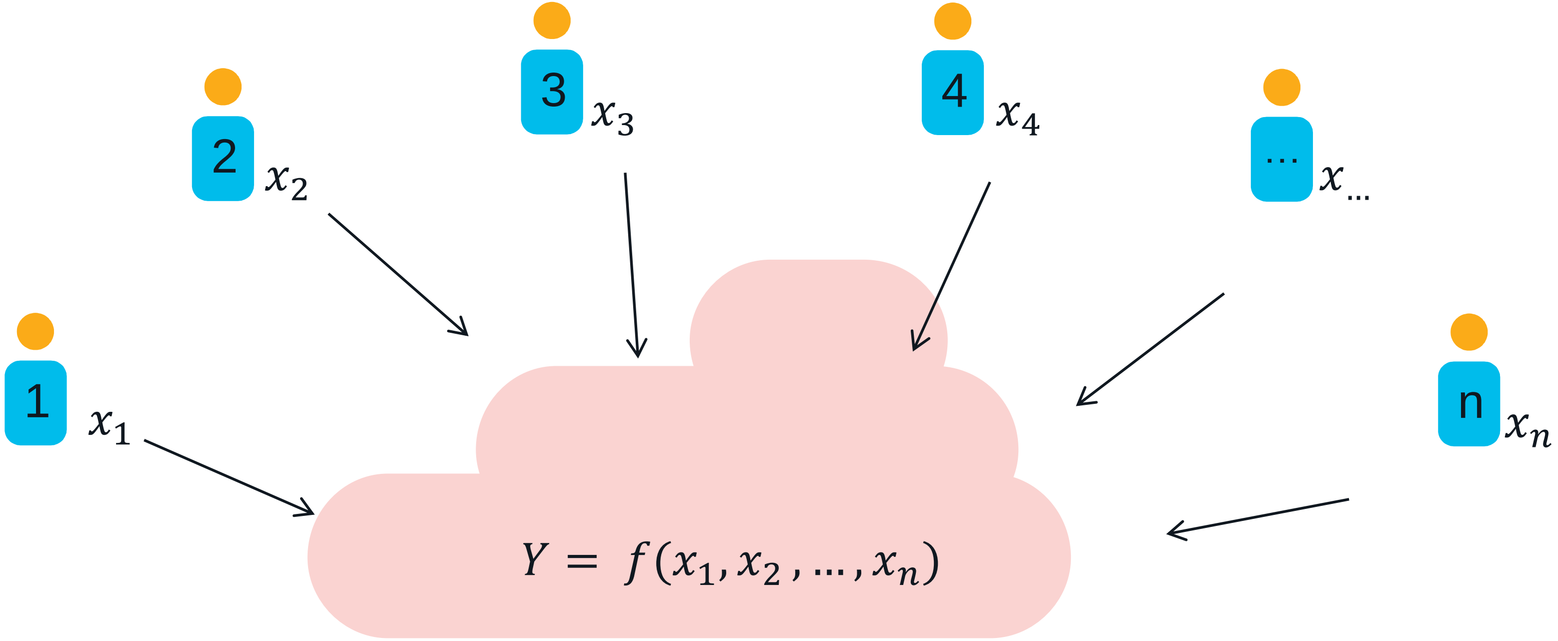
$$Enc(a) \cdot Enc(b) = g^a \cdot g^b = g^{a+b}$$

