конференция
РусКрипто

Ежегодная международная научно-практическая конференция

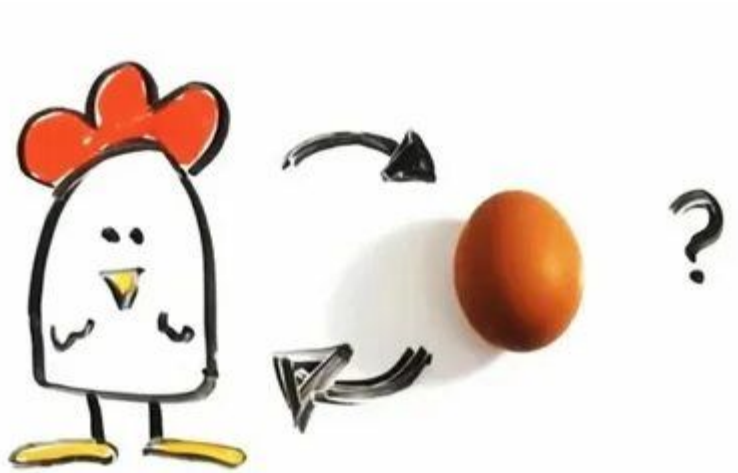
«РусКрипто'2023»

Дистанционное электронное голосование как источник инновационных криптографических задач

Г. Маршалко, Д. Матюхин
ФСБ России

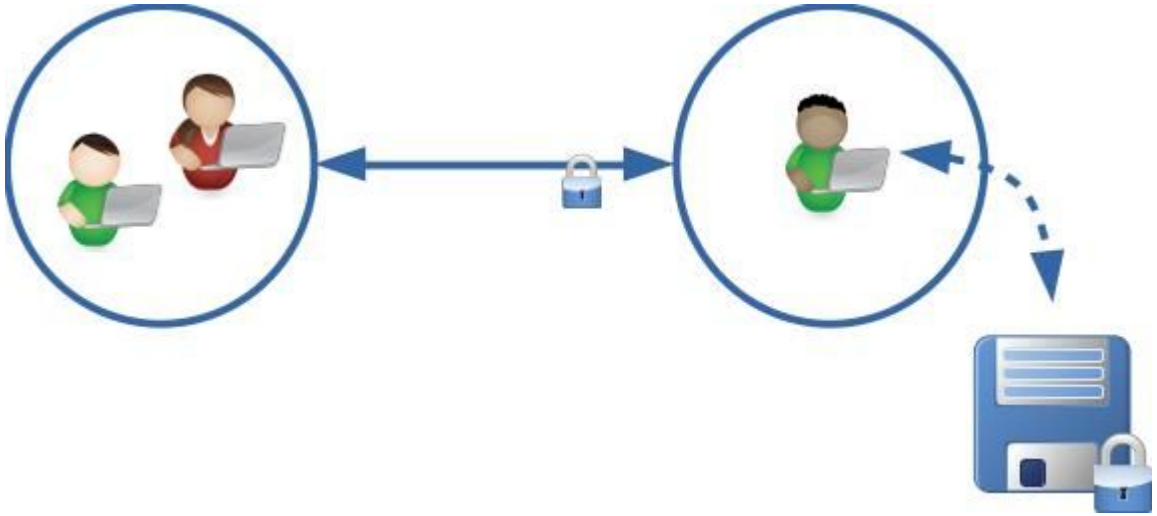
Что первично: курица или яйцо?

- Информационная система определяет требования к криптографическим механизмам или набор криптографических механизмов определяет требования к архитектуре системы?
- Можно ли разделить криптографические и функциональные свойства информационной системы?
- Что значит «безопасность информации при ее передаче, хранении и обработке»?



Классическое применение криптографических методов

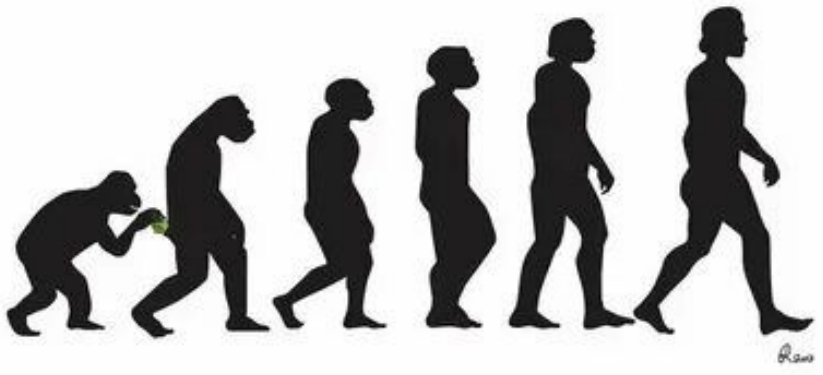
- Обеспечение конфиденциальности и контроль целостности информации при её передаче между контролируемыми зонами обработки и хранения, аутентификация источника данных
- Обеспечение конфиденциальности и контроль целостности информации при её хранении
- Обработка внутри контролируемой зоны оператором – реализация функционала информационной системы



