CS558 Network Security

hello

21

Lecture ~~20~~: OPAQUE

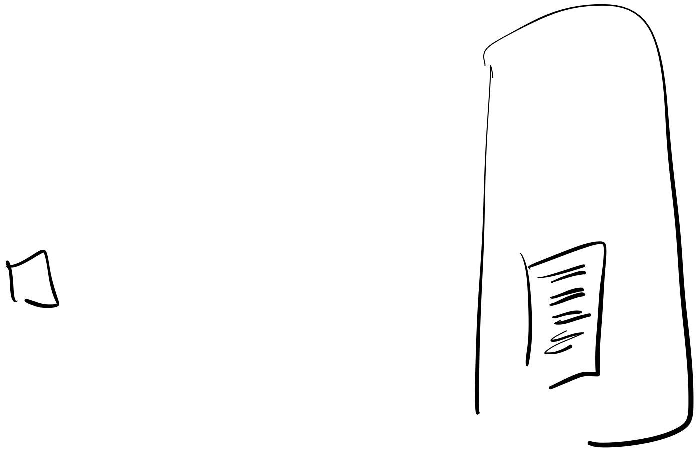
BOSTON UNIVERSITY

The Password Problem

- Dictionary Attacks
- Password Stealing

low Entropy / Easy to guesss

Passwords leaking



① Password Hashing

username : password

↓

username : H(password)

username : password

H(   )

equality check

Dictionary Attack

Precomputation attacks

② Salting the hash

username : Salt : H(Salt||Password)

Bob : Salt$_2$: H(Salt$_2$ || P$_2$)

