

-
- Midterm
 - Bloom Filters
 - cuckoo filters
 - IBLTs
-

Midterm

- Next week here
- Partial Credit!
- 8.5" x 11" Handwritten by YOU! cheat sheet double sided
- Topics • Anything prior to today
 - No Qs on elliptic curve underlying math
 - Mathematical groups
 - Diffie Helman
 - Schnorr sigs
 - Bitcoin Blockchain
 - POW
 - header structure, field purpose
 - Block structure
 - tx structure

- Merkle trees
- Cryptographic Hashes
- Blockchain block discovery (mining)
 - Math (Poisson, mining race eqn
target probabilities & difficulty

$$\text{difficulty} = \frac{\text{starting target}}{\text{current target}}$$

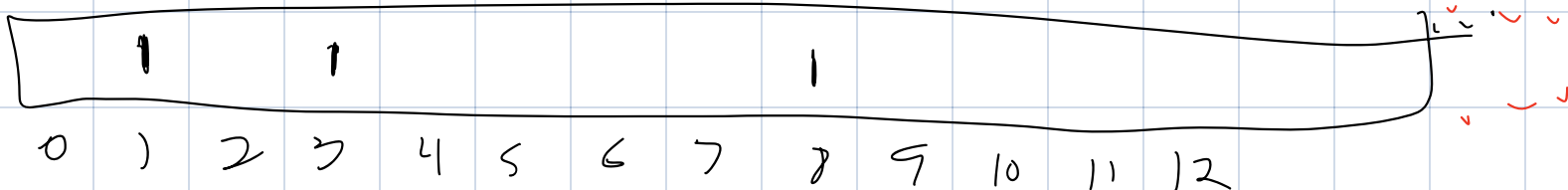
- Attacks

- selfish
- double spend
- Sybil
- eclipse
- attacks against groups (schnorr formations,
insecure groups)

- Networking

- clocking
- simple proofs

Bloom Filters



• insert ~~x~~
 $\rightarrow H_0(x) \stackrel{\text{mod } N}{=} 3$
 $\rightarrow H_1(x) = 1$

• insert y
 $H_0(y) = 1$
 $H_1(y) = 8$

• Lookup x $\rightarrow$

$H_0(x) = 3$ is bit 3 set?

is bit 1 set?

if all are set return **True**

MAYBE IN SET!

$\rightarrow$ any are NOT set return False

$\rightarrow$ Definitely not in set

• ~~Remove?~~

• Expansion X

• Union $\checkmark$

Cuckoo Filter / Hashing

N buckets (Binary Fuse Filter)

[insert x : $\rightarrow H_0(x) \bmod N \rightarrow \text{bucket}_0$
 $\rightarrow H_1(x) \bmod N \rightarrow \text{bucket}_3$

insert m bits of x
 if both filled, replace & reinsert!
 if it exists Return true $\checkmark$

Lookup x : $H_0(x) \bmod N \rightarrow$ does it match
 $H_1(x)$

if no matches Return False
NOT IN TABLE!

FPR: $\frac{1}{m}$

- deletion (Partly)
- expansion of size (partly)
- yes but may take a long time

IBLT Invertible Bloom Lookup Table

table of

0	1	2	
Count +2	1	15	
keysum 5	3	2	
valuesum 513	8	5	...

insert x, v : $h_0(x) = 0$

2, 5 $h_1(x) = 2$

lookup x : $h_0(x) = 0$

$h_1(x) = 2$

3, 8 $h_0(3) = 0$
 $h_1(3) = 1$

are any containers of count 1?

if so, do they match the key

Removal: invert
insert

Peel: $\rightarrow$ Loop

Look for bucket with count = 1

if found, remove item

if all buckets are count = 0, $\checkmark$

if all buckets are > 1 or 0 $\times$