



Password Authenticated Key Exchange Protocols

Xun Yi, Victoria University

Raylin Tso, National Cheng Chi University

Eiji Okamoto, University of Tsukuba



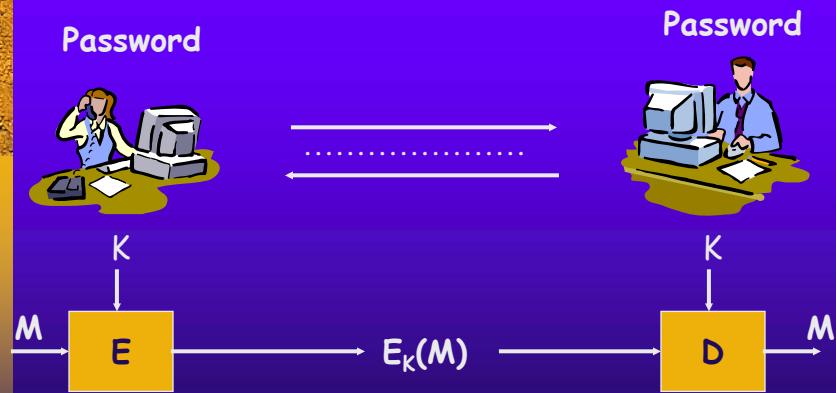
Abstract

- ◆ Scenario: client/server model
- ◆ Application: password-authenticated key exchange (PAKE)
- ◆ Proposals: client/server PAKE protocol from IBE, group PAKE protocol from IBE and IBS

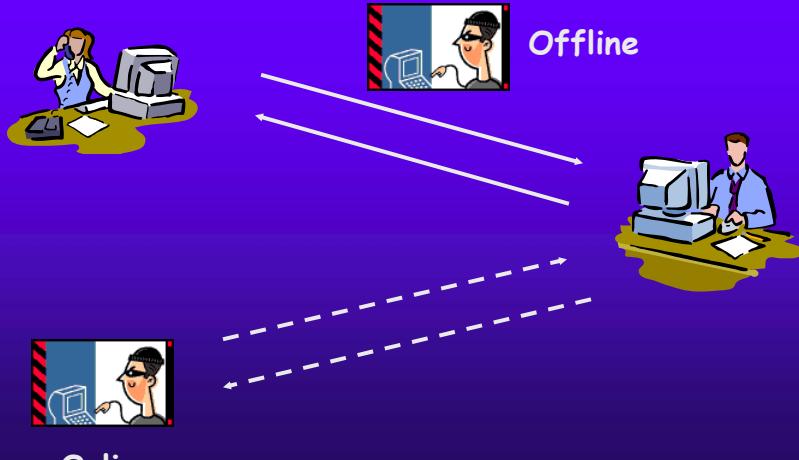
Outline

- ◆ Backgrounds
- ◆ Client/server PAKE from IBE
- ◆ Group PAKE from IBE and IBS
- ◆ Security and performance analysis
- ◆ Conclusion

What is PAKE?

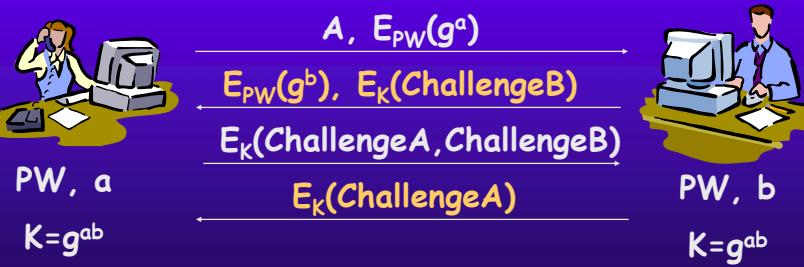


Dictionary Attack



First PAKE

- ◆ S. Bellovin and M. Merritt: Encrypted key exchange: Password-based protocols secure against dictionary attacks (1992).
- ◆ Built on Diffie-Hellman protocol (1976).



