7G-01

# How to make undeniable evidence on Secret handshakes

Somnath PANJA †1
ISI, Kolkata
somn.math2017(at)gmail.com

Sabyasachi DUTTA †2
Kyushu University
saby.math(at)gmail.com

Kouichi SAKURAI†3
Kyushu University & ATR
sakurai(at)inf.kyushu-u.ac.jp

## 1. Introduction

Secret handshake is a practical primitive that allows a group of authorized users to establish a shared secret key and authenticate each other anonymously. It provides a certain degree of user privacy and deniability which are also desirable for private conversations that require secure key establishment. Deniability allows authorized users to deny later their participating in conversations. This work investigates the deniability of existing secret handshakes, and show some flaws when semi-honest users keep digital evidence which may become a hindrance to deniability.

## 2. Background

Secret handshake protocol [1] was designed to protect user's privacy and security when two users want to communicate in a hostile network condition. Consider a situation when two parties A and B want to identify each other as members of a secret organization and then communicate. Thus, A wants to make sure that if B is not a member of the organization then he cannot learn anything about the identity of A once the protocol is run. However, if B is a member of the group then he can identify A as another member of the group.

The concept of secret handshake was first introduced by Balfanz et al. [1]. The security of the scheme was based on the hardness of bilinear Diffie-Hellman problem in random oracle model. The scheme was constructed from a pairing-based key agreement scheme. Castelluccia et al. [4] gave a more efficient scheme under the computational Diffie-Hellman assumption in the random oracle model. Apart from anonymity of the participant, few other properties are also desirable in the secret handshake setting, such as affiliation-hiding [6], unlinkability [7], and user untraceability [9]. The affiliation-hiding secret handshake is a stronger privacy preserving model than conventional secret handshake. In contrast to the conventional secret handshake, in affiliation-hiding secret handshake protocol, non-authorized users cannot identify the authorized users from their protocol conversations or computed session keys. Unlinkable secret handshake has the following features: multiple sessions with the same user cannot be linked together. Untraceble secret handshake allows authorized users (participants) to remain untraceable with respect to untrusted issuing authorities.

Deniability property is also desirable in the secret handshake setting. In the wake of recent revelations of mass surveillance by intelligence services, deniability has become a desirable property in secret handshake protocols and key exchange protocols. Deniable secret handshake protocols allow protocol participants to later plausibly deny their participation in the conversation, while still providing authentication to protocol participants during the conversation. This notion was popularized with the release of Off-the-Record Messaging (OTR) [2] protocol. Recently, Tian et al. proposed a framework for deniable secret handshake protocol (DSH) [11]. They have given a generic construction of a DSH protocol from any forward-secure secret handshake protocol. Deniability is a notion which is captured by simulation based paradigm. Suppose an adversary tries to convince a third party that a conversation is held between two members of a group by producing a proof (possibly, a transcript) of the conversation. A secret handshake protocol is said to be deniable if a simulator can generate an identical view of the conversation/ protocol transcript which is indistinguishable from the real view. There are two notions of deniability- full deniability and strong deniability. Full deniability captures the scenario when two honest users are faithfully performing the protocol and an outside adversary sees the communication transcripts. The adversary produces the transcript to a third party and claims that aforementioned honest parties talked to each other. Now if there is a simulator that can generate indistinguishable view without the certificates of honest users and master key of CA then we call the protocol fully deniable.

On the other hand, strong deniability is applicable to the scenario when one of the users is malicious and wants to trap an honest user with whom he is communicating. Now, if a simulator is given the same inputs as the malicious party (including secret certificates and randomness of the party) and it can produce an indistinguishable view from the real view then the protocol is said to be strongly deniable. For more

†1 This work was done during visit in Kyushu University 2018
†2 is supported by an International Invitation Program of National Institute of Information and Communications Technology (NICT) Japan.
†3 is supported by JSPS Kaken Kiban-C JP18K11297

literature on deniability in the context of key exchange protocol, we refer to [3, 5, 8, 10, 12, 13, 14].

When discussing deniability of participating in a protocol, there are two types of third party judges existing in the secure messaging literature viz. offline judges and online judges. An offline judge examines the transcripts of a protocol execution that occurred in the past and decides whether or not the parties mentioned in the transcript were actually involved in the conversation. The judge is given a protocol transcript, showing all transmitted data (usually encrypted) and chat transcript. When proving the deniability of the protocol, the judge is also given access to the long-term secret keys of all participants named in the transcript. The judge must decide whether these transcripts constitutes a proof of involvement of the parties in the question. An online judge interacts with a protocol participant, referred to as the informant, while the protocol conversation is occurring. The judge has a secure and private connection to the informant and may instruct the informant to execute certain action in the protocol. The judge may instruct the informant to corrupt a participant, compromising their secret keys. The judge does not have direct visibility into the network. The judge is informed when a participant is corrupted.