Multi-Party Computing

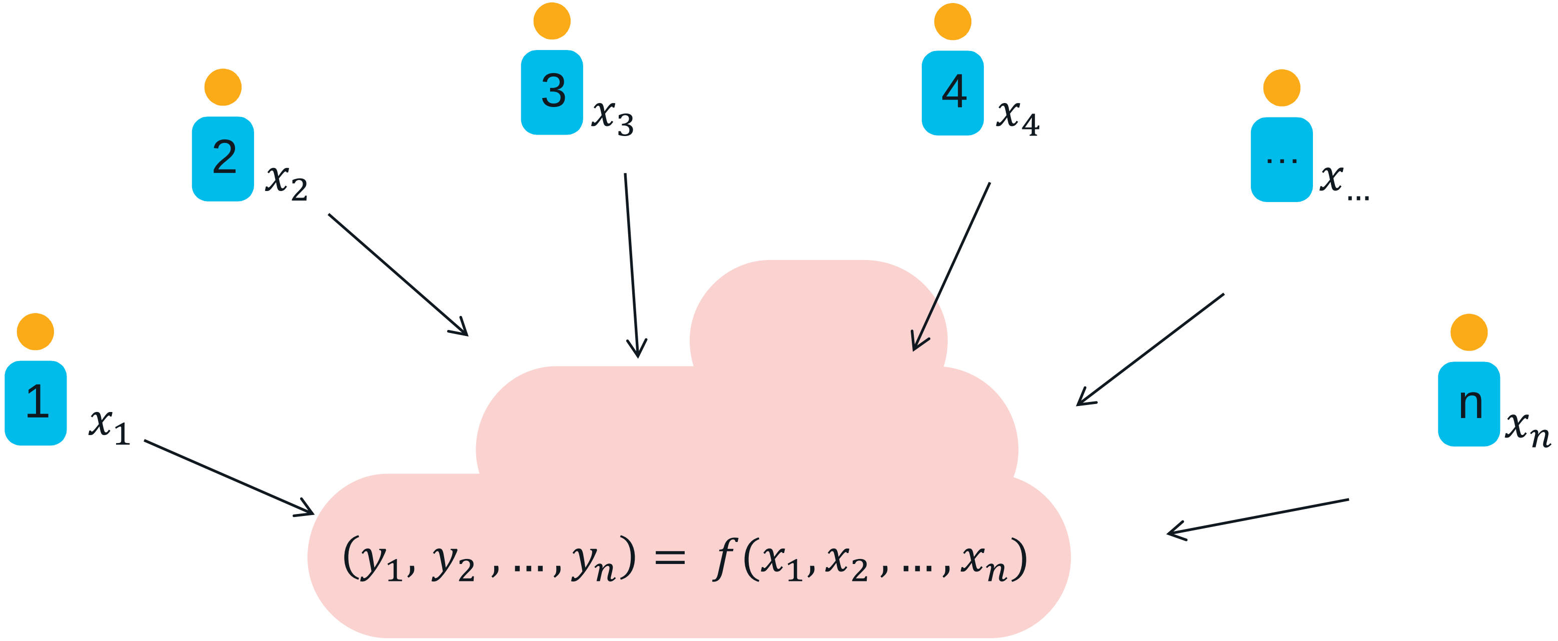
Introducing
Multi-Party Computing



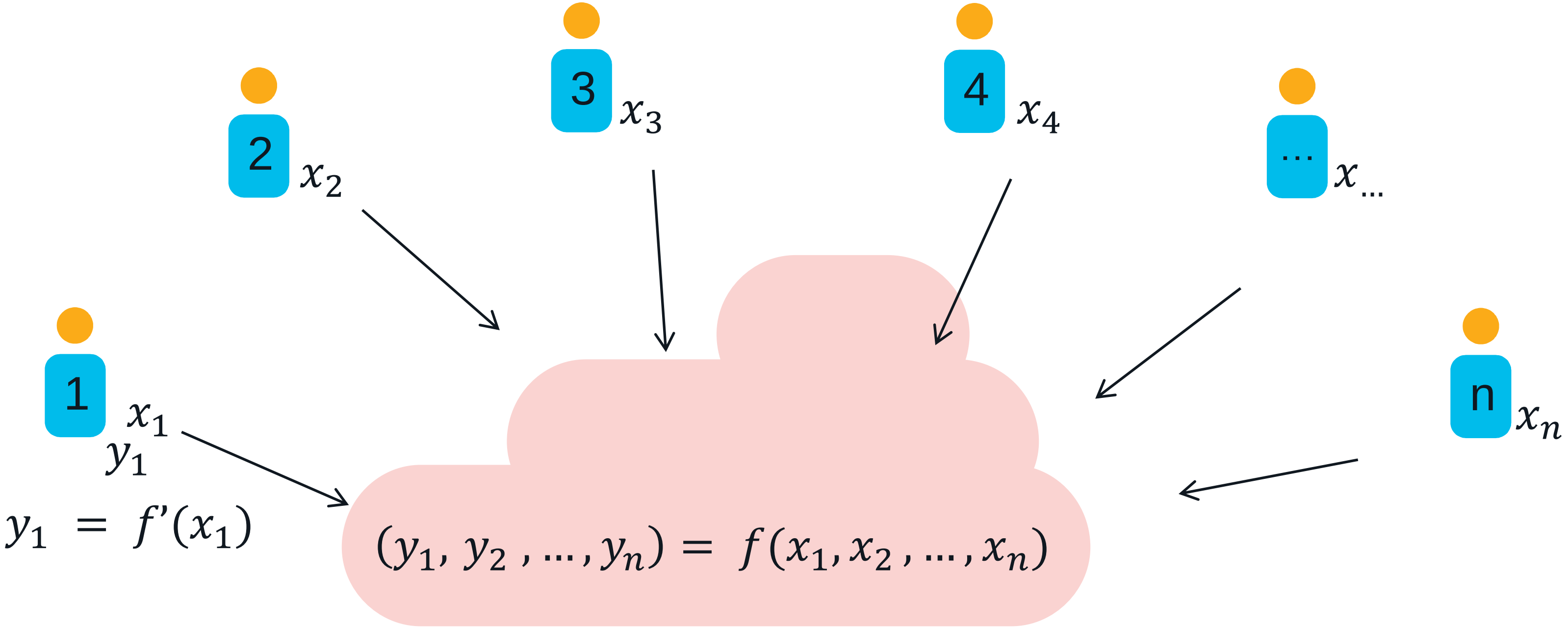
Introducing
Multi-Party Computing



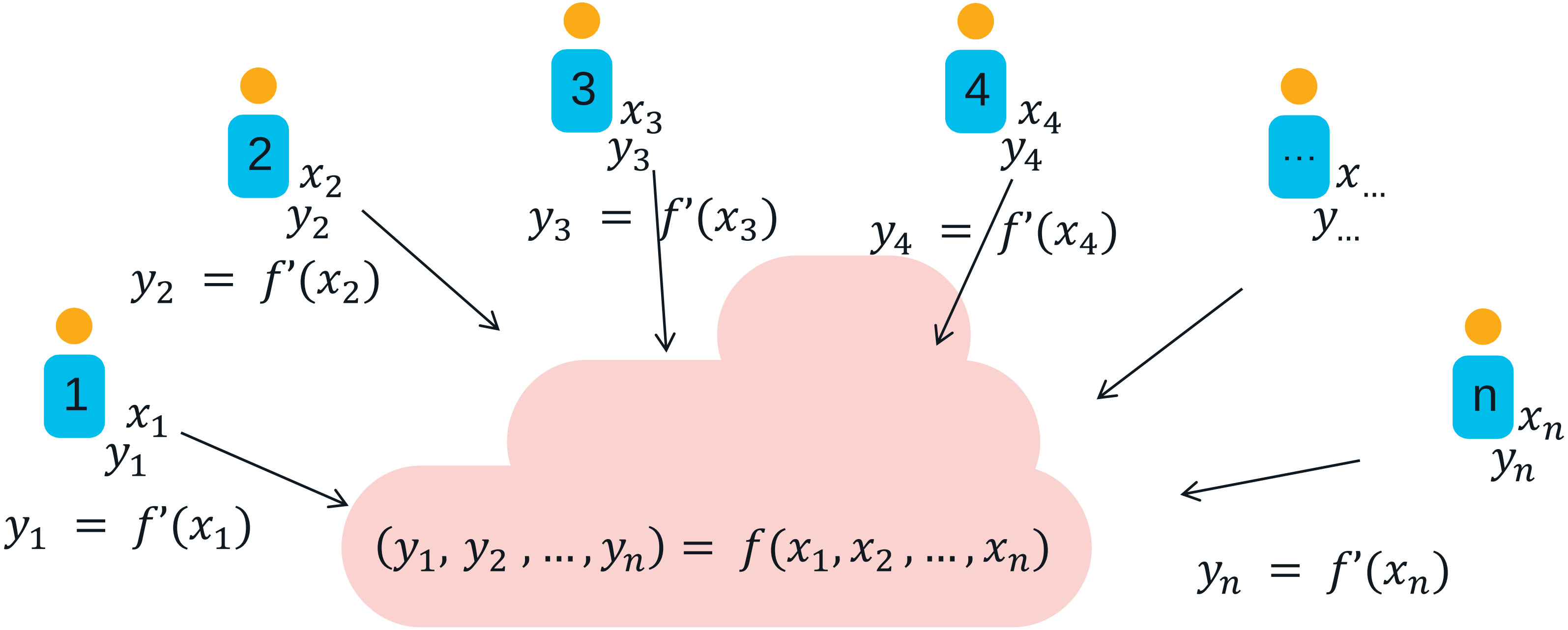
Introducing
Multi-Party Computing



