Электронные выборы

Лекция N 3 курса
“Современные задачи криптографии”

Юрий Лифшиц
yura@logic.pdmi.ras.ru

СПбГУ — SPRINT Lab

Осень’2005

“...всеобщее голосование бессмысленно. ...Вы, вероятно, согласитесь со мной, что гениальные люди встречаются редко, не правда ли? Но будем щедры и допустим, что во Франции их сейчас имеется человек пять. Прибавим, с такой же щедростью, двести высокоталантливых людей, тысячу других, тоже талантливых, каждый в своей области, и десять тысяч человек так или иначе выдающихся. Вот вам генеральный штаб в одиннадцать тысяч двести пять умов. За ним идет армия посредственности, за которой следует вся масса дурачья. А так как посредственность и дураки всегда составляют огромное большинство, то немыслимо представить, чтобы они могли избрать разумное правительство."

Г. де Мопассан. “Обед и несколько мыслей”

План лекции

1. **Постановка задачи**
2. **Примитивы и идеи**
   - Криптографические примитивы
   - Идеи для электронных выборов
3. **Два протокола электронных выборов**
   - Протокол Шаума
   - FOO-схема для выборов

План лекции

1. **Постановка задачи**
2. Примитивы и идеи
   - Криптографические примитивы
   - Идеи для электронных выборов
3. Два протокола электронных выборов
   - Протокол Шаума
   - FOO-схема для выборов

Мотивация

Ключевые преимущества

- Дешевые выборы
- Мобильность
- Проверяемость результатов

Мотивация

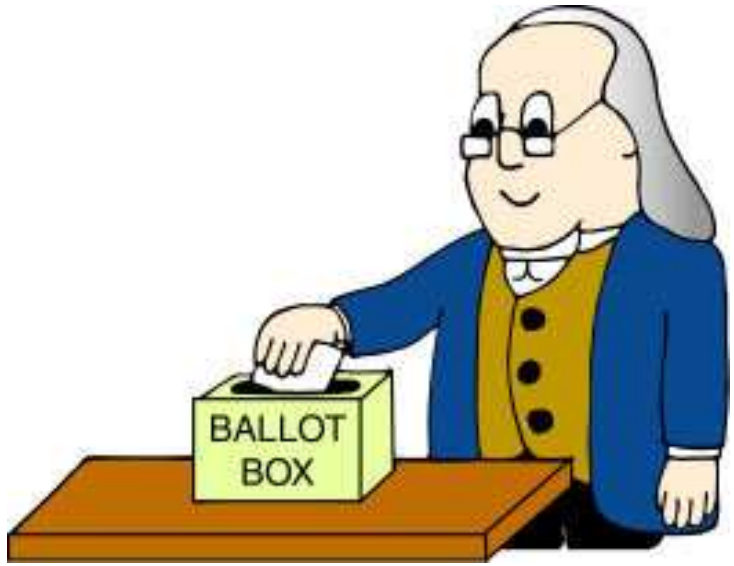
Ключевые преимущества

- Дешевые выборы
- Мобильность
- Проверяемость результатов

Возможное внедрение

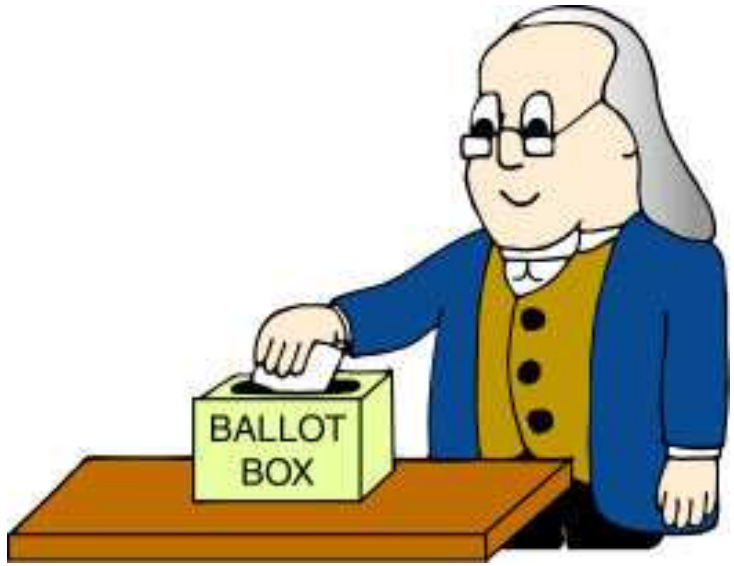
- Штат Аризона
- Дания
- Эстония

Типы выборов



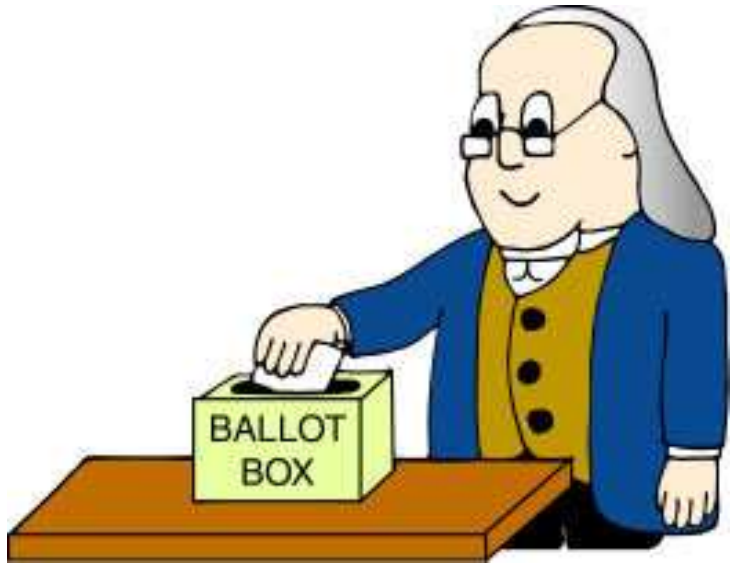
- Да / Нет

Типы выборов



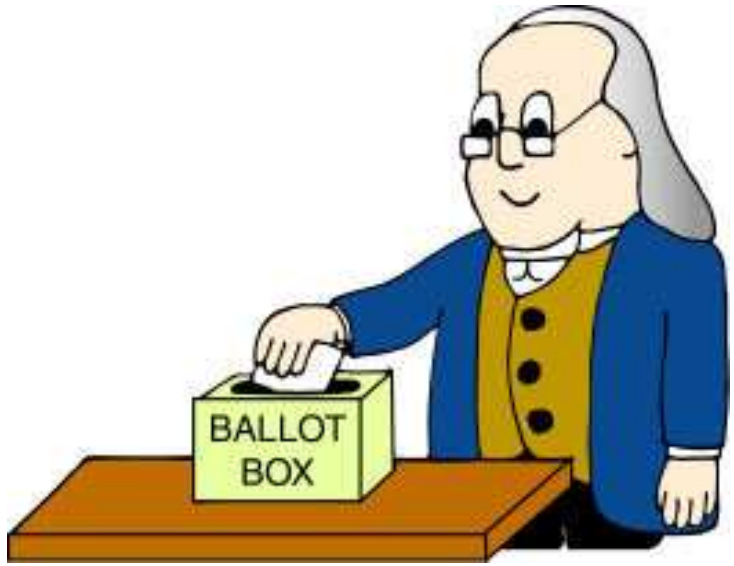
- Да / Нет
- “1 из L”

