

# Password-based Group Key Exchange in a Constant Number of Rounds

M. Abdalla, E. Bresson, O. Chevassut and D. Pointcheval

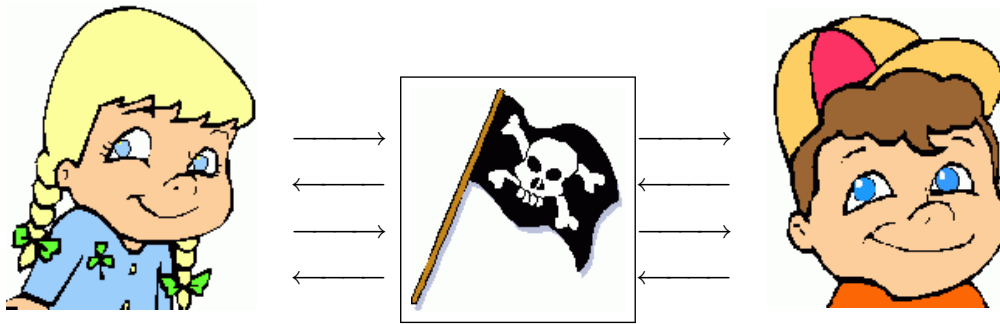
ENS and CELAR and LBNL and ENS

April 26<sup>th</sup>, 2006

- 1 Introduction
  - Authenticated Key Exchange
  - Dictionary attacks
  - Related work
- 2 Our results
  - Dictionary attack on Dutta-Barua
  - Key recovery attack on Lee-Hwang-Lee
  - Our repaired protocol
- 3 Conclusion

## Interaction context

A pool of  $n$  participants ( $n \geq 2$ ) try to commonly establish a symmetric session key, in the presence of an adversary.



The adversary tries to defeat the process: failure on the agreement, leakage of information, ...

## Definitions

### Definition (Security)

**Privacy:** No one except the legitimate players can obtain the established key.

**Authentication:** No one can prevent a terminating protocol to run normally, in particular no one can make a player believe there is a legitimate participant to talk with, if it is not the case.

### Definition (Adversary)

**Passive adversary:** Can only eavesdrop the communications

**Active adversary:** Can eavesdrop and modify the communications.

## Dictionary attacks (I)



A password is chosen in a small *dictionary* of size  $N$ ; this provides the adversary the ability to make an exhaustive search.

- ① A passive adversary can intercept communications (*transcripts*) and may try to test all the passwords one by one.
  - *off-line dictionary attacks*: the adversary may have much computing power.
- ② An active adversary can **additionally** try to guess the password and use it to impersonate a player.
  - *on-line guessing attacks*: easy to detect.

## Dictionary attacks (II)

What is impossible. . .

Completely prevent on-line attacks: any adversary can win after  $N$  attempts.

In practice, the impact of such attacks is *limited* using operational methods (counter, delay, . . .).

What can be (hopefully) achieved

Limit the adversary to on-line attacks only: this means off-line attacks must be made impossible.

A passive eavesdropping reveals nothing

An active attempt reveals nothing except. . . password's (in)validity.

## Password-based (group) key exchange

### Password-based authentication

- Initiated early 90's [BM92, GLNS93, Jab96]
- Formal models proposed in 2000 [BPR00, BMP00]
- Theoretical results follow [GL01, GL03]
- Further refinements [AFP05]

### Group Pw-based schemes

- Formal model [BCP02]
- Protocols [BCP02, BCP05]: linear complexity

### Group Constant-round schemes

- DH-like [BD94, KY03, Jou00]
- secret-sharing (polynomials): [BC04, LP99],
- fault-tolerance [CS04], 1-round [BN03]

### 1 Introduction

### 2 Our results

- Dictionary attack on Dutta-Barua
- Key recovery attack on Lee-Hwang-Lee
- Our repaired protocol

### 3 Conclusion

## Constant-round Group Key Exchange

### The Burmester-Desmedt protocol [BD94]

- **Round I** – Each player picks  $x_i$  and broadcasts:  $z_i = g^{x_i}$
  - **Round II** – Each  $U_i$  then broadcasts:  $X_i = Z_{i+1}/Z_i$ , with  $Z_k = g^{x_{k-1}x_k}$
- Each  $U_i$  sets his session key as  $K_i = Z_i^n X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i+n-2}$ .