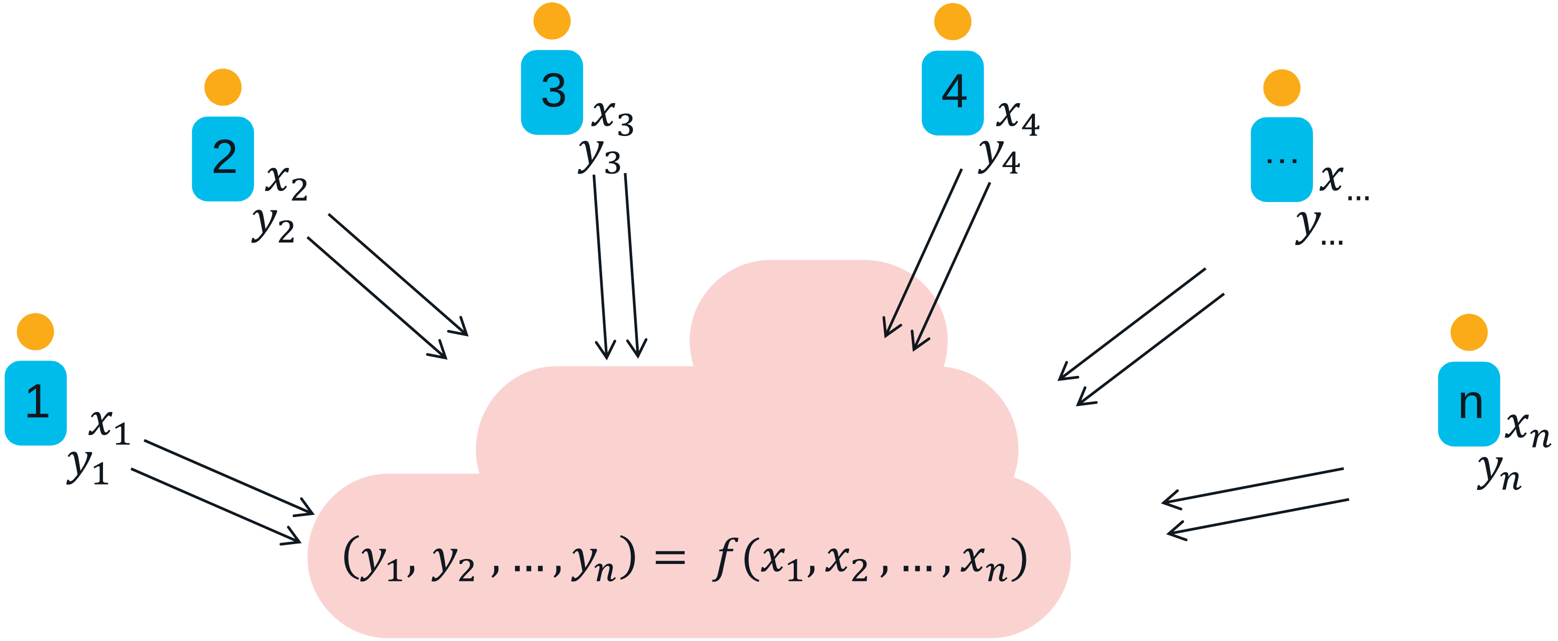
Introducing
Multi-Party Computing



Introducing
Multi-Party Computing

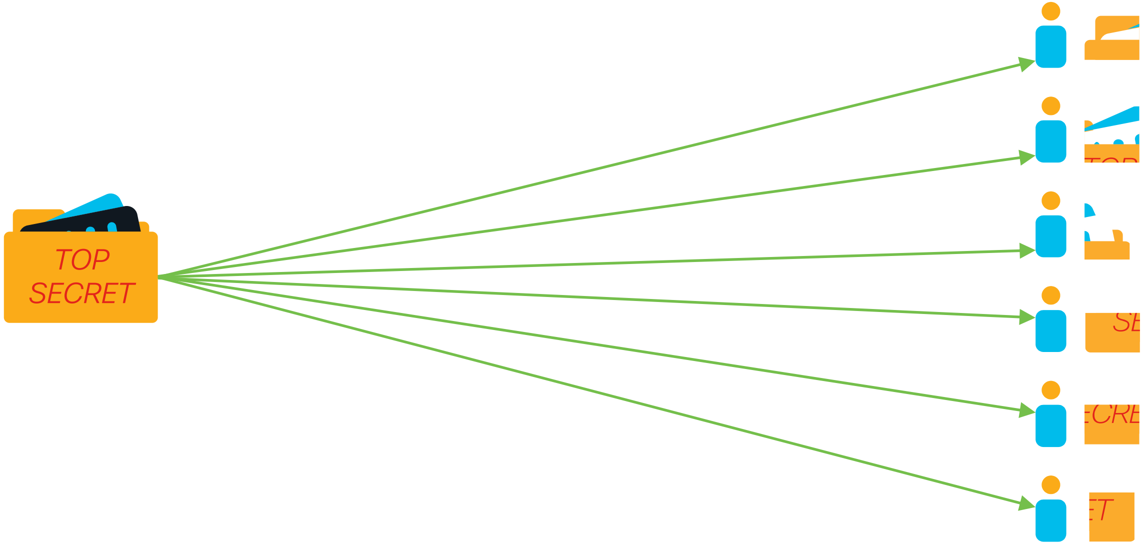


Introducing
Multi-Party Computing



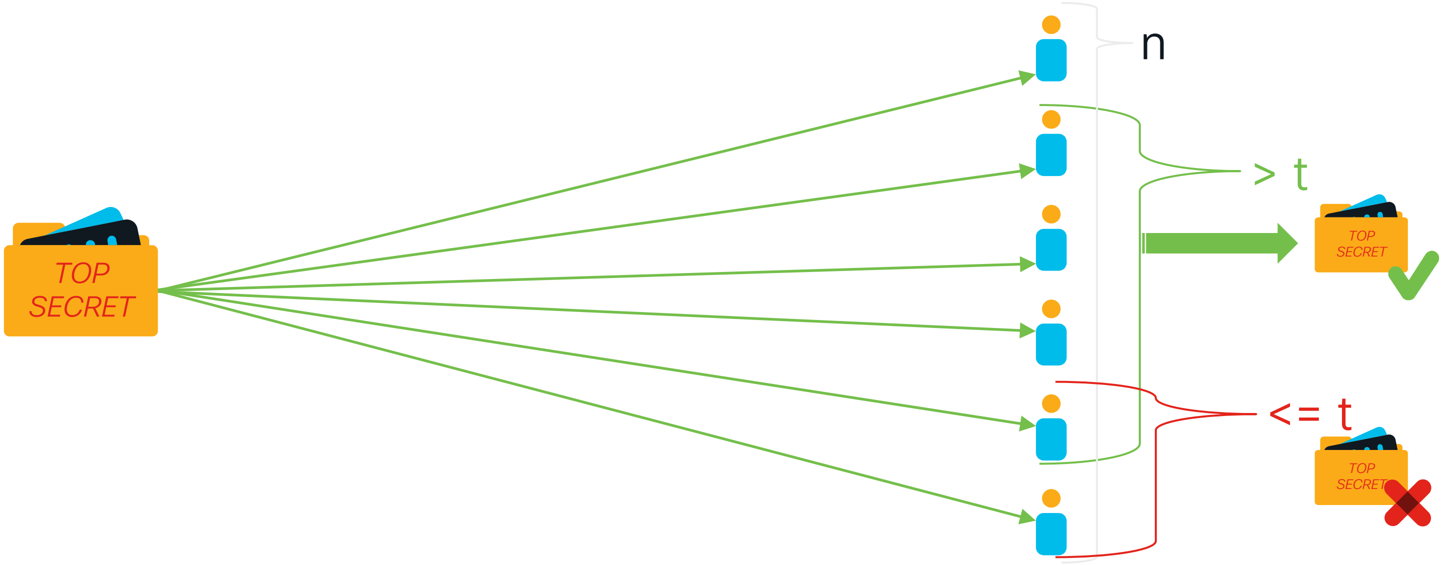
$$(y_1, y_2, \dots, y_n) = f(x_1, x_2, \dots, x_n)$$

An example:
Shamir Secret Sharing (1)

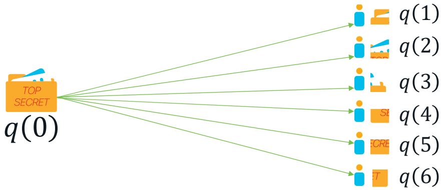


An example:
Shamir Secret Sharing (2)

(t+1)-out-of-n-threshold secret-sharing scheme



An example:
Shamir Secret Sharing (3)

