PAKE - Password Authenticated Key Exchange

Prof Bill Buchanan, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY

The problem with passwords, hashing and salt

User: alice

Password: qwerty

alice:$apr1$6Jda0$jkPR037bdd=

hash

salt

Hash(“123456”+”6Jda0”)

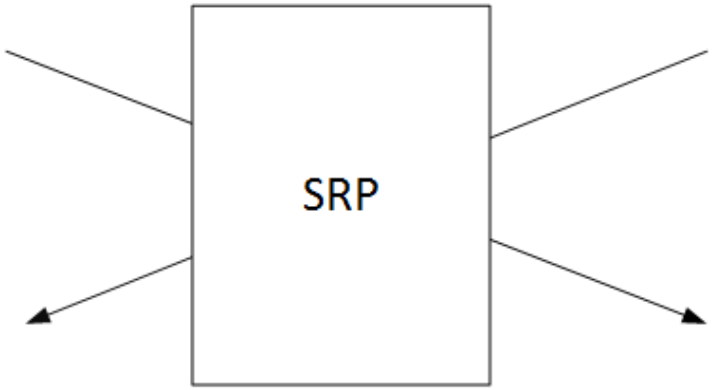
Hash(“password”+”6Jda0”)

Hash(“qwerty”+”6Jda0”)

SRP

“mysecret”

