

TOTAL PUZZLES AND CRYPTOGRAPHY

Chethan Kamath

Academic Sponsor: Nir Bitansky

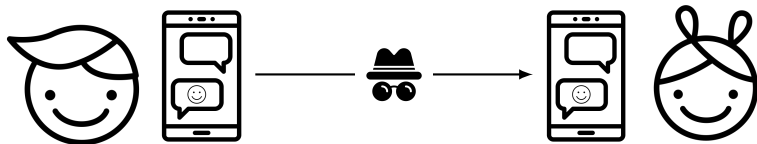
Host: Tel Aviv University

Azrieli Fellows Conference #1, February 2-nd, 2022

CRYPTOGRAPHY, IN A NUTSHELL

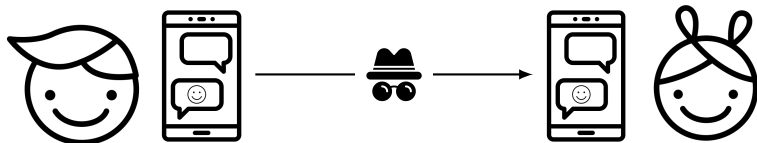


CRYPTOGRAPHY, IN A NUTSHELL



Privacy

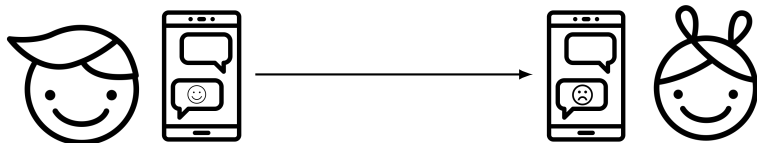
CRYPTOGRAPHY, IN A NUTSHELL



Privacy



CRYPTOGRAPHY, IN A NUTSHELL

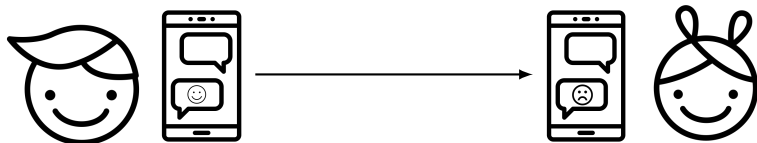


Privacy

Integrity



CRYPTOGRAPHY, IN A NUTSHELL



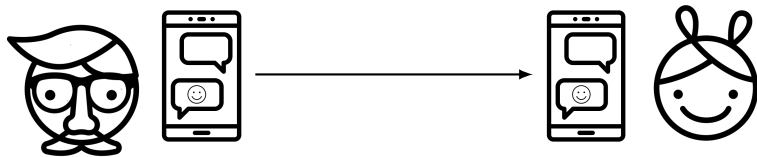
Privacy



Integrity



CRYPTOGRAPHY, IN A NUTSHELL



Privacy

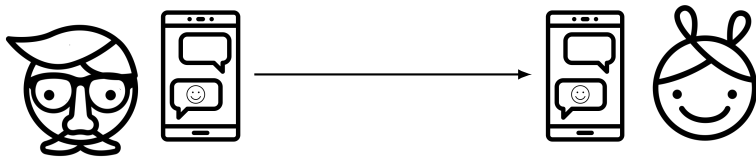


Integrity



Identity

CRYPTOGRAPHY, IN A NUTSHELL



Privacy



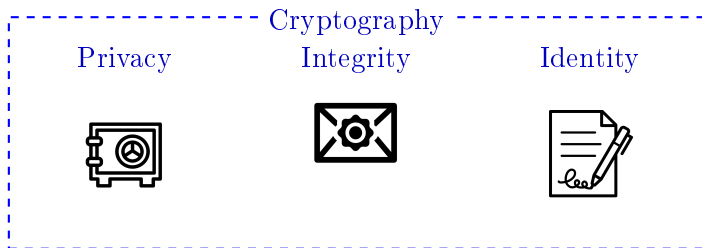