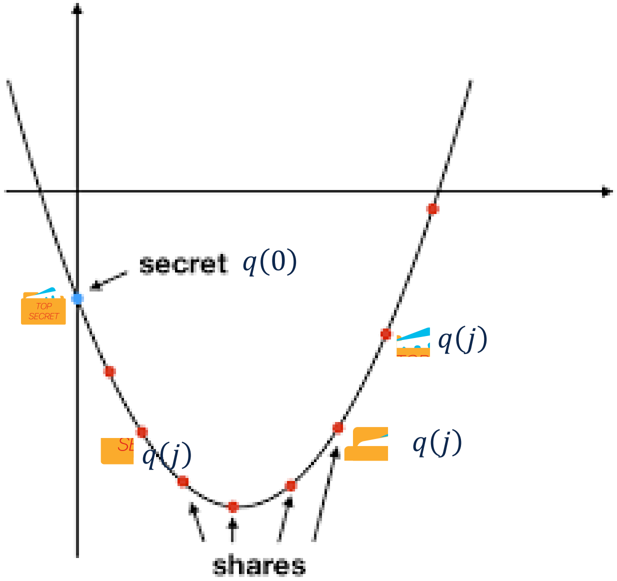


TOP SECRET S: Secret

$$q(0) = s$$

$$q(x) = \sum_{i=1}^{t} a^i x^i + s$$

distribute $q(j): j = 1, \ldots, n$



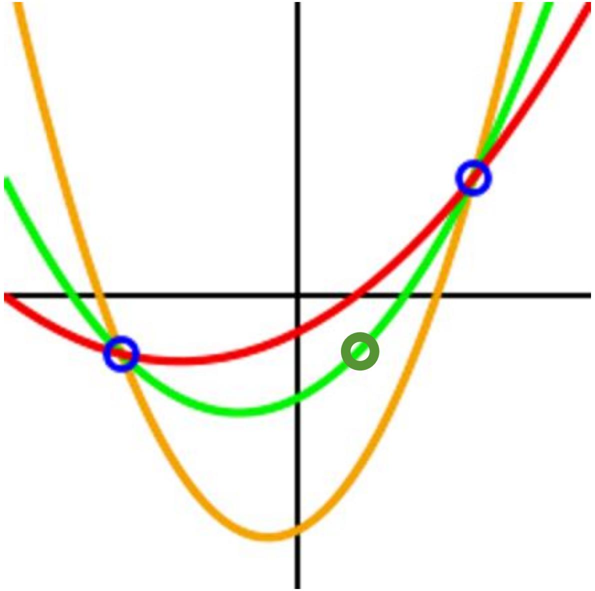
An example:
Shamir Secret Sharing (4)

