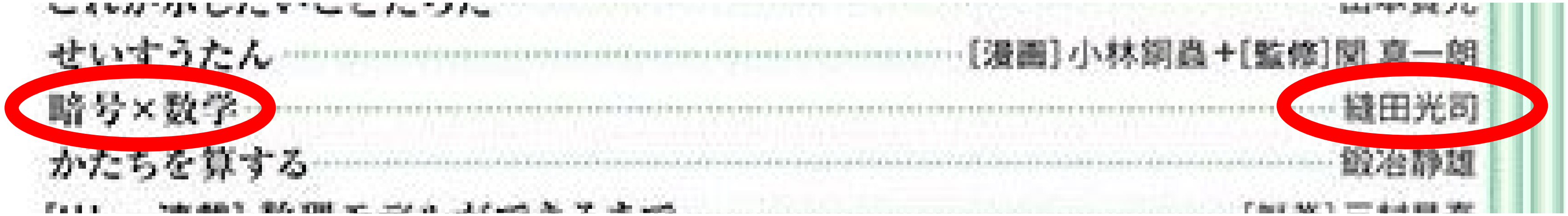
秘密計算と数学

縫田　光司（ぬいだ　こうじ）
九州大学 マス・フォア・インダストリ研究所

数学・数理科学5研究拠点合同市民講演会「数学・数理科学の未来!?」
2023年11月18日　@統計数理研究所

自己紹介

- 学生時代は（応用系でない）**数学**を専攻
- 現在は**数学**と**暗号**分野を並行して研究



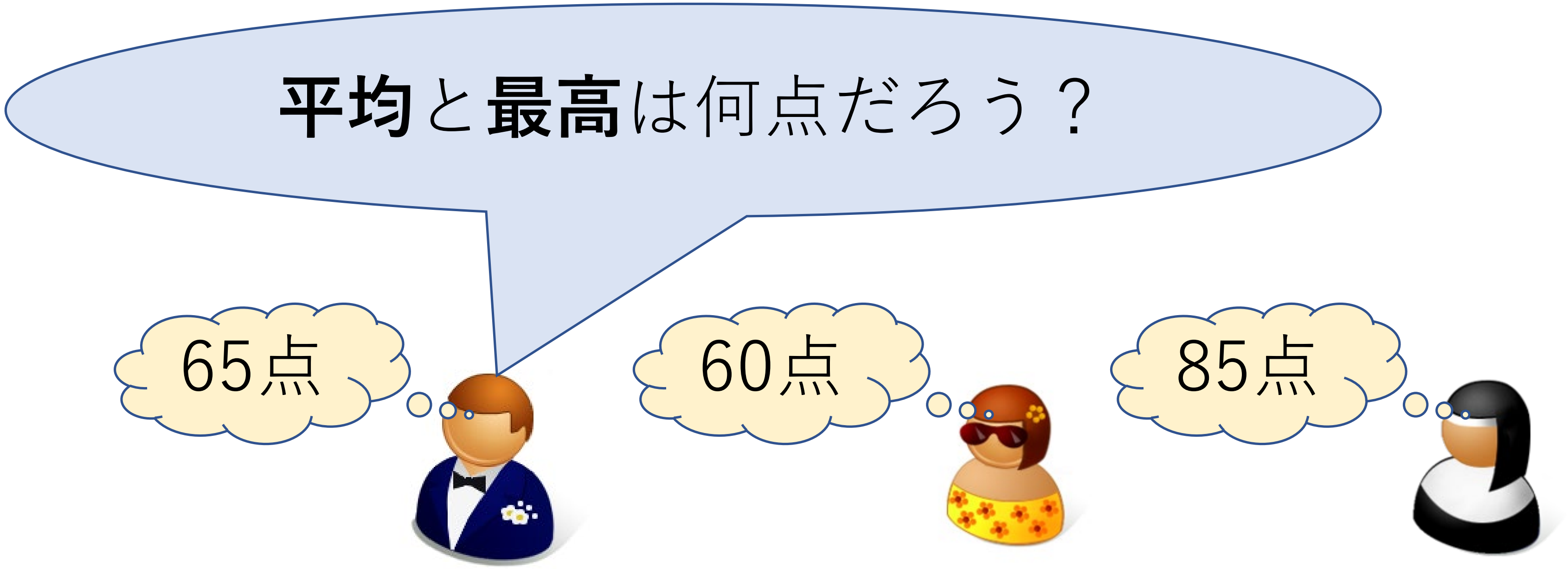
https://www.nippyo.co.jp/shop/magazine/8240.html

