The Hunting of the SNARK

Nir Bitansky

Ran Canetti

Alessandro Chiesa

Eran Tromer

Succint Noninteractive Argument of Knowledge

Kilian '92

Micali '00

Aiello Bhatt Ostrovsky Rajagopalan '00

Dwork Langberg Naor Nissim Reingold '04

Di Crescenzo Lipmaa '08

Mie '08

Gentry Wichs '11

Carroll '76

Verifier generates and publishes a reference string

Prover picks NP statement "exists w such that $M(x,w)=1$" and sends M,x, and a succint proof

Verifier efficiently checks proof and is convinced that prover knows a witness w.

Session 3 — Outsourcing and Delegating Computation

(Session Chair: Tal Moran)

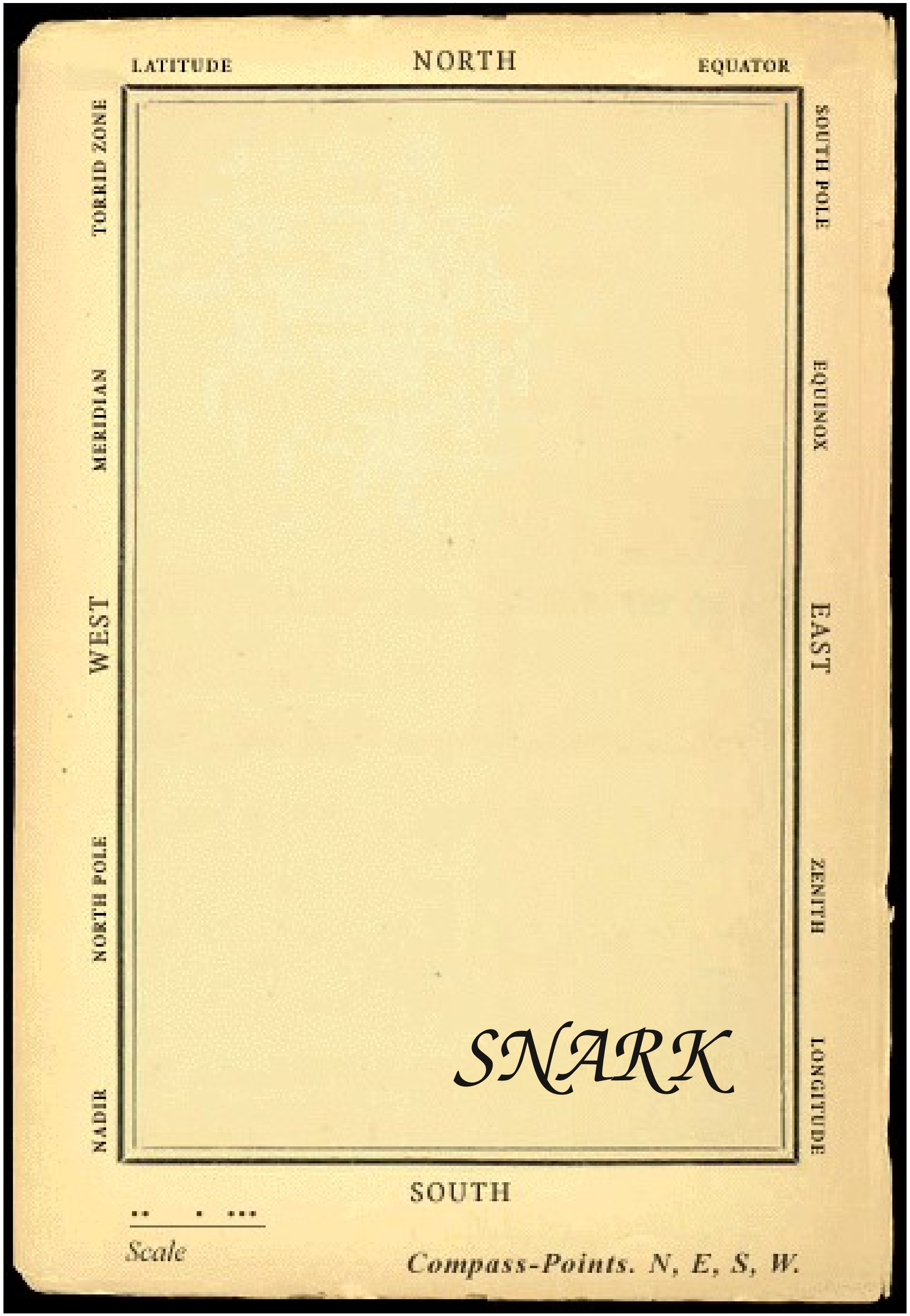
- ✓ 14:00 - 14:20: **Optimal Verification of Operations on Dynamic Sets**
  **Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos*
- ✓ 14:20 - 14:40: **Verifiable Delegation of Computation over Large Datasets**
  *Siavosh Benabbas, Rosario Gennaro, and *Yevgeniy Vahlis*
- 14:40 - 15:00: **Secure Computation on the Web: Computing Without Simultaneous Interaction**
  *Shai Halevi, *Yehuda Lindell, and Benny Pinkas*
- ✓ 15:00 - 15:20: **Memory Delegation**
  **Kai-Min Chung, Yael Tauman Kalai, Feng-Hao Liu, and Ran Raz*

