

Protocollen en Compositie

Pieter Rogaar
19 maart 2008



Introductie

- Definities
 - Protocol, adversary, veiligheidsparameter, omgeving, emulatie
- Compositiestelling en bewijs
- Alternatief raamwerk

Definitie: Protocol

- Doel bereiken
- ‘Zwarte doos’-functionaliteit
- Communicatie
- Notatie: π , ρ , φ

Definitie: Adversary

- Modelleert niet-ideale omgeving
- Buitenstaander
- Corrumpeert partijen, veel mogelijkheden
- Faciliteert communicatie tussen tegenstanders
- Notatie: A, S

Definitie:

Veiligheidsparameter

- Niet alles is perfect mogelijk of wenselijk
- Computacionele zekerheid
- Probabilistic Polynomial time Turing machine (PPT)
- Geeft mogelijkheid tot grotere veiligheid
- Notatie: k

Definitie: Omgeving

- Wat er met het protocol gebeurt
- Modelleert partijen en adversary
- Vaak: groter protocol waarin dit protocol opereert
- ‘Alle omgevingen’ \Rightarrow ‘alle omgevende protocollen’
- Notatie: Z

Definitie: Emulatie

- Ideaal protocol φ - zwarte doos
- Reële implementatie ρ van ideaal protocol
- Protocollen vergelijken - $(\forall A) (\exists S) (\forall Z)$
 - $\text{Exec}(\rho, A, Z) \approx \text{Exec}(\varphi, S, Z)$
- Volgorde van kwantoren

Compositiestelling

- Protocol ρ emuleert protocol φ
 - Zelfde zwakten
- Dan emuleert π^ρ het protocol π^φ
- Eén instantie - meerdere instanties

Bewijs: één instantie

- Dummy adversary is moeilijkst
- Haal grote protocol binnen omgeving
- Laat kleine protocol erbuiten

Foutieve intuïtie meerderere instanties

- Herhaaldelijk toepassen bewijs voor één instantie
- Probleem: Complexiteit kan opblazen

Bewijsschets (1/3)

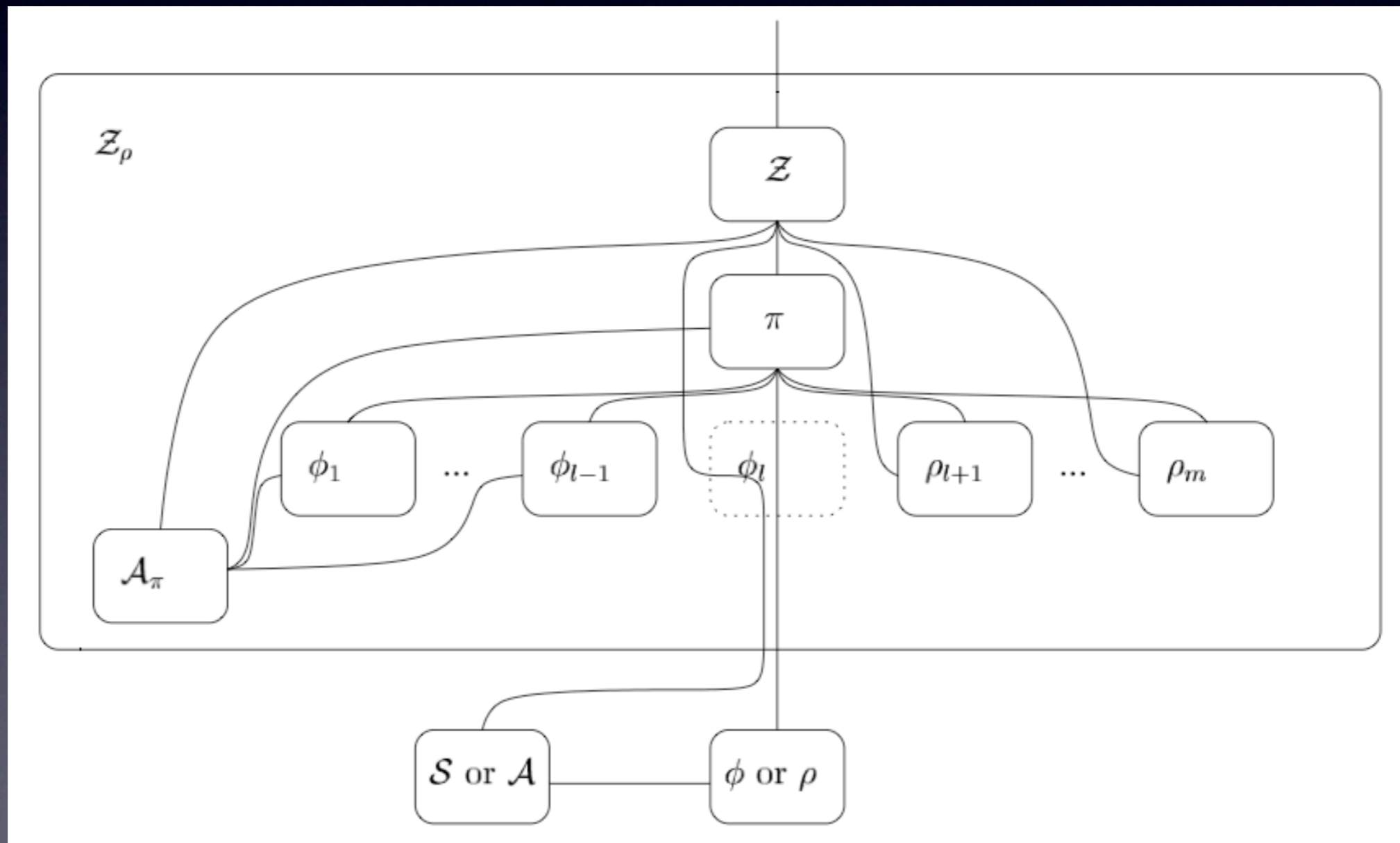
- We nemen aan: ρ emuleert protocol φ
- Construeer S tegen dummy adversary
- Maak adversary A_π tegen π^φ

Bewijsschets (2/3)

- Hybride tussenprotocollen construeren
- $\pi_m = \pi^\varphi$ en $\pi_0 = \pi^\rho$
- Stel er is een omgeving die onderscheid maakt
- Dan is er een overgang waarin dat tot uitdrukking komt

Bewijsschets (3/3)

- Haal dit protocol er buiten:



Alternatief: Indifferentiability

- Soortgelijk raamwerk
- Zwakkere notie van emulatie
- = meer protocollen voldoen
- Alleen compositie met één instantie

Indifferentiability: Tekortkomingen

- Volgorde van kwantoren in definitie omwisselen
- Dummy adversary toevoegen

Doelstelling

- Begrijpen en beschrijven van bewijs van Universal Composability
- Construeren van missende onderdelen in Indifferentiability
- Herschrijven van bewijs in Indifferentiability

Bibliografie en vragen

- Ran Canetti: Universally Composable Security: A new paradigm for cryptographic protocols (2005)
- Ueli Maurer, Renato Renner & Clemens Holenstein: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology (2004)
- Vragen?