First Formal Model of Security for PAKE

- ♦ M. Bellare, D. Pointcheval, and P. Rogaway: Authenticated key exchange secure against dictionary attacks (Eurocrypt 2000).
- ♦ V. Boyko, P. Mackenzie, and S. Patel: Provably secure password-authenticated key exchange using Diffie-Hellman (Eurocrypt 2000).
- ♦ Random oracle model versus standard model

$$\text{Adv}_{A,P}(k) \leq Q(k)/N + \varepsilon(k)$$

First Practical PAKE without Random Oracles

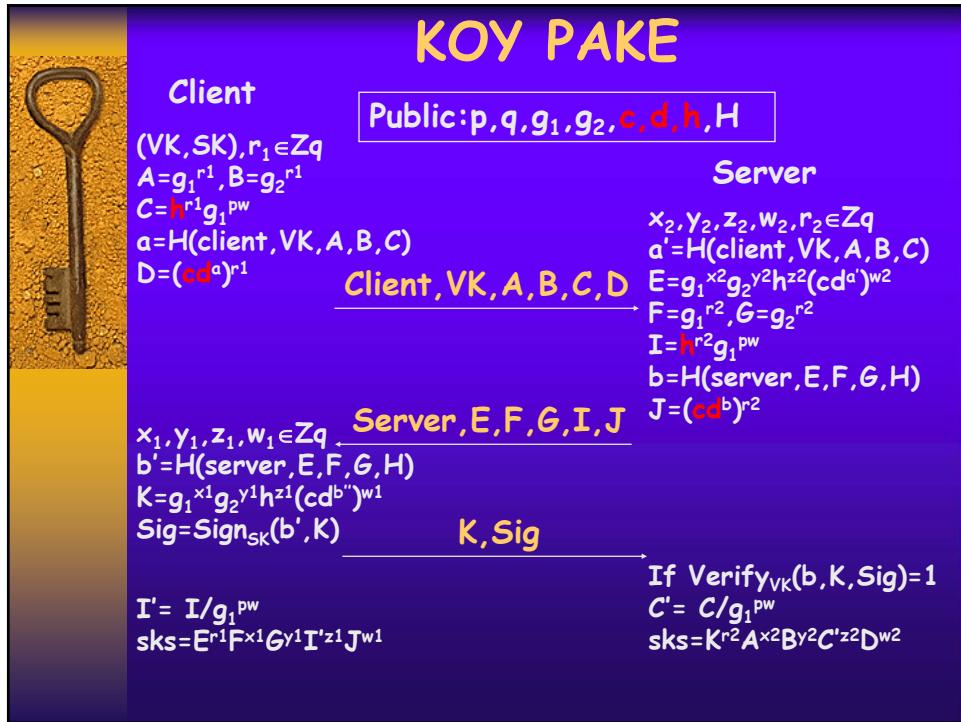
- ♦ J. Katz, R. Ostrovsky and M. Yung: Efficient password-authenticated key exchange using human-memorable passwords (Eurocrypt 2001).
- ♦ Built on Cramer-Shoup cryptosystem (1998)

$$\begin{aligned} E: k &\in \mathbb{Z}_q \\ u_1 &= g_1^k \\ u_2 &= g_2^k \\ e &= h^k m \\ a &= H(u_1, u_2, e) \\ v &= c^k d^ka \end{aligned}$$

$$S \xrightarrow{u_1, u_2, v, e}$$

$$\begin{array}{ll} \text{PK} & \text{SK} \\ c = g_1^{x_1} g_2^{x_2} & x_1, x_2 \\ d = g_1^{y_1} g_2^{y_2} & y_1, y_2 \\ h = g_1^z & z \in \mathbb{Z}_q \end{array}$$

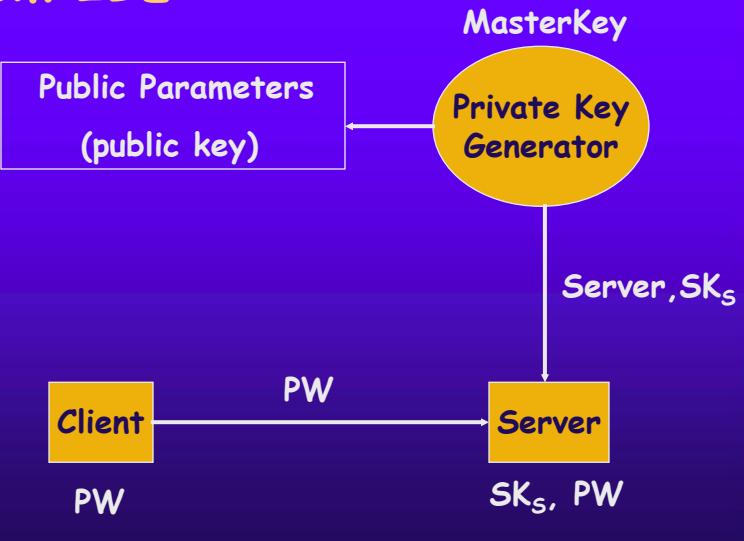
$$\begin{aligned} D: a &= H(u_1, u_2, e) \\ u_1^{x_1} u_2^{x_2} (u_1^{y_1} u_2^{y_2})^a &= v? \\ m &= e / u_1^z \end{aligned}$$



