Strong Corruptions in Group Key Exchange Protocols

Research Position Paper

Mark Manulis
Horst-Görtz Institute for IT Security
Ruhr-University of Bochum, Germany
mark.manulis@rub.de

November 23, 2006

Motivation

Group key exchange (GKE) protocols are foundational for the privacy and authentication issues in a variety of group applications. Participants of a GKE protocol obtain a secret shared key (group key) that can be further used in cryptographic primitives like symmetric encryption schemes and message authentication codes. Common for all GKE protocols is that during the protocol execution participants generate and compute some ephemeral secret data before they can obtain material used for the actual derivation of the group key. In case that group membership changes occur, so-called *dynamic* GKE protocols provide efficient operations to update the group key. Usually, this efficiency comes from the fact that participants reuse the previously obtained ephemeral secret data. Intuitively, this information when revealed may have serious impacts on the protocol security. In particular, when considering *strong corruptions* [7,13,14] – attacks, in which the adversary may break into the private memory of protocol participants, designing secure (dynamic) GKE protocols appears an interesting yet challenging task.

State of the Art

Currently, the security analysis in the area of (dynamic) GKE protocol focuses on some basic security requirements, described in the following.

The most basic security requirement for GKE protocols is called *(authenticated) key exchange (AKE) security*, e.g., [7, 8]: it ensures indistinguishability of the session group key from a random key sampled in the same space. This requirement can be combined with a flavor known as *(perfect) forward-secrecy*, a notion meaning that even if corrupting long-lived keys, the adversary cannot gain advantage in distinguishing previously established session keys. A more severe extension in which strong corruptions become an issue is the so-called *strong forward-secrecy* [7, 13, 14], in which the adversary in addition to the long-lived key reveals participant's internal data. The requirement of strong forward-secrecy can be achieved using a popular *erasure technique* [2, 7, 10, 13]. Though in static GKE protocols achieving strong forward-secrecy is trivial since the required ephemeral data is fresh for every protocol execution, it becomes more challenging in dynamic protocols where this data is usually reused in subsequent sessions. Currently, there exists no dynamic GKE protocol which provides strong forward-secrecy under standard cryptographic assumptions, e.g., security of [10] could only be proven in the random oracle model [3].

Another basic security requirement for GKE protocols is called *mutual authentication (MA) security* [6]: it ensures that all legitimate protocol participants and only them compute identical session group keys. As noticed in [9], these requirements must also hold in the presence of *malicious participants*; this means that, when corrupting, the adversary gets full control over the participants, thus making them deviating arbitrarily from the protocol specification; in fact [9] provides definitions of security against malicious participants, and a concrete generic solution (compiler) to prevent these attacks. Still, definitions in [9] do not consider attacks revealing internal states of honest protocol participants.

Mitchel *et al.* [12] gave informal definition of *key control*, to describe attacks where participants try to influence the resulting value of the computed session group key[1]. Ateniese *et al.* [1] proposed a related informally defined notion called *contributiveness* to encompass the fact that all participants must equally contribute to the computation of the group key and guarantee its freshness (see also [14]). These definitions state the main difference between (group) key distribution and (group) key exchange; in the latter no third party should be able to choose the resulting (group) key on behalf of other participants [11]. Following these requirements Bresson and Catalano [5] have (implicitly) considered the (weaker) case where honest participants have biased source of randomness so that the adversary can possibly gain extra information about the resulting group key. Deepening this, Bohli, Vasco and Steinwandt [4] gave definitions of key control and contributiveness considering a (stronger) case where participants wish to influence the resulting value of the group key deliberately. Still, their definitions are based on the model from [8] without consideration of strong corruptions.

Research Goals

Summarizing the above, security against strong corruptions is considered currently in a rather restrictive way, that is w.r.t. the requirement of *strong forward secrecy* in the context of AKE-security. Surely, this is an important step towards higher security standards for (dynamic) GKE protocols, however, further steps are needed in order to talk about security of GKE protocols against strong corruptions in general. Therefore, expanding the consideration of strong corruptions for other security requirements is an appealing, yet not resolved, task of research, which also implies the actual design of (dynamic) GKE protocols that can resist these powerful attacks.

