

# Password-authenticated protocols

## *A survey*

E. Bresson

CELAr, Cryptology Department

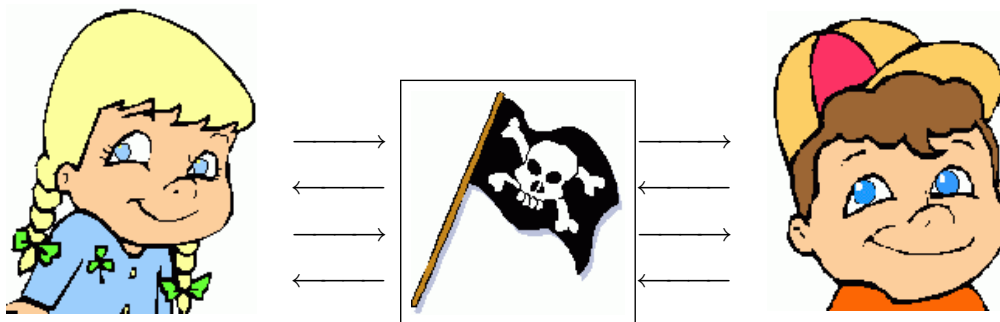
April 6<sup>th</sup>, 2006

- 1 Introduction
- 2 Security models
- 3 Computational Models
- 4 Main results
- 5 Conclusion

- 1 Introduction
  - Authenticated Key Exchange
  - Using short passwords
  - Dictionary attacks
- 2 Security models
- 3 Computational Models
- 4 Main results
- 5 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, ...

## Security Goals

### Definition (Privacy)

No one except the legitimate players can obtain the established key.

Key Exchange or **KE**. For a group of players, one talks about **GKE** (Group Key Exchange)

### Definition (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.

Authenticated Key Exchange or **AKE**. In case of groups: **GAKE**.

## Several kinds of adversaries

### Definition (Passive adversary)

Can only eavesdrop the communications.

Such an adversary threatens the *privacy* only.

### Definition (Active adversary)

Can eavesdrop and modify the communications.

Such an adversary can threaten both *authentication* and *privacy*.



## 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 (in the sense of Shannon).  
An active attempt reveals nothing except. . . password's (in)validity.

- 1 Introduction
- 2 Security models
  - Semantic security
  - Simulatability approach
  - Adapting the simulatability approach
  - Universal composition
- 3 Computational Models
- 4 Main results
- 5 Conclusion

## Indistinguishability approach

Initially: scenario AKE [BR93a], then pwAKE [BPR00]

### Queries capturing adversarial capabilities

- $\text{Execute}(U)$ : returns a *transcript* of an honest execution
- $\text{Send}(m, U)$ : sends the message  $m$  to player  $U$ ,
- $\text{Reveal}(U)$ : returns session key hold by player  $U$
- $\text{Corrupt}(U)$ : returns the password used by  $U$
- $\text{Test}^b(U)$ : returns the key  $sk$  if  $b = 1$ , or a random if  $b = 0$ .

$\text{Adv}^{\text{ake}}(\mathcal{A}) = \text{advantage}$  of  $\mathcal{A}$  in passing the Test (guessing  $b$ )

### Definition

Semantic security of  $sk$ : if  $\text{Adv}^{\text{ake}}(\mathcal{A}) - \frac{\text{Nb of Send}}{N} \approx \epsilon$

## Security = key indistinguishability

### Find-then-Guess (FtG)

- Many Reveal-queries
- Only one  $\text{Test}^b$ -query
- $\mathcal{A}$  searches for bit  $b$

### Real-or-Random (RoR)

- No Reveal-query
- Many Test-queries...
- ...with the same bit  $b$  !

### Theorem (Comparison FtG vs. RoR [AFP05])

For any protocol  $\mathcal{P}$  for authenticated key exchange, one has:

$$\text{Adv}_{\mathcal{P}}^{\text{ror-ake}}(t) \leq q_{\text{test}} \text{Adv}_{\mathcal{P}}^{\text{ftg-ake}}(t) \leq 2 \text{Adv}_{\mathcal{P}}^{\text{ror-ake}}(t)$$

## The security bound

### Meaning of the result

Upper-bounding the advantage by  $q_{send}/N$  means:

- The adversary cannot eliminate more than one password in an active attack.
- passive attacks are useless: the number of eavesdropped transcripts does not appear.

