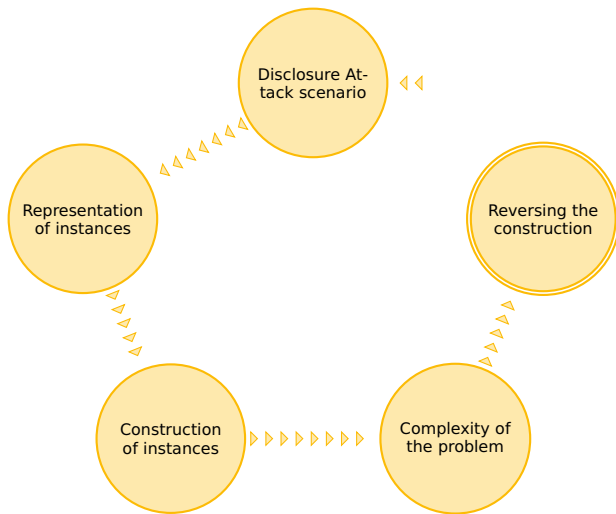


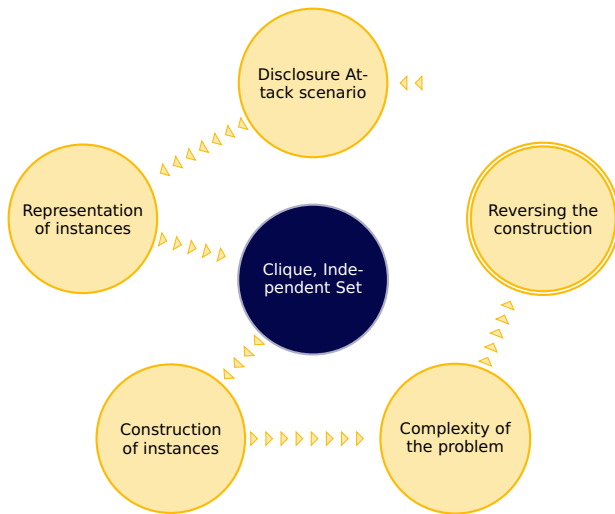
Disclosure Attacks in Polynomial Time

Stefan Berthold

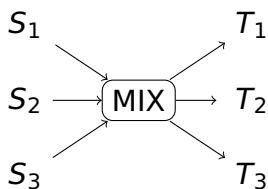
Faculty of Computer Science
Technische Universität Dresden
01062 Dresden, Germany

