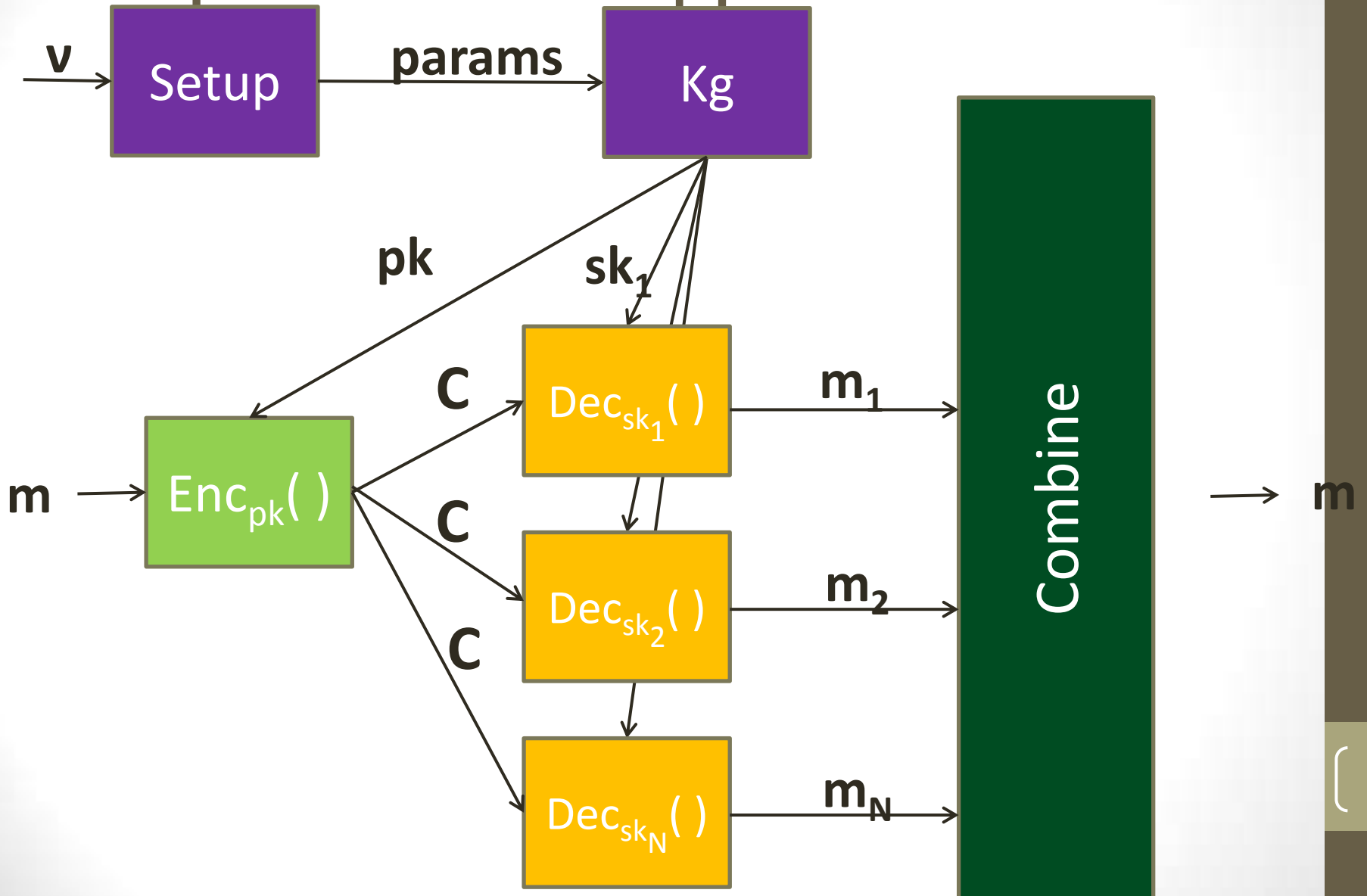


ПОДСЧЕТ ГОЛОСОВ БЕЗ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ

Пороговое шифрование



Пороговое шифрование

- **Описание:**

- **Key Generation(n, k):**
outputs $pk, vk, (sk_1, sk_2, \dots, sk_n)$
- **Encrypt(pk, m):** outputs a ciphertext C
- **Decrypt(C, sk_i):** outputs m_i
- **ShareVerify(pk, vk, C, m_i):** outputs accept/reject
- **Combine($pk, vk, C, \{m_{i_1}, m_{i_2}, \dots, m_{i_k}\}$):** outputs m

ElGamal

- **Setup(v)**: выбрать м. группу (G, \cdot) и ее генератор g
- **KG(G, g)**:
 $x \leftarrow \{1, \dots, |G|\};$
 $X \leftarrow g^x$
output (X, x)
- **ENC_x(m)**:
 $r \leftarrow \{1, \dots, |G|\};$
 $(R, C) \leftarrow (g^r, g^m X^r);$
output (R, C)
- **DEC_x((R, C))**: найти t такое что $g^t = C/R^x$
output $m=t$

(k,n) пороговая схема ElGamal

- Генерация ключей :
 - s_1, s_2, \dots, s_n по схеме Шамира.
 - Публичный ключ $X = g^s$ the verification key ключи проверок $X_1 = g^{s_1}, X_2 = g^{s_2}, \dots, X_n = g^{s_n}$.
 - Участнику i выдают $s_i = P(i)$
- Частичное дешифрование $(s_i, (R, C))$:
 - Сторона i вычисляет $m_i = R^{s_i}$
- Сбор $((R, C), m_1, \dots, m_N)$:
$$R^s = R^{P(0)} = R^{\sum s_i \prod_{j \in I - \{i\}} (-j)/(i-j)} = \prod R^{s_i c_i}$$
где $c_j = \prod_{i \in I - \{j\}} (-j)/(i-j)$ (произведение по $i \in I - \{j\}$)