Our research goals include the study of the basic security requirements for GKE protocols from the perspective of strong corruptions, and design of provably secure (dynamic) GKE protocols against such severe adversarial setting.

Results and Future Directions

We have solved most of the problems put in light above for static GKE protocols. We designed a new (game-based) security model considering a powerful adversary who is given access to the strong corruptions. We extended current definitions of AKE- and MA-security and formalized the notion of contributiveness. Additionally, we designed a static GKE protocol `TDH1`, which requires at most three communication rounds and is provably secure against strong corruptions according to our (extended) definitions. Some techniques applied in the construction of `TDH1` can be seen as generic for a variety of currently known GKE protocols.

Our future work focuses on the security model and design of provably secure dynamic GKE protocols under consideration of strong corruptions and standard cryptographic assumptions.

[1] Although [12] considers key control for two-party protocols similar threats become even more important in the multi-party case.

References

[1] G. Ateniese, M. Steiner, and G. Tsudik. Authenticated Group Key Agreement and Friends. In *Proceedings of the 5th ACM conference on Computer and Communications Security (CCS'98)*, pages 17–26. ACM Press, 1998.

[2] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated Key Exchange Secure Against Dictionary Attacks. In *Advances in Cryptology–EUROCRYPT'00*, volume 1807 of *Lecture Notes in Computer Science*, pages 139–155. Springer, May 2000.

[3] M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS'93)*, pages 62–73. ACM Press, 1993.

[4] J.-M. Bohli, M. I. G. Vasco, and R. Steinwandt. Secure Group Key Establishment Revisited. Cryptology ePrint Archive, Report 2005/395, 2005. `http://eprint.iacr.org/`.

[5] E. Bresson and D. Catalano. Constant Round Authenticated Group Key Agreement via Distributed Computation. In *Proceedings of the 7th International Workshop on Theory and Practice in Public Key Cryptography (PKC'04)*, volume 2947 of *Lecture Notes in Computer Science*, pages 115–129. Springer, 2004.

[6] E. Bresson, O. Chevassut, and D. Pointcheval. Provably Authenticated Group Diffie-Hellman Key Exchange - The Dynamic Case. In *Advances in Cryptology – ASIACRYPT'01*, volume 2248 of *Lecture Notes in Computer Science*, pages 290–390. Springer, December 2001.

[7] E. Bresson, O. Chevassut, and D. Pointcheval. Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions. In *Advances in Cryptology – EUROCRYPT'02*, volume 2332 of *Lecture Notes in Computer Science*, pages 321–336. Springer, Mai 2002.

[8] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater. Provably Authenticated Group Diffie-Hellman Key Exchange. In *Proceedings of the 8th ACM conference on Computer and Communications Security (CCS'01)*, pages 255–264. ACM Press, 2001.

[9] J. Katz and J. S. Shin. Modeling Insider Attacks on Group Key-Exchange Protocols. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 180–189. ACM Press, 2005.

[10] H.-J. Kim, S.-M. Lee, and D. H. Lee. Constant-Round Authenticated Group Key Exchange for Dynamic Groups. In *Advances in Cryptology – ASIACRYPT'04*, volume 3329 of *Lecture Notes in Computer Science*, pages 245–259, 2004.

[11] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996. ISBN:0-8493-8523-7.

[12] C. J. Mitchell, M. Ward, and P. Wilson. Key Control in Key Agreement Protocols. *Electronic Letters*, 34(10):980–981, 1998.

[13] V. Shoup. On Formal Models for Secure Key Exchange (Version 4). Technical Report RZ 3120, IBM Research, November 1999. Also available at `http://shoup.net/`.

[14] M. Steiner. *Secure Group Key Agreement*. PhD thesis, Saarland University, March 2002.