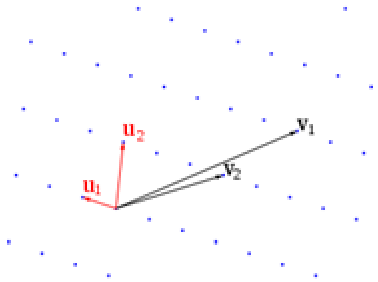
Random Oracles in a Quantum World

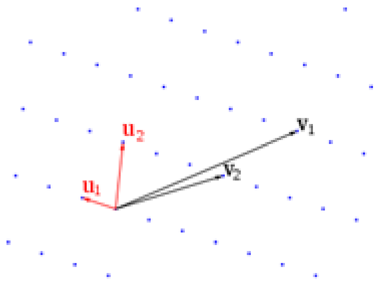
Crypto 2010 – Rump Session

Özgür Dagdelen (TU Darmstadt)
Marc Fischlin (TU Darmstadt)
Anja Lehmann (IBM Zurich)
Christian Schaffner (CWI)

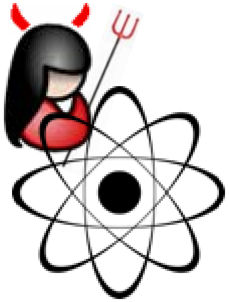
Quantum-Resistant Primitives



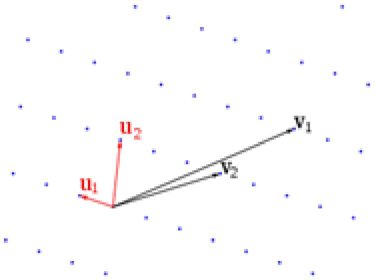
Quantum-Resistant Primitives



quantum-resistant
primitive/protocol

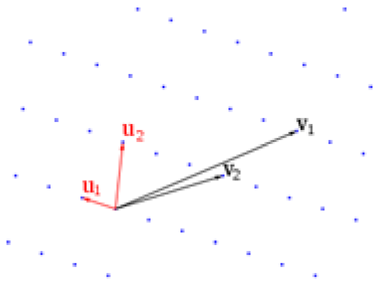


Quantum-Resistant Primitives



quantum-resistant
primitive/protocol

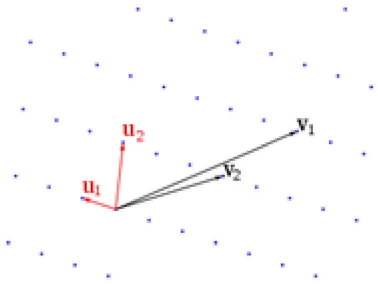
▶ Quantum-Resistant Primitives…with ROs?



quantum-resistant
primitive/protocol

random oracle

Quantum-Resistant Primitives…with ROs?



quantum-resistant
primitive/protocol

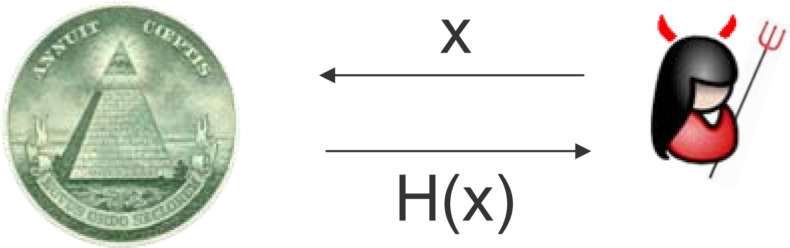
+

random oracle

=

???

▶ Quantum-Accessible Random Oracles

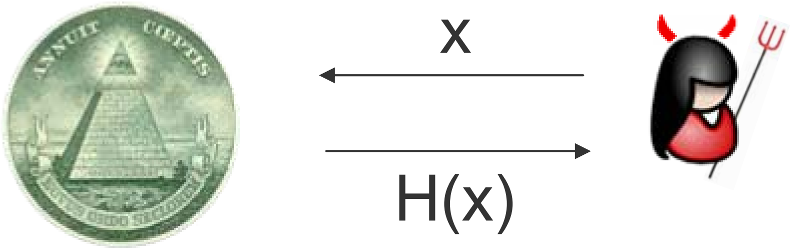


later replace Random Oracle by “strong implementation”