Mixnets

- Использование гомоморфных ф-ций сложно для сложных ф-ций
 - Вместо этого $\text{Enc}_{pk}(f(v_1, v_2, \dots, v_n))$ можно просто расшифровать голоса

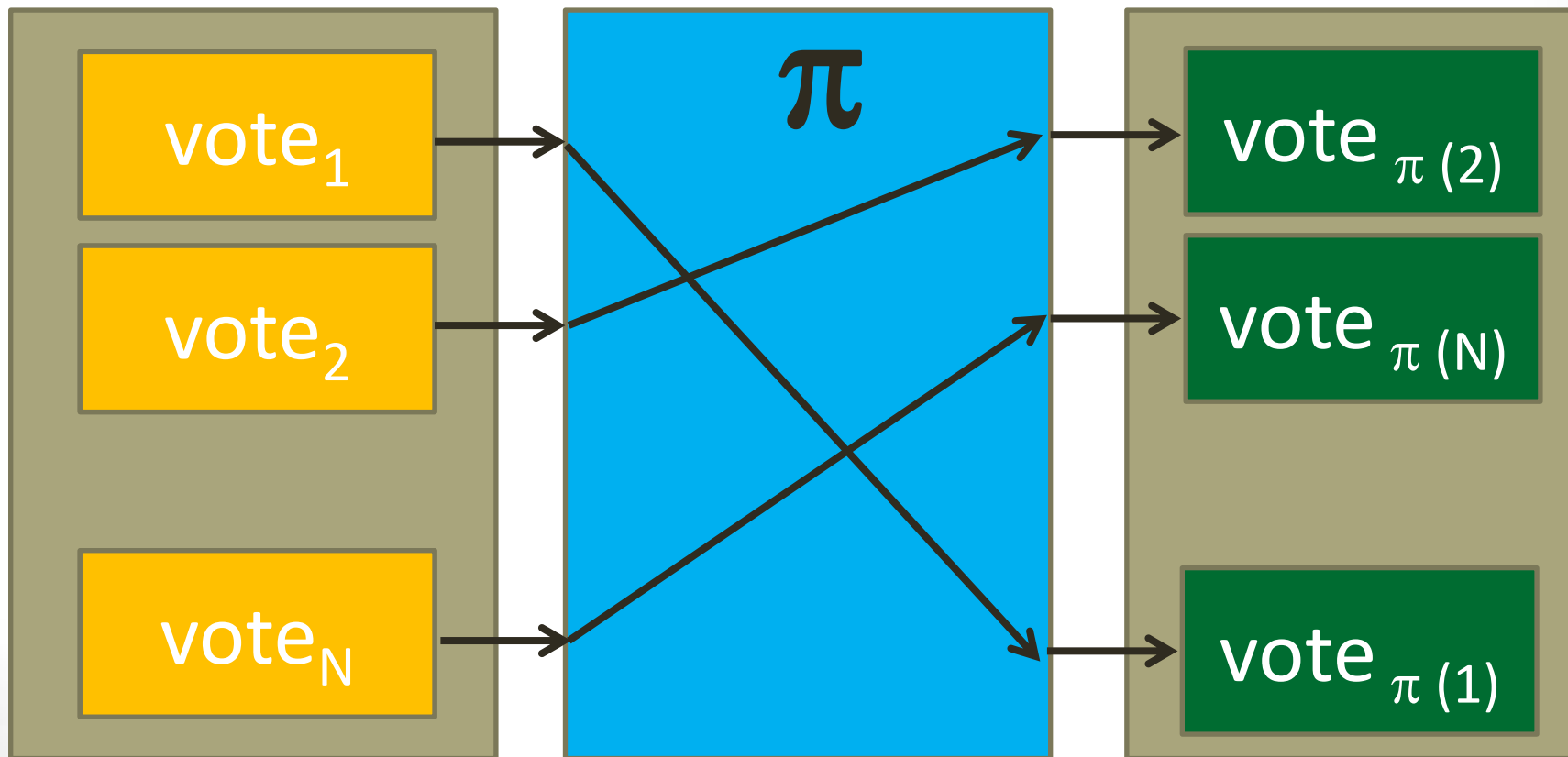
Дополнительная рандомизация



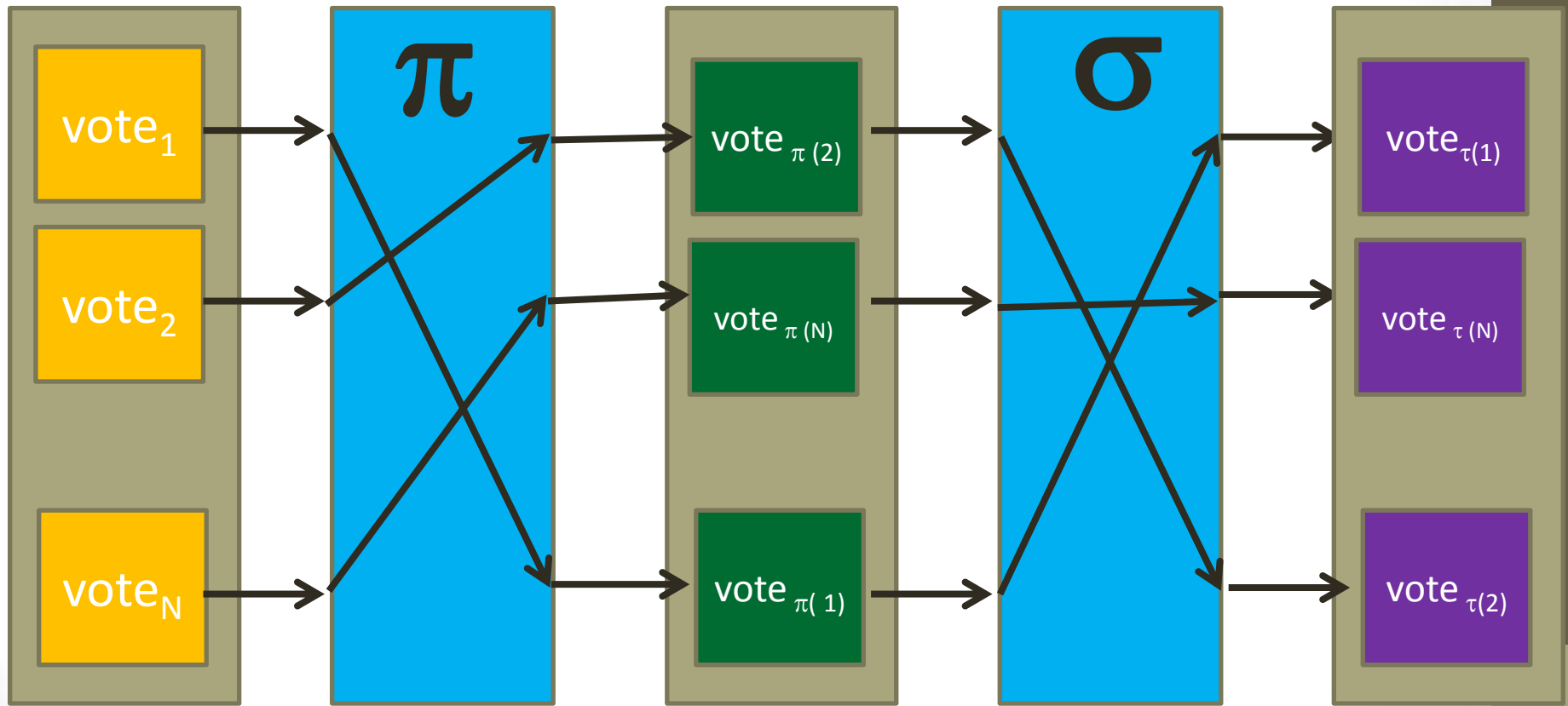
$$\text{Enc}_{pk}(m;r) \bullet \text{Enc}_{pk}(0;s) = \text{Enc}_{pk}(m;r+s)$$

