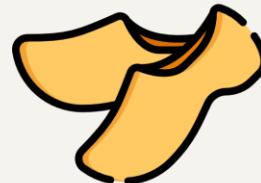




ia.cr/2025/971



Sabot



Efficient and Strongly Anonymous Bootstrapping of Communication Channels

Christoph Coijanovic¹, Laura Hetz², Kenneth G. Paterson², Thorsten Strufe¹

¹Karlsruhe Institute of Technology

²ETH Zurich



ia.cr/2025/971



Sabot



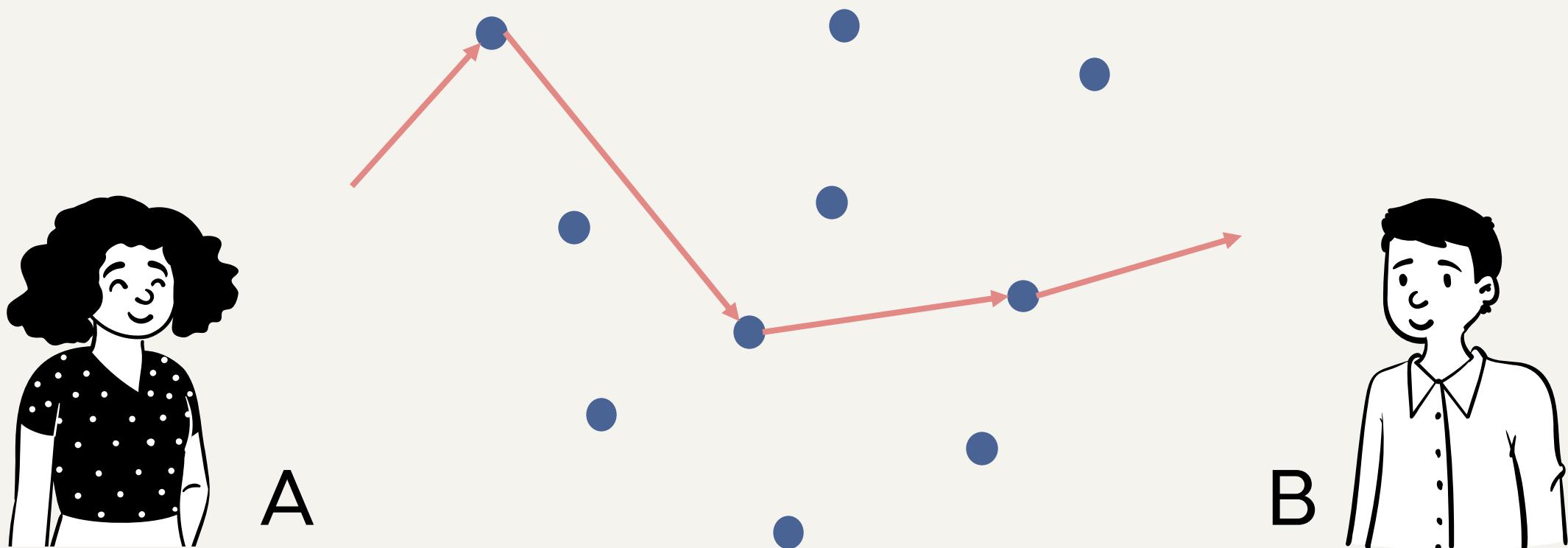
Efficient and Strongly Anonymous Bootstrapping of Communication Channels

Christoph Coijanovic¹, Laura Hetz², Kenneth G. Paterson², Thorsten Strufe¹

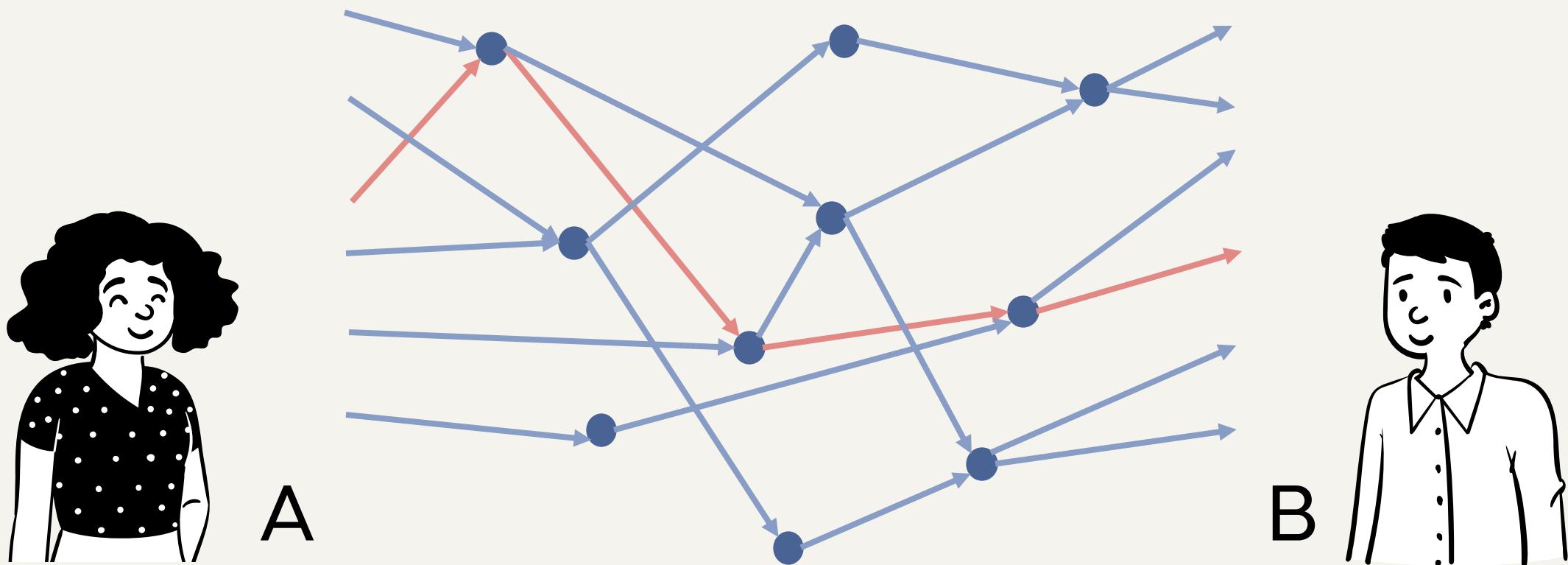
¹Karlsruhe Institute of Technology

²ETH Zurich

Anonymous Communication Networks (ACNs)



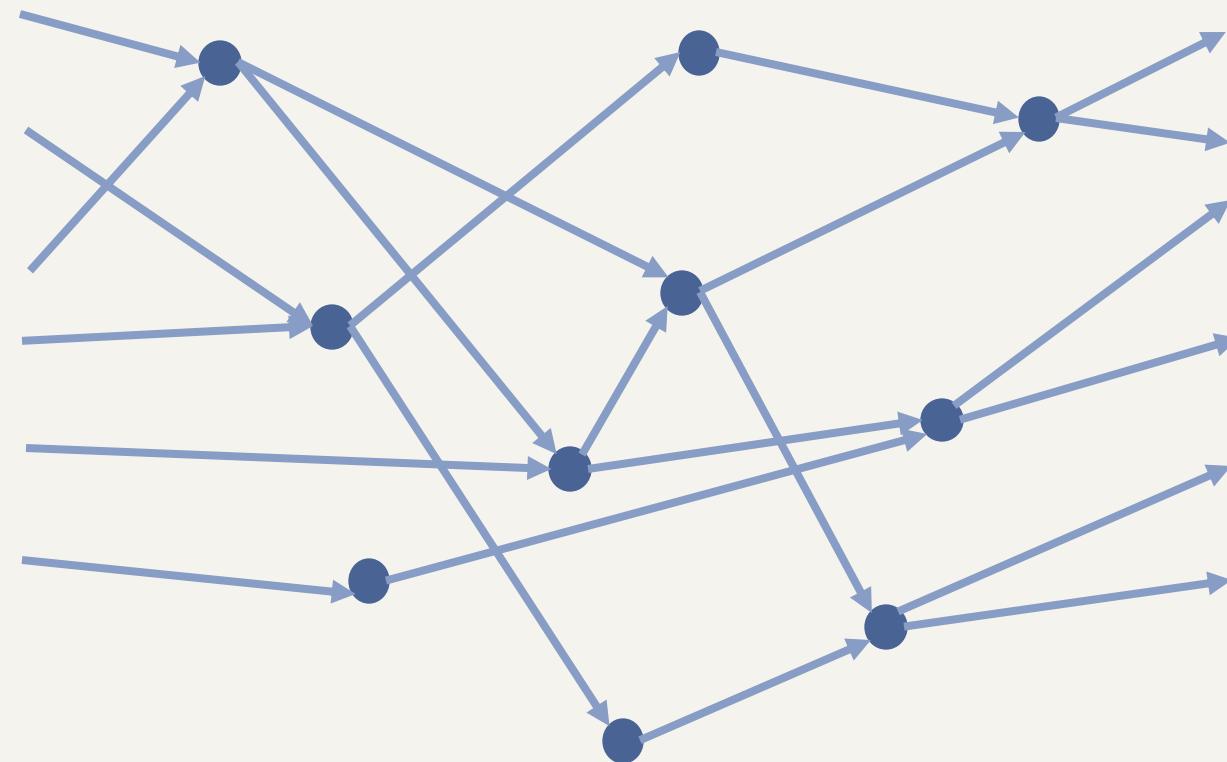
Anonymous Communication Networks (ACNs)



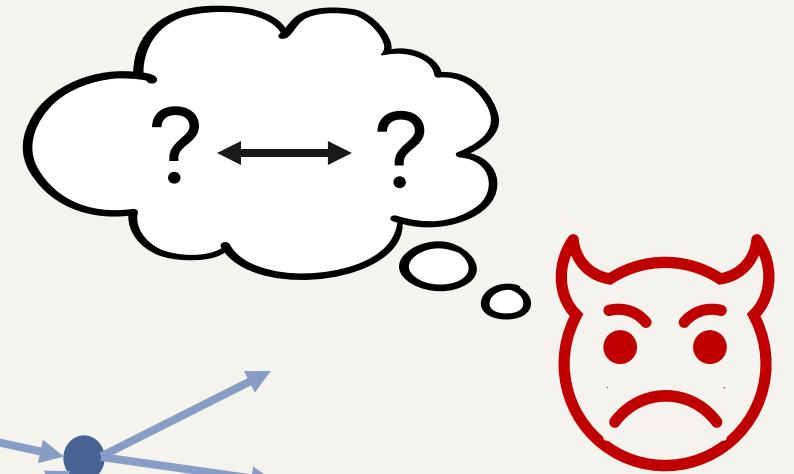
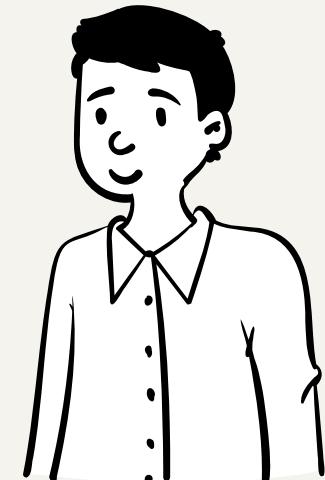
Anonymous Communication Networks (ACNs)



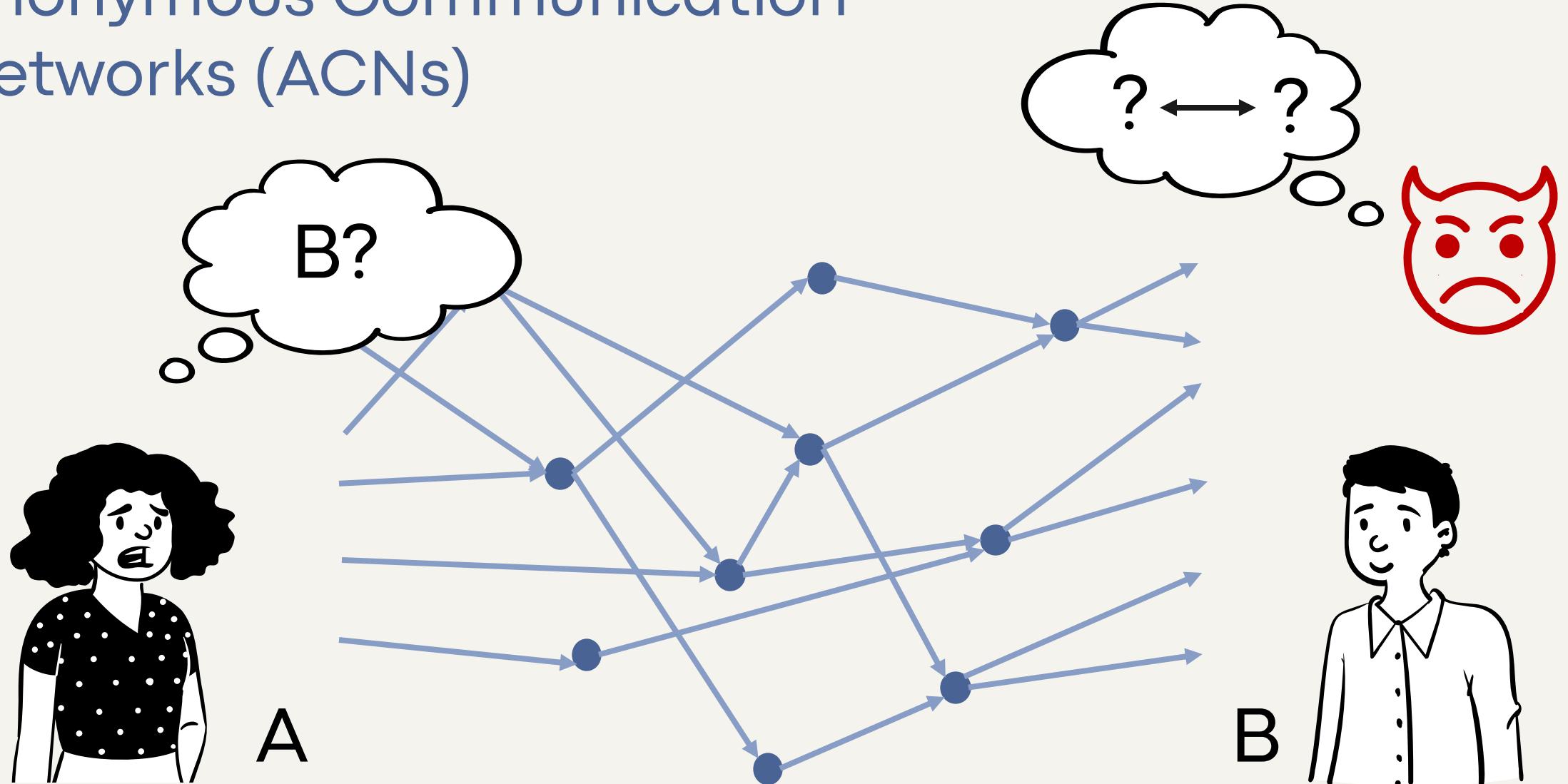
A



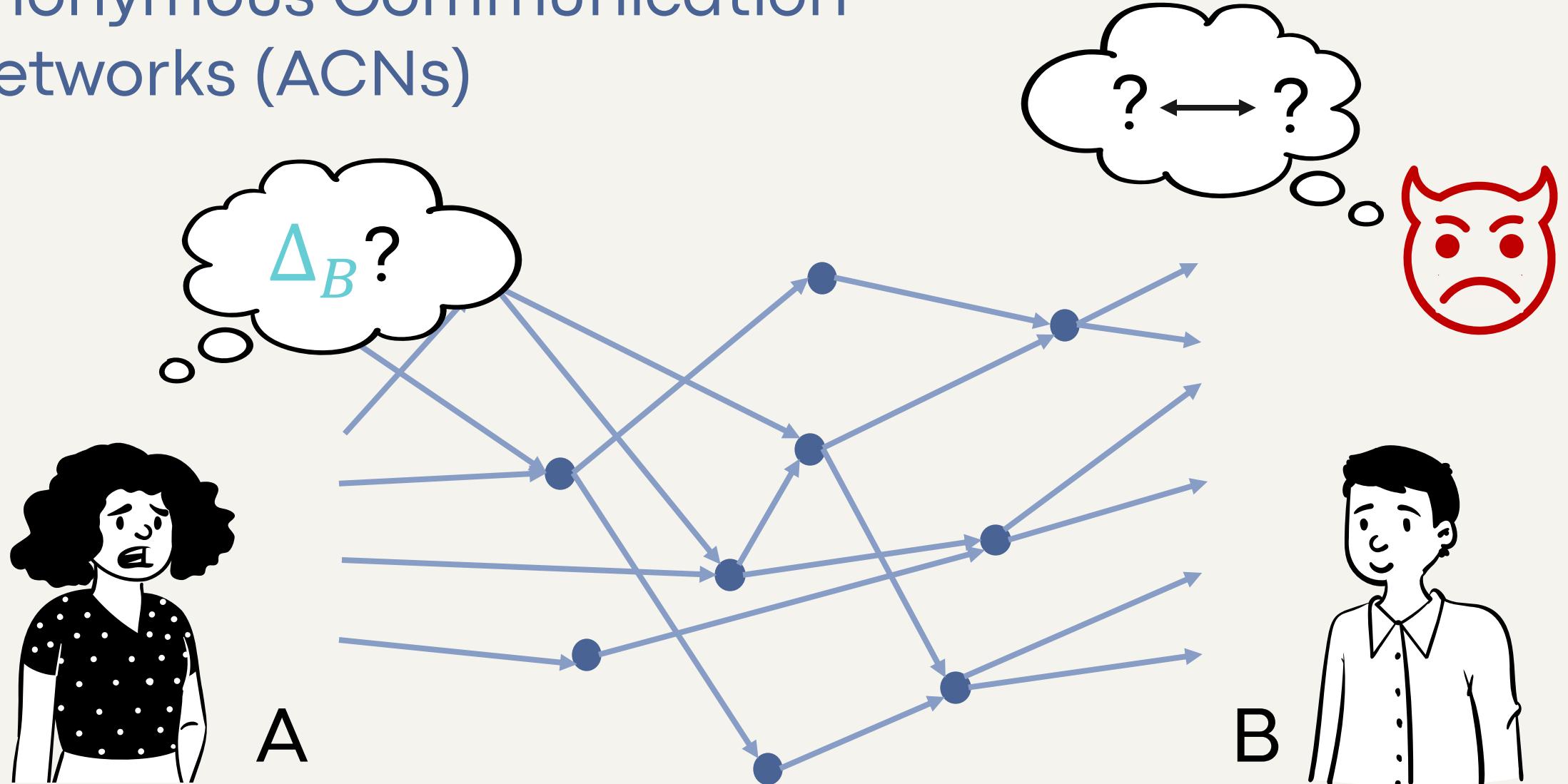
B



Anonymous Communication Networks (ACNs)



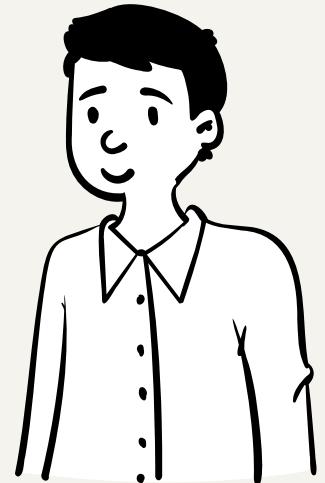
Anonymous Communication Networks (ACNs)



Bootstrapping

Retrieval of contact
information Δ

$$\Delta_B$$



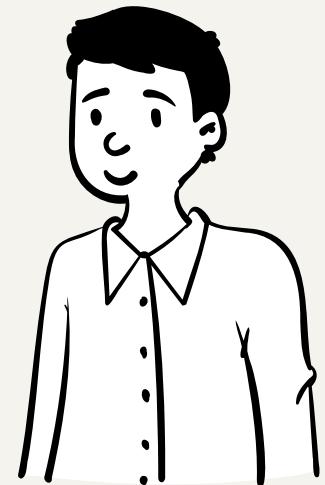
Bootstrapping

Retrieval of contact

information Δ

$$\Delta_A$$

$$\Delta_B$$



Bootstrapping

Retrieval of contact

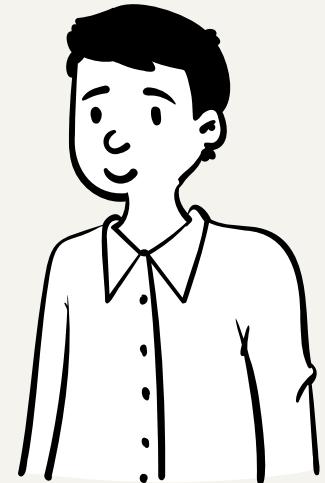
information Δ

$$\Delta_A$$

$$\Delta_B$$



Vuvuzela [1], Pung [2], Stadium [3], Karaoke [4],
XRD [5], Groove [6],

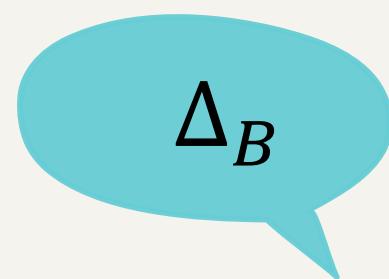
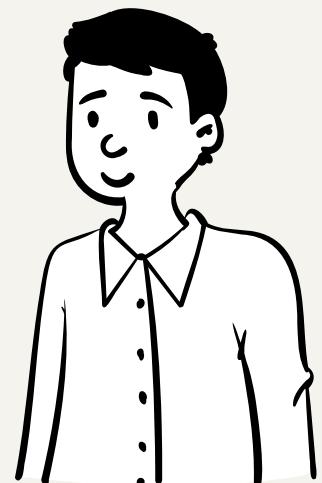


Bootstrapping

Retrieval of contact
information Δ



Vuvuzela [1], Pung [2], Stadium [3], Karaoke [4],
XRD [5], Groove [6],
MCMix [10], Clarion [11], Loopix [9]



Bootstrapping

Retrieval of contact
information Δ



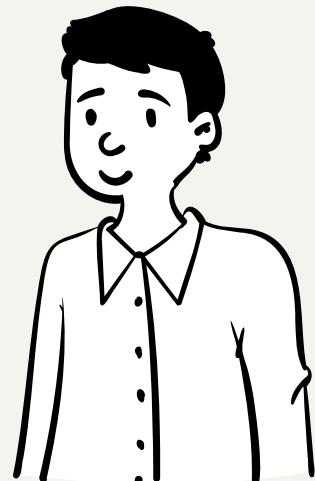
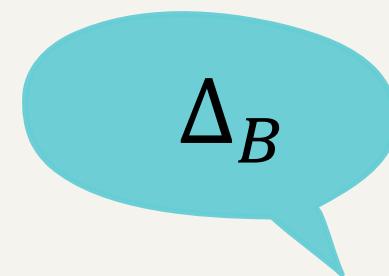
Vuvuzela [1], Pung [2], Stadium [3], Karaoke [4],
XRD [5], Groove [6],



MCMix [10], Clarion [11], Loopix [9]

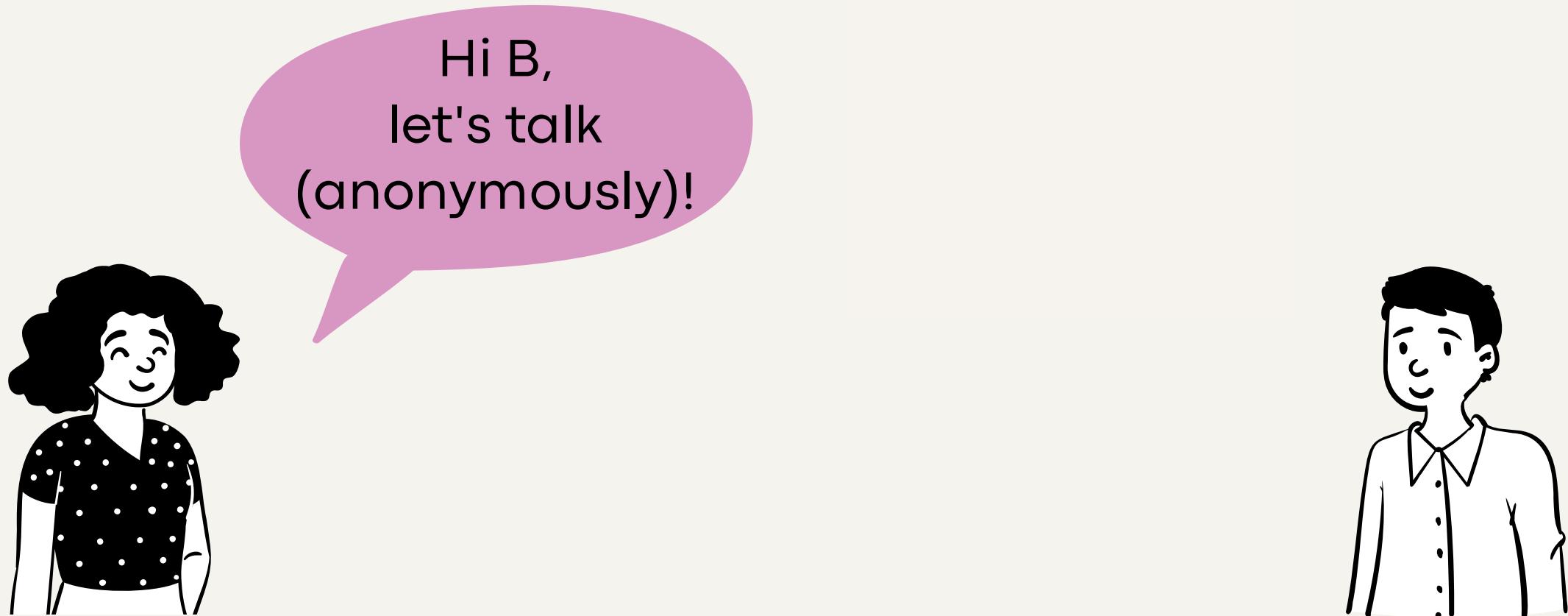


Sabre [12], Express [13]



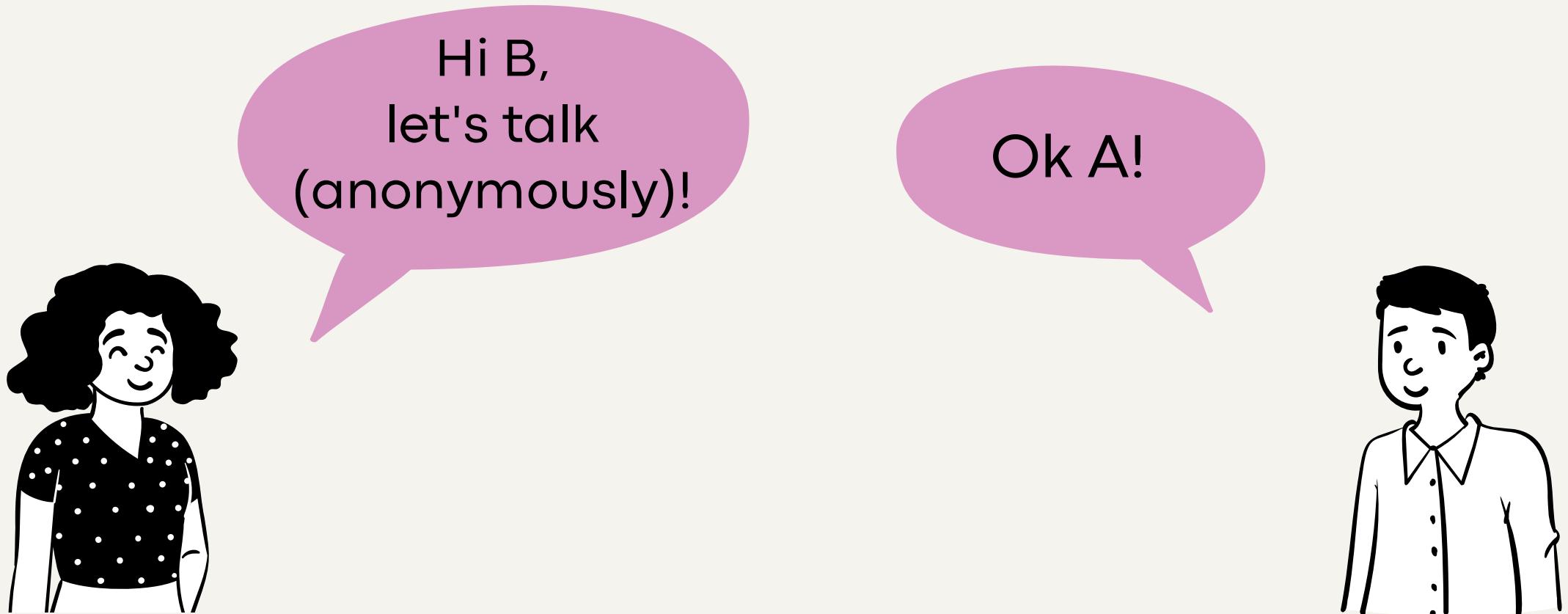
Bootstrapping

Notification



Bootstrapping

Notification (& ACK)



Bootstrapping

Notification (& ACK)

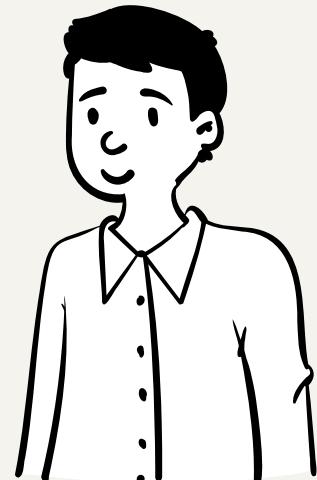


Hi B,
let's talk
(anonymously)!

Ok A!

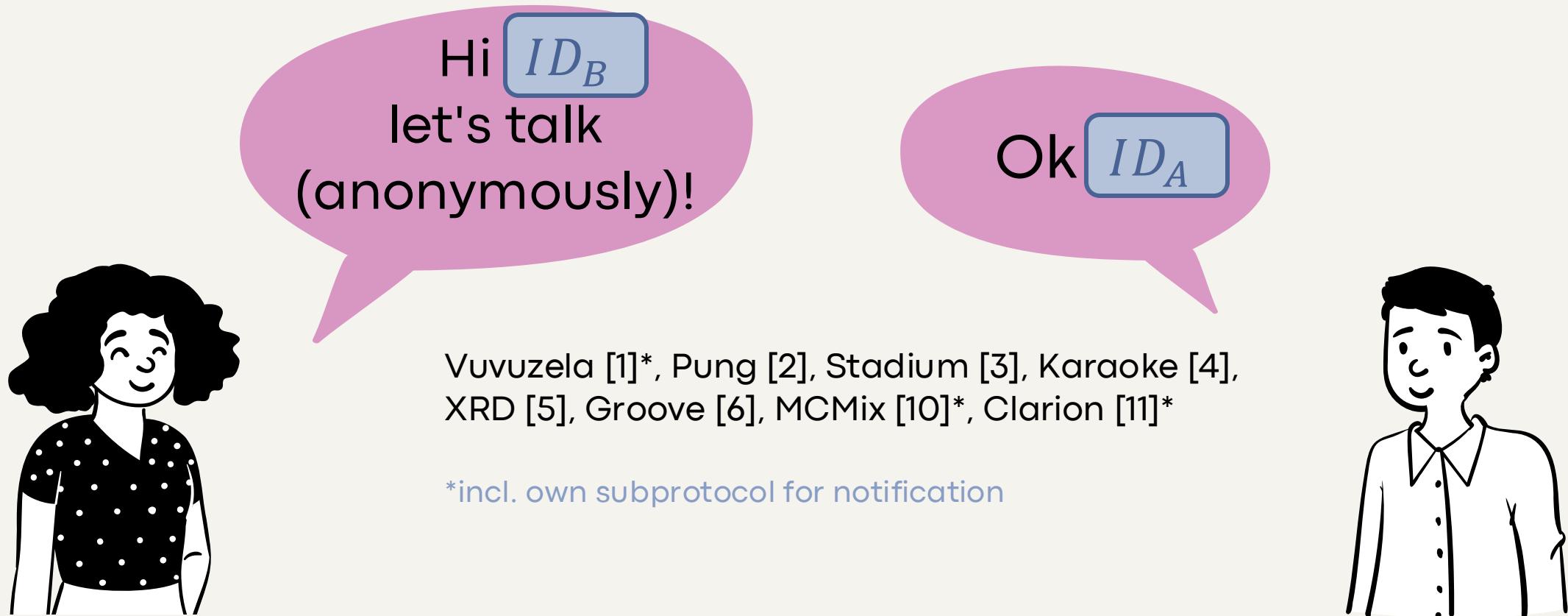
Vuvuzela [1]*, Pung [2], Stadium [3], Karaoke [4],
XRD [5], Groove [6], MCMix [10]*, Clarion [11]*

*incl. own subprotocol for notification



Bootstrapping

Notification (& ACK)



Bootstrapping

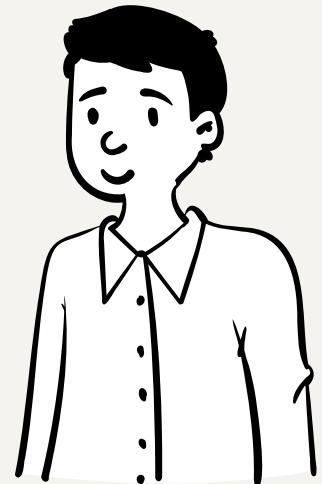


Let's talk!

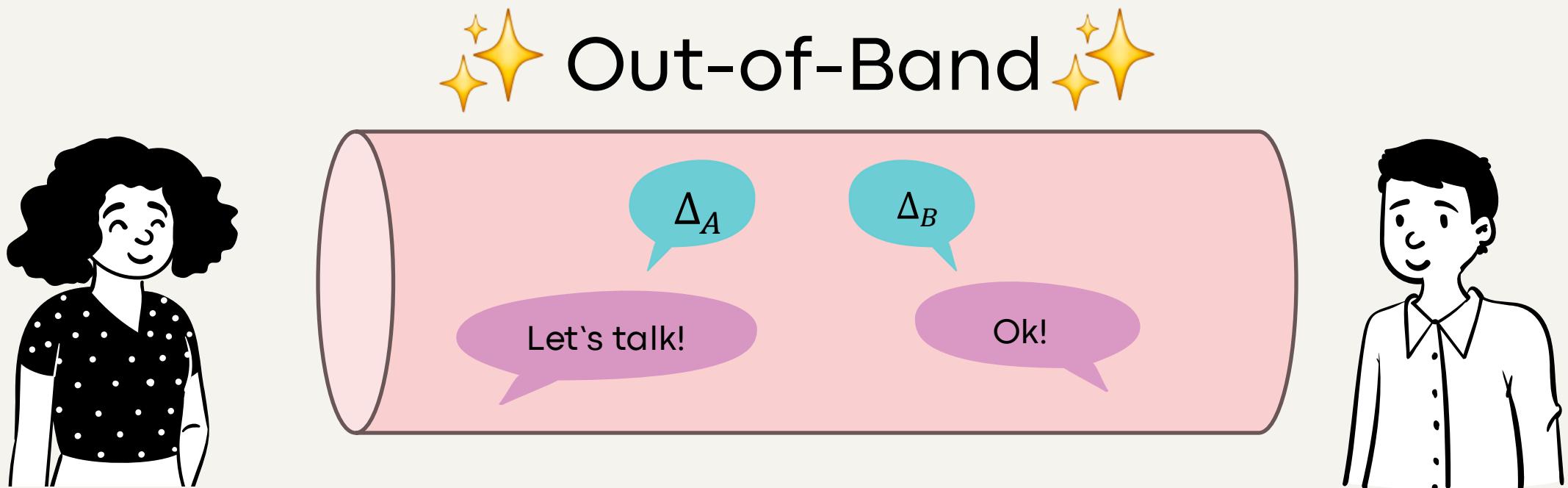
Δ_A

Δ_B

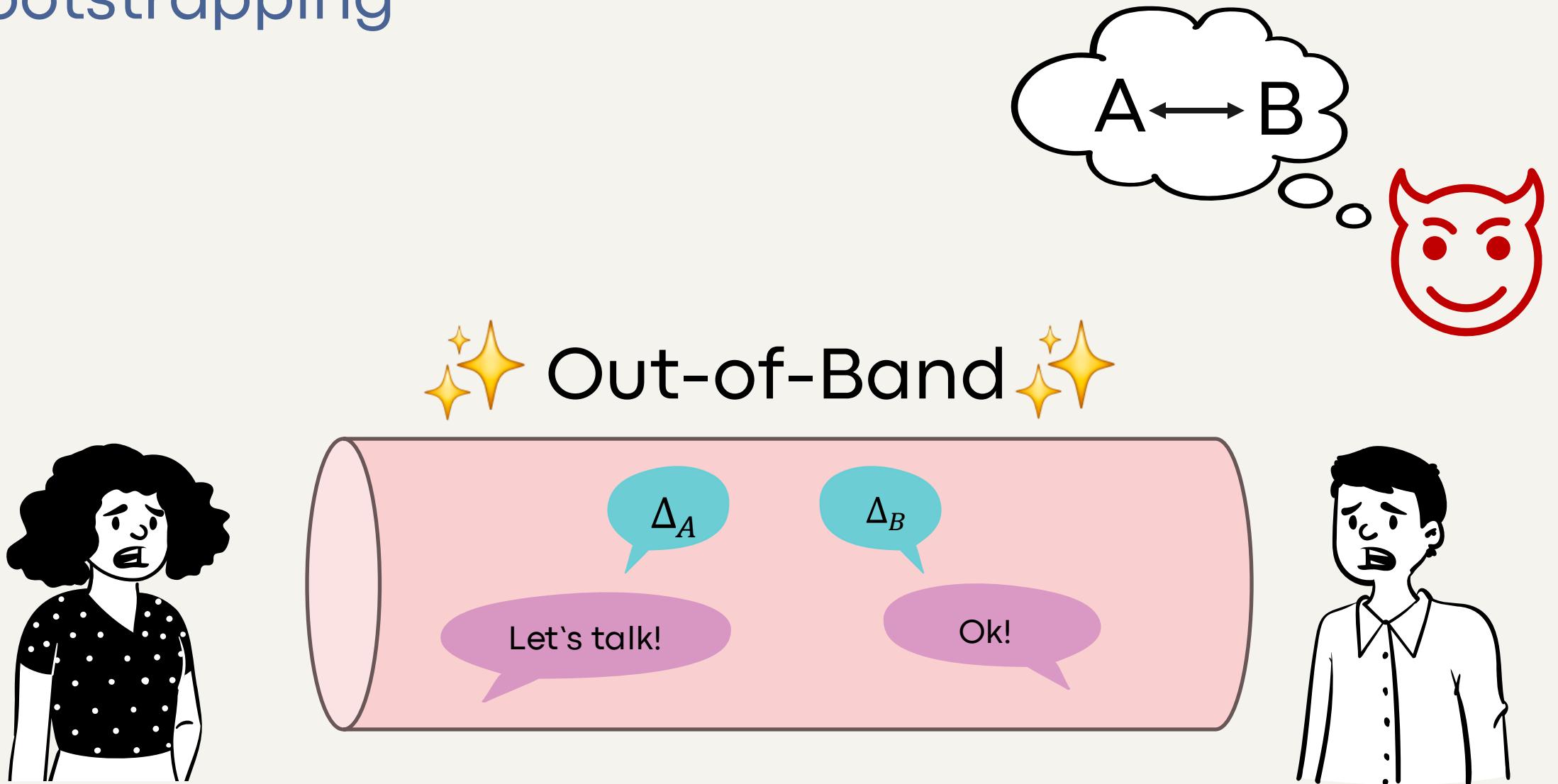
Ok!



Bootstrapping



Bootstrapping



Anonymous Bootstrapping



Related Work



Beginning
of Time

2016

Related Work

D. Lazar and N. Zeldovich.
"Alpenhorn: Bootstrapping Secure
Communication without Leaking
Metadata". USENIX OSDI 2016. [14]



-\(_\)



Beginning
of Time

2016

Icons made by Freepik from www.flaticon.com

Related Work

D. Lazar and N. Zeldovich.
“Alpenhorn: Bootstrapping Secure
Communication without Leaking
Metadata”. USENIX OSDI 2016. [14]



-\(\cup\)-

“Use Alpenhorn!”

Beginning
of Time

2016

Icons made by Freepik from www.flaticon.com

Related Work

D. Lazar and N. Zeldovich.
“Alpenhorn: Bootstrapping Secure
Communication without Leaking
Metadata”. USENIX OSDI 2016. [14]



C. Kocaoğullar et al.
“Pudding: Private User Discovery
in Anonymity Networks”.
IEEE S&P 2024. [15]



Icons made by Freepik from www.flaticon.com

Related Work

Notification

Information
Retrieval

Trust
Assumption

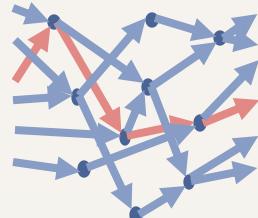
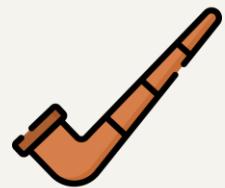
Privacy

Limitations



Related Work

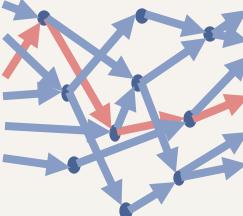
Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
--------------	-----------------------	------------------	---------	-------------



MixNet

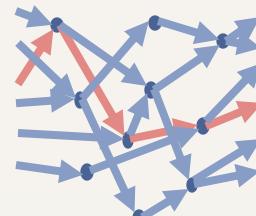


Related Work

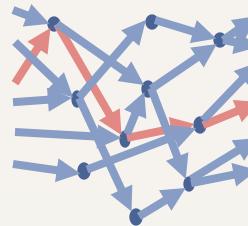
Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption		
		Server-issued precomputed packages		

Related Work

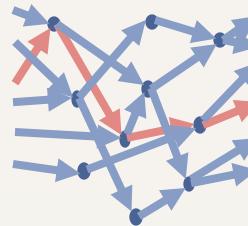
 weaker assumption /
stronger notion

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption	Anytrust	
	Server-issued precomputed packages	Honest Majority		

Related Work

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption	Anytrust	Differential Privacy
	Server-issued precomputed packages	Honest Majority	Membership Unobservability against clients Relationship Unobservability	

Related Work

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
 	 MixNet	Identity-Based Encryption	Anytrust	Differential Privacy
	Server-issued precomputed packages	Honest Majority	Membership Unobservability against clients Relationship Unobservability	Leaks popularity of receivers High bandwidth (≥ 7 MiB per bootstrapping) No formal security proof

Related Work

D. Lazar and N. Zeldovich.

“Alpenhorn: Bootstrapping Secure Communication without Leaking Metadata”. USENIX OSDI 2016. [14]



C. Kocaoğullar et al.

“Pudding: Private User Discovery in Anonymity Networks”. IEEE S&P 2024. [15]



This work



-\(\cup\)

Beginning
of Time

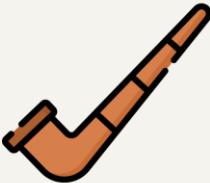
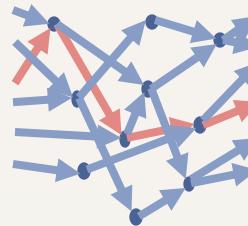
2016

“Use Alpenhorn!”

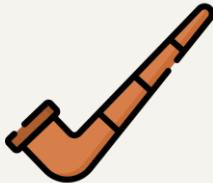
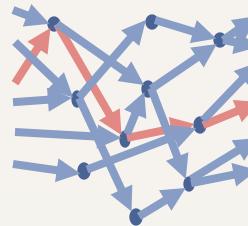
2024

2025

Comparison to related work

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption	Anytrust	Leaks popularity of receivers
	Server-issued precomputed packages	Honest Majority	Differential Privacy Membership Unobservability against clients Relationship Unobservability	High bandwidth (≥ 7 MiB per bootstrapping) No formal security proof
				

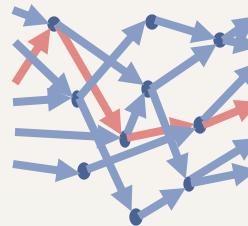
Comparison to related work

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption	Anytrust	Leaks popularity of receivers
	Server-issued precomputed packages	Honest Majority	Differential Privacy Membership Unobservability against clients Relationship Unobservability	High bandwidth (≥ 7 MiB per bootstrapping) No formal security proof
	Notification Matrix			

Comparison to related work

* 2 variants: honest-but-curious, malicious

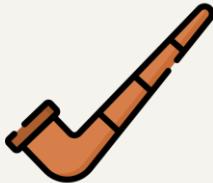
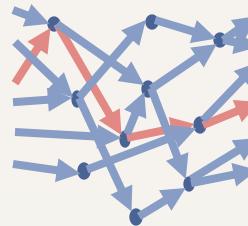
 weaker assumption / stronger notion

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption	Anytrust	Differential Privacy Leaks popularity of receivers
	Server-issued precomputed packages	Honest Majority	Membership Unobservability against clients Relationship Unobservability High bandwidth (≥ 7 MiB per bootstrapping) No formal security proof	
	Notification Matrix	(Authenticated)* Private Information Retrieval (PIR)		

Comparison to related work

* 2 variants: honest-but-curious, malicious

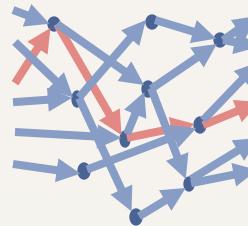
 weaker assumption / stronger notion

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption	Anytrust	Differential Privacy Leaks popularity of receivers
	Server-issued precomputed packages	Honest Majority	Membership Unobservability against clients Relationship Unobservability	High bandwidth (≥ 7 MiB per bootstrapping) No formal security proof
	Notification Matrix	(Authenticated)* Private Information Retrieval (PIR)	Anytrust*	

Comparison to related work

* 2 variants: honest-but-curious, malicious

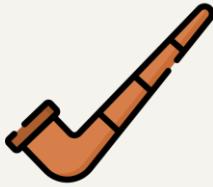
 weaker assumption / stronger notion

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	 MixNet	Identity-Based Encryption	Anytrust	Differential Privacy  Leaks popularity of receivers
	Server-issued precomputed packages	Honest Majority	Membership Unobservability against clients Relationship Unobservability No formal security proof	High bandwidth (≥ 7 MiB per bootstrapping)
Notification Matrix	(Authenticated)* Private Information Retrieval (PIR)	Anytrust*	Communication Unobservability	

Comparison to related work

* 2 variants: honest-but-curious, malicious

 weaker assumption / stronger notion

Notification	Information Retrieval	Trust Assumption	Privacy	Limitations
	Identity-Based Encryption	Anytrust	Differential Privacy	Leaks popularity of receivers
	MixNet Server-issued precomputed packages	Honest Majority	Membership Unobservability against clients Relationship Unobservability	High bandwidth (≥ 7 MiB per bootstrapping) No formal security proof
	Notification Matrix (Authenticated)* Private Information Retrieval (PIR)	Anytrust*	Communication Unobservability	No Membership Unobservability against clients