classical

quantum

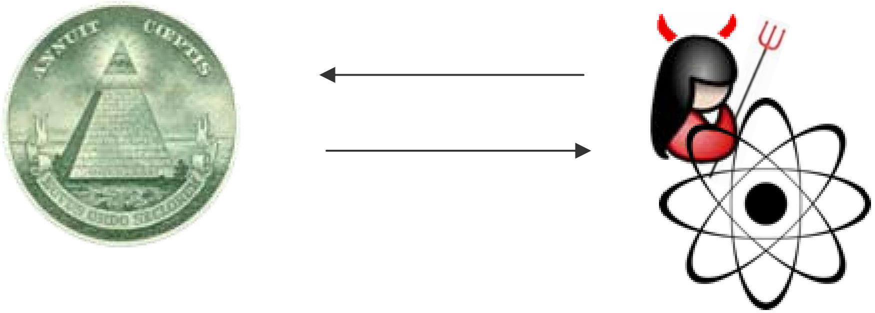
Quantum-Accessible Random Oracles



later replace Random Oracle by “strong implementation”

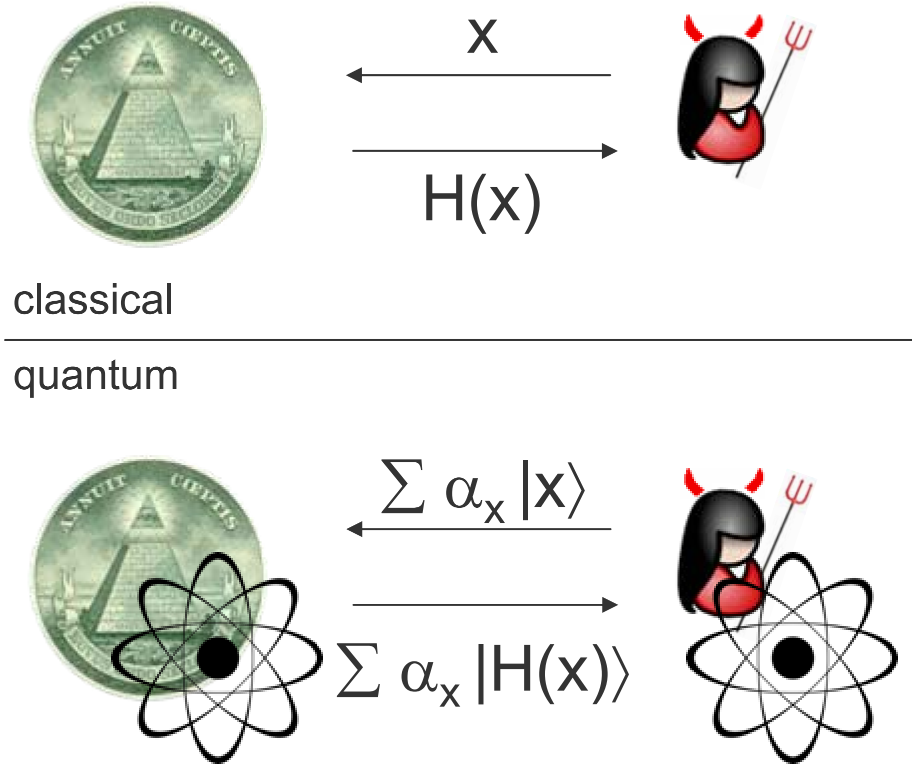
classical

quantum



<span>minimal</span> requirement: quantum-adversary may query RO about quantum states

▶ Quantum-Accessible Random Oracles



x

H(x)

classical

quantum

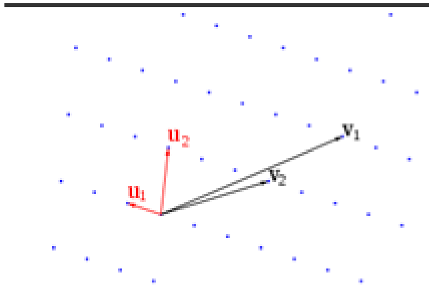
$\sum \alpha_x |x\rangle$

$\sum \alpha_x |H(x)\rangle$

later replace Random Oracle by “strong implementation”

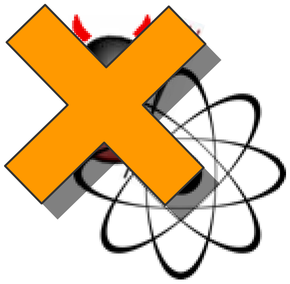
minimal requirement: quantum-adversary may query RO about quantum states

Do Results Carry over?

