New Protocols for Proving Knowledge of Arbitrary Secrets While not Giving Them Away

Wouter Teepe

Artificial Intelligence, University of Groningen,
Grote Kruisstraat 2/1, 9712 TS Groningen, The Netherlands,
email: w.g.teepe@ai.rug.nl

Abstract

This paper introduces and describes new protocols for proving knowledge of secrets without giving them away: if the verifier does not know the secret, he does not learn it [1]. An implementation van be found in this volume [2].

1 Introduction: Proving Secrets

In application domains where sensitive information plays an important role, such as police research, intelligence, finance and the medical domain, one may want to ask whether someone knows a specific fact. Because of the sensitivity of the information concerned, it is often undesirable for the specific fact itself to be told by way of posing the question. For example posing the question "Did you know that Geertje is pregnant?" will inform the asked person about a fact. If it is the aim to ask this very question without informing the asked person about the fact, we need dedicated protocols for asking such questions in a multi-agent context.

In these protocols, we recognise a *prover* and a *verifier*. Three role configurations exist for this type of protocols: (1) the prover may want to pro-actively prove knowledge of a secret, (2) a verifier may ask someone to prove knowledge of a secret, or (3) two players may mutually prove knowledge of a secret.

In essence, these protocols consist of the verifier asking the prover to modify the secret in a way chosen by the verifier, and to show the cryptographic hash value of this "altered secret". The number of computations needed for this can be reduced if we allow encrypted communication between the prover and the verifier.

The three role configurations together with the decision whether to use encryption, gives a total of six protocols, all shown in the extended paper [1].

2 Problem description

The following is a more precise description of when this type of protocols is needed.

Victor is a secret agent, and keeping secret his intelligence has a high priority. However, his mission is to protect Peggy from great dangers, so when needed,

protecting Peggy takes priority over keeping his information secret. Now he is confronted with the following situation: Victor does not know whether certain information known to him, is also known to Peggy. ("Peggy is kindly invited for a dinner at Mallory's place.")[1] Victor knows that Mallory is a very malicious person. If Peggy does know that she is kindly invited, Victor would like to send her a warning message ("Don't go there, it is a trap. You will get killed in case you go there."). However, if Peggy has somehow not received the invitation, Victor would like to keep his warning for himself, as well as his knowledge of Peggy's invitation. Therefore, Victor asks Peggy to prove her knowledge of the invitation. Only after the proof, Victor will disclose his warning to Peggy.

Peggy is willing to prove her knowledge of the invitation, but only if she can make sure Victor does not cheat on her, and actually finds out about the invitation because he tricks her into telling him (she has been invited). That is, she only wants to prove her knowledge of the invitation if Victor actually knew about the invitation beforehand.

The protocols described in the long version of this article facilitate the described situation. Both Victor and Peggy can initiate the protocol. Victor will not learn any property of the secret my means of the protocol. In the protocol, Peggy does not learn whether Victor actually knew about the invitation, other than from his possible next actions, such as sending a warning.

3 The ANITA project

The research contributing to the protocols and this demonstation is the Administrative and Normative Information-Transaction Agents project, ANITA for short. Its aim is to use multi-agent systems to provide methods for both complete and legitimate information exchange of sensitive information, such as in the Dutch police domain. The Dutch police offers us a very interesting application area for our protocols. Police investigation teams typically want to keep their files secret, but *do* want to know whether other teams are investigating on the same persons or locations. If indeed multiple teams are investigating on the same person, they would better co-operate, or at least make sure they do not hinder one another.

References

[1] W. Teepe. New protocols for proving knowledge of arbitrary secrets while not giving them away. In Sieuwert van Otterloo, Peter McBurney, Wiebe van der Hoek, and Michael Wooldridge, editors, *Proceedings of the Knowlegde and Games Workshop*, Liverpool, July 2004. available at `http://www.ai.rug.nl/~woutr/provingsecrets/`.

[2] Wouter Teepe. The secret prover: Proving possession of arbitrary files while not giving them away. same volume.

[1] For clarity, this information could be possession of a computer file stating the invitation. This sets apart the matter whether the information is truthful.