# Logical Composition of Zero-Knowledge Proofs

Andrew Clausen, http://www.econ.upenn.edu/∼clausen

October 6, 2007

## 1 Introduction

Alice is a director of a chemical company. She is appalled by delays to repairs of a leaky pipe that transports a chemical that kills small children. If Alice leaked the email anonymously, no-one would believe it is real. Alice could convince a journalist, Bob that she knows her private key with a zero-knowledge proof, but then she would lose her anonymity, and risk being fired, assassinated, stood up by James Bond, etc. Can Alice convince Bob that she is a director by convincing Bob that she knows one of the directors' private keys – but without revealing which one?

The whistleblower's problem is an example of a logical composition problem. Given zero-knowledge proofs for a set of assertions $\{\varphi_1, \ldots, \varphi_n\}$, is it possible to construct a zero-knowledge proof of an arbitrary proposition, such as

$$\varphi_1 \wedge (\varphi_2 \vee \neg\varphi_3)?$$

Three primitive cases to consider:

- Conjunction: This is trivial to implement. To prove $\psi \wedge \varphi$, run the proofs of $\psi$ and then $\varphi$ sequentially.
- Disjunction: This is non-trivial to implement. Simply proving the correct proposition would reveal too much information – namely which assertion is true. The rest of this note describes a technique to prove $\psi \vee \varphi$ when 3-step polynomial-time-prover ZKPs are available for $\psi$ and $\varphi$. Unfortunately, the resulting proof is only witness-indistinguishable rather than full zero-knowledge.
- Negation: This is impossible unless $\mathcal{NP} = \text{co}\mathcal{NP}$, as efficient provers only exist for languages in $\mathcal{NP}$.

This means the techniques described in this note will be able to construct witness-indistinguishable proofs for monotonic propositions – i.e. propositions that only use the $\vee$ and $\wedge$ connectives.

To prove a disjunction $\psi \vee \varphi$, the prover will simultaneously execute proofs of $\psi$ and $\varphi$. However, one of the ZKPs will be fake, and the other real. The verifier will not know which is fake, and will only be able to deduce that one of the assertions is true. To implement this partial faking, the prover will use a secret sharing scheme, which is the topic of the section 2. However, since the disjunction proof executes several proofs in parallel, it is unknown whether the resulting protocol is zero-knowledge. Instead, Cramer et al. [1994] show that their proofs are witness-indistinguishable. Section 3 defines this weaker notion of knowledge. Finally, section 4 describes the disjunction proof, and argues that it is indeed witness-indistinguishable.

## 2 Secret sharing schemes

Our motivation for using secret sharing is for constructing zero-knowledge proofs for disjunctions of propositions, which is described in the following section. But the original (and more intuitive) motivation for secret sharing schemes is controlling a group of agents' access to a secret. For example, they can enforce a rule that the nuclear weapon launch codes must only be released with the support of at least two-thirds of the cabinet members. Each member would be given a *secret share* such that the launch code can only be computed if at least two thirds of the shares are available.

More formally, a distributor that knows the secret $s$ would like to construct $n$ secret shares $\{s_i\}_{i=1}^n$, so that any subset containing at least $k$ of them can be used to compute $s$.

In Shamir [1979]'s secret sharing scheme, the distributor constructs the secret shares as follows:

**Protocol 1** (Secret sharing)**.** *Common input: $k, n \in \mathbb{N}$ with $k \leq n$.*
*Distributor's private input: $s \in \mathbb{F}$, where $\mathbb{F}$ is a finite field with at least $n+1$ elements.*
*Output: secret shares $\{s_i\}_{i=1}^n$, so that any $k$ shares can recover the secret $s$.*

1. The distributor chooses a random polynomial $f \in \mathbb{F}[x]$ of degree $k-1$ so that $f(0) = s$. That is, the distributor chooses the coefficients $f_1, \ldots, f_{k-1}$, and sets $f_0 = s$.
2. The distributor gives each receiver $i \in \{1, \ldots, n\}$ the share $s_i = (x_i, y_i) = (i, f(i))$.