Strictly speaking, the important quantity is the number of **sessions** initiated by the adversary, rather than the number of messages. . . (in particular for group protocols)

## Forward-secrecy and known-key attacks

### Forward-secrecy

The session key remains secure if  $\pi$  is revealed after the execution

Using the **Corrupt-query**

### Known-key attacks

The session and  $\pi$  remain secure if previous keys are exposed

Using the **Reveal-query**

### Theorem

- *[GL01] guarantees forward-secrecy and known-key attacks resistance.*
- *[KOY02] adds forward-secrecy which was missing in [KOY01]*

## Multiparty simulation: classical case [Bea91, MR91, C00]

Modeling Key Exchange [BCK98, Sho99]: emulate a TTP (*trusted third party*). Extended to passwords by Boyko *et al.* [BMP00].

### Ideal world

- $\mathcal{A}$  initiates the game
- TTP chooses  $sk$
- $A$  and  $B$  do not communicate
- $\mathcal{A}$  can “test” a  $\pi$

### Real world

- No TTP,  $A$  and  $B$  hold  $\pi$
- $A$  and  $B$  communicate
- $\mathcal{A}$  wins with proba  $1/N$

### Definition (Security)

Any real adversary can be emulated in the ideal world, the output distributions being  $\epsilon$ -indistinguishable [C00].

## Multiparty simulation: adapting the case

Definition proposed by Goldreich-Lindell [GL01]. Distributions are not indistinguishable anymore.

### Ideal world

- $A, B$ : password  $\pi$
- $A, B \rightarrow$  TTP:  $\pi$
- TTP  $\rightarrow A, B$ : uniform key  $sk$
- $\mathcal{A}$  can *abort*

### Real world

- No TTP,  $A$  and  $B$  hold  $\pi$
- $A$  and  $B$  communicate **only via  $\mathcal{A}$**
- $\mathcal{A}$  wins with proba  $1/N$

### Definition (Security: adapted to passwords)

- $\Rightarrow$  ( **$\mathcal{A}$  passive**) : Output distributions are  $\epsilon$ -indistinguishable
- $\Rightarrow$  ( **$\mathcal{A}$  active**) : Output distributions can be distinguished only with probability  $O(1/N) + \epsilon$

## Universal composition [C01]

In the Key Exchange setting, it is important to consider the notion of universal composition [CK02].

### How to manage the following?

- passwords are not uniformly distributed,
- password distribution can be unknown,
- a password can be used in several protocols,
- passwords can be correlated.

- Universal composition is welcome !!
- A definition involving “true” indistinguishability [BMP00] is better for protocol composition (rather than [GL01]).

- 1 Introduction
- 2 Security models
- 3 Computational Models**
  - Algorithmic problems
  - Standard models
  - Ideal models

- 4 Main results
- 5 Conclusion

## Cryptographic assumptions

### Definition (Diffie-Hellman problems [DH76, Bon98])

- CDH : given  $(g^x, g^y)$ , find  $g^{xy}$
- DDH : given  $(g^x, g^y, g^z)$ , decide if  $z = xy$

### Chosen-basis variants [AP05a, AP05b]

- C-CDH : given  $(X, A, B)$ , choose  $Y$ , then find **CDH** $(X, Y)$  and **CDH** $(X/A, Y/B)$
- C-DDH : given  $(X, A, B)$ , choose  $Y$ , then decide  $r = x$  or  $r = y$  on input:  
 $(Y^r, (X/A)^x, \mathbf{CDH}(X/A, Y)^x, (X/B)^y, \mathbf{CDH}(X/B, Y)^y)$

## Group Diffie-Hellman problems

### Definition (Group Diffie-Hellman problems)

Let  $I = \{1, \dots, n\}$  and  $x_1, \dots, x_n$  random. Given some values  $g^{\prod_{j \in J} x_j}$ , for some proper subsets  $J$  of  $I$ ,

- G-CDH : find  $g^{x_1 \cdots x_n}$
- G-DDH : decide if  $r = x_1 \cdots x_n$  on input  $g^r$

### Theorem (Reduction GDH to DH [BCP02b])

*If the collection of subsets  $J$  for which the exponentiations  $\prod_{j \in J} x_j$  are known, is "well formed" the GCDH and GDDH problems can be reduced to CDH and DDH, respectively.*

## Standards models

These models do not need a random oracle and so can be more reasonably instantiated.