Coffee Break

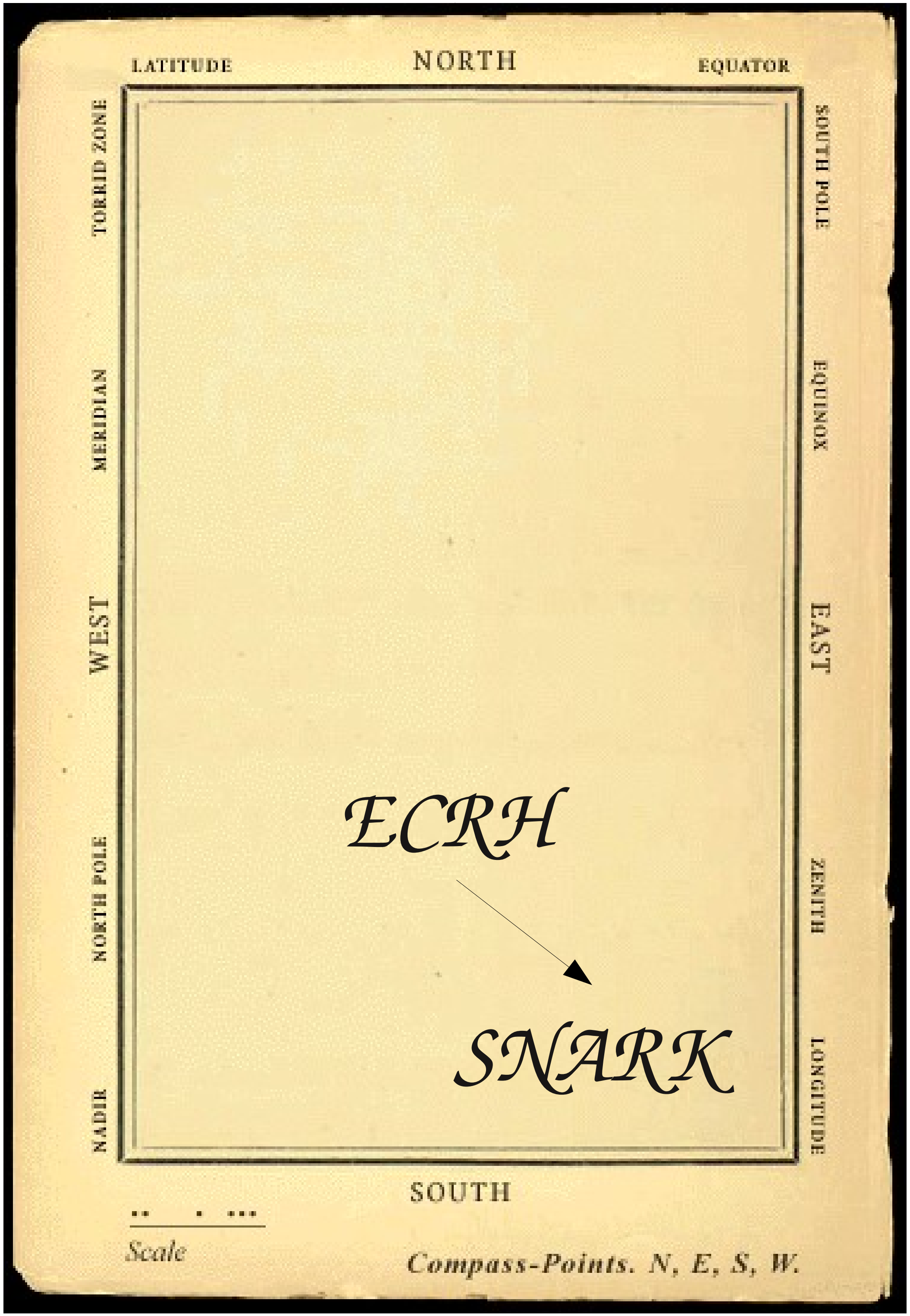
Session 4 — Symmetric Cryptanalysis and Constructions

(Session Chair: Orr Dunkelman)

- 15:50 - 16:10: **Automatic Search of Attacks on Round-Reduced AES and Applications**
  *Charles Bouillaguet, *Patrick Derbez, and Pierre-Alain Fouqu*
- 16:10 - 16:30:

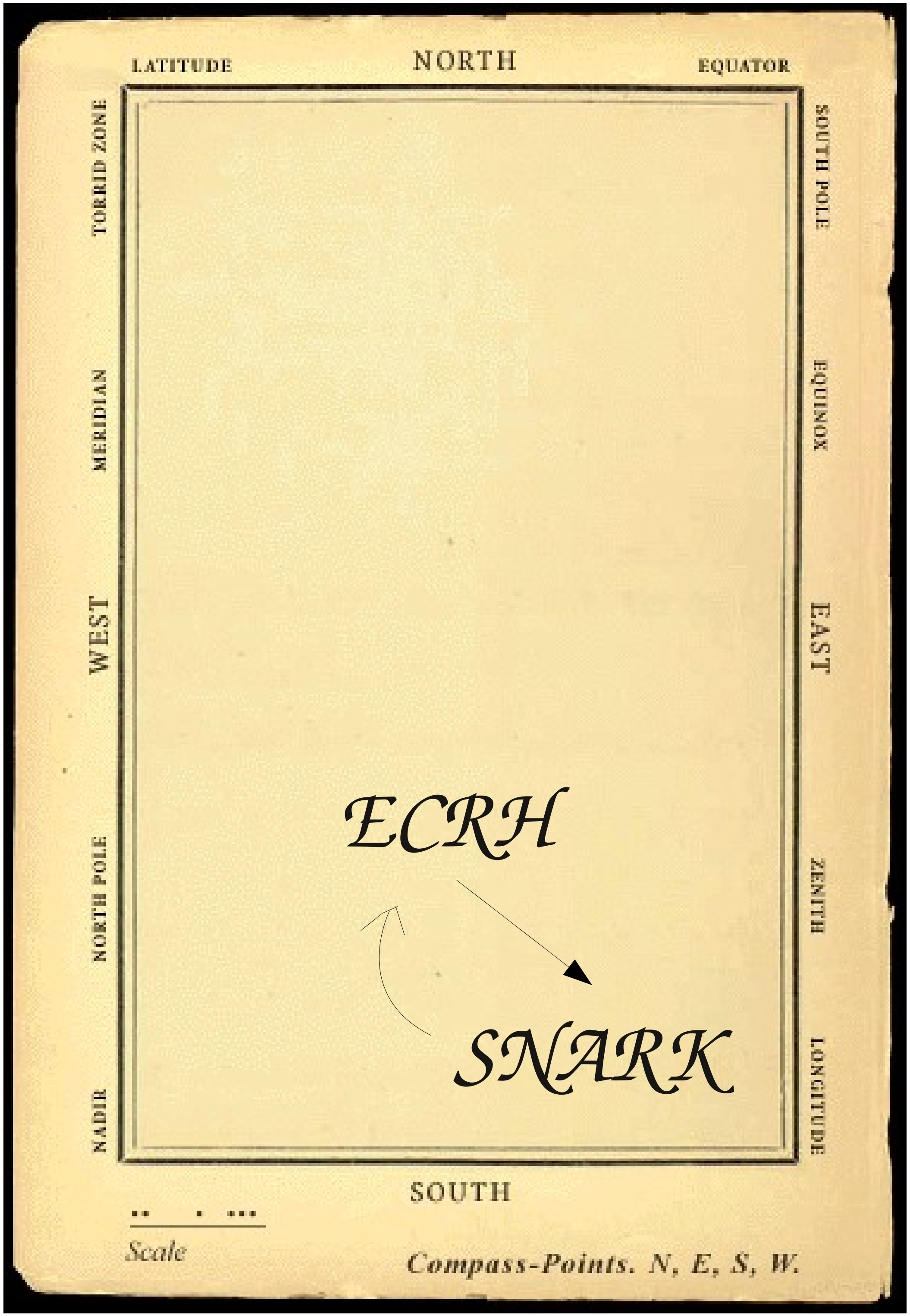

LATITUDE
NORTH
EQUATOR
TORRID ZONE
MERIDIAN
WEST
NORTH POLE
NADIR
SOUTH POLE
EQUINOX
EAST
ZENITH
LONGITUDE
SOUTH
Scale
Compass-Points. N, E, S, W.

SNARK


LATITUDE
NORTH
EQUATOR
TORRID ZONE
MERIDIAN
WEST
NORTH POLE
NADIR
SOUTH POLE
EQUINOX
EAST
ZENITH
LONGITUDE
SOUTH
Scale
Compass-Points. N, E, S, W.

