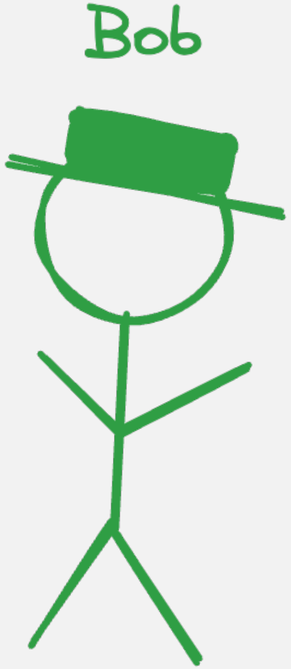
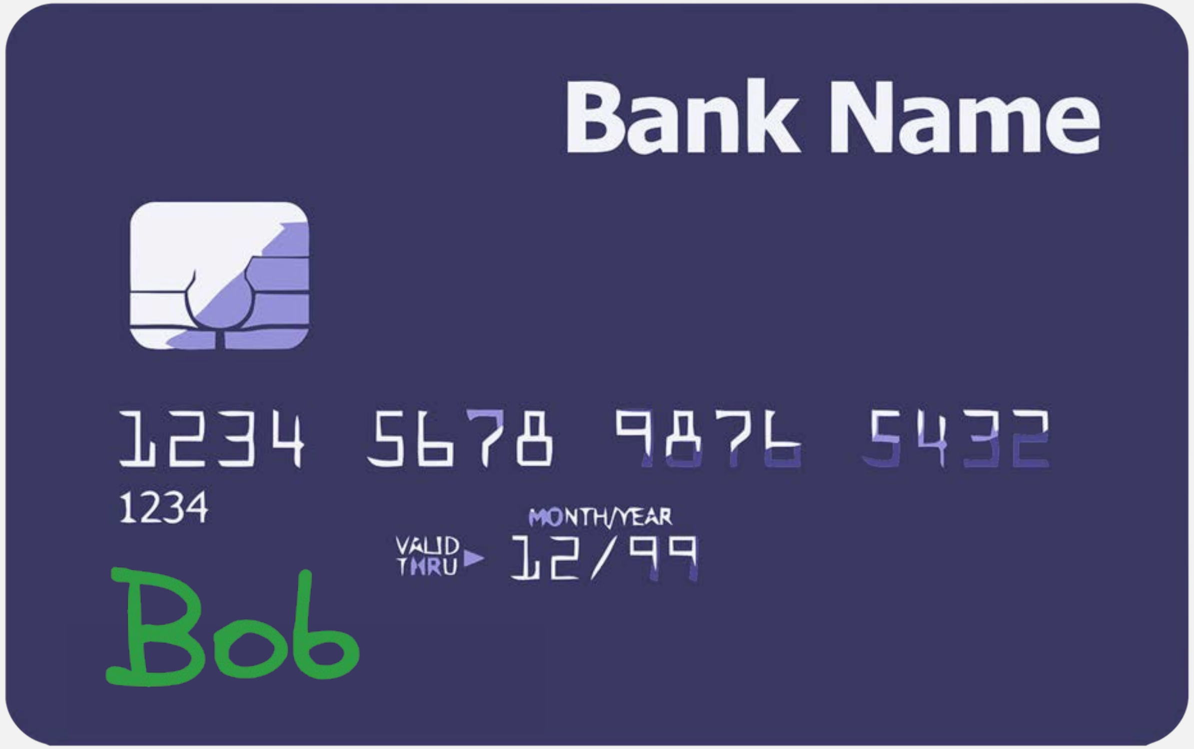
Multi-party computation