秘密計算とは

秘密計算とは

各自の**入力データは秘密**にしたまま
必要な情報のみを得る技術

例



秘密計算とは

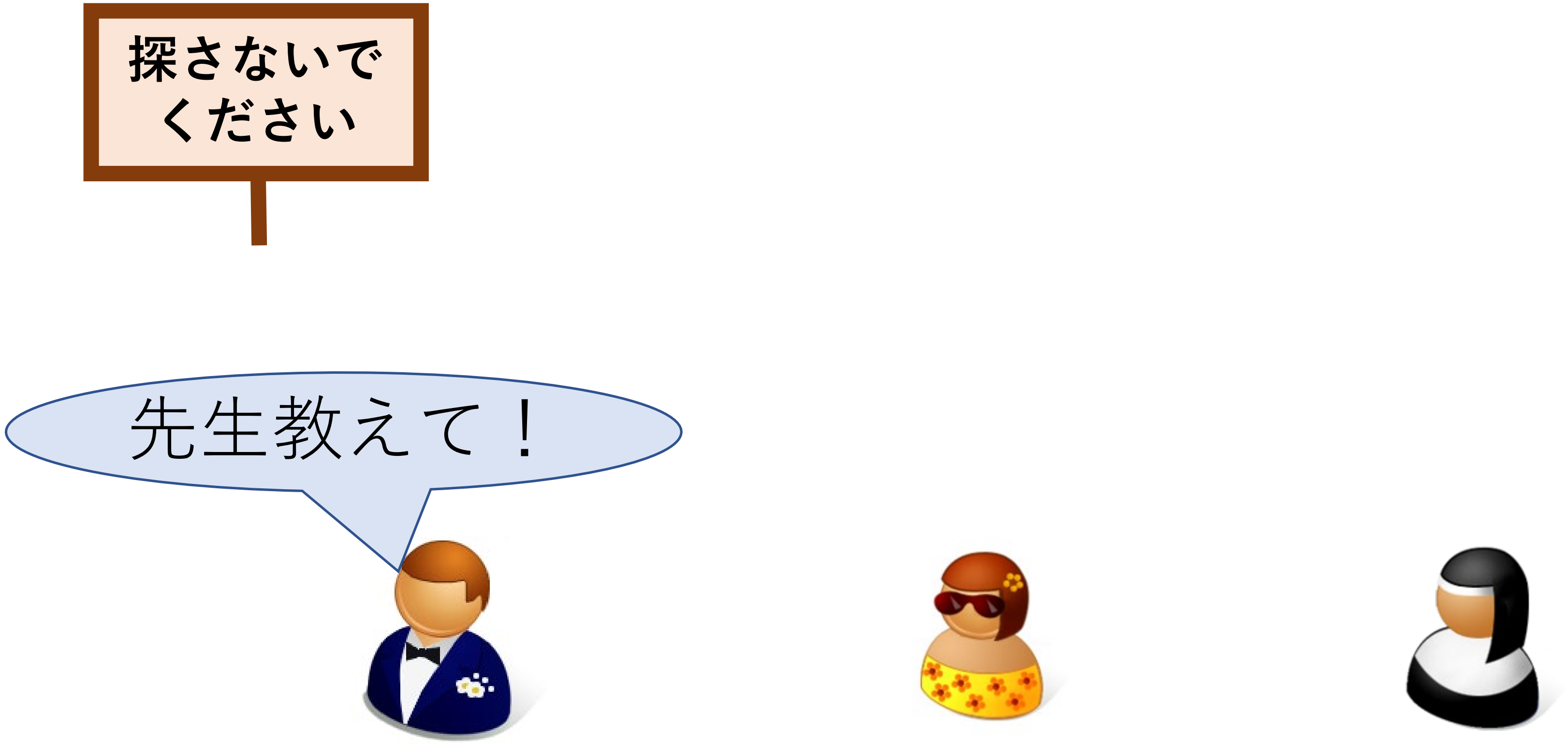
各自の**入力データは秘密**にしたまま
必要な情報のみを得る技術

例

秘密計算とは

各自の**入力データは秘密**にしたまま
必要な情報のみを得る技術

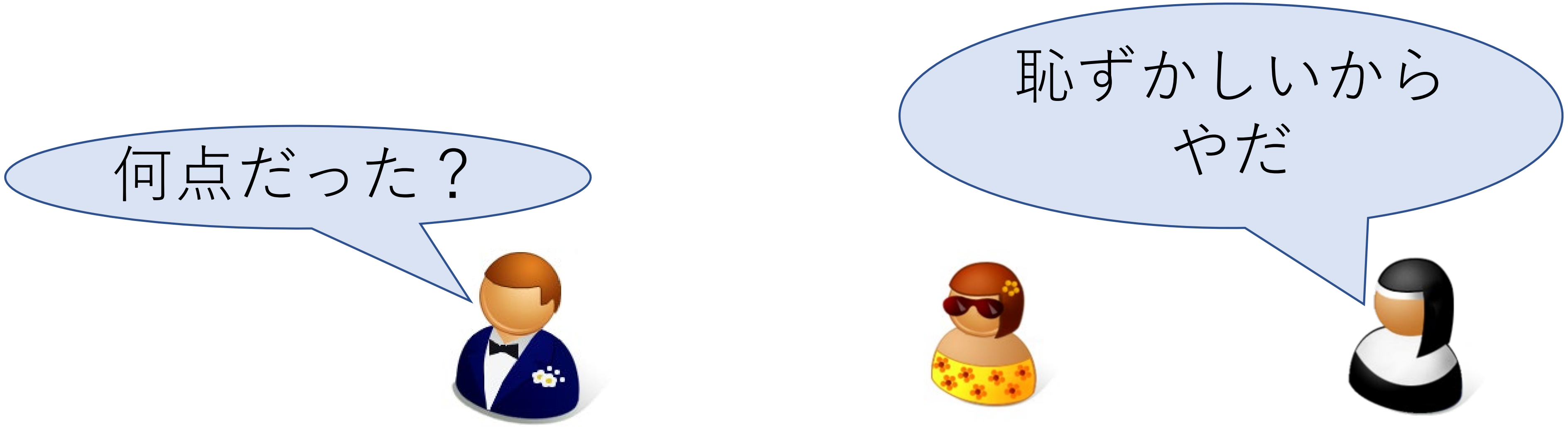
例



秘密計算とは

各自の**入力データは秘密**にしたまま
必要な情報のみを得る技術

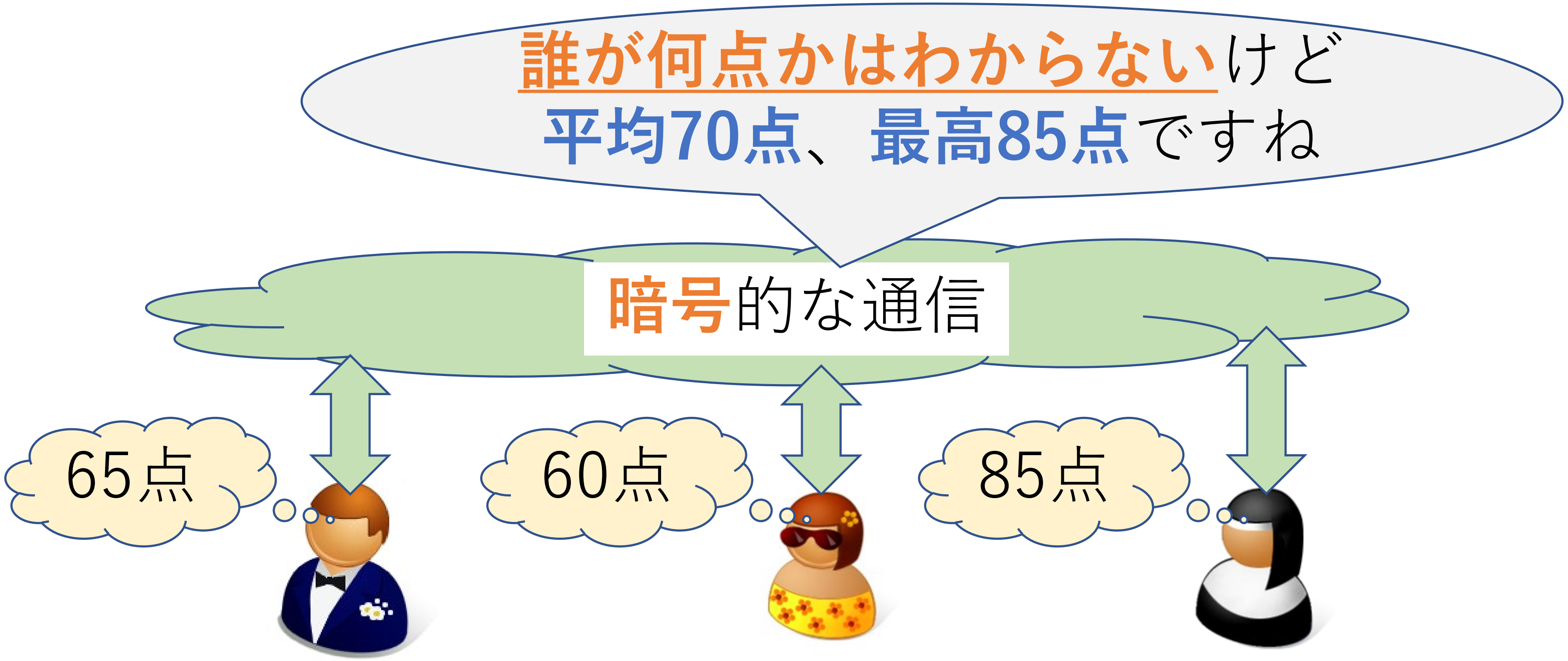
例



秘密計算とは

各自の**入力データは秘密**にしたまま
必要な情報のみを得る技術

例



秘密計算とは

各自の**入力データは秘密**にしたまま
必要な情報のみを得る技術

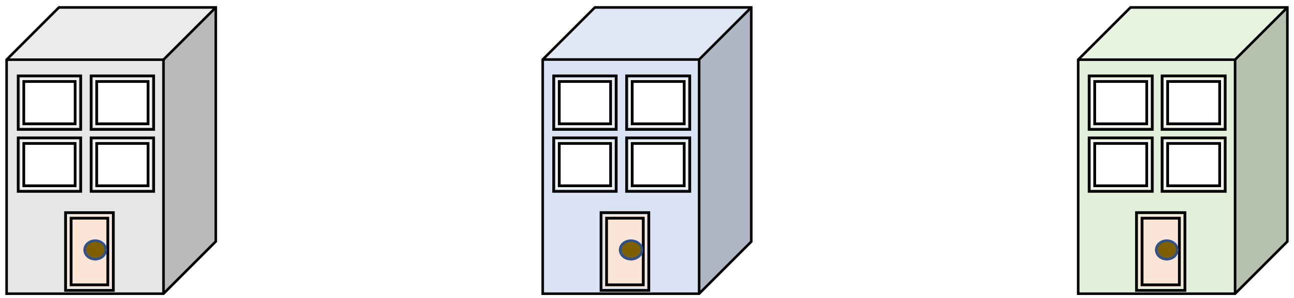
例

➢ **顧客データを統合して高精度の分析をしたい**

けれども

➢ **自社の顧客データを他社に渡したくない**

A社　B社　C社



秘密計算とは

各自の**入力データは秘密**にしたまま
必要な情報のみを得る技術

例

- 検索**内容を隠しつつ**
検索**結果を得たい**
（「秘匿検索」）

秘密計算の例

～（簡単な）投票～

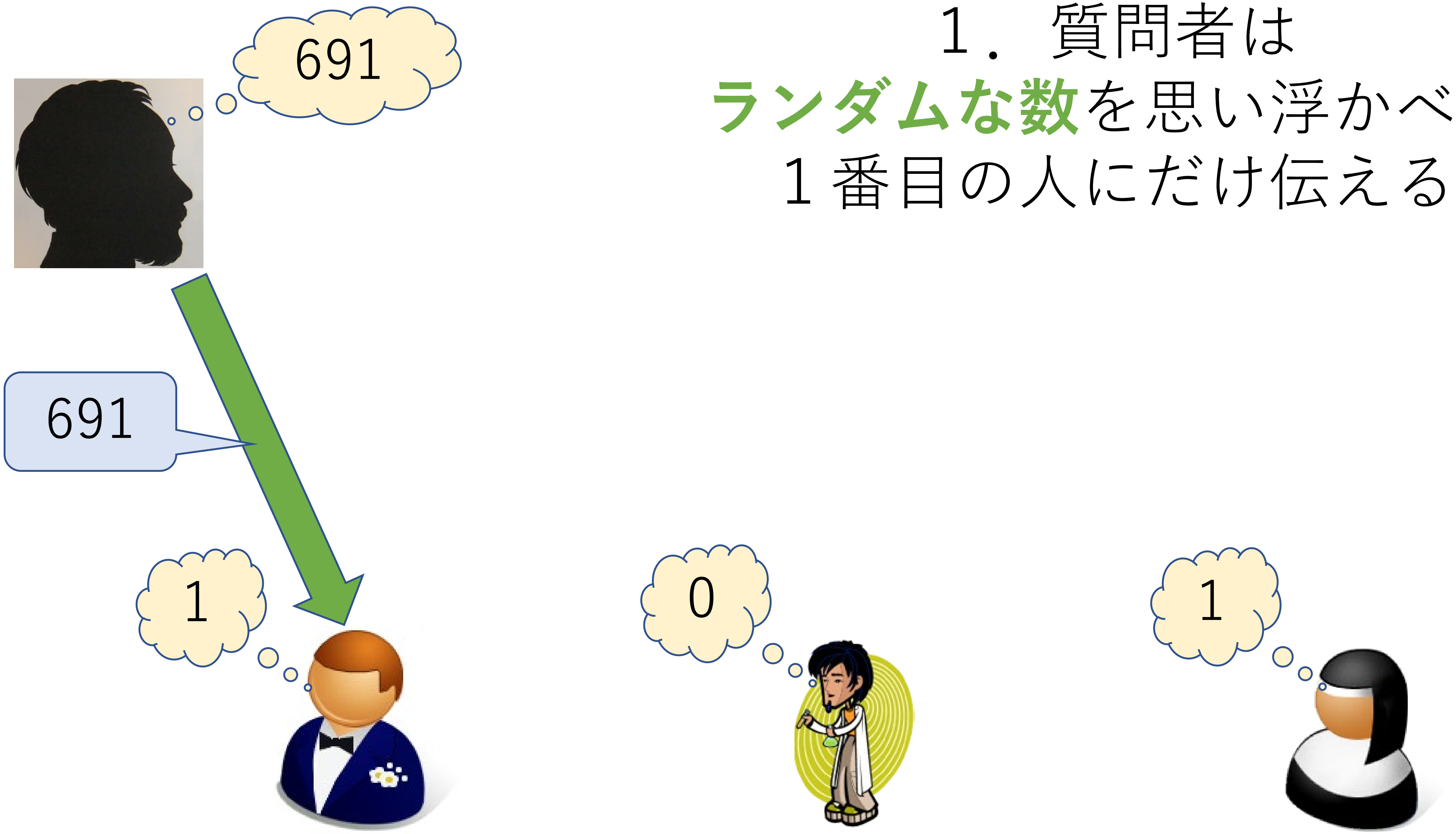
質問：
この講演は面白いですか？
(Yes / No)

