한성대 특강 25.09.25

패스워드기반 인증 및 키 합의 프로토콜
(Password-based Authenticated Key Exchange)

황 정 연

수리통계데이터사이언스학부
성신여대

목 차

- 배경: KE
- 연구 동향: PAKE
- 설계 원리
  - Strong Aymmetric PAKE
- 향후 주제

Key Exchange: DH

- KE 기법

Diffie-Hellman (DH) Key Exchange

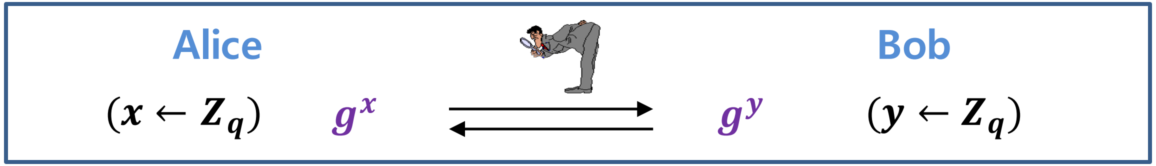
W. Diffie and M. Hellman, "New directions in cryptography". IEEE Transactions on Information Theory 22 (6): 644–654, 1976

수학적 파라미터

$\boldsymbol{G} = <\boldsymbol{g}>, |\boldsymbol{G}| = \boldsymbol{q}$

$\boldsymbol{Z_q} = \{\boldsymbol{0}, \boldsymbol{1}, \ldots, \boldsymbol{q-1}\}$

Public Parameters: $(\boldsymbol{G}, \boldsymbol{q}, \boldsymbol{g})$



Alice

$(\boldsymbol{x} \leftarrow \boldsymbol{Z_q})$ $\boldsymbol{g^x}$

$\boldsymbol{g^y}$ $(\boldsymbol{y} \leftarrow \boldsymbol{Z_q})$

Bob

Public Network

$\textbf{Shared Key} = \boldsymbol{g^{xy}}$

공격 모델:
Passive 공격(도청)

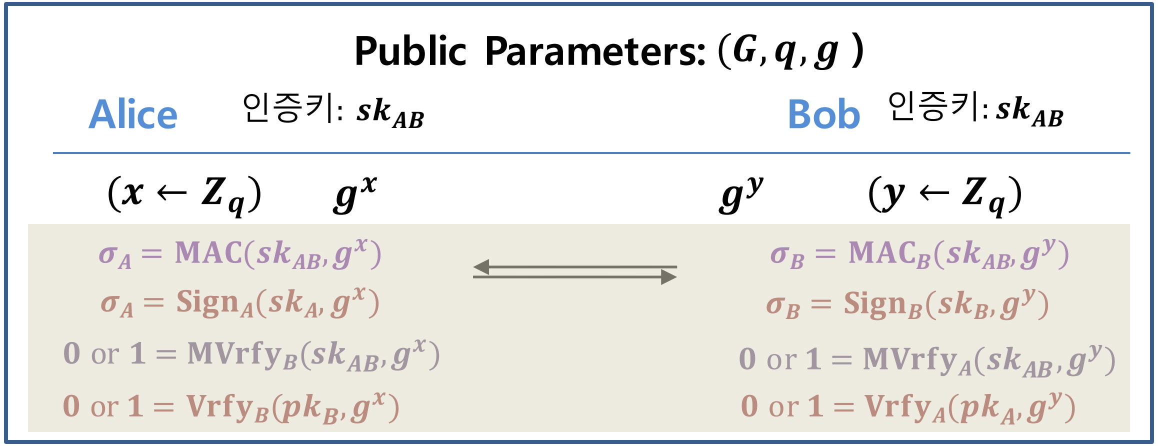
Computational Assumption:

- Computational DH (CDH) problem: to compute $\boldsymbol{g^{xy}}$
- Decisional DH (DDH) problem: to distinguish $\boldsymbol{g^{xy}}$ and $\boldsymbol{g^z}$ for random $\boldsymbol{z}$