Share your data without sharing

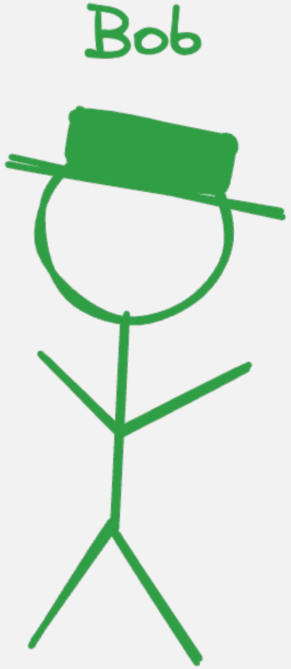
Security and Privacy

Credit card


Bob


Bank Name
1234 5678 9876 5432
1234
MONTH/YEAR
VALID THRU ▸ 12/99
Bob

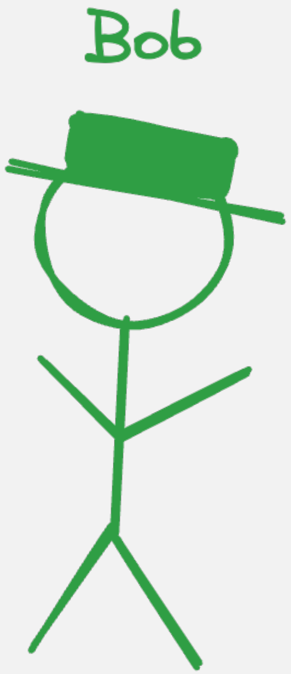
Income

