Augmented Password-Authenticated Key Exchange (AugPAKE)

draft-irtf-cfrg-augpake-01

SeongHan Shin and Kazukuni Kobara

AIST, JP

National Institute of Advanced Industrial Science and Technology AIST

独立行政法人
産業技術総合研究所（産総研）

Password

- Password is chosen from a small set of dictionary
  - It is convenient to users because they just remember his/her passwords
  - E.g., 4-digit pin-codes, alphanumerical passwords with 6 characters

- Password authentication is **widely deployed in practice**

- However, two exhaustive search attacks are possible
  - On-line dictionary attacks
    - An attacker should communicate with (at least) one party in order to verify a guessed password
    - But, it is ***controllable***
  - **Off-line dictionary attacks**
    - An attacker can verify more than one password with sophisticated manners

PAKE

- Password-Authenticated Key Exchange
- Password-only authentication + generation of session keys
  - It does **not rely on PKI**
  - Users do **not** need to carry **any devices**
  - **Very convenient**

- However, it is ***not trivial*** to design a secure PAKE protocol
  - Due to the existence of off-line dictionary attacks

- Which kind of security should be achieved in PAKE?
  - Security against off-line dictionary attacks (at least)

PAKE

- Inherent limitations of PAKE
  - On-line dictionary attacks are always possible
  - Server compromise always leads to password compromise

- PAKE can be classified into
  - Balanced PAKE
    - User U and server S share the same password w
  - **Augmented PAKE**
    - User U remembers his/her password w, and server S has password verifier (e.g., derived by applying one-way function to w)
    - Preferable because it provides extra protection for server compromise (i.e., resistance to server compromise)

Augmented PAKE

- A-EKE, AuthA, VB-EKE
- B-SPEKE
- PAK-X/Y/Z/Z+

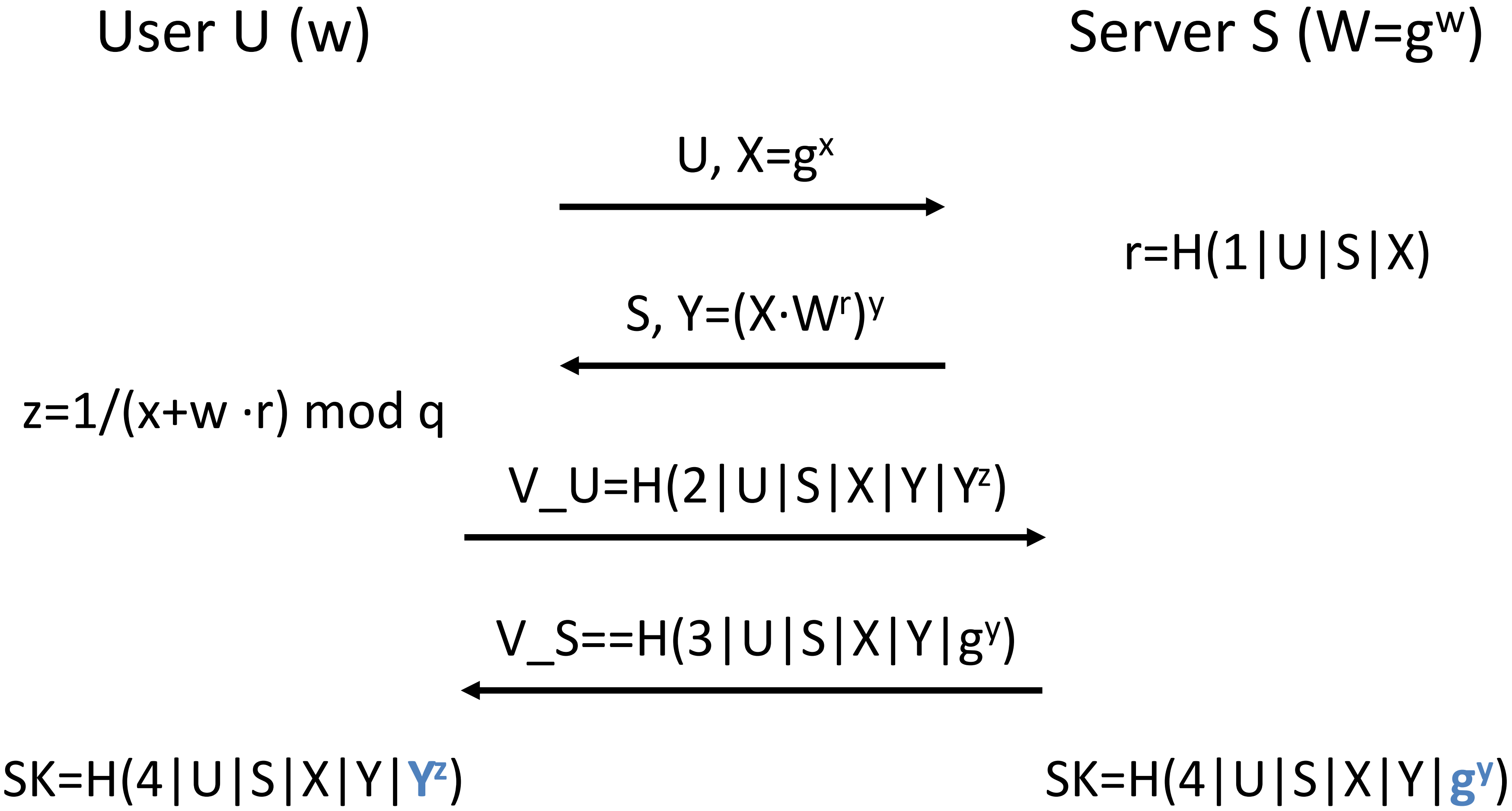
- AMP [IEEE 1363.2, ISO/IEC 11770-4]
- SRP [IEEE 1363.2, ISO/IEC 11770-4, RFC2945, RFC5054]

- **AugPAKE** (this talk)
- …

AugPAKE

- Efficiency
  - **Most efficient** over previous works (e.g., SRP and AMP)
  - Similar efficiency to plain DH key exchange
- Security
  - **Provably secure** [SKI10]
  - Security against passive attacks
  - Security against active attacks
  - Security against off-line dictionary attacks
  - Resistance to server compromise

AugPAKE Protocol



User U (w)

Server S ($W=g^w$)

U, $X=g^x$

$r=H(1|U|S|X)$

S, $Y=(X\cdot W^r)^y$

$z=1/(x+w\cdot r) \bmod q$

$V\_U=H(2|U|S|X|Y|Y^z)$

$V\_S==H(3|U|S|X|Y|g^y)$

$SK=H(4|U|S|X|Y|Y^z)$

$SK=H(4|U|S|X|Y|g^y)$

Features of 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**)

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

THANK YOU FOR YOUR ATTENTION!