

Криптографические протоколы

Лекция 10

Протоколы голосования

Деркач Максим Юрьевич

November 6, 2019

Ссылки

<https://habr.com/en/post/436560/>

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 конфиденциальность решений, принимаемых абонентами.

Данная задача решается при помощи специальных протоколов.

Протоколы голосования

Понятие протокола голосования

Наиболее часто используются такие протоколы голосования, в которых

1. каждый агент отправляет 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 иметь, 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. $A_i \rightarrow S : E_{K_{A_iS}}(u_i)$
2. S вычисляет результат и публикует его.

В данном протоколе не выполняются почти все вышеперечисленные условия.

Протокол 2

1. $A_i \rightarrow S : E_{K_{A_iS}}(\text{sign}_{A_i}(u_i))$
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. $A_i \rightarrow S' : request$
2. $S' \rightarrow A_i : R_i$ - (случайный регистрационный номер).
3. $S' \rightarrow S : \mathbb{R}$ - список всех выданных регистрационных номеров.
4. $A_i \rightarrow S : (ID_i, r_i, u_i)$
5. s проверяет: $r_i \in \mathbb{R}$?. Если верно, то
 - 5.1 $\mathbb{R} = \mathbb{R} \setminus \{r_i\}$
 - 5.2 $\mathbb{S} = \mathbb{S} \cup \{ID_i\}$ (в начале работы $\mathbb{S} = \emptyset$)
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. $A_i \rightarrow S : intention$
3. S публикует список всех избирателей, собирающихся принять участие в выборах
4. $S \rightarrow A_i : ID_i$ - (регистрационный номер).
5. $A_i \rightarrow S : ID_i, E_{K_{A_i}^{pub}}(ID_i, u_i)$
6. S публикует $E_{K_{A_i}^{pub}}(ID_i, u_i)$.
7. $A_i \rightarrow S : ID_i, K_{A_i}^{sec}$
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 $A_i \rightarrow S : ID_i, E_{K_{A_i}^{pub}}(ID_i, u_i), K_{A_i}^{sec}$
11. Если A_i хочет изменить свой выбор, то $A_i \rightarrow S : ID_i, E_{K_{A_i}^{pub}}(ID_i, u_i'), K_{A_i}^{sec}$

Протоколы голосования

Гомоморфное шифрование в протоколах голосования

1. Избиратель получает токен в виде бюллетеня, который изменяет соответственно своему выбору. Разные избиратели получают разные бюллетени.
2. Избиратель шифрует бюллетень и отправляет его так, чтобы организаторы голосования получили зашифрованный бюллетень.
3. Организаторы публикуют зашифрованные бюллетени на доске объявлений.
4. Организаторы комбинируют зашифрованные бюллетени для подсчёта зашифрованного итога. Затем они расшифровывают его (но не сами бюллетени!) и публикуют результаты.

Получив результат и зашифрованные голоса, любой может проверить его корректность.

Протоколы голосования

Гомоморфное шифрование в протоколах голосования

На 4-м шаге организаторы комбинируют криптограммы для создания новой криптограммы, шифрующей сумму отдельных голосов.

Для этого схемы электронного голосования используют схему шифрования $Enc()$, в которой можно подсчитать $Enc(v1 + v2)$, имея на руках только $Enc(v1)$ и $Enc(v2)$, и не зная ключа шифрования. Такие схемы шифрования называются гомоморфными ($Enc(v1) \times Enc(v2) = Enc(v1 + v2)$).

К примеру, если сильно упростить, избиратели США производят следующие действия 8 ноября:

Получают от организаторов бюллетень «Клинтон» и бюллетень «Трамп» (для простоты рассмотрим всего двух кандидатов).

Пишут на одном бюллетене $Enc(1)$, а на другом – $Enc(0)$, используя в качестве ключа публичный ключ, выданный организаторами.

Протоколы голосования

Гомоморфное шифрование в протоколах голосования

Зашифрованные бюллетени затем публикуются на доске объявлений вместе с ID избирателя. Все знаю, кто

проголосовал, но невозможно понять, за кого именно, поскольку каждые $Enc(0)$ и $Enc(1)$ уникальны, а мы используем сильное и рандомизированное шифрование. Если

бы шифрование было детерминистское, избирателя можно было бы заставить раскрыть его голос, вычислив $Enc(0)$ заново и сравнив его со значением на доске.

Протоколы голосования

Выбор без ЦИК

Рассмотрим случай, когда в голосовании участвуют 4 избирателя, которые используют одну и ту же асимметричную

$$KC. m_i = E_{K_{A_1}^{pub}}(u_{i1}, r_{i1})$$

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

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

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

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

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

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

$$v_{i3} = E_{K_{A_4}^{pub}}(v_{i4}, r_{i5})$$

v_i - бюллетень избирателя A_i

Протоколы голосования

Выбор без ЦИК

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