- 「yes」→ 1、「no」→ 0
- 何人が「yes」か知りたい
  → **全員の数の合計**

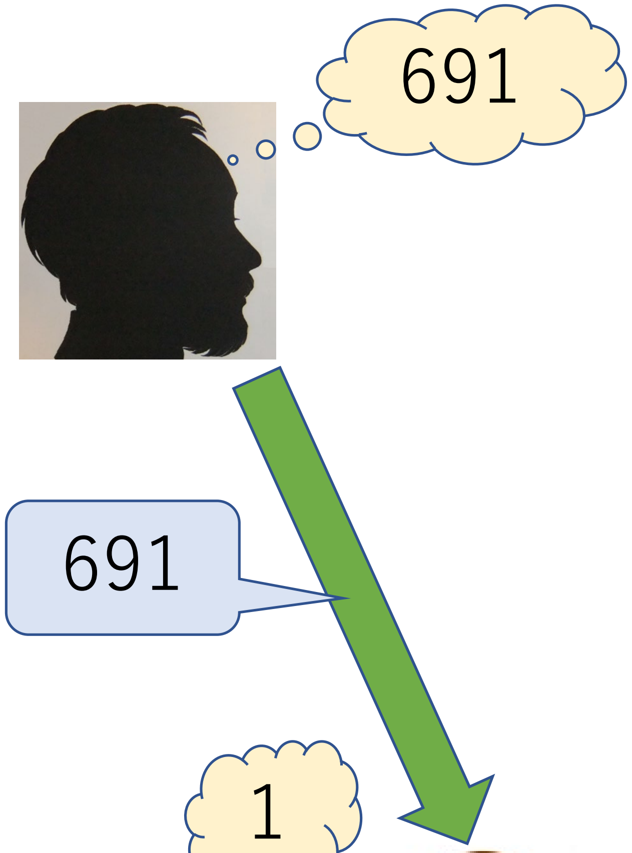
本人に直接は
言いにくい…

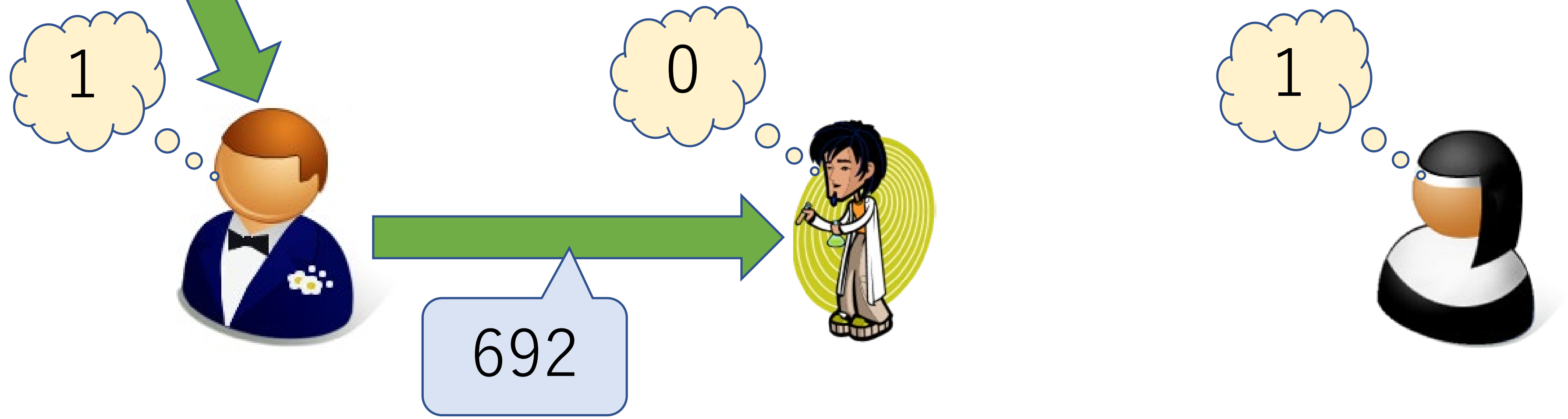
方法（仮）

１．質問者は
ランダムな数を思い浮かべて
１番目の人にだけ伝える

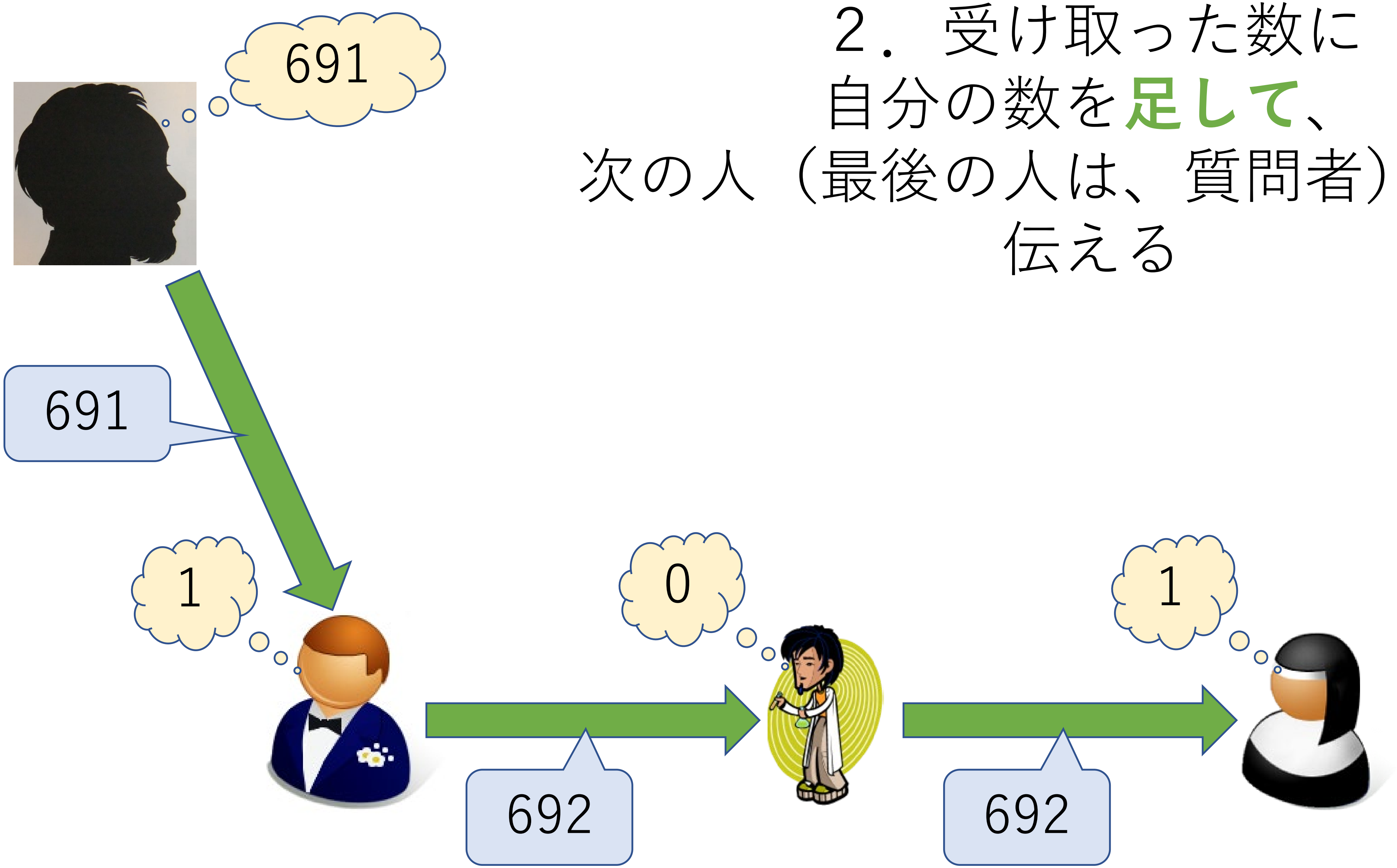


2．受け取った数に
自分の数を**足して**、
次の人（最後の人は、質問者）だけに
伝える

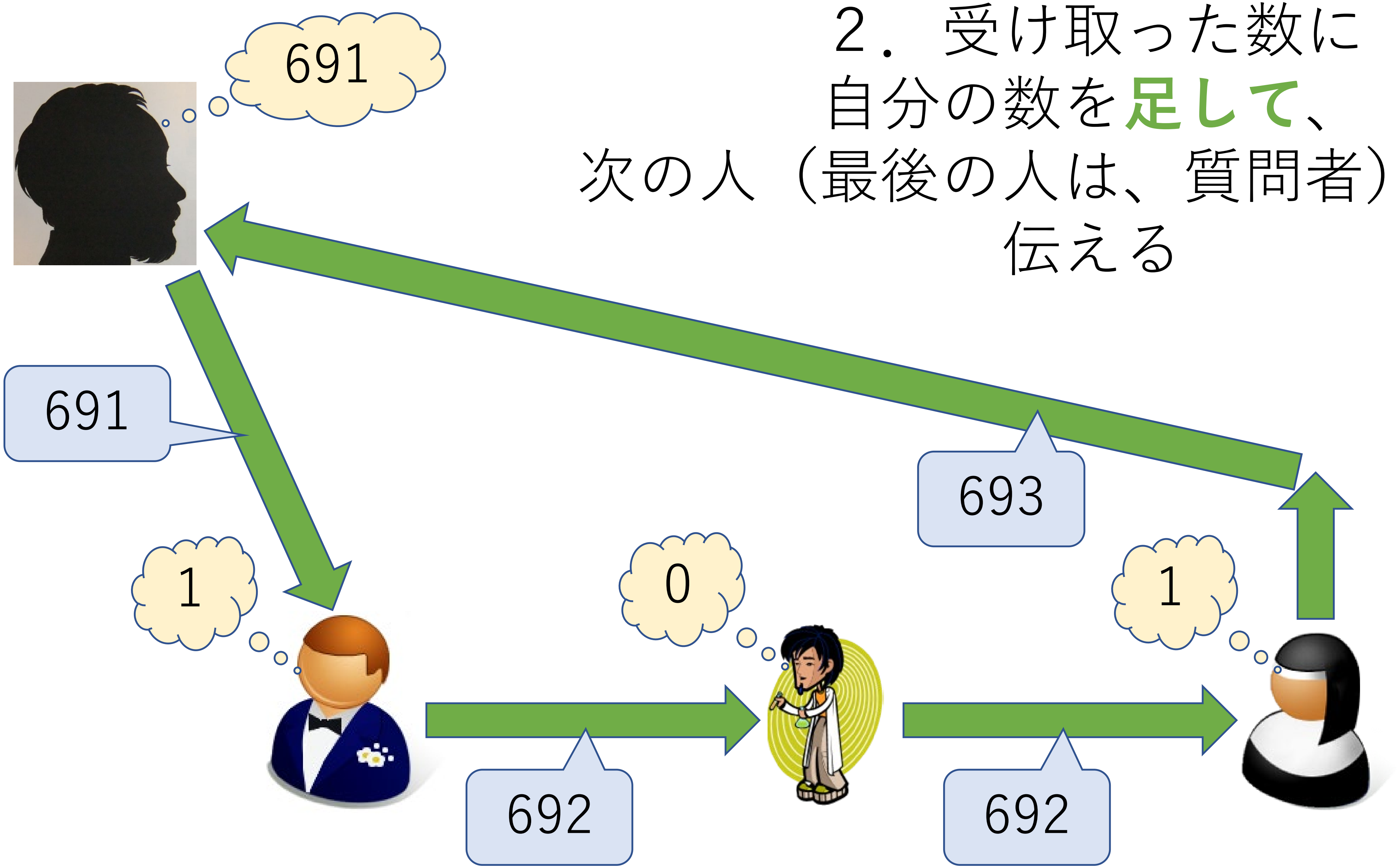




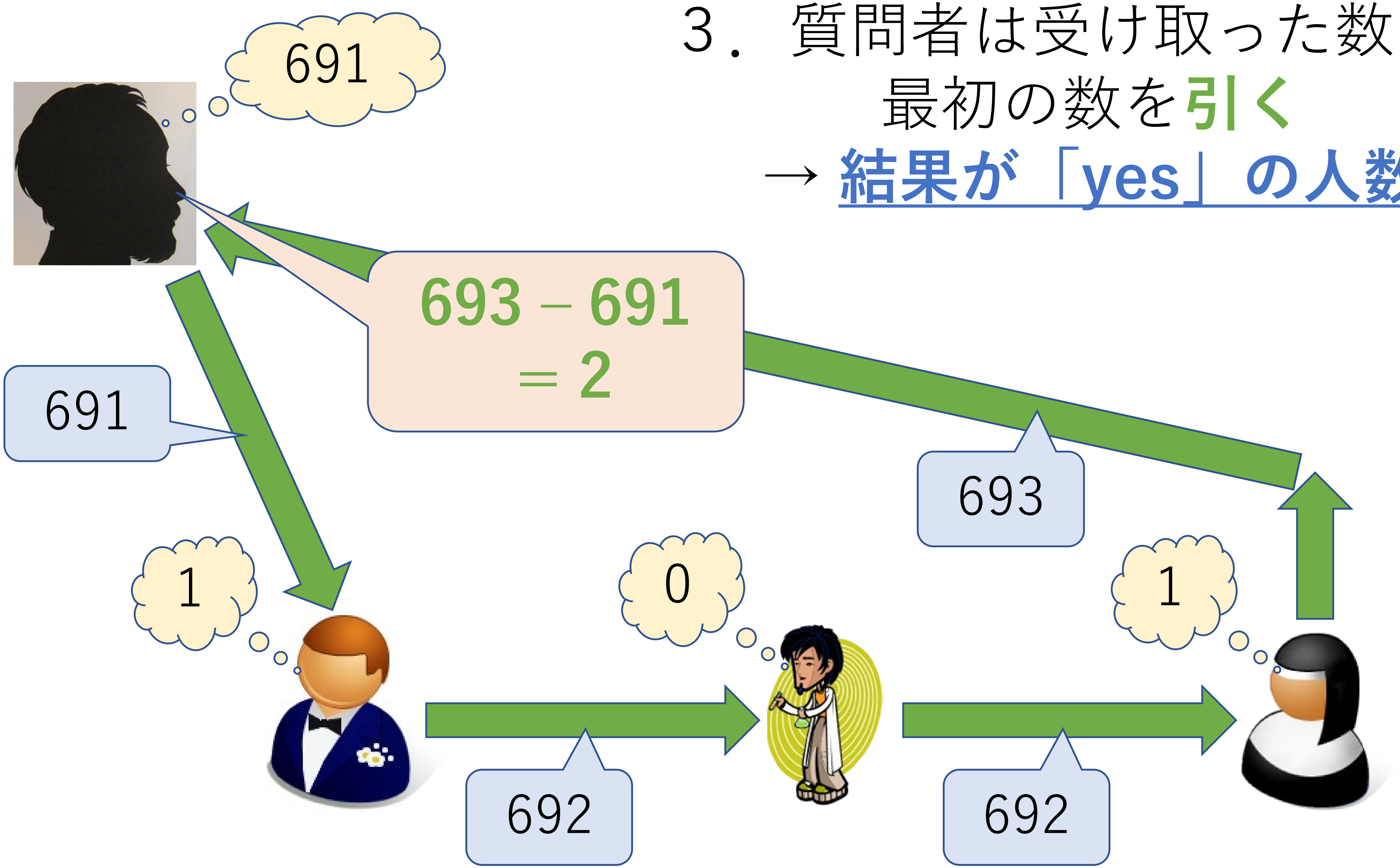
2．受け取った数に
自分の数を**足して**、
次の人（最後の人は、質問者）だけに
伝える



