

## Re: Nightingale and Cut-and-Choose Proofs

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-07/1394.html>

---

**From:** David Wagner (*daw\_at\_taverner.cs.berkeley.edu*)

**Date:** 07/30/04

Date: Fri, 30 Jul 2004 03:02:52 +0000 (UTC)

flip wrote:

> "*cut-and-choose proofs*".

This is a specific technique used in constructing zero-knowledge proofs.

Suppose I want to get you to sign a value of the form  $y = H(\text{"David Wagner"}, n)$  where  $n$  is a secret number I claim to know, but I want to keep secret from you. You aren't willing to sign just anything, but you are willing to sign values of this form (because they have my name).

Here is a trick for accomplishing this. I generate 1000 values  $y_1, \dots, y_{1000}$  with  $y_i = H(\text{"David Wagner"}, n_i)$  where each  $n_i$  is picked uniformly and independently at random. I send you all of the  $y_i$  values. You choose an index  $j$ , say  $j=57$ , and challenge me to reveal all the  $n_i$  values except for  $i=57$ . So, I send you  $n_1, \dots, n_{56}, n_{58}, \dots, n_{1000}$ . You confirm that these are consistent with the  $y_i$  values received earlier, and if they are, you send me a signature on  $y_{57}$ . At the end of this protocol, I have a signature on  $y_{57} = H(\text{"David Wagner"}, n_{57})$ , you don't know  $n_{57}$ , and you have some assurances that the value you signed is indeed the hash of my name followed by some number. If I try to cheat, my chance of success is at most  $1/1000$ . I think this gives you the idea.

I don't know where the name "cut-and-choose" came from, but I can easily imagine it came from the standard protocol for fairly splitting a cake between two parties (i.e., you cut, I choose).