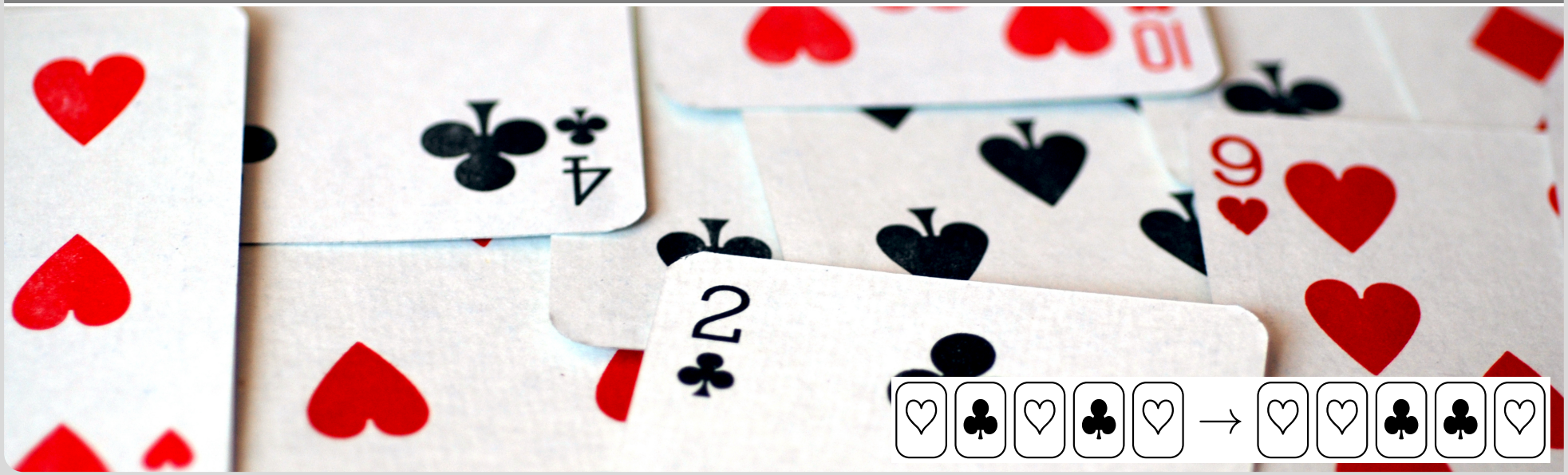
Karlsruher Institut für Technologie

Deck- und kartenminimale spielkartenbasierte sichere Mehrparteienberechnung

Praxis der Forschung WiSe 2017/18 | Alexander Koch

FAKULTÄT FÜR INFORMATIK, INSTITUT FÜR THEORETISCHE INFORMATIK



Probleme beim Fernsehabend

Grafik/Gestaltung von Stefan Walzer

Erster Versuch: Software-Krypto-Protokolle

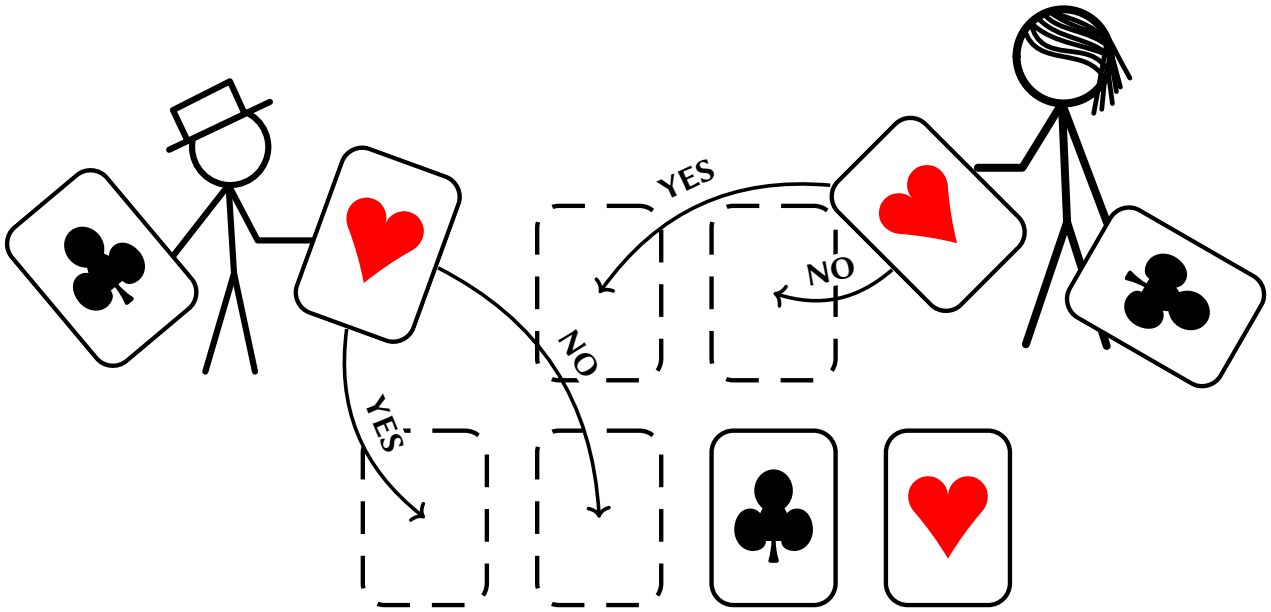
Erster Versuch: Software-Krypto-Protokolle

