

## Is this simple scheme secure?

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-01/2070.html>

---

**From:** NYC (*name\_at\_company.com*)

**Date:** 01/30/04

Date: Fri, 30 Jan 2004 21:20:22 +0100

Suppose we have 2 individuals A & B and a message M.

Both A & B claims to know M however none of them trusts that the other party knows M and they don't want to give M to the other party in case the other party doesn't already know it.

A demands that B proves that he knows M. What protocol can be used for B to convince A that he knows M in case A itself knows M, and without revealing anything if A doesn't know M.

A can't just ask B to send a hash, because maybe B knows just the hash and not the message itself (for example, B might have overheard a conversation A has with another party about the same thing).

My simple suggestion is:

- 1) A generates, say, a 20-byte random message C and sends it to B
- 2) B calculates  $P = \text{SHA}(C | M)$  and sends it to A.
- 3) A verifies that  $P = \text{SHA}(C | M)$ .

Even though B might now  $\text{SHA}(M)$  and/or  $\text{SHA}(X | M)$  for many values of X, and even though he is of course fully capable of generating  $\text{SHA}(C)$  I don't think any of this helps him in generating  $\text{SHA}(C | M)$ . Also, I don't think A can calculate M based on information on C and  $\text{SHA}(C|M)$ .

However, if it this simple, why all this talk about zero-knowledge proofs etc.? I read a brief note about it, and seemed very complex involving Hamiltonian circuits and whatnot.