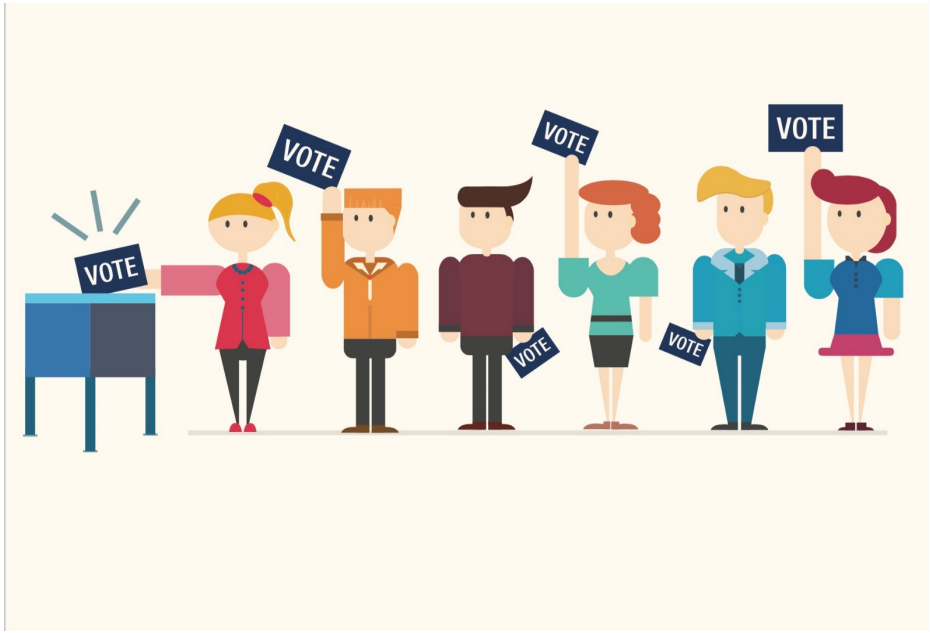
Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Криптографические протоколы в системах электронного голосования

Станислав Смышляев, к.ф.-м.н.,
Заместитель генерального директора, КриптоПро

Дистанционное электронное голосование (ДЭГ)

Голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием программно-технического комплекса ДЭГ, доступ к которому участнику голосования предоставляется на специальном портале, размещенном в информационно-телекоммуникационной сети «Интернет».



VS

Участники

- избиратель
- организатор голосования
- регистратор
- урна (доска бюллетеней)
- серверы подсчета голосов
- наблюдатель

Основные этапы

- инициализация системы:
  - выработка ключевого материала
  - формирование списка избирателей
- регистрация:
  - авторизация и аутентификация избирателей
  - выдача избирателям права на голосование
- волеизъявление:
  - заполнение бюллетеней избирателями и отправка их урне
- подведение итогов:
  - подсчет и публикация результатов голосования
- аудит:
  - проверка корректности учета голосов избирателями и наблюдателями

Свойства безопасности: базовые

- **верифицируемость избирателей**: в голосовании принимают участие только граждане, включенные в список избирателей
- **конфиденциальность результатов**: до окончания голосования никому не известны результаты
- **анонимность голосов**: невозможно определить, кто как проголосовал
- **корректность учета голосов**: все валидные голоса учтены и учтены корректно
- **проверяемость**
  - **личная**: каждый избиратель может проверить, что его голос учтен корректно
  - **всеобщая**: любой сторонний наблюдатель имеет доступ к итоговому списку бюллетеней и может проверить, что подсчет голосов осуществлялся корректным образом
- **1 избиратель – 1 голос**
- **надежность/доступность**: избиратели всегда имеют доступ к системе голосования

Свойства безопасности: дополнительные

- защита от принуждения и продажи голосов
- сокрытие факта голосования
- возможность разрешения споров