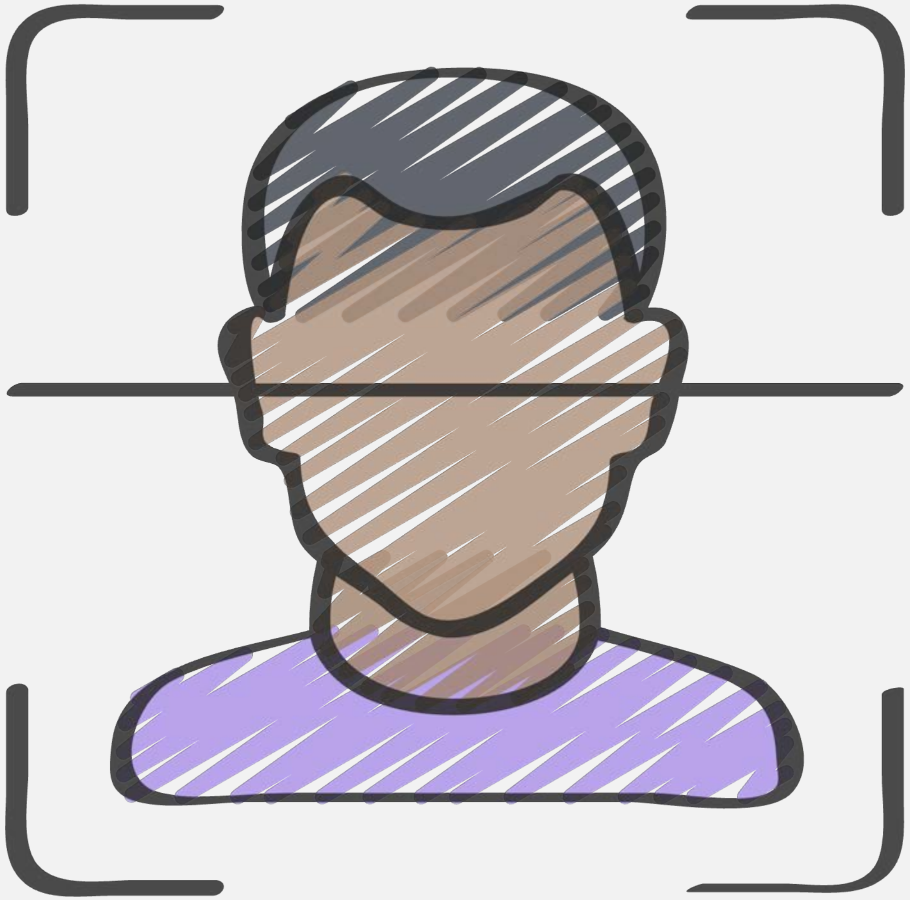


100K $

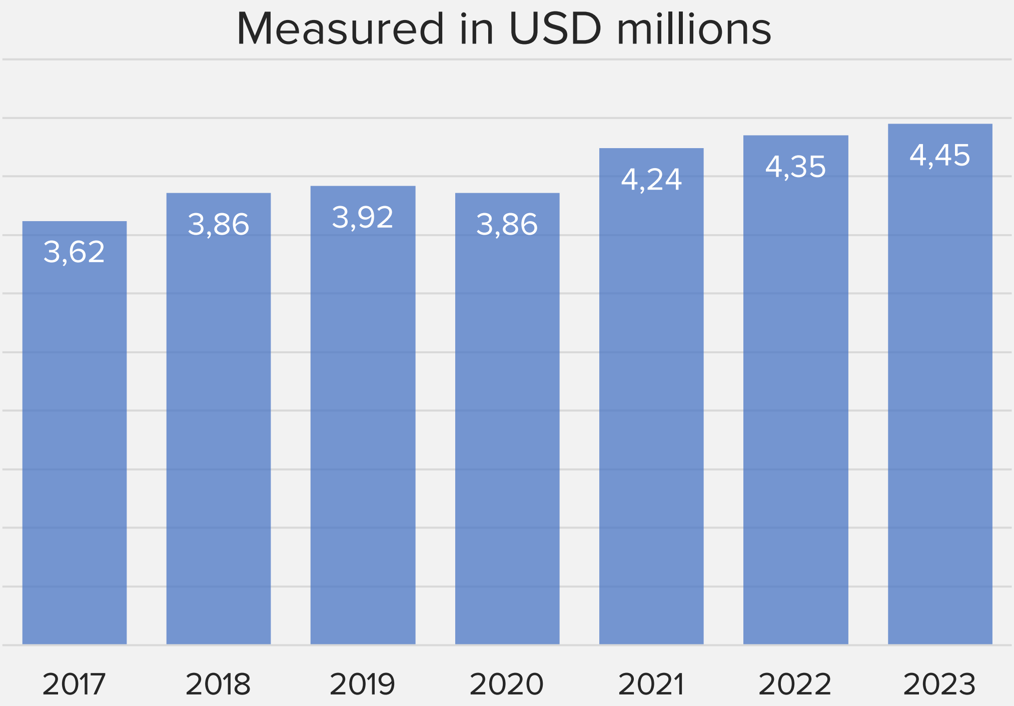
annually

Biometrics

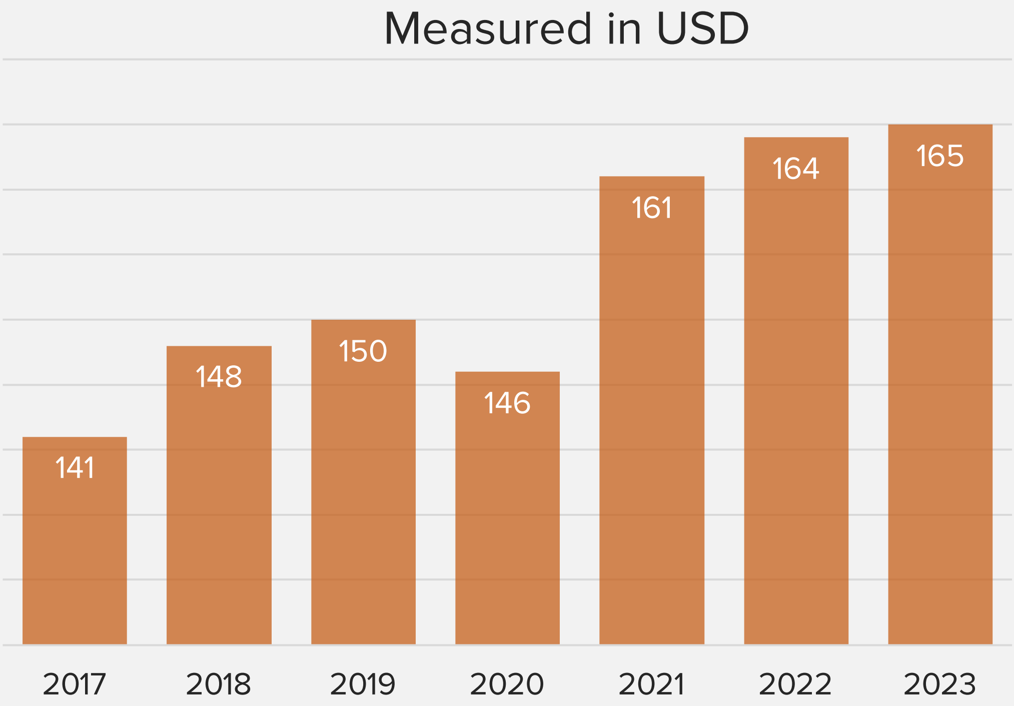




Anxiety



The cost of a data breach

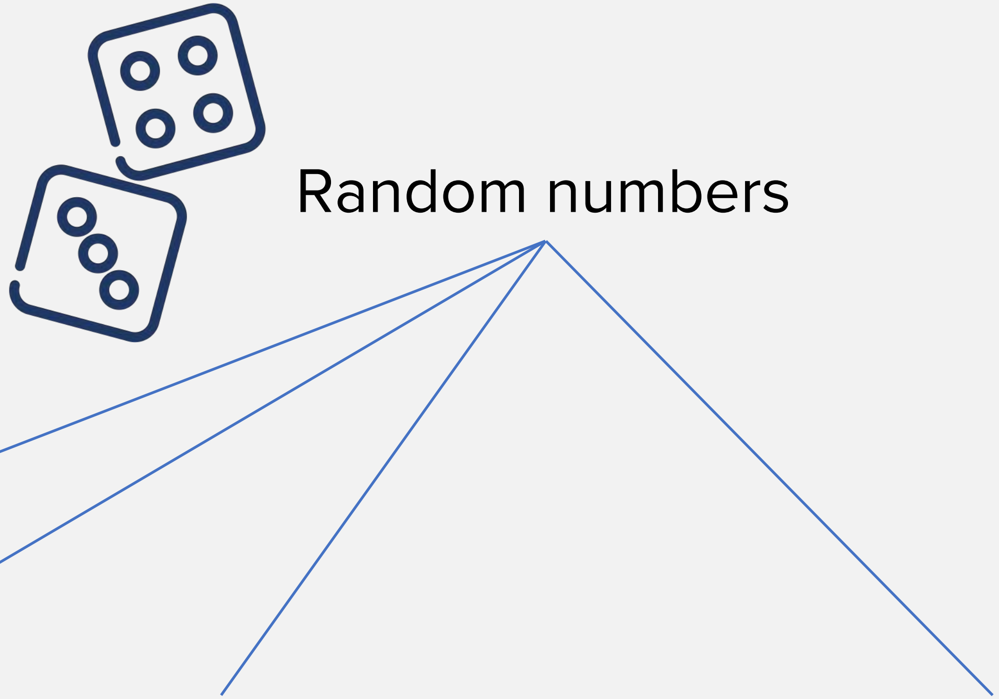