Then, any group of agents with at least $k$ members can reconstruct the secret:

**Protocol 2** (Secret reconstruction)**.** *Input: any $k$ of the shares $\{s_i\}_{i=1}^n = \{(x_i, y_i)\}_{i=1}^n$.*
*Output: $s$.*

1. Use Lagrangian interpolation to construct $f$ from $S$. That is, solve the $k$ simultaneous equations $\sum_{j=0}^{k-1} f_j x_i^j = y_i$ for the polynomial coefficients $f_0, \ldots, f_{k-1}$:
2. Output $s = f(0) = f_0$.

If the threshold of $k$ shares is met, then the secret reconstruction succeeds because every degree $k-1$ polynomial is uniquely determined by any $k$ points it passes through. (While this is a fundamental result for $\mathbb{R}[x]$, the generalization to finite fields with at least $k+1$ elements is also standard.) Thus, $k$ points on the polynomial $f$ contain enough information to recover $f$ completely, and hence the secret $s = f(0)$. Since the equations are all linear, they can be solved with standard finite field arithmetic.

If fewer than $k$ people reveal their secret shares $s_i$, then any choice of $f(0)$ is consistent with some polynomial in $\mathbb{F}[x]$, so no information is revealed about $s$.

# 3 Witness-indistinguishable proofs

If zero-knowledge proofs are executed in parallel, they may no longer be zero-knowledge. (See section 4.5.4 of Goldreich [2001].) This is a problem for Cramer et al. [1994]'s disjunction proof, which works by pretending to simultaneously proving all of the assertions. A weaker notion of zero-knowledge can be preserved, however. There is also second motivation for studying weak notions of zero-knowledge: since these proofs are easier to design, a procedure for upgrading them to full zero-knowledge would be useful.

The weakest possible definition of almost-zero-knowledge would be if the verifier were not curious, then no information would be leaked from conversations with the prover. (Full zero-knowledge requires that no information leaks for *all* verifiers, not merely one innocent verifier.)

**Definition 3** (Honest verifier zero-knowledge proof)**.** *An interactive proof system $(P, V)$ of a language $L$ is* honest verifier zero-knowledge *if there exists a polynomial time simulator $M$ such that $\{view_V^P(x)\}_{x \in L}$ is indistinguishable from $\{M(x)\}_{x \in L}$.*

Recall that a polynomial-time prover must have some private input called a witness to help it convince the verifier. For example, in the whistleblower's problem, Alice needs to know her own private key. But several other witnesses would also suffice, such as the CEO's key or the CFO's key. An interactive proof is witness-indistinguishable if it does not give any useful information about which witness the prover used.

**Definition 4** (Witness-indistinguishable proof)**.** *An interactive proof system $(P, V)$ of a language $L \in \mathcal{NP}$ is* witness-indistinguishable *for a witness relation $R_L$ if: for every PPT verifier $V^*$ and for every sequence of pairs of witnesses $\{(w_x^1, w_x^2)\}_{x \in L}$ with $\{w_x^1, w_x^2\} \subseteq R_L(x)$, the ensembles*

$$\{\langle P(w_x^1), V^*(z)\rangle(x)\}_{x \in L, z \in \{0,1\}^*} \text{ and } \{\langle P(w_x^2), V^*(z)\rangle(x)\}_{x \in L, z \in \{0,1\}^*}$$

*are computationally indistinguishable.*

It will be convenient to work with 3-step proofs.

**Protocol 5** (3-step schema)**.** *Proves:* $x \in L$.
*Common input:* $x$.
*Prover's private input: a witness* $w$*, where* $(x, w) \in R_L$.

1. Offer: The prover randomly picks $m^1$ independently of $w$, and sends it to the verifier.
2. Challenge: The prover picks a challenge $c$ uniformly at random, and sends it to the prover.
3. Response: The prover responds with $m^2$, based on $(w, m^1, c)$.
4. The verifier checks $m^2$, based on $(x, m^1, c)$.