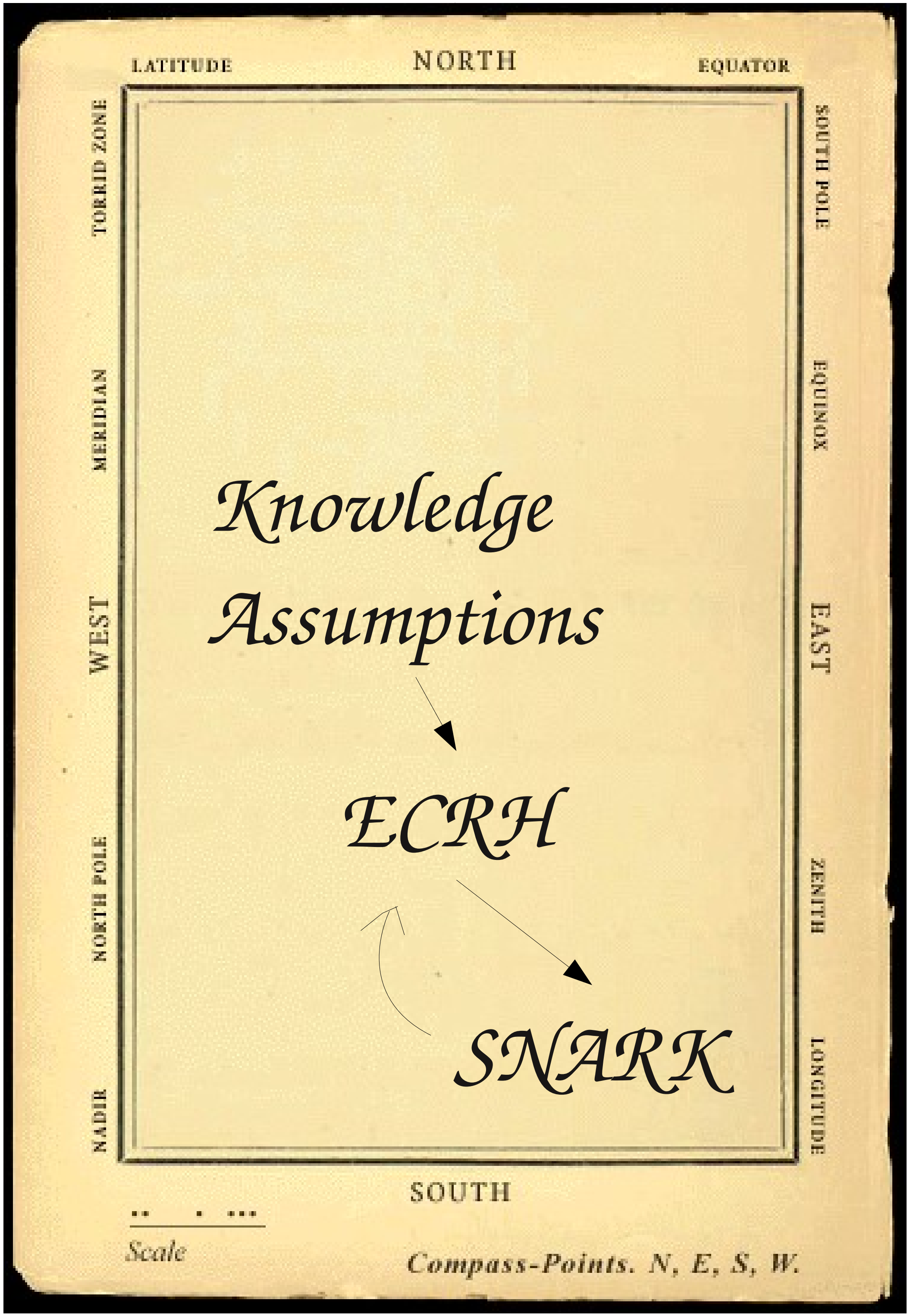
ECRH

SNARK


LATITUDE
NORTH
EQUATOR
TORRID ZONE
MERIDIAN
WEST
NORTH POLE
NADIR
SOUTH POLE
EQUINOX
EAST
ZENITH
LONGITUDE
SOUTH
Scale
Compass-Points. N, E, S, W.