$$(g^r, g^m X^r) \cdot (g^s, g^0 X^s) = (g^{r+s}, g^m X^{r+s})$$

Mixnet



Mixnet



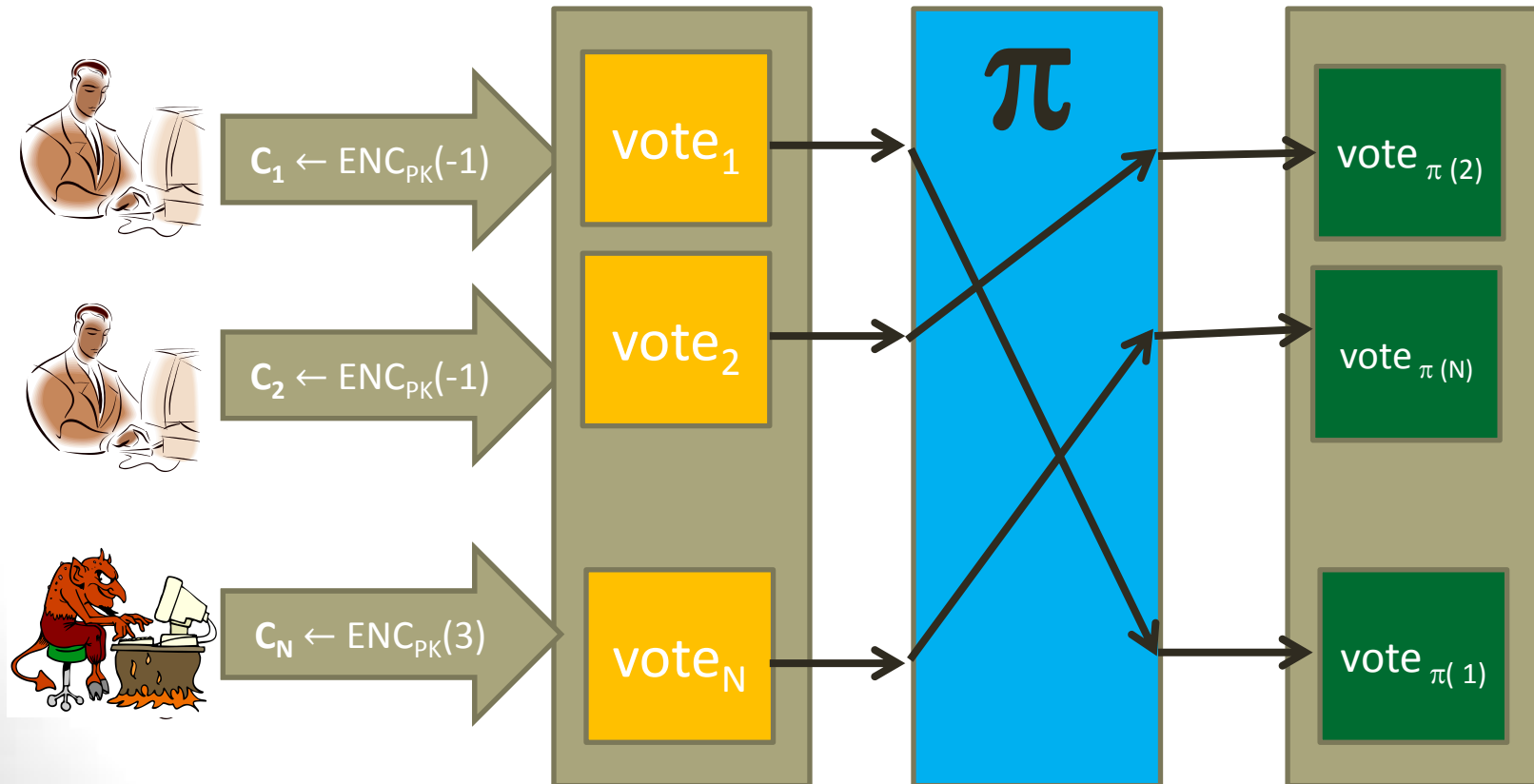
$$\tau = \pi; \sigma$$

Атака со стороны голосующих

ВВ



SK

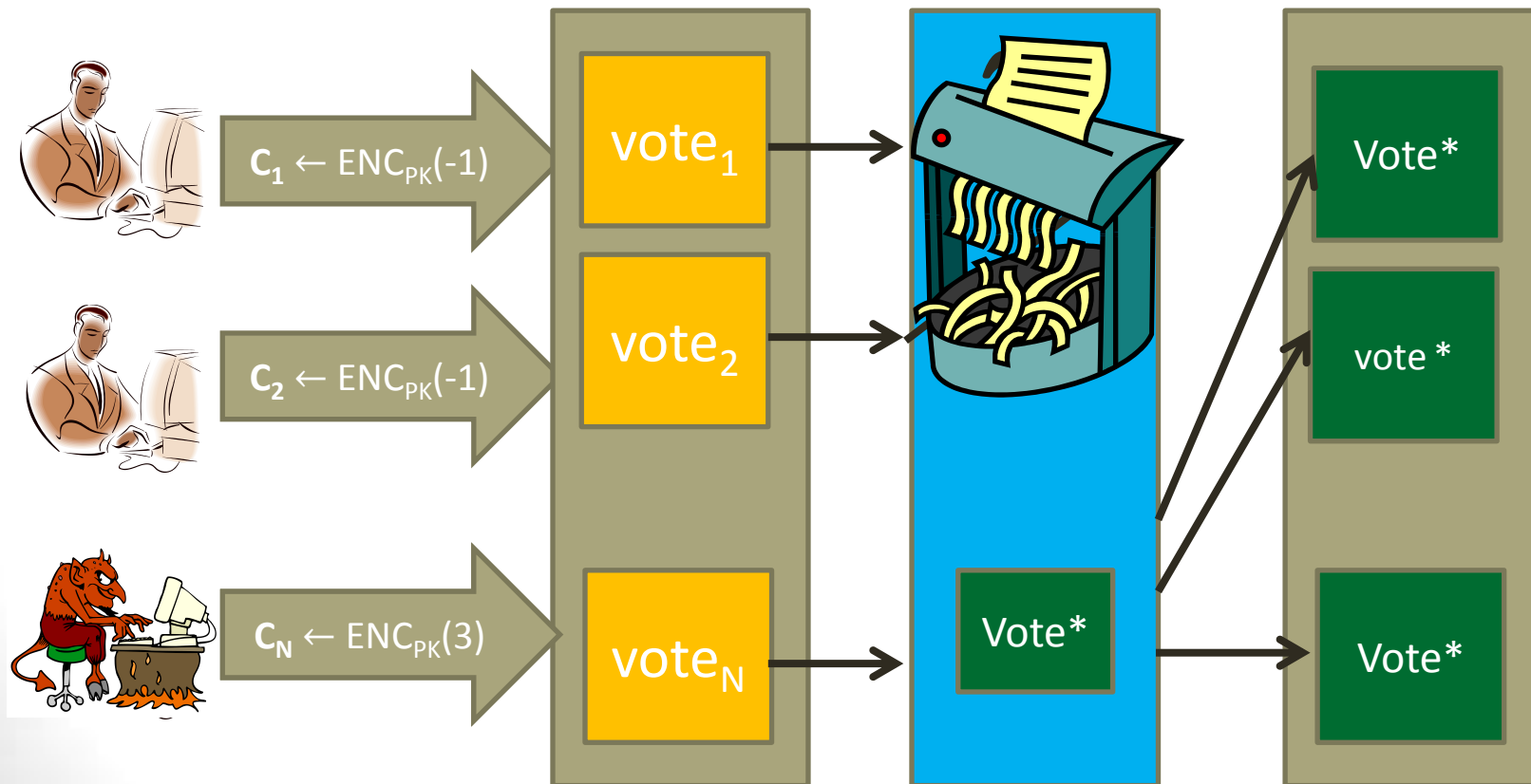


Атака со стороны перестановочной сети

ВВ

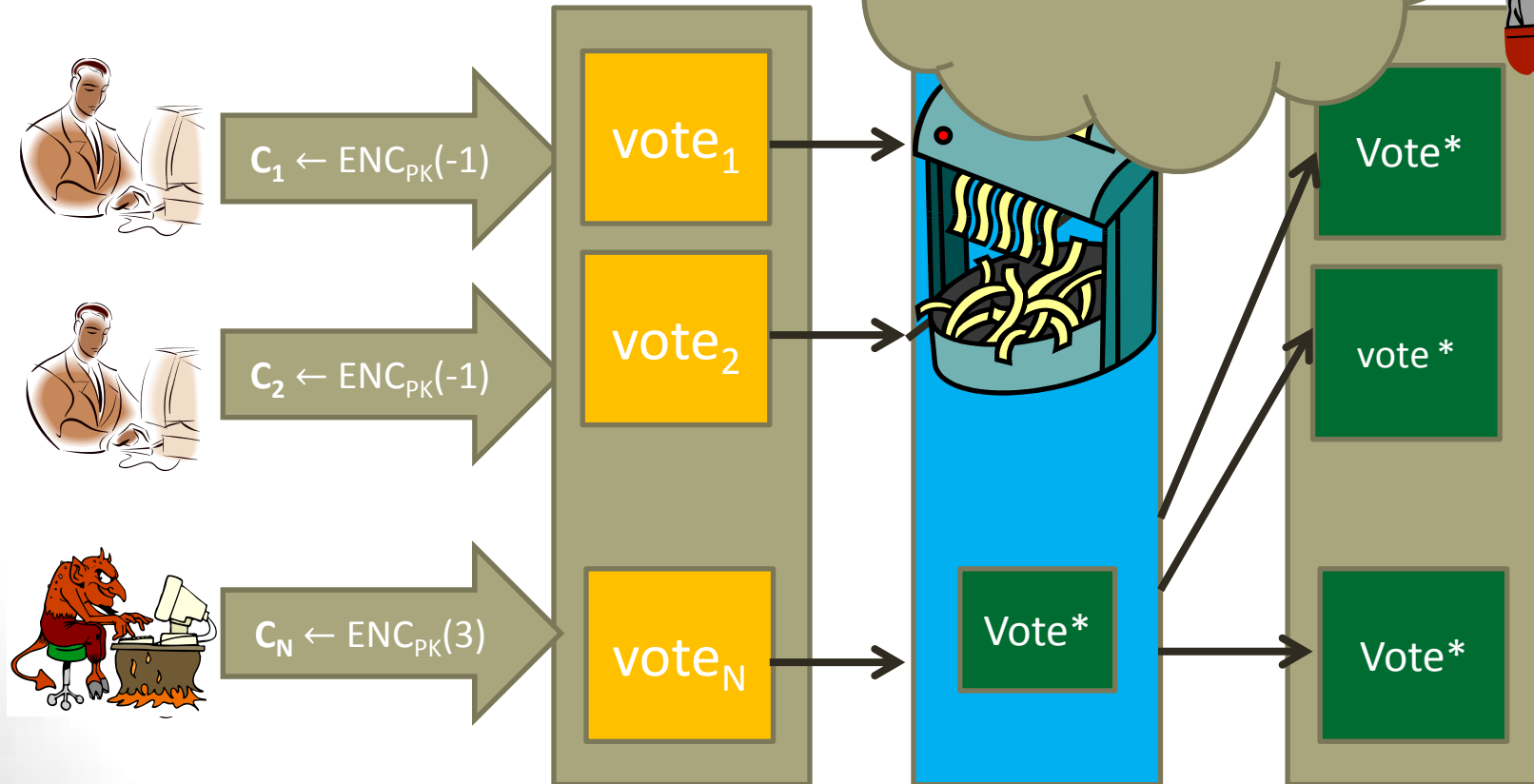