ДЭГ: долгий путь к криптографически защищенной обработке данных

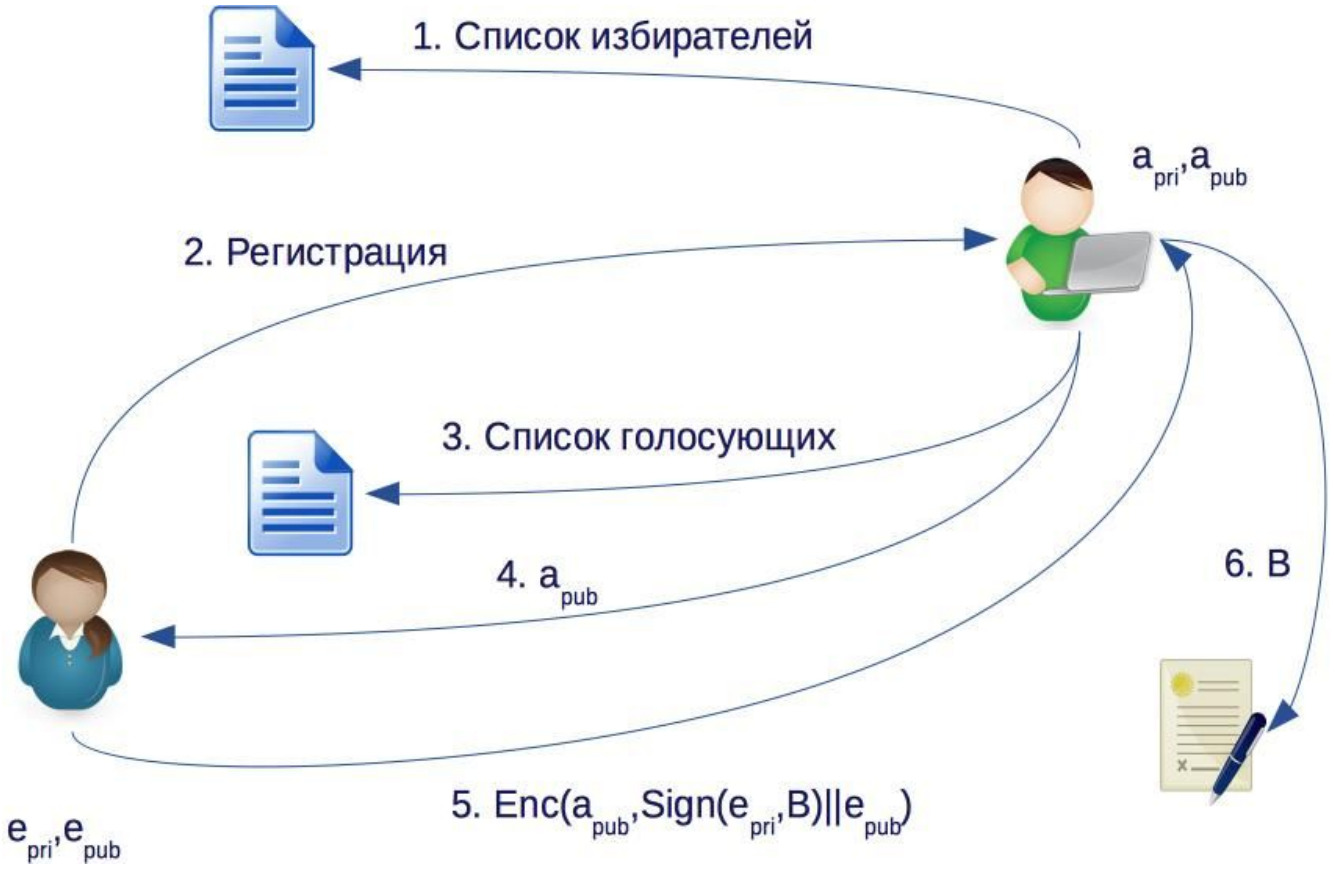
- Более 30 лет эволюционного развития
- Реализация избирательных прав граждан с помощью информационных и криптографических технологий через:
  - Контроль целостности компонентов системы, процессов и циркулирующих в ней данных
  - Обеспечение конфиденциальности промежуточных результатов голосования
  - Обеспечение анонимности избирателей
  - Аутентификацию участников
  - Аудит системы в целом и результатов ее работы
  - Обеспечение доступности системы...*

*) P.G. Neumann, Security criteria for electronic voting, 1993



Базовый протокол: Нурми-Саломаа

- Защита от внешнего нарушителя
- Конфиденциальность голоса
- Субъекты:
  - Избиратель
  - Организатор
- Механизмы:
  - Схемы цифровой подписи и асимметричного шифрования