Способы обеспечения свойств безопасности

верифицируемость избирателей	аутентификация избирателей + подпись регистратора
конфиденциальность результатов	распределенный ключ шифрования + шифрование бюллетеней
	схема обязательств (commitment)
анонимность голосов	mixnet (протокол конфиденциальных вычислений – MPC)
	распределенный ключ шифрования + гомоморфное шифрование
	подпись вслепую (бюллетеня/ключа проверки подписи бюллетеня)
корректность учета голосов проверяемость	публикация бюллетеней
	доказательства с нулевым разглашением/verifiable MPC

Криптографические механизмы

- Аутентификация избирателей:
  - ЕСИА (по сертификату)
  - ЕСИА/ЕБС
- Обычная подпись:
  - ГОСТ Р 34.10-2012
- Шифрование бюллетеней:
  - VKO (Р 50.1.113–2016)
  - ГОСТ Р 34.12-2015
  - ГОСТ Р 34.13-2015
  - MGM (Р 1323565.1.026-2019)
- Схема обязательств:
  - HMAC (Р 50.1.113–2016)

Криптографические механизмы

✓ Аутентификация избирателей:
- ЕСИА (по сертификату)
- ЕСИА/ЕБС

✓ Обычная подпись:
- ГОСТ Р 34.10-2012

✓ Шифрование бюллетеней:
- VKO (Р 50.1.113–2016)
- ГОСТ Р 34.12-2015
- ГОСТ Р 34.13-2015
- MGM (Р 1323565.1.026-2019)

✓ Схема обязательств:
- HMAC (Р 50.1.113–2016)

✗ Протоколы разделения секрета

✗ Протоколы конфиденциальных вычислений

✗ Гомоморфное шифрование

✗ Подпись вслепую

✗ Доказательства с нулевым разглашением

Криптографические механизмы

- Протоколы разделения секрета:
  - имеет смысл рассматривать как протоколы с доверенным участником (дилером), так и без него
  - кандидаты:
    - схема Шамира – с дилером
    - протокол DKG Pedersen'91 (есть атака, предложен ряд модификаций) – без дилера
- Протоколы конфиденциальных вычислений:
  - сложная область, существующие решения основаны на нестандартных механизмах (например, oblivious transfer)
- Гомоморфное шифрование:
  - достаточно аддитивной гомоморфности
  - кандидат: схема шифрования Эль-Гамаля на эллиптических кривых

Криптографические механизмы

- Подпись вслепую

Существующие решения:

- на основе задачи DLog в группе точек эллиптической кривой:
  - на основе схемы Шнорра (сломана для случая параллельных сессий, но есть модификация)
  - на основе ГОСТ Р 34.10-2012 (нет обоснования стойкости)
- на основе спариваний (BLS) – нет pairing-friendly кривых
- на основе задачи факторизации (RSA)

Криптографические механизмы

- Доказательства с нулевым разглашением:
  - схемы для общего случая (zk-SNARK и т.п.) – сложные/неэффективные/мало изученные
  - схемы для частных случаев:

1) доказательство корректности открытого текста
   - должно быть совместимо с алгоритмом гомоморфного шифрования
   - кандидат: disjunctive Chaum-Pedersen proof
   - необходимо расширить на случай множественного выбора

2) доказательство корректности расшифрования
   - должно быть совместимо с протоколом разделения секрета и алгоритмом шифрования
   - кандидат: Chaum-Pedersen proof

Вопросы для обсуждения

1. Обеспечиваемые свойства безопасности: критичные и опциональные.
2. Международный опыт создания протоколов для ДЭГ: какие из механизмов уже в достаточной степени изучены?
3. Насколько децентрализованной должна быть система ДЭГ, чтобы можно было обеспечить требуемые свойства безопасности?
4. Роль распределенного реестра (блокчейна) как фундамента для ДЭГ.
5. Сложности технической реализации с учетом требований ФСБ России.
6. Как может реализоваться и распространяться пользовательский компонент?