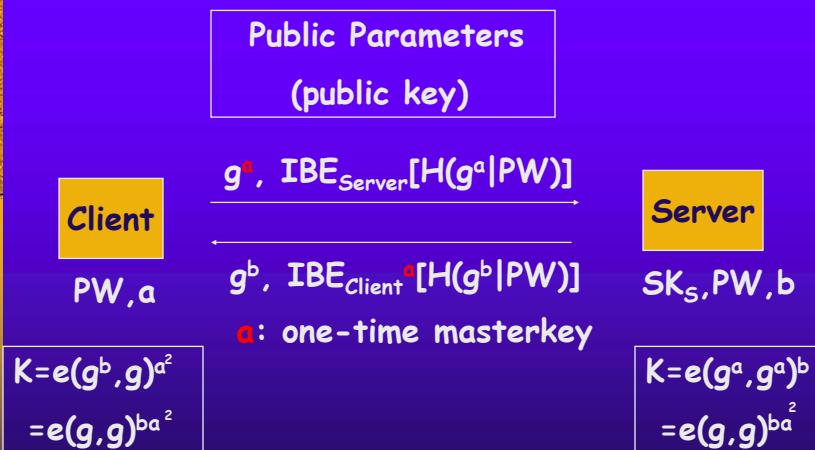
Motivations

- ◆ Common reference model versus IBE
- ◆ Implicit authentication versus explicit authentication
- ◆ PAKE security model versus ID-based PAKE security model

Security Model for PAKE from IBE



Client/Server PAKE from IBE



Practical IBE without Random Oracles

- ♦ C. Gentry: Practical identity-based encryption without random oracles (Eurocrypt 2006).
- ♦ Truncated decisional augmented bilinear Diffie-Hellman exponent (ABDHE) assumption

$$q, g, g_1 = g^a, h_1, h_2, h_3, H, \alpha: \text{MasterKey}$$

$$\begin{array}{ccc}
 \text{SecretKey} & & \\
 d_{ID} = \{(r_{ID,i}, h_{ID,i}): i=1,2,3\} & & \\
 h_{ID,i} = (h_i g^{r_{ID,i}})^{1/(\alpha - ID)} & & \\
 \begin{array}{c}
 E: s \in \mathbb{Z}_q \quad u = g^s g_1^{-sID} \\
 v = e(g, g)^s \\
 w = m \cdot e(g, h_1)^{-s} \\
 b = H(u, v, w) \\
 y = e(g, h_2)^s e(g, h_3)^{sb}
 \end{array} & \xrightarrow{u, v, w, y} & \begin{array}{l}
 R \\
 D: b = H(u, v, w) \\
 e(u, h_{ID,2} h_{ID,3}^{-b}) v^{r_{ID,2} + r_{ID,3}b} = y? \\
 m = w \cdot e(u, h_{ID,1}) v^{r_{ID,1}}
 \end{array}
 \end{array}$$