It is easy to see that for any  $i$ , we have

$$K_i = \prod_{j=1}^{j=n} Z_j = g^{x_1x_2 + x_2x_3 + \cdots + x_nx_1}$$

## Adding Authentication

### Asymmetric authentication

Authentication added by Katz-Yung [KY03] using a generic *compiler*

Dynamic case considered by Kim-Lee-Lee [KLL04]

### Password authentication

Encrypt the flows using the password as a key (in the ideal cipher model): only the password will decrypt correctly

Eliminate redundancy in the plaintexts to avoid dictionary attacks

### Not so simple!

This naive approach does not work: the product of plaintexts in the 2<sup>nd</sup> round is 1  $\implies$  *dictionary attack*

## Adding Password Authentication

### A first (still naive) attempt

Values in Round  $i$  are “masked” with a product by  $h^{pw}$

- Each player picks  $x_i$  and broadcasts:  $z_i^* = g^{x_i} h^{pw}$
- Each  $U_i$  broadcasts:  $X_i = Z_{i+1}/Z_i$ , with  $Z_k = g^{x_{k-1}x_k}$   
 Each  $U_i$  sets his session key as  $K_i = Z_i^n X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i+n-2}$ .

### Does not work neither!

- Adversary sends  $z_1^* = g^{u_1}$  and  $z_3^* = g^{u_3}$ , for known  $u_1$  and  $u_3$
- Waits for receiving  $X_2$ . One easily checks  $X_2 = \left(\frac{z_2^*}{h^{pw}}\right)^{u_3 - u_1}$

## First attempt by Dutta and Barua [DB06]

### Proposed Protocol

- $U_i$  picks  $x_i$  and computes  $z_i = g^{x_i}$ , then broadcasts:  
 $z_i^* = \mathcal{E}_{pw}(z_i)$
- $U_i$  recover  $z_{i-1}$  and  $z_{i+1}$ , then computes  $K_i^L = \mathcal{H}(z_{i-1}^{x_i})$  and  
 $K_i^R = \mathcal{H}(z_{i+1}^{x_i})$  “left-key and right-key”
- For  $i = 1, \dots, n-1$ ,  $U_i$  broadcasts  $\mathcal{E}'_{pw}(k_i \| X_i)$ , where  
 $X_i = K_i^L \oplus K_i^R$  plaintexts are random...
- $U_n$  broadcasts  $\mathcal{E}'_{pw}(k_n \| X_n)$ , where  $X_n = k_n \oplus K_n^R$
- They can all recover the  $k_i$ 's and set the session key as  
 $\mathcal{H}(k_1 \| \cdots \| k_n)$

## Description of the attack

### The encryption key is common...

- Adversary  $\mathcal{A}$  plays the role of  $U_3$ , with honest users  $U_1$  and  $U_2$
- $\mathcal{A}$  waits for  $z_1^* = \mathcal{E}_{pw}(z_1)$  and  $z_2^* = \mathcal{E}_{pw}(z_2)$  and sends  $z_3^* = z_1^*$ . this forces  $x_3 = x_1$
- $U_2$  computes  $X_2 = K_2^L \oplus K_2^R = \mathcal{H}(g^{x_1 x_2}) \oplus \mathcal{H}(g^{x_2 x_3}) = 0^{\ell_{\mathcal{H}}}$
- Thus  $pw$  is the only password that decrypts the received  $\mathcal{E}'_{pw}(k_2 \| X_2)$  accordingly