2． 受け取った数に
自分の数を**足して**、
次の人（最後の人は、質問者）だけに
伝える

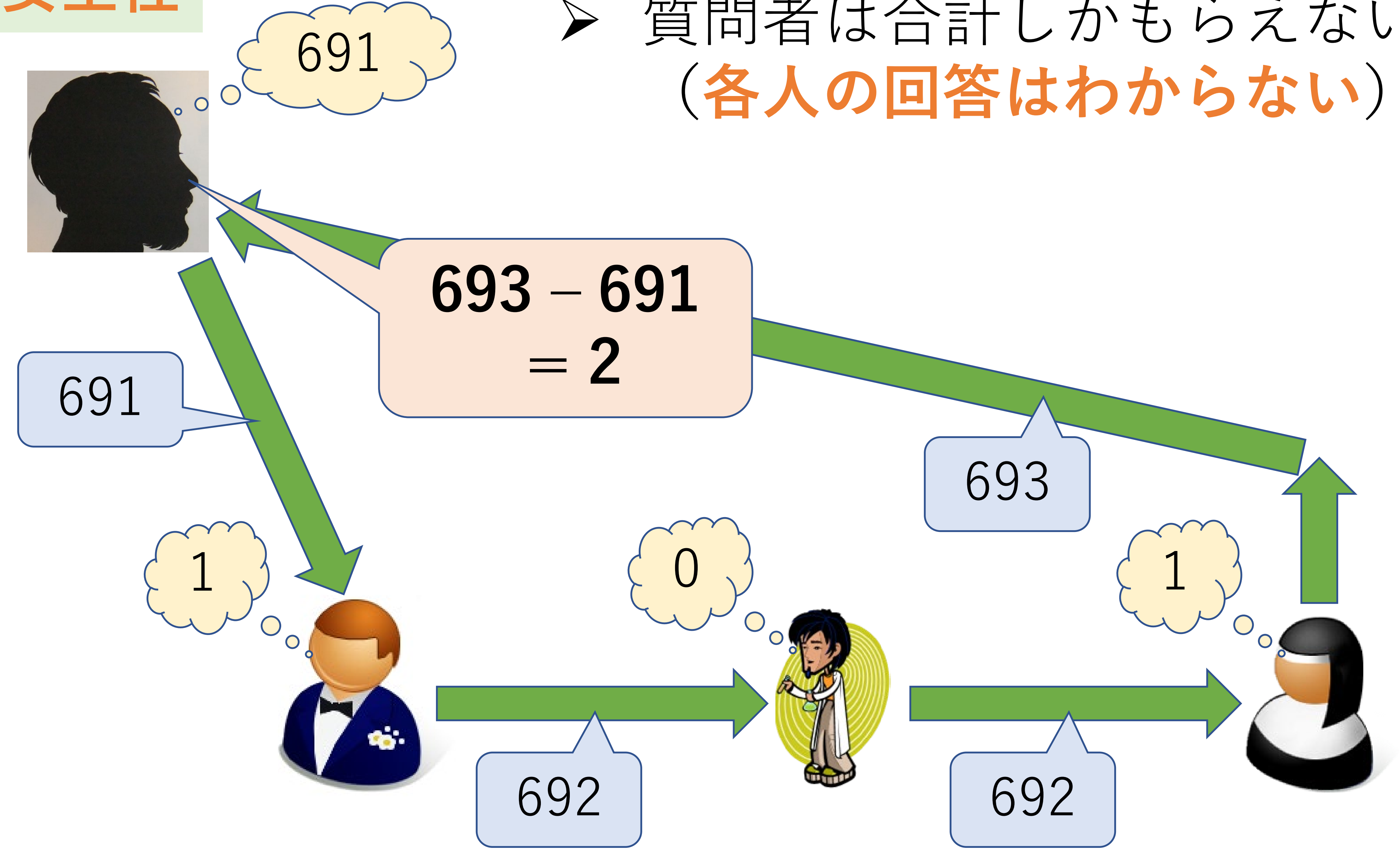


3． 質問者は受け取った数から
最初の数を**引く**
→ **結果が「yes」の人数**



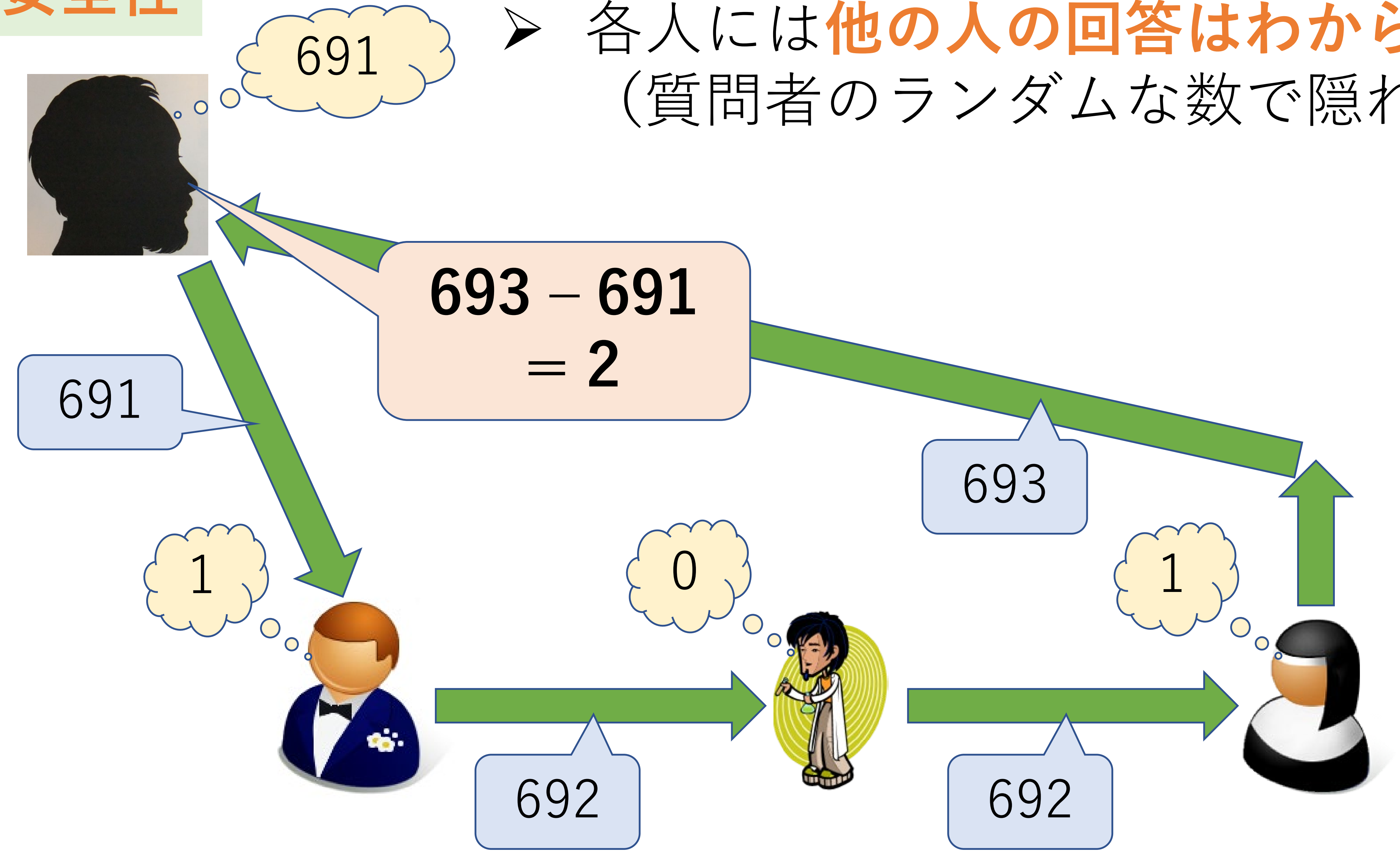
安全性

- ➢ 質問者は合計しかもらえない
  （**各人の回答はわからない**）

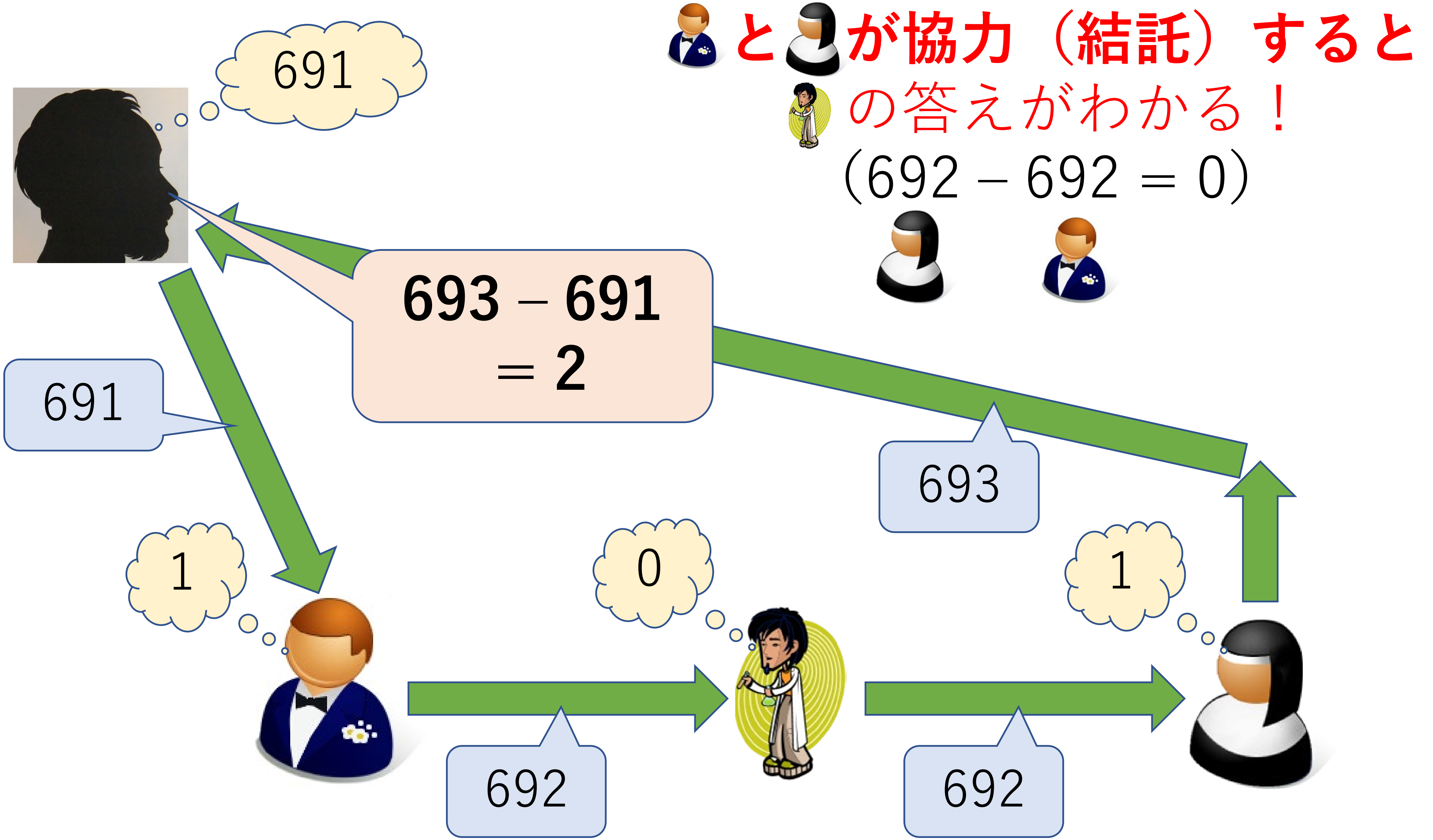


安全性

- 各人には**他の人の回答はわからない**
  （質問者のランダムな数で隠れている）

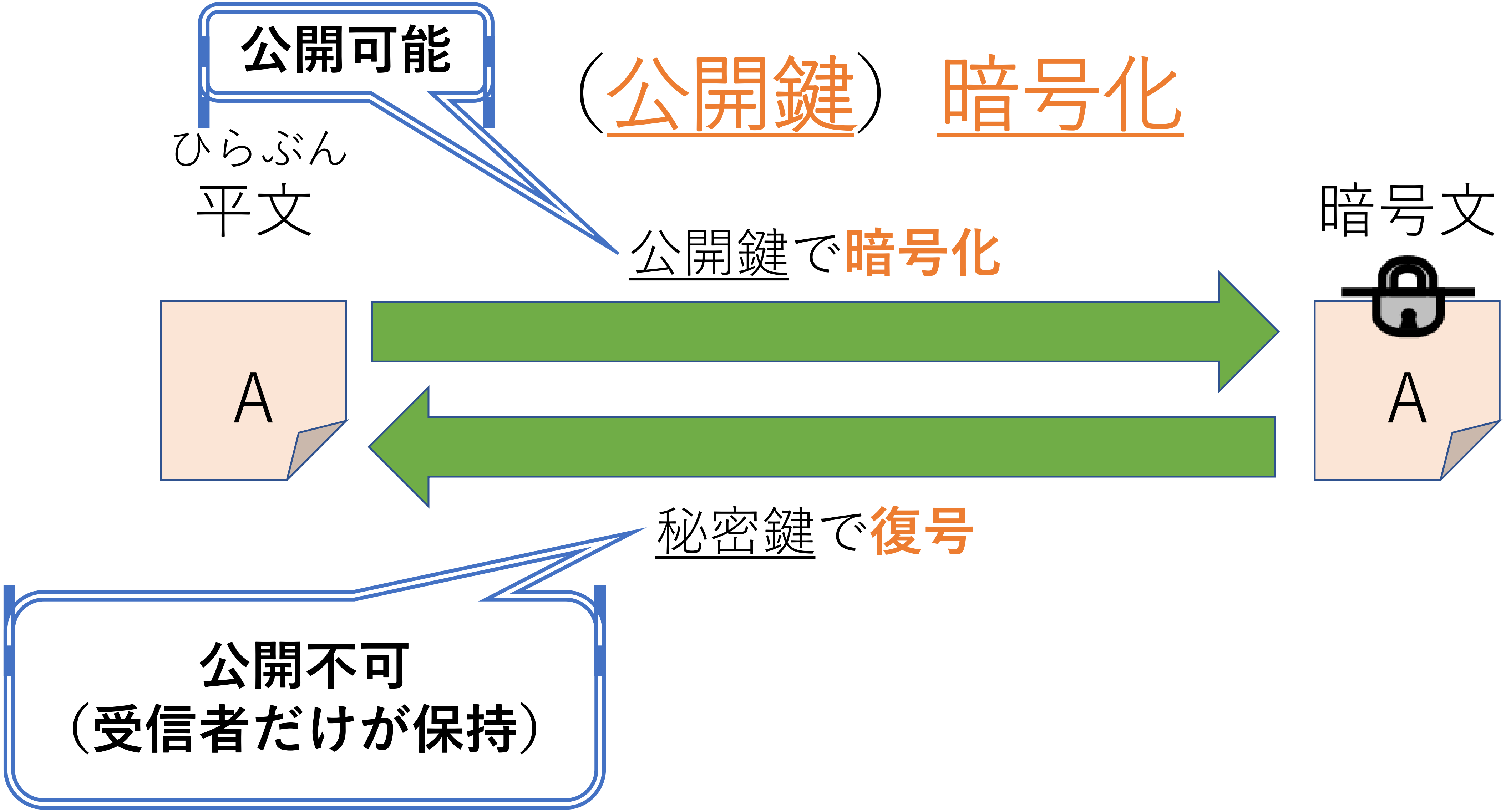


ところが


とが協力（結託）すると
の答えがわかる！
(692 – 692 = 0)
691
691
693 – 691
= 2
693
1
0
1
692
692

解決策：準同型暗号

（公開鍵）暗号化



パイエ暗号（概略）

$N = pq$（$p, q \geq 5$は異なる**素数**でビット長が等しい）

平文 $m \in \mathbb{Z}/N\mathbb{Z}$の暗号文（$r$は**乱数**）

$$[[\boldsymbol{m}]] \coloneqq (\mathbf{1} + \boldsymbol{N})^{\boldsymbol{m}} \boldsymbol{r}^{\boldsymbol{N}} \bmod \boldsymbol{N}^{\mathbf{2}}$$