## 3. Our Contribution

We consider the scenario which lies in between- one of the users is neither completely honest nor completely malicious but is semi-honest. Semi-honest party follows the protocol as required but may store randomness/ other values to extract more information than he is expected to get if he behaves honestly.

We show that in presence of a semi-honest user, the protocol of Tian et al. [11] is not fully- deniable. More specifically, if the responder of a SH protocol is semi-honest and maintains receipt(s) then a simulator is unable to generate a transcript which is indistinguishable from the transcript generated during the real execution of the protocol - resulting in the loss of full-deniability for the initiator. We then propose a possible countermeasure to fix the issue.

Note: Our attack of making evidence (a kind of receipt) on the proposed secret handshake protocol was inspired from the third author's previous work on 3-round interactive protocol [15], which analysis a dishonest verifier's private randomness.

We notice that there may be a subjective issue about the model of deniability. However, this work opens up possibilities to standardize definitional set up for deniability in the context of secret handshake.

## References


1. Balfanz, D., Durfee, G., Shankar, N., Smetters, D. K., Staddon, J. and Wong, H.- C.,"Secret Handshakes from Pairing-Based Key Agreements", In IEEE S&P 2003: pp. 62-73.
2. 2. Borisov, N., Goldberg, I., Brewer, E.,"Off-the-record communication, or, why not to use PGP", In Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, pp. 77-84 (2004).
3. Bellare, M., Rogaway, P.,"Random Oracle is Practical: A Paradigm for Designing Efficient Protocols,", In ACM CCS'93 2003: 180-196 (2003).
4. Castelluccia, C., Jarecki, S. and Tsudik, G., "Secret Handshakes from CA-Oblivious Encryption", ASIACRYPT 2004: 293-307 (2004).
5. Di Raimondo, M., Gennaro, R. and Krawczyk, H., "Deniable authentication and key exchange", In ACM CCS 2006: 400-409 (2006).
6. Jarecki, S., Kim, J., Tsudik, G., "Group secret handshakes or affiliation- hiding authenticated group key agreement.". In Abe, M. (ed.) CT- RSA 2007. LNCS , vol. 4377, pp. 287-308. Springer, Heidelberg (2006). https://doi.org/10.1007/11967668 19.
7. Jarecki, S., Liu, X., 'Private mutual authentication and conditional oblivious trans- fer.'. In Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 90107. Springer, Heidelberg (2009). https://doi.org/10.1007/978–3–642–03356–8 6.
8. Jiang, S., Safavi-Naini, R.: 'An efficient deniable key exchange protocol (extended abstract)'. In FC 2008, 4752 (2008).
9. Manulis, M., Poettering, B., Tsudik, G.: 'Affiliation-hiding key exchange with un- trusted group authorities.'. In Zhou, J., Yung, M. (eds.) ACNS 2010., vol. 6123, pp. 402419. Springer, Heidelberg (2010). https://doi.org/10.1007/978–3–642–13708–2 24.
10. Pass, R., "On Deniability in the Common Reference String and Random Oracle Model", CRYPTO 2003: 316-337 (2003).
11. Tian Y., Li Y., Zhang Y., Li N., Yang G., Yu Y.: 'DSH: Deniable Secret Hand- shake Framework.'. In Su C., Kikuchi H. (eds) Information Security Practice and Experience. ISPEC 2018. Lecture Notes in Computer Science, vol 11125. Springer, Cham.
12. Nik Unger and Ian Goldberg.: 'Deniable Key Exchanges for Secure Messaging.'. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communica-tions Security,, pages 12111223. ACM, 2015
13. Yao, A.C.-C., Zhao, Y.: 'Privacy-preserving authenticated key-exchange over internet.'. In IEEE TIFS, 9(1), 125140 (2014).
14. Yung, M. and Zhao, Y., "Interactive Zero-Knowledge with Restricted Random Oracles", In TCC 2006: 21-40 (2006).
15. Kouichi Sakurai, Toshiya Itoh:On the Discrepancy between Serial and Parallel of Zero-Knowledge Protocols CRYPTO 1992: 246-259