Integrity



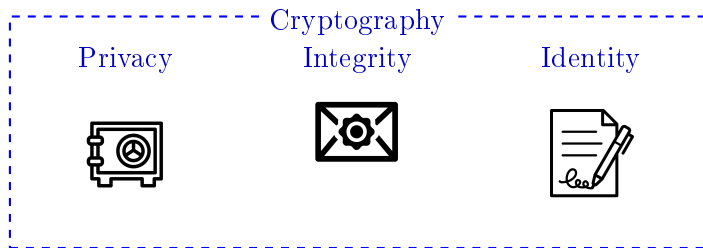
Identity



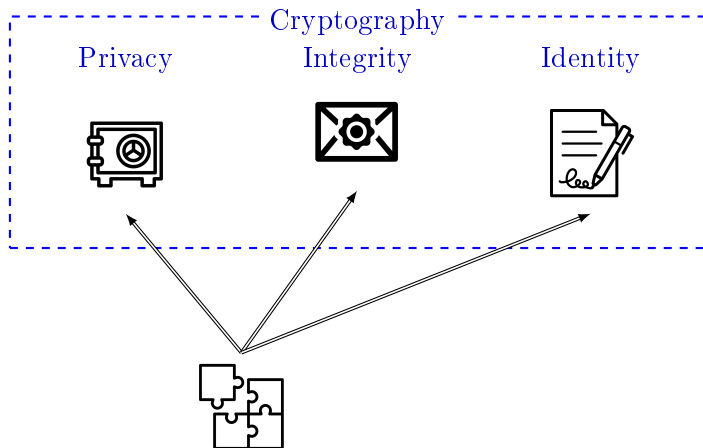
CRYPTOGRAPHY, IN A NUTSHELL



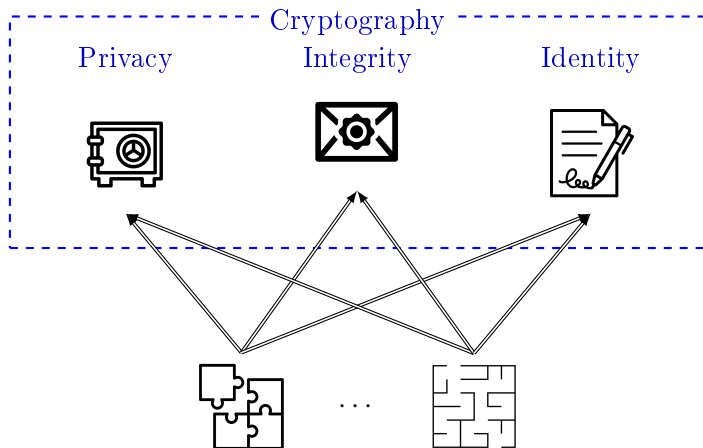
BUILDING CRYPTOGRAPHY FROM PUZZLES



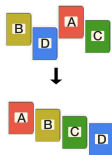
BUILDING CRYPTOGRAPHY FROM PUZZLES



BUILDING CRYPTOGRAPHY FROM PUZZLES



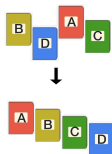
WHAT KIND OF PUZZLES?



SORT

—————Hardness—————→

WHAT KIND OF PUZZLES?

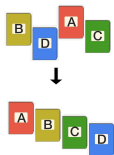


SORT

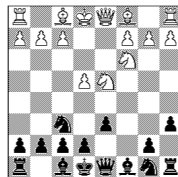
—————Hardness—————→

► Hard to solve

WHAT KIND OF PUZZLES?



SORT

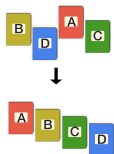


CHES

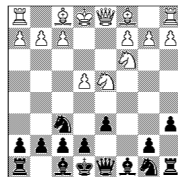
—————Hardness—————→

► Hard to solve

WHAT KIND OF PUZZLES?