Erster Versuch: Software-Krypto-Protokolle

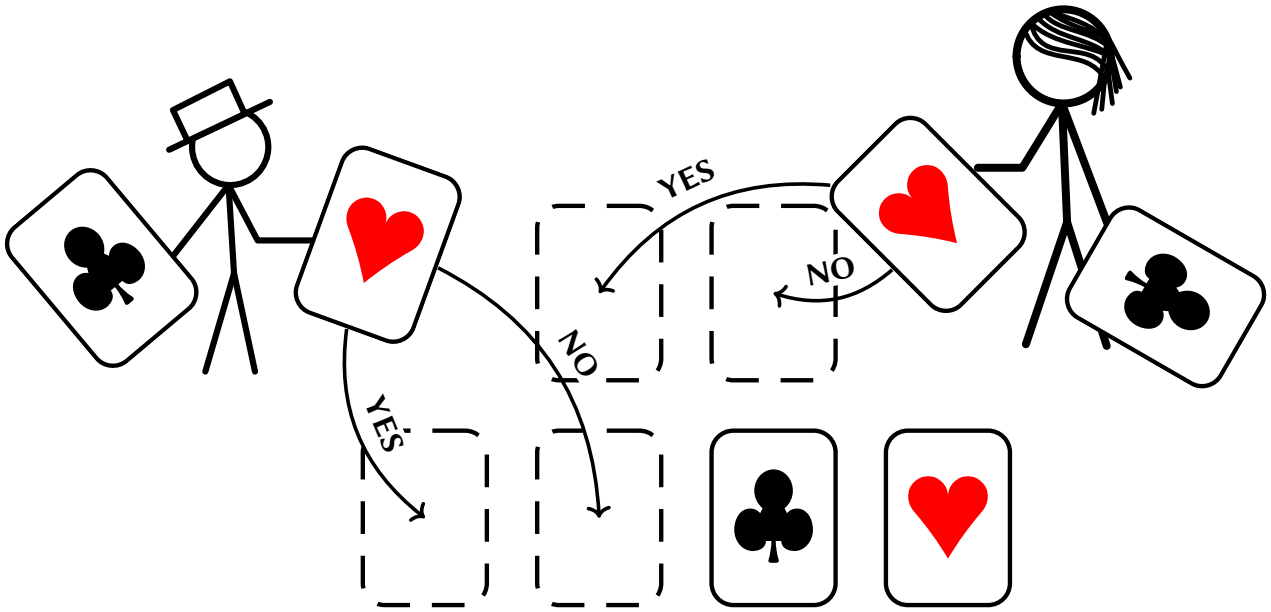
Erster Versuch: Software-Krypto-Protokolle