Key Exchange: DH

- KE 기법 **+ 인증 수단**

DH KE + 인증 수단(대칭, 비대칭)



Public Parameters: (G, q, g)

Alice 인증키: sk_{AB}

Bob 인증키: sk_{AB}

$(x \leftarrow Z_q)$ g^x

g^y $(y \leftarrow Z_q)$

$\sigma_A = \mathrm{MAC}(sk_{AB}, g^x)$

$\sigma_A = \mathrm{Sign}_A(sk_A, g^x)$

$0 \text{ or } 1 = \mathrm{MVrfy}_B(sk_{AB}, g^x)$

$0 \text{ or } 1 = \mathrm{Vrfy}_B(pk_B, g^x)$

$\sigma_B = \mathrm{MAC}_B(sk_{AB}, g^y)$

$\sigma_B = \mathrm{Sign}_B(sk_B, g^y)$

$0 \text{ or } 1 = \mathrm{MVrfy}_A(sk_{AB}, g^y)$

$0 \text{ or } 1 = \mathrm{Vrfy}_A(pk_A, g^y)$

인증 계층

$$\textbf{Shared Key} = g^{xy}$$

[Secuirty]

- DDH Assumption
- Secuirty of MAC, Signature (Existential unforgeability under chosen message attacks)

수학적 파라미터

$G = \langle g \rangle, |G| = q$

$Z_q = \{0, 1, \ldots, q-1\}$

Public Network

공격 모델:
Active 능동 공격(수정,변조,..)

Authenticated KE: DH + 약한 인증 정보

- Authenticated KE : DH KE + 강한 인증 정보

→ 기법구성: EASY !!

User 이용성: 복잡

- Authenticated KE : DH KE + 약한 인증 정보 (PassWord)

→ **기법구성: challenging !!**

User 이용성: EASY (human-memorable)

No Moore's Law for human memory
Still 4~6 digits

Authenticated KE: DH + 약한 인증 정보

고민 거리들

- 약한 인증 정보 (Password)

  "Most" (> 80%) passwords have fewer than 22 bits of entropy
  M. Weir, S. Aggarwal, M. Collins, H. Stern,
  " Testing Metrics for Password-Creation Policies by Attacking Large Sets of Revealed Passwords ", ACM CCS, 162–175, 2010

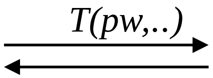
- Dictionary Attack

  Try $2^{22} + \alpha$ 가지 비트열 (PW=1000101010101010101111)

- On-line/Off-line Dictionary Attack

  On-line attack: try a guessed PW with the server (limited!)

  Off-line attack: try a guessed PW with the protocol transcript (basic goal)



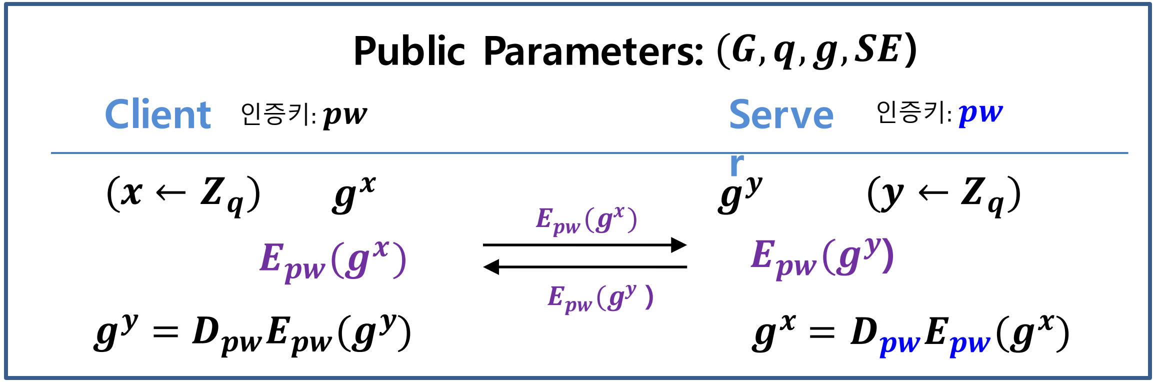
Authenticated KE: DH + 약한 인증 정보

[구성 예: 최초]