復号の方法は省略：正しく復号できることの証明には
二項定理、**オイラーの定理**、**中国式剰余定理**などを用いる

[P. Paillier, EUROCRYPT 1999]

パイエ暗号（概略）

$N = pq$（$p, q \geq 5$は異なる**素数**でビット長が等しい）

平文 $m \in \mathbb{Z}/N\mathbb{Z}$の暗号文（$r$は**乱数**）

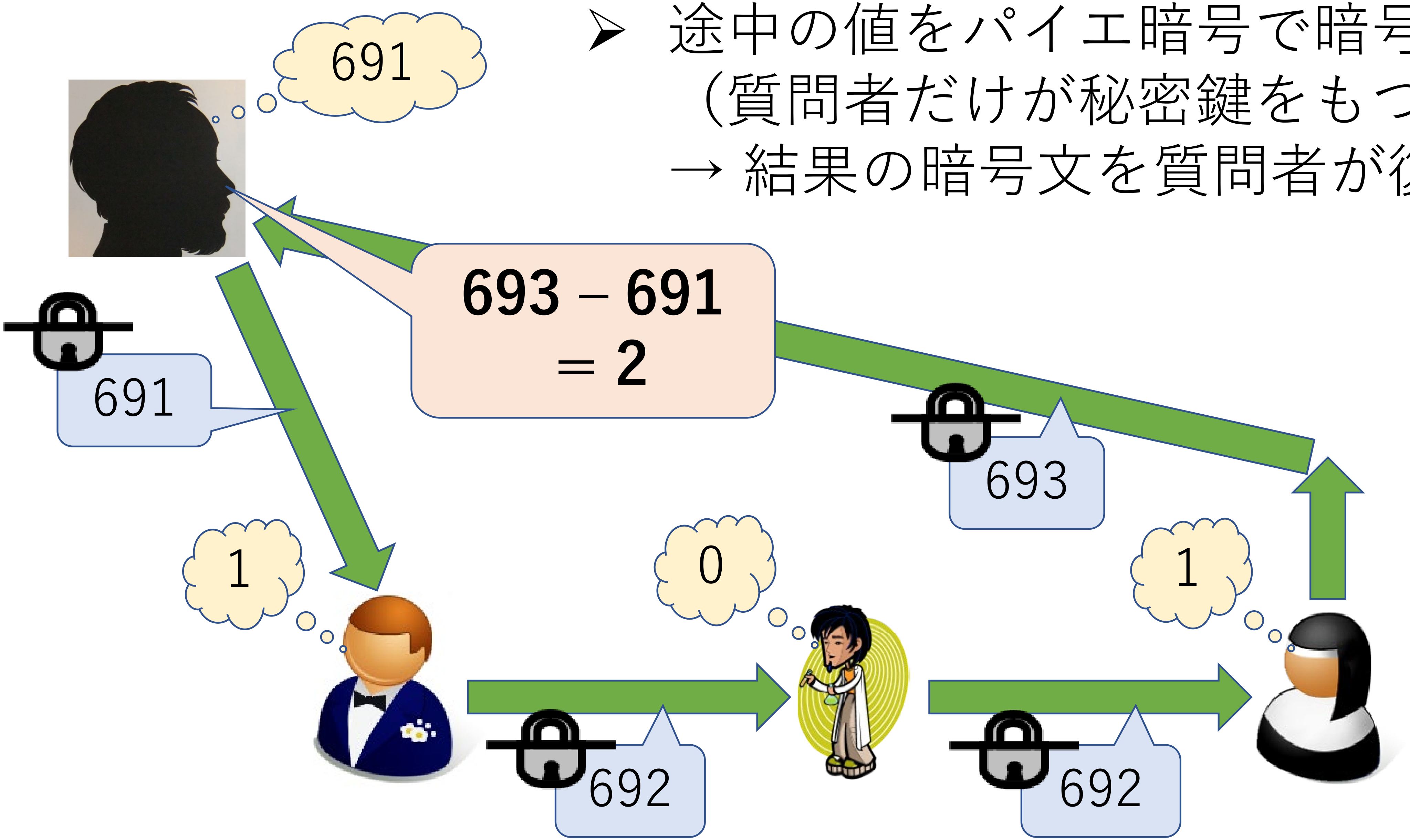
$$[[\boldsymbol{m}]] \coloneqq (\mathbf{1} + \boldsymbol{N})^{\boldsymbol{m}} \boldsymbol{r}^{\boldsymbol{N}} \ \mathbf{mod}\ \boldsymbol{N}^{\mathbf{2}}$$

$$\boxed{[[\boldsymbol{m}_{\mathbf{1}}]] \cdot [[\boldsymbol{m}_{\mathbf{2}}]] = [[\boldsymbol{m}_{\mathbf{1}} + \boldsymbol{m}_{\mathbf{2}}]]}$$