Per-record cost of a data breach

Source: https://www.ibm.com/downloads/cas/E3G5JMBP

MPC in a Nutshell

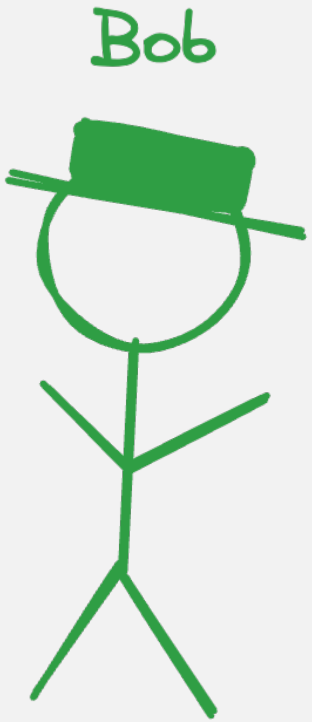
Secret Sharing



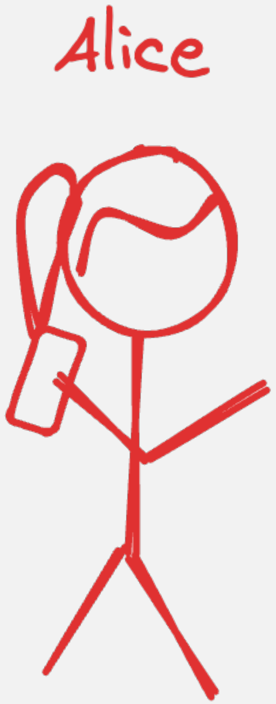
Random numbers

$$x = x_1 + x_2 + x3 + \cdots + x_n$$