Erster Versuch: Software-Krypto-Protokolle

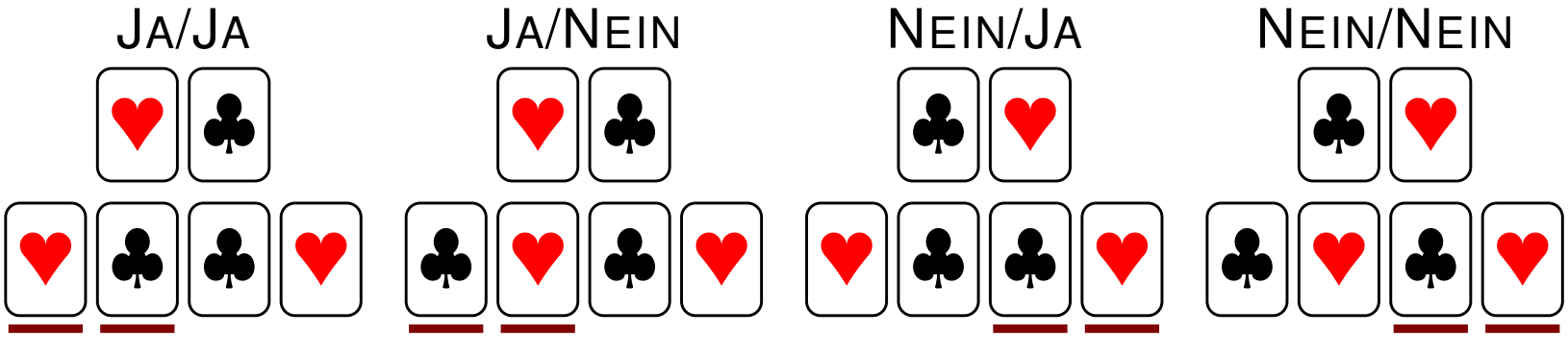
UND berechnen mit 6 Karten [MS09]



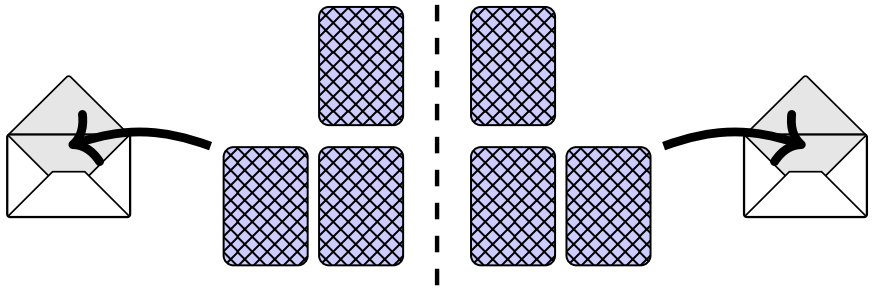
UND berechnen mit 6 Karten [MS09]



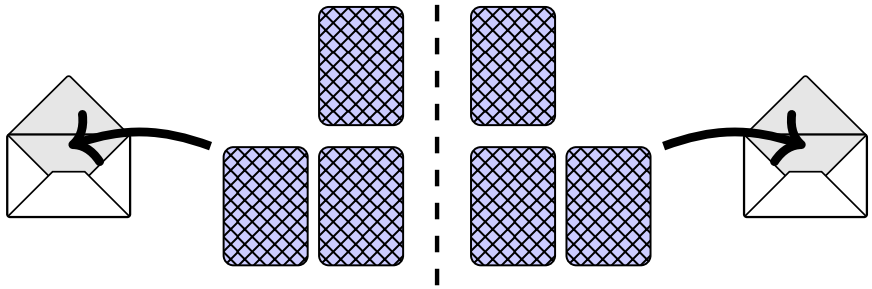
Konfigurationen:

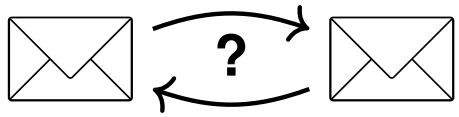


UND berechnen mit 6 Karten [MS09]

