Efficient Multiparty Protocols Using Generalised Parseval's Identity and the Theta Algebra

Giorgio Sonnino & Alberto Sonnino

MMCTSE 2022

Multi-Party Computation

Compute $E(a_1, a_2, a_3, \ldots, a_k)$

User 1

Secret: a_1

User 1

Secret: a_2

User 3

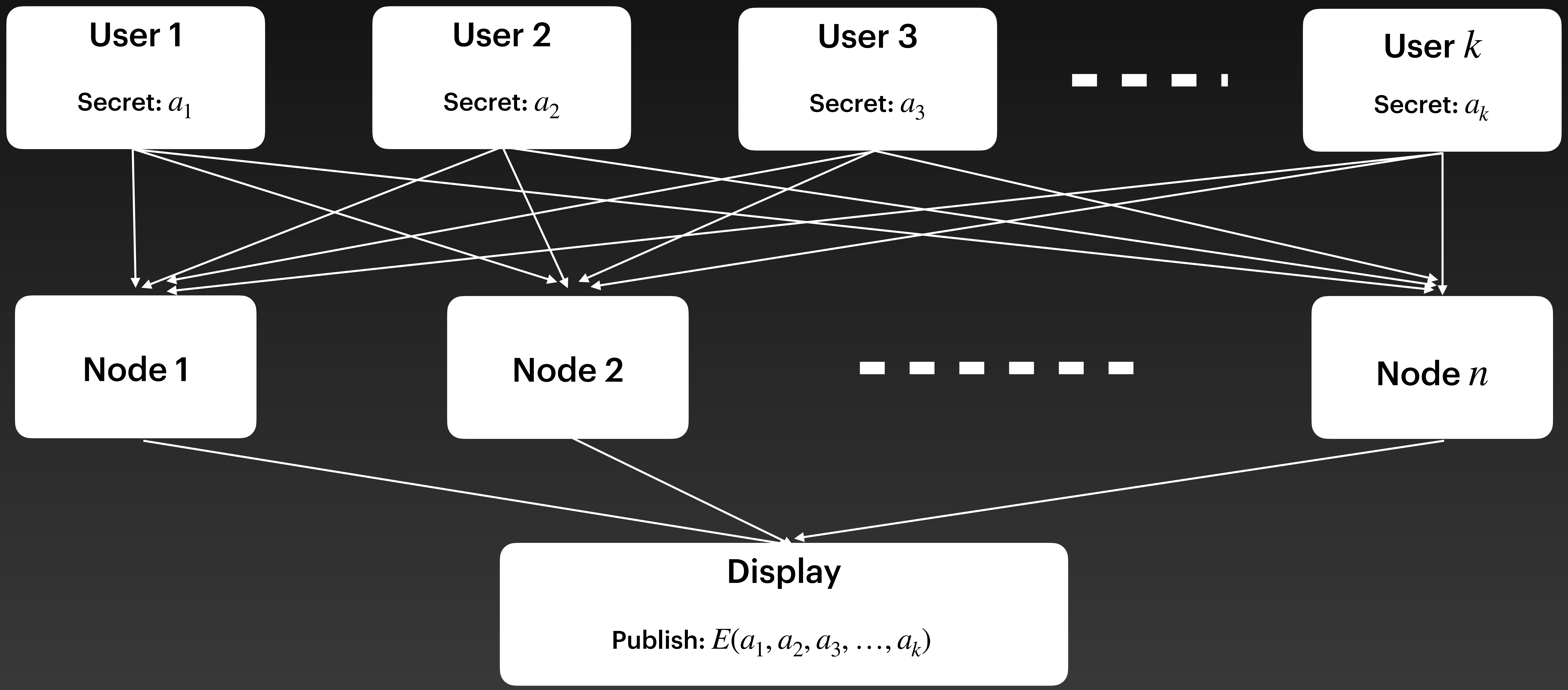
Secret: a_3

User k

Secret: a_k

Multi-Party Computation

