秘密分散と秘密計算

ゆかたゆ

例題

- Aさん，Bさん，Cさんが居ます。
- 3人の平均体重を知りたいです。
- お互いに体重を知られたくないです。

問．どうすれば良いでしょうか？

注意点

- 理論の厳密な解説ではありません
- 説明が不十分な点があります

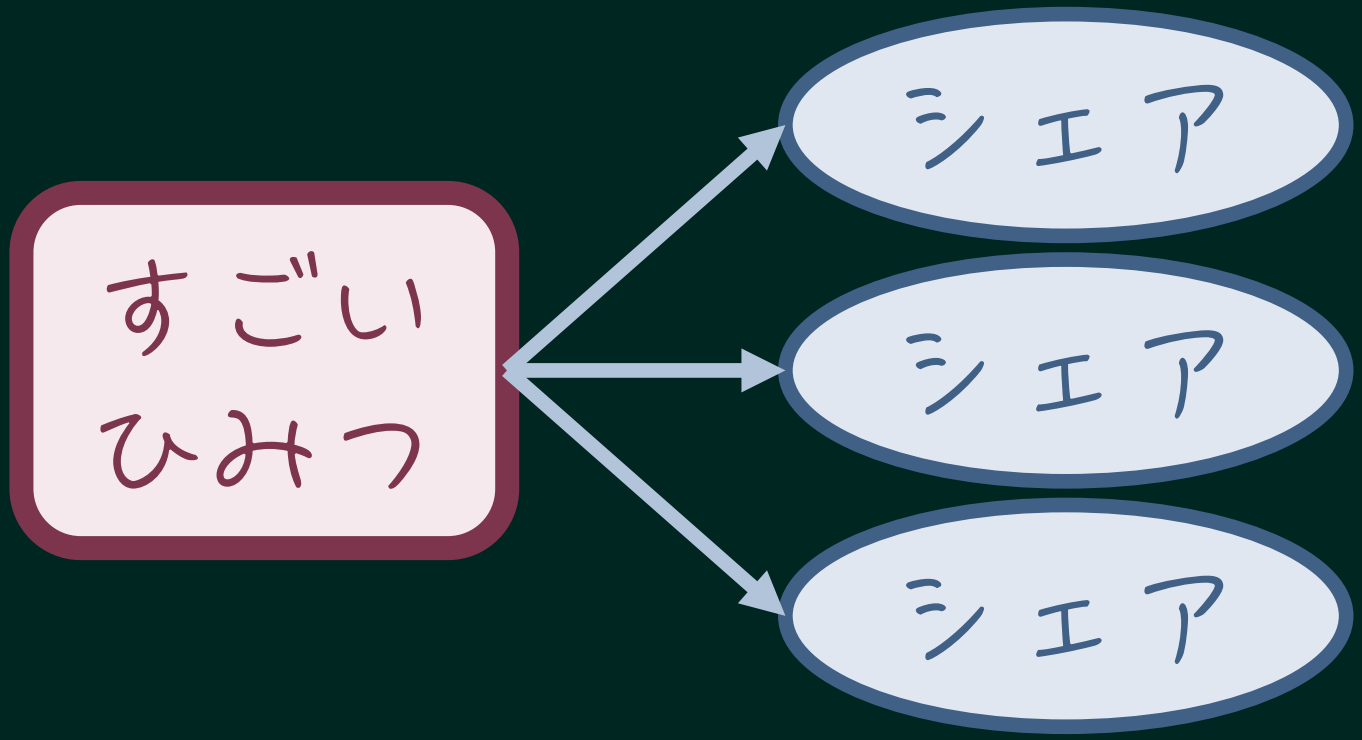
お品書き

- 秘密分散とは
- Shamirの秘密分散法
- 準同型と秘密計算

秘密分散とは

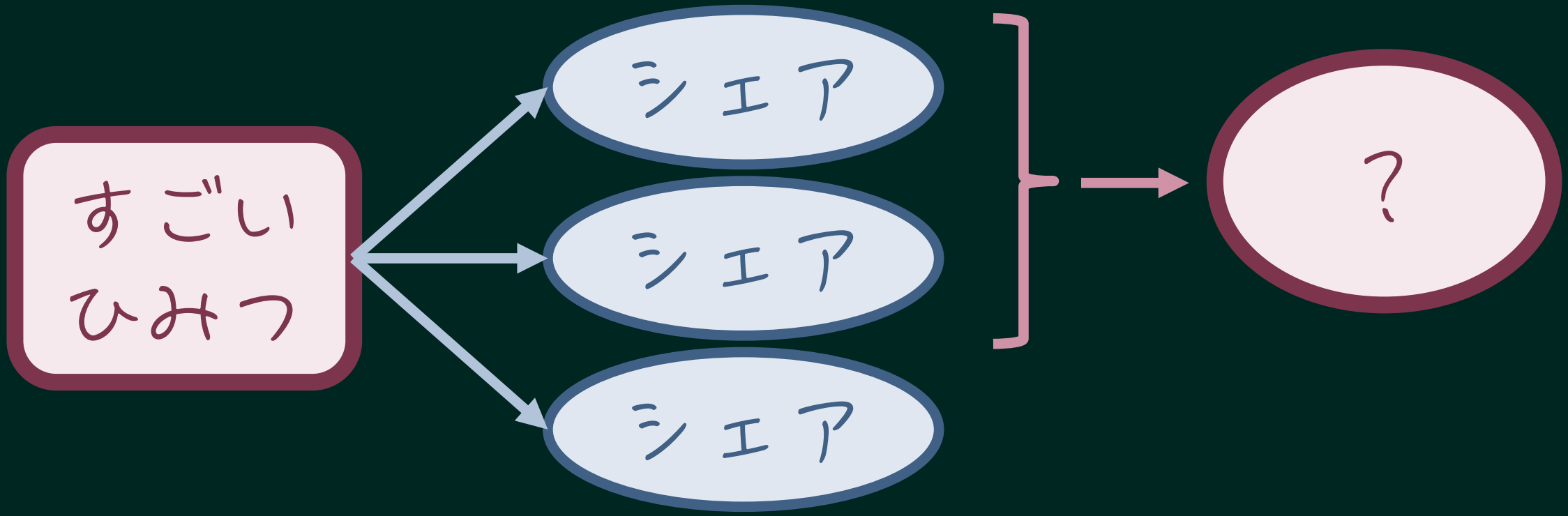
秘密分散とは？

秘密の情報を分散して保存する方法



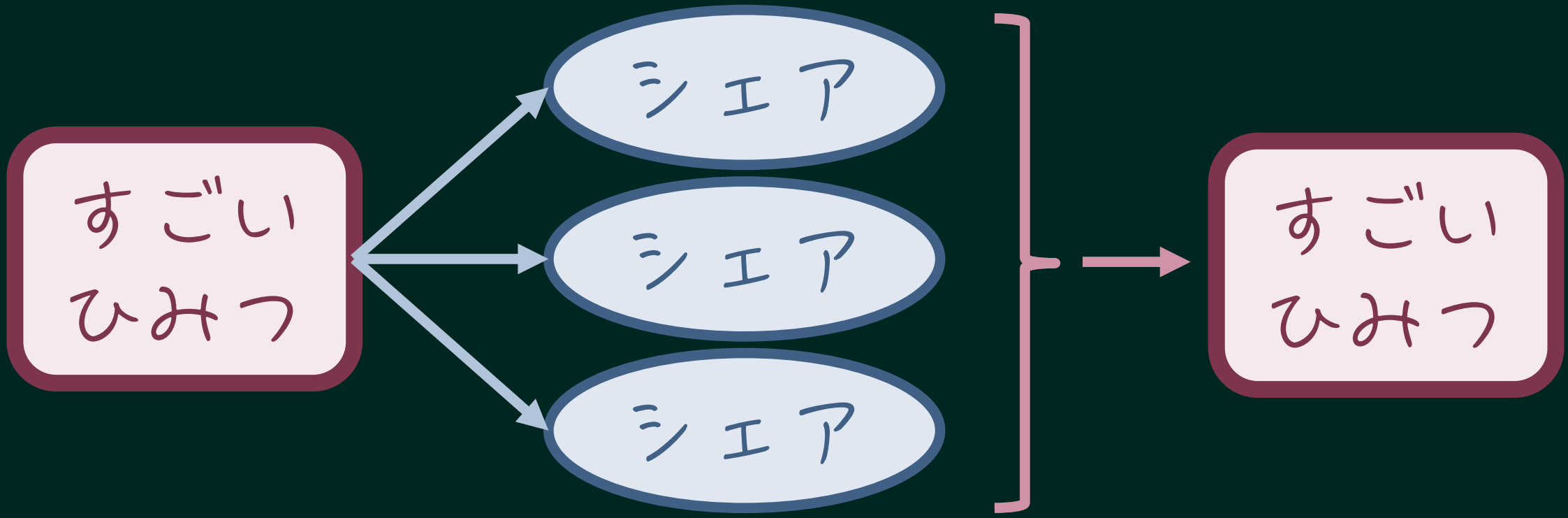
秘密分散とは？