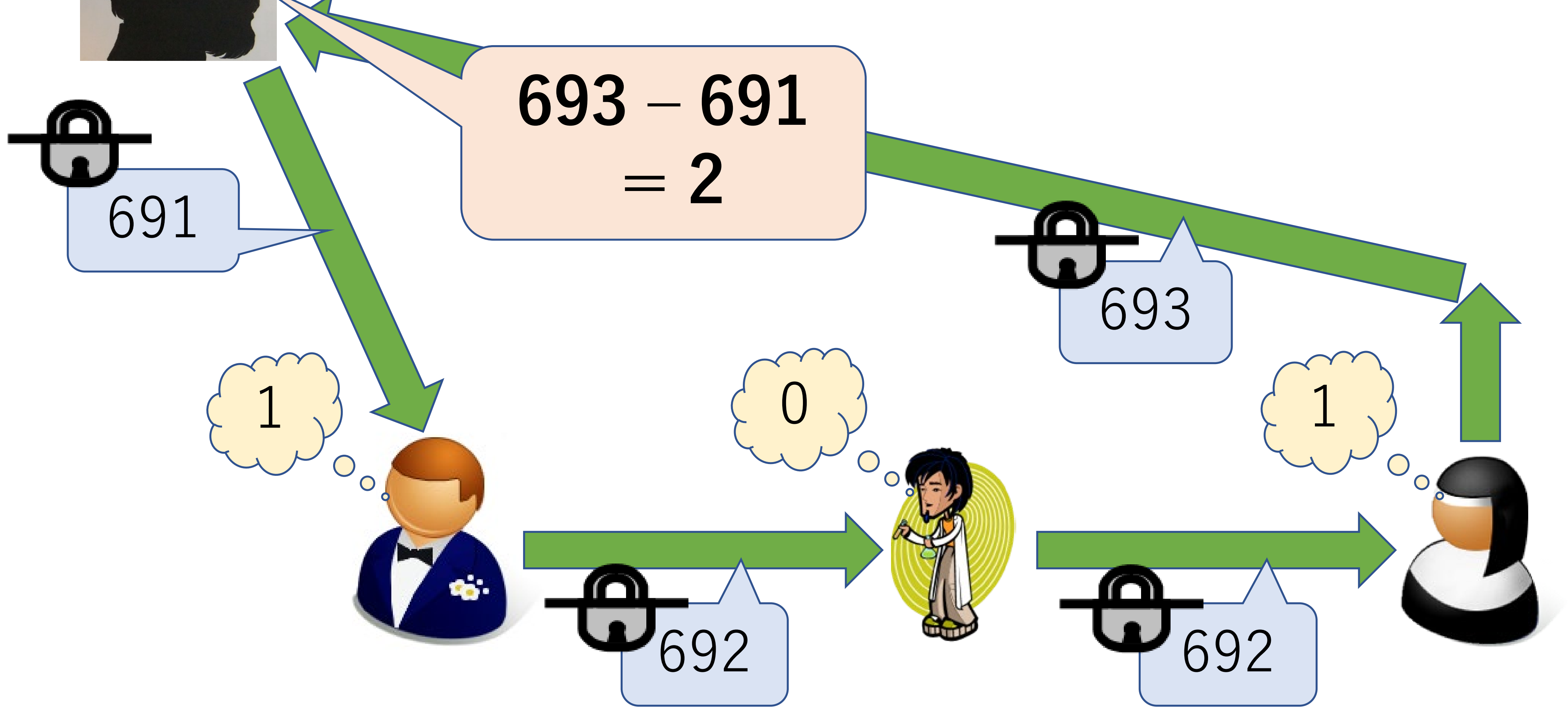
↑「暗号化したまま中身を足し算できる」

：（**加法**）**準同型暗号**

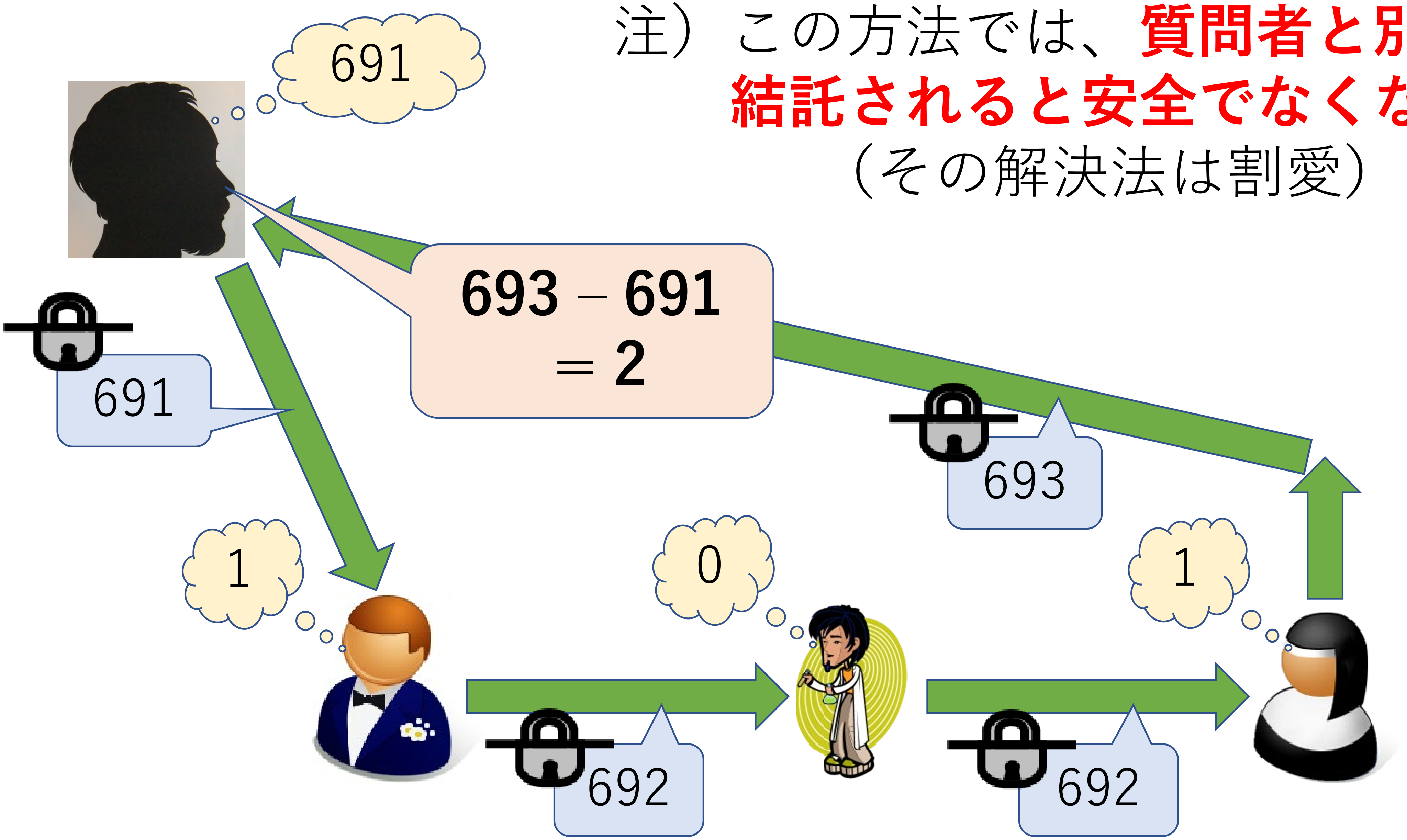
- 途中の値をパイエ暗号で暗号化
  （質問者だけが秘密鍵をもつ）
  → 結果の暗号文を質問者が復号