Compute $E(a_1, a_2, a_3, \ldots, a_k)$

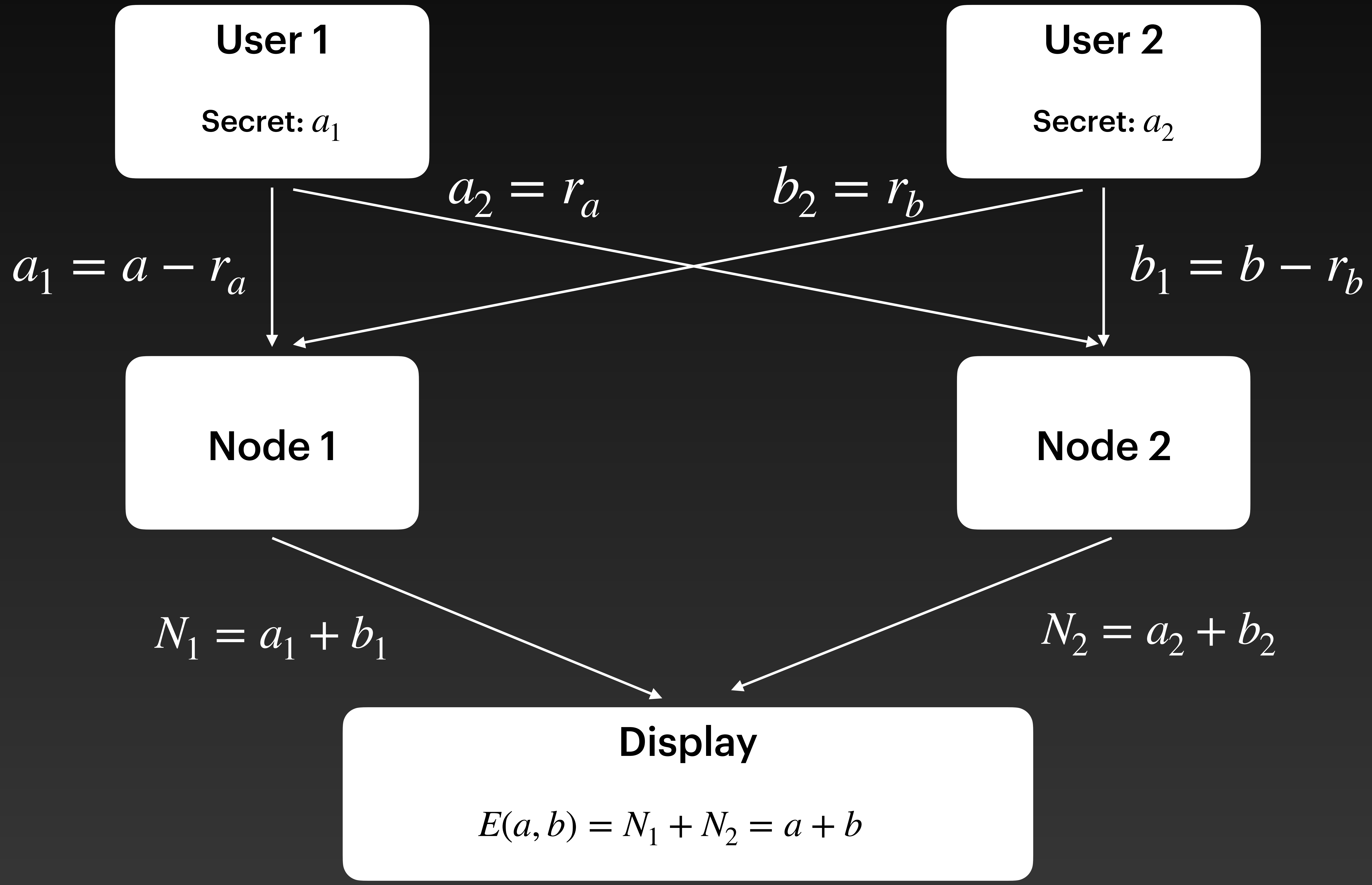


Multi-Party Computation

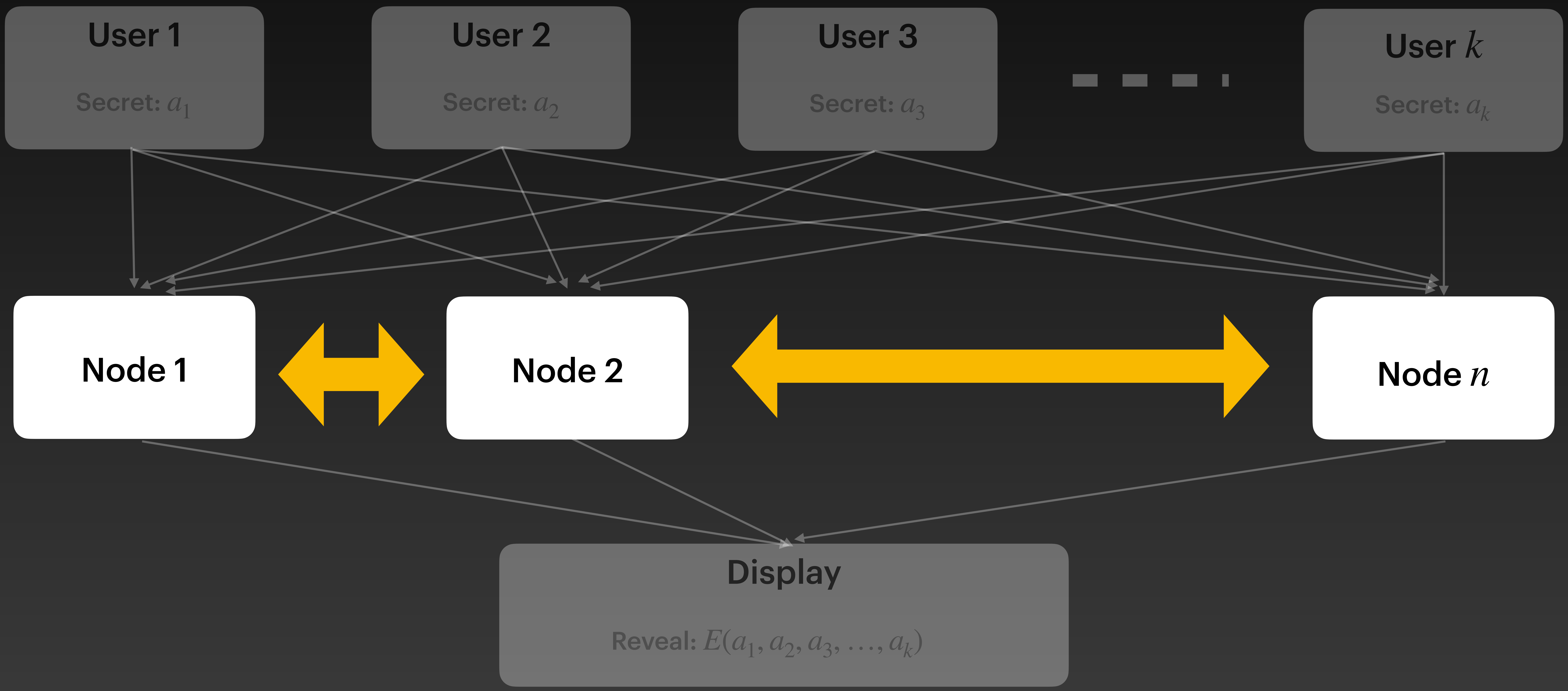
Compute $E(a_1, a_2, a_3, \ldots, a_k)$

- Only the user know its own secret
- Only the final expression E is public (no intermediary values)
- Despite a subset of (corrupted) nodes collude