September 5, 2008





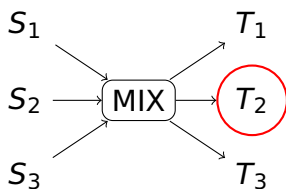
Intersection Attack & Disclosure Attack



Symbols

- S_i — subjects
- T_j — targets
- T_2 — honeypot
- S_1, S_3 — target persons

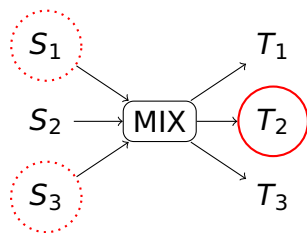
Intersection Attack & Disclosure Attack



Symbols

- S_i — subjects
- T_j — targets
- T_2 — honeypot
- S_1, S_3 — target persons

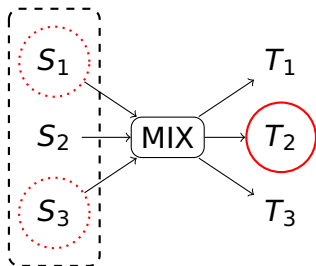
Intersection Attack & Disclosure Attack



Symbols

- S_i — subjects
- T_j — targets
- T_2 — honeypot
- S_1, S_3 — target persons

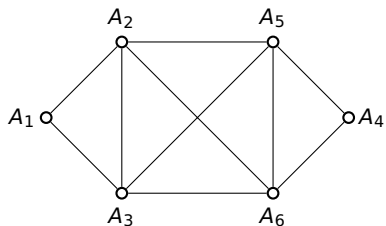
Intersection Attack & Disclosure Attack



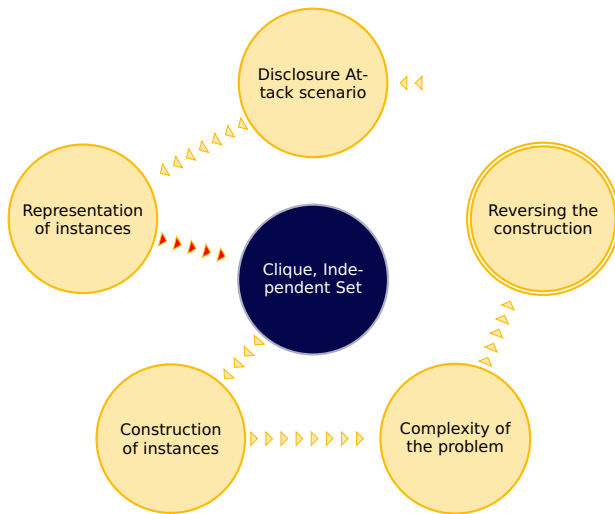
Symbols

- S_i — subjects
- T_j — targets
- T_2 — honeypot
- S_1, S_3 — target persons

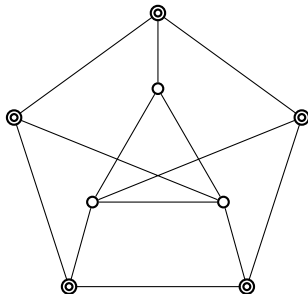
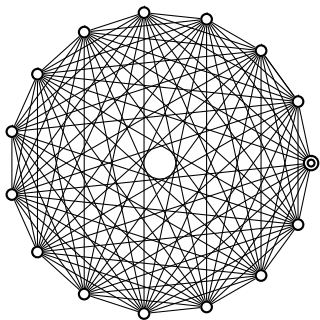
Graph & Table Representation



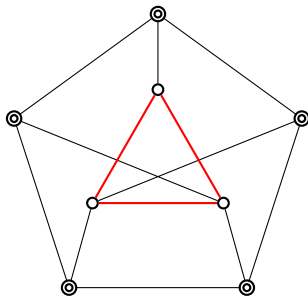
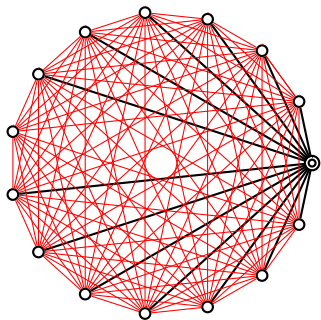
	<i>a</i>	<i>b</i>	<i>c</i>	other persons
A_1	x			$N_1 \dots$
A_2	x		x	$N_2 \dots$
A_3	x		x	$N_3 \dots$
A_4		x		$N_4 \dots$
A_5		x	x	$N_5 \dots$
A_6		x	x	$N_6 \dots$



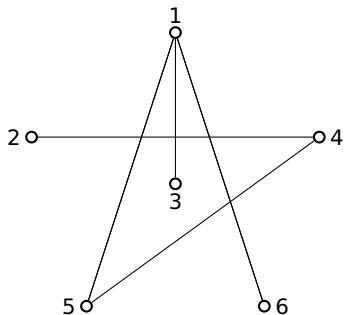
Clique Problem



Clique Problem

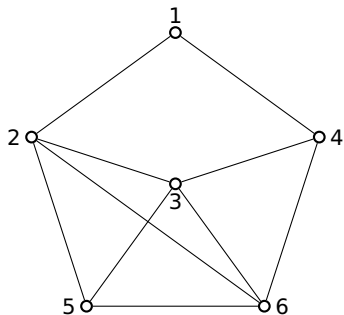


Disclosure Attack & Clique



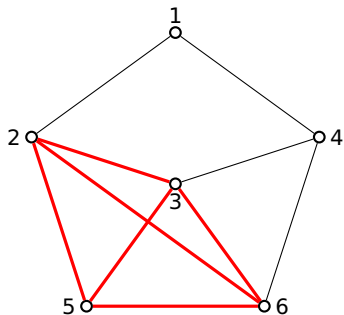
	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
A_1	x	x	x		
A_2				x	
A_3	x				
A_4				x	x
A_5		x			x
A_6			x		