Типы выборов



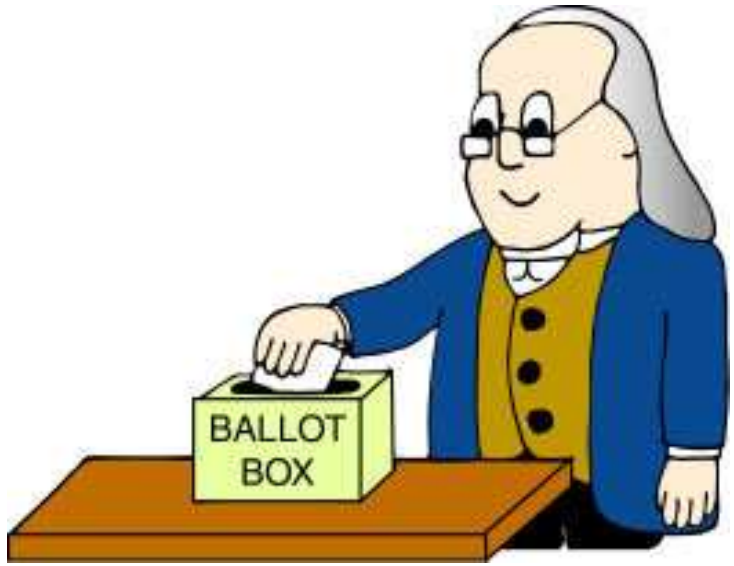
- Да / Нет
- “1 из L”
- “K из L”

Типы выборов



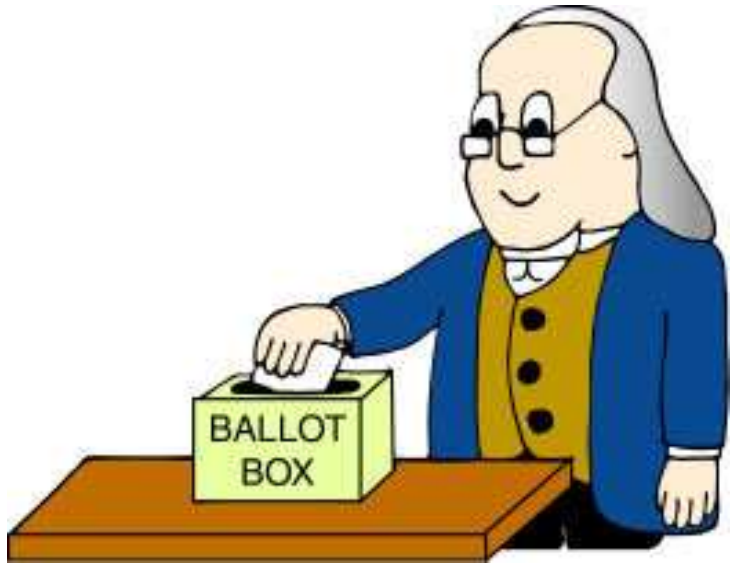
- Да / Нет
- “1 из L”
- “K из L”
- Упорядоченный вариант “K из L”

Типы выборов



- Да / Нет
- “1 из L”
- “K из L”
- Упорядоченный вариант “K из L”
- “1-L-K” — выбрать K элементов из одного из L списков

Типы выборов



- Да / Нет
- “1 из L”
- “K из L”
- Упорядоченный вариант “K из L”
- “1-L-K” — выбрать K элементов из одного из L списков
- Открытый ответ

Фазы выборов

Инициализация

- Объявляется вопрос
- Создается список голосующих
- Генерируются ключи для криптосистем

Фазы выборов

Инициализация

- Объявляется вопрос
- Создается список голосующих
- Генерируются ключи для криптосистем

Голосование

- Голосующие взаимодействуют с организаторами
- В итоге организаторы получают “электронный контейнер” с голосом

Фазы выборов

Инициализация

- Объявляется вопрос
- Создается список голосующих
- Генерируются ключи для криптосистем

Голосование

- Голосующие взаимодействуют с организаторами
- В итоге организаторы получают “электронный контейнер” с голосом

Подсчет голосов

- Организаторы вычисляют и публикуют результат выборов
- Желающие проверяют честность выборов

Требования к схеме выборов

- **Контроль над избирателями:** только те, кто в списке; только один голос на человека

Требования к схеме выборов

- **Контроль над избирателями:** только те, кто в списке; только один голос на человека
- **Тайна голосования:** нельзя узнать выбор конкретного избирателя

Требования к схеме выборов

- **Контроль над избирателями:** только те, кто в списке; только один голос на человека
- **Тайна голосования:** нельзя узнать выбор конкретного избирателя
- **Индивидуальный контроль:** можно проверить, что твой голос посчитан

Требования к схеме выборов

- **Контроль над избирателями:** только те, кто в списке; только один голос на человека
- **Тайна голосования:** нельзя узнать выбор конкретного избирателя
- **Индивидуальный контроль:** можно проверить, что твой голос посчитан
- **Универсальный контроль:** можно проверить что результат выборов верен

Требования к схеме выборов

- **Контроль над избирателями:** только те, кто в списке; только один голос на человека
- **Тайна голосования:** нельзя узнать выбор конкретного избирателя
- **Индивидуальный контроль:** можно проверить, что твой голос посчитан
- **Универсальный контроль:** можно проверить что результат выборов верен
- **Устойчивость:** некорректные действия отдельных избирателей не могут сорвать выборы

Требования к схеме выборов

- **Контроль над избирателями:** только те, кто в списке; только один голос на человека
- **Тайна голосования:** нельзя узнать выбор конкретного избирателя
- **Индивидуальный контроль:** можно проверить, что твой голос посчитан
- **Универсальный контроль:** можно проверить что результат выборов верен
- **Устойчивость:** некорректные действия отдельных избирателей не могут сорвать выборы
- **Неподтверждаемость голоса:** после выборов нельзя доказать, что избиратель голосовал определенным образом

План лекции

1. Постановка задачи

2. **Примитивы и идеи**
   - Криптографические примитивы
   - Идеи для электронных выборов

3. Два протокола электронных выборов
   - Протокол Шаума
   - FOO-схема для выборов

Гомоморфное шифрование

Криптосистема с открытым ключом — пара алгоритмов E и D, таких что $D(E(x)) = x$ и, зная E, трудно построить D.