Addition of Secrets

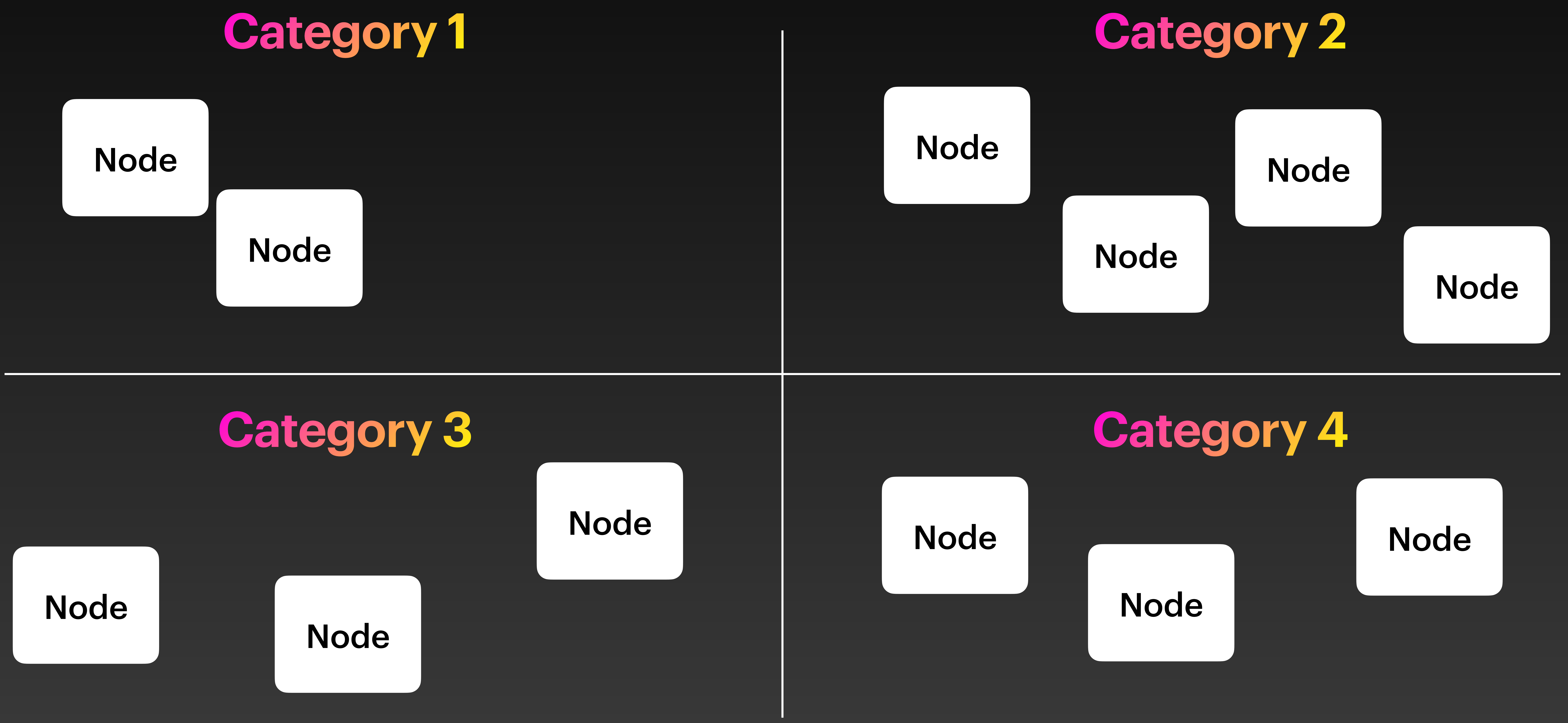


Addition & Multiplication



Trust Assumptions

At least one honest node from 3 categories



Example Computation

Alice

$$E \equiv x_1 a + x_2 b + yab$$

Alice
Secret: *a*

Bob
Secret: *b*

Node 1

Node 2

Node 3

Node 4

Example Computation

Alice

Secret: *a*

Compute: $A_1^{(1)}$; $A_1^{(2)}$; $B_1^{(1)}$; $B_1^{(2)}$

- Public: $f(x) = (1 + \sin(2\pi\tau)/(2\pi\tau))^{-1/2}\cos(\pi\tau x/L)$
- Break: $x_1 a = a_1 + a_2 + a_3 + a_4$
- Pick: $\omega_{1,m} = a_{1,m} + ib_{1,m}$ and $\omega_1^{(0)} = a_1^{(0)} + ib_1^{(0)}$
- Define: $(\alpha^{(0)}, \alpha_m)$ as the cosine component of $f(x)$
- Define: $(\alpha_1^{(0)}, \alpha_{1,m}) \equiv (|y|^{1/2} a\alpha^{(0)}, |y|^{1/2} a\alpha_m)$