とが協力（結託）しても
の答えが**暗号化されていて不明**
→ **安全性が強化**された



注）この方法では、**質問者と別の人に結託されると安全でなくなる**
（その解決法は割愛）



別の秘密計算の例

～（簡単な）秘匿検索～

修学旅行の写真あるよー

任意のクラスメイトに対して
ある写真が存在して
そのクラスメイトが写ってるよー

１枚ください

まいどあり
誰の写真ですか？

え～♥
それはヒミツ♥

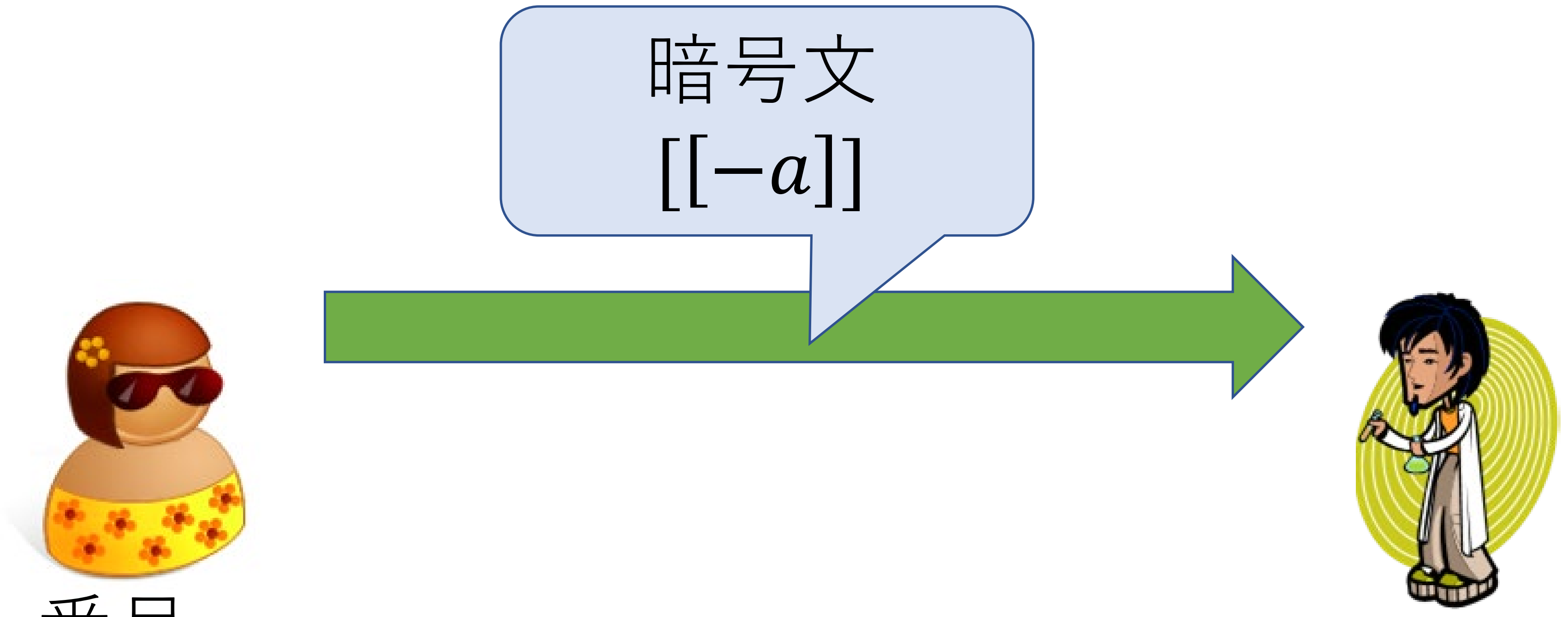
無茶言うな

方法

- 欲しい写真の番号 a
- 準同型暗号の復号鍵

- 写真の番号 b
- 写真データ m

- $a = b$ **のときだけ** m を渡したい
- a **は秘密にしたい**（「紛失通信」）



番号a
復号鍵

番号b　データm
公開鍵

暗号文
$[[-a]]$

$[[r(b-a)+m]]$
を計算
（rは乱数）

番号a
復号鍵

番号b　データm
公開鍵

暗号文
$[[-a]]$

$[[r(b-a)+m]]$
を計算
（rは乱数）

番号a
復号鍵

$[[r(b-a)+m]]$

番号b　データm
公開鍵

$r(b-a)+m$

復号

番号a
復号鍵

暗号文
$[[-a]]$

$[[r(b-a)+m]]$
を計算
（rは乱数）

$[[r(b-a)+m]]$

番号b　データm
公開鍵

計算の正しさ

$a = b \rightarrow$ 結果は m
（正しいデータ）

$r(b-a)+m$

暗号文
$[[-a]]$

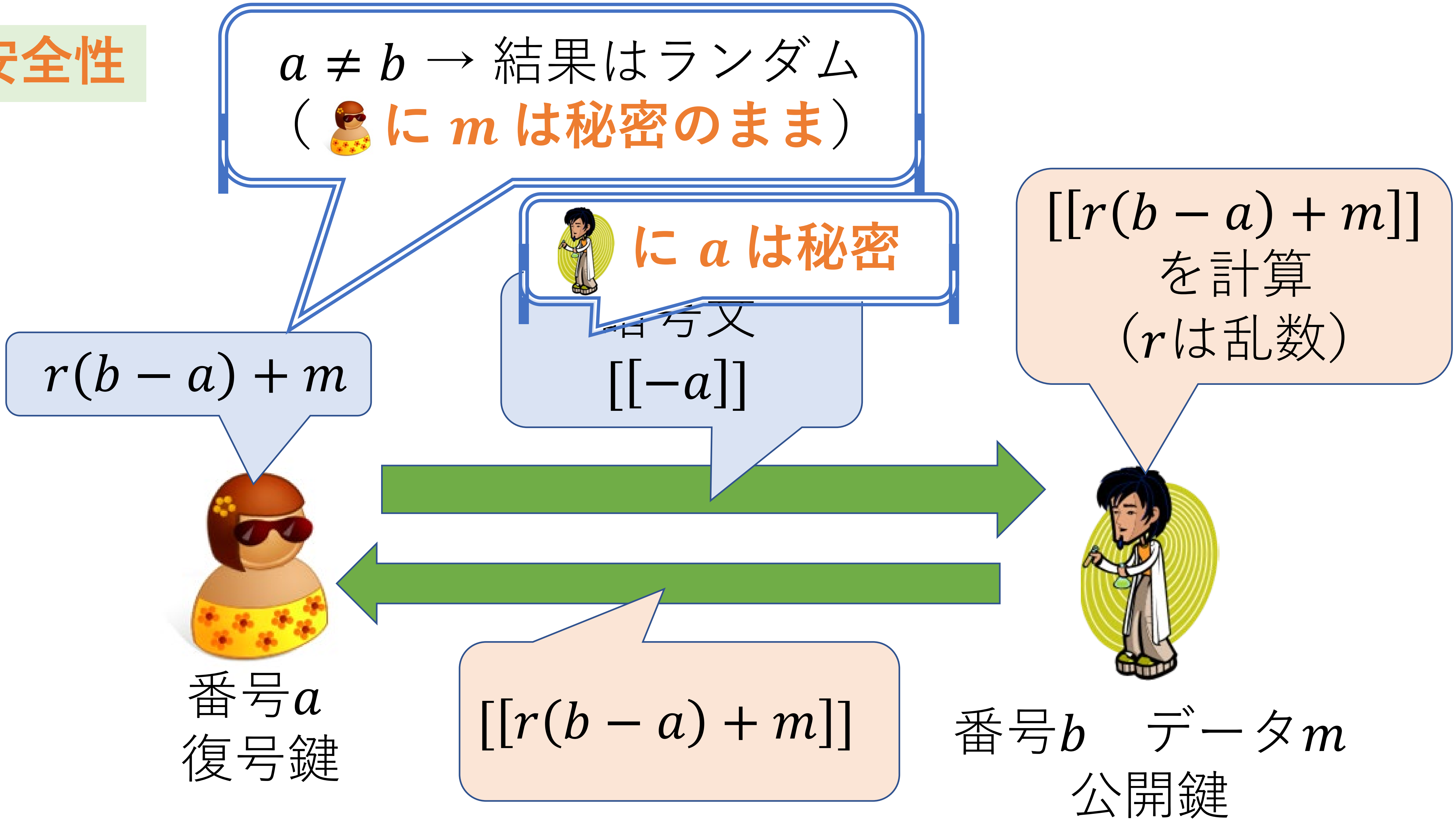
$[[r(b-a)+m]]$
を計算
（rは乱数）

番号a
復号鍵

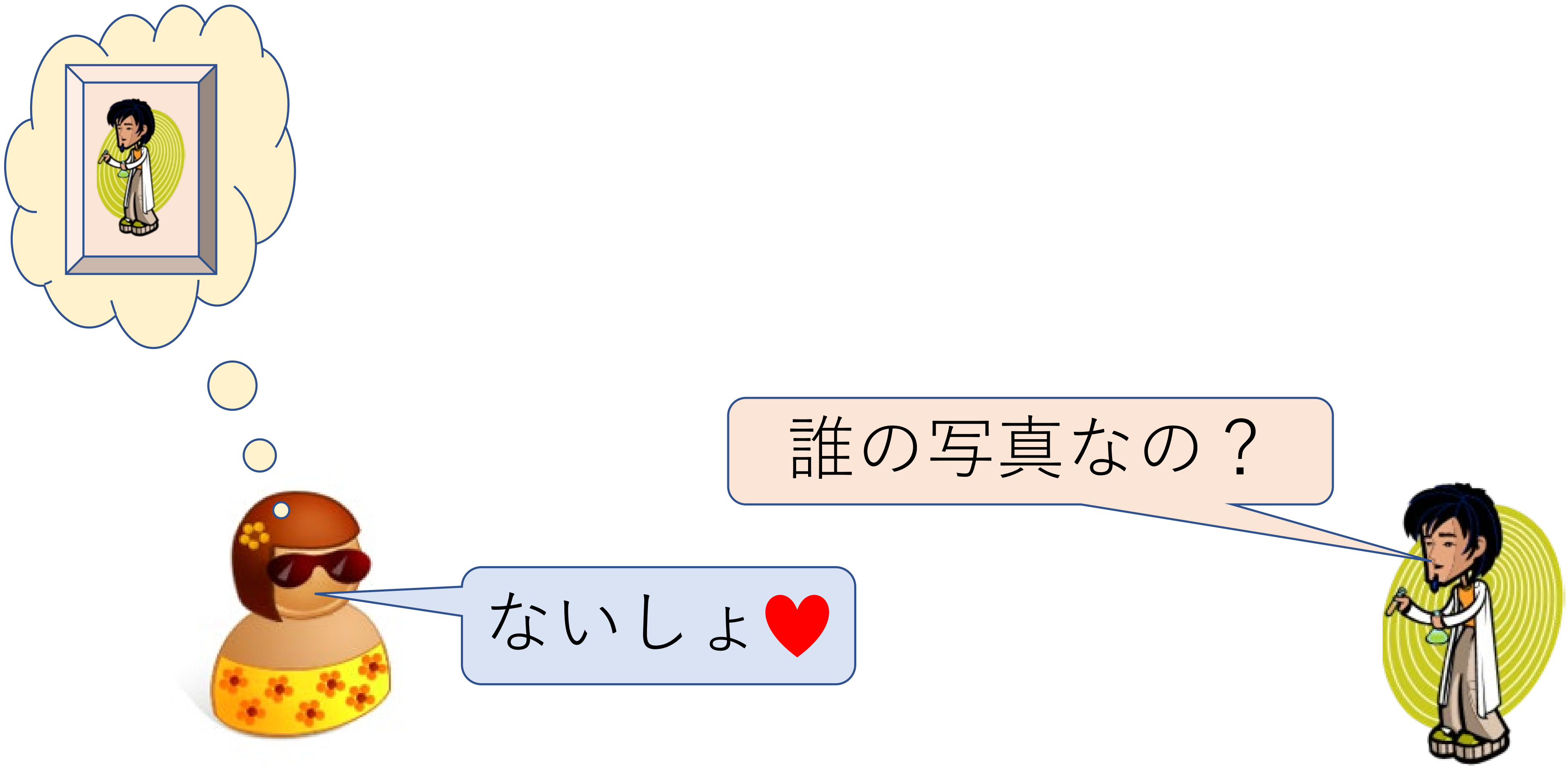
$[[r(b-a)+m]]$

番号b　データm
公開鍵

安全性



$a \neq b \to$ 結果はランダム
（ に m は秘密のまま）
に a は秘密
$r(b-a)+m$
$[[-a]]$
$[[r(b-a)+m]]$
を計算
（rは乱数）
$[[r(b-a)+m]]$
番号a
復号鍵
番号b　データm
公開鍵


誰の写真なの？
ないしょ♥

完全準同型暗号と
秘密計算

完全準同型暗号と秘密計算

- 暗号化のまま**任意の演算**ができる
  → **より複雑な秘密計算**を実現しやすい

[C. Gentry, STOC 2009]

完全準同型暗号と秘密計算

- 暗号化のまま**任意の演算**ができる
  → **より複雑な秘密計算**を実現しやすい
- 主に**足し算**と**掛け算**の組み合わせで秘密計算を行う
  - つまり、関数を**多項式**で表示することになる

- 応用の研究例：機械学習、遺伝子配列解析、…
- （ただし、まだわりと効率が悪い → 重点的研究課題）

完全準同型暗号と秘密計算

- 暗号化のまま**任意の演算**ができる
  → **より複雑な秘密計算**を実現しやすい
- 主に**足し算**と**掛け算**の組み合わせで秘密計算を行う