- EKE (Encrypted Key Exchange) – Bellovin-Merritt

  "Encrypted key exchange: Password-based protocol secure against dictionary attack",
  IEEE Symposium on Research in Security and Privacy 1992

SE : Symmetric Encryption (예. AES)



Public Parameters: (G, q, g, SE)

Client 인증키: pw

Server 인증키: pw

$(x \leftarrow Z_q)$ g^x

$E_{pw}(g^x)$

$\xrightarrow{E_{pw}(g^x)}$

$\xleftarrow[E_{pw}(g^y)]{}$

g^y $(y \leftarrow Z_q)$

$E_{pw}(g^y)$

$g^y = D_{pw}E_{pw}(g^y)$

$g^x = D_{pw}E_{pw}(g^x)$

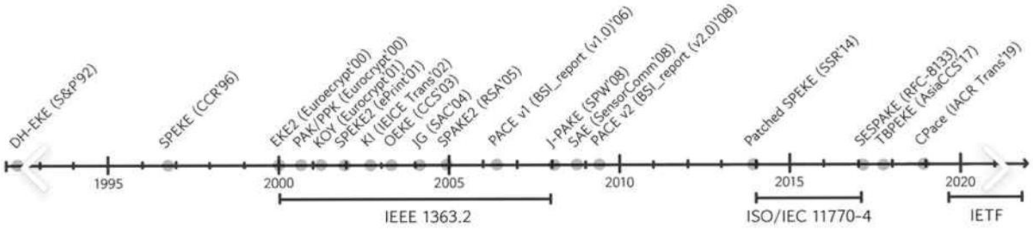
$$\textbf{Shared Key} = g^{xy}$$

Off-line attack: Wrong PW pw' 적용 ⇒ 혼돈과 확산: $g^r \leftarrow D_{pw'}E_{pw}(g^y)$

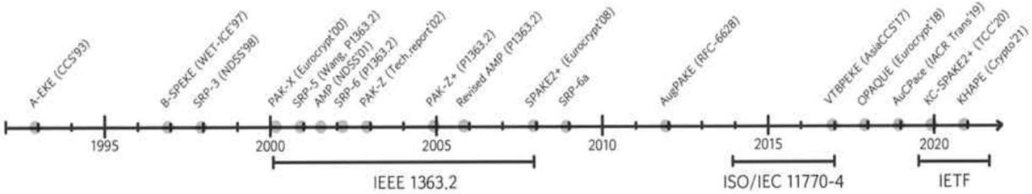
but need Random Permutation: Ideal Cipher

Authenticated KE: DH + 약한 인증 정보

[관련 연구]



대칭형 PAKE 연구 및 표준화 동향



비대칭형 PAKE 연구 및 표준화 동향

Authenticated KE: DH + 약한 인증 정보

[관련 연구]

… http://www.jablon.org/passwordlinks.html#Jab97

- M. Bellare, D. Pointcheval; P. Rogaway, Eurocrypt'00
  "Authenticated Key Exchange Secure against Dictionary Attacks"
- V. Boyko, P. MacKenzie, and S. Patel, Eurocrypt'00
  "Provably secure password authentication and key exchange using Diffie-Hellman"
- J. Katz,, R. Ostrovsky, M. Yung, Eurocrypt'01
  "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords "
- C. Gentry, P. MacKenzie, and Z. Ramzan, Crypto'06
  "A Method for Making Password-Based Key Exchange Resilient to Server Compromise "
- J. Katz, V. Vaikuntanathan, TCC'11
  "Round-Optimal Password-Based Authenticated Key Exchange"
- F. Benhamouda, O. Blazy, C. Chevalier, D. Pointcheval, D. Vergnaud, CRYPTO'13
  "New Techniques for SPHFs and Efficient One-Round PAKE Protocols"
  Full version: "New Smooth Projective Hash Functions and One-Round Authenticated Key Exchange"
  IACR Cryptology ePrint Archive 2015: 188 (2015)

PAKE: 종류 (대칭 vs 비대칭)

즉시 Client Impersonation Attack !!