秘密の情報を分散して保存する方法



秘密分散とは？

秘密の情報を分散して保存する方法



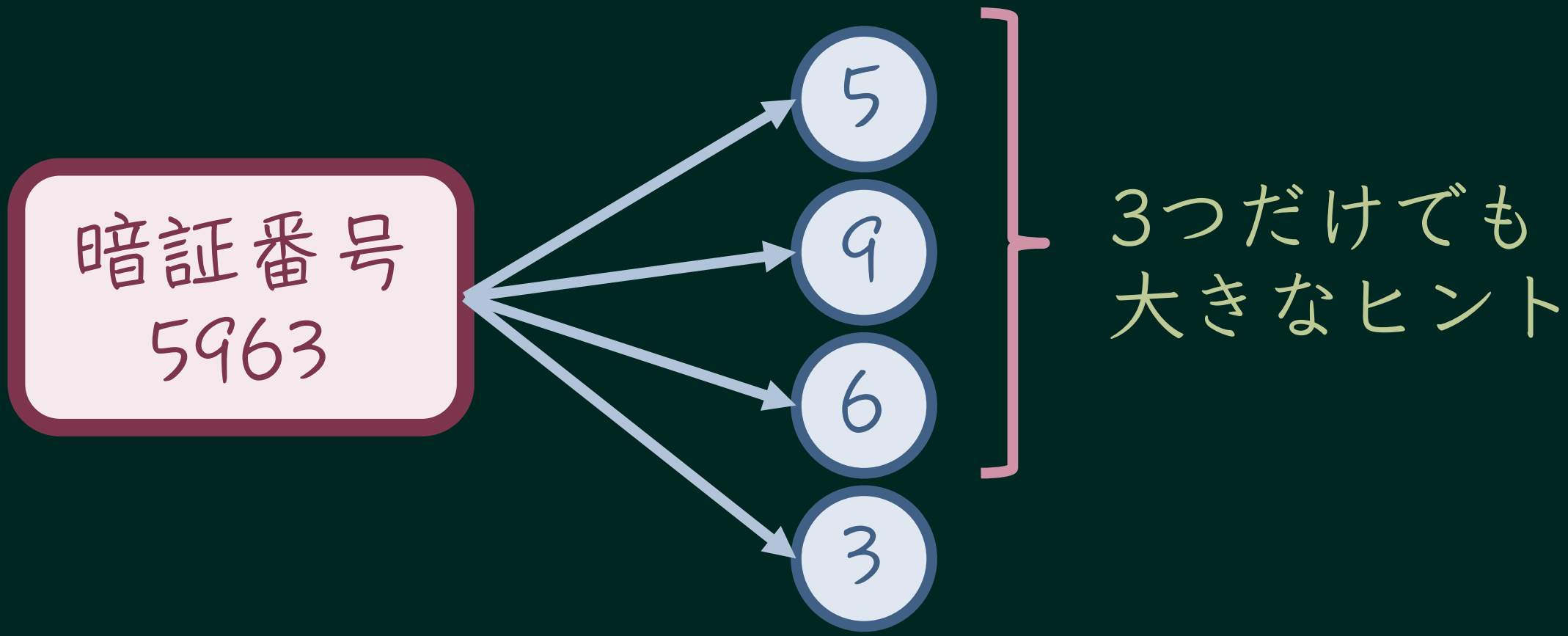
秘密分散の閾値（しきい）

n個中 k個 が集まれば戻せる
→ (k, n)閾値法

たとえば
3個中 2人 が居れば戻せる
→ (2,3)閾値法

余談

秘密分散の良くない例



Shamirの秘密分散法

前提知識

n次方程式のグラフ
$(n+1)$つの点を通る
} 一意に定まる

たとえば

$ax^2+bx+c=0$ ← 3点あれば定まる

分散方法（1/2）

1. 秘密をsとする

2. $(k-1)$次関数 f を作る
   - 定数項は s
   - 係数は乱数

たとえば