Гомоморфное шифрование

Криптосистема с открытым ключом — пара алгоритмов E и D, таких что $D(E(x)) = x$ и, зная E, трудно построить D.

Криптосистему называют **гомоморфной относительно сложения**, если существует полиномиально вычислимая функция F, такая что $F(E(x_1), E(x_2)) = E(x_1 + x_2)$

Гомоморфное шифрование

Криптосистема с открытым ключом — пара алгоритмов E и D, таких что $D(E(x)) = x$ и, зная E, трудно построить D.

Криптосистему называют **гомоморфной относительно сложения**, если существует полиномиально вычислимая функция F, такая что $F(E(x_1), E(x_2)) = E(x_1 + x_2)$

Факт: есть криптосистема (основанные на трудности дискретного логарифмирования), обладающие этим свойством. В ней F — просто умножение.

Гомоморфное шифрование

Криптосистема с открытым ключом — пара алгоритмов E и D, таких что $D(E(x)) = x$ и, зная E, трудно построить D.

Криптосистему называют **гомоморфной относительно сложения**, если существует полиномиально вычислимая функция F, такая что $F(E(x_1), E(x_2)) = E(x_1 + x_2)$

Факт: есть криптосистема (основанные на трудности дискретного логарифмирования), обладающие этим свойством. В ней F — просто умножение.

Обладает ли криптосистема RSA какой-нибудь гомоморфностью?

Гомоморфное шифрование

Криптосистема с открытым ключом — пара алгоритмов E и D, таких что $D(E(x)) = x$ и, зная E, трудно построить D.

Криптосистему называют **гомоморфной относительно сложения**, если существует полиномиально вычислимая функция F, такая что $F(E(x_1), E(x_2)) = E(x_1 + x_2)$

Факт: есть криптосистема (основанные на трудности дискретного логарифмирования), обладающие этим свойством. В ней F — просто умножение.

Обладает ли криптосистема RSA какой-нибудь гомоморфностью?

Построить криптосистему, гомоморфную относительно и сложения, и умножения

Слепая подпись

Протокол слепой подписи — протокол обмена сообщениями между Алисой и Бобом, в результате которого Боб получит подпись Алисы на нужном ему сообщении, а Алиса не узнает, что она подписала.

Слепая подпись

Протокол слепой подписи — протокол обмена сообщениями между Алисой и Бобом, в результате которого Боб получит подпись Алисы на нужном ему сообщении, а Алиса не узнает, что она подписала.

Факт: протоколы слепой подписи уже разработаны (тоже основаны на дискретном логарифме)

Тайна голосования

Пусть мы отказываемся от тайны голосования.
Предложите схему для проведения выборов

Тайна голосования

Пусть мы отказываемся от тайны голосования.
Предложите схему для проведения выборов

Решение: Каждый избиратель присылает пару (свое имя, свой выбор) и подпись к этой паре.

Тайна голосования

Пусть мы отказываемся от тайны голосования.
Предложите схему для проведения выборов

Решение: Каждый избиратель присылает пару (свое имя, свой выбор) и подпись к этой паре.

Два пути к тайне голосования:

(1) Все видят голос, но никто не знает, чей он
Основной инструмент — анонимный канал

Тайна голосования

Пусть мы отказываемся от тайны голосования.
Предложите схему для проведения выборов

Решение: Каждый избиратель присылает пару (свое имя, свой выбор) и подпись к этой паре.

Два пути к тайне голосования:

(1) Все видят голос, но никто не знает, чей он
Основной инструмент — анонимный канал
Проблема — контроль за избирателями

Тайна голосования

Пусть мы отказываемся от тайны голосования.
Предложите схему для проведения выборов

Решение: Каждый избиратель присылает пару (свое имя, свой выбор) и подпись к этой паре.

Два пути к тайне голосования:

(1) Все видят голос, но никто не знает, чей он
Основной инструмент — анонимный канал
Проблема — контроль за избирателями

(2) Все видят, чей бюллетень, но никто не может расшифровать выбор
Основной инструмент — гомоморфное шифрование

Тайна голосования

Пусть мы отказываемся от тайны голосования.
Предложите схему для проведения выборов

Решение: Каждый избиратель присылает пару (свое имя, свой выбор) и подпись к этой паре.

Два пути к тайне голосования:

(1) Все видят голос, но никто не знает, чей он
Основной инструмент — анонимный канал
Проблема — контроль за избирателями

(2) Все видят, чей бюллетень, но никто не может расшифровать выбор
Основной инструмент — гомоморфное шифрование
Проблема — выборы по сложным вопросам

Псевдонимы

Как построить контроль за избирателями при использовании анонимного канала?

Псевдонимы

Как построить контроль за избирателями при использовании анонимного канала?

Первая фаза: создание псевдонима

- Избиратель общается с организаторами и в итоге создает специальное сообщение (псевдоним)
- Организаторы не знают этот псевдоним
- Избиратель может создать только один псевдоним

Псевдонимы

Как построить контроль за избирателями при использовании анонимного канала?

Первая фаза: создание псевдонима

- Избиратель общается с организаторами и в итоге создает специальное сообщение (псевдоним)
- Организаторы не знают этот псевдоним
- Избиратель может создать только один псевдоним

Вторая фаза: голосование

- Избиратель по анонимному каналу посылает пару (псевдоним, голос)
- По завершении времени выборов суммируются голоса с корректными псевдонимами

План лекции

1. Постановка задачи

2. Примитивы и идеи
   - Криптографические примитивы
   - Идеи для электронных выборов

3. **Два протокола электронных выборов**
   - Протокол Шаума
   - FOO-схема для выборов

Протокол Шаума [1981]

N организаторов, у каждого своя криптосистема E_i, D_i
Общая память (“доска бюллетеней”) у всех участников выборов

Протокол Шаума [1981]

N организаторов, у каждого своя криптосистема E_i, D_i
Общая память (“доска бюллетеней”) у всех участников выборов

Протокол:

1. Каждый участник i посылает на доску $E_1(E_2(\ldots E_N(K_i)))$, где K_i — его зашифрованный голос

Протокол Шаума [1981]

N организаторов, у каждого своя криптосистема E_i, D_i
Общая память (“доска бюллетеней”) у всех участников выборов

Протокол:

1. Каждый участник i посылает на доску $E_1(E_2(\ldots E_N(K_i)))$, где K_i — его зашифрованный голос
2. Организаторы по-очереди снимают свое шифрование и переставляют сообщения местами

Протокол Шаума [1981]

N организаторов, у каждого своя криптосистема E_i, D_i
Общая память (“доска бюллетеней”) у всех участников выборов

Протокол:

1. Каждый участник i посылает на доску $E_1(E_2(\ldots E_N(K_i)))$, где K_i — его зашифрованный голос
2. Организаторы по-очереди снимают свое шифрование и переставляют сообщения местами
3. После всех N раундов получается список из голосов многократно переставленных между собой

Протокол Шаума [1981]

N организаторов, у каждого своя криптосистема E_i, D_i
Общая память (“доска бюллетеней”) у всех участников выборов

Протокол:

1. Каждый участник i посылает на доску $E_1(E_2(\ldots E_N(K_i)))$, где K_i — его зашифрованный голос
2. Организаторы по-очереди снимают свое шифрование и переставляют сообщения местами
3. После всех N раундов получается список из голосов многократно переставленных между собой
4. Участники проверяют, что их голос есть в списке Каждый участник

Протокол Шаума [1981]

N организаторов, у каждого своя криптосистема E_i, D_i
Общая память (“доска бюллетеней”) у всех участников выборов

Протокол:

1. Каждый участник i посылает на доску $E_1(E_2(\ldots E_N(K_i)))$, где K_i — его зашифрованный голос
2. Организаторы по-очереди снимают свое шифрование и переставляют сообщения местами
3. После всех N раундов получается список из голосов многократно переставленных между собой
4. Участники проверяют, что их голос есть в списке Каждый участник
5. Теперь участник i посылает на доску $E_1(E_2(\ldots E_N(K_i^{-1}||K_i)))$

Недостатки схемы Шаума

Какие недостатки видите вы?

Недостатки схемы Шаума

Какие недостатки видите вы?

- Если обнаружены ошибки — нужно проводить голосование заново, а информация о голосах уже раскрыта

Недостатки схемы Шаума

Какие недостатки видите вы?

- Если обнаружены ошибки — нужно проводить голосование заново, а информация о голосах уже раскрыта
- Объединившись, организаторы могут узнать кто как голосовал

Недостатки схемы Шаума

Какие недостатки видите вы?

- Если обнаружены ошибки — нужно проводить голосование заново, а информация о голосах уже раскрыта
- Объединившись, организаторы могут узнать кто как голосовал
- Свойство неподтверждаемости не выполнено

Недостатки схемы Шаума

Какие недостатки видите вы?

- Если обнаружены ошибки — нужно проводить голосование заново, а информация о голосах уже раскрыта
- Объединившись, организаторы могут узнать кто как голосовал
- Свойство неподтверждаемости не выполнено
- Можно скопировать чужой голос

FOO-схема

Организаторы: “Раздающий бюллетени” и “Считающий голоса”

FOO-схема

Организаторы: “Раздающий бюллетени” и “Считающий голоса”

Протокол

1. Каждый избиратель шифрует свой голос своим ключом

FOO-схема

Организаторы: “Раздающий бюллетени” и “Считающий голоса”

Протокол

1. Каждый избиратель шифрует свой голос своим ключом
2. Избиратели вслепую подписывают свой шифрованный голос у “раздающего”

FOO-схема

Организаторы: “Раздающий бюллетени” и “Считающий голоса”

Протокол

1. Каждый избиратель шифрует свой голос своим ключом
2. Избиратели вслепую подписывают свой шифрованный голос у “раздающего”
3. Они анонимно посылают подписанный голос “считающему”, он публикует список полученных голосов

FOO-схема

Организаторы: “Раздающий бюллетени” и “Считающий голоса”

Протокол

1. Каждый избиратель шифрует свой голос своим ключом
2. Избиратели вслепую подписывают свой шифрованный голос у “раздающего”
3. Они анонимно посылают подписанный голос “считающему”, он публикует список полученных голосов
4. Избиратели проверяют, что их голос есть в списке

FOO-схема

Организаторы: “Раздающий бюллетени” и “Считающий голоса”

Протокол

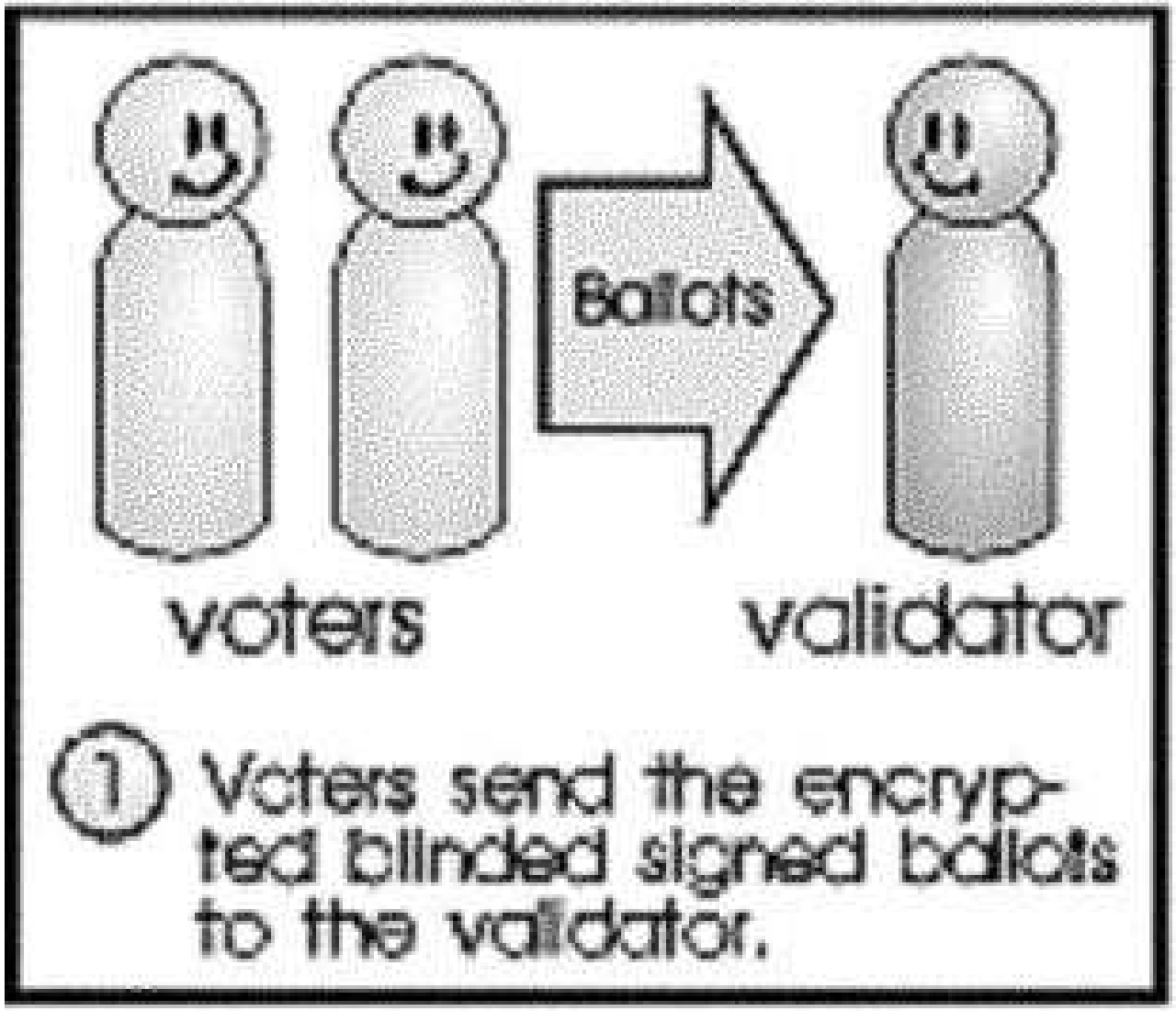
1. Каждый избиратель шифрует свой голос своим ключом
2. Избиратели вслепую подписывают свой шифрованный голос у “раздающего”
3. Они анонимно посылают подписанный голос “считающему”, он публикует список полученных голосов
4. Избиратели проверяют, что их голос есть в списке
5. Теперь Избиратели анонимно высылают ключи для расшифровки голосов