Example Computation

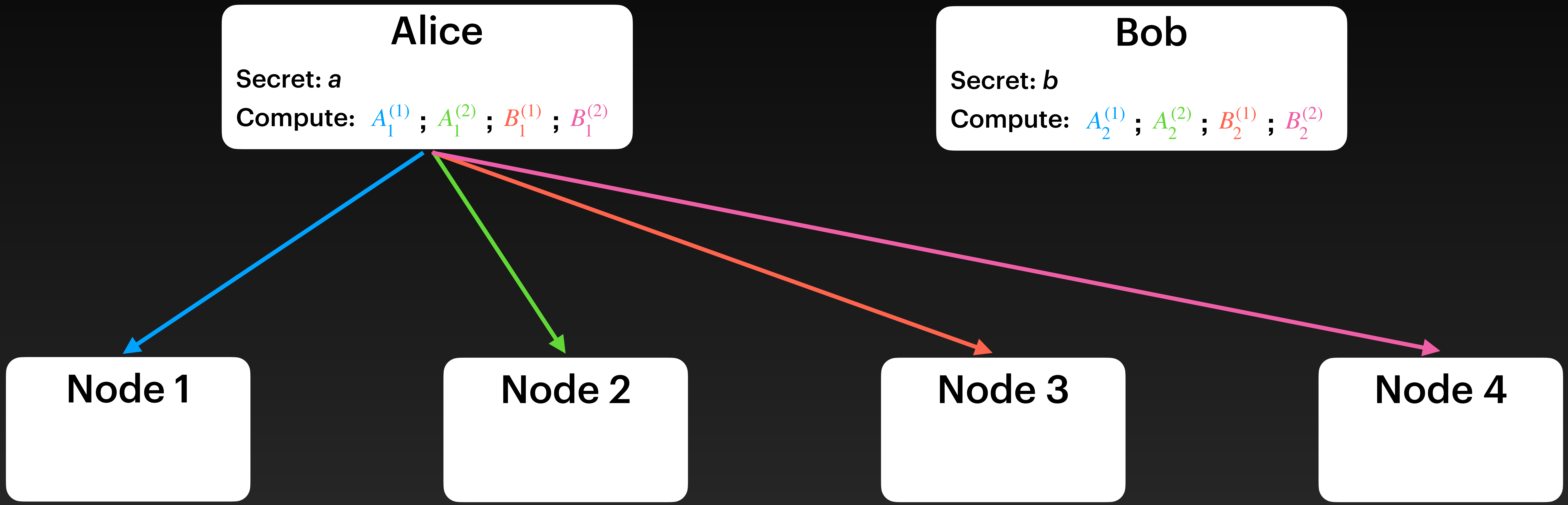
Alice

Secret: *a*

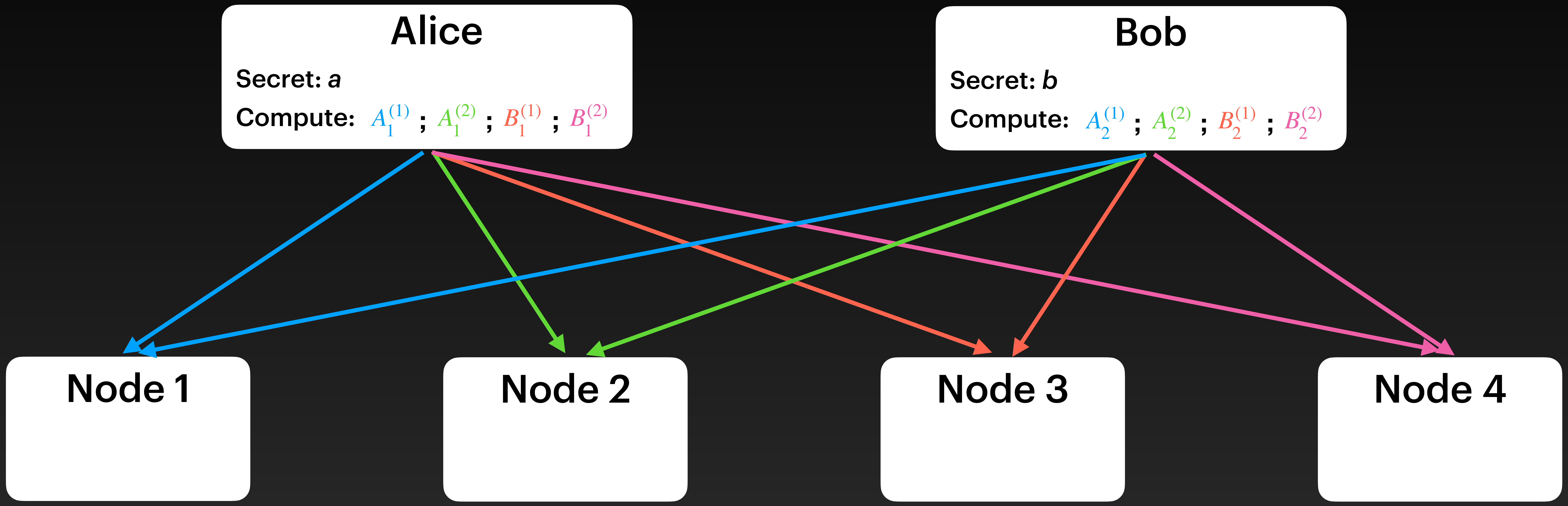
Compute: $A_1^{(1)}$; $A_1^{(2)}$; $B_1^{(1)}$; $B_1^{(2)}$

- Compute: $A_1^{(1)} = \{a_1, \alpha_1^{(0)} + \omega_1^{(0)}, \alpha_{1,m} + \omega_{1,m}\}$
- Compute: $A_1^{(2)} = \{a_2, \alpha_1^{(0)} - \omega_1^{(0)}, \alpha_{1,m} - \omega_{1,m}\}$
- Compute: $B_1^{(1)} = \{a_3, \alpha_1^{(0)} + i\omega_1^{(0)}, \alpha_{1,m} + i\omega_{1,m}\}$
- Compute: $B_1^{(2)} = \{a_4, \alpha_1^{(0)} - i\omega_1^{(0)}, \alpha_{1,m} - i\omega_{1,m}\}$

