

Fixing OCSP for Fun and Profit

David Adrian
@davidcadrian



UNIVERSITY OF
MICHIGAN

OCSP Is Unreliable

Certificate revocation doesn't work.

CRLs are too big and slow.

CRLSets are too small.

OCSP is slow / unreliable / fails open / leaks visited domains.

OCSP stapling is **fail open**.

Solutions

OCSP Must-Staple is too **scary**. Web servers are **bad at stapling**.

Chrome Expect-Staple preload list is only useful for measurement papers.

What to do? How do we really solve revocation?

Gamification!

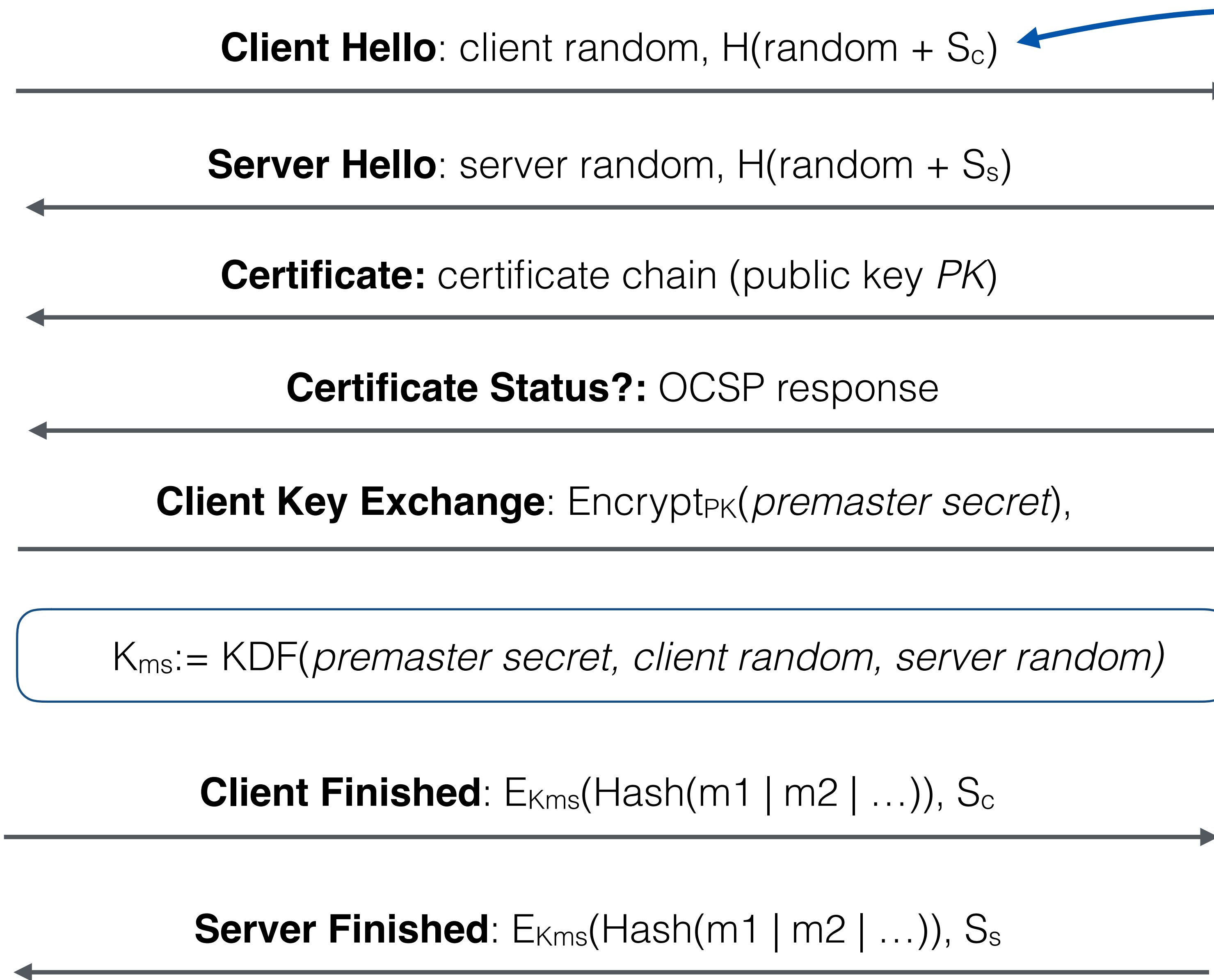
OCSP Suspect-Staple

Client and server guess if web server will correctly staple

Commit to guess in Client/ServerHello

Incentivize servers to staple

Gamification!



LSB 1 = Yes
LSB 0 = No





	Client: Yes Server: Yes	Client: Yes Server: No	Client: No Server: Yes	Client: No Server: No
Server Staples	—	—	Server sends client a bobcat	Client sends server candy
Server Does Not Staple	Client sends server a bobcat	—	Server sends client candy	—

Coming to an IETF standard near you!

Fixing OCSP for Fun and Profit

David Adrian
@davidcadrian



UNIVERSITY OF
MICHIGAN