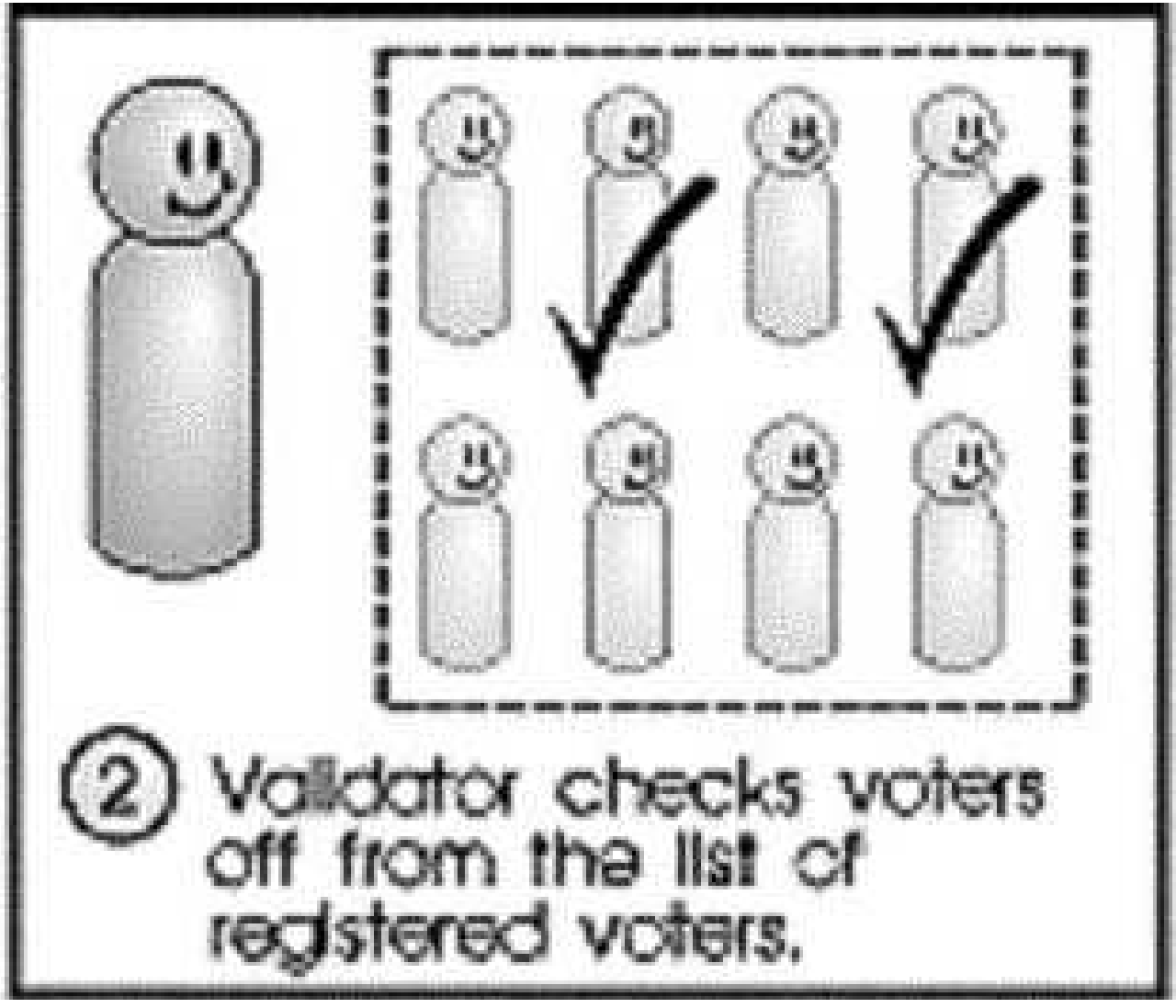
FOO-схема

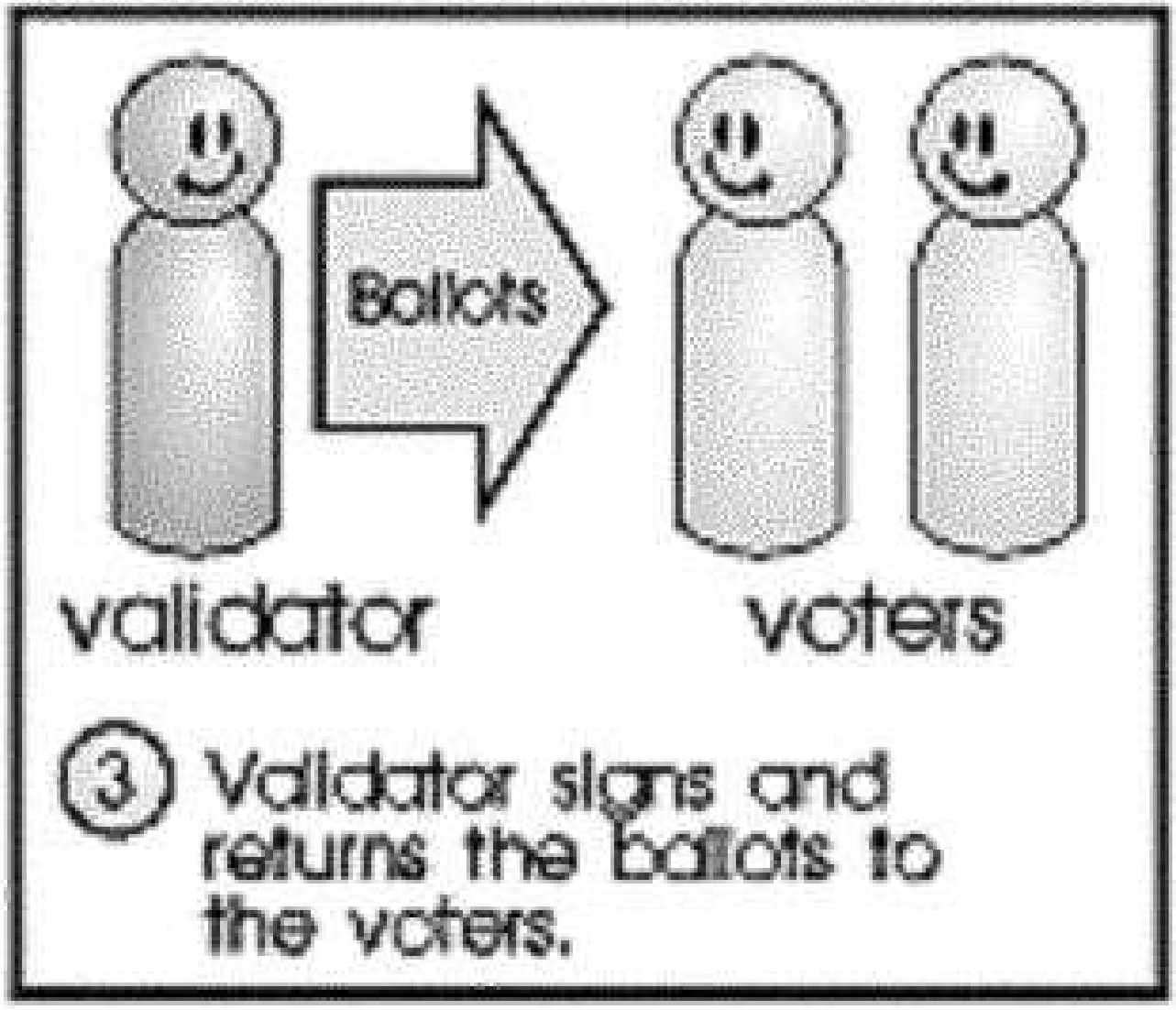
Организаторы: “Раздающий бюллетени” и “Считающий голоса”