- Symmetric (or Balanced (ISO 11770-4))

Client 인증키: $\boldsymbol{pw}$ (or $\boldsymbol{H}(\boldsymbol{pw})$) Server 인증키: $\boldsymbol{pw}$ (or $\boldsymbol{H}(\boldsymbol{pw})$)

Server Compromise: PW화일 누출 (대규모 사용자 비밀정보)

- Asymmetric (or Augumented (ISO 11770-4))

Client 인증키: $\boldsymbol{pw}$ Server 인증키: $\boldsymbol{F}(\boldsymbol{pw})$

일방향 함수

Off-line Dictionary Attack: PW

Client Impersonation Attack

PAKE: Type (대칭 vs 비대칭)

[관련 연구]

- MacKenzie: PAK-Z
- GMR06: Generic Method: Signature based (fixing PAK-Z)
  C. Gentry, P. MacKenzie, and Z. Ramzan, "A Method for Making Password-Based Key Exchange Resilient to Server Compromise", Crypto'06
- Kwon: AMP (Authentication via Memorable Password)
  T. Kwon, "Authentication and key agreement via memorable password," In NDSS (Network and Distributed Systems Security), 2001
- Wu: SRP (Secure Remote Password Protocol)
  T. Wu, "The Secure Remote Password Protocol", In NDSS (Network and Distributed Systems Security), pp. 97-111, 1998
- Jablon: (B-)SPEKE (Simple Password Exponential Key Exchange)
  D. Jablon. "Strong Password-Only Authenticated Key Exchange". Computer Communication Review (ACM SIGCOMM) 26 (5): 5–26, Oct. 1996
  D. Jablon. "Extended password methods immune to dictionary attack". In WETICE '97 Enterprise Security Workshop, Cambridge, MA, June 1997

PAKE: Type (대칭 vs 비대칭)

[구성 예]

- Generic Method: **Signature based**

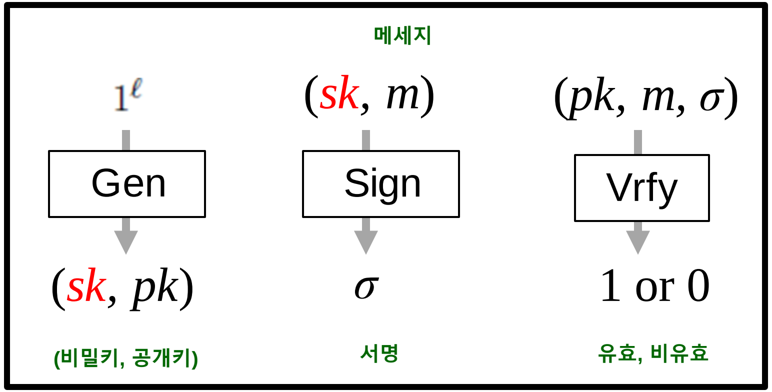
  C. Gentry, P. MacKenzie, and Z. Ramzan, Crypto'06
  "A Method for Making Password-Based Key Exchange Resilient to Server Compromise"