## Another scheme by Lee-Hwang-Lee [LHL04]

### Proposed Protocol

- $U_i$  picks  $x_i$  and computes  $z_i = g^{x_i}$ , then broadcasts:  
 $z_i^* = \mathcal{E}_{pw}(z_i)$
- $U_i$  recover  $z_{i-1}$  and  $z_{i+1}$ , then computes  $K_i = \mathcal{H}(z_{i+1}^{x_i})$  and  $K_{i-1} = \mathcal{H}(z_{i-1}^{x_i})$  "left-key and right-key"
- $U_i$  broadcasts  $(w_i)$ , where  $w_i = K_{i-1} \oplus K_i$
- They can all recover the  $K_i$ 's and set the session key as  $\mathcal{H}'(K_1 \| \dots \| K_n)$

Very similar to the Dutta-Barua protocol, however the "redundant" stuff is not encrypted anymore...

## Description of the attack

### The sessions can be interleaved...

- Adversary  $\mathcal{A}$  starts  $U_1$  twice and receives  $z_1^* = \mathcal{E}_{pw}(g^{x_1})$  and  $z_1'^* = \mathcal{E}_{pw}(g^{x_1'})$
- $\mathcal{A}$  feeds the first session with  $U_2 : z_1'^*$ ,  $U_3 : z_1^*$ ,  $U_4 : z_1'^*$
- $\mathcal{A}$  feeds the second session with  $U_2 : z_1^*$ ,  $U_3 : z_1'^*$ ,  $U_4 : z_1^*$
- Then  $K_1 = K_2 = K_3 = K_4 = \mathcal{H}(g^{x_1 x_1'})$ , and in turn  $w_1 = w_2 = w_3 = w_4 = 0$ . Thus messages from players  $U_2$ ,  $U_3$  and  $U_4$  can be simulated. the honest instance  $U_1$  accepts!
- The same holds in the second session
- $\mathcal{A}$  can simply corrupt one session: the key in the other session is the same

## Our protocol

### Proposed Protocol

- $U_i$  chooses a nonce  $N_i$  and broadcasts  $(U_i, N_i)$   
 The session is  $S = U_1 || N_1 || \dots || U_n || N_n$ ; each user will use  $k_i = \mathcal{H}(S, i, pw)$  as a symmetric key
- $U_i$  picks  $x_i$ , computes  $z_i = g^{x_i}$  and sends  $z_i^* = \mathcal{E}_{k_i}(z_i)$
- $U_i$  extracts  $z_{i-1}$  and  $z_{i+1}$ , computes  $Z_i = z_{i-1}^{x_i}$  and  $Z_{i+1} = z_{i+1}^{x_i}$ , then broadcasts  $X_i = Z_{i+1}/Z_i$
- $U_i$  computes  $K_i = Z_i^n X_i^{n-1} X_{i+1}^{n-2} \dots X_{i+n-2}$ , and sends its authenticator  $\text{Auth}_i = \mathcal{H}'(S, \{z_j^*, X_j\}_j, K_i, i)$
- $U_i$  checks all authenticators and sets  $sk_i = \mathcal{G}(S, \{z_j^*, X_j, \text{Auth}_j\}_j, K_i)$

## Security result

### Theorem (Security against dictionary attacks)

*The presented protocol establishes a semantically secure session key, in the ideal-cipher model, provided the DDH assumption holds in the considered group family.*

$$\text{Adv}_P^{\text{ake}}(\mathcal{A}) \leq \frac{2q_{\text{active}}}{|\mathcal{D}|} + 4nq_{\text{session}}\text{Adv}_{\mathbb{G}}^{\text{ddh}} + \text{negl}(\ell)$$

**On the security bound:** We upper-bound  $\mathcal{A}$ 's advantage using the number of messages he made: **he cannot test more than 1 password per message;**

**Improvements?** It is still possible to test several passwords **per session.**

## Conclusion

- Efficient, simple active attacks on two schemes:
  - Password-recovery attack on Dutta-Barua scheme
  - Session key recovery attack on Lee-Hwang-Lee scheme
- A repaired scheme with provable security
- Open questions:
  - Find other constant-round password-based protocols
  - Optimal security bound for such protocols ?