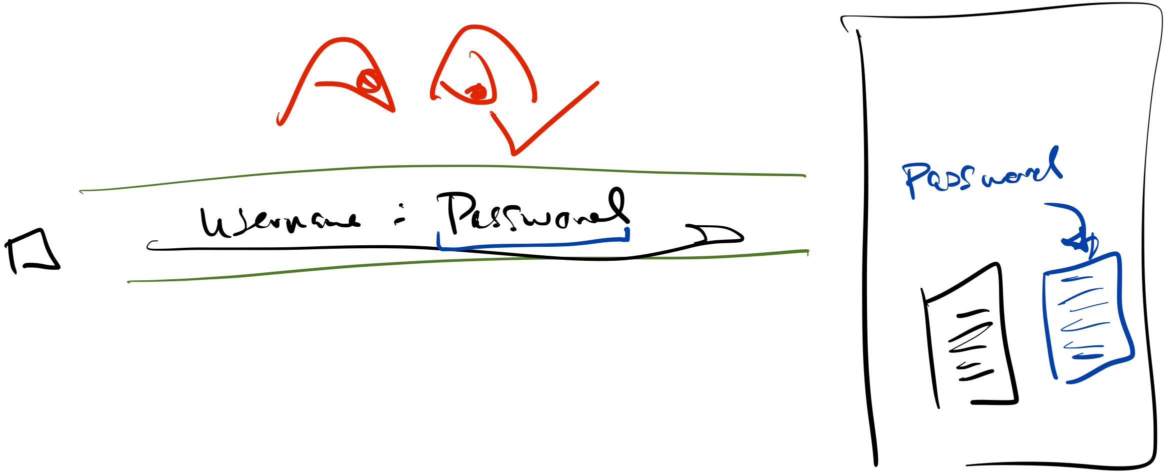
↑

"Slow" hash functions

Time-lock Puzzles and Memory Hardness

$H(H(H(H(\text{Salt} \| \text{pwd}))))$

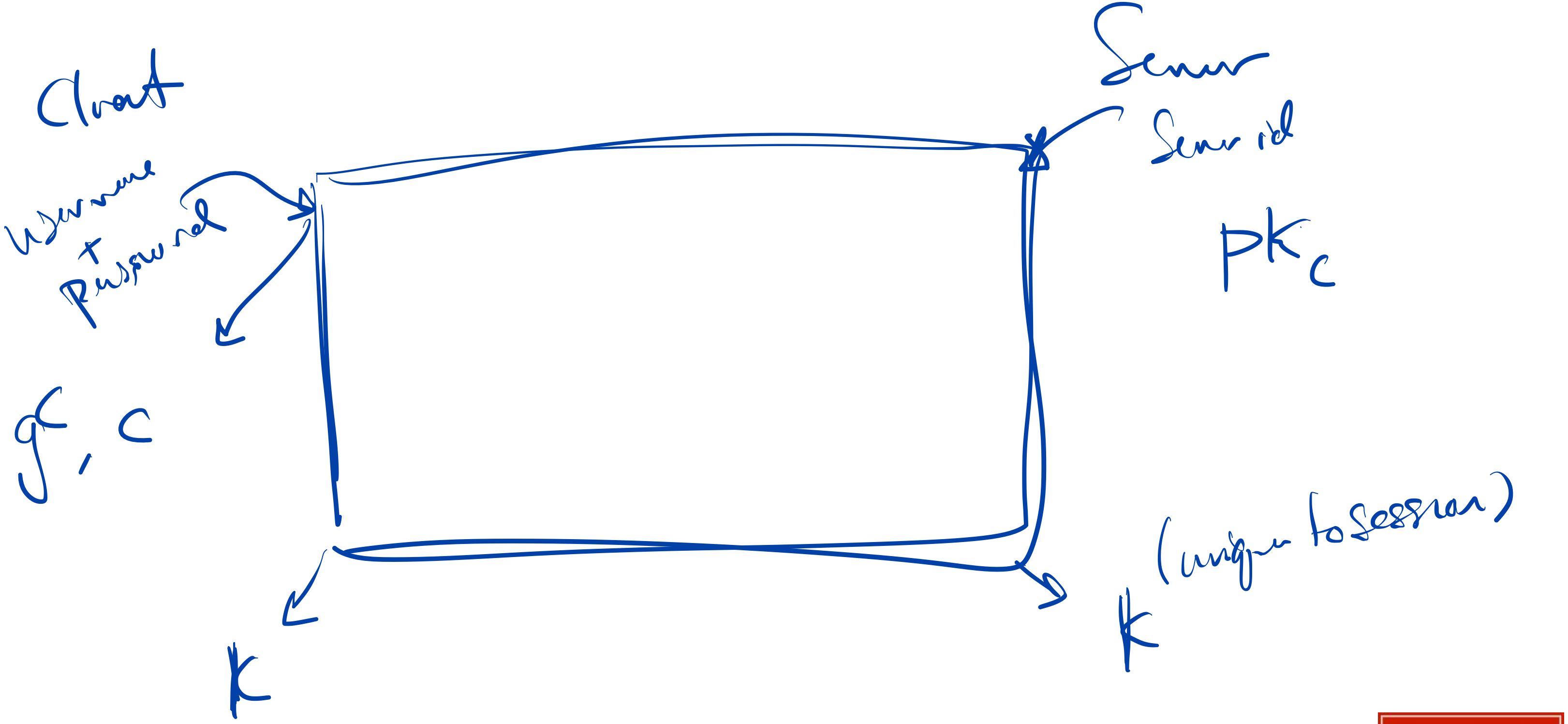
SCRYT


Username : Password