Disclosure Attack & Clique



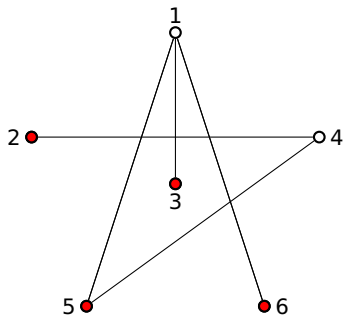
	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
A_1	x	x	x		
A_2				x	
A_3	x				
A_4				x	x
A_5		x			x
A_6			x		

Disclosure Attack & Clique



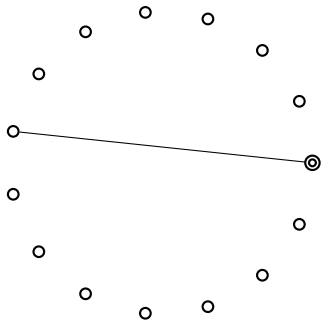
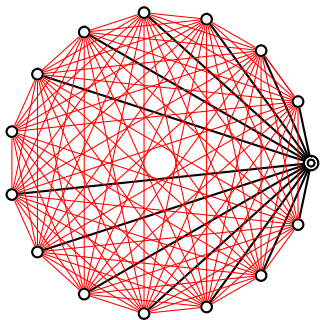
	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
A_1	x	x	x		
A_2				x	
A_3	x				
A_4				x	x
A_5		x			x
A_6			x		

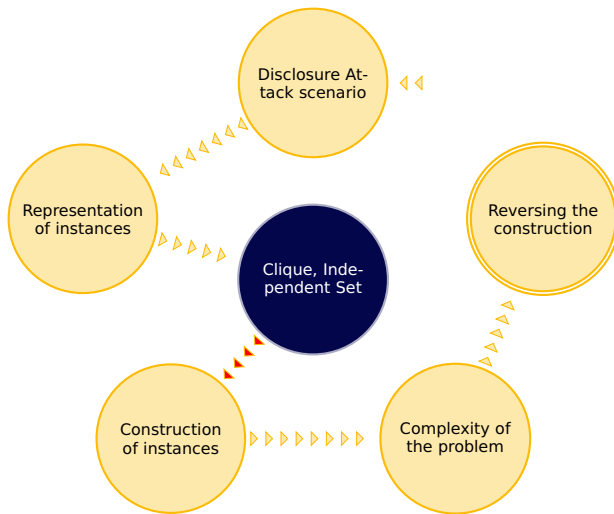
Disclosure Attack & Clique



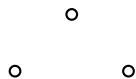
	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
A_1	x	x	x		
A_2				x	
A_3	x				
A_4				x	x
A_5		x			x
A_6			x		

Independent Set Problem

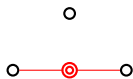




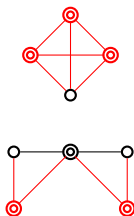
How to Create Problem Instances



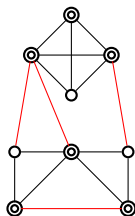
Step 1)



Step 2)