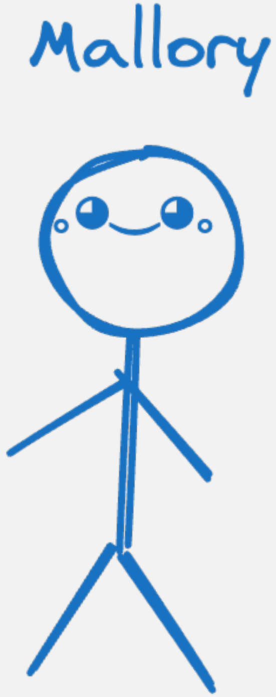
Addition/Subtraction



3

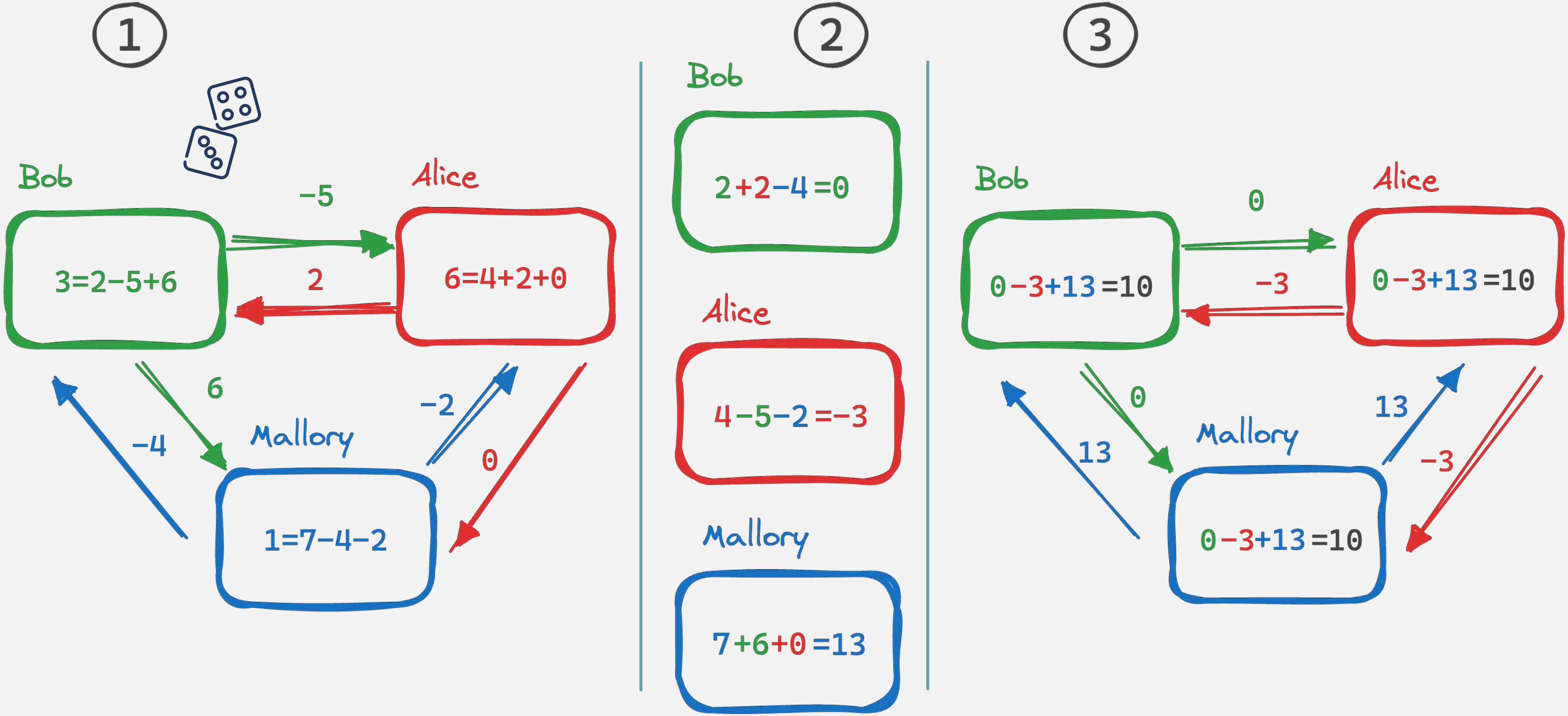


6

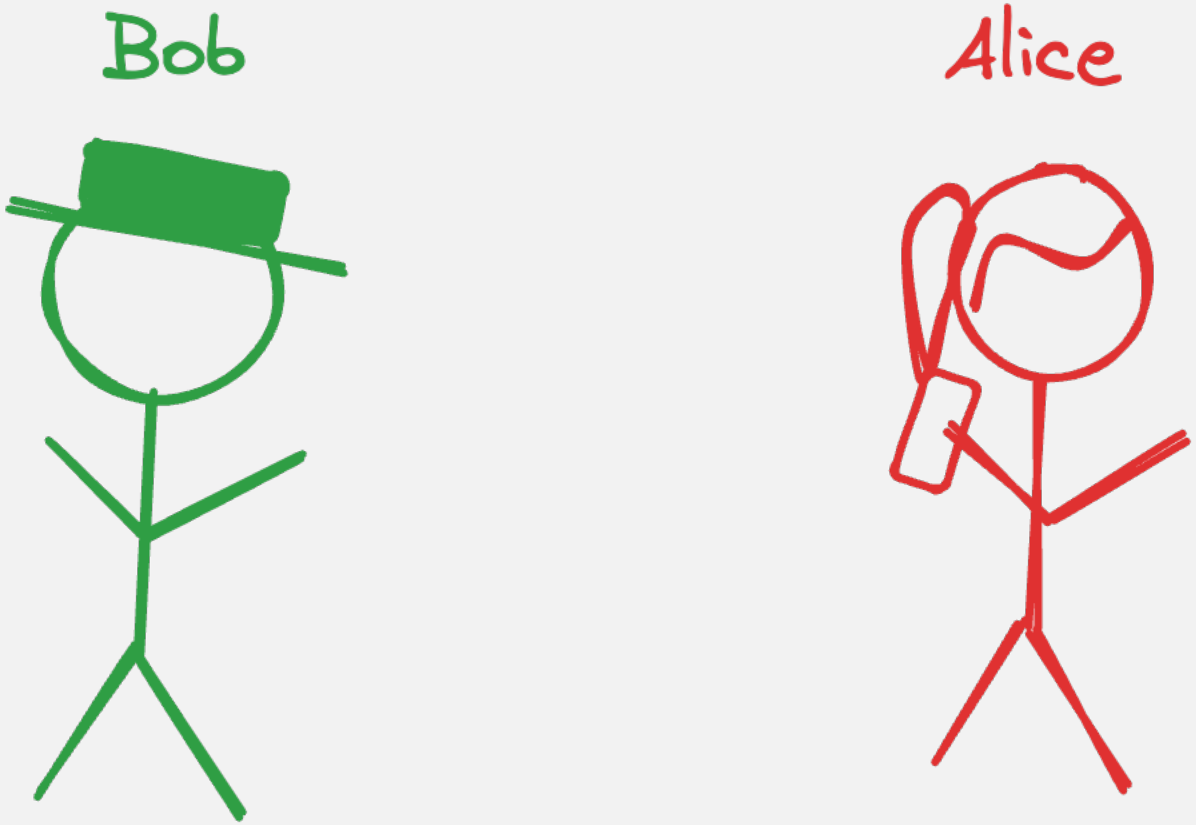


1

Addition/Subtraction



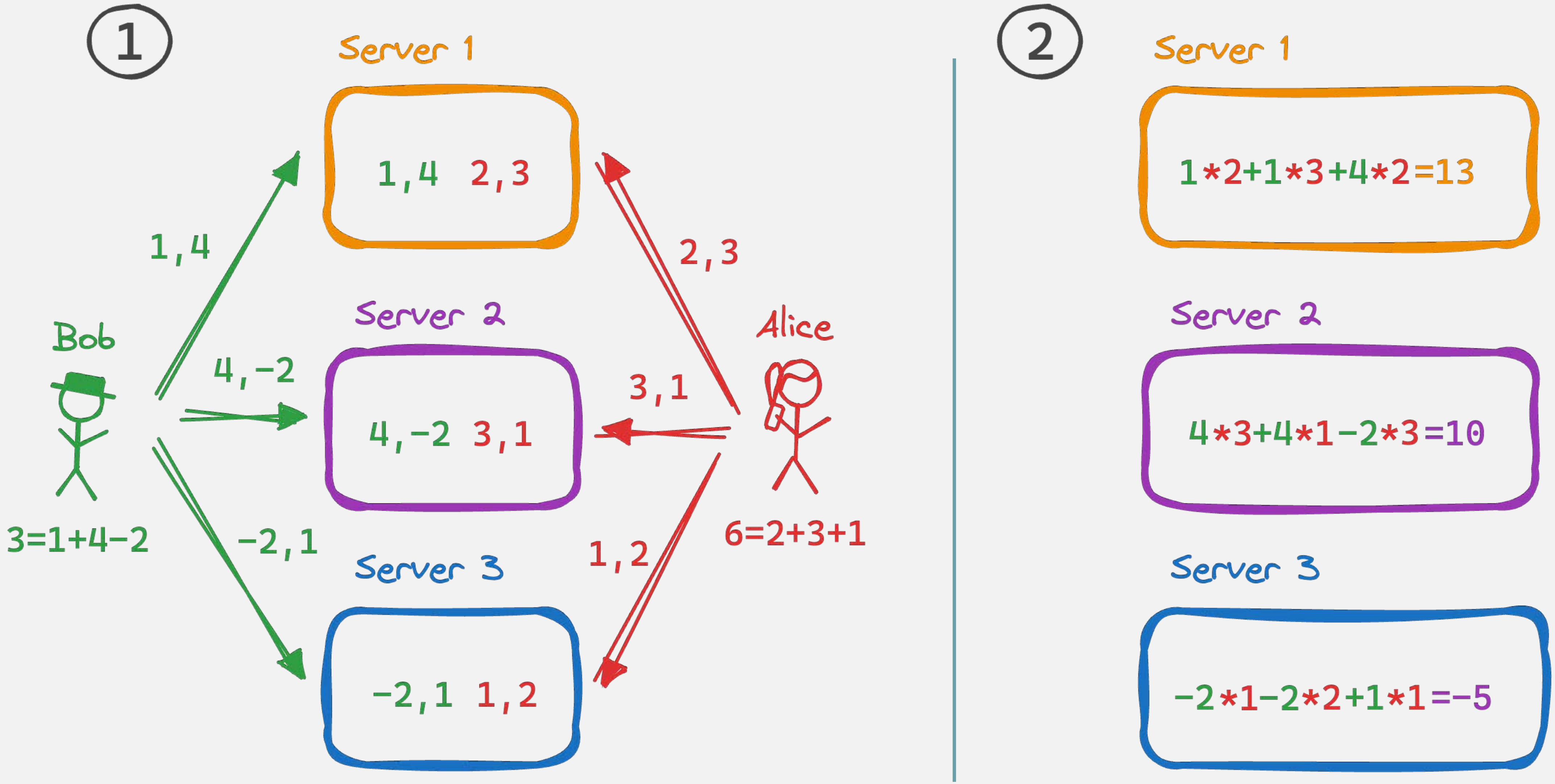
Multiplication



3

6