SORT

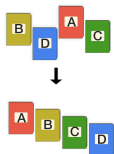


CHES

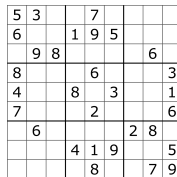
—————Hardness—————→

- ▶ Hard to solve
- ▶ Easy to check solution

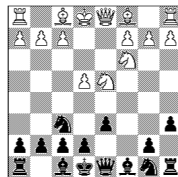
WHAT KIND OF PUZZLES?



SORT



SUDOKU

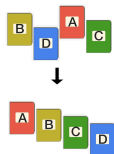


CHES

—————Hardness—————→

- ▶ Hard to solve
- ▶ Easy to check solution

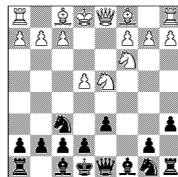
WHAT KIND OF PUZZLES?



SORT



SUDOKU

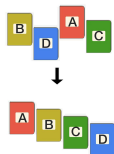


CHES

—————Hardness—————→

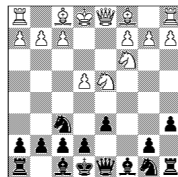
- ▶ Hard to solve
- ▶ Easy to check solution
- ▶ Easy to generate instances with solution

WHAT KIND OF PUZZLES?



$$39 = 13 \times 3$$

5	3		7			
6			1	9	5	
	9	8				6
8			6			3
4		8		3		1
7			2			6
	6				2	8
			4	1	9	5
			8		7	9



Sort

Factor

Sudoku

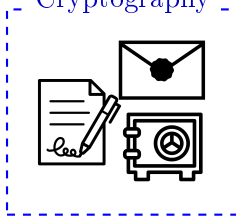
Chess

—————Hardness—————→

- ▶ Hard to solve
- ▶ Easy to check solution
- ▶ Easy to generate instances with solution

TOTAL PUZZLES: SOLUTION GUARANTEED

Cryptography

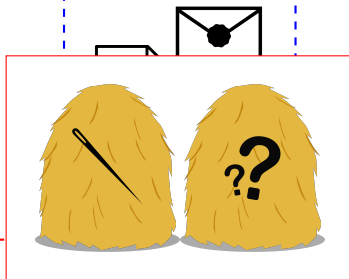


$$39 = 13 \times 3$$

FACTOR

TOTAL PUZZLES: SOLUTION GUARANTEED

Cryptography



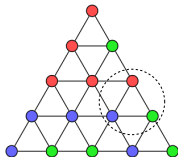
$$39 = 13 \times 3$$

FACTOR

Total Puzzles

TOTAL PUZZLES: SOLUTION GUARANTEED

Cryptography



SPERNER

$$39 = 13 \times 3$$

FACTOR



NASH

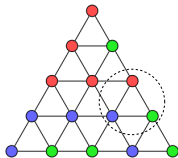
Total Puzzles

TOTAL PUZZLES: SOLUTION GUARANTEED

Cryptography



Economics



SPERNER

$$39 = 13 \times 3$$

FACTOR



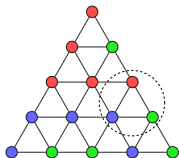
NASH

Total Puzzles

My Research: How Cryptography
relates to Total Puzzles?

HOW CRYPTOGRAPHY RELATES TO TOTAL PUZZLES?

