Криптографические протоколы

Лекция 10

Протоколы голосования

Деркач Максим Юрьевич

October 18, 2018

Ссылки

Протоколы голосования

Понятие протокола голосования

Задача голосования заключается в том, что несколько абонентов должны совместно выбрать решение из некоторого множества возможных решений. Каждый абонент заполняет свой бюллетень, отражающий решение этого агента.
Совместное решение вырабатывается путем обработки всех бюллетеней.
Часто при процедуре голосования важно обеспечить конфеденциальность решений, принимаемых абонентами.
Данная задача рещается при помощи специальных протоколов.

Протоколы голосования

Понятие протокола голосования

Наиболее часто используются такие протоколы голосования, в которых

1. каждый агент отсылает свой бюллетень некоторому доверенному агенту, называемому **Центральной Избирательной Комиссией(ЦИК)**, которого мы будем обозначать ниже символом s;
2. ЦИК обрабатывает полученные от агентов бюллетени, и публикует результаты голосования.

Протоколы голосования

Понятие протокола голосования

Условия на процедуру голосования, которые должен обеспечить протокол, могут имет, например, следующий вид.

1. Голосовать могут только те агенты, которые имеют на это право.
2. Каждый избиратель может голосовать только один раз.
3. Невозможно установить, за кого проголосовал каждый избиратель.
4. Невозможно использовать дубликат заполненного бюллетеня.
5. Невозможно изменить результат голосования каждого избирателя.
6. Каждый избиратель может проверить, что его бюллетень учтён.
7. Всем известно, кто участвовал в голосовании.

Протоколы голосования

Примеры

Протокол 1

u_i - бюллетень избирателя a_i

1. $A_i -> S : E_{K_{A_i S}}(u_i)$
2. S вычисляет результат и публикует его.

В данном протоколе не выполняются почти все вышеперечисленные условия.

Протокол 2

1. $A_i -> S : E_{K_{A_i S}}(sign_{A_i}(u_i))$
2. S вычисляет результат и публикует его.

Протоколы голосования

Протоколы голосования с ЦИК и ЦУР

Для противодействия возможной нечестности со стороны ЦИК, можно использовать **Центральное Управление Регистрации (ЦУР)**. Необходимое условие корректности протокола является отсутствие обмена между ЦУР и ЦИК.

1. $A_i -> S'$: *request*
2. $S' -> A_i$: R_i - (случайный регистрационный номер).
3. $S' -> S$: $\Re$ - список всех выданных регистрационных номеров.
4. $A_i -> S$: (ID_i, r_i, u_i)
5. s проверяет: $r_i \in \Re$?. Если верно, то
   5.1 $\Re = \Re \backslash \{r_i\}$
   5.2 $\Im = \Im \cup \{ID_i\}$ (в начале работы $\Im = \emptyset$)
6. после получения всех бюллетеней s публикует результат, и список записей вида (ID_i, u_i)
7. S' публикует всех список зарегистрированных a_i

Протоколы голосования

Улучшенный протокол голосования

1. S публикует список всех абонентов, имеющих право голосовать
2. $A_i -> S : intention$
3. S публикует список всех избирателей, собирающихся принять участие в выборах
4. $S -> A_i : ID_i$ - (регистрационный номер).
5. $A_i -> S : ID_i, E_{K_{A_i}^{pub}}(ID_i, u_i)$
6. S публикует $E_{K_{A_i}^{pub}}(ID_i, u_i)$.
7. $A_i -> S : ID_i, K_{A_i}^{sec}$
8. S расшифровывает бюллетени и обрабатывает их
9. S публикует результаты голосования, и все $u_i, E_{K_{A_i}^{pub}}(ID_i, u_i)$
10. Если A_i обнаружил, что его u_i учтен неверно, то $A_i -> S : ID_i, E_{K_{A_i}^{pub}}(ID_i, u_i), K_{A_i}^{sec}$
11. Если A_i хочет изменить свой выбор, то $A_i -> S : ID_i, E_{K_{A_i}^{pub}}(ID_i, u_i'), K_{A_i}^{sec}$

Протоколы голосования

Выбор без ЦИК

Рассмотрим случай, когда в голосовании участвуют 4 избирателя, которые используют одну и ту же асимметричную КС. $m_i = E_{K^{pub}_{A_1}}(u_{i1}, r_{i1})$