TOP SECRET S: Secret

$$q(0) = s$$

$$q(x) = \sum_{i=1}^{t} a^{i}\, x^{i} + s$$

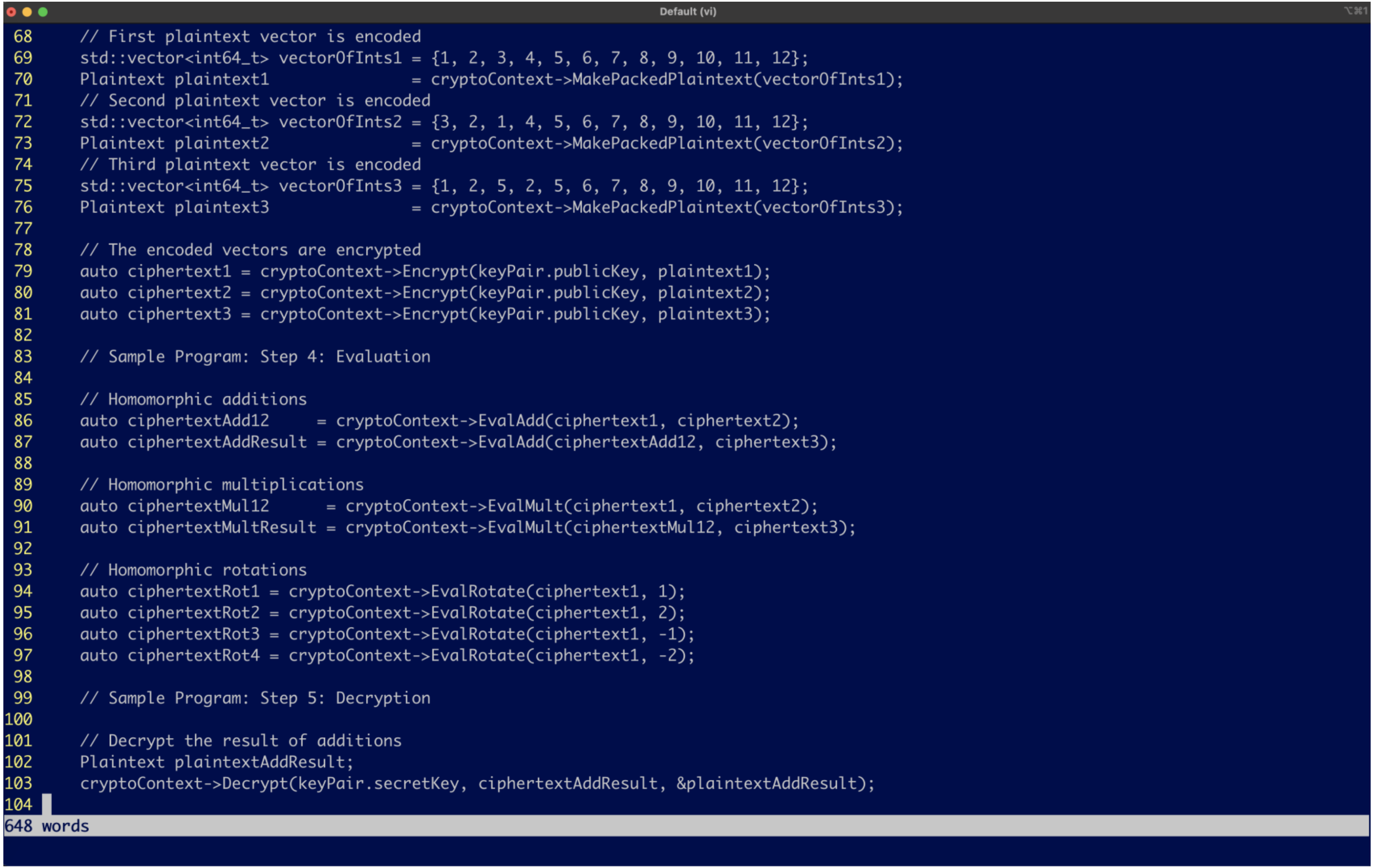
distribute $q(j): j = 1, \ldots, n$



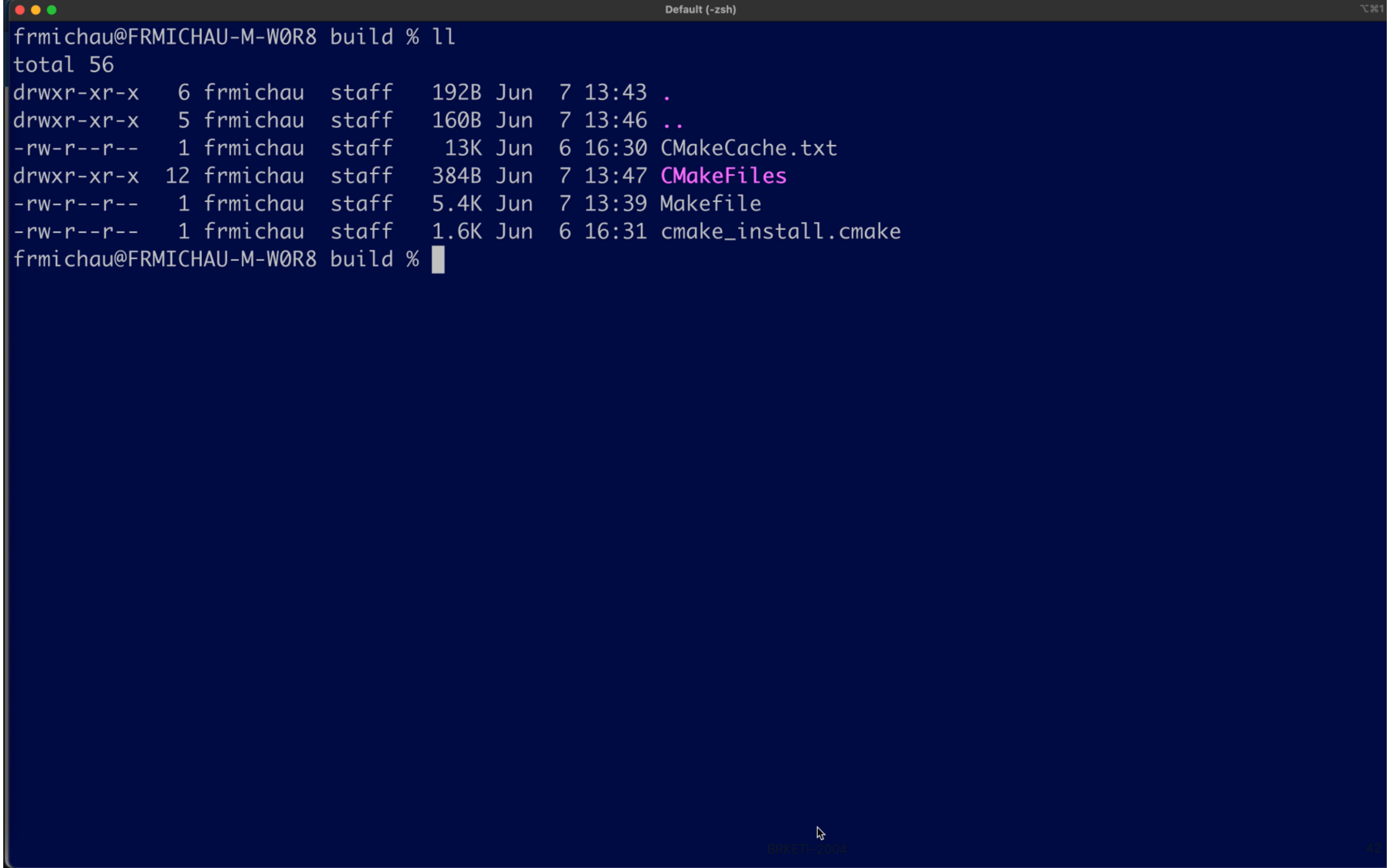
If < t+1
(here 2 ○ dots) → TOP SECRET ✗

If <= t+1
(here 2 ○ dots and ○) → TOP SECRET ✓

Demo with openFHE



```
    // First plaintext vector is encoded
    std::vector<int64_t> vectorOfInts1 = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12};
    Plaintext plaintext1               = cryptoContext->MakePackedPlaintext(vectorOfInts1);
    // Second plaintext vector is encoded
    std::vector<int64_t> vectorOfInts2 = {3, 2, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12};
    Plaintext plaintext2               = cryptoContext->MakePackedPlaintext(vectorOfInts2);
    // Third plaintext vector is encoded
    std::vector<int64_t> vectorOfInts3 = {1, 2, 5, 2, 5, 6, 7, 8, 9, 10, 11, 12};
    Plaintext plaintext3               = cryptoContext->MakePackedPlaintext(vectorOfInts3);

    // The encoded vectors are encrypted
    auto ciphertext1 = cryptoContext->Encrypt(keyPair.publicKey, plaintext1);
    auto ciphertext2 = cryptoContext->Encrypt(keyPair.publicKey, plaintext2);
    auto ciphertext3 = cryptoContext->Encrypt(keyPair.publicKey, plaintext3);

    // Sample Program: Step 4: Evaluation

    // Homomorphic additions
