HW1

Tianbo Qiu (tq2137)

February 11, 2019

Problem 1

1

Preimage resistant: Given the output y of n bits, it will take $O(2^n)$ time to find the preimages x such that $y = h(x)$.
Collision resistant: Given an output size of n bits, it will take $O(2^{\frac{n}{2}})$ time to find two distinct values x and x' such that $h(x) = h(x')$.
Second preimage resistant: Given an output of n bits and a message x, it will take $O(2^n)$ time to find another message x' such that $h(x) = h(x')$.

2

False, the hash value of the message is encrypted with a user's private key.

3

RSA and Elliptic Curve can be used for digital signature.

4

For any point G on the elliptic curve, a new point $Q = kG$ for a scalar k forms a cyclic subgroup. Given G and Q, it is computationally infeasible to find k. Suppose $k = 2^n$, it will take $O(2^n)$ time to find k.

Problem 2

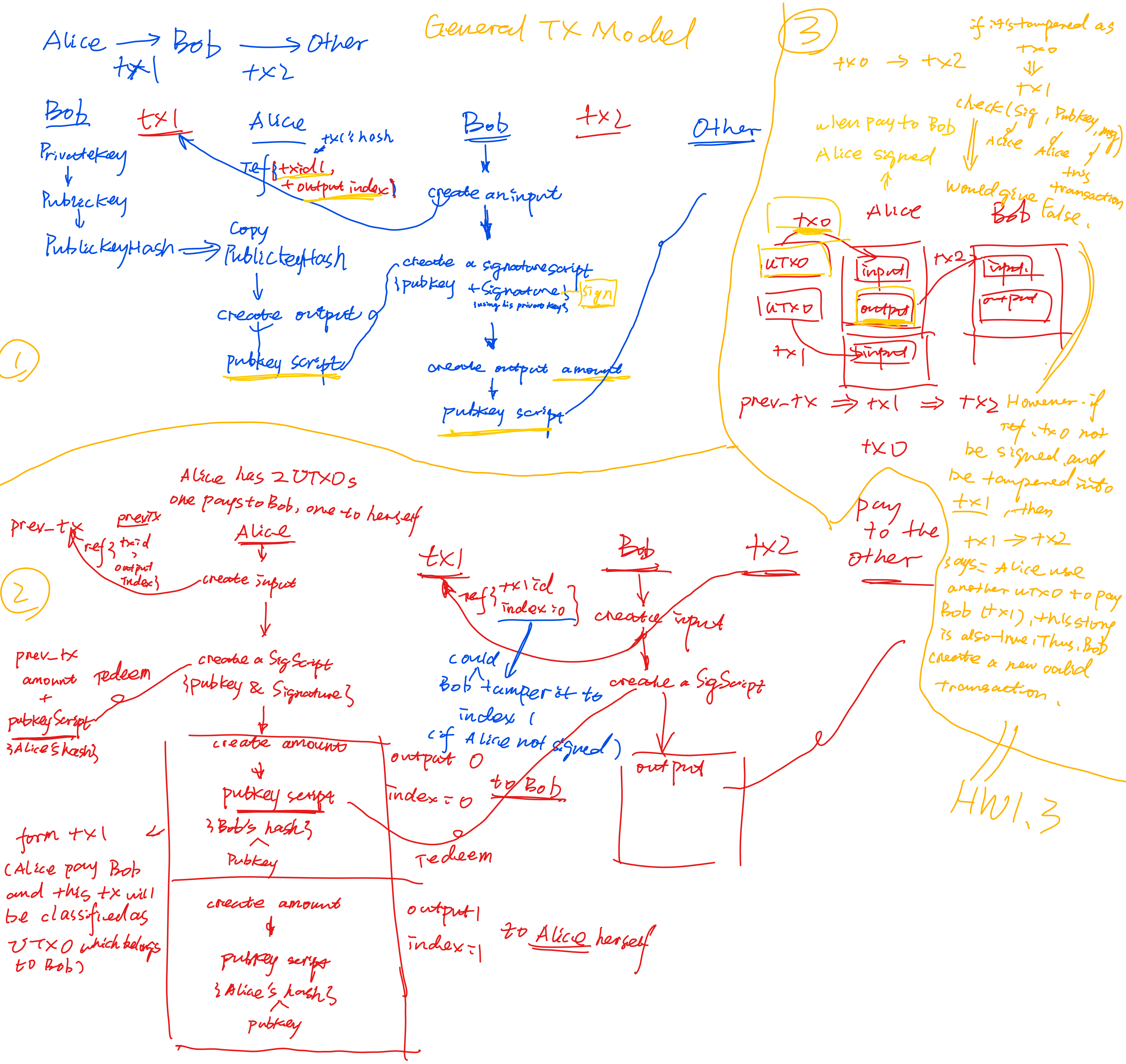
Given $n = 1.2\sqrt{N}$.

$$\begin{aligned} Pr[r_i = r_j | i \neq j] &= 1 - \frac{N-1}{N}\frac{N-2}{N}\cdots\frac{N-n+1}{N} = 1 - \prod_{i=1}^{n-1}(1 - \frac{i}{N}) \\ &\geq 1 - \prod_{i=1}^{n-1} e^{-\frac{i}{N}} = 1 - e^{-\frac{1}{N}\sum_{i=1}^{n-1} i} \geq 1 - e^{-\frac{n^2}{2N}} \end{aligned} \tag{1}$$

$$n = 1.2\sqrt{N} \Rightarrow \frac{n^2}{2N} = 0.72 \Rightarrow (1) \geq 1 - e^{-0.72} = 0.53 \geq \frac{1}{2} \tag{2}$$

Problem 3

1


General TX Model
Alice → Bob → Other
tx1
tx2
Bob
Privatekey
Pubkey
PublicKeyHash
Copy
PublicKeyHash
create output
pubkey script
tx1
Alice
tx1's hash
ref{txid1, + output index}
Bob
create an input
create a signatureScript
{pubkey + Signature}
(using his private keys)
sign
create output amount
pubkey script
tx2
Other
1
3
tx0 → tx2
if it's tampered as
tx0
tx1
check(Sig, Pubkey, msg)
Alice Alice this
would give transaction False.
when pay to Bob
Alice signed
tx0
Alice
Bob
UTXO
UTXO
input
output
tx2
input
output
tx1
input
prev_tx ⇒ tx1 ⇒ tx2
However, if ref, tx0 not be signed and be tampered into tx1, then
tx1 → tx2
says: Alice use another UTXO to pay Bob (tx1), this story is also true. Thus, Bob create a new valid transaction.
tx0
pay to the other
HW1.3
Alice has 2 UTXOs
one pays to Bob, one to herself
2
prev_tx
prevTx
ref{txid, output index}
Alice
create input
create a SigScript
{pubkey & Signature}
prev_tx
amount
+
pubkeyScript
{Alice's hash}
redeem
create amount
pubkey script
{Bob's hash}
Pubkey
create amount
pubkey script
{Alice's hash}
pubkey
form tx1
(Alice pay Bob and this tx will be classified as UTXO which belongs to Bob)
output 0
index = 0
to Bob
redeem
output 1
index = 1
to Alice herself
tx1
ref{tx1 id, index = 0}
could
Bob tamper it to index 1
(if Alice not signed)
Bob
create input
create a SigScript
output
tx2