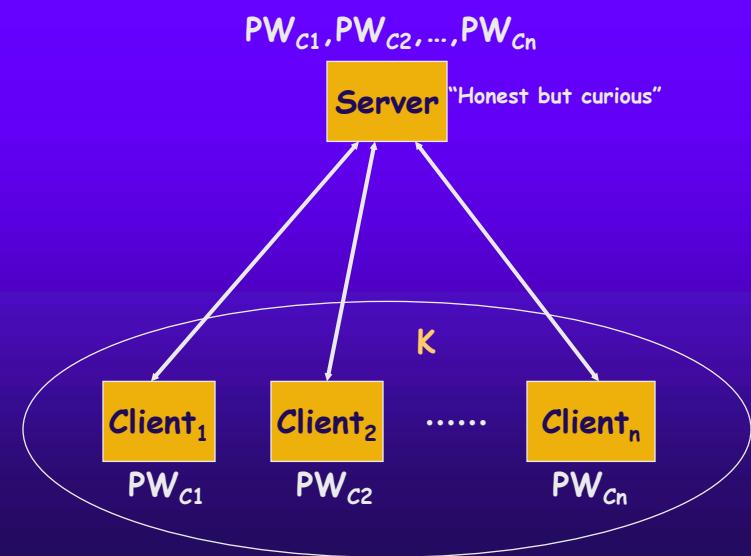
Security of Client/Server PAKE from IBE without Random Oracles

- ♦ IBE is secure against the adaptive chosen ciphertext attack.
- ♦ A new decisional Diffie-Hellman (NDDH) assumption: given $g, g^a, g^b, Z \in G$, it is hard to decide if $Z = e(g, g)^{ba^2}$
- ♦ ABDHE: $(g', g'_{q+2}, g, g_1, \dots, g_q, Z)$, it is hard to decide if $Z = e(g_{q+1}, g')$ where $g_i = g^{a^i}$
- ♦ NDDH is harder than ABDHE because let $g_{(q+1)/2} = g^x$, $g' = g^y$, then $e(g_{q+1}, g') = e(g, g)^{yx^2}$

KOY versus Client/Server PAKE from IBE (Client side)

| | KOY | YTO-1 |
|--------|-------------|-------------|
| Rounds | 3 | 2 |
| Auth. | Implicit | Explicit |
| Comm. | 12 | 10 |
| Comp. | 16 + 1 Sign | 14 + 2 Pair |

Extension to Group PAKE



Group PAKE from IBE

- ♦ Broadcasting communication model
- ♦ Clients run a group key exchange protocol P to obtain K
- ♦ Authentication



Security of Group PAKE from IBE and IBS

- ♦ Trust model
- ♦ IBE is secure against the adaptive chosen ciphertext attack.
- ♦ IBS is existential unforgeability under the chosen message attack.
- ♦ Group PAKE from IBE and IBS has been proved to be secure without random oracles.



Abdalla et al's Group PAKE versus ID-based Group PAKE

| | Abdalla et al. | YTO-2 |
|---------------|---|------------------------------------|
| Compiler | 2-party PAKE, Burmester- Desmedt KE | Group KE, Client/server PAKE |
| Trusted model | Each user is honest | Server is honest |
| Auth model | n pairs of users | All clients to server |
| Rounds | 5 | 4 |



Conclusion

- ♦ Client/server model
- ♦ Client/server PAKE from IBE is more efficient than existing 2-party PAKE without random oracles.
- ♦ Group PAKE from IBE and IBS is a new way to construct group PAKE protocols.



References

1. M. Abdalla, J. M. Bohli, M. I. G. Vasco, R. Steinwandt. (Password) authenticated key establishment: From 2-party to group. In Proc. TCC'07, pages 499-514, 2007.
2. M. Abdalla, P. A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. IEEE Proceedings in Information Security, 153(1): 27-39, Mar. 2006.
3. M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Proc. Eurocrypt'00, pages 139-155, May 2000.
4. S. M. Bellovin and M. Merritt. Encrypted key exchange: Password-based protocol secure against dictionary attack. In Proc. 1992 IEEE Symposium on Research in Security and Privacy, pages 72-84, May 1992.
5. D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In Proc. Crypto'01, pages 213-229, 2001.
6. M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In Proc. Eurocrypt'94, pages 275-286, 1995.
7. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Proc. Crypto'98, pages 13-25, 1998.
8. C. Gentry. Practical identity-based encryption without random oracle. In Proc. Eurocrypt'06, pages 445-464, 2006.
9. J. Katz, R. Ostrovsky, and M. Yung. Efficient password-authenticated key exchange using human-memorable passwords. In Proc. Eurocrypt'01, pages 457-494, 2001.
10. J. Katz and M. Yung. Scalable protocols for authenticated group key exchange. In Proc. CryptO'03, pages 110-125, 2003.