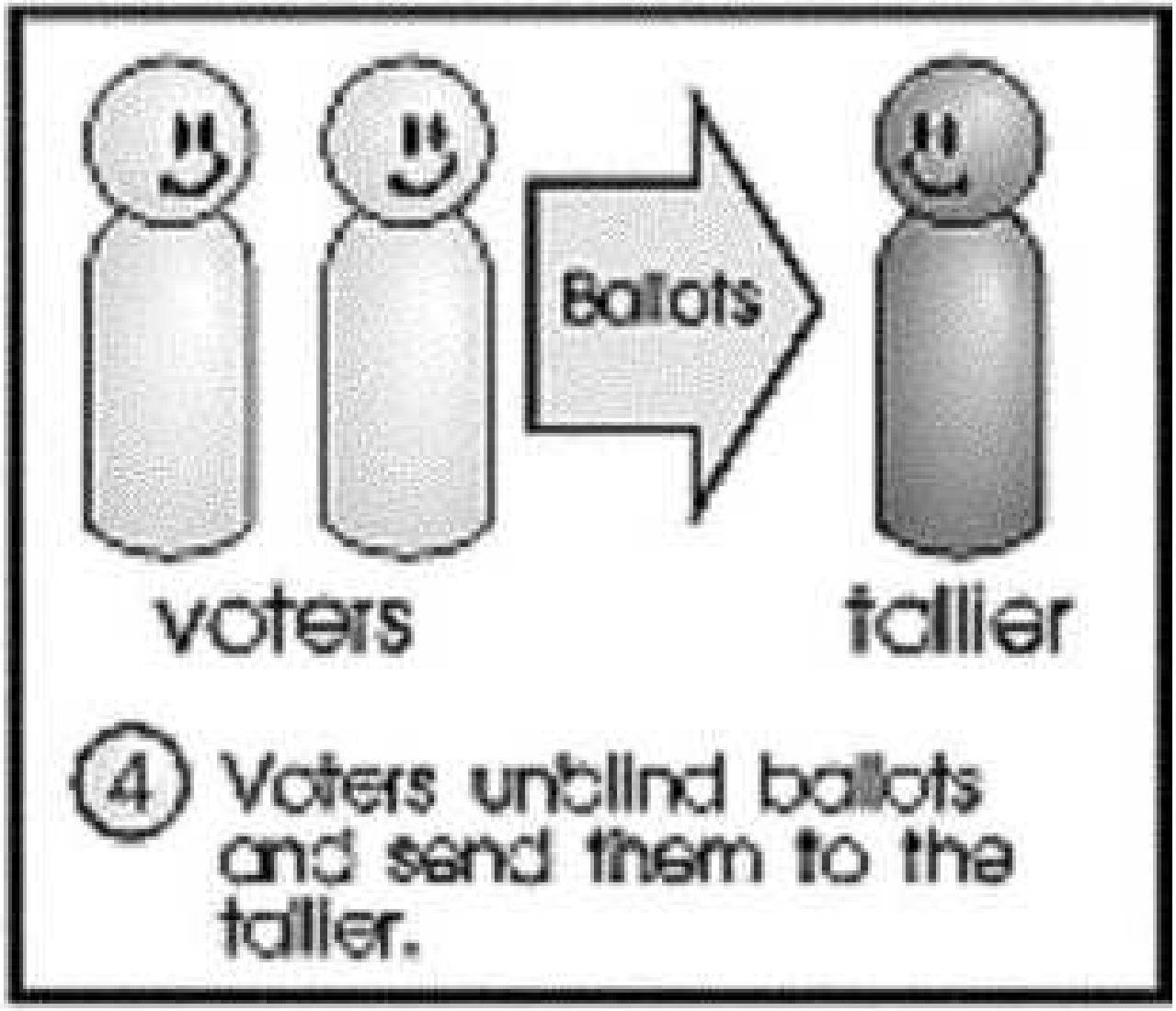
Протокол

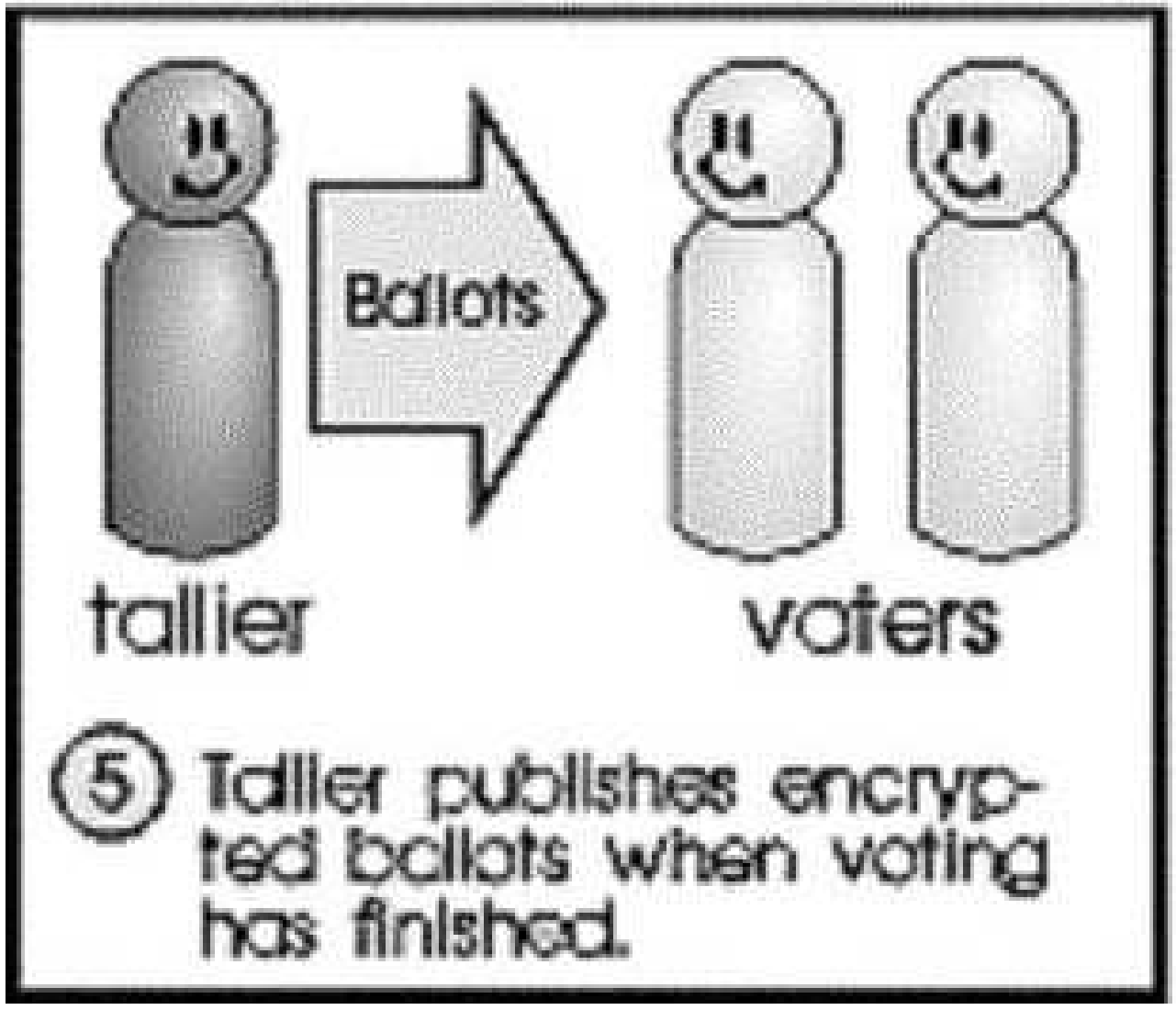
1. Каждый избиратель шифрует свой голос своим ключом
2. Избиратели вслепую подписывают свой шифрованный голос у “раздающего”
3. Они анонимно посылают подписанный голос “считающему”, он публикует список полученных голосов