For example, the graph isomorphism zero-knowledge proof has this form. To prove $G_1 \cong G_2$, the prover gives the verifier a random graph $m^1 = G_3$ that is isomorphic to the other graphs. The verifier issues a challenge $c \in \{1, 2\}$. The prover responds with an isomorphism establishing $G_c \cong G_3$.

**Lemma 6.** *Every 3-step interactive proof* $(P, V)$ *that is honest verifier zero-knowledge is witness-indistinguishable.*

# 4 Witness-indistinguishable proofs of disjunctions

Cramer et al. [1994] prove $\varphi \vee \psi$ by providing a genuine proof for one of the propositions, and a fake proof for the other. The prover is forced to answer a difficult challenge for any proposition, but can rig an easy challenge for the remaining proposition. The verifier only knows that one of the challenges was difficult, but does not know which one. The verifier concludes that at least one of the propositions is true.

For example, suppose the whistleblower Alice establishes her identity by proving that two graphs $G_1$ and $G_2$ are isomorphic. Her boss uses a different pair of graphs $H_1$ and $H_2$. Alice could prove she is either herself or her boss by proving $(G_1 \cong G_2) \vee (H_1 \cong H_2)$. At the end of the proof, the verifier will see a valid transcript of each proof – that is $(G_3, c, G_c \cong G_3)$ and $(H_3, c', H_{c'} \cong H_3)$. But the $c'$ challenge will be rigged so that Alice can answer it easily.

Cramer et al. [1994] implement this idea using a 2-of-2 secret sharing scheme. The verifier picks a challenge $c$ to be "shared", and requires the prover split the challenge into two shares, $c^\varphi$ and $c^\psi$ so that all of the shares are needed to reveal the "secret", $c$. Each share gives the challenge in the proof of each proposition. The requirement that the shares reveal $c$ imposes a one-degree-of-freedom constraint on the shares, leaving the prover to pick one and only one of the challenges. [1]

**Protocol 7** (Disjunctions)**.** *Proves:* $\varphi_1 \vee \varphi_2$ *using 3-step proofs for* $\varphi_1$ *and* $\varphi_2$.
*Common input:* $(x_1, x_2)$*, the common inputs to* $\varphi_1$ *and* $\varphi_2$.
*Prover's input: a witness of either assertion,* $w \in R_1(x_1) \cup R_2(x_2)$.

1. If $\varphi_1$ is true, then the prover randomly picks $m_1^1$ and generates a fake proof of $\varphi_2$ (using the simulator, which exists if $\varphi_2$ is honest verifier zero knowledge), consisting of $(m_2^1, c_2, m_2^2)$. We omit the symmetric case for $\varphi_2$.
2. The prover sends $(m_1^1, m_2^1)$ to the verifier.
3. The verifier sends the prover a random challenge $c$.
4. The prover has to pick $(c_1, c_2)$ and a polynomial $p(x) = p_0 + p_1 x$ such that $p(0) = c$, $p(1) = c_1$ and $p(2) = c_2$. If $\varphi_1$ is true, then the prover has already picked $c_2$, so the constraints imply $c_1 = c - c_2$. Then the prover computes $m_1^2$ honestly.

[1] In fact, their results are substantially more general. They generalize secret schemes, and generalize the duality between propositions and secret schemes, so that they can prove any monotonic proposition.

5. The prover sends $(p, c_1, c_2, m_1^2, m_2^2)$ to the verifier.

6. The verifier checks that $p(0) = c$, $p(1) = c_1$ and $p(2) = c_2$, and checks each proof $(m_i^1, c_i, m_i^2)$.

**Theorem 8.** *If the proofs of $\varphi_1$ and $\varphi_2$ are 3-step (honest-verifier) zero-knowledge, then Protocol 7 is a witness-indistinguishable proof of $\varphi_1 \vee \varphi_2$.*

# References


Ronald Cramer, Ivan Damgard, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Proceedings of CRYPTO '94*, pages 174–187. Springer-Verlag, 1994.

Oded Goldreich. *Foundations of Cryptography*, volume 1. Cambridge University Press, 2001.

Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.