Университет ИТМО, факультет программной инженерии и компьютерной техники
Двухнедельная отчётная работа по «Информатике»: аннотация к статье
Дата лекции: ___17.09.2020_____ Дата сдачи: __01.10.2020_____

Выполнил(а) Сенина М.М., № группы *P3112*, оценка _____
Фамилия И.О. студента — не заполнять

**Название статьи/главы книги/видеолекции**
*Можно ли генерировать случайные числа, если мы не доверяем друг другу?*

| **ФИО автора статьи (или e-mail)** | **Дата публикации (не старше 2018 года)** | **Размер статьи (от 400 слов)** |
|---|---|---|
| *Александр Скиданов*<br>*https://habr.com/users/SkidanovAlex/* | *«29» Сентября 2020* | *1971 слов* |

**Прямая полная ссылка на источник и сокращённая ссылка**
*https://habr.com/ru/company/near/blog/521090/*

**Теги, ключевые слова или словосочетания**
*Случайные числа, криптография, распределённые системы*

**Перечень фактов, упомянутых в статье**
1. *Считается, что чтобы считать случайное число очень хорошим, т.е. честным, надо, чтобы на результат не мог повлиять злоумышленник среди пользователей, чтобы результат был непредсказуемым для всех пользователей, и процесс был бы защищённым от того, что какой-то процент пользователей отклонится от протокола.*
2. *Метод RANDAO + VDF – основан на проведении двух фаз – генерации локального случайного числа у пользователя и предоставления хеша этого числа, как знака о готовности к следующей фазе, и раскрытие сгенерированных чисел пользователями по установленному порядку.*
3. *Метод стирающихся кодов – основан на трёх фазах – генерация случайных чисел-строк и доказательства их валидности у пользователей, разбиение этих строк на подстроки и шифровка подстрок для каждого другого пользователя в системе их открытыми ключами, сверка того что все зашифрованные подстроки валидны – расшифровка и определение итогового случайного числа по более чем 2/3 полученных чисел.*
4. *Метод пороговых подписей – применяется обычно для совместной подписи общего сообщения, в нём пользователи тоже на основании текста и приватного ключа сообщения генерируют свои личные подписи, и любых 2/3 подписей достаточно для получения итоговой подписи, на которую оставшаяся 1/3 повлиять не сможет.*

**Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)**
1. *Метод RANDAO + VDF – простой в реализации, если брать простую VDF функцию.*
2. *Метод стирающихся кодов работает даже, если в системе 1/3 злоумышленников.*
3. *Метод пороговых подписей требует куда меньшее количество по сравнению с методом стирающихся кодов, хотя гарантии имеет те же.*

**Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)**
1. *Чтобы делать очень хорошие простые числа надо иметь много пользователей в системе.*
2. *Метод RANDAO + VDF – плохо (долго и не безопасно) работает, если у кого-то из пользователей есть очень хорошее оборудование.*
3. *Алгоритмы согласия с результатами (алгоритмы консенсуса) во всех трёх алгоритмах играют ведущую роль и определяют реальные параметры алгоритма, так что заранее судить и абсолютно чётно сравнивать их сложно.*

**Ваши замечания, пожелания преподавателю *или* анекдот о программистах[1]**
*— Сколько программистов надо, чтобы закрутить лампочку?*
*— Ни одного! Это аппаратная проблема, программисты их не решают.*
*(хотя тыжпрограммист никто не отменял, наверное…)*