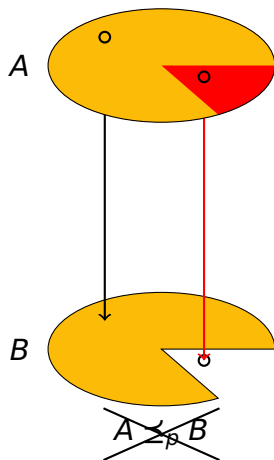
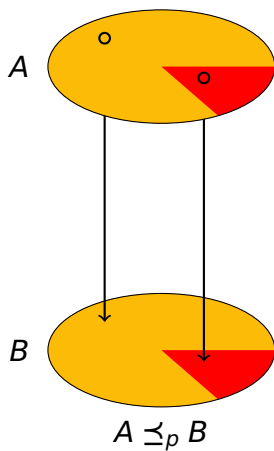


Step 3)

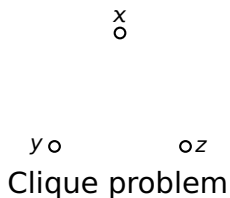


Step 4)

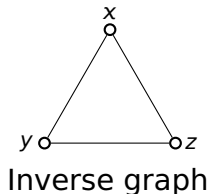
Proofs by Reduction



The Proof of NP-completeness Fails!



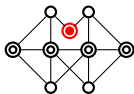
	{x, y}	{x, z}	{y, z}
A_x	x	x	
A_y		x	x
A_z	x		x



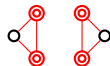
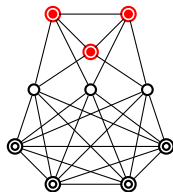
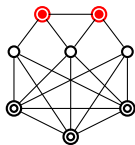
	a	b	c
A_1	x	x	
A_2		x	x
A_3	x		x

Reduction: $CLIQUE \leq_p IS$ ~~$\leq_p DA$~~

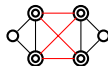
Greedy is No Good Strategy



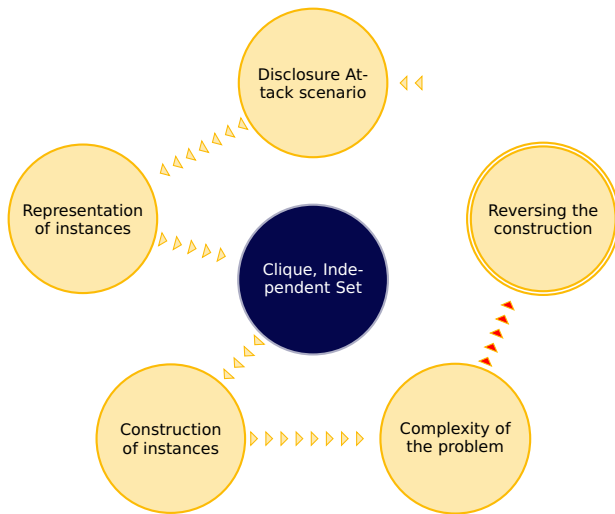
Step 1)



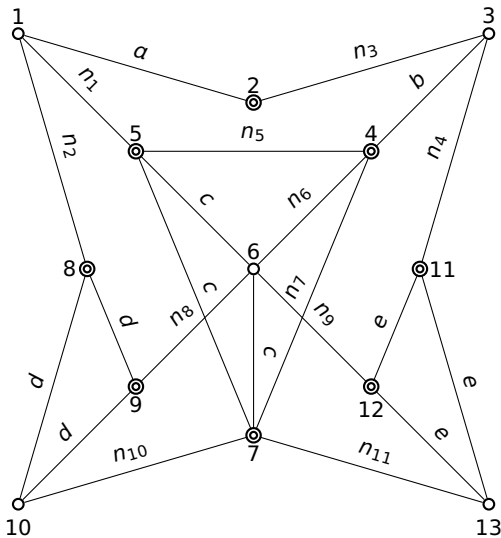
Step 3)



Step 4)