SK



Атака со стороны

Голосующие
ничего не решают.
Все решают люди,
подсчитывающие
голоса



Угрозы

- **Голосующие:** плохо отформатированные голоса; проблематично для гомоморфного подсчета
- **Перемешивающий сервер:** может полностью подменить бюллетени
- **ЦИК:** может врать про результаты подсчетов

ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Интерактивное

СВИДЕТЕЛЬСТВО [GMW91]

Хочет убедить Verifier в каком-то свойстве X . Формально, что $: \text{Rel}(X, w)$ для некоторого w .
Например: что знает такое w

Accept/
Reject

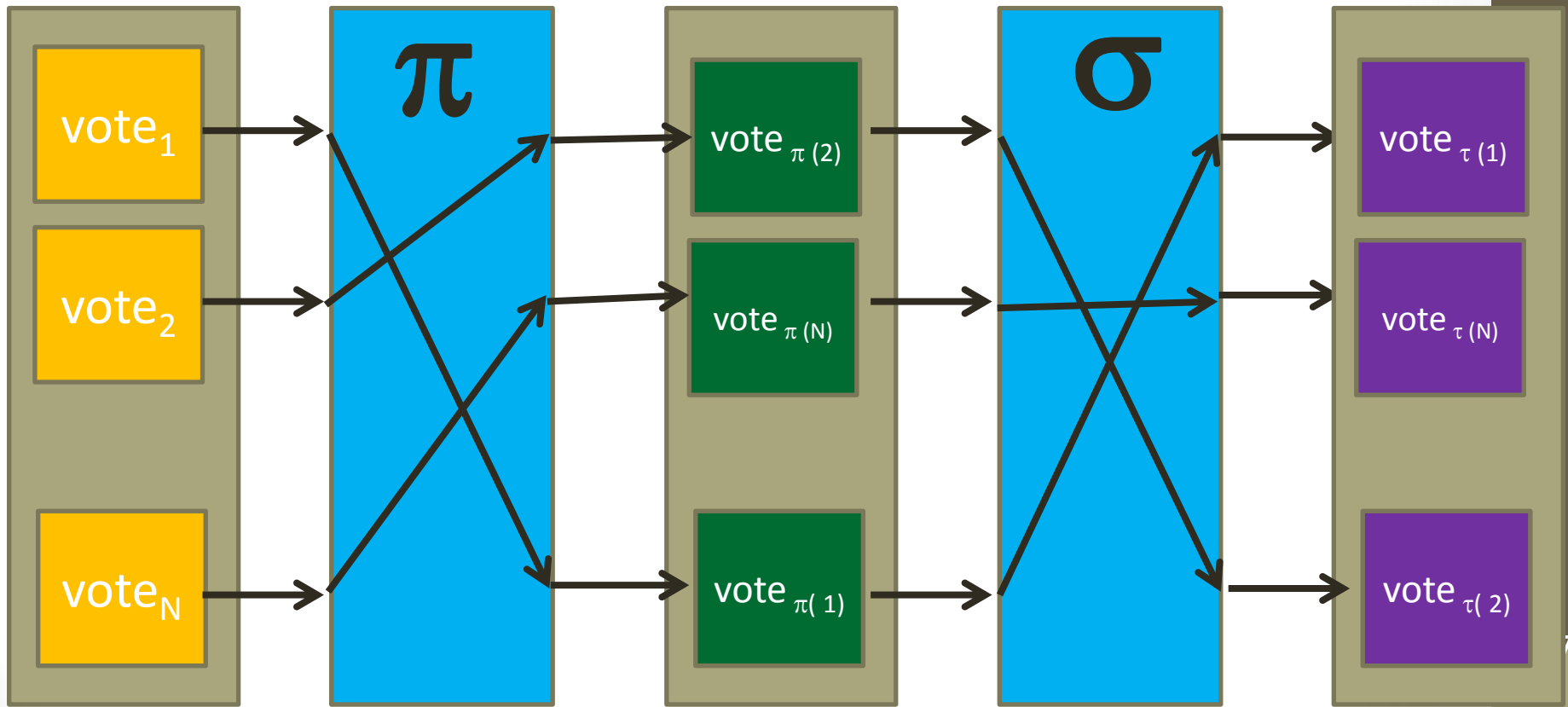
Примеры:

- $\text{Rel}_{g,h}((X,Y),z)$ iff $X=g^z$ and $Y=h^z$
- $\text{Rel}_{g,X}((R,C),r)$ iff $R=g^r$ and $C=X^r$
- $\text{Rel}_{g,X}((R,C),r)$ iff $R=g^r$ and $C/g=X^r$
- $\text{Rel}_{g,X}((R,C),r)$ iff $(R=g^r$ and $C=X^r)$ or $(R=g^r$ and $C/g=X^r)$
- $\text{Rel}_L(X,w)$ iff $X \in L$

Свойства

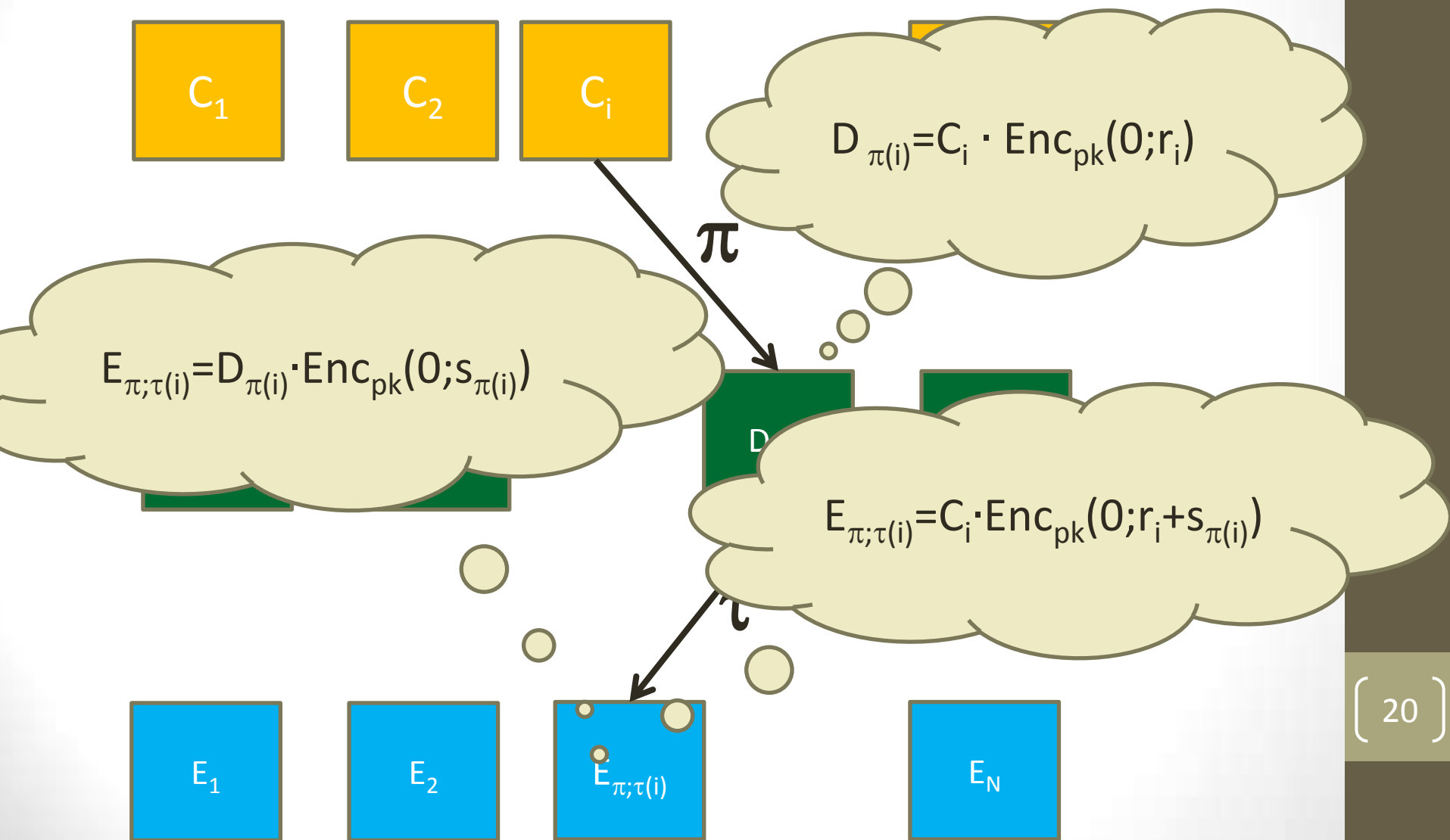
- **Полнота:** честный Prover всегда докажет честному Verifier правильность утверждения
- **Soundness:** нечестный Prover может обманывать только с очень малой вероятностью
- **Zero knowledge:** Никакая дополнительная информация не разглашается
- **Proof of knowledge:** из успешной проверки можно извлечь свидетеля

Mixnet



$$\tau = \pi; \sigma$$

Проверяемая перестановка



Проверяемая перестановка [KS95]

