Towards *Interactive Belief, Knowledge & Provability*: Possible Application to *Zero-Knowledge Proofs*

→ Ph.D. Thesis Chapter 5

*Simon Kramer*

December 18, 2007

**Target audience:** Cryptographers, Computer Scientists, Logicians, Philosophers
Overall Argument

1. Zero-Knowledge proofs have a natural (logical) formulation in terms of modal logic.
2. Modal operators of interactive belief, knowledge, and provability are definable as natural generalisations of their non-interactive counterparts.
Overview

1. Introduction
   i. Motivation
   ii. Goal
   iii. Prerequisites
      - individual knowledge
      - propositional Knowledge
      - spatial implication
      - evidence & Belief, proof & Provability
      - epistemic implication

2. Interactive individual knowledge, proof & Provability

3. Application to Zero-Knowledge proofs

4. Interactive evidence & Belief

5. Conclusion
Introduction
Motivation

How to redefine modern cryptography in terms of modal logic?
probabilistic polynomial-time Turing-machines

⇒ low-level & operational definitions (how)
⇒ mentally intractable proofs
⇒ Modern cryptography is cryptic.

How to generalise non-interactive modal concepts to the interactive setting? [van Benthem]

⇒ from monologue to dialogue
⇒ rational agency (game theory)
Introduction

Goal

To redefine modern cryptography in terms of modal logic

- high-level & declarative definitions (*what*)
- mentally tractable proofs
- Logical cryptology.

To define **interactive** belief, knowledge, and provability

- building blocks for rational agency
Introduction
Prerequisites (1/5)

**Individual knowledge (knowledge of messages):**
- name generation
- message reception
- message analysis
- message synthesis

**via message analysis**

\[
\text{Eve } k \{\mathcal{M}\}_k \xRightarrow{\text{Eve } k} k \\
\text{Eve } k \mathcal{M}
\]

**via message synthesis**

\[
\text{Eve } k \mathcal{M} \xRightarrow{\text{Eve } k} k \\
\text{Eve } k \{\mathcal{M}\}_k
\]
Propositional Knowledge (Knowledge of the truth of propositions) — almost:

\[ K \vdash K_b(\phi \rightarrow \phi') \rightarrow (K_b(\phi) \rightarrow K_b(\phi')) \]

\[ T \vdash K_b(\phi) \rightarrow \phi \]

\[ 4 \vdash K_b(\phi) \rightarrow K_b(K_b(\phi)) \]

\[ 5 \vdash \neg K_b(\phi) \rightarrow K_b(\neg K_b(\phi)) \]

\[ \frac{\vdash \phi}{\vdash K_b(\phi)} \]
Introduction
Prerequisites (3/5)

Spatial implication (assume — guarantee):

\[ \models \phi \triangleright \phi' \quad : \text{iff} \quad \text{for all extensions } \models \phi'' \text{ of } \models \phi \text{ by } \models \phi', \]

\[ \text{if } \models \phi \text{ then } \models \phi'' \models \phi' \]

\[ \langle \epsilon \cdot I(\text{Eve}, \{\| M \|_k\}, P) \models \text{Eve } k \ k \triangleright \text{Eve } k \ M \]

\[ \models \text{Eve } k \ M \triangleright \text{Eve } k \ M \quad \not\models \neg \text{Eve } k \ M \triangleright \neg \text{Eve } k \ M \]
Introduction
Prerequisites (4/5)

Provability (other than Artëmov’s) & proof:

\[ \mathsf{P}_b(\phi) := \exists m (m \text{ proofFor} \phi \land b k m) \]
\[ m \text{ proofFor} \phi := \forall (c : \mathsf{Adv}) (c k m \triangleright K_c(\phi)) \]

Belief and evidence:

\[ m \text{ evidenceFor} \phi := \forall (c : \mathsf{Adv}) (K_c(\phi) \triangleright c k m) \]
\[ \mathsf{B}_b(\phi) := \exists m (m \text{ evidenceFor} \phi \land b k m) \]

Theorem: \( \mathsf{P}_a \) is S4
Theorem: \( \mathsf{B}_a \) is KD4
**Introduction**

**Prerequisites (5/5)**

**Epistemic implication** *(if — then possibly because)*:

\[
\langle \epsilon \cdot I(Eve, \{|M|\}_k) \cdot I(Eve, k), P \rangle \models Eve_k M \supseteq Eve_k k
\]