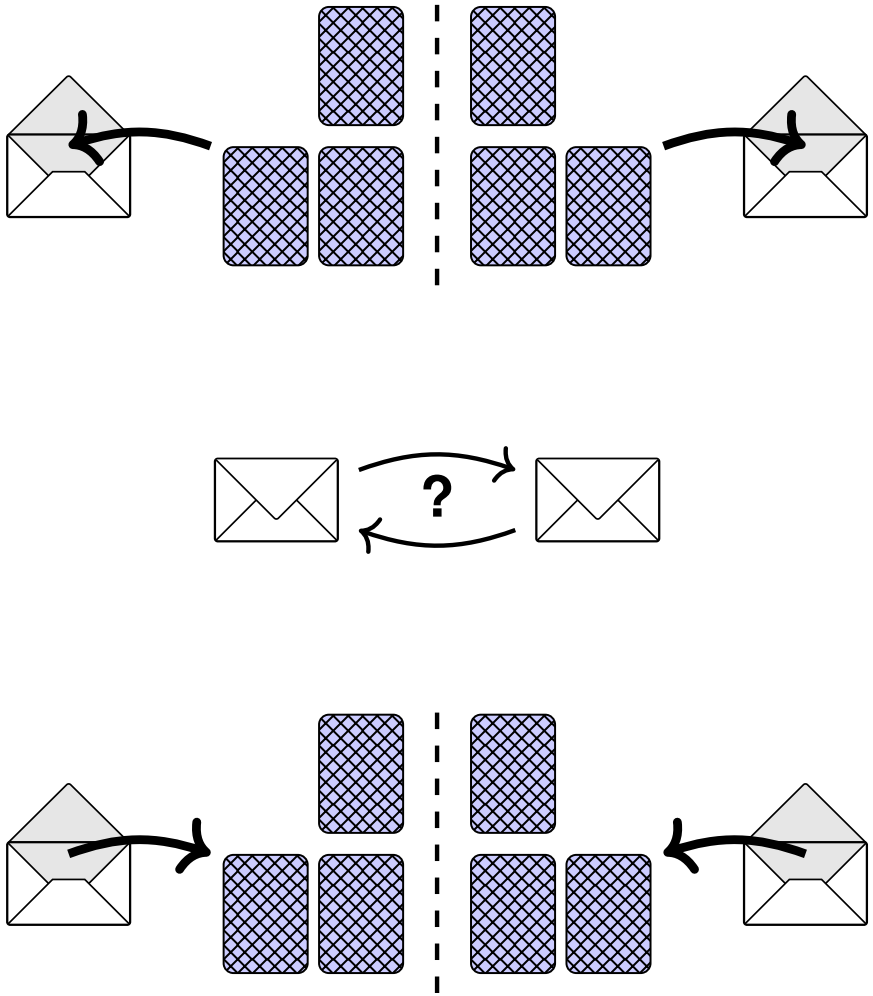


UND berechnen mit 6 Karten [MS09]

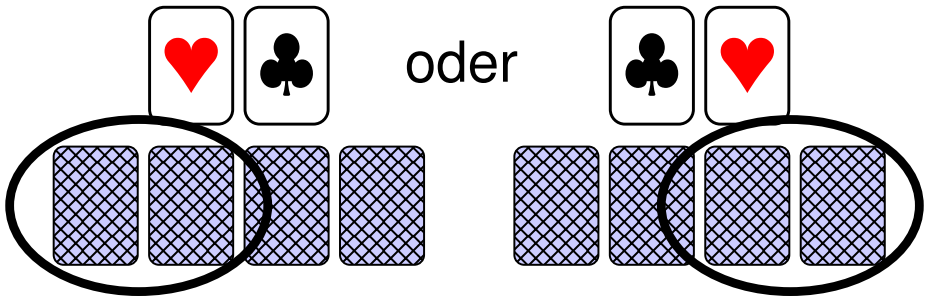




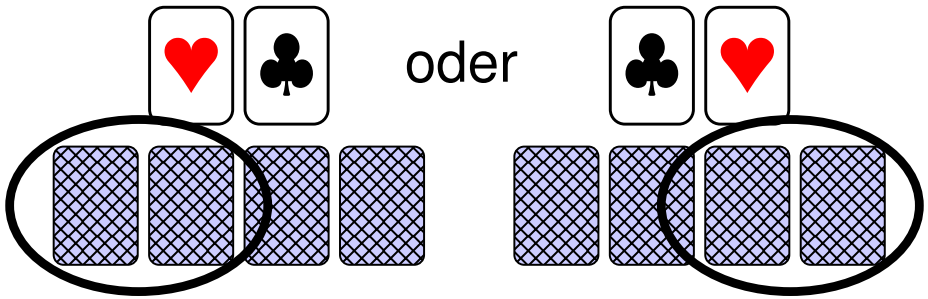
UND berechnen mit 6 Karten [MS09]



UND berechnen mit 6 Karten [MS09]



UND berechnen mit 6 Karten [MS09]



Forschungsfrage:
Wieviele Karten braucht man für ein UND-Protokoll, wenn alle Karten unterscheidbar sind? (Normales Spielkarten-Deck)

Bei guten Teamplayern: Ein Team mit bis zu drei Studierenden möglich

Nützlich: Gruppentheorie-Grundkenntnisse (Gruppenaktionen, Orbits)