AugPAKE Update
draft-irtf-cfrg-augpake-03

SeongHan Shin and Kazukuni Kobara

AIST, JP

RECAP AUGPAKE

PAKE

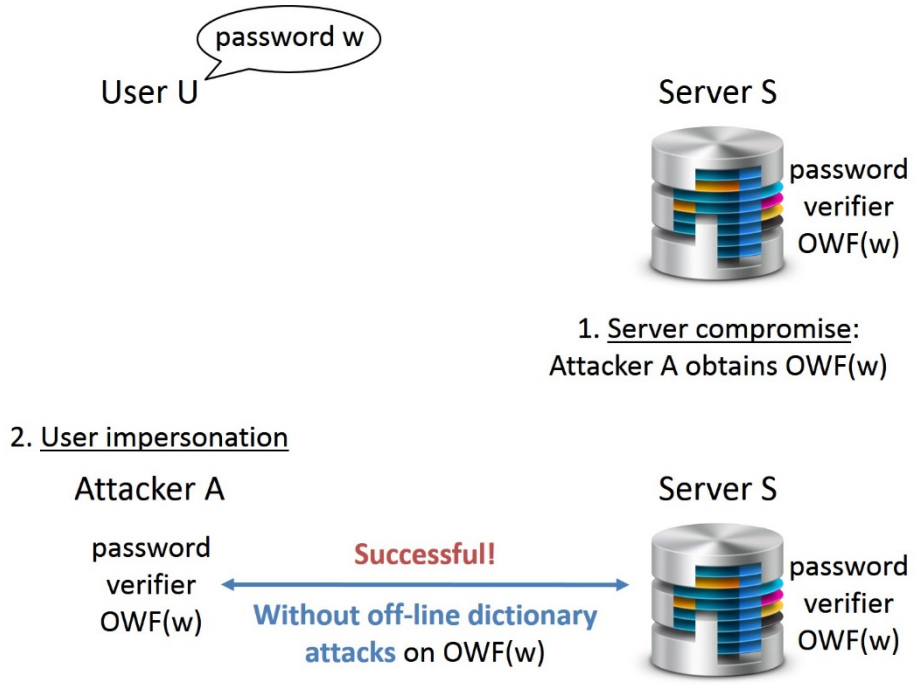
- Password-Authenticated Key Exchange
  - It does **not rely on PKI**
  - Users do **not** need to carry **any devices**
  - **Very convenient**
- Which kind of security should be achieved in PAKE?
  - **Security against off-line dictionary attacks** (at least)
- Inherent limitations of PAKE
  - On-line dictionary attacks are always possible
    - But, controllable
  - Server compromise always leads to password compromise

PAKE (cont)

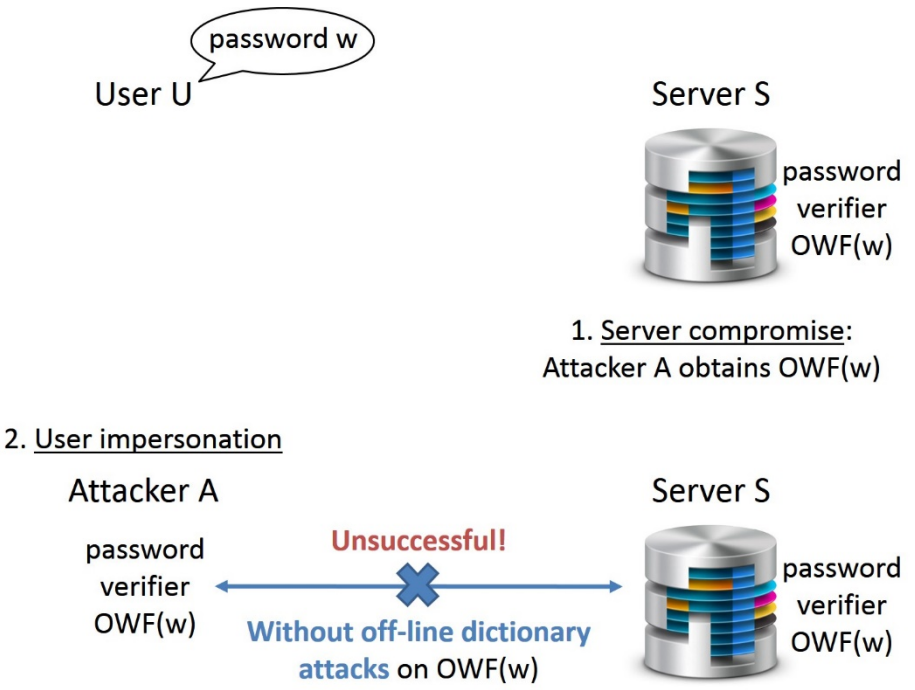
- PAKE can be classified into
  - Balanced PAKE
    - Security against off-line dictionary attacks
  - **Augmented PAKE**
    - Security against off-line dictionary attacks
    - Plus extra protection for server compromise (i.e., resistance to server compromise)
    - Examples: A-EKE, AuthA, VB-EKE, B-SPEKE, PAK-X/Y/Z/Z+, AMP [IEEE 1363.2, ISO/IEC 11770-4], SRP [IEEE 1363.2, ISO/IEC 11770-4, RFC2945, RFC5054], **AugPAKE**, …

PAKE (cont)

Balanced PAKE



Augmented PAKE



AugPAKE

- Security
  - **Provably secure** in RO model [SKI10]
  - Security against passive/active/off-line dictionary attacks + resistance to server compromise

- **Highly efficient**

	Modular exp. of user (excluding pre-computable costs)	Modular exp. of server (excluding pre-computable costs)
DH key exchange	2 (1)	2 (1)
AugPAKE	**2** (**1**)	**2.17** (**1.17**)

  - Most efficient over SRP and AMP

Other Features of AugPAKE

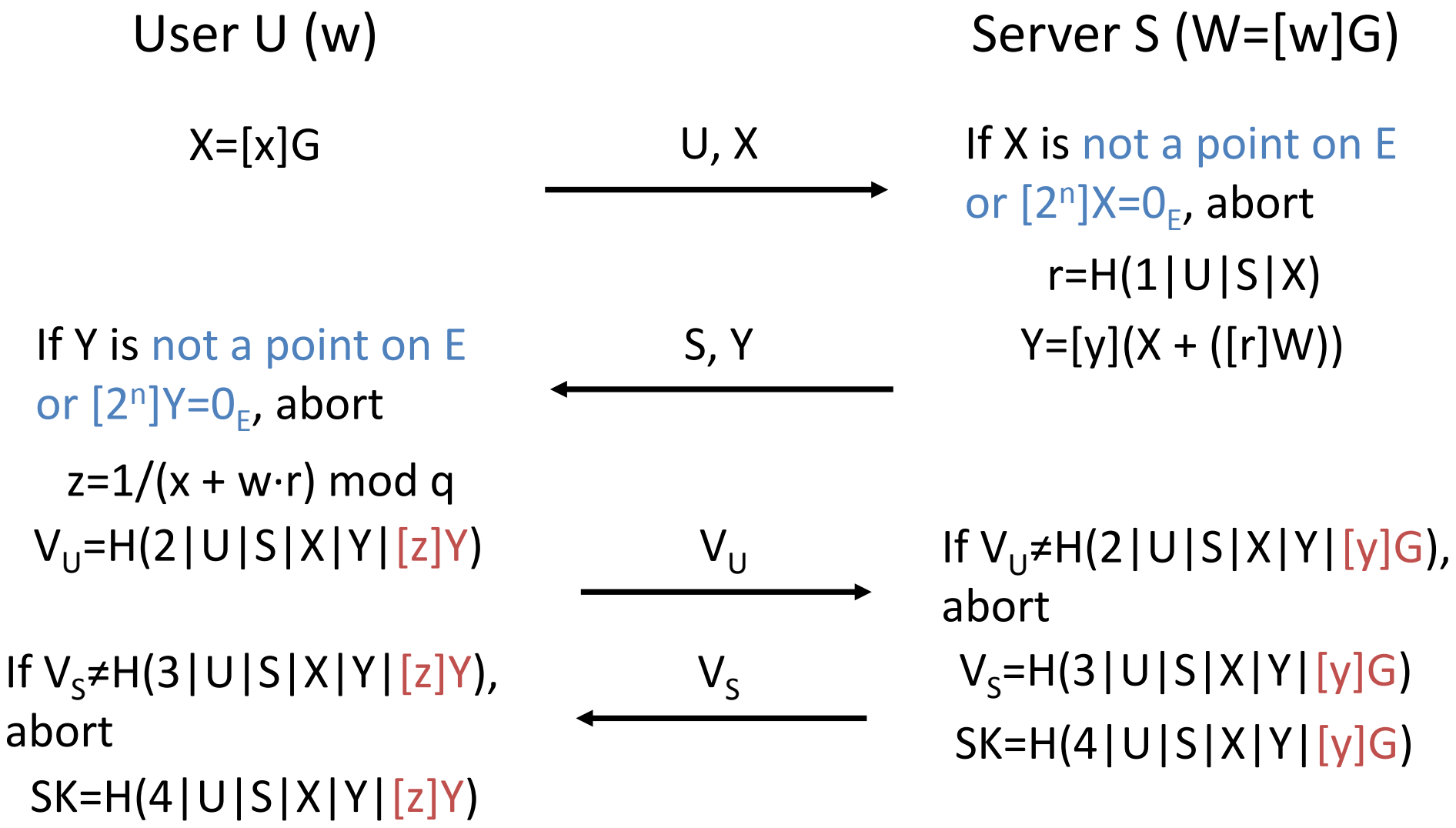
- **Over any cryptographically secure DH groups**
  - Neither FDH nor ideal cipher used
- IPR disclosure
  - **Royalty-free license of AugPAKE**
  - https://datatracker.ietf.org/ipr/2037/
- Can be easily converted to 'balanced' one

DIFF FROM -01

AugPAKE over EC Groups

- Domain parameters
  - p, q: sufficiently large primes, and q (order of the desired group)
  - m: some positive integer
  - Elliptic curve E with point at infinity 0_E
    - $y^2 = x^3 + a\,x + b$ over GF(p) or
    - $y^2 + x\,y = x^3 + a\,x^2 + b$ over GF(2^m)
  - #E: number of points on E
  - k: cofactor (#E/q) satisfying **$k=2^n\ q_1\ q_2\ \ldots\ q_t$ where $n=\{0,1,2,3\}$ and every primes $q_i > q$ for $i=1, 2, \ldots, t$.** Optionally, **$k=2^n$**
  - G: generator for a subgroup of q points on E

EC-AugPAKE


User U (w)
Server S (W=[w]G)
X=[x]G
U, X
If X is not a point on E or [2^n]X=0_E, abort
r=H(1|U|S|X)
Y=[y](X + ([r]W))
S, Y
If Y is not a point on E or [2^n]Y=0_E, abort
z=1/(x + w·r) mod q
V_U=H(2|U|S|X|Y|[z]Y)
V_U
If V_U≠H(2|U|S|X|Y|[y]G), abort
V_S=H(3|U|S|X|Y|[y]G)
V_S
If V_S≠H(3|U|S|X|Y|[z]Y), abort
SK=H(4|U|S|X|Y|[z]Y)
SK=H(4|U|S|X|Y|[y]G)

THANK YOU FOR YOUR ATTENTION!