Symmetric PAKE

$$\boldsymbol{DS} = (\textbf{KeyGen}, \textbf{Sign}, \textbf{Vrfy})$$

$$\boldsymbol{E_k(M) = k \oplus M||H(M)}$$

Asymmetric PAKE



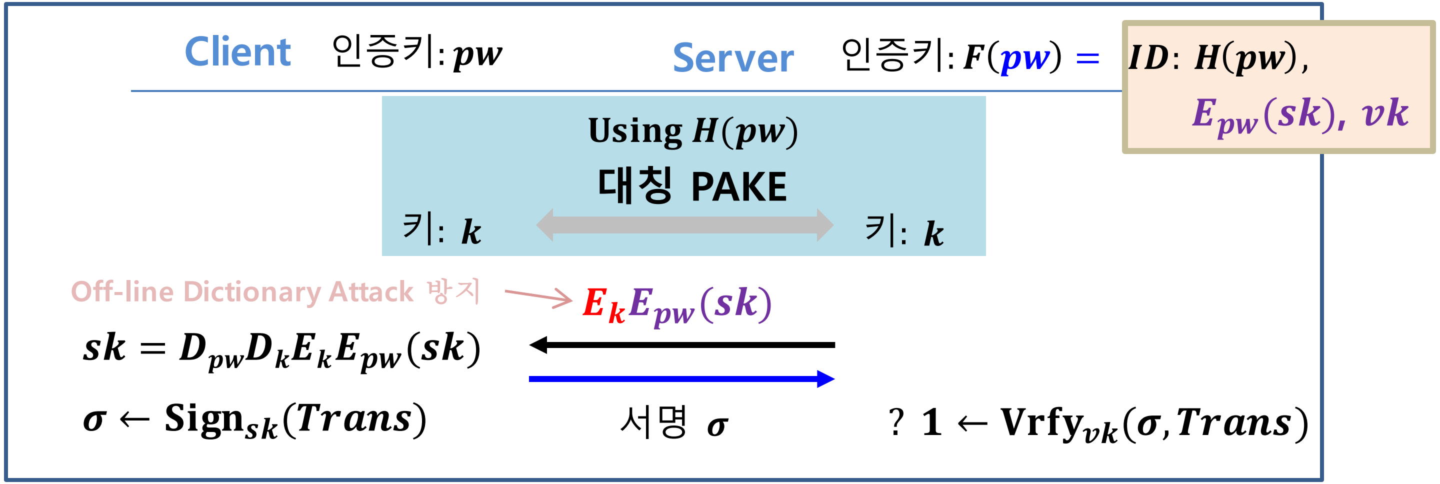
[GMR88] S. Goldwasser, S. Micali, and R.L. Rivest,
A digital signature scheme secure against adaptive chosen-message attacks, SIAM J. Computing 1988

PAKE: Type (대칭 vs 비대칭)

[구성 예]

- Generic Method: **Signature based construction**

C. Gentry, P. MacKenzie, and Z. Ramzan, Crypto'06
"A Method for Making Password-Based Key Exchange Resilient to Server Compromise"



Client 인증키: pw

Server 인증키: $F(pw) =$ $ID: H(pw),$ $E_{pw}(sk),\ vk$

Using $H(pw)$

대칭 PAKE

키: k ⟷ 키: k

Off-line Dictionary Attack 방지 → $E_k E_{pw}(sk)$

$sk = D_{pw} D_k E_k E_{pw}(sk)$

$\sigma \leftarrow \mathrm{Sign}_{sk}(Trans)$

서명 σ

$? \; 1 \leftarrow \mathrm{Vrfy}_{vk}(\sigma, Trans)$

Proof of Possession of a Password

PAKE: 종류: 비대칭 vs 강한 비대칭형

- Asymmetric PAKE 구조

Client 인증키: pw Server 인증키: $\boldsymbol{F(pw)}$

fewer than 22 bits of entropy

deterministic ?