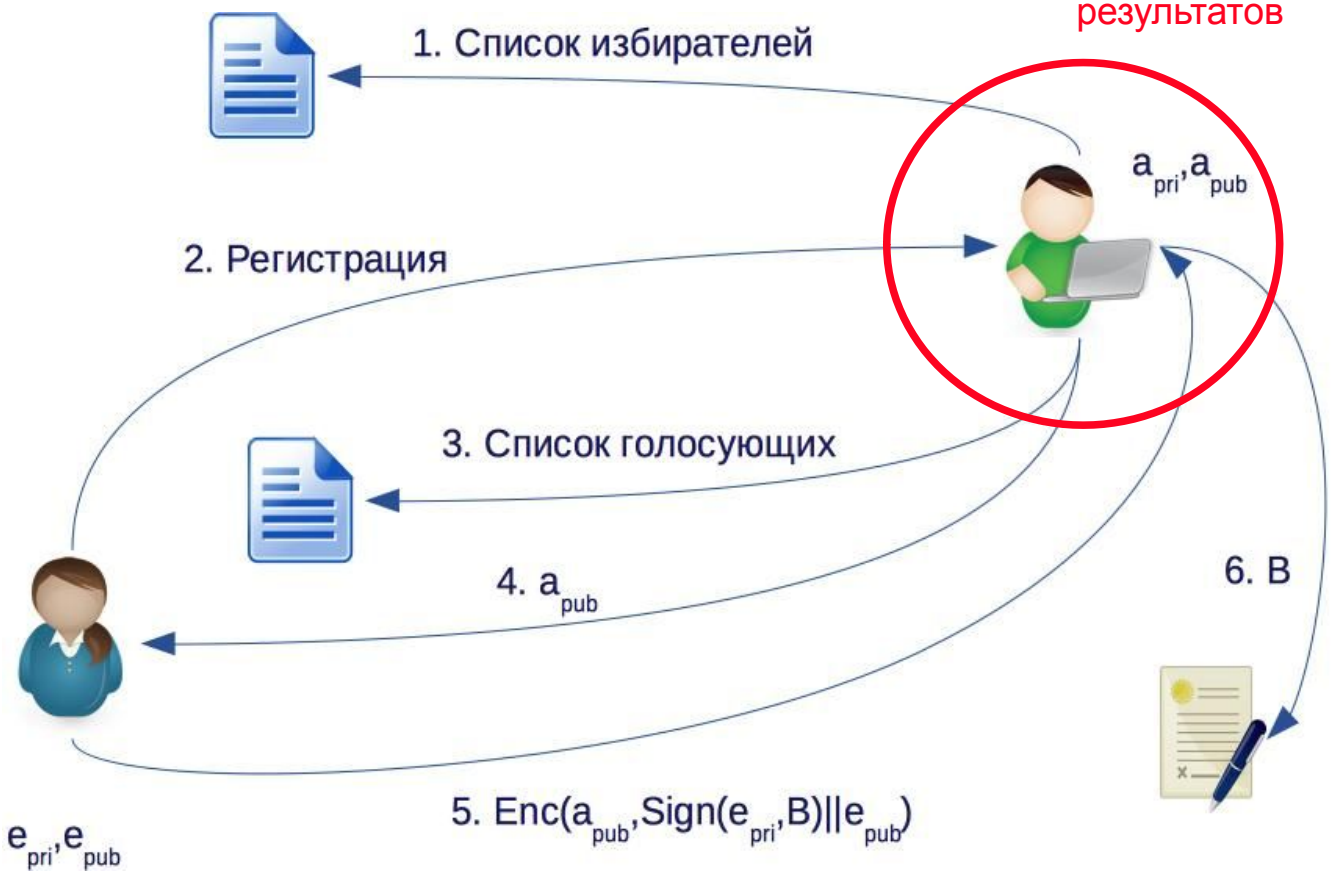


H. Nurmi, A. Salomaa, Conducting secret ballot elections in computer networks: Problems and solutions, 1983

Базовый протокол: Нурми-Саломаа

Деанонимизация, нарушение целостности результатов

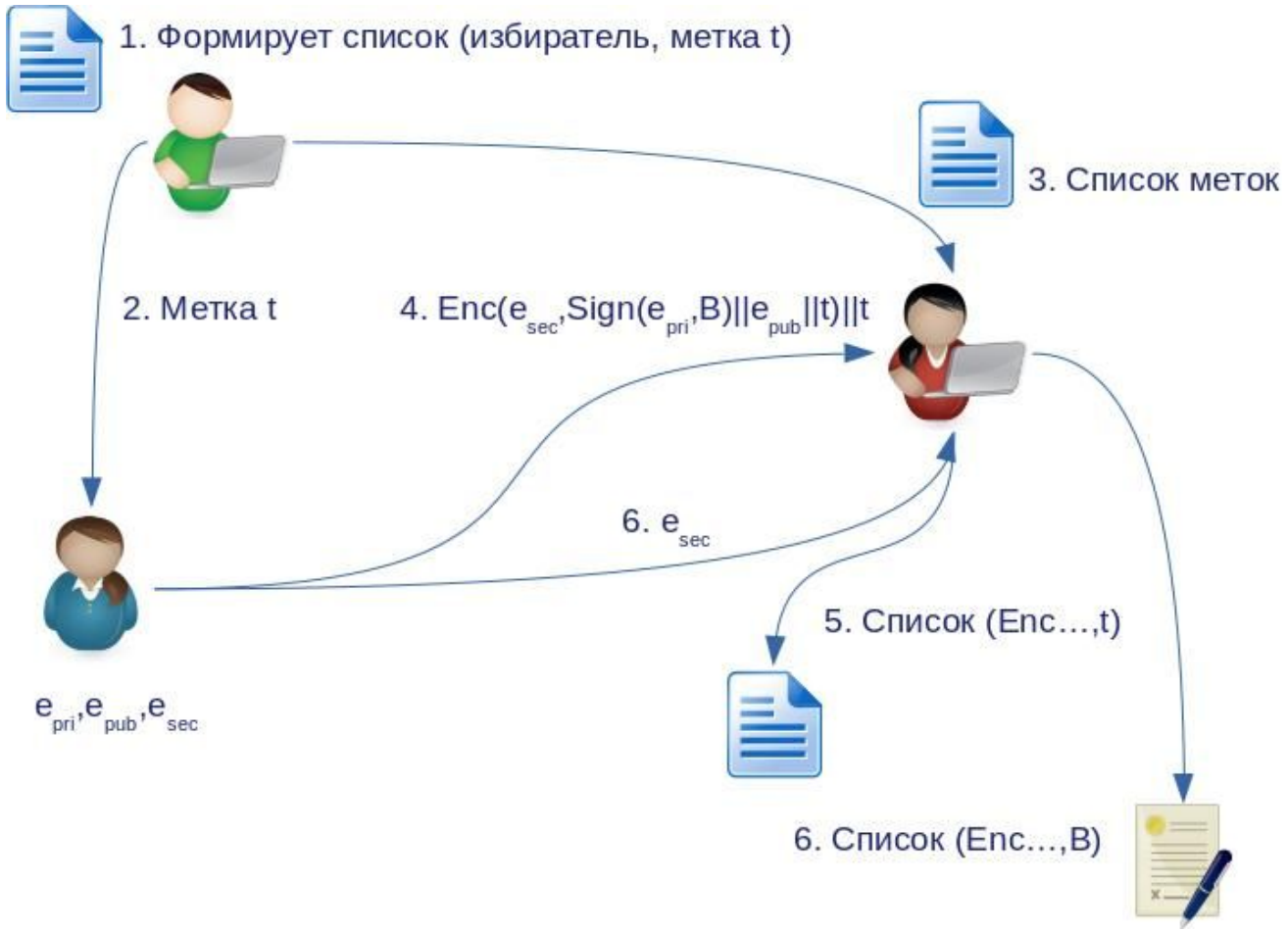
- Защита от внешнего нарушителя
- Конфиденциальность голоса
- Субъекты:
  - Избиратель
  - Организатор
- Механизмы:
  - Схемы цифровой подписи и асимметричного шифрования



H. Nurmi, A. Salomaa, Conducting secret ballot elections in computer networks: Problems and solutions, 1983

Протокол Нурми-Саломаа-Сантина

- Частичная защита от внутреннего нарушителя за счет введения регистратора
- Анонимность избирателя при доверенном регистраторе, контроль целостности результатов голосования (за счет разделения регистрации и подсчета голосов)
- Субъекты:
  - Избиратель
  - Организатор
  - Регистратор
- Механизмы:
  - Схемы цифровой подписи и симметричного шифрования



H. Nurmi, A. Salomaa, L. Santean, Secret ballot elections in computer networks, 1991

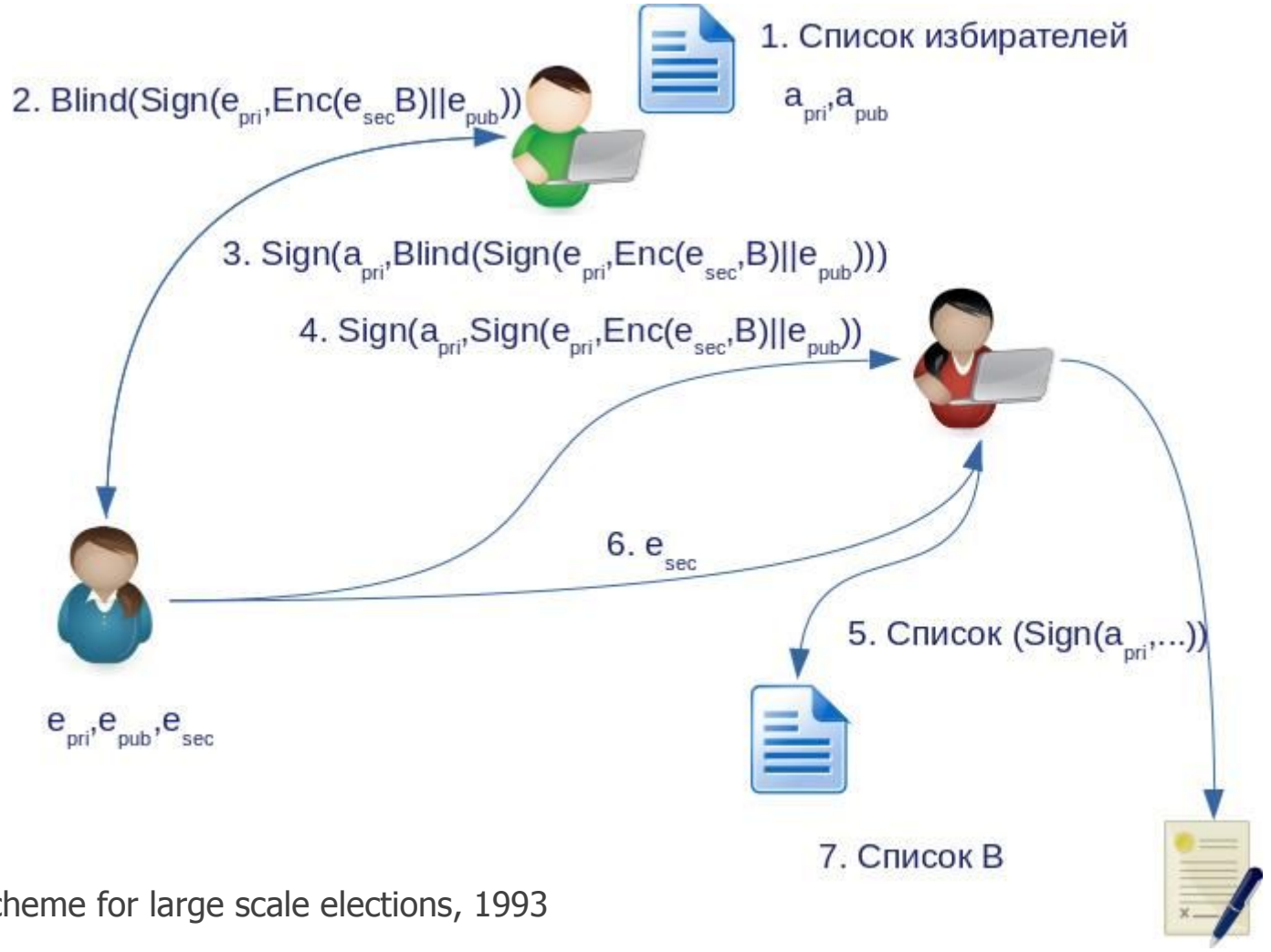
Протокол Нурми-Саломаа-Сантина

- Частичная защита от внутреннего нарушителя за счет введения регистратора
- Анонимность избирателя при доверенном регистраторе, контроль целостности результатов голосования (за счет разделения регистрации и подсчета голосов)
- Субъекты :
  - Избиратель
  - Организатор
  - Регистратор
- Механизмы:
  - Схемы цифровой подписи и симметричного шифрования

H. Nurmi, A. Salomaa, L. Santean, Secret ballot elections in computer networks, 1991

Протокол Фуджиоки-Окамото-Охты

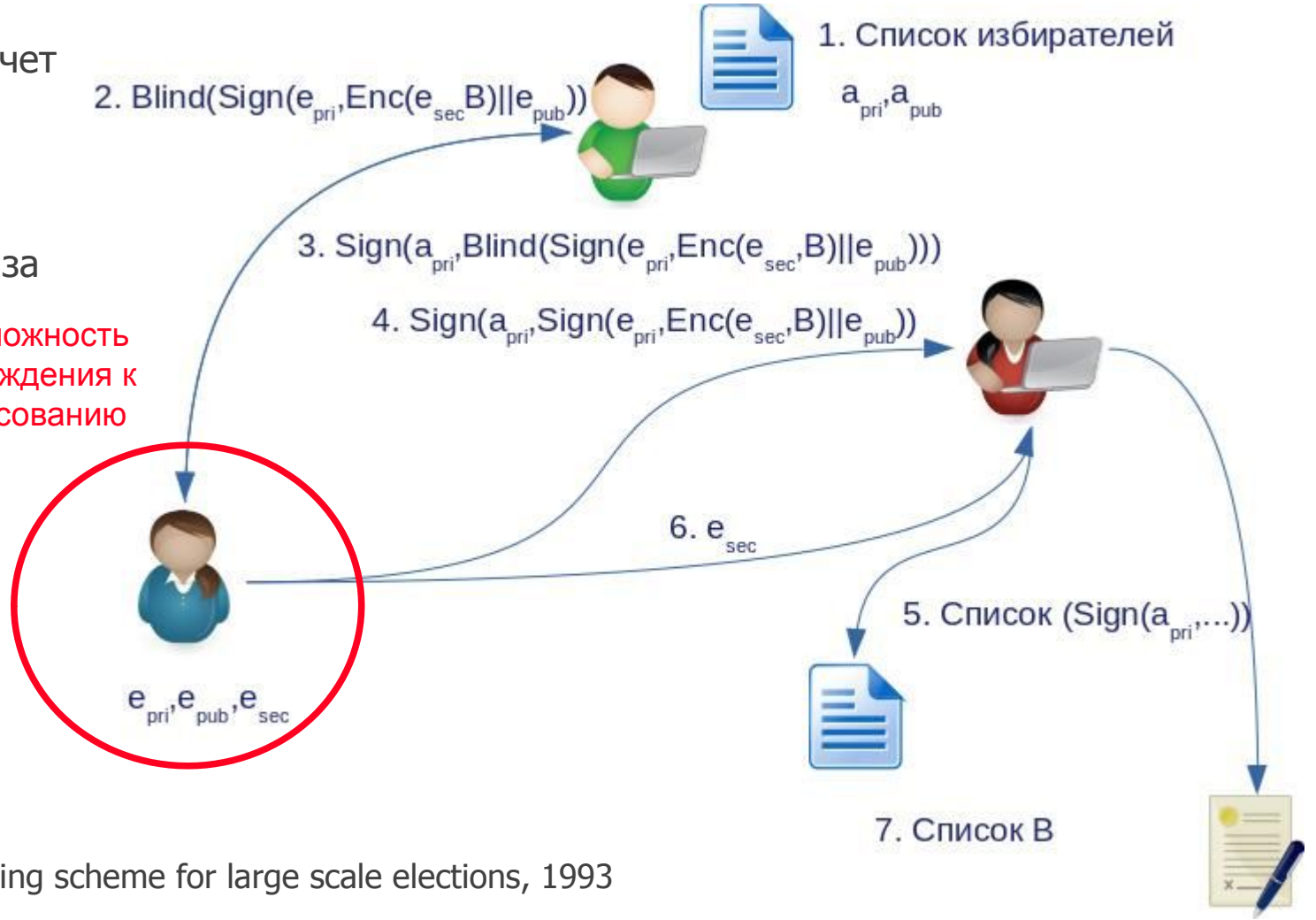
- Защита от нарушителя – регистратора за счет использования подписи вслепую
- Анонимность избирателя и контроль целостности результатов голосования (решение проблемы сговора организаций) за счет использования подписи вслепую
- Субъекты:
  - Избиратель
  - Организатор
  - Регистратор
- Механизмы:
  - Схемы подписи вслепую и симметричного шифрования



A. Fujioka, T. Okamoto, K. Ohta, A practical secret voting scheme for large scale elections, 1993

Протокол Фуджиоки-Окамото-Охты

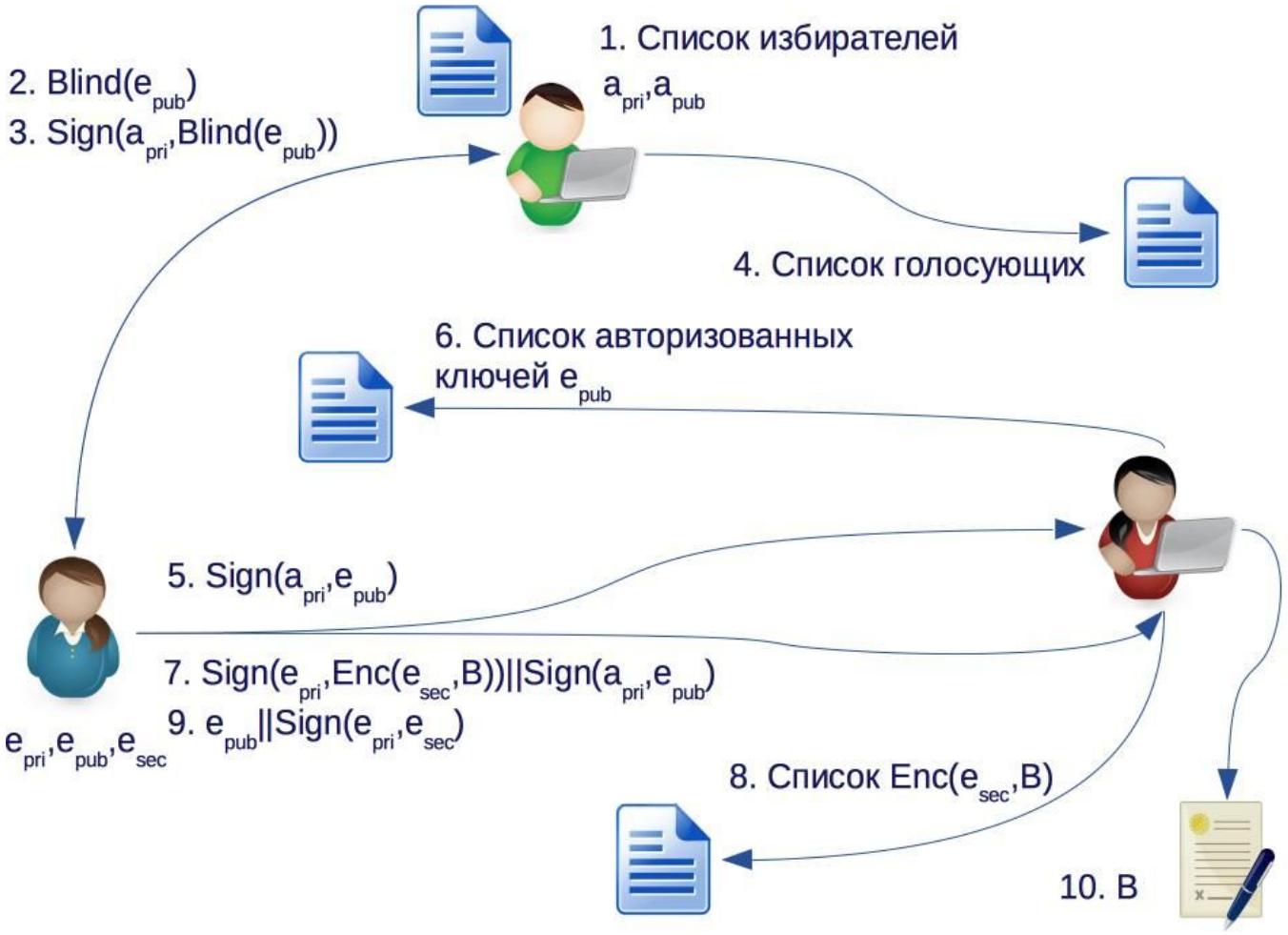
- Защита от нарушителя – регистратора за счет использования подписи вслепую
- Анонимность избирателя и контроль целостности результатов голосования (решение проблемы сговора организаций) за счет использования подписи вслепую
- Субъекты:
  - Избиратель
  - Организатор
  - Регистратор
- Механизмы:
  - Схемы подписи вслепую и симметричного шифрования



A. Fujioka, T. Okamoto, K. Ohta, A practical secret voting scheme for large scale elections, 1993

Протокол Хе-Су

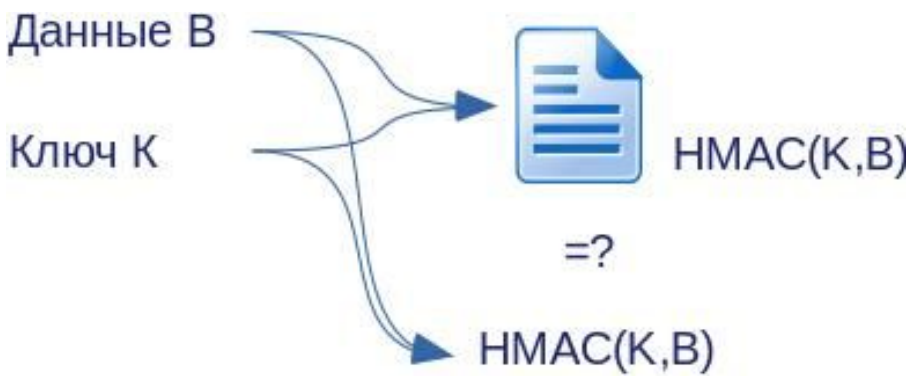
- Защита от принуждения к голосованию за счет возможности переголосования (подписывается ключ, а не бюллетень)
- Наиболее широкий перечень обеспечиваемых свойств
- Субъекты:
  - Избиратель
  - Организатор
  - Регистратор
- Механизмы:
  - Схемы подписи вслепую и симметричного шифрования
-