ECRH

SNARK

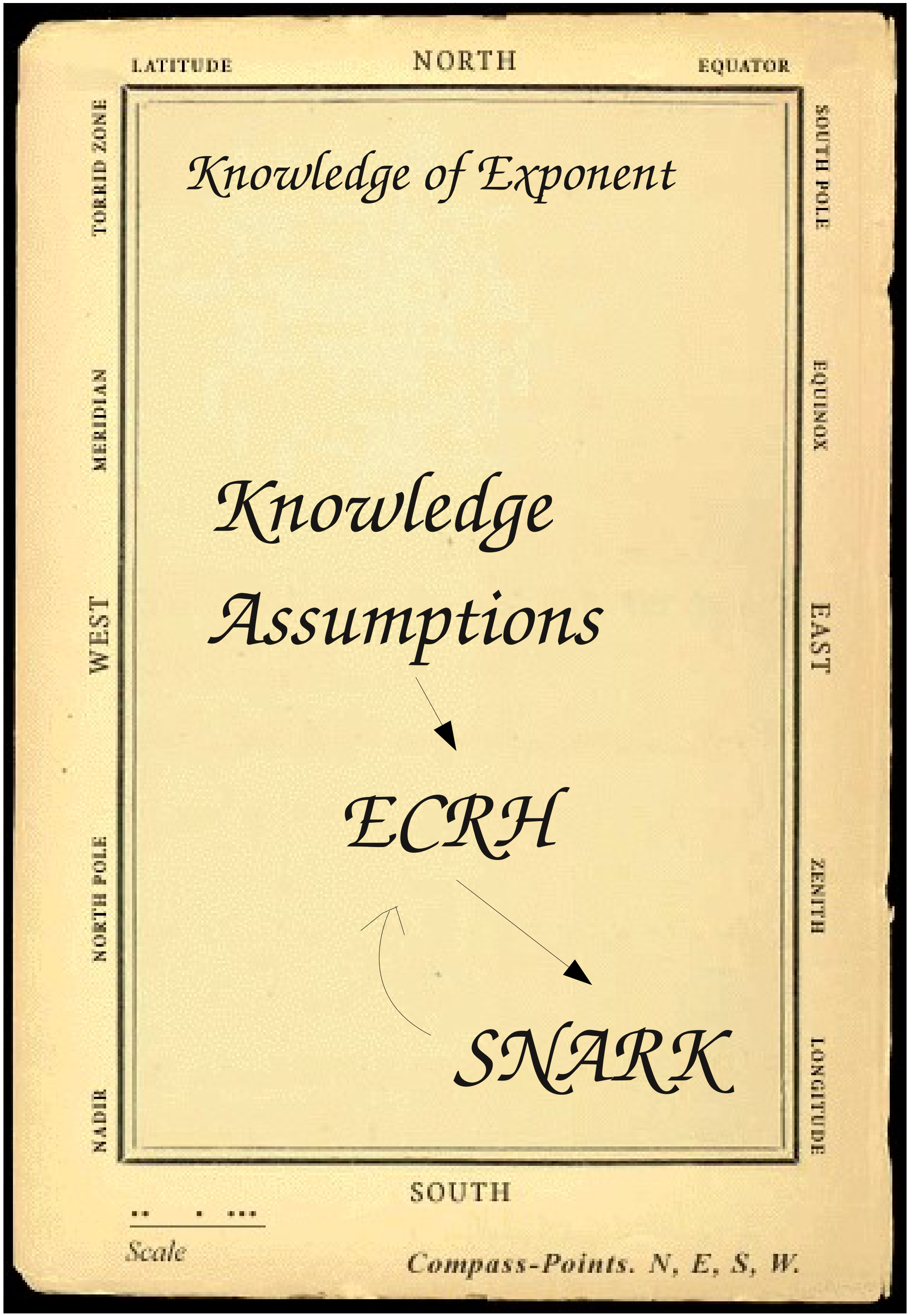


Knowledge Assumptions

ECRH

SNARK

Knowledge of Exponent

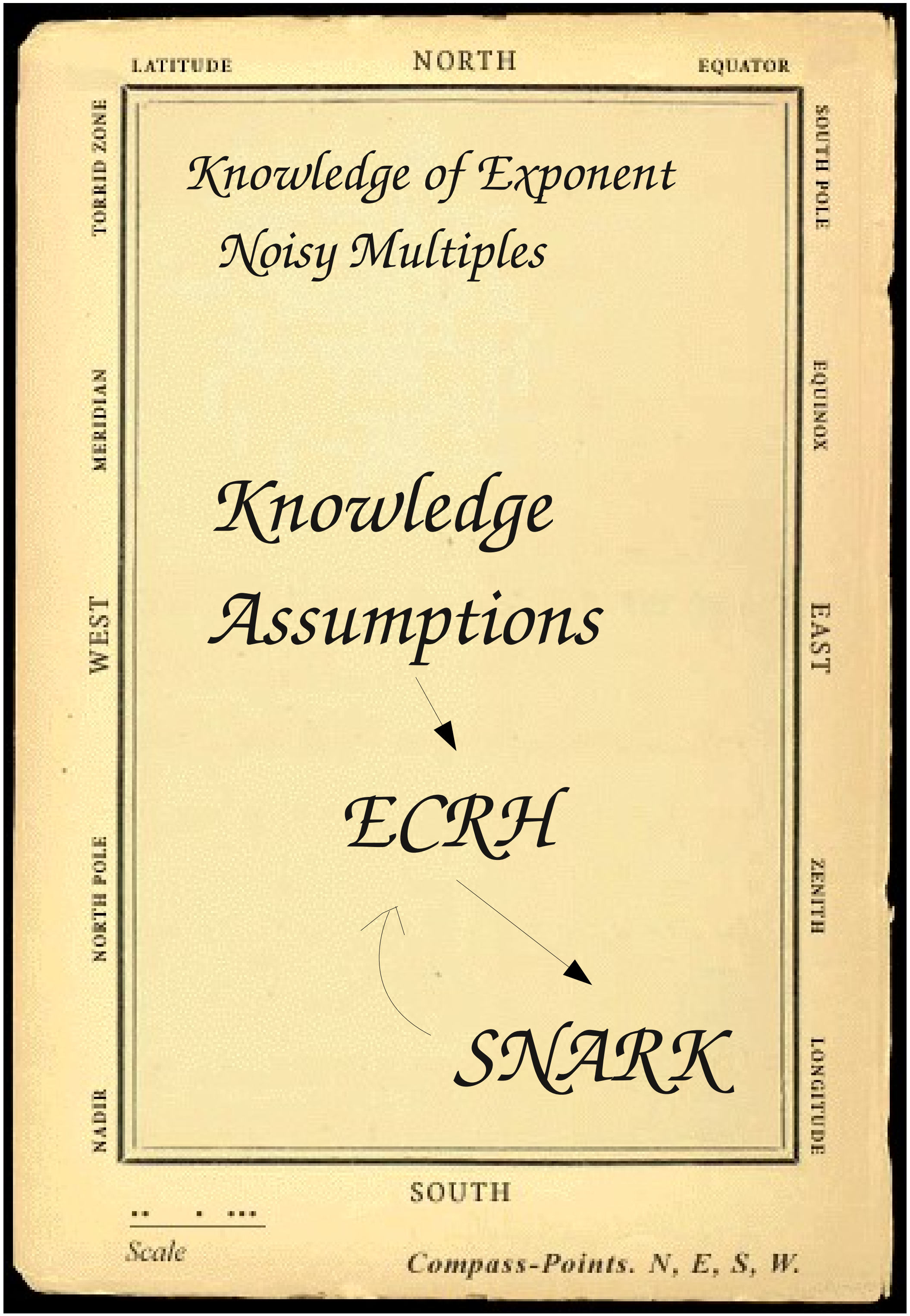


Knowledge Assumptions

ECRH

SNARK

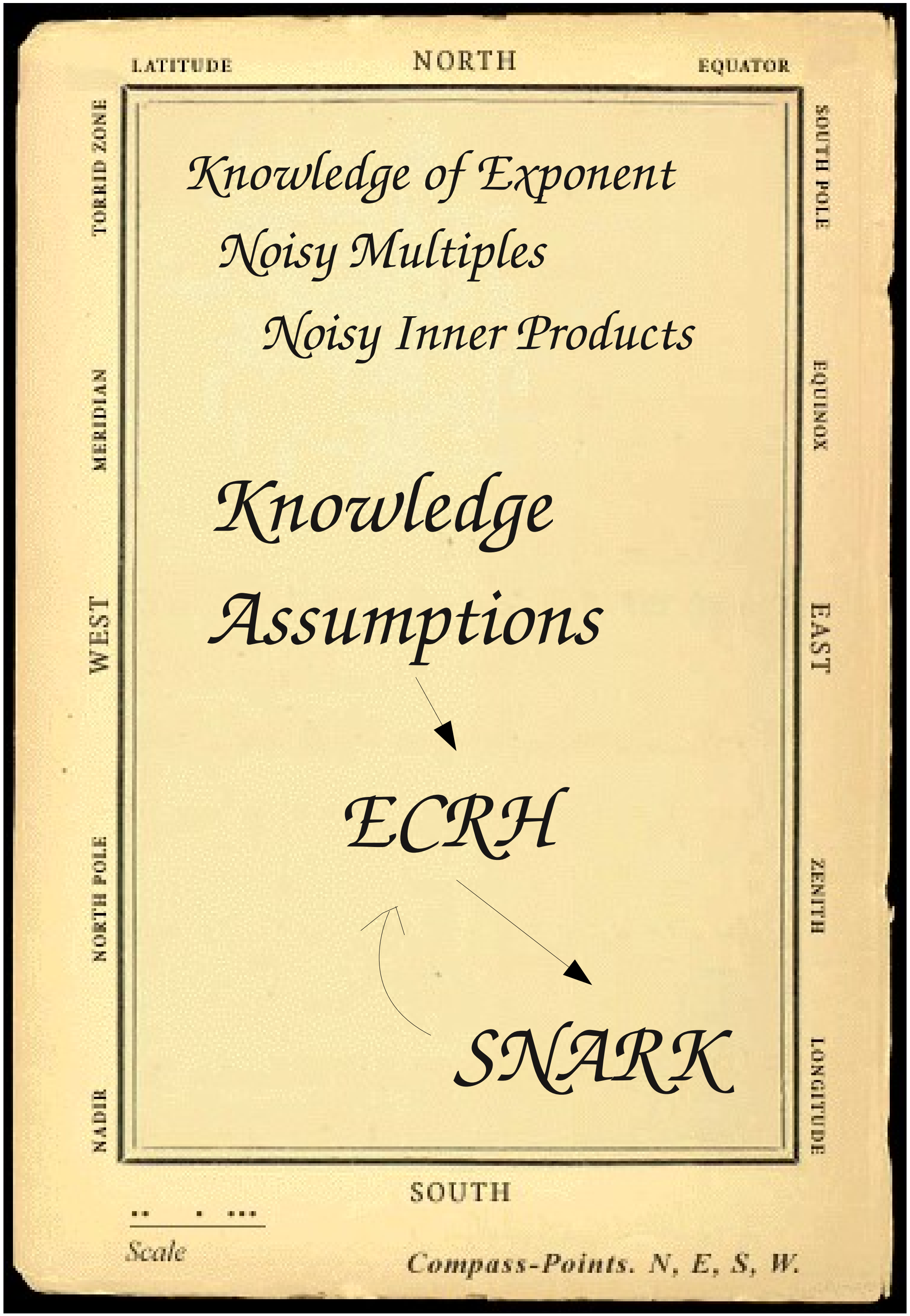
Knowledge of Exponent Noisy Multiples



Knowledge Assumptions

ECRH