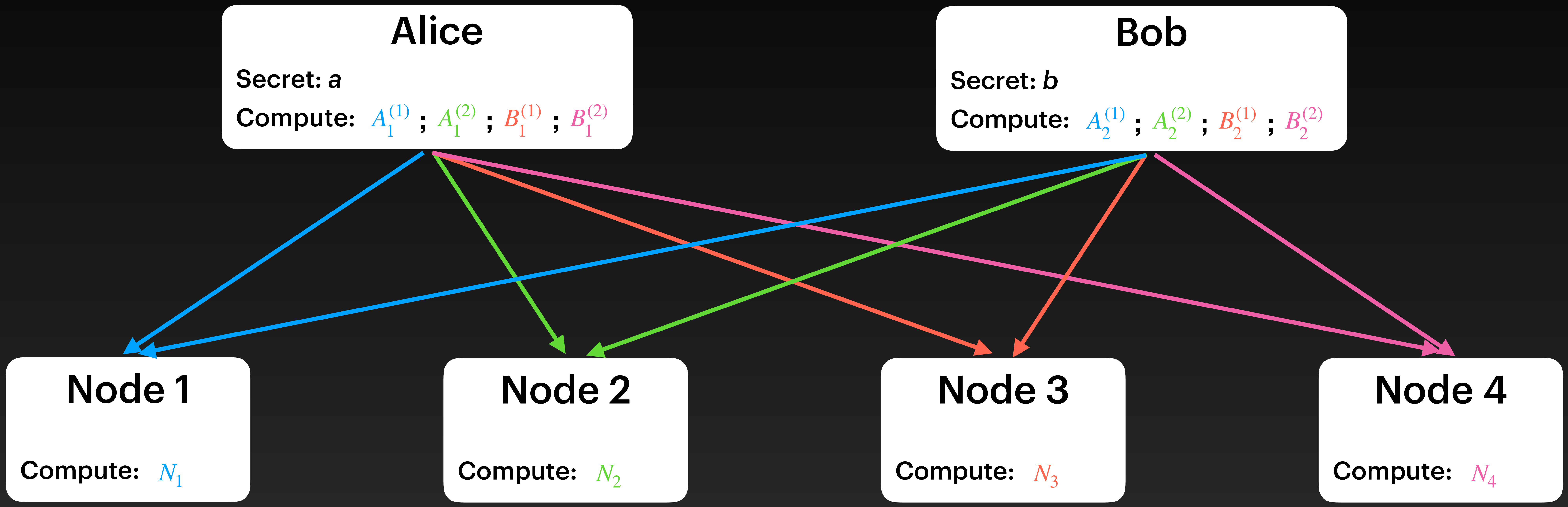
Example Computation



Example Computation



Example Computation



Example Computation

Node 1

Compute: N_1

Node 2

Compute: N_2

Node 3

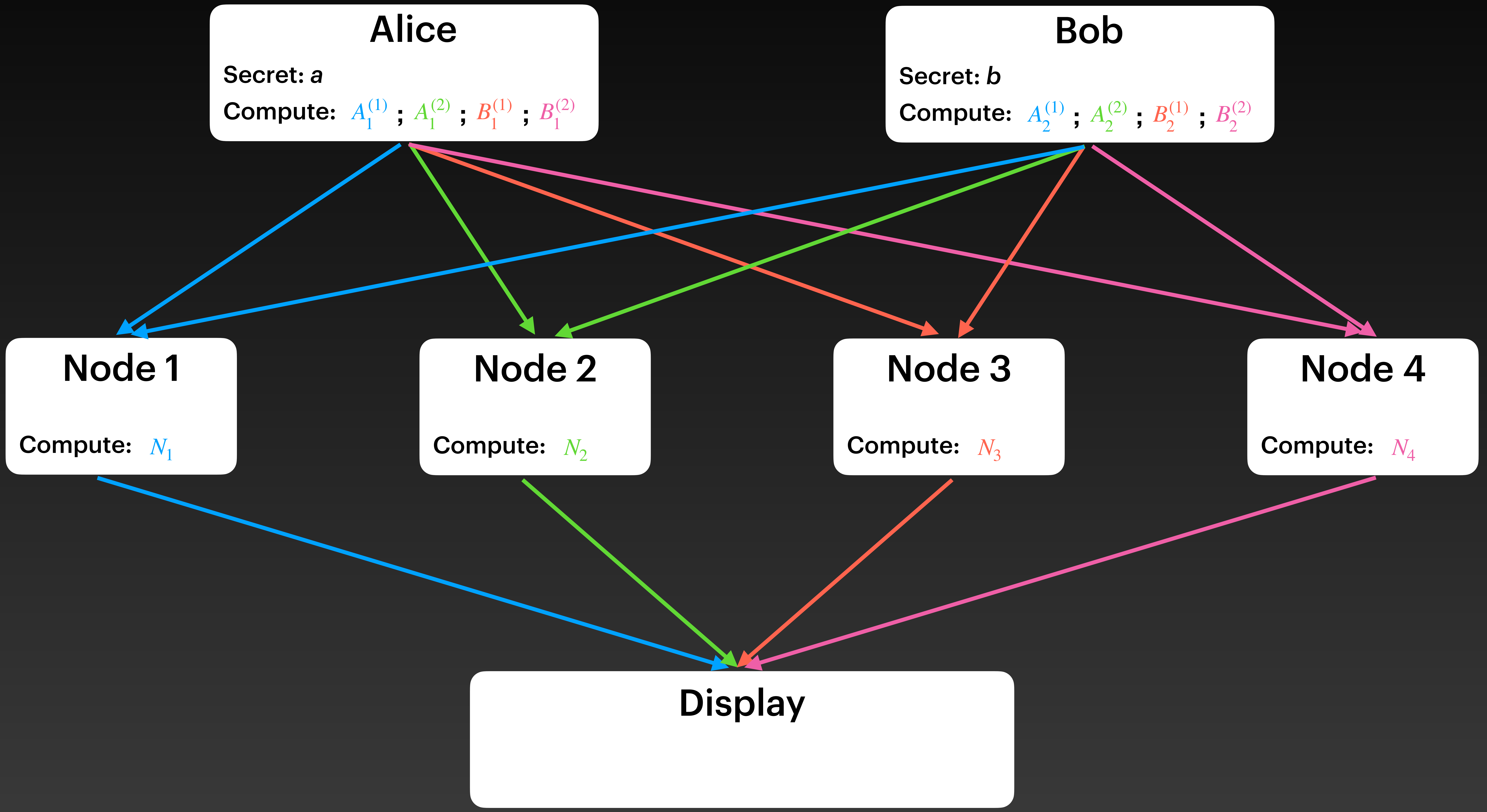
Compute: N_3

Node 4

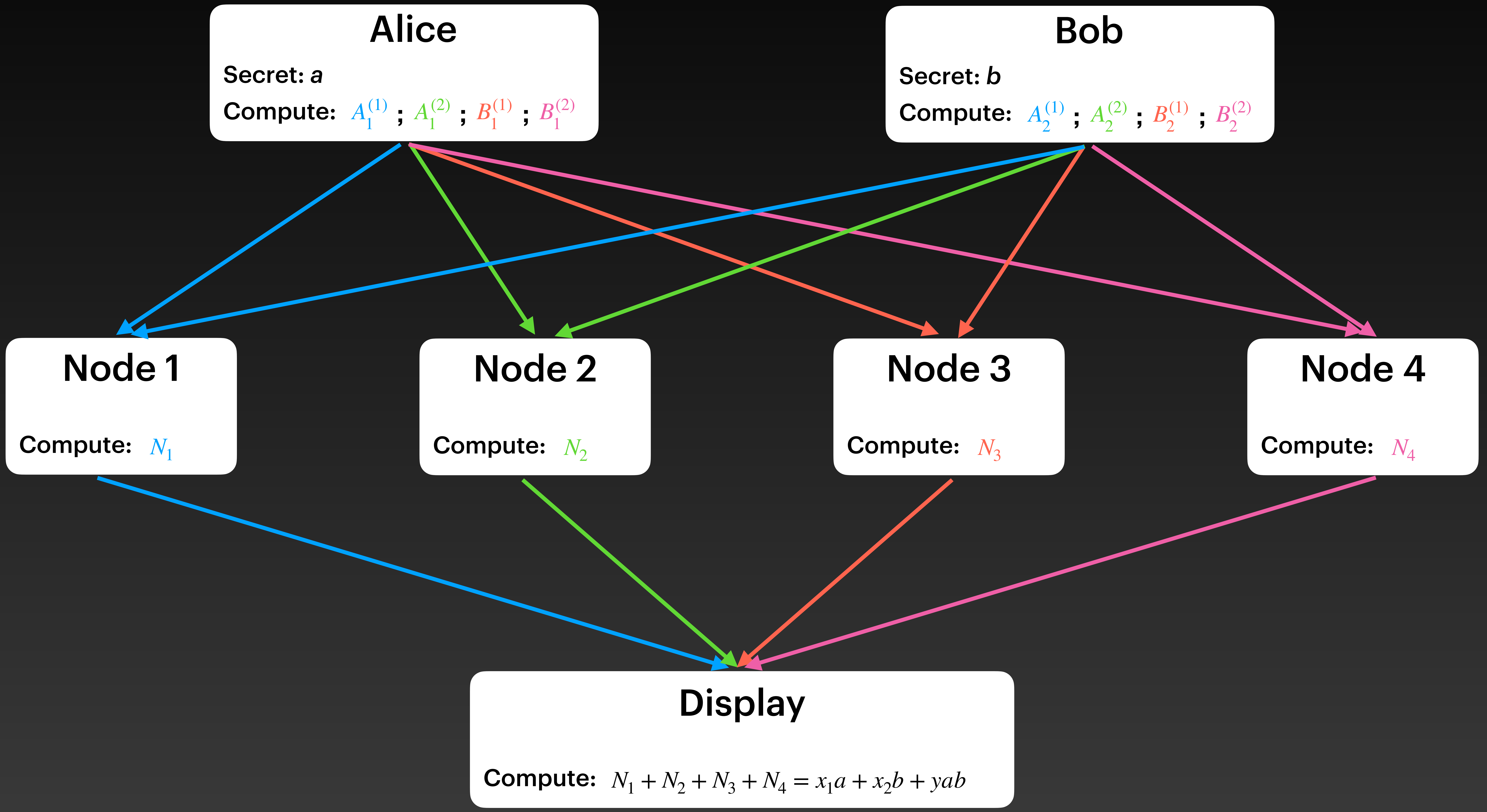
Compute: N_4

- $N_1 = a_1 + b_1 \pm \left(\frac{1}{8}(\alpha_1^{(0)} + \omega_1^{(0)})(\alpha_2^{(0)} + \omega_2^{(0)}) + \frac{1}{4}\sum_{m=1}^{\infty}(\alpha_{1,m} + \omega_{1,m})(\alpha_{2,m} + \omega_{2,m})\right)$
- $N_2 = a_2 + b_2 \pm \left(\frac{1}{8}((\alpha_1^{(0)} - \omega_1^{(0)})(\alpha_2^{(0)} - \omega_2^{(0)})) + \frac{1}{4}\sum_{m=1}^{\infty}((\alpha_{1,m} - \omega_{1,m})(\alpha_{2,m} - \omega_{2,m}))\right)$