Q. He, Z. Su, A New Practical Secure e-Voting Scheme, 1997

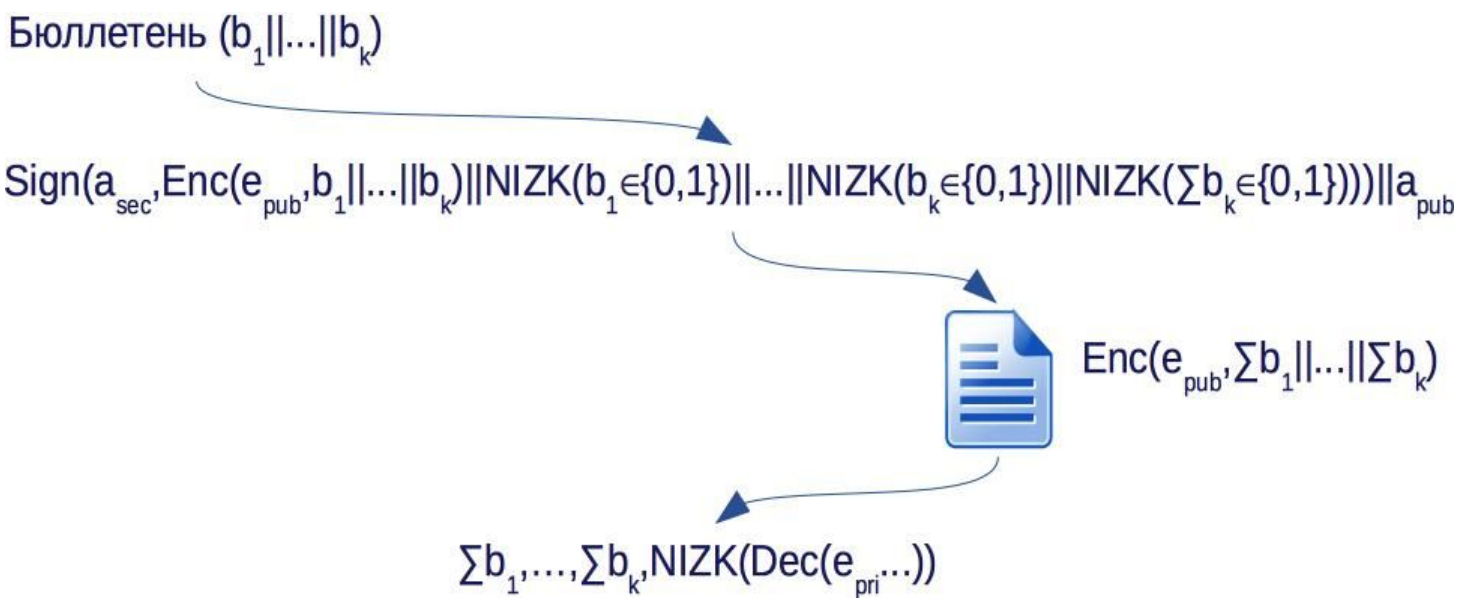
Ближе к реальной жизни: новые механизмы для новых задач

- Необходимость публикации списков + тайна волеизъявления = схемы обязательств
- Возможность последующей проверки корректности списка
- Обеспечивает конфиденциальность данных до момента проверки



Ближе к реальной жизни: новые механизмы для новых задач

- Быстрота подсчета голосов + конфиденциальность промежуточных итогов = схема гомоморфного шифрования + доказательство корректности заполнения бюллетеня (NIZK/подпись) + доказательство корректности расшифрования
- Позволяет конфиденциально предвычислять результаты голосования



Ближе к реальной жизни: новые механизмы для новых задач

- Отказоустойчивость + расширенная защита от внутреннего нарушителя = распределенный реестр + схема разделения секрета
- Позволяет обеспечить корректное функционирование системы при некотором количестве внутренних нарушителей

Все вместе: криптографически защищенная обработка информации

Простая и понятная реализация функционала системы через криптографические преобразования:

$$(s_1, ..., s_k) = Dec\left(a_{pri}, \sum_i \left(Enc(a_{pub}, b_1^{(i)}), ..., Enc(a_{pub}, b_k^{(i)})\right)\right),$$

где $a_{pri} = \sum_{t=1}^{l} a_{pri,t}$, а i такое, что

$NIZK(b_1^{(i)} \in \{0,1\}) = 1,$

...

$NIZK(b_k^{(i)} \in \{0,1\}) = 1,$

$NIZK(\sum_{j=1}^{k} b_j^{(i)} \in \{0,1\}) = 1,$

$Verify\left(e_{pub,i}, Sign(e_{pri,i}, Enc(a_{pub}, b_1^{(i)})||...||Enc(a_{pub}, b_k^{(i)})||NIZK(b_1^{(i)})||...||NIZK(b_k^{(i)})||NIZK(\sum_{j=1}^{k} b_j^{(i)})\right) = 1,$

$Verify(a_{pub}, Sign(a_{pri}, e_{pub,i})) = 1,$

$e_{pub,i}$ ранее не использовался

К чему пришли с точки зрения архитектуры

- Реализуется криптографический контроль целостности информации при обработке
- Обеспечивается конфиденциальность информации при обработке
- Можно рассматривать как единое СКЗИ со сложным набором криптографических функций

- Большое число участников с различными функциями – усложняется анализ возможных действий нарушителя
  - Отсутствие в ряде случаев контролируемой зоны
  - Функциональные свойства системы неотделимы от её криптографических свойств

К чему пришли с точки зрения криптографических механизмов

- Архитектура подобных систем требует разработки/исследования новых классов криптографических механизмов
- Архитектура подобных систем требует исследования новых моделей безопасности классических механизмов, в том числе с оценкой их взаимного влияния

- Решение этих задач позволит создать строительные блоки для новых классов информационных систем