- Prover знает $C_1, C_2, \dots, C_n, D_1, D_2, \dots, D_n$, перестановку π и случайные монеты r_1, r_2, \dots, r_n такие что $D_i = C_{\pi(i)} \cdot \text{Enc}_{pk}(0; r_i)$
- Prover выбирает перестановку τ и случайные s_1, s_2, \dots, s_n и потом он вычисляет и отправляет $\{E_{\pi; \tau(i)} = D_{\pi(i)} \cdot \text{Enc}_{pk}(0; s_{\pi(i)})\}_i$
- Verifier выбирает случайный бит b и отправляет его Prover
- Prover отвечает следующим образом
 - If $b=0$ then посылает $(\pi; \tau)$ и $r_1 + s_{\pi(1)}$
 - If $b=1$ then посылает $\tau, s_1, s_2, \dots, s_n$
- Когда verifier получил $\sigma, q_1, q_2, \dots, q_n$ он проверяет равенства:
 - If $b=0$: $E_{(\pi; \tau)(i)} = C_i \cdot \text{Enc}_{pk}(0; r_i)$
 - If $b=1$: $E_{\tau(i)} = D_i \cdot \text{Enc}_{pk}(0; r_i)$

Helios

helios

IACR Elections 2012

public election created by  David Pointcheval

[Share](#) [Tweet](#)

Election of the IACR Directors

[questions \(1\)](#) | [voters & ballots](#) | [trustees \(3\)](#)

This election is complete.

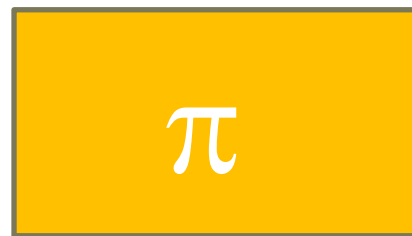
Tally

Question #1
Director

Thomas Peyrin	166
Anna Lysjanskaya	270
Thomas Berson	226
Michel Abdalla	242
Xavier Boyen	157

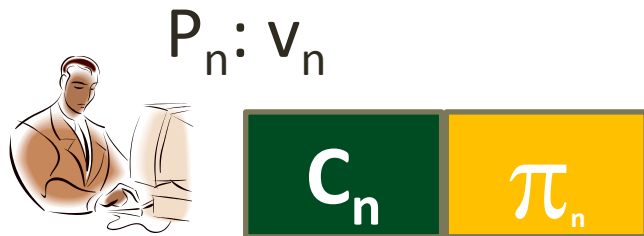
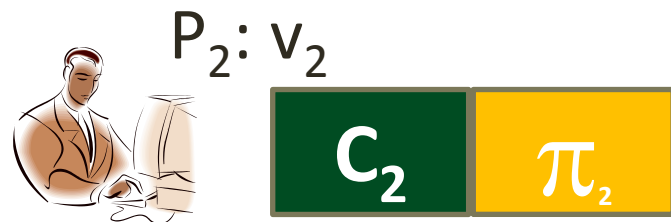
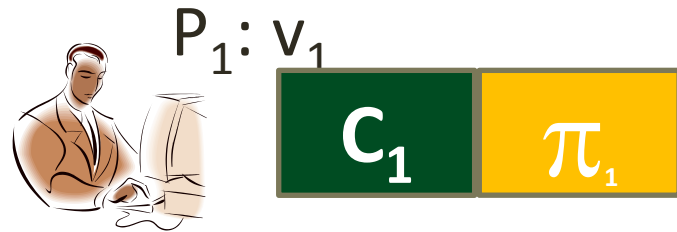
Helios: Подготовка голоса

$P: v$

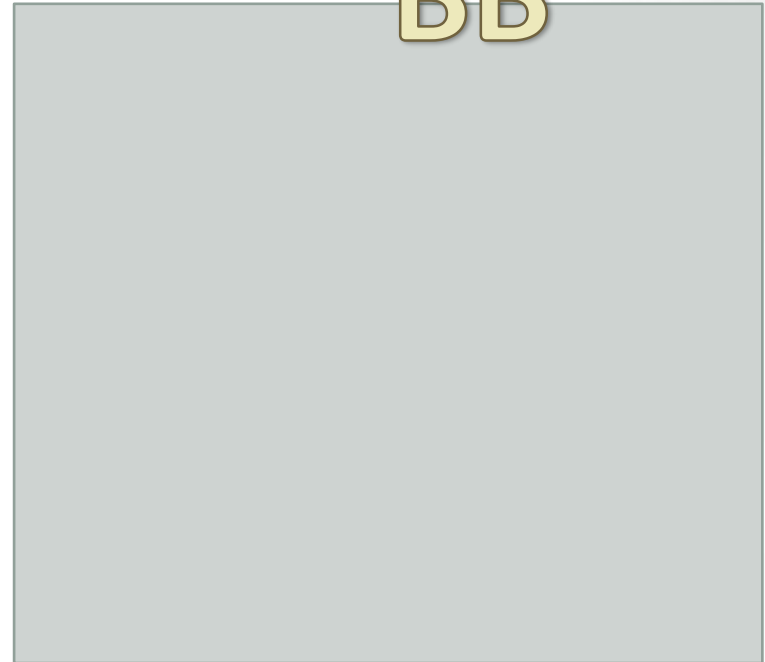


- $C = ENC_{PK}(v)$ шифрование голоса на публичном ключе для данных выборов
- π доказательство, что C верно

