Crypto Circus

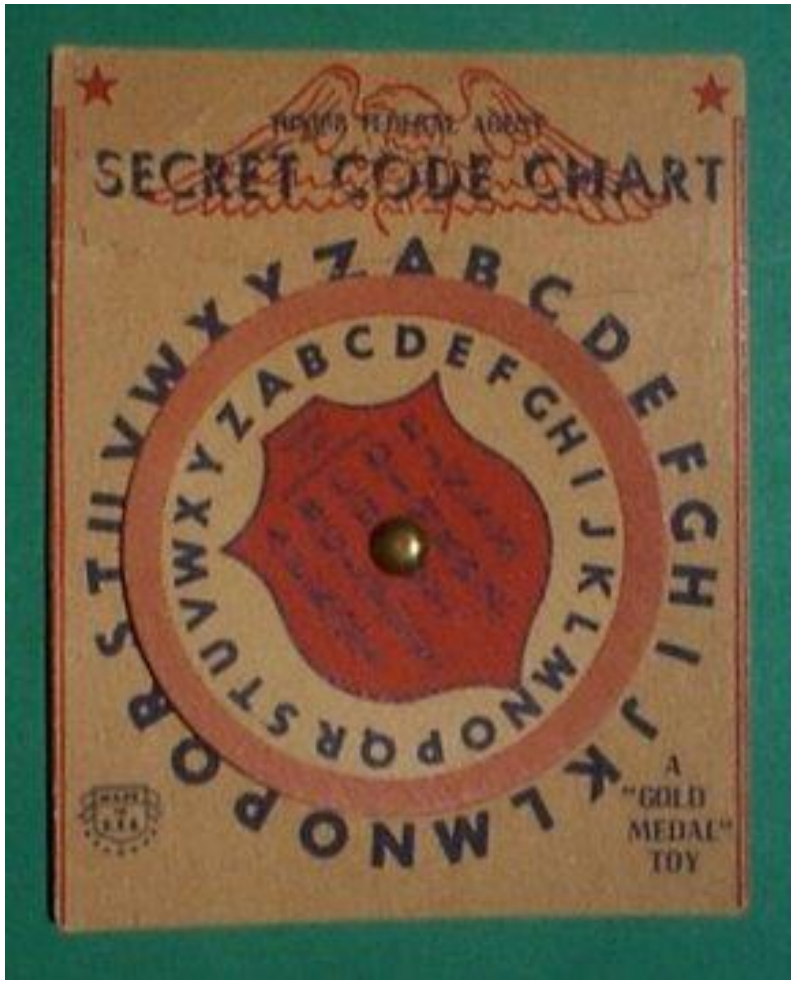
Berry Schoenmakers
Faculteit Wiskunde & Informatica
Coding & Crypto groep

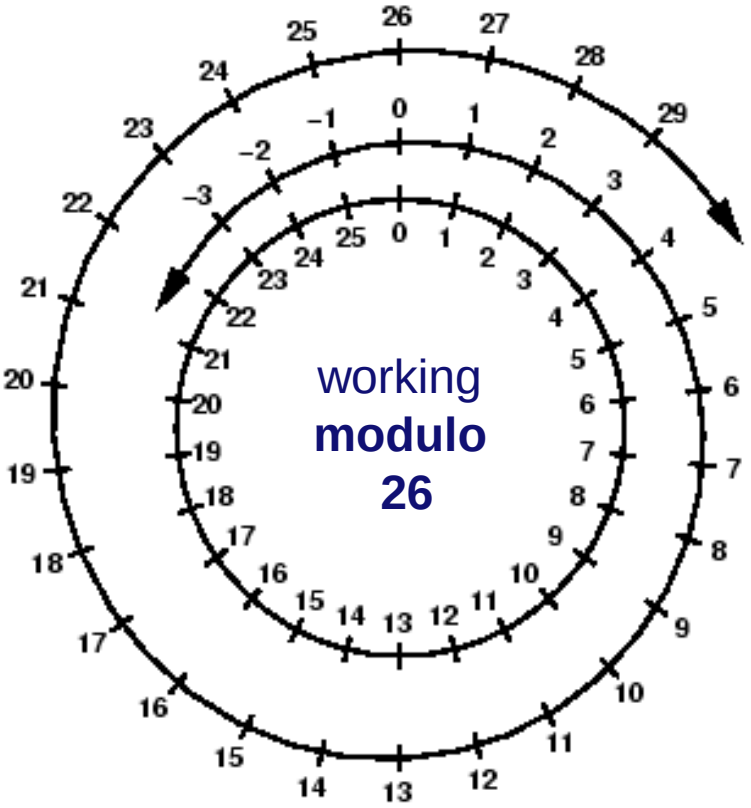
TU/e Technische Universiteit Eindhoven University of Technology

