Two Formal Views of Authenticated Group Diffie-Hellman Key Exchange

E. Bresson[1], O. Chevassut[2,3], O. Pereira[2],
D. Pointcheval[1] and J.-J. Quisquater[2]

[1] Ecole Normale Supérieure, 75230 Paris Cedex 05, France,
{Emmanuel.Bresson, David.Pointcheval}@ens.fr
[2] UCL Crypto Group, B-1348 Louvain-la-Neuve, Belgium,
{pereira, quisquater}@dice.ucl.ac.be
[3] Lawrence Berkeley National Laboratory, Berkeley, CA 94720, USA,
OChevassut@lbl.gov

February 28, 2002

Abstract

With the advance of multicast communication infrastructures several works address the task of sharing a session key among a group of users. Some of theses works extend the Diffie-Hellman protocol to the multi-party setting but can not by lack of adequate formal models provide stringent arguments to support the security of their protocols. Fortunately, formal models and formal treatments have recently been carried out by both the cryptographic community and the formal-method community. In this talk we present our two approaches and our results in each model. This talk is also a first step toward filling out the gap between two "views" of the authenticated group Diffie-Hellman key exchange.

The first theoretical concepts of public-key cryptography go back to Diffie and Hellman in 1976 [10] and the first public-key cryptosystem only two years later to Rivest, Shamir and Adleman [23]. In their seminal paper *New Directions in Cryptography*, Diffie and Hellman provided a method whereby two principals communicating over an insecure network can agree on a secret value, i.e. a value that a computationally bounded adversary can not recover by eavesdropping on flows exchanged between the two principals. Nowadays with the advance of multicast communication infrastructures [2, 8, 13] come the need to extend this method to allow a pool of principals to agree on a secret value. We refer to this extension as the group Diffie-Hellman protocol [24].

In their original publication, the Diffie-Hellman protocol and the group Diffie-Hellman protocol were designed to protect against a (passive) adver-

sary that only eavesdrop on messages. However, when it comes to use it in practice, a much stronger adversary need to be considered. In the real-world the adversary has complete control over all the network communications: it may choose to relay, reschedule, inject, alter messages between players; it may choose to impersonate a player and so on. One way to prevent these attacks is to add authentication services to the Diffie-Hellman protocol. However despite of the superficial simplicity of this task, many protocols have later found to be flawed [4, 11, 20]. Some flaws even took years before to be discovered. One way to avoid many of the flaws is to complete formal proofs of security.

Recently, formal treatments of the authenticated group Diffie-Hellman problem have been completed [6, 5, 9, 16, 17, 20, 21]. In [6, 5] we analyze this cryptographic problem in the framework of complexity theory by building on the work of Bellare et al. [3]. In our formalization, a process referred to as an oracle running on some machine is modeled as an instance of a player and the capabilities of the adversary are modeled through queries to these oracles. The notion of semantic security captures what it means to securely exchange a session key. We prove protocols secure by constructing a successful algorithm from a well-define "hard" computational problem that uses the adversary as a subroutine. This is what the notion of reduction is all about. Unfortunately, reductions are usually difficult to carry out and barely systematic.

Another trend is to verify cryptographic protocols using "logical" approaches [7, 14, 15, 19, 25]. The model we presented in [20, 21] belong to these ones. Theses methods typically assume perfect cryptography and consider the messages exchanged as the assembly of symbolic elements (identifiers, keys, nonces, . . .). These simplifications make protocol analysis much more systematic and often automatic (typically through the use of model checkers or theorem provers). Security proofs carried out in these models have often been criticized by the cryptographic community because of to the more abstract model of the adversary. Nevertheless, these methods permitted the analysis of more important and diversified systems and the discovery of attacks against numerous practical protocols. Furthermore, several works have been recently carried out in order to bridge the gap between the logic and the complexity approaches [1, 18, 12, 22], by showing the computational soundness of logical models.

In our two complementary approaches of the authenticated group Diffie-Hellman key exchange we identified models and security properties. By pursuing two formal treatment in parallel we were able to discover attacks against published protocols and modified them to achieve provable security. The structure of these proofs depicts quite well the main benefits and drawbacks of each technique. The complexity-based cryptography allowed us to determine which part of the security of the group Diffie-Hellman decision problem is injected in the analyzed protocols, what gives indications

about the security parameters to be used in the practice. However, to be more manageable, this analysis does not capture attacks scenarios implying simultaneous and concurrent sessions of the protocol. These last attacks schemes are precisely the ones for which logical techniques have shown their great efficiency. By applying techniques of this category, we were able to discover systematically several unpublished attacks scenarios, and prove security properties for slight variants of other ones. However, these proofs were constructed in the abstraction of the involved cryptographic primitives characteristics.

