Student: Maksim Kryuchkov
Group: M3339
Date: 3 октября 2018 г.

KEK

Oracul

Def *Оракул*
Черный ящик
$O : \{0,1\}* \to \{0,1\}*$
Если новая строка, он выдает случайную строку, иначе выдает то, что уже было раньше, то есть хеширует строку.
Смотрит в хеш-таблицу, если там ничего нет, выдает случайную строку

Anna, Boris and Victor

A(k) – m – Б(k) – m – B
Виктор притворяется Анной, ему известно m, H
Можно вместо m слать $(m, H(k||m))$
Если H определенного вида, то можно дописывать сообщение m.
Есть стандарт HMAC - не позволяющий подобным образом дописывать сообщения.

Крипто-конверт на основе хеш-функции

А, Б.
Выкидывают биты, если ксор равен 0 выигрывает Анна, иначе Борис.
Как поиграть в такую игру?
Анна кладет свой бит в конверт, как и Борис. Чужой конверт нельзя вскрыть. Можно вскрыть, когда владелец дает некоторый ключ. В конверте не может оказаться другого значения, нежели было то что было положено.
$params \leftarrow Gen(1^n)$
$c \leftarrow Commit(params, m, r)$
$\{accept, reject\} = Reveal(params, c, m, r)$
Нас интересуют два свойства
1. Секретность - зная c и params нельзя ничего сказать о сообщении m.
2. Целостность - зная params, m, r - нельзя найти m' и r', такие что $m \neq m'$, но $Commit(params, m, r) = Commit(params, m', r')$
Пример крипто-конверта
$Gen = \emptyset$
$Commit(m, r) = H(m||r)$
$Reveal(c, m, r) = (c = H(m, r))$

Data Structures

4 функции: setup, prove, verify, update
Есть много файлов, мы их загружаем в облако

Хотим, чтобы нам выдали один файл.
Хеш-список плох, потому что выдает много памяти?
Def *Merkle tree*
Есть набор сообщений m_i. Считаем от них хеши, помещаем в листья
Есть уровень h_{00}, h_{01}, над ними нод $h_0 = H(h_{00}||h_{01})$
Этои индукционный переход построения дерева
$auth(D_0)$
d_0 - вершина дерева
D_0 - листья
В качестве доказательства π выступают соседи по пути наверх
Verify видимо просто хеширует все подряд по пути наверх и проверяет на равенство в конце.
Разреженные деревья
Кроме доказательства наличия можно делать и доказательства отсутствия

sha256 в джаве base64 в джаве