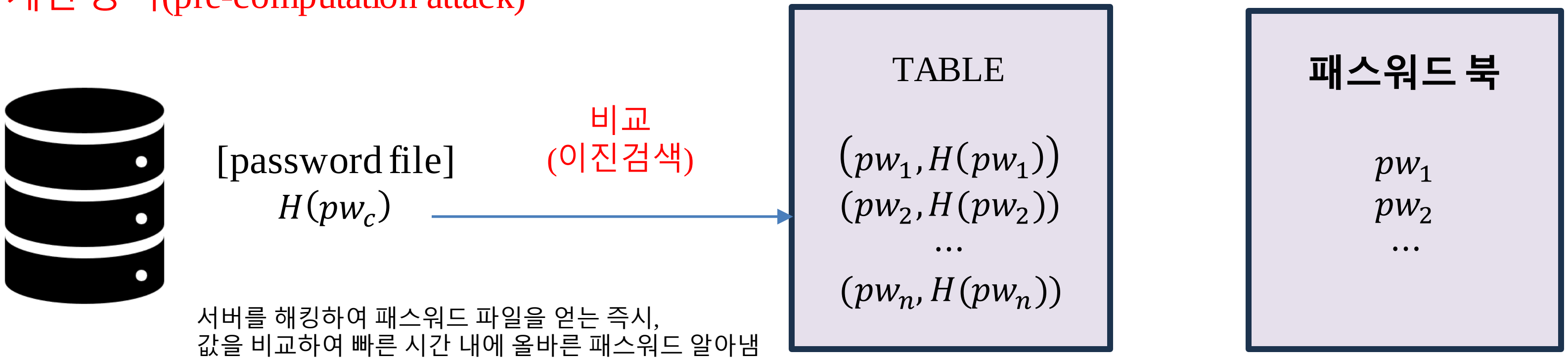
공격자: 패스워드 후보들에 대응되는
패스워드 검증 정보를 테이블(table)
형태로 저장함

0000…00 ~ 1111…11

사전계산 공격(pre-computation attack)

사전계산 테이블
(pre-computation table)

패스워드 북 또는 사전
(Ditionary)



[password file]
$H(pw_c)$

비교
(이진검색)

TABLE

$(pw_1, H(pw_1))$
$(pw_2, H(pw_2))$
$\cdots$
$(pw_n, H(pw_n))$

패스워드 북

pw_1
pw_2
$\cdots$

서버를 해킹하여 패스워드 파일을 얻는 즉시,
값을 비교하여 빠른 시간 내에 올바른 패스워드 알아냄

PAKE: 강한 비대칭형

대부분의 aPAKE는 사전계산 공격에 안전하지 않다고 알려져 있음.

위 단점을 보완하고자 사전계산 공격에
강인한 PAKE(strong asymmetric PAKE, saPAKE)
관련 연구가 진행

S. Jarecki, H. Krawczyk, and J. Xu. OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks. In EUROCRYPT, pp. 456-486. Springer, 2018.

H. Krawczyk. The OPAQUE Asymmetric PAKE Protocol, draft-krawczyk-cfrg-opaque-06, https:// www.ietf.org/archive/id/draft-krawczyk-cfrg-opaque-06.txt, June 2020.

J Hesse, S. Jarecki, H. Krawczyk, and C. Wood. Password-Authenticated TLS via OPAQUE and Post-Handshake Authentication. Cryptology ePrint Archive, Paper 2023/220