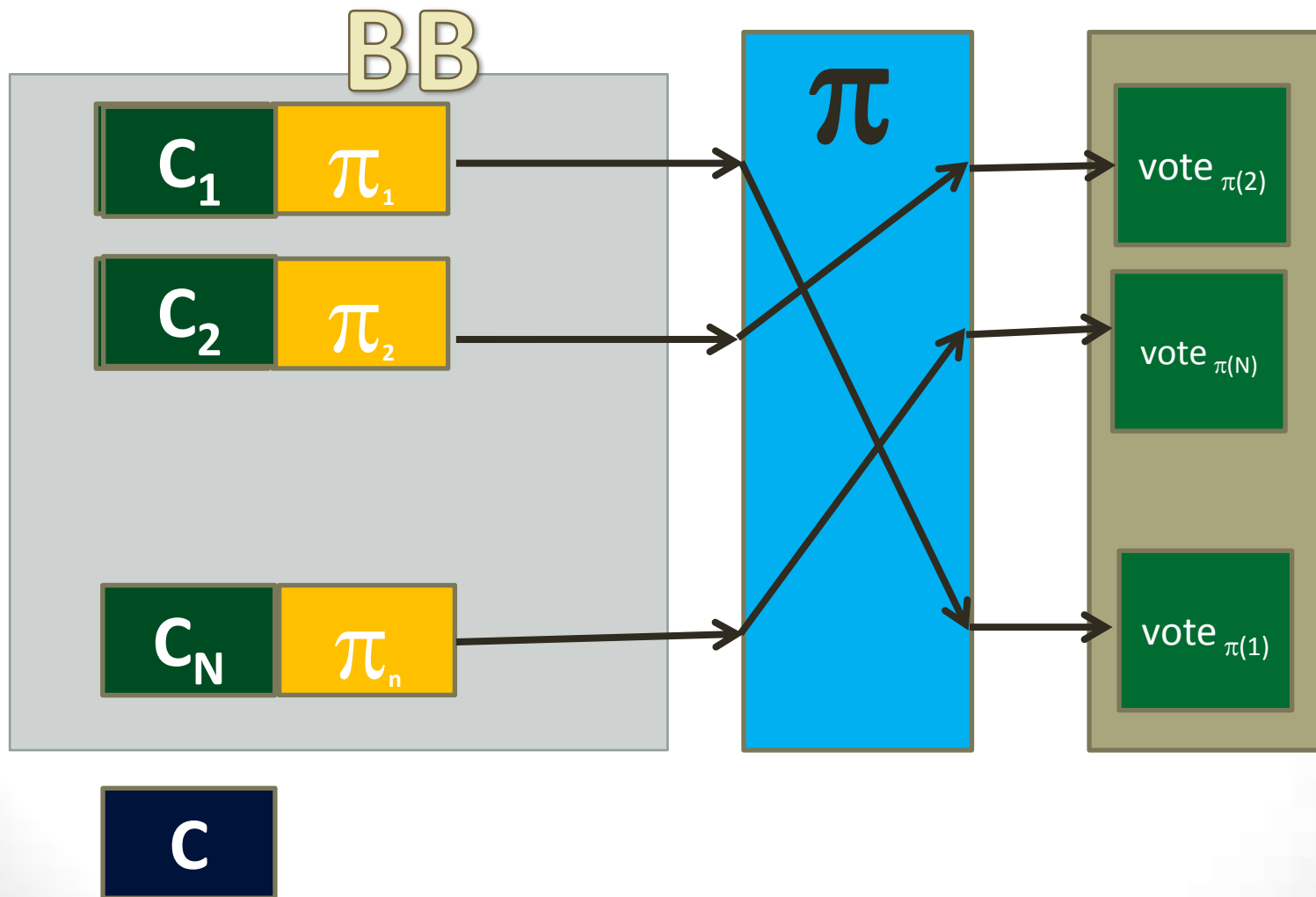
Helios: voting



BB




Helios: Подсчет голосов

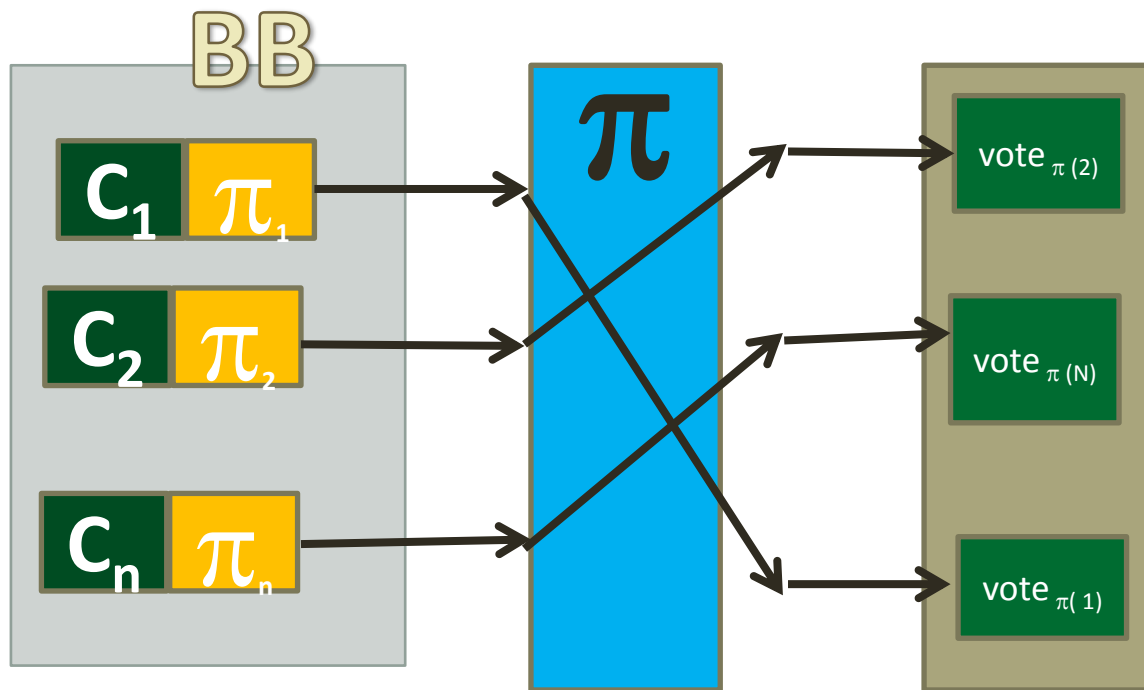


Helios

 $P_1: v_1$

 $P_2: v_2$

 $P_n: v_n$



C

