CSE 539: Applied Cryptography

Class:                   Date:                  Spring 2015

Diagram:

\[ f(x) \]

Correct?

An example of a cipher to address anonymous time is a timestamp.
A time stamped

TT stereo (ALice & know of bec

TT trusted time stamps

Sonno (Alice, bee, know)

Alice creates a document

Trust report by
Alice sees it.

Like a sheriff, by TT.

"Alice, TS, here already!"

Alice tells TT: Because.
See it, but make it

The looked forward for
Alice is given $D_n$ and $\text{Hash}(L_n-1)$.

$L_n = H(2D_{n-1}, H_{n-1}, H_{n-2}, \ldots, L_{n-2})$

Sign $W_n \rightarrow H_n \rightarrow H_{n-1} \rightarrow H_{n-2}$

Sign $W_n \rightarrow H_n \rightarrow H_{n-1} \rightarrow H_{n-2}$

If $W_n$ succeeds to Alice

If $W_n$ succeeds to Alice
An is

Lot of peers each have

No shared path

DHT > distributed hash table

Dishbusted protocol
for each element \( \eta \in (H^0)^3 \), \( \eta = (\eta^1, \eta^2, \eta^3) \)
So there was a 50.

As I researched, say so.

Some people misunderstand the
people to think her Investiga-

Alicia needed to get those (ex)

I'd like a reduction function

I msg each lead to a unique


I read the document.

- Understandably
- Inappropriately
- Very frequently
- Unfairly
- Apparently
- Disturbingly

Alice is already to sign for her

Frey S. Greene
Signature
Existential forgery.

Alice signs $D_1$ & $D_2$ \rightarrow $s_1$, $s_2$

Bob creates $D_1 \times D_2 = D'$

$s_1 \times s_2 = s'$

$s'$ is Alice's sig on $D'$
Some person

Join approval to be
an member can be
from friend & signs a brief card
be part of everyone in
friend, best, & Alice delicious

Grand Signature
In conclusion, we have

An essential lesson

Always prepare for each

Accomplished

To keep things meaningful
Alice issues a large # of group certificates to each member.

Member sign using any member's cert.

random sign using any cert belongs to member I -

(Alice can track)
2. Bed cannot see (see: L6620)

1. No medical examination

Given these events:

Alice used bed to bleeding

Alice gave BOC to L6620

Bled: Signature
$\mathbb{E}_{\text{perm}(m)} \pi(m)$