$$f(x) = 12x^2 + 5x + s$$

分散方法（2/2）

3. n人それぞれに $f(1), f(2), \ldots, f(n)$ を渡す

4. k個の $f(x)$ から f を復元できる

5. $f(0)$ が元の秘密

たとえば

$$f(x) = 12x^2 + 5x + s$$
$$f(0) = s$$

余談

ラグランジュ補完

$f(x_1), f(x_2), \ldots, f(x_n)$ から多項式fを求める公式

$$f(x) = \sum_{i=1}^{n+1} f(x_i) \frac{f_i(x)}{f_i(x_i)}$$

$$\text{where } f_i(x) = \prod_{k \neq i} (x - x_k)$$

証明は略。

準同型と秘密計算

秘密計算とは

- 内容を秘密にしたまま計算する方法
- 準同型性のある写像を上手く用いる
- 比較演算に弱い

準同型とは

$f(x \cdot y) = f(x) \cdot f(y)$ が成り立つこと

言い換えると

写像が構造を保つこと。

秘密計算で非常に重要な性質

Shamirの方法の準同型

sの破片とtの破片を用意する
足し合わせると，$(s+t)$の破片になる

たとえば

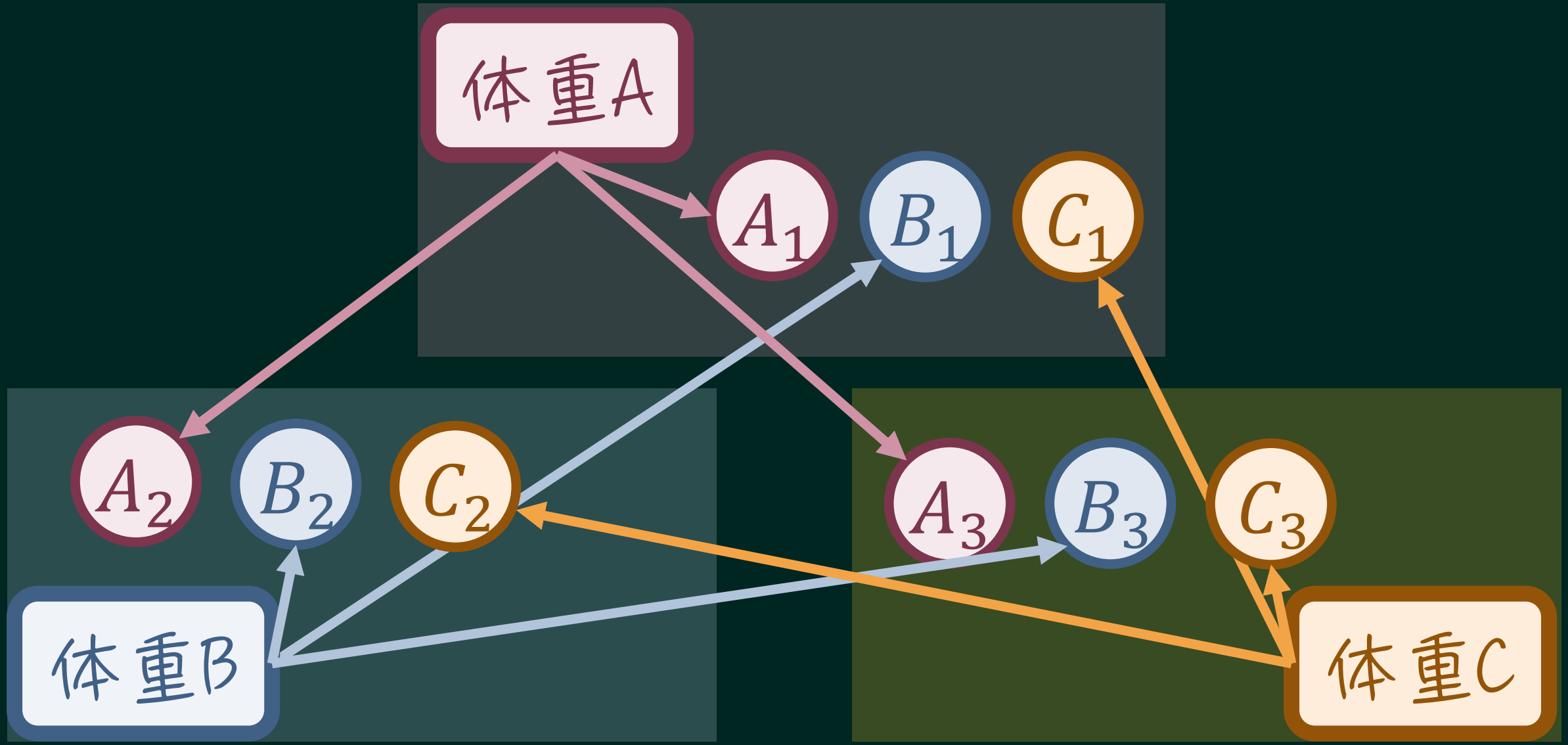
$$f_s(x) = 12x^2 + 5x + s$$
$$f_t(x) = 35x^2 + 2x + t$$
$$f_s(x) + f_t(x) = 47x^2 + 7x + (s+t)$$

