Ring of Gyges:

Accountable Anonymous Broadcast from Secure Multi-Party Computation (MPC)

Wentao Dong, Peipei Jiang, Huayi Duan, Cong Wang, Lingchen Zhao, and Qian Wang

香港城市大學 City University of Hong Kong

NDSS SYMPOSIUM

Scope: (What)

"The Ring of Gyges"
Invisibility

"Anonymous Communication"
Anonymity

Motivation: (Why)

Privacy & Security

Scenario: (When & Where)

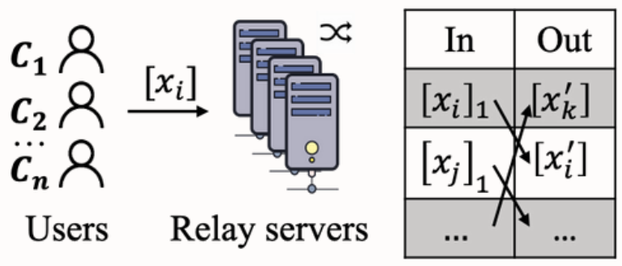
Gyges (Accountable Anonymous Broadcast) from MPC [NDSS'25] (How)

Rabin, **Yao**, Goldreid, Micali, Wigderson, Ben-Or, Goldwasser, Chaum

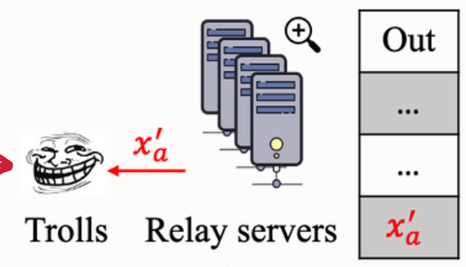
Preliminary:

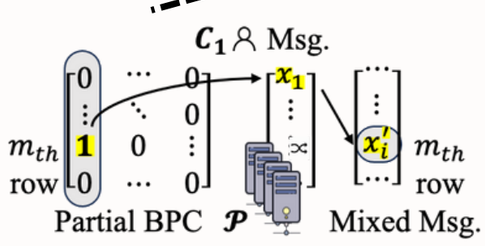
1. *Multi-party computation*
2. *Anonymous communication*

Architecture overview of *Gyges*

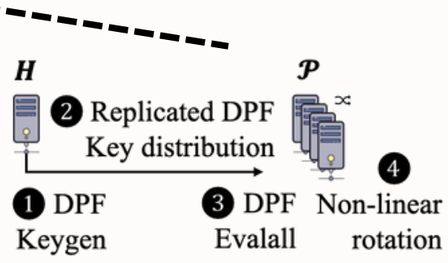


1. *Sender anonymity from multi-party shuffle*
2. *Selective traceability from multi-party trace*

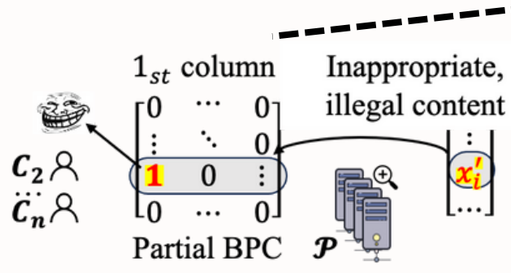




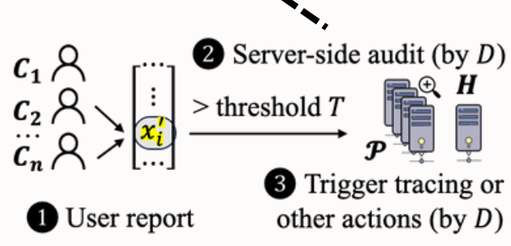
Secret-shared shuffle



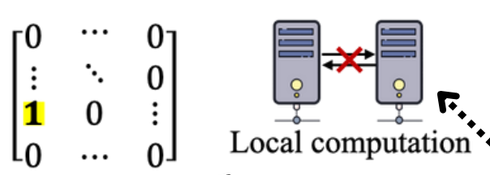
Shuffle Correlation Generation

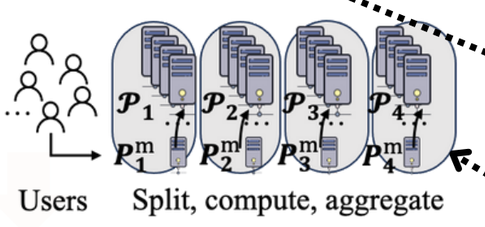


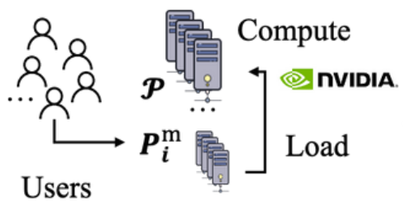
Secret-shared trace



Moderation policy







$\forall P_i \in \mathcal{H}, \quad \Pr[\text{Output}_i = f(x)_i] = 1.$

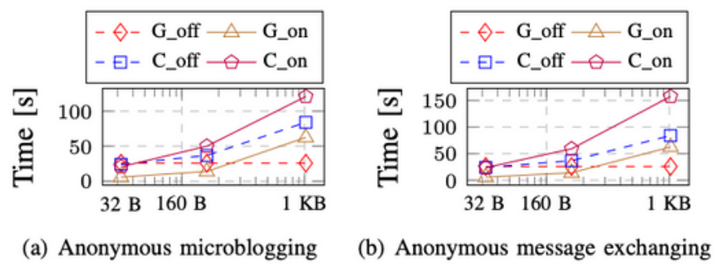
Other Considerations (What Else?)

1. **Anonymity Loves Efficiency**
   a. Silent (non-interactive) shuffle
   b. Sparsity-aware optimization
2. **Anonymity loves Company**
   a. Horizontal scaling
   b. Vertical scaling
3. **Anonymity loves Robustness**
   a. Private "G.O.D"
4. **Anonymity with Accountability**
   a. Selective traceability

Ref.†,‡,♮		N	Clarion [11]	RPM-I, II, III [21]		*Gyges*
Shuffle	Comm. [MB]	10^3	0.228	0.485	0.097	-	0
		10^4	2.289	0.742	0.961	2.763	0
		10^5	22.888	-	-	27.632	0
		10^6	228.881	-	-	-	0
	Time [s]	10^3	0.075	0.051	0.022	-	0.013
		10^4	0.718	1.485	0.581	0.556	0.155
		10^5	7.629	-	-	13.681	1.774
		10^6	95.089	-	-	-	27.945
Trace	Time [s]	10^5	-	-	-	-	0.035

Ref.†			Traceable mixnets [28]	*Gyges*
Shuffle	$n = 4$, $N = 10^4$	Time [s]	343	0.155
Trace		Comm. [MB]	4.1	0.005
		Time [s]	681.6	0.134

Ref.†	Env.	# servers per party		
		1	2	3
Throughput [10^7 entry/min]	*Gyges*-CPU (w/ sparsity)	1.266	2.531	3.797
	Gyges-GPU (w/o sparsity)	1.546	3.092	4.639



(a) Anonymous microblogging (b) Anonymous message exchanging

Some Results