PAKE: 강한 비대칭형: OPAQUE

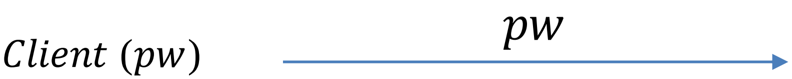
- Asymmetric PAKE 구조

Client 인증키: $\boldsymbol{pw}$ Server 인증키: $\boldsymbol{F(pw)}$

Randomized

OPAQUE - Registration

대칭키 암호화 스킴
$Enc_k(x)$: 키 k로 암호화
$Dec_k(x)$: 키 k로 복호화
H, H': Hash function



$Server$

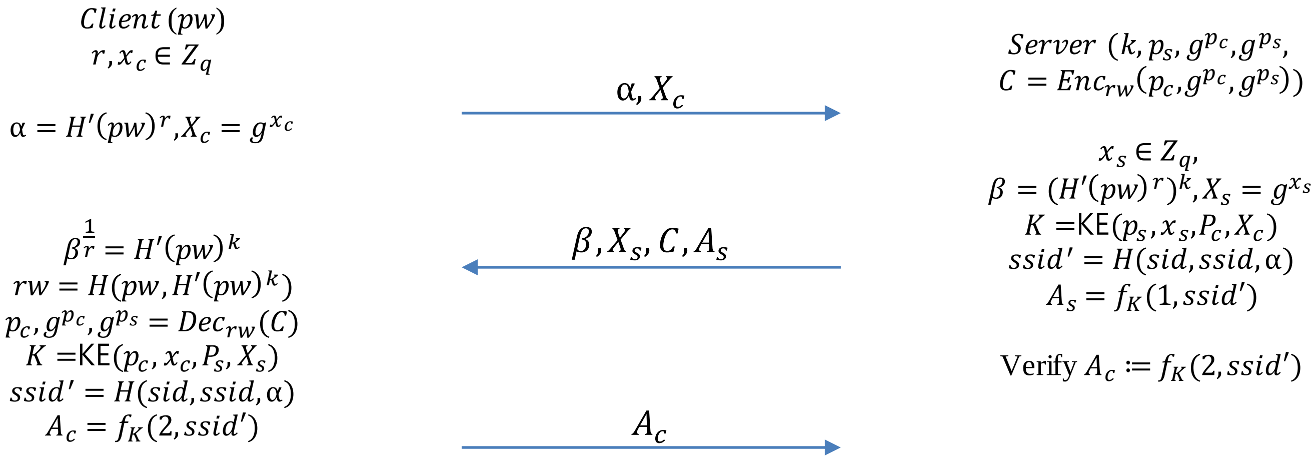
$$k_s \in Z_q$$
$$rw = H(pw, H'(pw)^{k_s})$$
$$p_s, p_c \in Z_q$$
$$P_s = g^{p_s}, P_c = g^{p_c}$$
$$C = Enc_{rw}(p_c, P_c, P_s)$$

Store (k_s, p_s, P_s, P_c, C)

PAKE: 강한 비대칭형

- OPAQUE - Login

$$\mathrm{KE}(p_s, x_s, P_c, X_c) = H((X_c P_c{}^{e_c})^{x_s+e_s p_s}) = H((g^{x_c+e_c p_c})^{x_s+e_s p_s})$$
$$\mathrm{KE}(p_c, x_c, P_s, X_s) = H((X_s P_s{}^{e_s})^{x_c+e_c p_c}) = H((g^{x_s+e_s p_s})^{x_c+e_c p_c})$$
$$e_c = H(X_c, S, ssid'), e_s = H(X_s, C, ssid')$$



$Client\ (pw)$

$r, x_c \in Z_q$

$\alpha = H'(pw)^r, X_c = g^{x_c}$

$\xrightarrow{\alpha, X_c}$

$Server\ (k, p_s, g^{p_c}, g^{p_s},$
$C = Enc_{rw}(p_c, g^{p_c}, g^{p_s}))$

$x_s \in Z_q,$
$\beta = (H'(pw)^r)^k, X_s = g^{x_s}$
$K = \mathrm{KE}(p_s, x_s, P_c, X_c)$
$ssid' = H(sid, ssid, \alpha)$
$A_s = f_K(1, ssid')$

$\xleftarrow{\beta, X_s, C, A_s}$

$\beta^{\frac{1}{r}} = H'(pw)^k$
$rw = H(pw, H'(pw)^k)$
$p_c, g^{p_c}, g^{p_s} = Dec_{rw}(C)$
$K = \mathrm{KE}(p_c, x_c, P_s, X_s)$
$ssid' = H(sid, ssid, \alpha)$
$A_c = f_K(2, ssid')$

$\xrightarrow{A_c}$

Verify $A_c \coloneqq f_K(2, ssid')$

Q&A

감사합니다.