**Derivation of individual knowledge**

\[
\begin{align*}
\epsilon \cdot I(Eve, \{|M|\}_k) \cdot I(Eve, k) & \vdash_{I(Eve,k)} I(Eve, \{|M|\}_k) \\
\epsilon \cdot I(Eve, \{|M|\}_k) \cdot I(Eve, k) & \vdash_{I(Eve,k)} \{M\}_k \\
\epsilon \cdot I(Eve, \{|M|\}_k) \cdot I(Eve, k) & \vdash_{I(Eve,k),I(Eve,\{|M|\}_k)} M
\end{align*}
\]
**Towards Interactive Belief, Knowledge & Provability**

**Interactive individual knowledge, proof & Provability**

\[ M' \supseteq_{(a,b)} M := b \land M' \land (b \land M' \supseteq a \land M) \]

**2-party interactive proof**

\[ M \text{ iProofFor}_{(a,b)} \phi := M \text{ iProofFor}^a_{(a,b)} \phi \]

\[ (M, \square) \text{ iProofFor}^c_{(a,b)} \phi := \exists M (M \land M \text{ proofFor} \phi) \]

\[ (M, (M', I)) \text{ iProofFor}^c_{(a,b)} \phi := M' \supseteq_{(a,b)} M \land (M', I) \text{ iProofFor}^c_{(b,a)} \phi \]
Possible Application to Zero-Knowledge Proofs (1/3)

2-party Interactive Provability

\[ \text{IP}_{(a,b)}(\phi) := \exists m (m \text{ iProofFor}_{(a,b)} \phi) \]

Zero-Knowledge proofs (definition)

"Zero-knowledge proofs are defined as those [interactive] proofs that convey no additional knowledge other than the correctness of the proposition [\(\phi\)] in question." [GMR89]

\[ \text{ZK}_{(a,b)}(\phi) := \text{IP}_{(a,b)}(K_a(\exists m'(K_b(m' \text{ proofFor } \phi))) \land \neg \exists m''(K_a(K_b(m'' \text{ evidenceFor } \phi)))) \]
Spelled out, \( a \) (the verifier) knows through interaction with \( b \) (the prover) that \( b \) knows a proof (\( m' \)) for the proposition \( \phi \), however \( a \) does not know that proof nor any evidence (\( m'' \)) that could corroborate the truth of \( \phi \). (Observe the importance of the scope of the existential quantifiers.) Philosophically speaking, \( a \) has pure propositional knowledge of \( \phi \), i.e., \( a \) has zero individual (and thus zero intuitionistic—no witness!) knowledge relevant to the truth of \( \phi \). In Goldreich’s words, it is “as if [the verifier] was told by a trusted party that the assertion holds” [Gol05, Page 39].
Possible Application to Zero-Knowledge Proofs (3/3)

Zero-Knowledge proofs (conjecture)

“[A]nything that is feasibly computable from a zero-knowledge proof is also feasibly computable from the (valid) assertion itself.” [Gol05, Page 39]

\[ \vdash \phi \rightarrow ((K_a(\varphi) \supseteq ZK_{(a,b)}(\phi)) \rightarrow (K_a(\varphi) \supseteq \phi)) \]
**Towards Interactive Belief, Knowledge & Provability**

**Interactive evidence & Belief**

2-party *interactive* evidence

\[
M \text{iEvidenceFor}_{(a,b)}(\phi) := M \text{iEvidenceFor}_{(a,b)}^a(\phi) \\
(M, \Box) \text{iEvidenceFor}_{(a,b)}^c(\phi) := c \land M \land M \text{ evidenceFor }\phi \\
(M, (M', I)) \text{iEvidenceFor}_{(a,b)}^c(\phi) := M' \supseteq_{(a,b)} M \land (M', I) \text{iEvidenceFor}_{(b,a)}^c(\phi)
\]

2-party *interactive* Belief

\[
\text{IB}_{(a,b)}(\phi) := \exists m (m \text{iEvidenceFor}_{(a,b)}(\phi))
\]
Conclusion

1. Modern cryptography is cryptic due to its machine-based definitions.
2. This deep-rooted problem must be administered a radical remedy: redefinition.
3. Modal logic is a good candidate remedy.