Multiplication



1,4 2,3

4,-2 3,1

-2,1 1,2

1,4

4,-2

-2,1

2,3

3,1

1,2

3=1+4-2

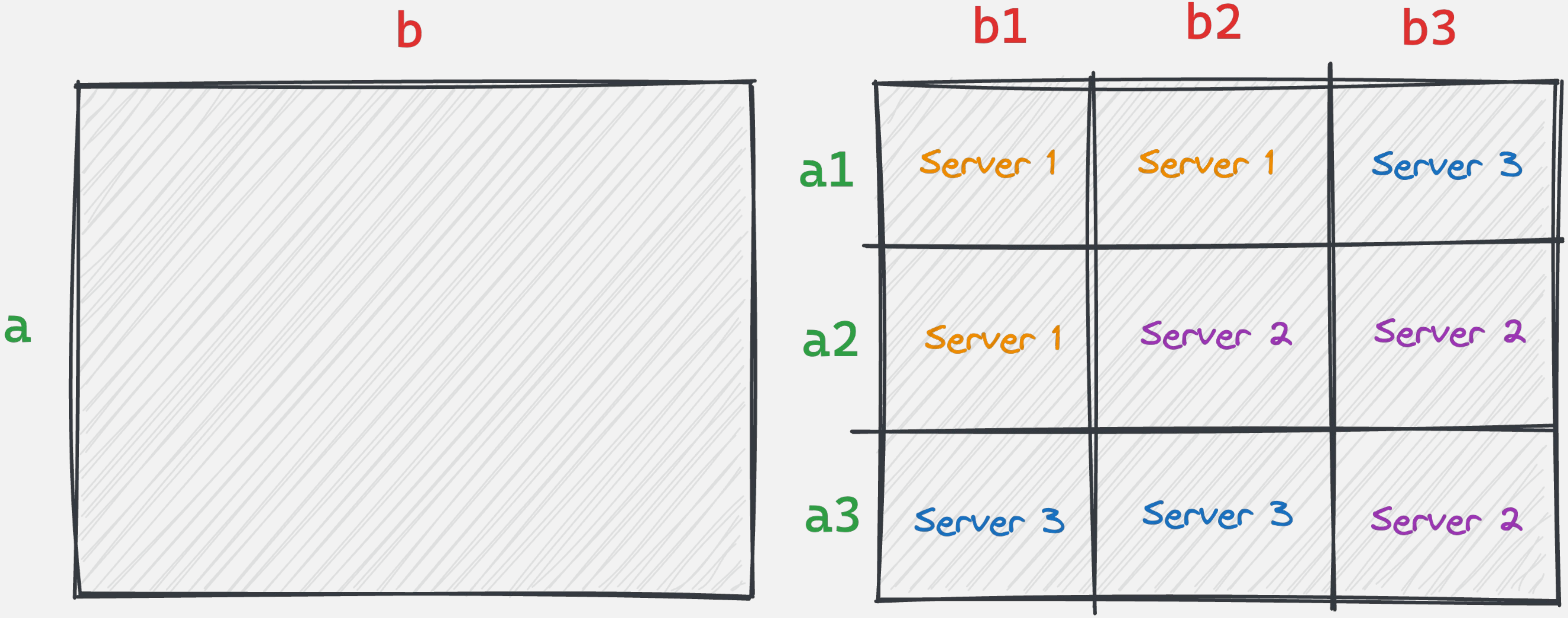
6=2+3+1

1*2+1*3+4*2=13

4*3+4*1-2*3=10

-2*1-2*2+1*1=-5

Multiplication

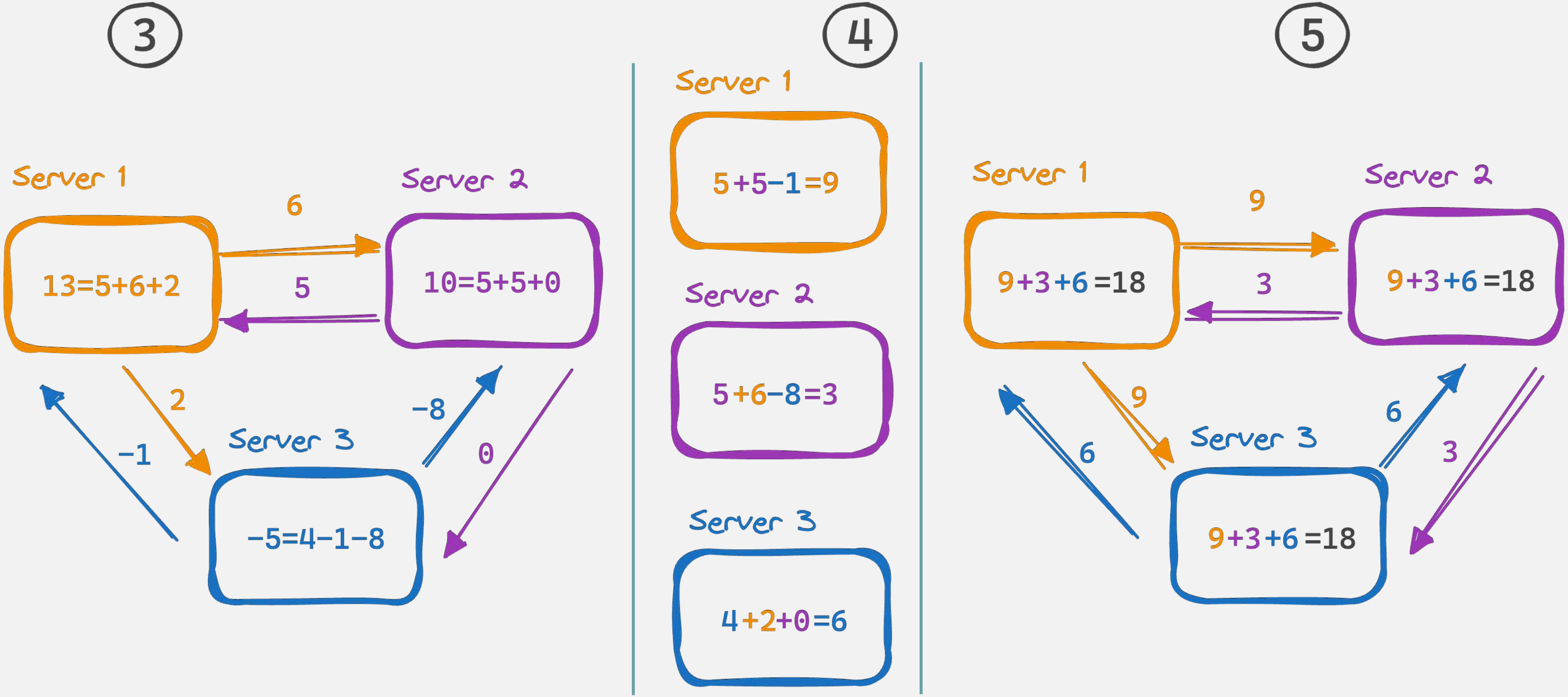


	b1	b2	b3
a1	Server 1	Server 1	Server 3
a2	Server 1	Server 2	Server 2
a3	Server 3	Server 3	Server 2

Multiplication

	b1	b2	b3
a1	Server 1 Server 3	Server 1	Server 3
a2	Server 1	Server 1 Server 2	Server 2
a3	Server 3	Server 2	Server 3 Server 2