- $N_3 = a_3 + b_3 \pm \left(\frac{1}{8}((\alpha_1^{(0)} + i\omega_1^{(0)})(\alpha_2^{(0)} + i\omega_2^{(0)})) + \frac{1}{4}\sum_{m=1}^{\infty}((\alpha_{1,m} + i\omega_{1,m})(\alpha_{2,m} + i\omega_{2,m}))\right)$
- $N_4 = a_4 + b_4 \pm \left(\frac{1}{8}((\alpha_1^{(0)} - i\omega_1^{(0)})(\alpha_2^{(0)} - i\omega_2^{(0)})) + \frac{1}{4}\sum_{m=1}^{\infty}((\alpha_{1,m} - i\omega_{1,m})(\alpha_{2,m} - i\omega_{2,m}))\right)$

Example Computation



Example Computation



Main Ingredients

Generalised Parseval's Identity

- Apply to n functions
- Apply convolution in a "tree"

Novel Definition of Theta's Algebra

- Algebra of complex numbers not working
- Require:

$$-1 = \zeta^{(2)} = \zeta^{(4)} = \zeta^{(6)} = \ldots$$
$$+i = \zeta^{(1)} = \zeta^{(3)} = \zeta^{(5)} = \ldots$$

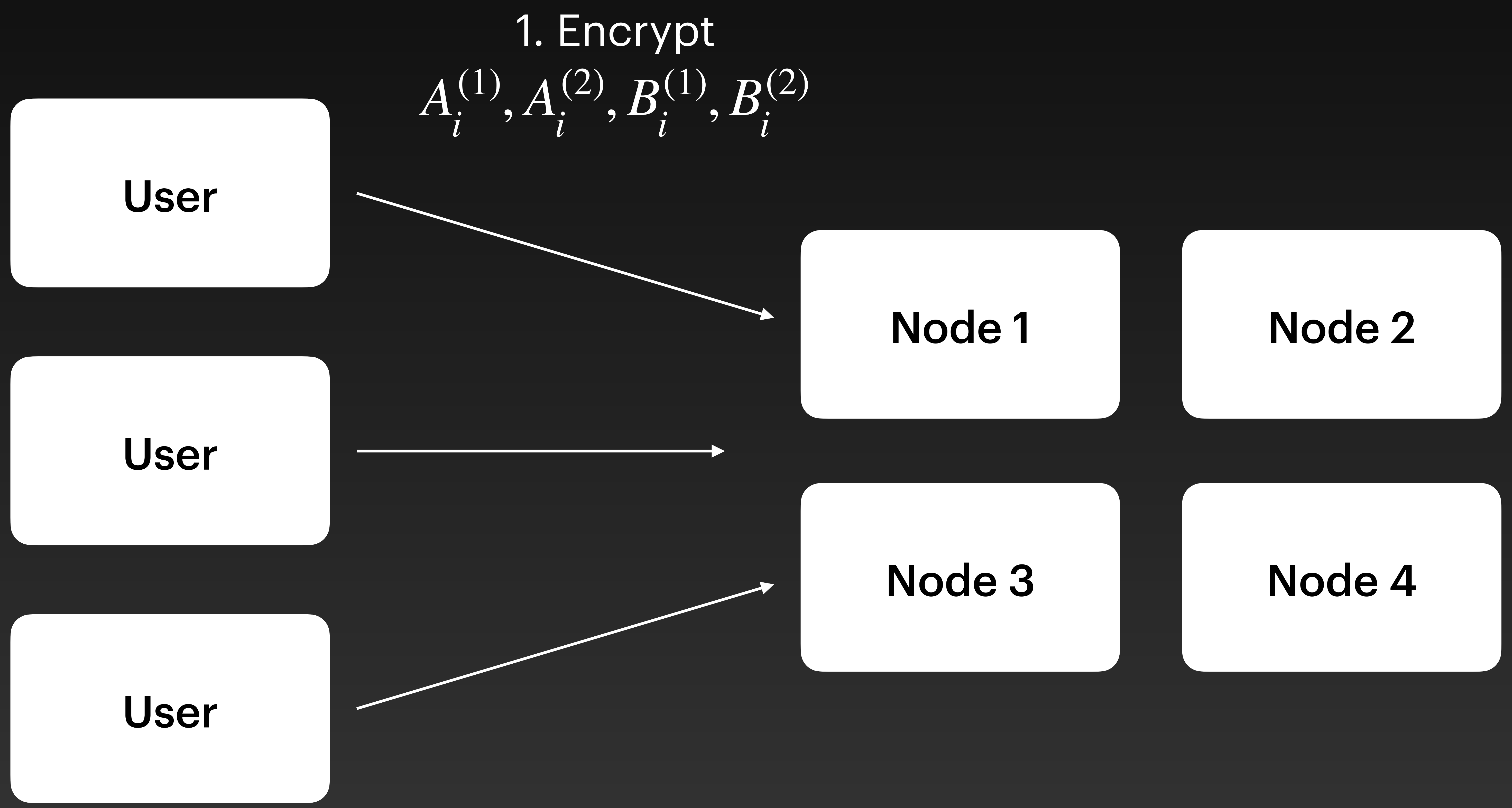
Want to know more?