4. Избиратели проверяют, что их голос есть в списке
5. Теперь Избиратели анонимно высылают ключи для расшифровки голосов
6. Голоса расшифровываются, публикуются и подсчитываются

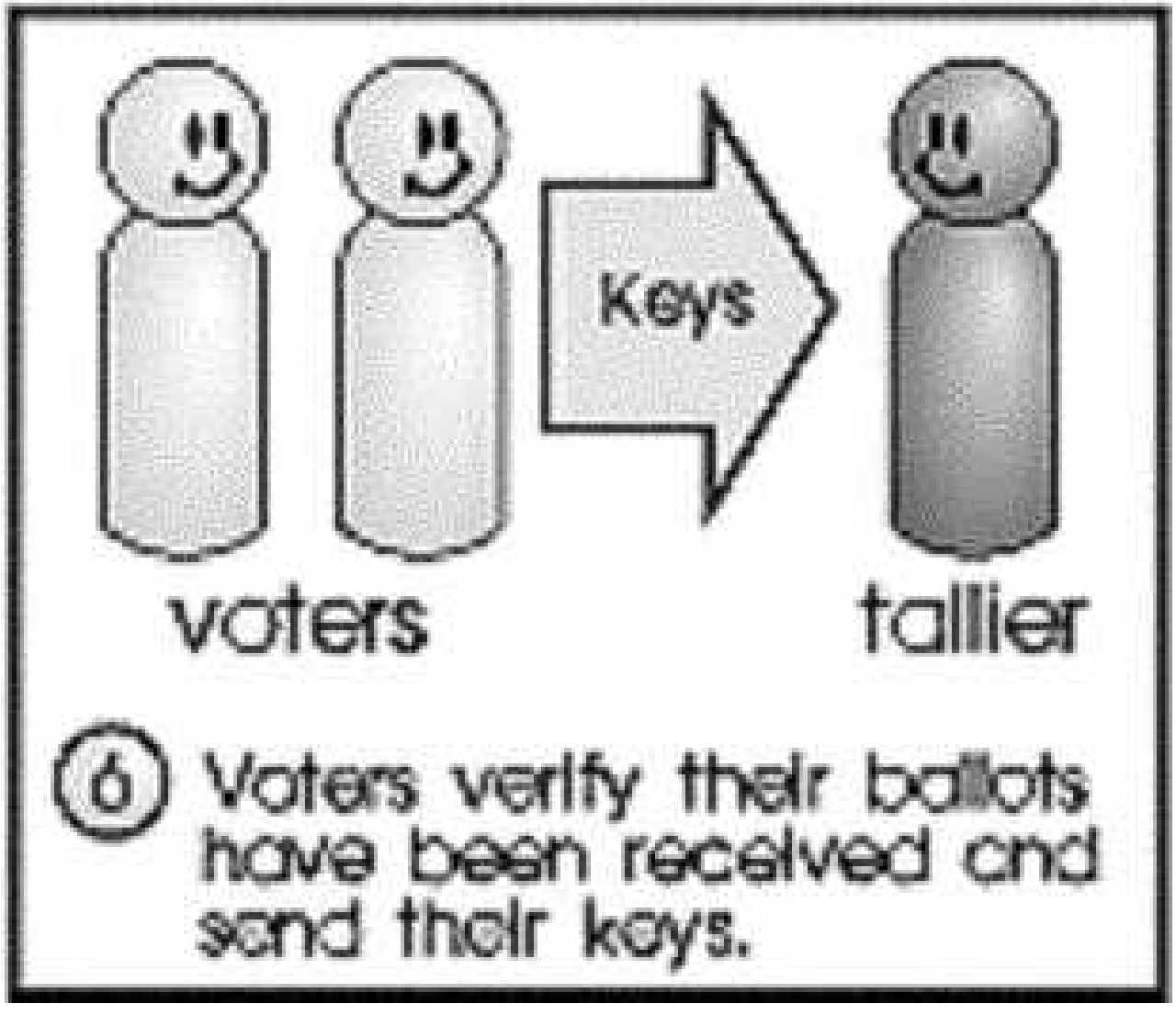

Ballots
voters
validator
1 Voters send the encrypted blinded signed ballots to the validator.