  - つまり、関数を**多項式**で表示することになる

- 関数の多項式表示の性質の例：
  奇素数pについて、p進法で表示された整数の
  掛け算における繰り上がりの値を与える関数が
  ベルヌーイ数を用いて表示される

秘密計算と乱数と「病的な反例」

暗号技術と疑似乱数

- 暗号技術では**乱数**が多用される
- 理想的な乱数（厳密な一様乱数）は
  理論的に扱いやすいが**実装上は高コスト**

暗号技術と疑似乱数

- 暗号技術では**乱数**が多用される
- 理想的な乱数（厳密な一様乱数）は
  理論的に扱いやすいが**実装上は高コスト**
- **暗号学的疑似乱数**：厳密な一様乱数ではないが、
  厳密な一様乱数と「計算量的に識別不可能」
  - 「現実的な時間では両者の見分けがつかない」

暗号技術と疑似乱数

- 暗号技術では**乱数**が多用される
- 理想的な乱数（厳密な一様乱数）は
  理論的に扱いやすいが**実装上は高コスト**

- 暗号技術設計の方法論：
  理想的な乱数を仮定して暗号方式を設計し、
  実装の際には暗号学的疑似乱数に置き換える

暗号技術と疑似乱数

- 暗号学的疑似乱数の安全性は、
  暗号方式が**「理想的な乱数のとき安全」であれば**
  「暗号学的疑似乱数に置き換えた実装も安全」と
  なることを期待して定義されている

暗号技術と疑似乱数

- 暗号学的疑似乱数の安全性は、
  暗号方式が**「理想的な乱数のとき安全」であれば**
  「暗号学的疑似乱数に置き換えた実装も安全」と
  なることを期待して定義されている
- 暗号分野の専門家にとっては直感的に妥当な期待
  - 大抵の種類の暗号技術では実際に成立（証明可能）

暗号技術と疑似乱数

- 暗号学的疑似乱数の安全性は、
  暗号方式が**「理想的な乱数のとき安全」であれば「暗号学的疑似乱数に置き換えた実装も安全」**と
  なることを期待して定義されている
- 暗号分野の専門家にとっては直感的に妥当な期待
  - 大抵の種類の暗号技術では実際に成立（証明可能）
- しかし、**すべての暗号技術の種類について成立すると証明されたわけではない**

疑似乱数と秘密計算の安全性

- 話者の研究：秘密計算では、（単体では安全な）暗号学的疑似乱数を用いて実装したときに**安全でなくなってしまう場合が存在**する
  - このことを示す**「病的な」反例**を実際に構成（数学者としての**<u>技能</u>**が活用された事例）

[<u>N</u>., PKC 2021]

疑似乱数と秘密計算の安全性

- 話者の研究：秘密計算では、（単体では安全な）暗号学的疑似乱数を用いて実装したときに**安全でなくなってしまう場合が存在**する
  - このことを示す**「病的な」反例**を実際に構成（数学者としての**技能**が活用された事例）

[N., PKC 2021]

- 注）ある**仮定を満たす暗号学的疑似乱数を用いれば安全性が保たれる**ことを後続研究で証明

[N. Heseri and N., IWSEC 2022]

暗号×数学