Cryptography



SPERNER

$$39 = 13 \times 3$$

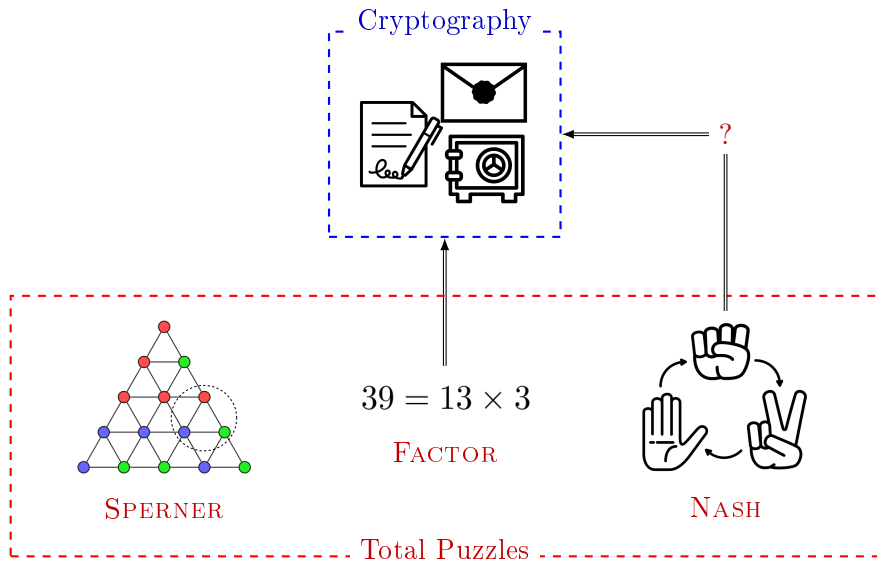
FACTOR



NASH

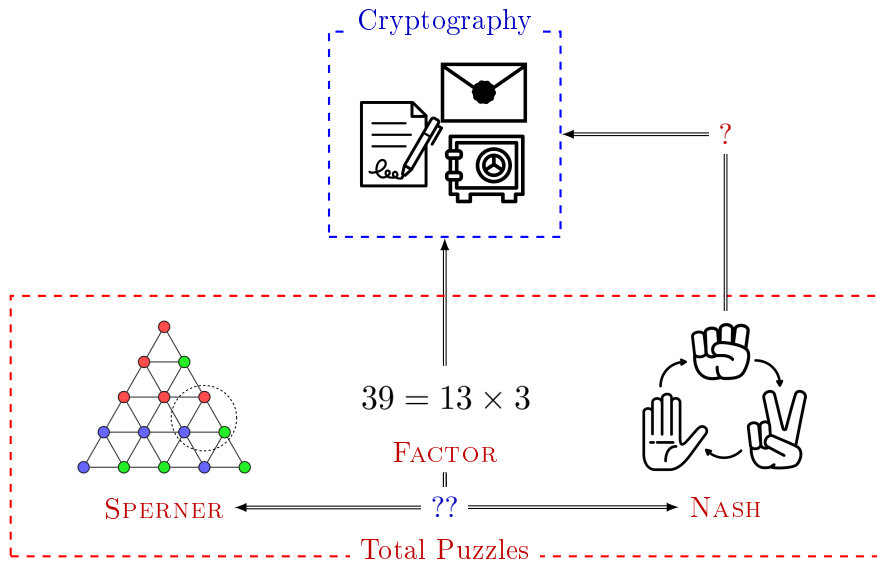
Total Puzzles

HOW CRYPTOGRAPHY RELATES TO TOTAL PUZZLES?



? implies other sources of puzzles

HOW CRYPTOGRAPHY RELATES TO TOTAL PUZZLES?



?? implies hard tasks in other domains

Thank you!

ACKNOWLEDGEMENTS: NOUN PROJECT

- ▶ Zuzanna Nebes: Man (40215) and Girl (52698)
- ▶ mynamepong: Messaging (2209028), Jigsaw (1932661)
- ▶ Youmena: Vault (1008679)
- ▶ Bartama Graphic: Spy (3780474)
- ▶ Adrien Coquet: Seal (3777066), Disguise (4237095)
- ▶ iconforyou: Signature (2901037)
- ▶ Juan Pablo Bravo: Maze (369000)
- ▶ Lucas Helle: Rock-papper-and-scissors (2837622)
- ▶ Angelo Troiano: Stock market (4364257)
- ▶ Tobais F Wolf: Sad (3062) and Happy (151275)
- ▶ Adele Lopez: Sperner