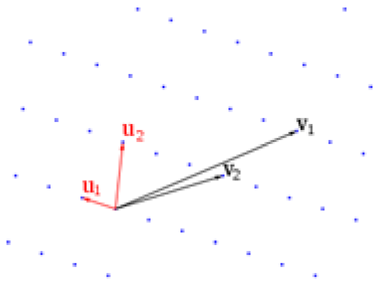


+

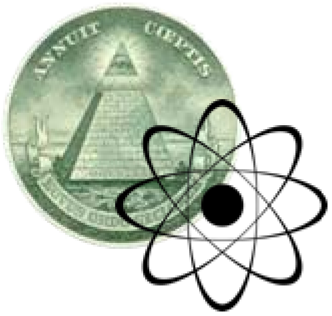
=



vs

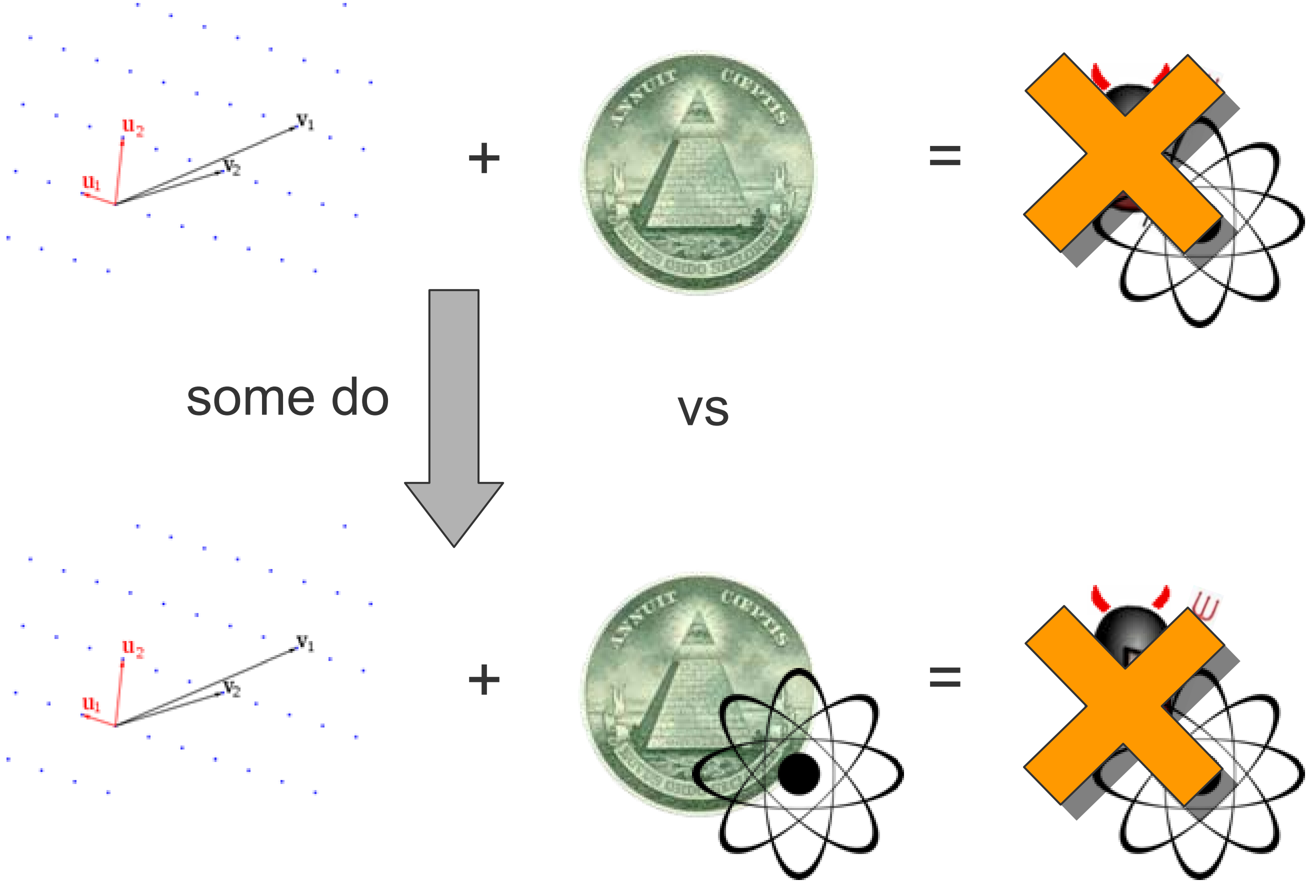


+



=

Do Results Carry over?