2 cases :

- the “plain” model [GL01]: no *setup* assumption, only a password is given
- the standard model with CRS (*Common Random String*): there might be a public key in the CRS. . .

## Ideal models

### The *Random Oracle Model* (ROM) [BR93a]

Function providing a fixed-length output, that is purely random for each new input.

There exists schemes secure in ROM and totally breakable for any instantiation of the function [CGH98].

### The *Ideal Cipher Model* (ICM) [BPR00]

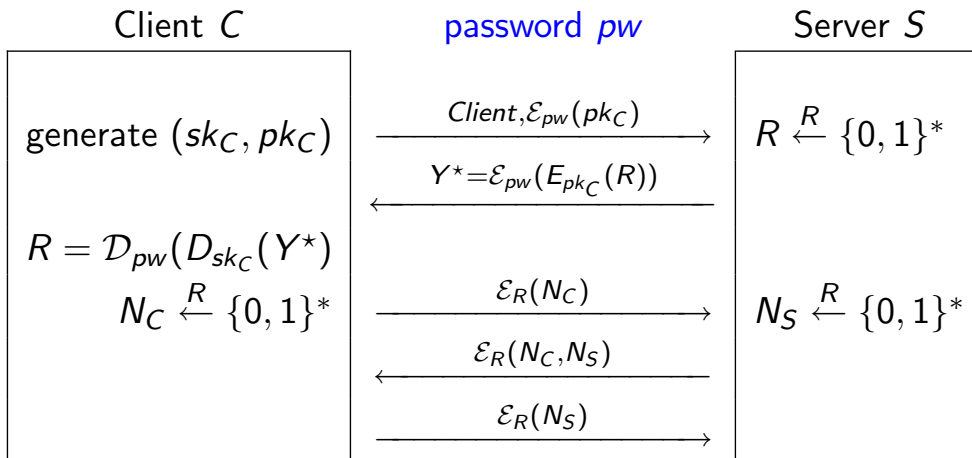
Family of permutations (with their inverses) indexed by keys, where all permutations are perfectly independent and random.

This model is (strictly?) stronger than ROM.

- 1 Introduction
- 2 Security models
- 3 Computational Models
- 4 Main results**
  - 2-party protocols
  - Protocols for groups
- 5 Conclusion

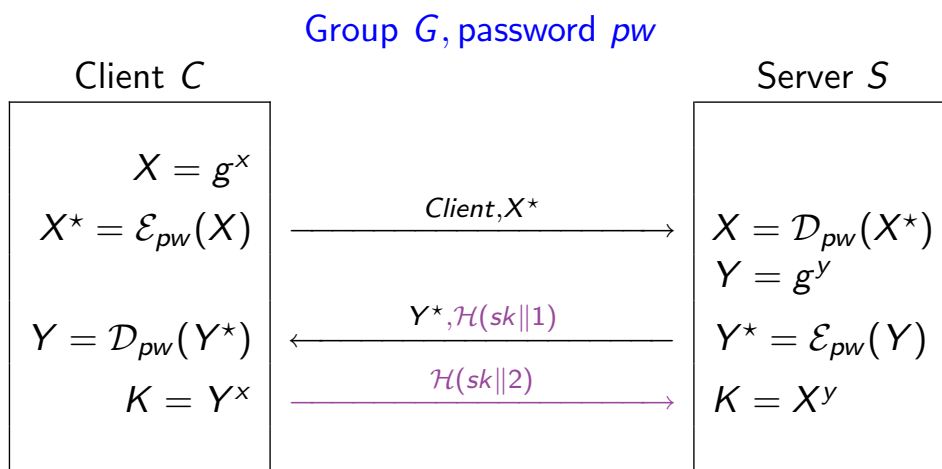
## EKE: Encrypted Key Exchange ( [BM92])

Encryption: symmetric ( $\mathcal{E}, \mathcal{D}$ ), asymmetric ( $E, D$ )



Session key:  $R$

## EKE2: Encrypted Key Exchange revisited ( [BPR00] )



Session key:  $sk = \mathcal{H}(C, S, X, Y, K)$  for pwKE  
 Key:  $sk' = \mathcal{H}(sk||0)$  for pwAKE

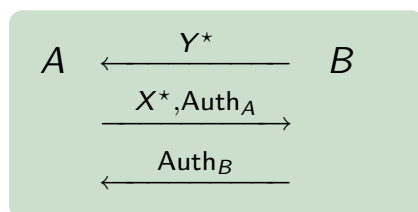
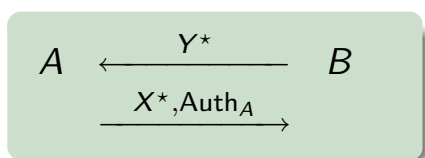
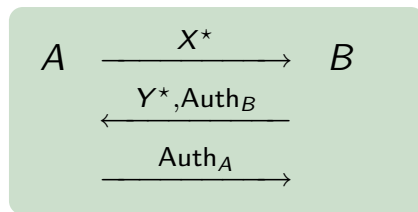
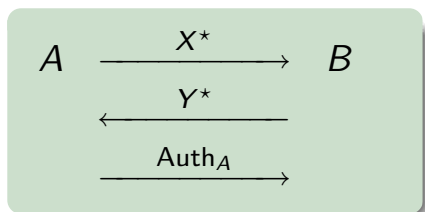
## History of EKE protocols

### Protocols derived from the previous one

- Generic framework (AuthA) [BR00]: heuristic security
- Protocol EKE2 [BPR00]: directly derived from AuthA
  - formal modal (*queries* + indistinguishability )
  - security proof in the ideal cipher model (ICM)
- Protocol PAK [BMP00]: instantiation of AuthA
  - formal model (multiparty simulatability)
  - security under the random oracle (ROM); but intricate proof

## Protocols AuthA for 2 parties ( [BR00], IEEE P1363)

Unilateral or bilateral (“mutual”) authentication  
 Protocol initiated either by A, or by B



## Instantiations and applications of AuthA

How to implement an ideal cipher  $X^* = \mathcal{E}_{pw}(X)$ ?

- PAK [BMP00]: multiplicative mask  $X^* = X \cdot \mathcal{H}(pw, \dots)$ . Needs a full-domain hash function.
- SPAKE [AP05a]: algebraic version:  $X^* = X \times U^{pw}$ . More flexibility.

How to adapt these protocols?

- Protocol OEKE (*One-Encryption Key Exchange*):  $X$  in clear
  - security proof in ICM [BCP03]
  - security proof in ROM [BCP04]
- SOKE [ABCM+06]: a version of SPAKE especially designed for TLS [BESW01]



## Constant-round pwGAKE

### History of Burmester-Desmedt [BD94]

- A protocol for KE [BD94] and AKE [KY03], independent of the number of players
  - Tentative to convert it into *password-based* [DB06]
  - Dictionary attacks, repaired scheme and security proof (ICM model) [ABCP06]
- 
- Each player picks  $x_i$  and broadcasts:  $\mathcal{E}_{pw}(g^{x_i})$
  - Each  $U_i$  then broadcasts:  $\mathcal{E}_{pw}(\Gamma_i/\Gamma_{i+1})$ , with  $\Gamma_k = g^{x_{k-1}x_k}$

### Not so simple!

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



## Conclusion








- Multiplicity of possible scenarii, definitions, assumptions
- Multiplicity of proposed protocols (attacks...)
- Formalization appears, inspired from other primitives
- Unifying the treatment of the problem

## Bibliography I

-  M. F. Abdalla, E. Bresson, O. Chevassut, B. Möller and D. Pointcheval. *Provably secure password-based authentication in TLS*. ACM ASIA CCS 2006, pp. 35–45.
-  M. F. Abdalla, E. Bresson, O. Chevassut and D. Pointcheval. *Password-based group key exchange in constant rounds*. PKC '06, to appear.
-  M. F. Abdalla, P.-A. Fouque, and D. Pointcheval. *Password-based authenticated key exchange in the three-party setting*. PKC '05, pp. 65–84.
-  M. F. Abdalla and D. Pointcheval. *Simple password-based encrypted key exchange protocols*. CT-RSA '05, pp. 191–208.
-  M. F. Abdalla and D. Pointcheval. *Interactive Diffie-Hellman assumptions with applications to password-based authentication*. Financial Crypto '05, pp. 341–356.
-  D. Beaver. *Secure multi-party protocols and zero-knowledge proof systems tolerating a faulty minority*. J. of Crypto., 4(2):75–122.
-  M. Bellare, R. Canetti, and H. Krawczyk. *A modular approach to the design and analysis of authentication and key exchange protocols*. STOC '98, pp. 419–428.










## Bibliography II

-  M. Bellare, D. Pointcheval, and Ph. Rogaway. *Authenticated key exchange secure against dictionary attacks*. Eurocrypt '00, pp. 139–155.
-  M. Bellare and Ph. Rogaway. *Random oracles are practical: a paradigm for designing efficient protocols*. ACM-CCS '93, pp. 62–73.
-  M. Bellare and Ph. Rogaway. *The AuthA protocol for password-based authenticated key exchange*. IEEE P1363.
-  S. M. Bellare and M. Merritt. *Encrypted key exchange: Password-based protocols secure against dictionary attacks*. Symposium on Security and Privacy, pp. 72–84.
-  D. Boneh. *The decision Diffie-Hellman problem*. ANTS III, pp. 48–63.
-  V. Boyko, Ph. D. McKenzie, and S. Patel. *Provably secure password-authenticated key exchange using Diffie-Hellman*. Eurocrypt '00, pp. 156–171.
-  E. Bresson, O. Chevassut and D. Pointcheval. *Group Diffie-Hellman key exchange secure against dictionary attacks*. Asiacrypt '02, pp. 497–514.



## Bibliography III

-  E. Bresson, O. Chevassut, and D. Pointcheval. *The group Diffie-Hellman problems*. SAC '02, pp. 325–338.
-  E. Bresson, O. Chevassut, and D. Pointcheval. *Security proofs for an efficient password-based key exchange*. ACM-CCS '03, pp. 241–250.
-  E. Bresson, O. Chevassut, and D. Pointcheval. *New security results on encrypted key exchange*. PKC '04, pp. 145–158.
-  E. Bresson, O. Chevassut, and D. Pointcheval. *Password-authenticated group Diffie-Hellman key exchange*. Int. J. of Wireless and Mobile Computing, to appear.
-  E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater. *Provably authenticated group Diffie-Hellman key exchange*. ACM-CCS '01, pp. 255–264.
-  J. P. Buhler, T. Eirich, M. Steiner, and M. Waidner. *Secure password-based cipher suite for TLS*. ACM Trans. on Info. and Syst. Security, 4(2):134–157.
-  M. Burmester and Y. G. Desmedt. *A secure and efficient conference key distribution system*. Eurocrypt '94, pp. 275–286.








## Bibliography IV

-  R. Canetti. *Security and composition of multi-party cryptographic protocols*. J. of Cryptology, 13(1):143–202.
-  R. Canetti. *Universally composable security: A new paradigm for cryptographic protocols*. FOCS '01, pp. 136–145.
-  R. Canetti, O. Goldreich, and S. Halevi. *The random oracle methodology, revisited*. STOC '98, pp. 209–218.
-  R. Canetti and H. Krawczyk. *Universally composable notions of key exchange and secure channels*. Eurocrypt '02, pp. 337–351.
-  W. Diffie and M. E. Hellman. *New directions in cryptography*. IEEE-IT 22(6):644–654.
-  R. Dutta and R. Barua. *Password-based encrypted group key agreement*. IJNS, 3(1):23–34.
-  O. Goldreich and Y. Lindell. *Session-key generation using human passwords only*. Crypto '01, pp. 408–432.



## Bibliography V

-  J. Katz, R. Ostrovsky, and M. Yung. *Efficient password-authenticated key exchange using human-memorable passwords*. Eurocrypt '01, pp. 475–494.
-  J. Katz, R. Ostrovsky, and M. Yung. *Forward secrecy in password-only key exchange protocols*. SCN '02.
-  J. Katz and M. Yung. *Scalable protocols for authenticated group key exchange*. Crypto '03, pp. 110–125.
-  S. Micali and Ph. Rogaway. *Secure computation*. Crypto '91, pp. 392–404.
-  V. Shoup. *On formal models for secure key exchange*. IBM RZ 3120.
-  A. C. Yao. *How to generate and exchange secrets*. FOCS '86, pp. 162–167.