Password

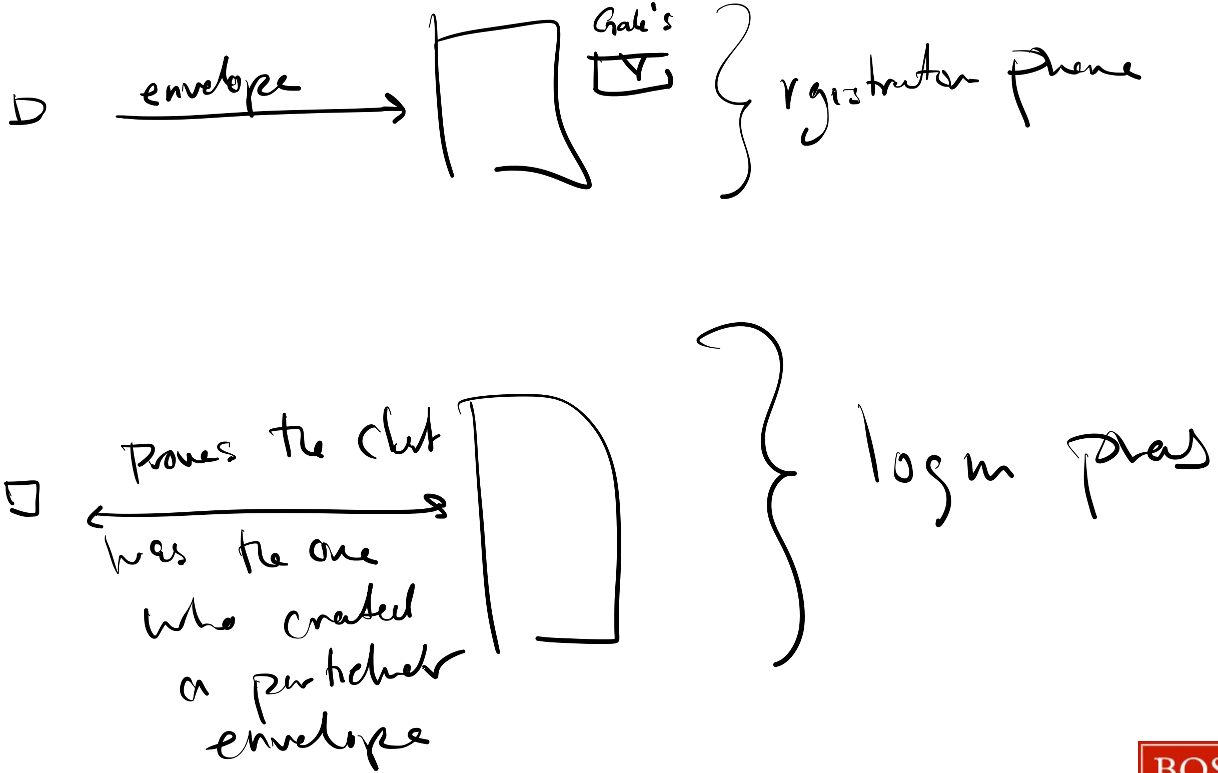
OPAQUE Goals

- Authenticated Server
- Authenticated Client
- Client only needs a username/password
- Forward Secrecy
- Pre-computation Resistant

Password Authenticated Key Exchange

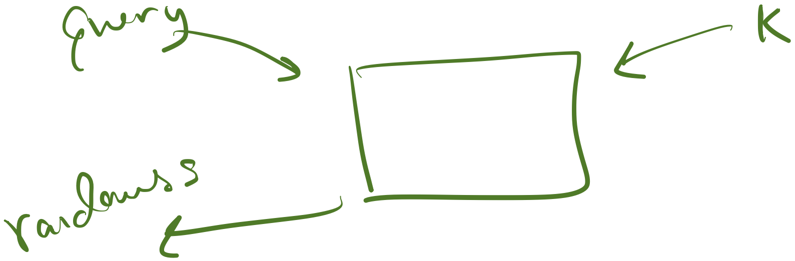


OPAQUE At a High Level



Oblivious $\underbrace{\text{Pseudorandom Functions}}$

$PRF(K, query) \longrightarrow$ looks random



$H(alice) \rightarrow g_1$

$H(Bob) \rightarrow g_2$

$H: \{0,1\}^* \longrightarrow \mathbb{G} \rightarrow g$

query Client

Server k

$H(\text{query}) \rightarrow g$

$b \leftarrow \mathbb{Z}_q$ $\xrightarrow{g^b}$

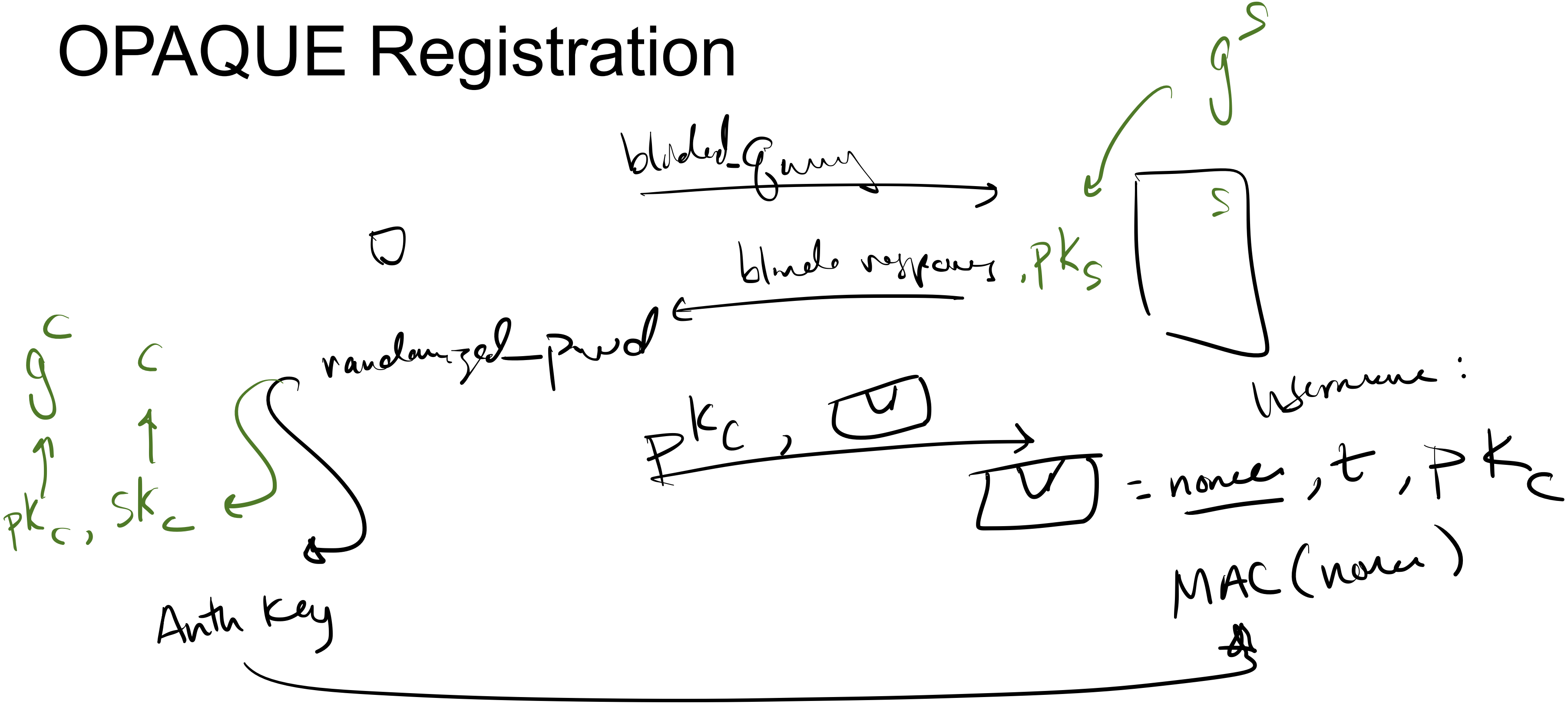
b^{-1}

$\xleftarrow{(g^b)^k}$

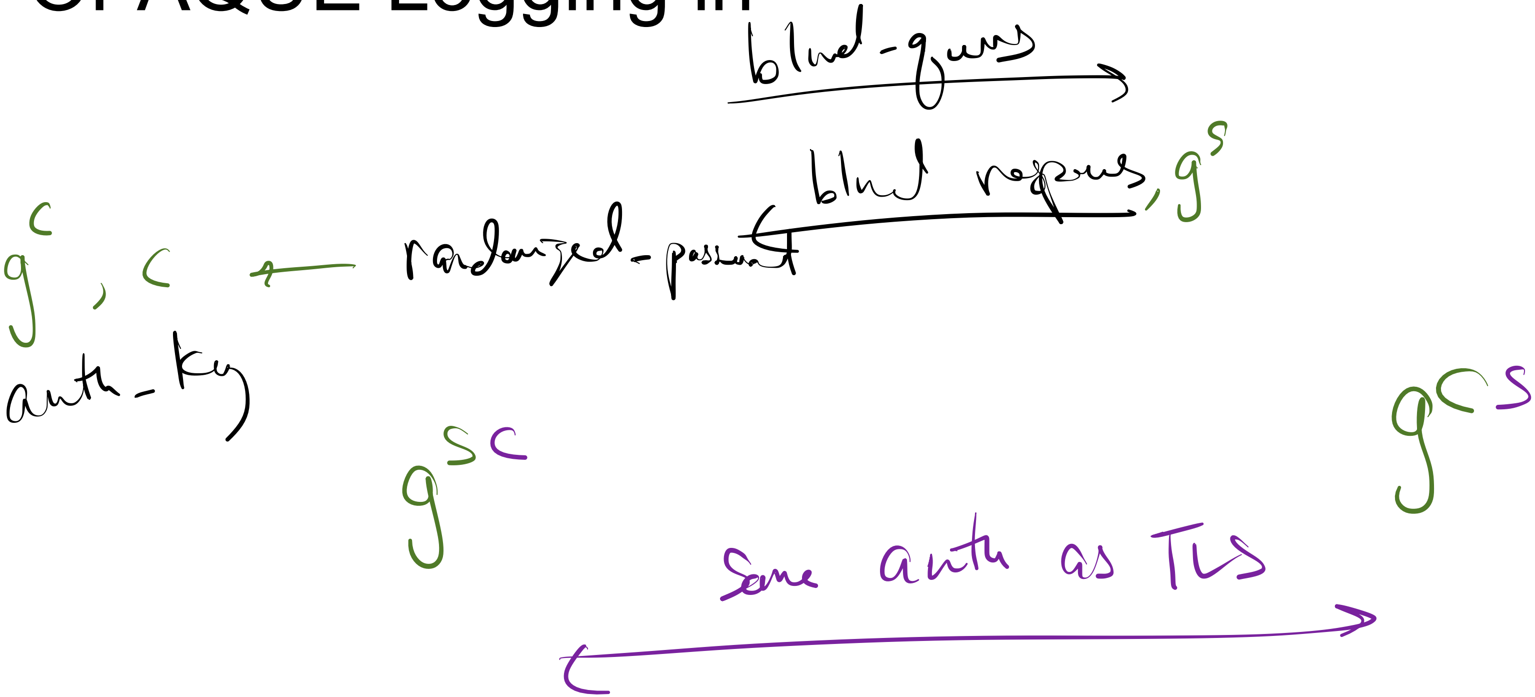
$$\left(g^{bk}\right)^{b^{-1}}$$

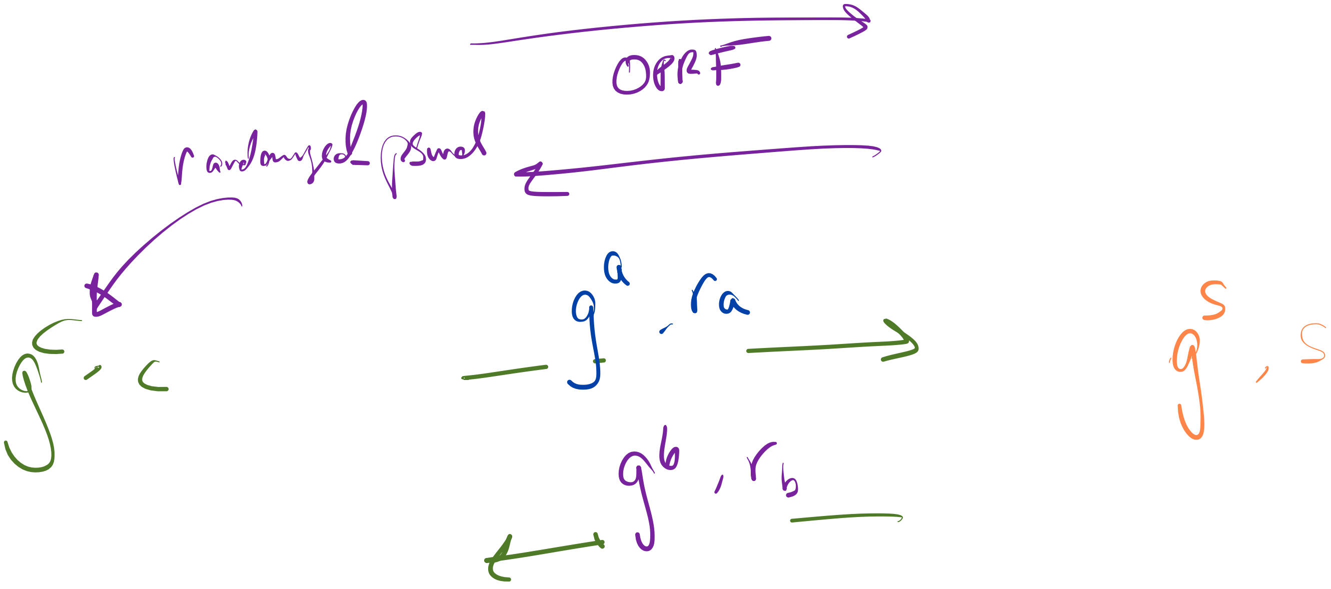
$$= g^{b \cdot b^{-1} \cdot k} = g^k$$

OPAQUE Registration

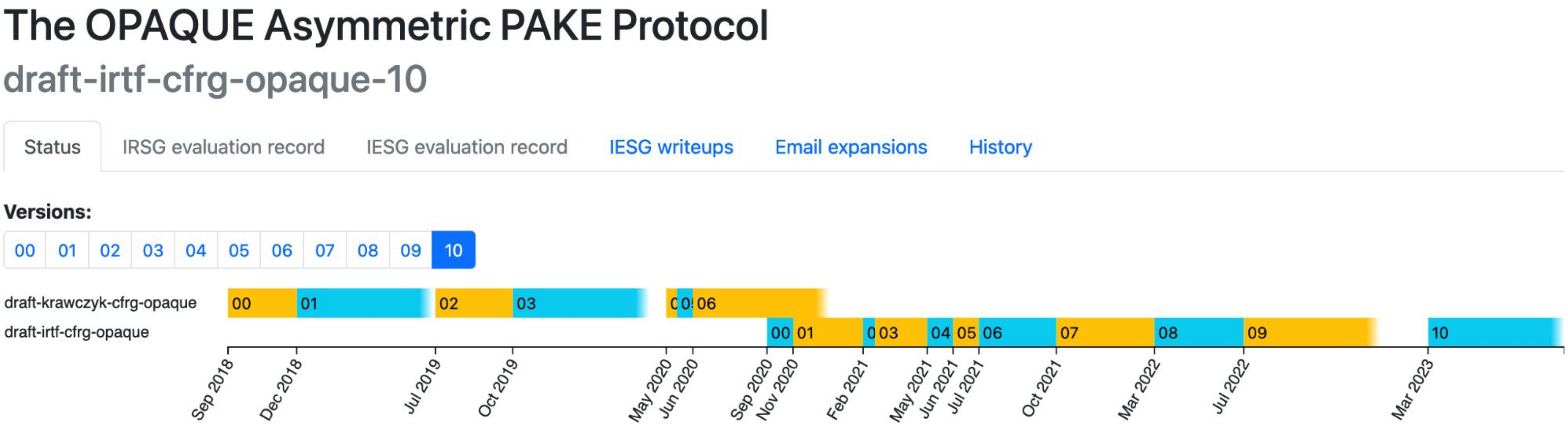


OPAQUE Logging in





$$K = H(g^{as} \| g^{bc} \| g^{ab} \| r_a \| r_b \| \text{nonce})$$



The OPAQUE Asymmetric PAKE Protocol

draft-irtf-cfrg-opaque-10