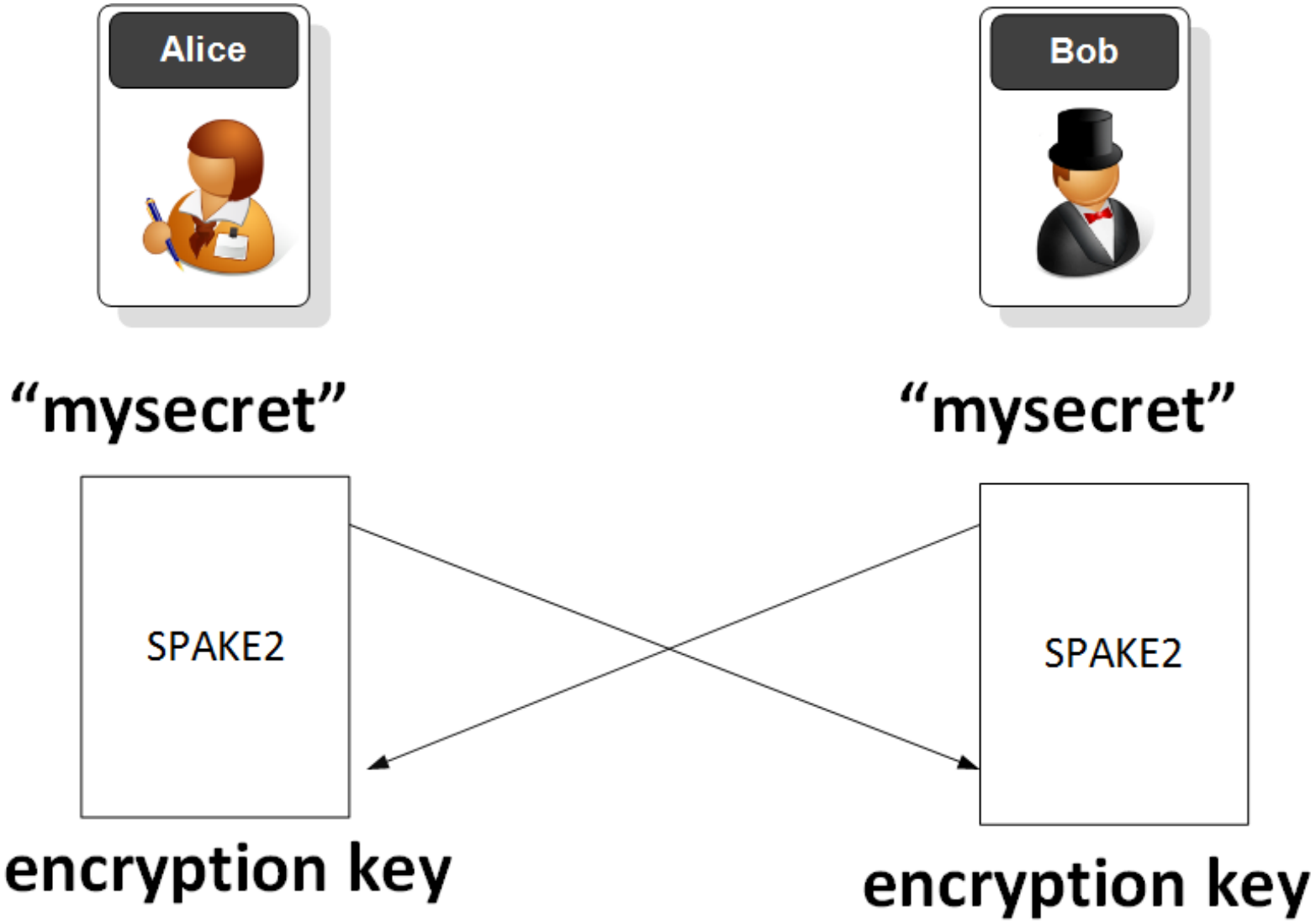
Stored secret



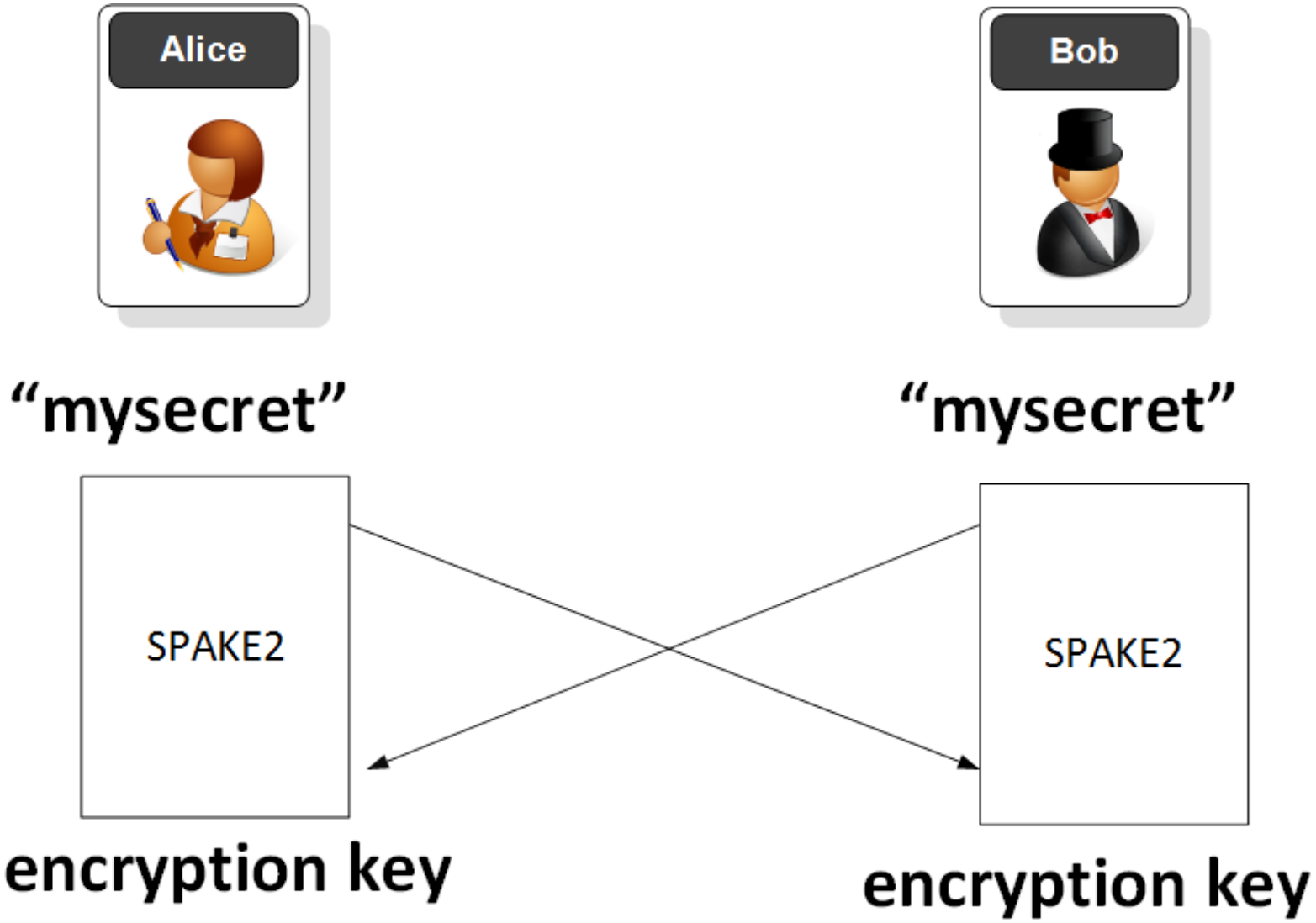
encryption key

encryption key

SPAKE2 (Password-Authenticated Key Exchange)