This talk is a first attempt to evaluate the benefits and shortcomings of two formal models for the authenticated group Diffie-Hellman key exchange. We will first highlight the security goals for the authenticated group Diffie-Hellman key exchange to achieve and then show how these goals can be meet in both models. Our goal in this talk is to show how to take advantage of both approaches and also to fill out the gap between two "views" in cryptography.

References

[1] M. Abadi and P. Rogaway. Reconciling two views of cryptography. In *Proceedings of the IFIP International Conference on Theoretical Computer Science 2000*, pages 3–22, 2000.

[2] D. A. Agarwal, O. Chevassut, M.R. Thompson, and G. Tsudik. An Integrated Solution for Secure Group Communication in Wide-Area Networks. In *Proc. of 6th IEEE Symposium on Computers and Communications*, 2001.

[3] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Advances in Cryptology - Proceedings of EUROCRYPT '00*, pages 139–155. LNCS Vol. 1807, 2000.

[4] R. Bird, I. Gopal, A. Hertzberg, P. Janson, S. Kutten, R. Molva, and M. Yung. Systematic Design of Two-Party Authentication Protocols. In *Proceedings of Crypto'91*, pages 44–61. LNCS Vol. 576, 1991.

[5] E. Bresson, O. Chevassut, and D. Pointcheval. Provably authenticated group Diffie-Hellman key exchange - the dynamic case. In C. Boyd, editor, *Advances in Cryptology - Proceedings of AsiaCrypt 2001*, pages 290–309. LNCS Vol. 2248, 2001.

[6] E. Bresson, O. Chevassut, D. Pointcheval, and J-J Quisquater. Provably authenticated group Diffie-Hellman key exchange. In P. Samarati, editor, *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 255–264. ACM Press, 2001.

[7] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. In *Proceedings of the Royal Society*, volume 426 number 1871, 1989.

[8] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Nao r, and B. Pinkas. Issues in Multicast Security: A Taxonomy and Efficient Constructions. In *Proc. of INFOCOM '99*, March 1999.

[9] I. Cervesato, C. Meadows, and P. Syverson. Formalizing GDOI group key management requirements in NPATRL. In *Eighth ACM Conference on Computer and Communication Security*, pages 235–244. ACM Press, 2001.

[10] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[11] W. Diffie, P. van Oorschot, and M. Wiener. Authentication and authenticated key exchange. *Designs, Codes and Cryptography*, 2(2):107–125, 1992.

[12] J. Guttman, F. J. Thayer Fábrega, and L. Zuck. The faithfulness of abstract protocol analysis: Message authentication. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, 2001.

[13] T. Hardjono and G. Tsudik. IP Multicast Security: Issues and Directions. *Annales de Telecom*, 2000.

[14] G. Lowe. Casper: A compiler for the analysis of security protocols. *Journal of Computer Security*, 6:53–84, 1998.

[15] C. Meadows. The NRL protocol analyzer : an overview. *Journal of Logic Programming*, 26(2):113–131, 1996.

[16] C. Meadows. Extending formal cryptographic protocol analysis techniques for group protocols and low-level cryptographic primitives. In *Proceedings of the Workshop on Issues in the Theory of Security*, 2000.

[17] C. Meadows and P. Narendran. A unification algorithm for the group diffie-hellman protocol. In *Proceedings of the Workshop on Issues in the Theory of Security*, 2002.

[18] D. Micciancio and B. Warinschi. Completeness theorems for the abadi-rogaway language of encrypted expressions. In *Proceedings of the Workshop on Issues in the Theory of Security*, 2002.

[19] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.

[20] O. Pereira and J-J. Quisquater. A security analysis of the cliques protocols suites. In *Proceedings of the 14-th IEEE Computer Security Foundations Workshop*, pages 73–81. IEEE Computer Society Press, 2001.

[21] O. Pereira and J-J. Quisquater. Security analysis of the cliques protocols suites: 1st results. In *Proceedings of IFIP Sec'01*, pages 151–166. Kluwer Publishers, 2001.

[22] B. Pfitzmann, M. Schunter, and M. Waidner. Cryptographic security of reactive systems. In *Electronic Notes in Theoretical Computer Science*, volume 32. Elsevier Science Publishers, 2000.

[23] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of*

the *ACM*, 21(2):120–126, 1978.

[24] M. Steiner, G. Tsudik, and M. Waidner. Diffie-hellman key distribution extended to group communication. In *Proceedings of IEEE ICDCS'97*, 1997.

[25] F. J. Thayer, J. H. Herzog, and J. Guttman. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 7(2/3):191–230, 1999.