Multiplication



3

Server 1

13=5+6+2

Server 2

10=5+5+0

Server 3

−5=4−1−8

4

Server 1

5+5−1=9

Server 2

5+6−8=3

Server 3

4+2+0=6

5

Server 1

9+3+6=18

Server 2

9+3+6=18

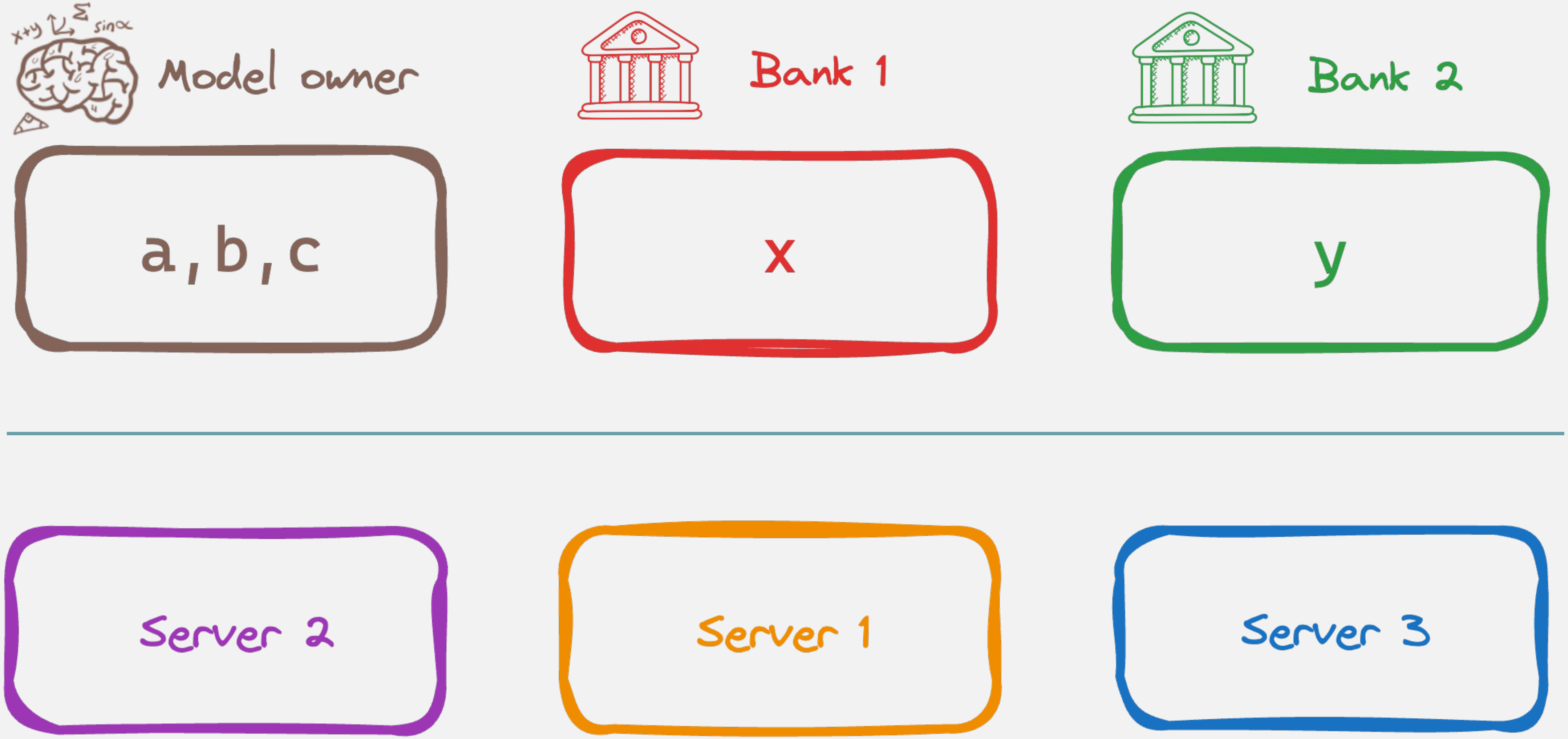
Server 3

9+3+6=18

Linear Regression

$$y = ax + by + c$$

Real (*almost*) case



Model owner

a, b, c

Bank 1

x

Bank 2

y

Server 2

Server 1

Server 3

Drawbacks

Higher costs

Communication overhead

Complexity

Computing overhead

Closing thoughts

Security Consideration

1. Randomness (don’t use import random)
2. Modular arithmetic (we need “endless” numbers)
3. Risk of maliciousness (honest but curious)
4. Risk of collusion (trust but check)

Playground

CrypTen

https://github.com/facebookresearch/CrypTen

Conclusions

1. Promotes privacy and data utility;
2. Reveals only the final result (unlike Federated Learning);
3. Less resource-intensive than other methods (e.g. Homomorphic encryption);
4. More practical than other methods (e.g. differential privacy);
5. More independent than hardware methods (e.g. Intel SGX);

Thank You!

Peter Emelianov, Bloomtech

https://www.linkedin.com/in/emelianovpeter/