SPAKE2 (Password-Authenticated Key Exchange)



SPAKE2 (Password-Authenticated Key Exchange)

$X = xG$ and $T = wM + X$

The value of T is sent to Bob. Bob also creates w, and picks a random number (y) from 0 to p (a prime number). He then calculates:

$Y = yG$ and $S = wN + Y$

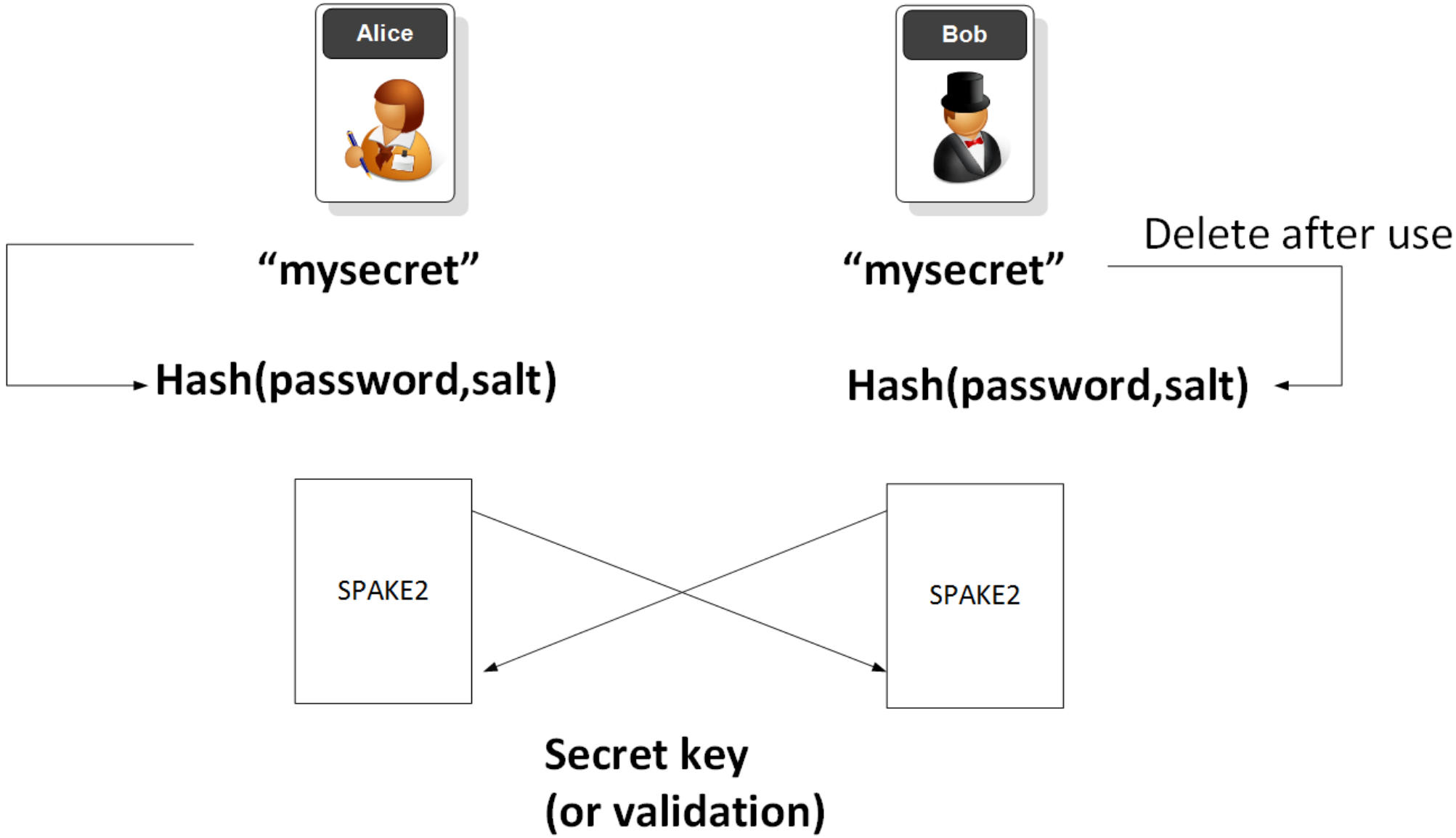
Bob sends the value of Y to Alice.