    auto ciphertextAdd12     = cryptoContext->EvalAdd(ciphertext1, ciphertext2);
    auto ciphertextAddResult = cryptoContext->EvalAdd(ciphertextAdd12, ciphertext3);

    // Homomorphic multiplications
    auto ciphertextMul12      = cryptoContext->EvalMult(ciphertext1, ciphertext2);
    auto ciphertextMultResult = cryptoContext->EvalMult(ciphertextMul12, ciphertext3);

    // Homomorphic rotations
    auto ciphertextRot1 = cryptoContext->EvalRotate(ciphertext1, 1);
    auto ciphertextRot2 = cryptoContext->EvalRotate(ciphertext1, 2);
    auto ciphertextRot3 = cryptoContext->EvalRotate(ciphertext1, -1);
    auto ciphertextRot4 = cryptoContext->EvalRotate(ciphertext1, -2);

    // Sample Program: Step 5: Decryption

    // Decrypt the result of additions
    Plaintext plaintextAddResult;
    cryptoContext->Decrypt(keyPair.secretKey, ciphertextAddResult, &plaintextAddResult);

648 words
```



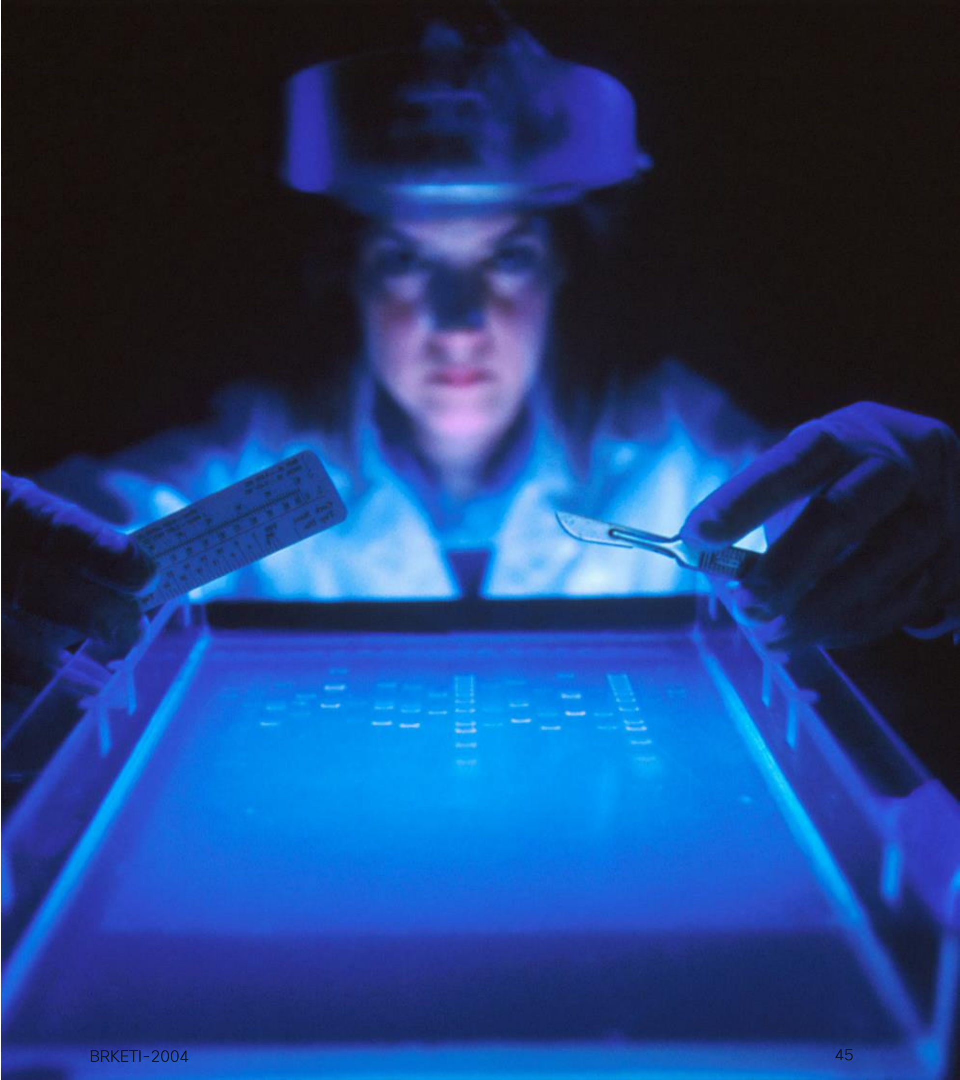
```
frmichau@FRMICHAU-M-W0R8 build % ll
total 56
drwxr-xr-x   6 frmichau  staff   192B Jun  7 13:43 .
drwxr-xr-x   5 frmichau  staff   160B Jun  7 13:46 ..
-rw-r--r--   1 frmichau  staff    13K Jun  6 16:30 CMakeCache.txt
drwxr-xr-x  12 frmichau  staff   384B Jun  7 13:47 CMakeFiles
-rw-r--r--   1 frmichau  staff   5.4K Jun  7 13:39 Makefile
-rw-r--r--   1 frmichau  staff   1.6K Jun  6 16:31 cmake_install.cmake
frmichau@FRMICHAU-M-W0R8 build % 
```