SNARK



Knowledge of Exponent

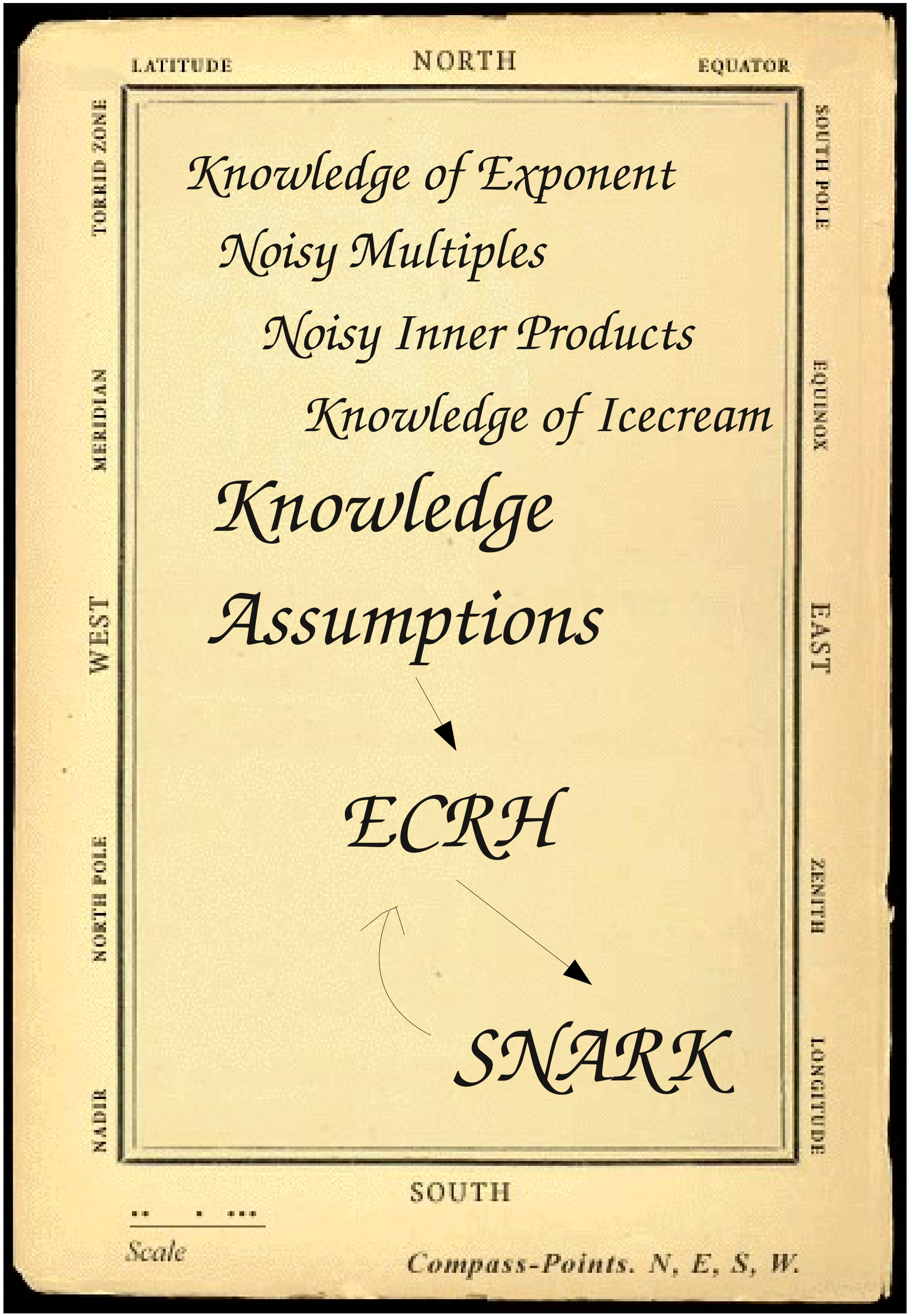
Noisy Multiples

Noisy Inner Products

Knowledge Assumptions

ECRH

SNARK



Knowledge of Exponent

Noisy Multiples

Noisy Inner Products

Knowledge of Icecream

Knowledge

Assumptions

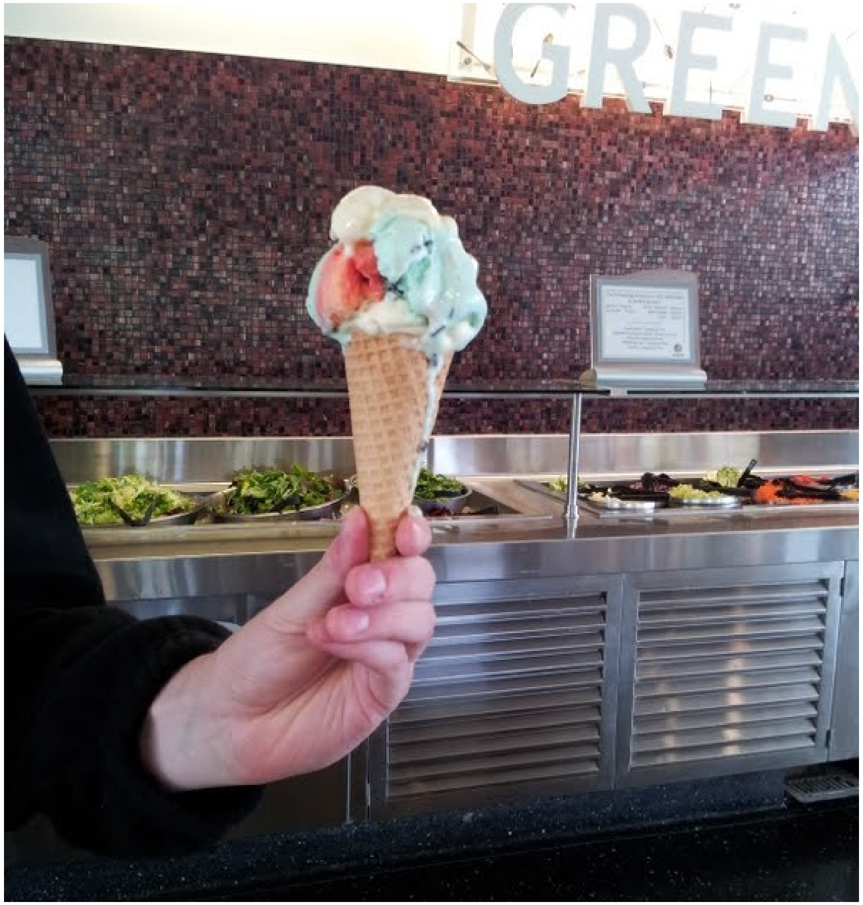
ECRH

SNARK

Knowledge of Icecream Assumption

$\forall$ poly-size adversary $\mathcal{A}$
$\exists$ a poly-size extractor $\mathcal{E}_{\mathcal{A}}^{\mathcal{H}}$

$$\Pr_{h \leftarrow \mathcal{H}_k}\left[\begin{array}{c} y \leftarrow \mathcal{A}(h) \\ \exists x : h(x) = y \end{array} \wedge \begin{array}{c} x' \leftarrow \mathcal{E}_{\mathcal{A}}^{\mathcal{H}}(h) \\ h(x') \neq y \end{array}\right] \leq \mathrm{negl}(k)$$



The method employed I would gladly define,
While I have it so clear in my head,
If I had but the slides and you had but the time —
But much yet remains to be said.

http://eprint.iacr.org/2011/443