Alice calculates $K(Alice) = x(S - wN)$, and Bob calculates $K(Bob) = y(T - wM)$. These values are basically:

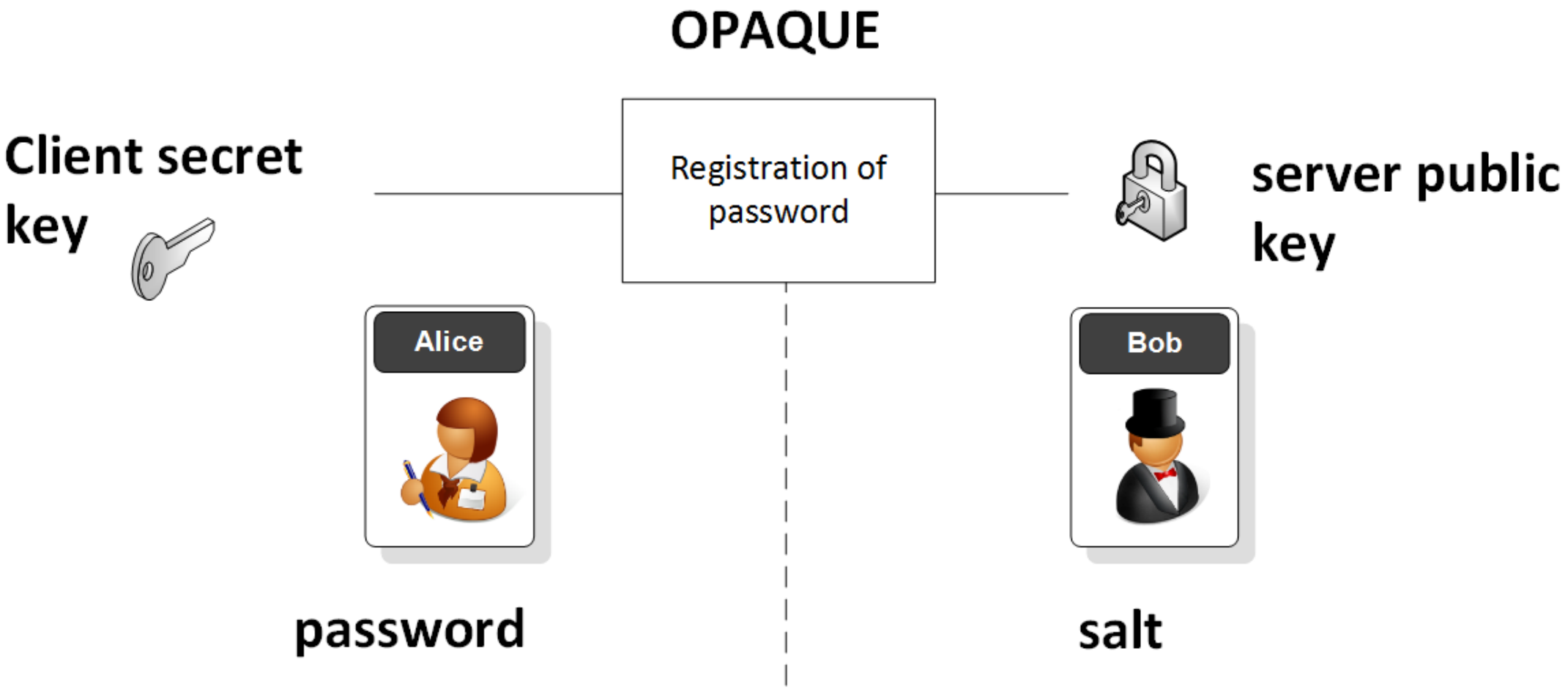
$K(Bob) = x(S - wN) = x(wN + Y - wN) = xY = xyG$

