The Group Diffie-Hellman Problems

Emmanuel Bresson
(ENS, France)

Olivier Chevassut (LBNL, USA)
David Pointcheval (ENS, France)

OUTLINE

- Motivation
- Related Work
- Two-party Diffie-Hellman key exchange
- Group Diffie-Hellman key exchange
- Relation between the group DH problems and the DH problems
- Conclusion
Motivation

- An increasing number of distributed applications need to communicate within groups, e.g.
  - collaboration and videoconferencing tools
  - replicated servers and distributed computations
- An increasing number of applications have security requirements
  - privacy of data
  - protection from hackers, viruses and trojan horses
- A method to establish a group session key is needed

Objectives

- Studying algorithmic problems in the discrete logarithm setting
  - Diffie-Hellman problems
  - Group Diffie-Hellman problems
- Why finding reductions between the group DH and the two-party DH problems
  - To get confidence in the group DH problems
  - To correctly choose security parameters for them
  - To securely design group key agreement protocols
Related Work

■ Design methodology
  - based on complexity theory
  - successful at avoiding flaws
  - useful to validate cryptographic algorithms

■ Prior Results
  - « Group DH key exchange under standard assumptions », Eurocrypt ’02
  - « Provably authenticated group DH key exchange - dynamic case », Asiacrypt ’01
  - « Provably authenticated group DH key exchange », ACM CCS ’01

Provable Security Methodology

1. Specification of a model of computation

2. Definition of the security goals

3. Statement of the intractability assumptions
   - computational/decisonal Diffie-Hellman problems (CDH/DDH)
   - group computational/decisonal DH problems (GCDH/DDH)

4. Description of a group DH key exchange scheme and its proof of security
   - proof shows by contradiction that the algorithm achieves the security goals under the intractability assumptions
The Diffie-Hellman protocol [DH76]

- 2-party key exchange protocol

- Establishing a secure channel between two parties is reduced to the problem of generating a session key sk
- The session key is used to achieve data secrecy and integrity

\[ sk = g^{x_1 x_2} \]

The Diffie-Hellman problems

- Computational problem (CDH)
  - Given \( g^{x_1}, g^{x_2} \), is the enemy able to compute the shared secret \( g^{x_1 x_2} \)?

- Decisional problem (DDH)
  - Given \( g^{x_1}, g^{x_2} \), is the enemy able to distinguish the shared secret \( g^{x_1 x_2} \) from a given random value \( g^r \)?
Security of the DH protocol

- **CDH assumption (weaker than DDH)**
  - If CDH holds, the key $H(g^{x_1x_2})$ is semantically secure, in the random oracle model
- **DDH assumption**
  - If DDH holds, the key $g^{x_1x_2}$ is semantically secure

Basic reductions to the discrete logarithm problem

- Fix a multiplicative group $G$, and an element $g$
- **Discrete logarithm problem (DL)**
  - Given $y \in \langle g \rangle$, find $x$ such that $y = g^x$
- One easily gets
  - DL $\Rightarrow$ CDH $\Rightarrow$ DDH
Group Diffie-Hellman Protocols

- Defined by three algorithms
  - SETUP \( (all\ cases) \)
  - REMOVE \( (dynamic\ case) \)
  - JOIN \( (dynamic\ case) \)

- The session key is
  - \( sk = H(g^{x_1 x_2 \ldots x_n}) \)

The SETUP Algorithm

- Ring-based protocols
- Compute step by step a generalized DH values

\[ sk = H(g^{x_1 x_2 x_3}) \]
The **REMOVE** Algorithm

\[ sk = H(g^{x_1x_2x_3}) \]

---

The **JOIN** Algorithm

- Initiated by player with the highest index in group

\[ sk = H(g^{x_1x_2x_3x_4}) \]
The Group Computational DH Assumption

- The CDH generalized to the multi-party case
  - given some subsets of indices in $I = \{1, \ldots, n\}$ and all the values $g^{\prod_{i \in J} x_i}$ for every given subset $J$ of $I$,
  - one has to compute the value $g^{x_1 \cdot \cdot \cdot x_n}$
- Example with four parties ($n=4$ and $I = \{1,2,3,4\}$)
  - given the values $g^{x_1}$, $g^{x_1 x_2}$, $g^{x_1 x_2 x_3}$, $g^{x_1 x_2 x_3 x_4}$, $g^{x_2}$, $g^{x_2 x_3}$, $g^{x_2 x_3 x_4}$, $g^{x_3}$, $g^{x_3 x_4}$, $g^{x_4}$
  - compute the last value $g^{x_1 x_2 x_3 x_4}$

The Group Decisional DH Assumption

- The DDH generalized to the multi-party case
  - given some subsets of indices in $I = \{1, \ldots, n\}$ and all the values $g^{\prod_{i \in J} x_i}$ for every given subset $J$ of $I$,
  - one has to distinguish the value $g^{x_1 \cdot \cdot \cdot x_n}$ from a random one
- Example with four parties ($n=4$ and $I = \{1,2,3,4\}$)
  - given the values $g^{x_1}$, $g^{x_1 x_2}$, $g^{x_1 x_2 x_3}$, $g^{x_1 x_2 x_3 x_4}$, $g^{x_2}$, $g^{x_2 x_3}$, $g^{x_2 x_3 x_4}$, $g^{x_3}$, $g^{x_3 x_4}$, $g^{x_4}$
  - distinguish the last value $g^{x_1 x_2 x_3 x_4}$ from a random one
Reducing GDDH to DDH

- Let $\mathcal{F}_n$ be a collection of subsets of $I_n=\{1,\ldots,n\}$
  - E.g., the above triangular structure (flows)
  - For a « good » type of collection of subsets,
    - $\text{adv}^{\text{gddh}}\mathcal{F}(t) \leq (2n-3)\text{adv}^{\text{ddh}}(t^*)$
    - with $t^* \leq t + t_G \sum \gamma_i$ and where $\gamma_i$ is the size of $\mathcal{F}_i$

- We can see GDDH as a standard assumption!

Reducing GCDH to DDH and CDH

- Let $\mathcal{F}_n$ be a collection of subsets of $I_n=\{1,\ldots,n\}$
  - E.g., the above triangular structure (flows)
  - For a « good » type of collection of subsets,
    - $\text{suc}^{\text{gcdh}}\mathcal{F}(t) \leq \text{suc}^{\text{cdh}}(t) + (n-2)\text{adv}^{\text{ddh}}(t^*)$
    - with $t^* \leq t + t_G \sum \gamma_i$ and where $\gamma_i$ is the size of $\mathcal{F}_i$

- Can we see GCDH as a (hybrid) standard assumption?
Hierarchy among problems

- GCDH → GDDH
- DL → CDH → DDH
- Theorem 2
- Theorem 1

Conclusion and Future Work

- Contributions
  - Formalizing the group Diffie-Hellman problems
  - Studying the case where a reduction applies
  - Reducing GDH assumptions to DDH or, better, CDH

- Future work
  - Reducing GCDH to CDH only?