- Handling general expressions
- Generalisation to multiple users
- Example of numerical evaluation
- Application of Chebyshev polynomials

https://arxiv.org/abs/2208.09852

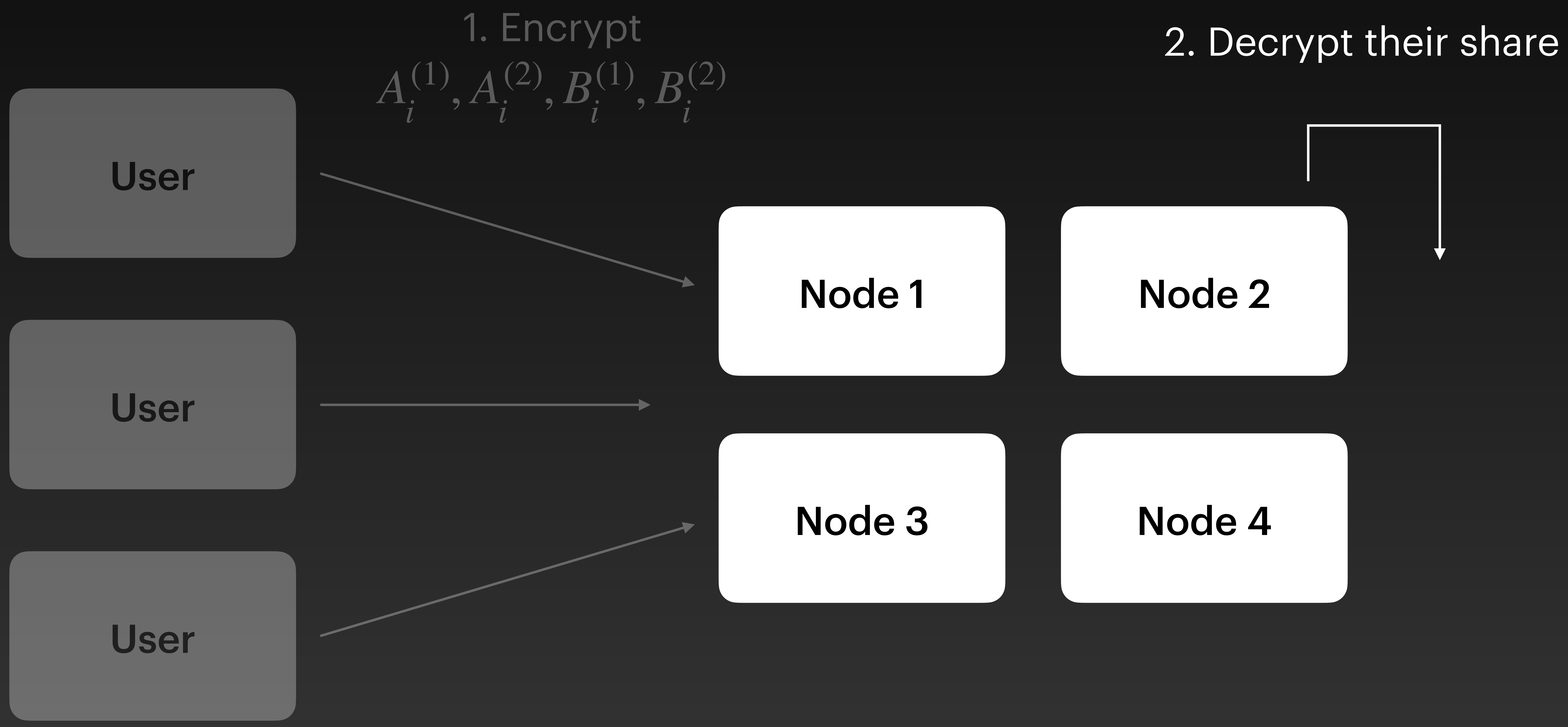
MPC on Blockchains

Motivation



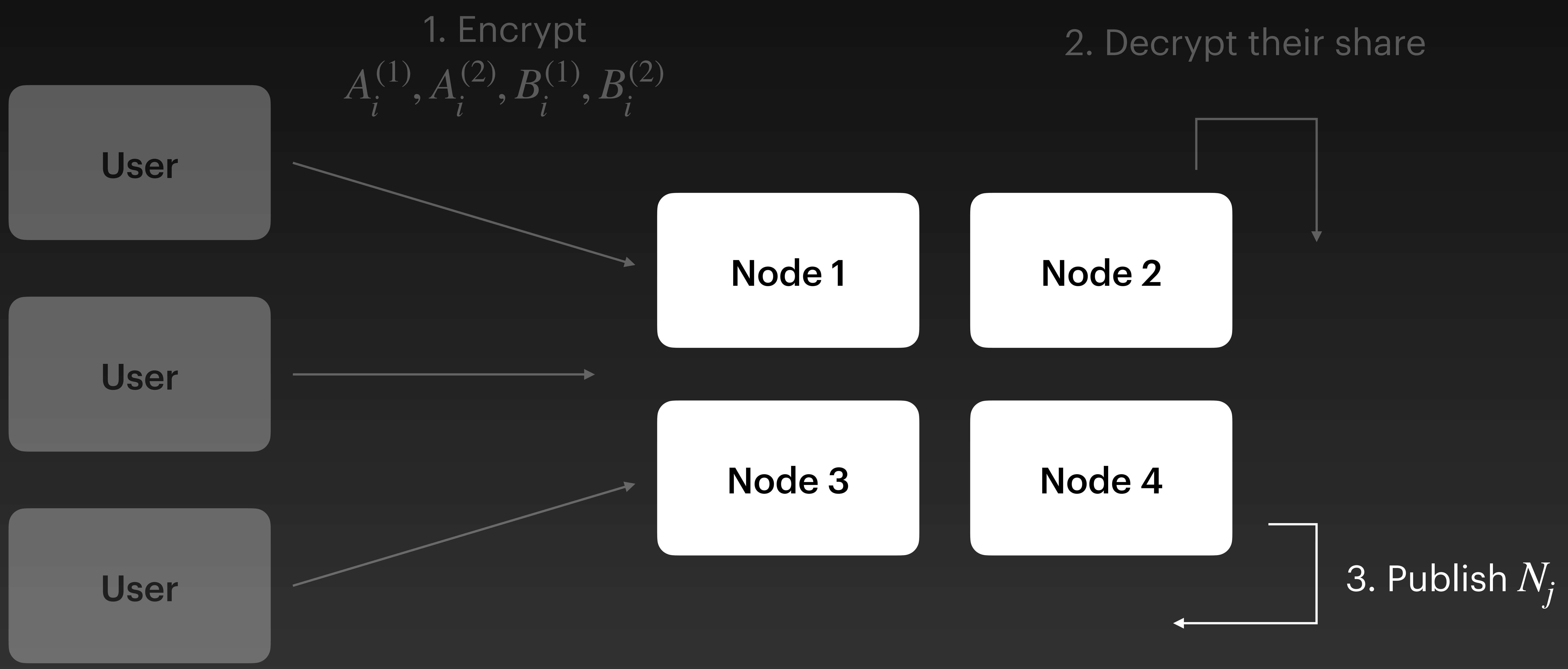