例題（再掲）

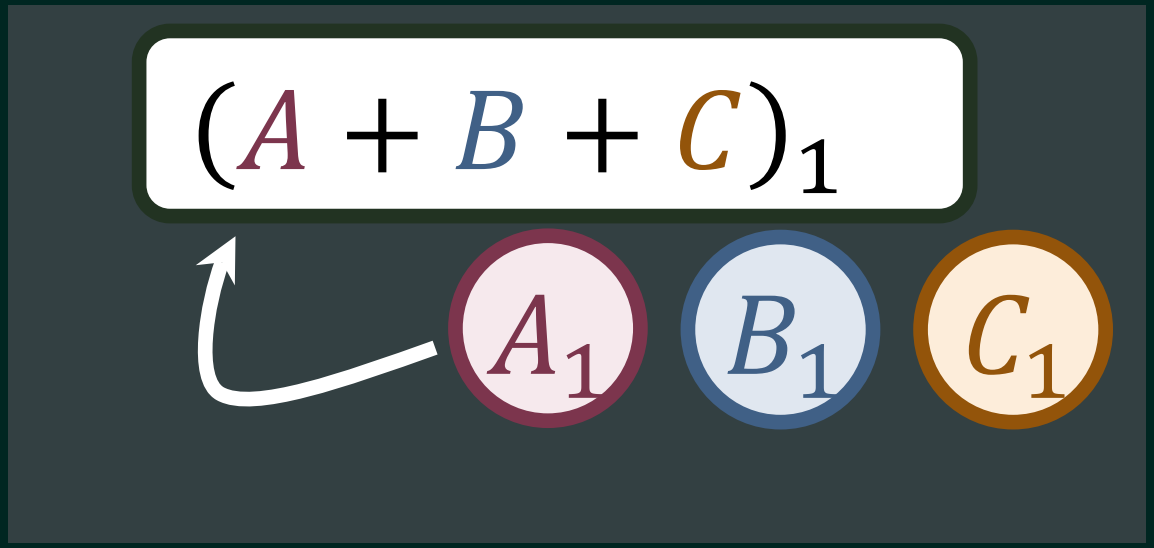
- Aさん，Bさん，Cさんが居ます。
- 3人の平均体重を知りたいです。
- お互いに体重を知られたくないです。