Where innovation starts

Crypto 1.0

Caesar





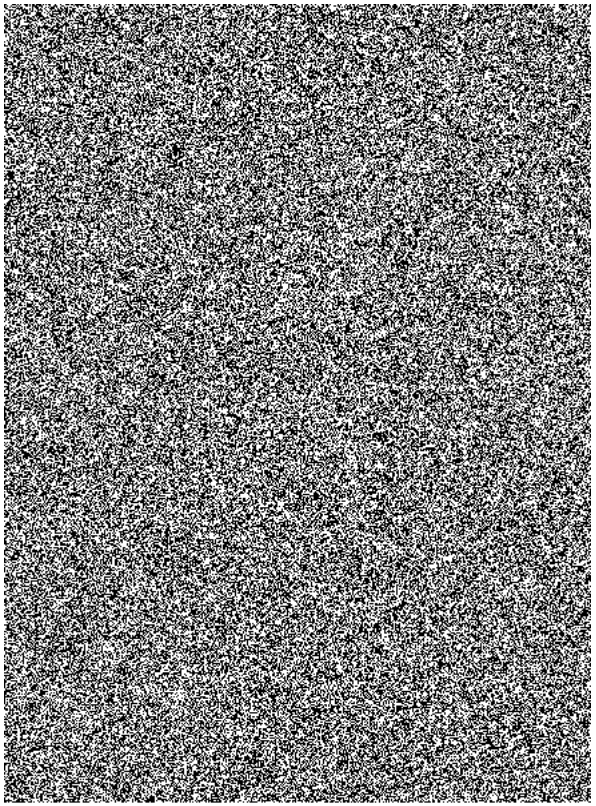
Rekenen met versleutelde data

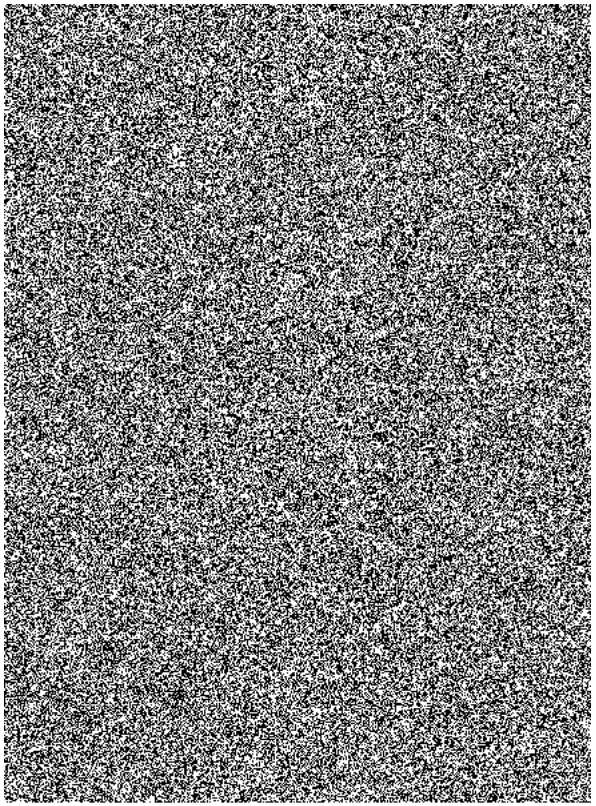
Zonder steeds te ontsleutelen!