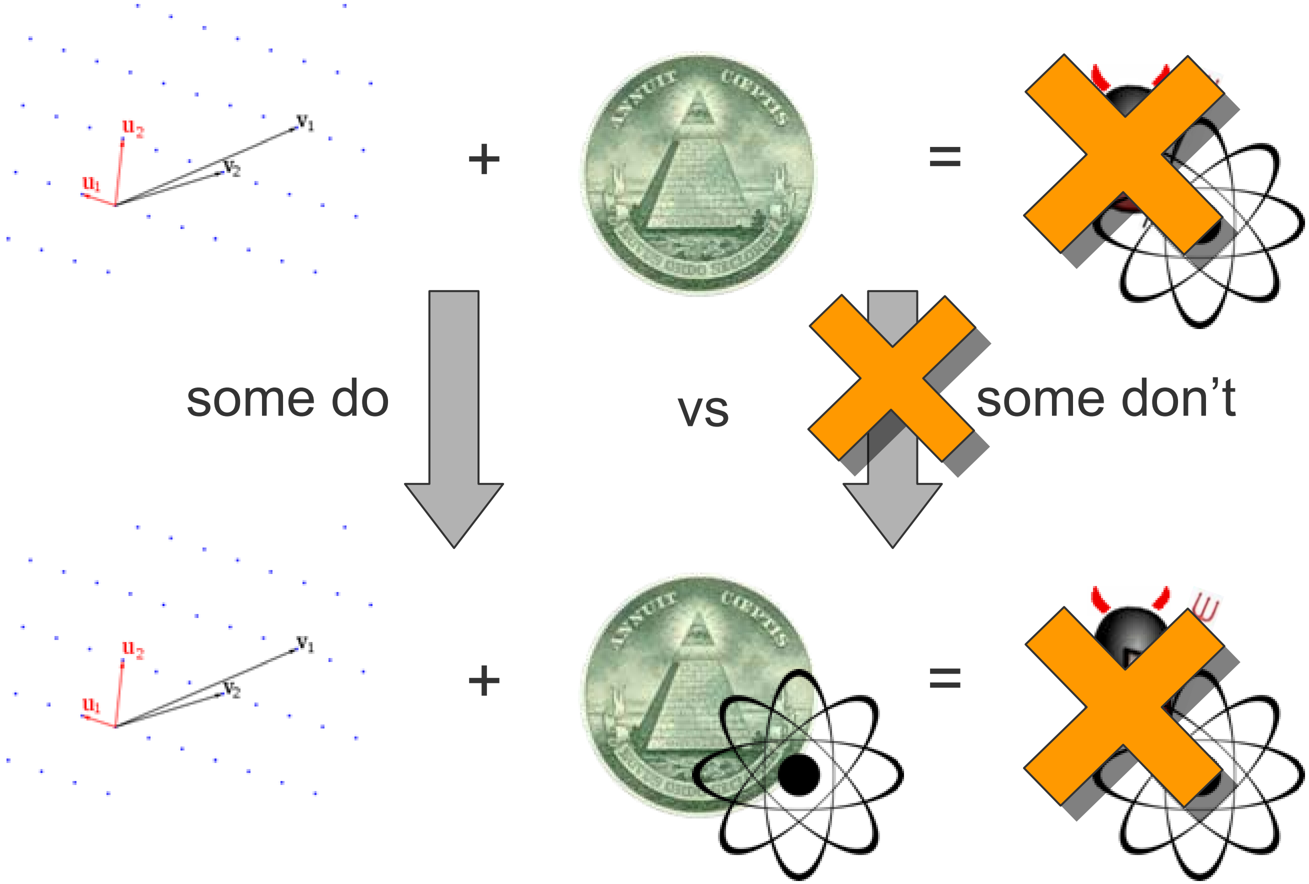
+ =

some do

vs

+ =

Do Results Carry over?



+ =

some do

vs

some don't

+ =

▶ What if I want to know more?

Random Oracles in a Quantum World

Ö.Dagdelen, M.Fischlin, A.Lehmann, C.Schaffner

eprint 2010/428