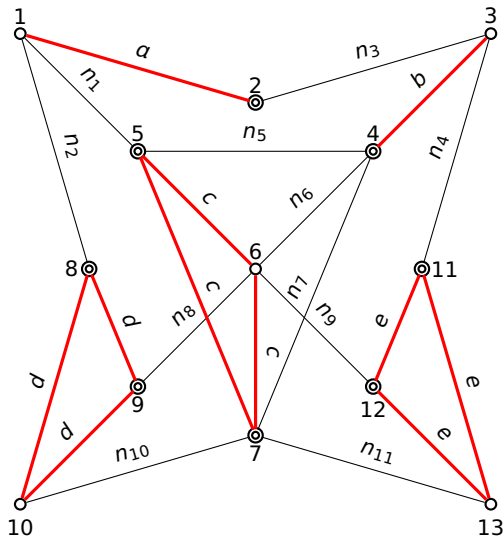
Target Persons in Graph Representation



Possible cliques

- (9,1,1,1,1)
- (8,2,1,1,1)
- (7,3,1,1,1)
- (7,2,2,1,1)
- (6,4,1,1,1)
- (6,3,2,1,1)
- (6,2,2,2,1)
- (5,5,1,1,1)
- (5,4,2,1,1)
- (5,3,3,1,1)
- (5,3,2,2,1)
- (5,2,2,2,2)
- (4,4,3,1,1)
- (4,4,2,2,1)
- (4,3,3,2,1)
- (4,3,2,2,2)
- (3,3,3,3,1)
- (3,3,3,2,2)

Target Persons in Graph Representation



Possible cliques

(9,1,1,1,1)

(8,2,1,1,1)

(7,3,1,1,1)

(7,2,2,1,1)

(6,4,1,1,1)

(6,3,2,1,1)

(6,2,2,2,1)

(5,5,1,1,1)

(5,4,2,1,1)

(5,3,3,1,1)

(5,3,2,2,1)

(5,2,2,2,2)

(4,4,3,1,1)

(4,4,2,2,1)

(4,3,3,2,1)

(4,3,2,2,2)

(3,3,3,3,1)

(3,3,3,2,2) ←

Seeking Targets in Table Representation

	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>n</i> ₁	<i>n</i> ₂	<i>n</i> ₃	<i>n</i> ₄	<i>n</i> ₅	<i>n</i> ₆	<i>n</i> ₇	<i>n</i> ₈	<i>n</i> ₉	<i>n</i> ₁₀	<i>n</i> ₁₁	other	
<i>A</i> ₁	x					x	x											<i>N</i> ₁ ...
<i>A</i> ₂	x							x										<i>N</i> ₂ ...
<i>A</i> ₃		x						x	x									<i>N</i> ₃ ...
<i>A</i> ₄		x								x	x	x						<i>N</i> ₄ ...
<i>A</i> ₅			x			x				x								<i>N</i> ₅ ...
<i>A</i> ₆			x								x		x	x				<i>N</i> ₆ ...
<i>A</i> ₇			x									x				x	x	<i>N</i> ₇ ...
<i>A</i> ₈				x			x											<i>N</i> ₈ ...
<i>A</i> ₉				x									x					<i>N</i> ₉ ...
<i>A</i> ₁₀				x											x			<i>N</i> ₁₀ ...
<i>A</i> ₁₁					x				x									<i>N</i> ₁₁ ...
<i>A</i> ₁₂					x									x				<i>N</i> ₁₂ ...
<i>A</i> ₁₃					x												x	<i>N</i> ₁₃ ...

	<i>a</i>	<i>b</i>	<i>n</i> ₁	<i>n</i> ₂	<i>n</i> ₃	<i>n</i> ₄	<i>n</i> ₅	<i>n</i> ₆	<i>n</i> ₇	<i>n</i> ₈	<i>n</i> ₉	<i>n</i> ₁₀	<i>n</i> ₁₁	other persons
<i>A</i> ₁	x		x	x										<i>N</i> ₁ ...
<i>A</i> ₂	x				x									<i>N</i> ₂ ...
<i>A</i> ₃		x			x	x								<i>N</i> ₃ ...
<i>A</i> ₄		x					x	x	x					<i>N</i> ₄ ...

Thanks for your attention!

Questions?