Naor, Shamir ‘97

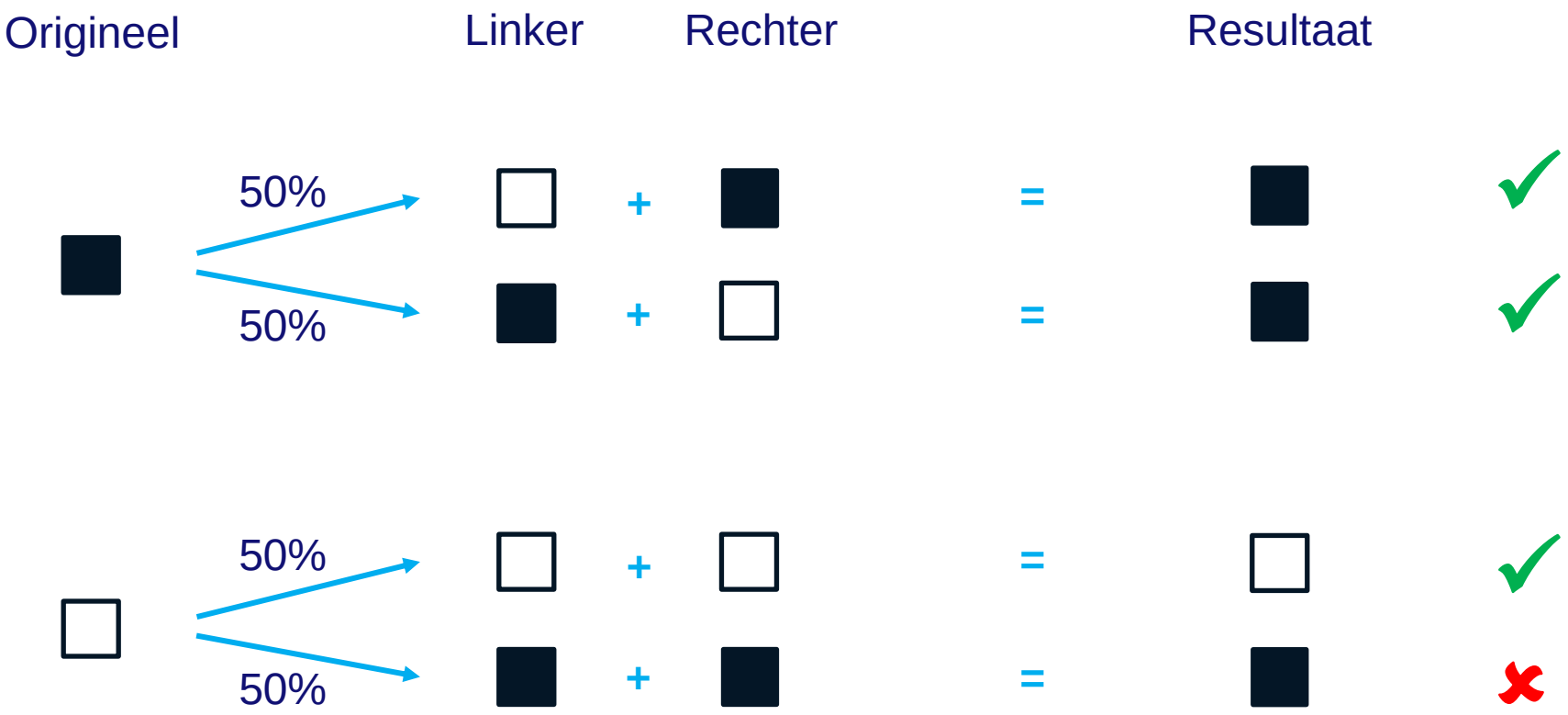
Encryptie met Transparanten

Visual Secret sharing





Visual Secret sharing



Naor, Naor, Reingold, ‘99

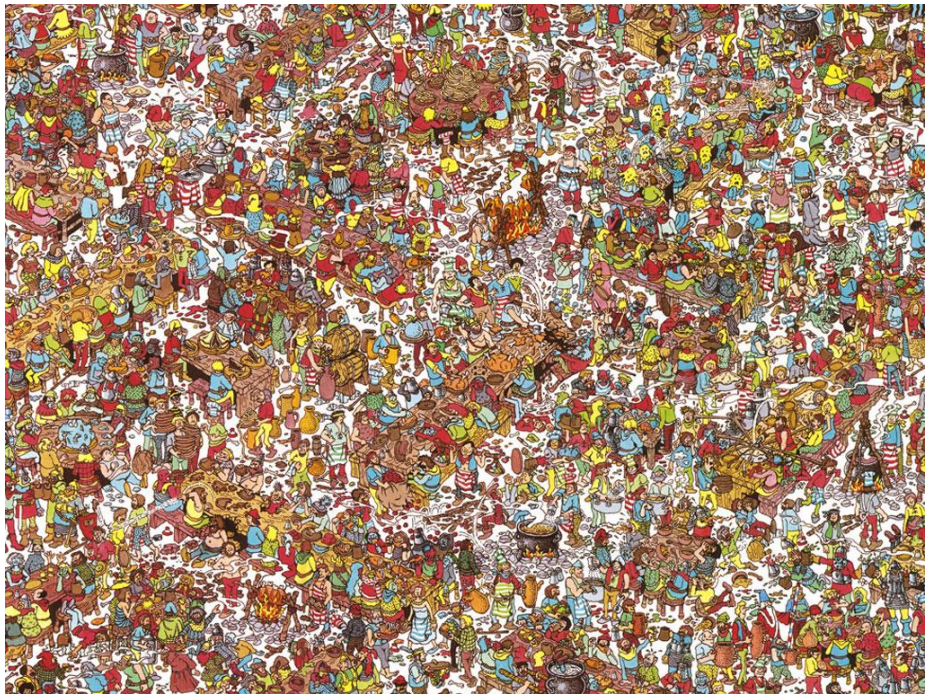
“Waar is Wally?” in Zero-Knowledge

Waar is Wally?

Vind

Wally

in



Bert den Boer, ‘89

Zero-Knowledge Matchmaking

Matchmaking

Alice:

voor “ja”

voor “nee”

scheider:

Bob:

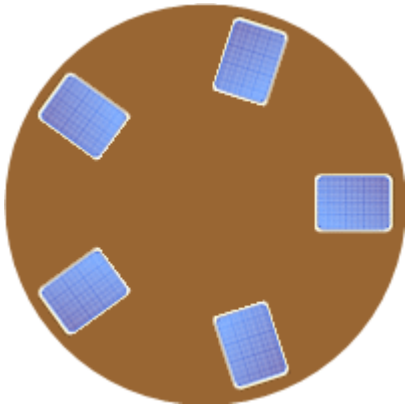
voor “ja”

voor “nee”

Stel Alice denkt “ja”

Stel Bob denkt “ja”

Alice en Bob couperen en openen de kaarten …



Matchmaking

ja  ja

Match!

ja  nee

nee  ja

nee  nee

Deze drie gevallen zijn niet van elkaar te onderscheiden.

Als je `nee' kiest, weet je niet wat de ander heeft gekozen.

Matchmaking with a Smile

Tom Verhoeff's Smiley (in Mathematica):

http://demonstrations.wolfram.com/ZeroKnowledgeMatchmaker/

AND functie

x	y	x ∧ y
0	0	0
0	1	0
1	0	0
1	1	1

Vragen

?

Voor meer informative, zie
http://www.win.tue.nl/~berry/2WC13/LectureSlides.pdf

Author's address

Berry Schoenmakers

Coding and Crypto group
Dept. of Math. and CS
TU Eindhoven

berry@win.tue.nl
http://www.win.tue.nl/~berry/