Quantum resistance

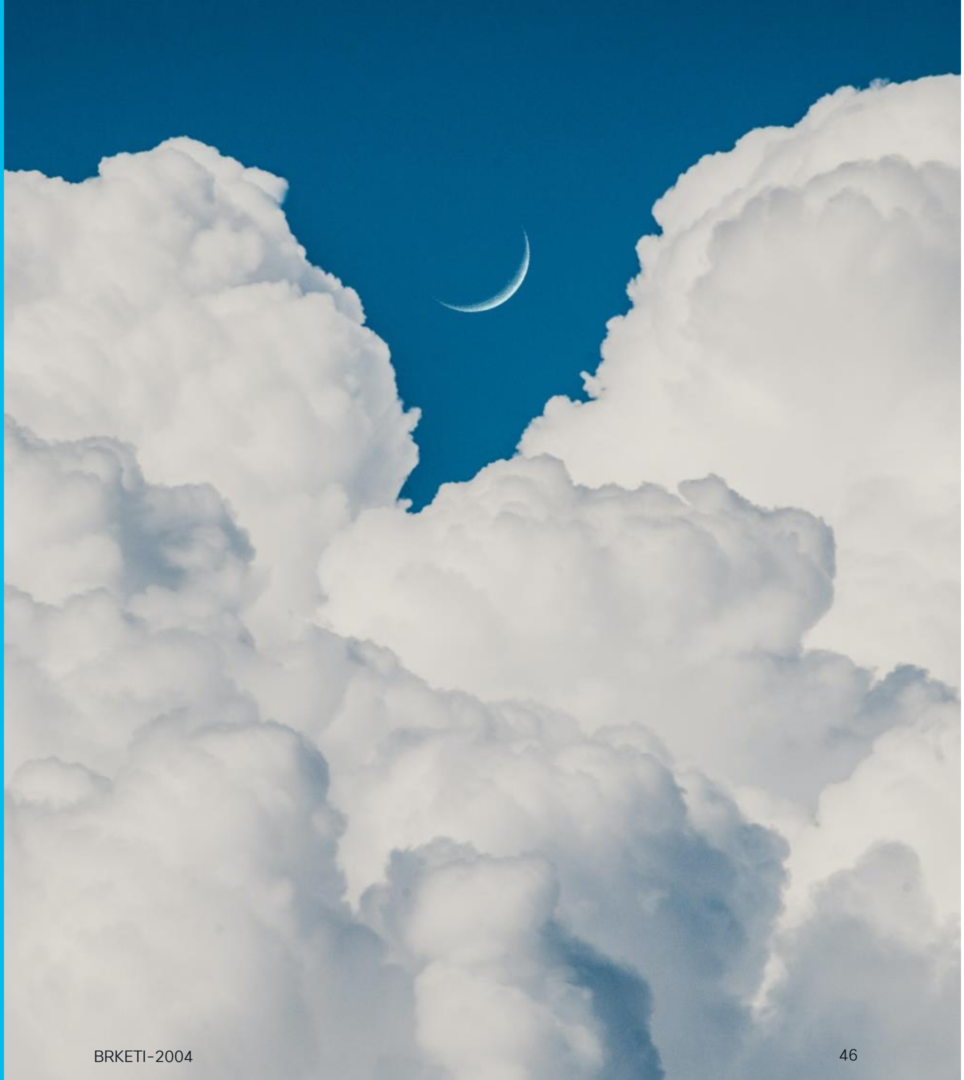
- Depending on specific algo
- FHE supports algorithm based on lattice
- Sharmir Secret Sharing is resistant

Some Use Cases

medical research



privacy-safe cloud outsourcing



Summary and Key Takeaways

Key Takeaways

- World is complex enough
  - Keep things as simple as possible
- New tools are available: FHE and MPC
  - Focus on the needs while keeping privacy and security

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

#CiscoLive

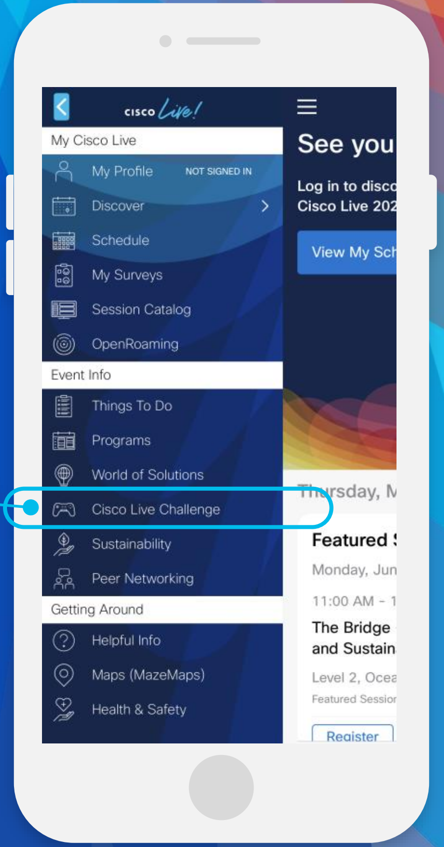
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

cisco Live!

Let's go

#CiscoLive