## Bibliography I

- [AFP05] M. F. Abdalla, P.-A. Fouque, and D. Pointcheval. *Password-based authenticated key exchange in the three-party setting*. PKC'05, pp. 65–84.
- [BPR00] M. Bellare, D. Pointcheval, and Ph. Rogaway. *Authenticated key exchange secure against dictionary attacks*. Eurocrypt'00, pp. 139–155.
- [BR93a] M. Bellare and Ph. Rogaway. *Random oracles are practical: a paradigm for designing efficient protocols*. ACM-CCS '93, pp. 62–73.
- [BM92] S. M. Bellare and M. Merritt. *Encrypted key exchange: Password-based protocols secure against dictionary attacks*. Symposium on Security and Privacy, pp. 72–84.
- [BN03] C. Boyd and J. M. Nieto. *Round-optimal contributory conference key agreement*. PKC03, pp. 161–174.
- [BMP00] V. Boyko, Ph. D. McKenzie, and S. Patel. *Provably secure password-authenticated key exchange using Diffie-Hellman*. Eurocrypt'00, pp. 156–171.
- [BC04] E. Bresson and D. Catalano. *Constant round authenticated group key agreement via distributed computation*. PKC04, pp. 115–129.

## Bibliography II

- [BCP02] E. Bresson, O. Chevassut and D. Pointcheval. *Group Diffie-Hellman key exchange secure against dictionary attacks*. Asiacrypt'02, pp. 497–514.
- [BCP05] E. Bresson, O. Chevassut, and D. Pointcheval. *Password-authenticated group Diffie-Hellman key exchange*. Int. J. of Wireless and Mobile Computing, to appear.
- [BD94] M. Burmester and Y. G. Desmedt. *A secure and efficient conference key distribution system*. Eurocrypt'94, pp. 275–286.
- [CS04] C. Cachin and R. Strobl. *Asynchronous group key exchange with failures*. PODC.04, pp. 357–366.
- [DB06] R. Dutta and R. Barua. *Password-based encrypted group key agreement*. IJNS, 3(1):23–34.
- [GL03] R. Gennaro and Y. Lindell. *A framework for password-based authenticated key exchange*. Eurocrypt'03, pp. 524–543.
- [GL01] O. Goldreich and Y. Lindell. *Session-key generation using human passwords only*. Crypto'01, pp. 408–432.

## Bibliography III

- [GLNS93] L. Gong, T. M. A. Lomas, R. M. Needham, and J. H. Saltzer. *Protecting poorly chosen secrets from guessing attacks*. *IEEE J. on Sel. Areas in Comm.*, 11(5):648–656.
- [Jab96] D. P. Jablon. *Strong password-only authenticated key exchange*. *SIGCOMM Comp. Comm. Rev.*, 26(5):5–26.
- [Jou00] A. Joux. *A one-round protocol for tripartite Diffie-Hellman*. *ANTS IV*, pp. 385–394.
- [KY03] J. Katz and M. Yung. *Scalable protocols for authenticated group key exchange*. *Crypto '03*, pp. 110–125.
- [KLL04] H. Kim, S. Lee and D. H. Lee. *Constant-round authenticated key exchange for dynamic groups*. *Asiacrypt 04*, pp. 245–259.
- [LHL04] S. Lee, J. Y. Hwang and D. H. Lee. *Efficient password-based group key exchange*. *TrustBus 2004*, pp. 191–199.
- [LP99] C.-H. Li and J. Pieprzyk. *Conference key agreement from secret sharing*. *ACISP 99*, pp. 64–76.