MPC on Blockchains

Motivation



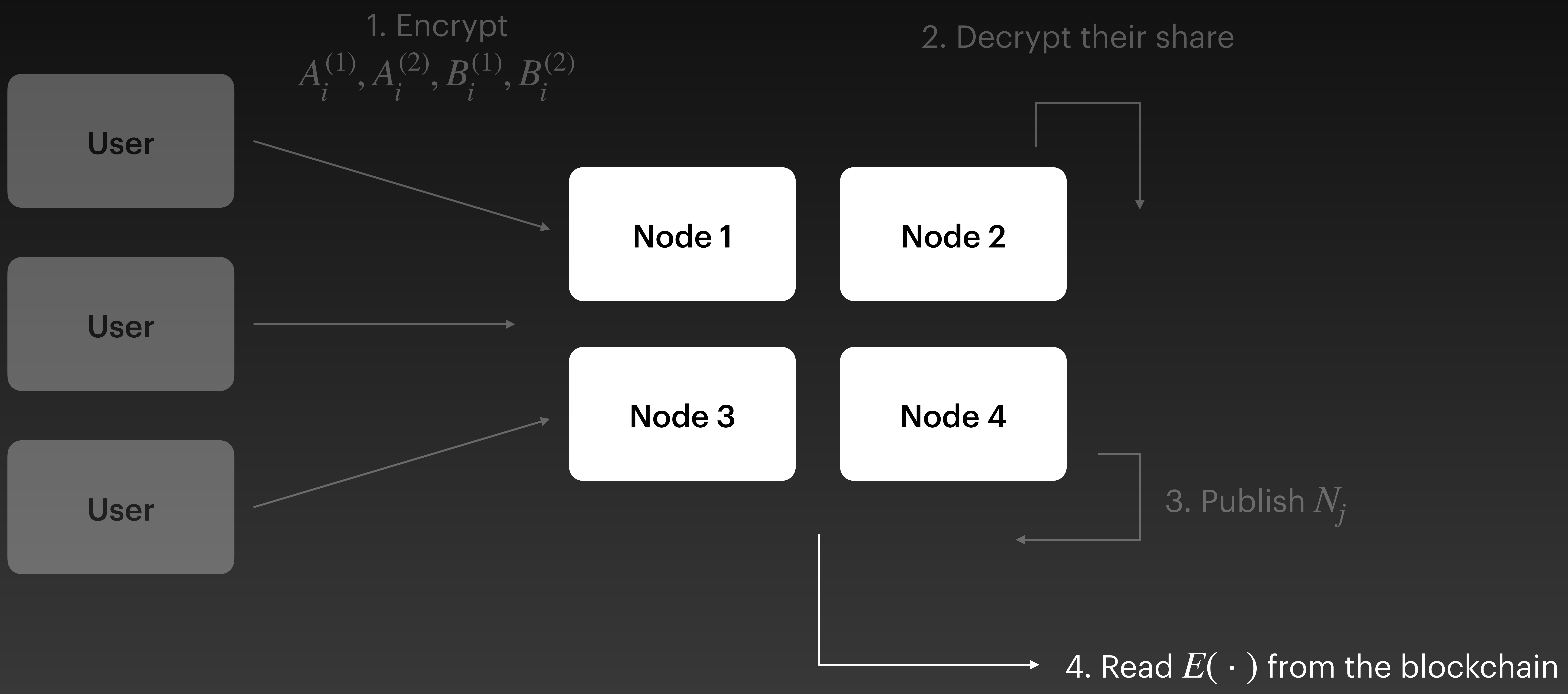
MPC on Blockchains

Motivation



MPC on Blockchains

Motivation



Next Steps?

- Express all operations in fine fields
- Formal security proofs

Engineering

alberto@mystenlabs.com

Math

giorgio.sonnino@ulb.be