Blockchain Technology and Applications(CS731)
Indian Institute of Technology Kanpur
Homework Assignment Number 2

Student Name: Shivank Garg
Roll Number: 160658
Date: February 15, 2019

QUESTION
1

1 Hash functions and proofs of work

Let, $H : P \times S = \{1, 2, ..., 2^n - 1\}$ is a collision resistant hash function.
Now, construct $H' : P \times S = \{1, 2, ..., 2^{n'} - 1\}$ such that $n' = n + \log_2 d$,and fixed difficulty is d H' has n' bits as defined. Also, we can now assume H' is concatenation of H and a string(D) of $\log_2 d$ bits $H' = D|H$ Since, H is a collision resistant. Therefore, H' is also collision resistant. Because if we find a collision in H', then there is also a collision in H. Since H is part of H', therefore if H' is same for two value then H has to be.

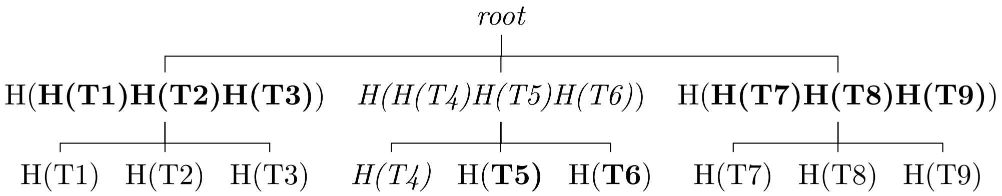
If D = 0 then there will be zeroes in the beginning of H'. Hence, H' is of effective length $(n' - \log_2 d)$ bits. Now, For every puzzle $p \epsilon P$ it is trivial to find a solution $s \epsilon S$ such that $H'(p, s) < 2n'/d$. Therefore, H', being collision resistant, is not proof of work secure with difficulty d.

Blockchain Technology and Applications(CS731)
Indian Institute of Technology Kanpur
Homework Assignment Number 2

Student Name: Shivank Garg
Roll Number: 160658
Date: February 15, 2019

QUESTION 2

Part (a)



Given, Alice commits S into a ternary Merkle tree. She also published(or stored) the root, so that it cannot be tempered or changed by some adversary. Now, if she wants to prove to B that T4 is in S, she will calculate H(T4) and follow the path to root by calculating Hash of other hashes with it. These other hashes are given to Bob as proof at time of committing S. If the calculated root hash matches with stored root hash, it is proved using **Binding Property**.
Note- In graph, **Bold** values denotes the hashes that bob has as proof. *Italic* value denotes the hashes that are computed to prove that T4 is in S.

Part (b) Length of proof that some T_i is in $S = (k-1)log_k n$. where tree is k-ary and n are total number of leaf nodes.
Length of proof comes out to be of O(height of k-tree), since it Alice has traverse along the height of tree.

Part (c) In Binary tree, Computational cost is $\log_2 n$.
In k-ary tree, total computational cost is $(k-1)log_k n$. Since there are $(k-1)$ nodes at each level to be hashed to compute the parent. We can write $(k-1)log_k n = \frac{(k-1)log_2 n}{log_2 k}$

$\frac{k-1}{\log_2 k} > 1 \implies$ if k increases then $(k-1)log_k n$ increases, therefore, computational cost increases in k-ary tree than binary tree.(overhead is more in k-ary tree)

$$Ratio(comparison) = \frac{(k-1)}{\log_2 k}$$

Advantage of using k-ary merkle tree(over binary) is verification of $T_i \epsilon S$ is faster than binary merkle tree, since less number of hashes are being computed at time of verfication.

$$\frac{Number\ of\ hashes\ to\ verify\ T_i\ in\ k-ary\ tree}{Number\ of\ hashes\ to\ verify\ T_i\ in\ binary\ tree} = \frac{1}{log_2 k}$$

Blockchain Technology and Applications(CS731)
Indian Institute of Technology Kanpur
Homework Assignment Number 2

Student Name: Shivank Garg
Roll Number: 160658
Date: February 15, 2019

QUESTION 3

Part (a) Bob stores hashes of phone number(10^{10} permutation) mapped with 'contact name' on his server. Now, Bob can launch a rainbow table attack on his server to know the actual phone number. Size of rainbow table is large but bob can use special hardware to brute-force hash all the possible phone number and search them in his database.

Part (b) Using a random nonce(r) will prevent the rainbow table attack, but now Bobcrypt users will not be able to discover other Bobcrypt users. This is because application will now produce different nonce(r)for different users and this makes Hash(N,r) different. and there is no way to match the contacts phone number hash, so that, App will unable to tell which of the alice's friends use BobCrypt.

Blockchain Technology and Applications(CS731)
Indian Institute of Technology Kanpur
Homework Assignment Number 2

Student Name: Shivank Garg
Roll Number: 160658
Date: February 15, 2019

QUESTION 4

Problem 4 :

Part (a) ScriptSig: $< password >$
script: $< password >$ `OP_SHA1` $< 0xeb271cbcc2340d0b0e6212903e29f22e578ff69b >$ `OP_EQUAL`

Part (b) This Transaction does not contain any signatures and thus any transaction attempting to spend them can be replaced with a different transaction sending the funds somewhere else, since password is visible to everyone and they can make new version that transfers bitcoin to them.

Part (c) Yes, Implementing P2SH will fix this security issue. Since, the recipient must provide a script matching the script hash and data which makes the script evaluate to true. Pay-to-script is hidden from blockchain. Recipients of the sent bitcoins will then generate a signature script, which is used to satisfy a P2SH. In this implementation, only Alice knows the script, so her password cannot leak unless she redeem the the transaction from script.

Blockchain Technology and Applications(CS731)
Indian Institute of Technology Kanpur
Homework Assignment Number 2

QUESTION 5

Student Name: Shivank Garg
Roll Number: 160658
Date: February 15, 2019

Part (a) Alice should send to bob, all block headers from block containing her transaction to current block header and merkle proof of her transaction. With all information of all the block headers upto that transaction, bob can first verify all the block-headers, then he can verify that the merkle proof of that transaction obtain correct merkle root. After this computation, he can be sure that the transaction is valid.

Part (b)

$$n = 256, k = 8,$$

Size of Bitcoin Header = 80 Bytes
number of SHA256 hashes in merkle proof of binary merkle tree = $log_2 n = 8$ Size of SHA256 hash = 32 Bytes
So, total proof size = $80 * 8 + 32 * 8 = 896 Bytes$

Part (c) If the new field is used, we can reduce the proof size such that, the Alice's transaction containing block is smallest in size, then it is Best Case. Expected proof size = 256 bytes. Since only merkle proof is sent.
Worst case proof size = same as in part (b) = $O(k * 80 + 32 * \log_k n)$

Blockchain Technology and Applications(CS731)
Indian Institute of Technology Kanpur
Homework Assignment Number 2

Student Name: Shivank Garg
Roll Number: 160658
Date: February 15, 2019

QUESTION 6

Problem 6 :

Part (a) Bitcoinia can implement LOCK_TIME feature of bitcoin, by changing the field to saturday(or weekend). So that, miners will not accept the transaction until the LOCK_TIME field is exceeded.

Part (b) In new design, factory can generate week n+1 keys when week n keys are printed. Now, at the time of printing week n private key, factory can sign a transaction with it to pay on Week n+1 address (HASH(week n+1 public key)) with LOCK_TIME of monday(when next lottery is being opened). In this design, factory is assumed to be trustworthy as they are responsible of organizing lottery. Else, no way is possible if factory is malicious.