$K(Alice) = y(T - wM) = y(wM + X - wN) = yX = xyG$

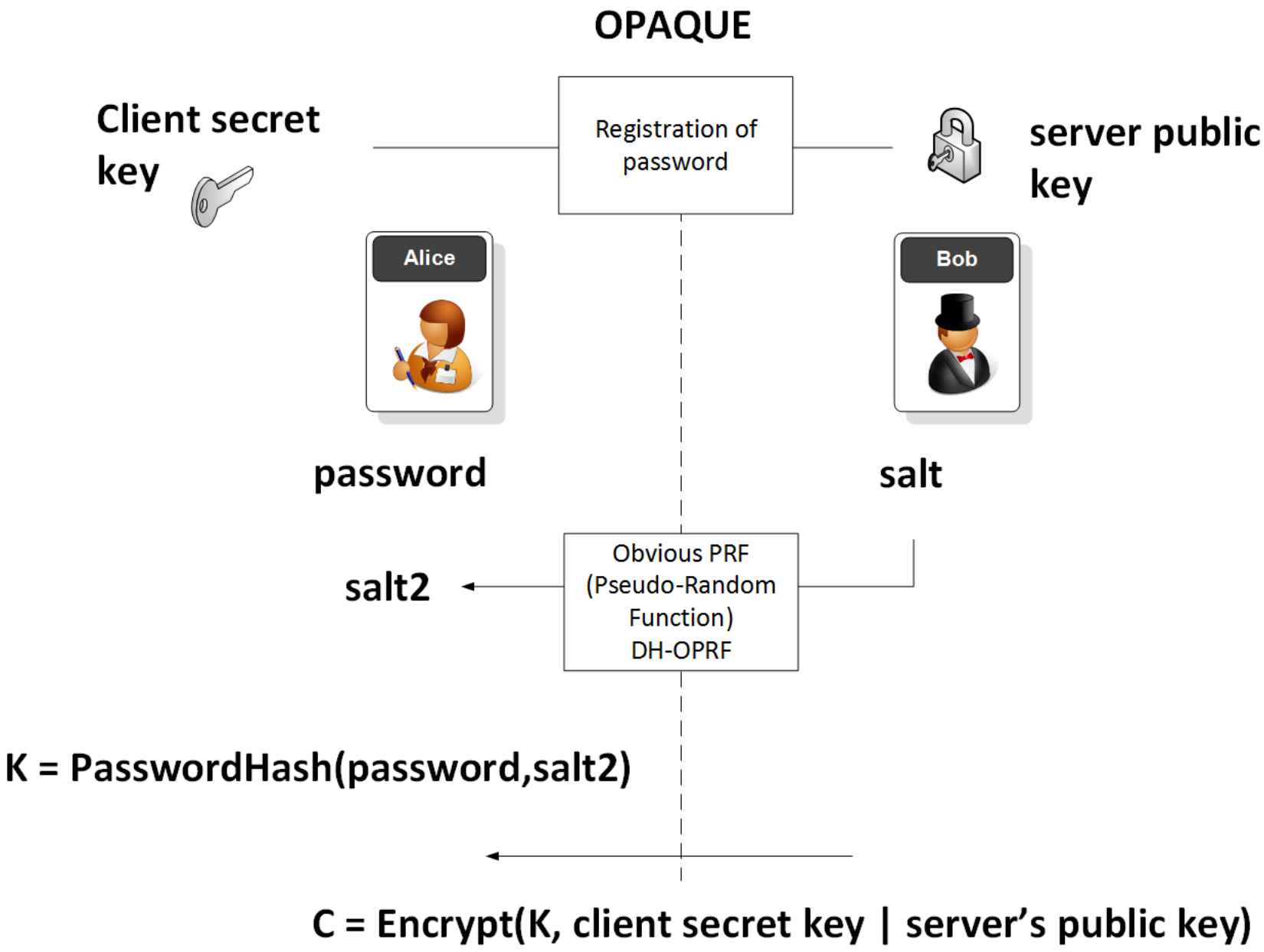
Proving Password



OPAQUE


OPAQUE
Client secret key
Registration of password
server public key
Alice
Bob
password
salt

OPAQUE


OPAQUE
Client secret key
Registration of password
server public key
Alice
Bob
password
salt
salt2
Obvious PRF (Pseudo-Random Function) DH-OPRF
K = PasswordHash(password,salt2)
C = Encrypt(K, client secret key | server's public key)

PAKE - Password Authenticated Key Exchange

Prof Bill Buchanan, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY