



---

# Group Diffie-Hellman Key Exchange

## Secure Against Dictionary Attacks

Olivier Chevassut

(Ernest Orlando Lawrence Berkeley National Lab)

Emmanuel Bresson and David Pointcheval

(École Normale Supérieure)

---

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

## Outline



- Motivation
- Setting
- Related Work
- Model of Security
- Definitions of Security
- A Protocol for Password-Based Key Exchange
- Theorem of Security
- Conclusion

---

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

# Motivation



- An increasing number of distributed applications need to communicate within small groups, e.g.
  - conferencing and meeting
  - personal networking
  - emergency rescue and military operations
- An increasing number of distributed applications have security requirements
  - privacy of data
  - protection from hackers
  - protection from viruses
- Group communication must address security needs

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

# Setting



- Member characteristics
  - relatively small group (up to 100 members)
  - members have similar compute power
  - no hierarchy among members (no client/server model)
- Mobile Ad hoc Networks
  - no security infrastructure
  - no fixed networking infrastructure
  - multicast communication capabilities

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

## Prior Work



- “Provably Authenticated Group DH Key Exchange”, ACM CCS’01
  - all the members join the group at once (static membership)
  - public-key infrastructure
  - treatment in the framework of provable security
  - a provably secure protocol for authenticated group DH key exchange

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

## How Provable Security works



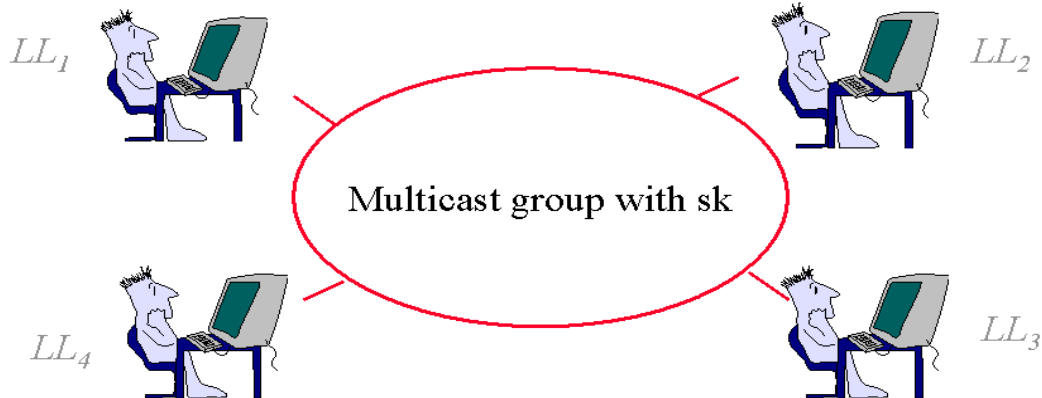
- 1. Specification of a model of computation**
  - instances of players are modeled via oracles
  - adversary controls all interactions among the oracles
  - adversary’s capabilities are modeled by queries to the oracles
  - adversary plays a game against the oracles
- 2. Definition of the security goals**
  - authentication, freshness and secrecy of session keys, forward-secrecy
- 3. Statement of the intractability assumptions**
  - group computational/decisional Diffie-Hellman (GCDH/GDDH)
- 4. Description of the algorithm and its proof of security**
  - proof shows by contradiction that the algorithm achieves the security goals under the intractability assumptions

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

## Model of Communication



- A set of  $n$  players
  - each player is represented by an oracle
  - each player holds a long-lived key (LL)
- A multicast group consisting of a set of players

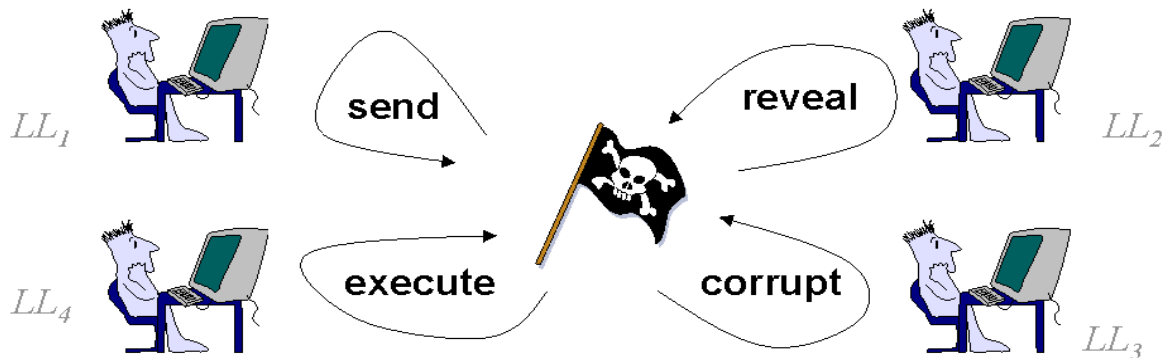


Asiacrypt – Dec 1-5, 2002 - O. Chevassut

## Modeling the Adversary

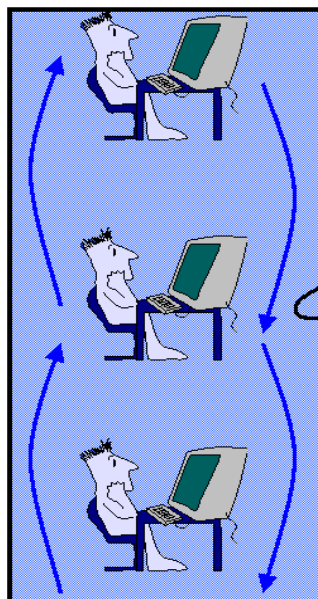


- Adversary's capabilities modeled through queries
  - send: send messages to instances
  - execute: obtain honest executions of the protocol
  - reveal: obtain an instance's session key
  - corrupt: obtain a player's long-lived key



Asiacrypt – Dec 1-5, 2002 - O. Chevassut

## Freshness Related Queries



*sk* is Fresh if it is known by the players but not the adversary

reveal

(*sk*)

(*LL*)

corrupt

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

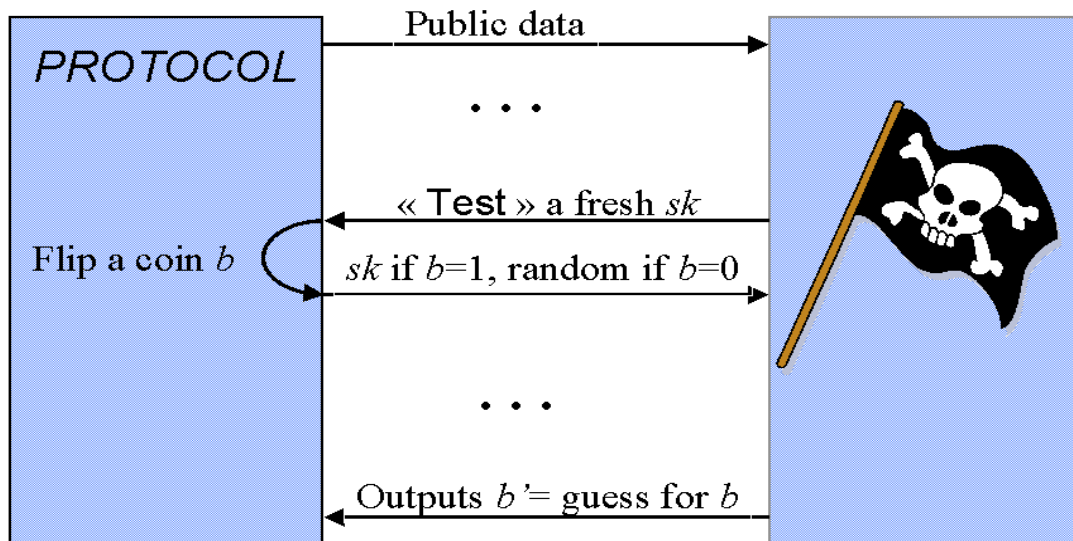
## Security Goal : AKE Authenticated Key Exchange



- Implicit authentication
  - only the intended partners can compute the session key
- Semantic security
  - the session key is indistinguishable from a random string
  - modeled via a Test-query
- Security against dictionary attacks
  - passive eavesdropping does not help the adversary in computing any information about the password

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

# Security Definitions (AKE)



Asiacrypt – Dec 1-5, 2002 - O. Chevassut

# Intractability Assumption: GCDH Group Computational Diffie-Hellman



- The CDH assumption generalized to the multi-party case
  - given the values  $g^{\prod x_i}$  for some choice of proper subset of  $\{1, \dots, n\}$
  - one has to compute the value  $g^{x_1 \dots x_n}$
- Example with three parties ( $n=3$  and  $I=\{1,2,3\}$ )
  - given the set of values
 

	$g^{x_1}$	$g$
$g^{x_1 x_2}$	$g^{x_1}$	$g^{x_2}$
$g^{x_1 x_2}$	$g^{x_1 x_3}$	$g^{x_2 x_3}$
  - compute the value  $g^{x_1 x_2 x_3}$
- The GCDH is equivalent to the DDH and CDH, SAC'98

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

# A Protocol for Password-Based Group Key Exchange



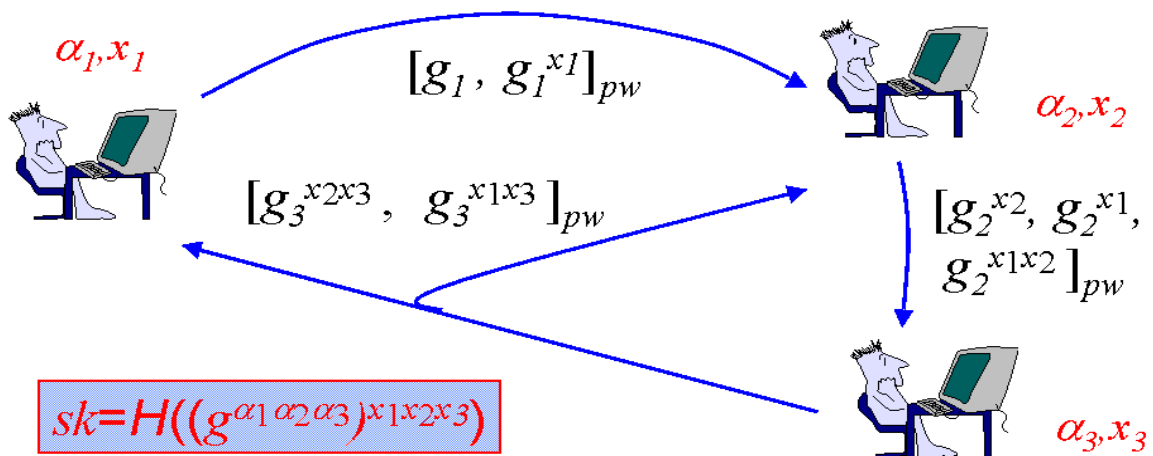
- The session key is
  - $sk = H(g^{x_1 x_2 \dots x_n})$
- Ring-based algorithm are encrypted under the password:
  - up-flow: the contributions of each instance are gathered
  - down-flow: the last instances broadcasts the result
  - instances compute the session key from the broadcast
- Many details abstracted out

Asiacrypt – Dec 1-5, 2002 - O. Chevassut

## The Algorithm



- Up-flow:  $U_i$  raises received values to the power of the values  $(x_i, \alpha_i)$  and forwards to  $U_{i+1}$
- Down-flow:  $U_n$  processes the last up-flow and broadcasts



Asiacrypt – Dec 1-5, 2002 - O. Chevassut

# Security Measurement (AKE) : Dictionary Attacks



- Theorem

$$\begin{aligned} \text{Adv}^{\text{ake}}(T, q_s, q_e) &\leq 2q_s/N + 2q_s \cdot \text{Adv}^{\text{mddh}}(T') \\ &\quad + 2 \cdot q_h \cdot \text{Succ}^{\text{gcdh}}(T') + \text{Cte} \\ T' &\leq T + n \cdot (3q_s + q_e) \cdot T_{\text{exp}}(k) \end{aligned}$$

- Ideal-cipher assumption

- Security against dictionary attacks

- the adversary's advantage grows essentially with the ratio of interactions (number of send-queries) to the number of password

## Defining the Games



- Game 0 : the adversary plays against the oracles in order to defeat the AKE-security of the protocol
- Game 1: we delete the executions in which the adversary has guessed the password
- Game 2 : we simulate the protocol flows using the elements from a GCDH-tuple
- Game 3 : we simulate the protocol flows using the elements from a GCDH-tuple whose value  $g^{x_1 \dots x_n}$  is unknown
- Game 4 : we answer at random to the Test-query and thus fix the adversary's probability of correctly guessing the bit to be 1/2.
- $\text{Proba}[\text{Adversary has guessed the password}] = 2q_s/N + q_s \cdot \text{Adv}^{\text{mddh}}(T')$

# Conclusion and Future Work

---



- **Summary**
  - A security model for security against dictionary attacks
  - A password group key agreement protocol
  - A proof of security
- **Limitations**
  - Random-oracle and ideal-cipher assumptions
- **Work in Progress**
  - “Key Agreement for Heterogeneous Mobile Devices”,
  - “Proofs of Security for the IEEE P1363 AuthA Protocol and Extensions”