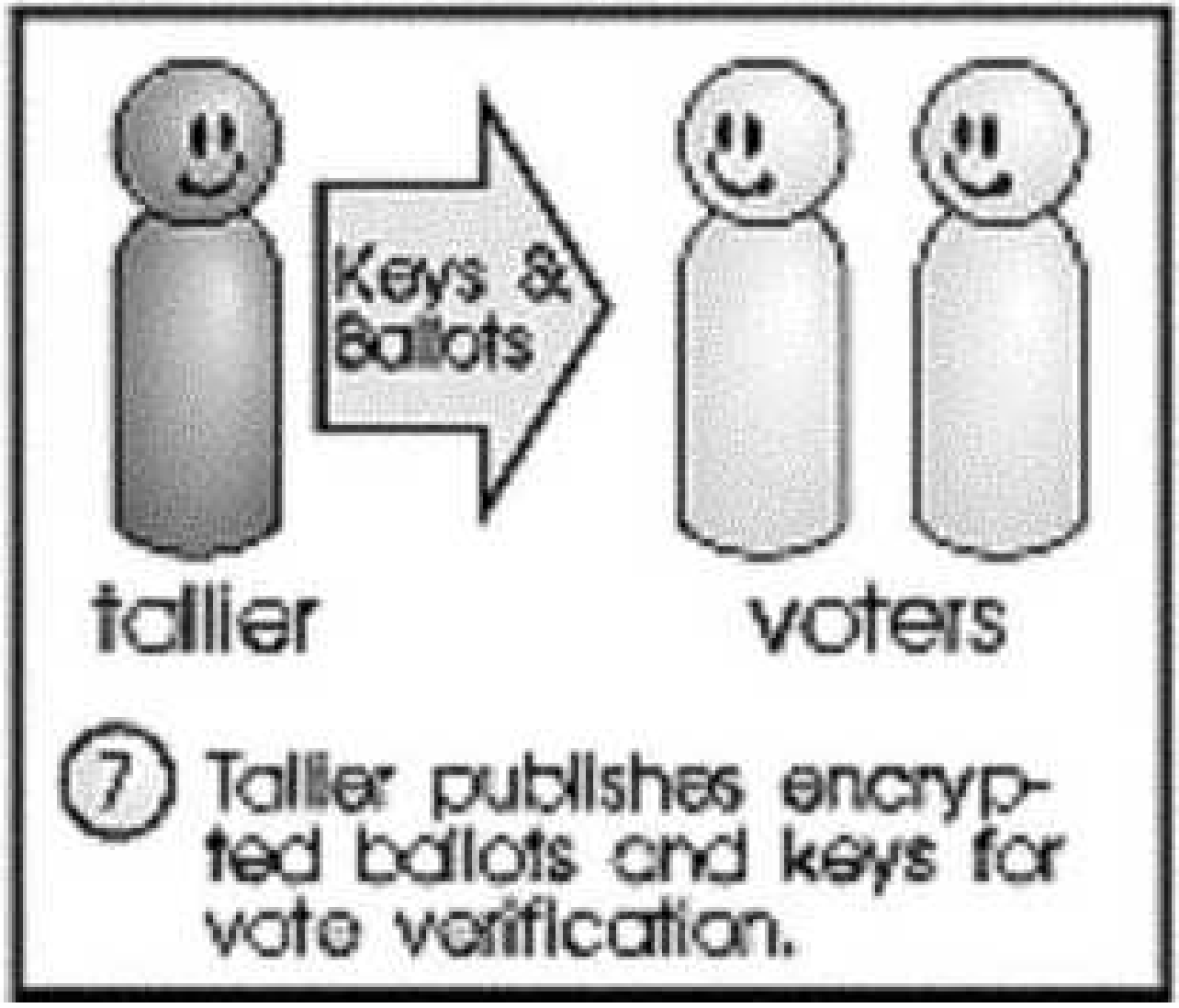

2 Validator checks voters off from the list of registered voters.


Ballots
validator
voters
③ Validator signs and returns the ballots to the voters.


Ballots
voters
tallier
④ Voters unblind ballots and send them to the tallier.


Ballots
tallier
voters
5 Tallier publishes encrypted ballots when voting has finished.


Keys
voters
tallier
6 Voters verify their ballots have been received and send their keys.



(7) Tallier publishes encrypted ballots and keys for vote verification.

Анализ FOO-схемы

Выполнены требования:

- Контроль за избирателями
- Тайна голоса
- Индивидуальный контроль
- Результаты открываются только после окнончания выборов

Анализ FOO-схемы

Выполнены требования:

- Контроль за избирателями
- Тайна голоса
- Индивидуальный контроль
- Результаты открываются только после окнончания выборов

Не выполнены требования:

- Универсальный контроль
- Неподтверждаемость

Последний слайд

Если не запомните ничего другого:

- Требования к выборам: контроль за избирателями, тайна голосования, контроль за подсчетом голосов, устойчивость, неподтверждаемость

Последний слайд

Если не запомните ничего другого:

- Требования к выборам: контроль за избирателями, тайна голосования, контроль за подсчетом голосов, устойчивость, неподтверждаемость
- Основные идеи: гомоморфное шифрование, анонимный канал, псевдонимы

Последний слайд

Если не запомните ничего другого:

- Требования к выборам: контроль за избирателями, тайна голосования, контроль за подсчетом голосов, устойчивость, неподтверждаемость
- Основные идеи: гомоморфное шифрование, анонимный канал, псевдонимы
- Протокол, удовлетворяющий ВСЕМ требованиям, пока не найден

Последний слайд

Если не запомните ничего другого:

- Требования к выборам: контроль за избирателями, тайна голосования, контроль за подсчетом голосов, устойчивость, неподтверждаемость
- Основные идеи: гомоморфное шифрование, анонимный канал, псевдонимы
- Протокол, удовлетворяющий ВСЕМ требованиям, пока не найден

Последний слайд

Если не запомните ничего другого:

- Требования к выборам: контроль за избирателями, тайна голосования, контроль за подсчетом голосов, устойчивость, неподтверждаемость
- Основные идеи: гомоморфное шифрование, анонимный канал, псевдонимы
- Протокол, удовлетворяющий ВСЕМ требованиям, пока не найден

Вопросы?