$u_{i1} = E_{K^{pub}_{A_2}}(u_{i2}, r_{i2})$

$u_{i2} = E_{K^{pub}_{A_3}}(u_{i3}, r_{i3})$

$u_{i3} = E_{K^{pub}_{A_4}}(u_{i4}, r_{i4})$

$u_{i4} = E_{K^{pub}_{A_1}}(v_{i1})$

$v_{i1} = E_{K^{pub}_{A_2}}(v_{i2})$

$v_{i2} = E_{K^{pub}_{A_3}}(v_{i3})$

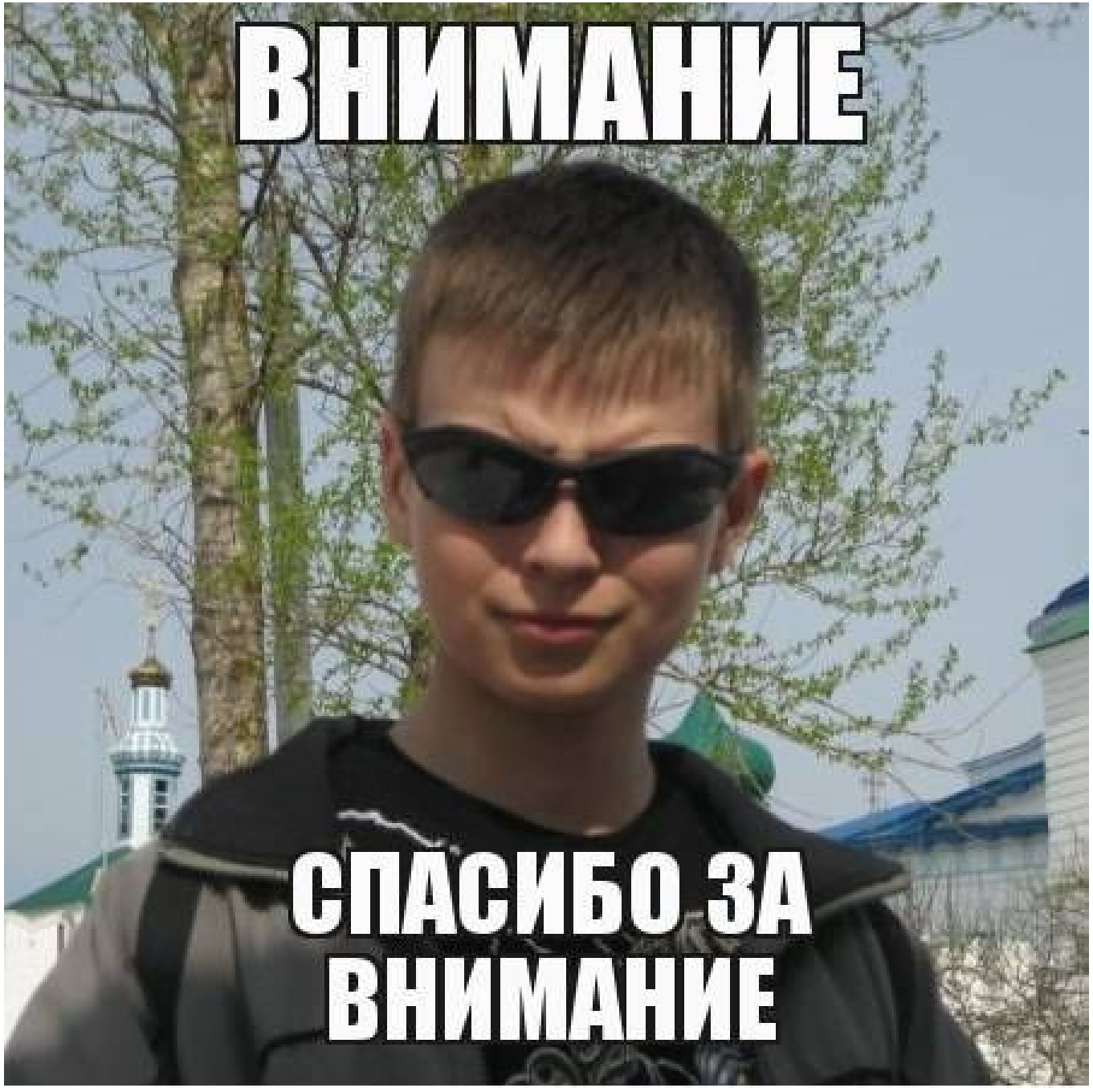
$v_{i3} = E_{K^{pub}_{A_4}}(v_{i,r_{i5}})$

v_i - бюллетень избирателя A_i

Протоколы голосования

Выбор без ЦИК

1. $\forall i\ A_i -> A_i : m_i$
2. $A_1 -> A_2 : \{u_{i1} \mid i{=}1,\ldots,4\}$
3. $A_2 -> A_3 : \{u_{i2} \mid i{=}1,\ldots,4\}$
4. $A_3 -> A_4 : \{u_{i3} \mid i{=}1,\ldots,4\}$
5. $A_4 -> A_1 : \{u_{i4} \mid i{=}1,\ldots,4\}$
6. $A_1 -> \{A_2, A_3, A_4\} : \{sign_{A_1}(v_{i1}) \mid i = 1, \ldots, 4\}$
7. $A_2 -> \{A_1, A_3, A_4\} : \{sign_{A_2}(v_{i2}) \mid i = 1, \ldots, 4\}$
8. $A_3 -> \{A_2, A_1, A_4\} : \{sign_{A_3}(v_{i3}) \mid i = 1, \ldots, 4\}$
9. $A_4 -> \{A_2, A_3, A_1\} : \{sign_{A_4}(v_{i4}) \mid i = 1, \ldots, 4\}$


ВНИМАНИЕ
СПАСИБО ЗА ВНИМАНИЕ