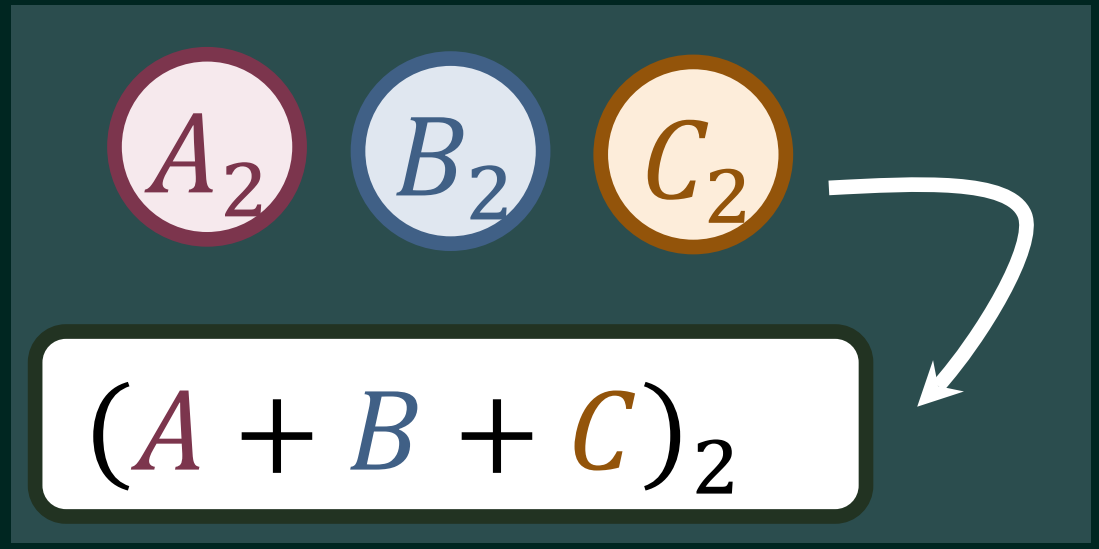
問．どうすれば良いでしょうか？

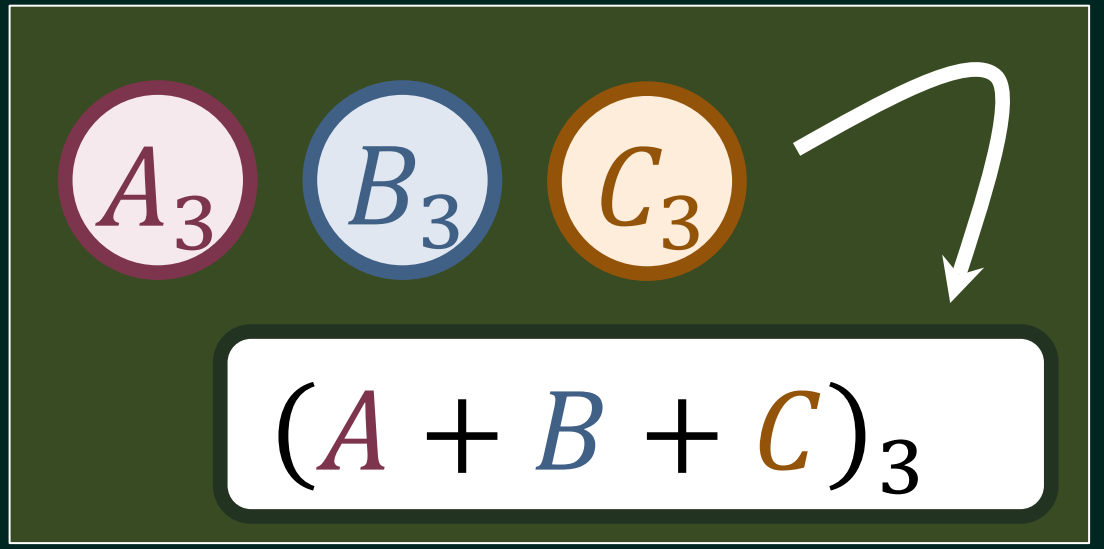
例題の解答例（1/3）



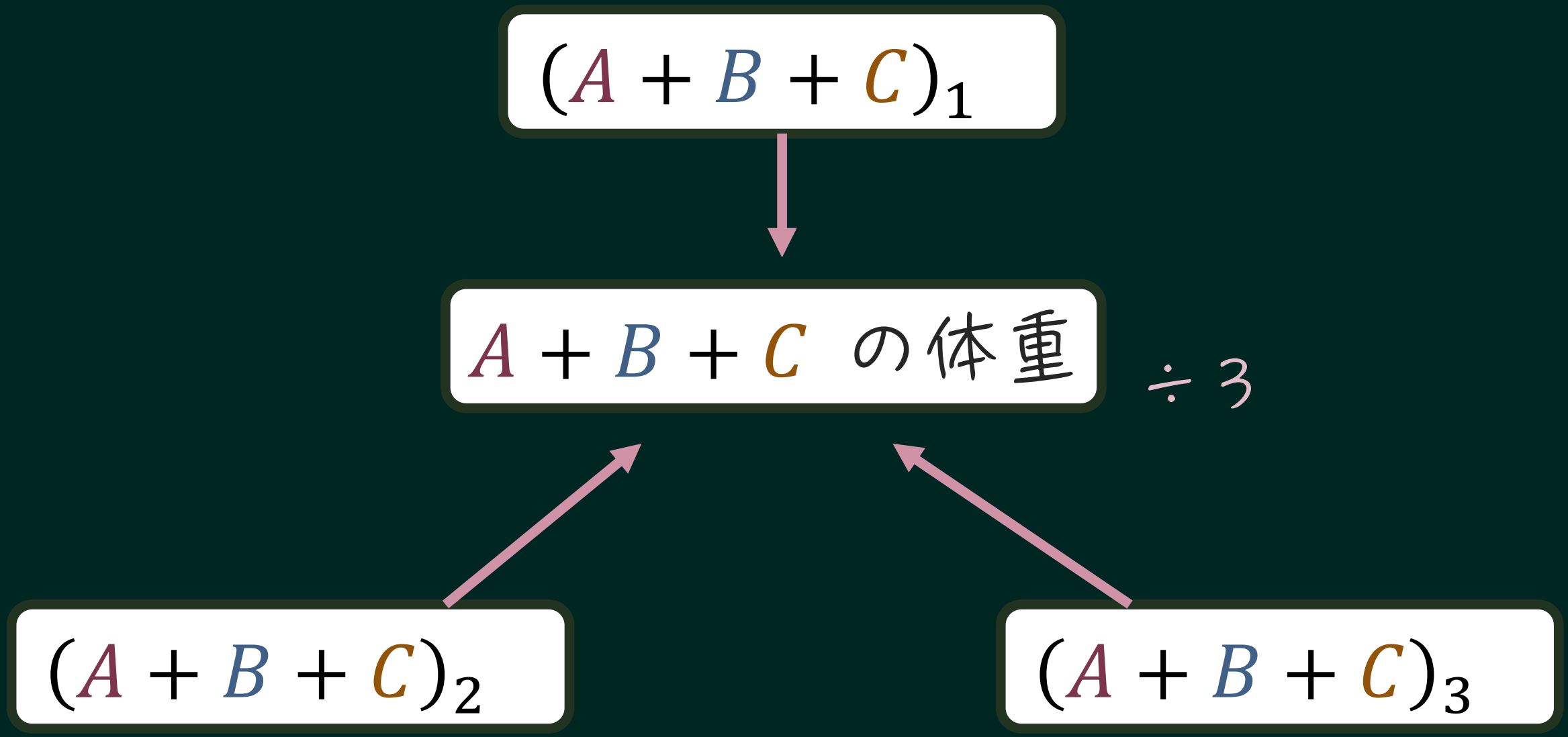
例題の解答例（2/3）







例題の解答例（3/3）



やってみよう

プログラムを書きました（言語はC++）
URLは概要欄にあります。

余談ですが
全員の体重が100以下と仮定して
$GF(307)$ の上で計算しています。

その他の秘密計算

- 準同型暗号を用いたもの
  - BFV
  - CKKS形式
  - TEHE形式

など。

まとめ

伝えたいこと

- 秘密分散
  → 冗長化と内容の分散を同時に行える

- 秘密計算
  → 内容を秘密にしたまま計算ができる

終わり