SABOT

Registration

Public identifier
outside of ACN
known to other clients

$$ID_B$$

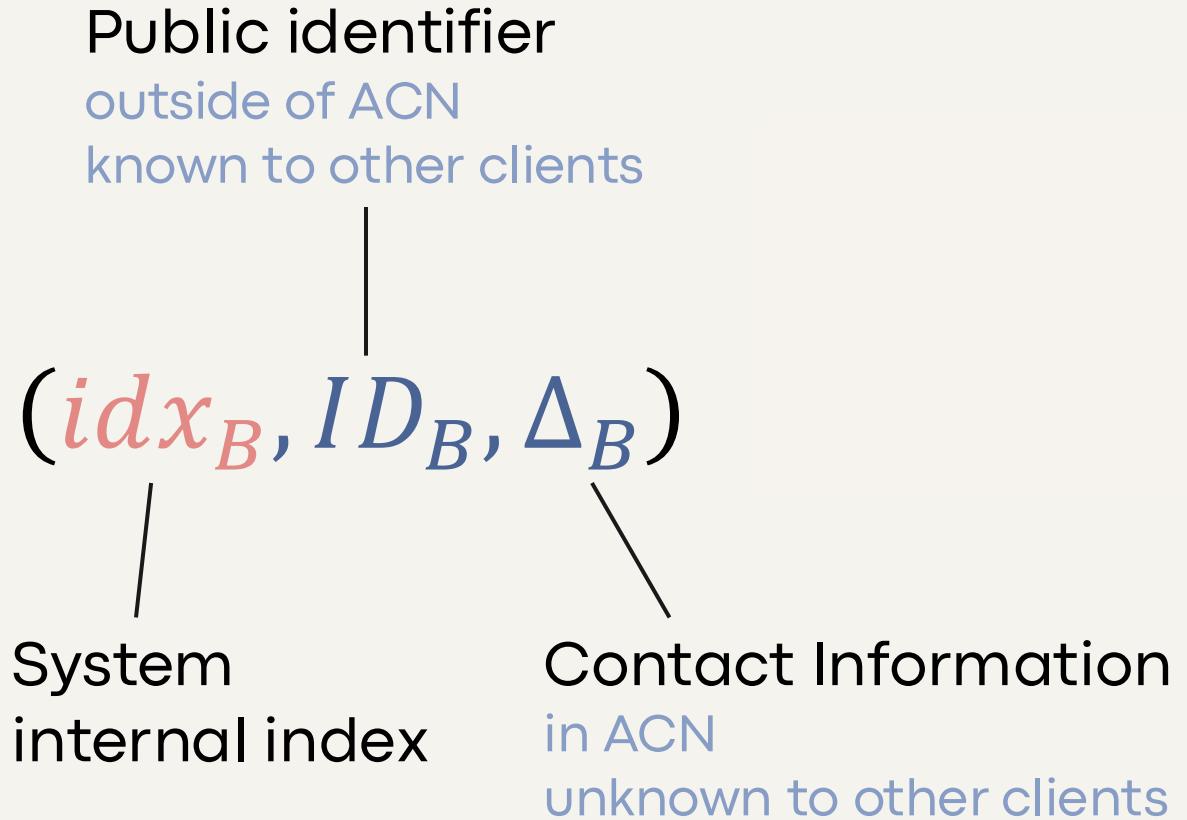
Registration

Public identifier
outside of ACN
known to other clients

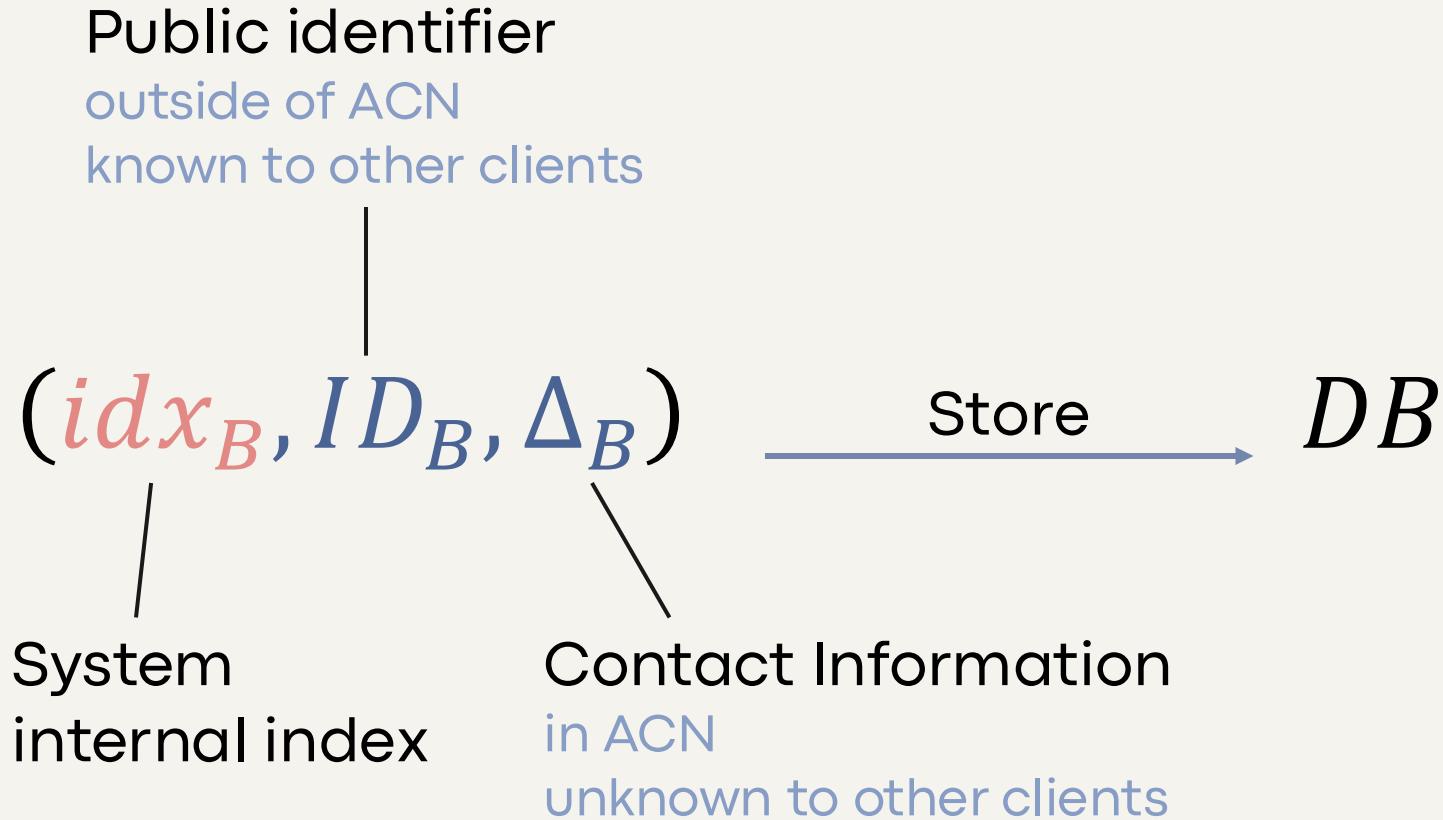
ID_B, Δ_B

Contact Information
in ACN
unknown to other clients

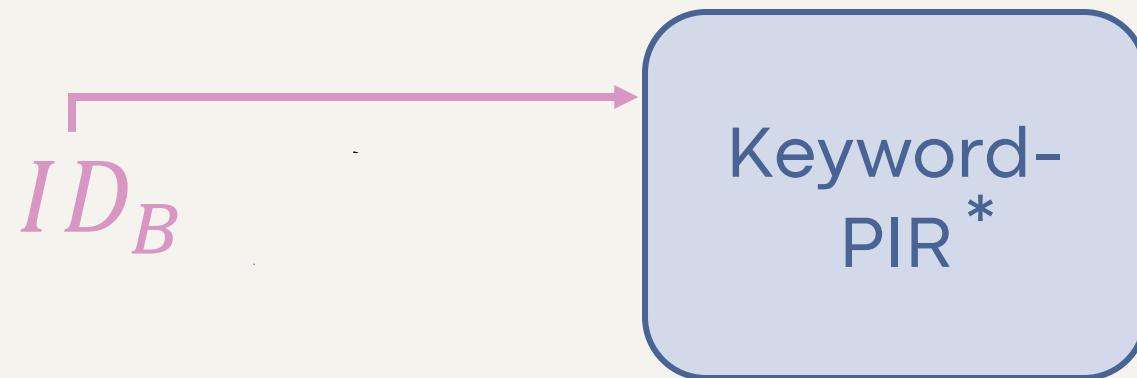
Registration



Registration



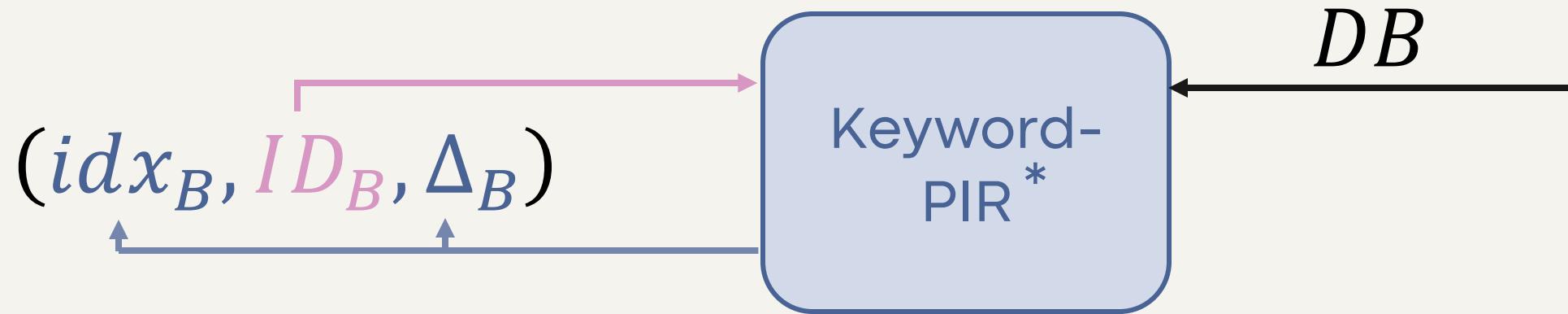
Sender Retrieval



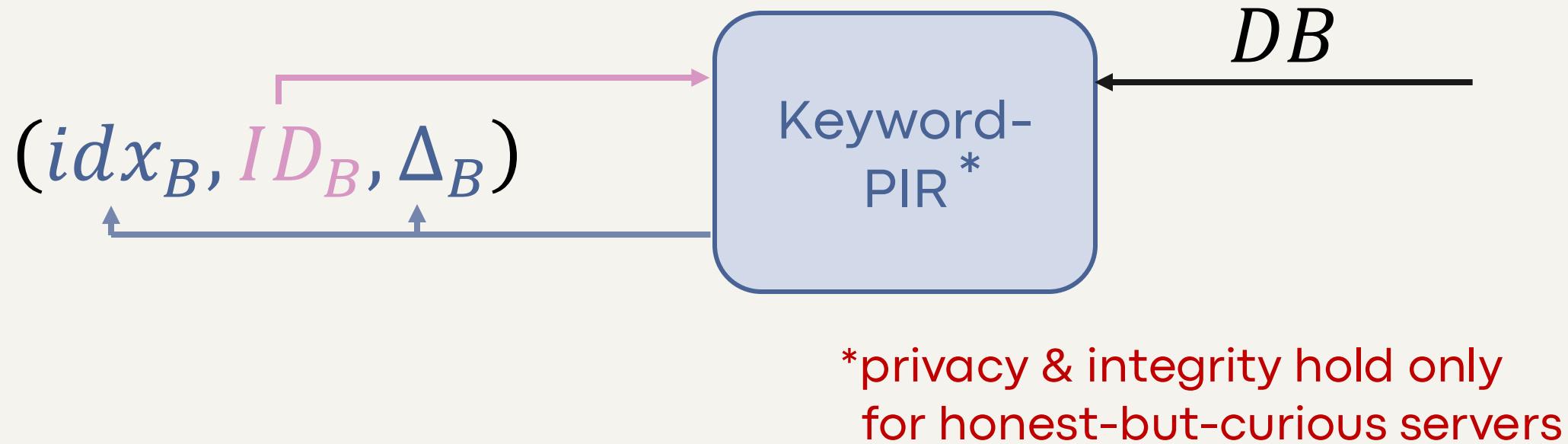
Sender Retrieval



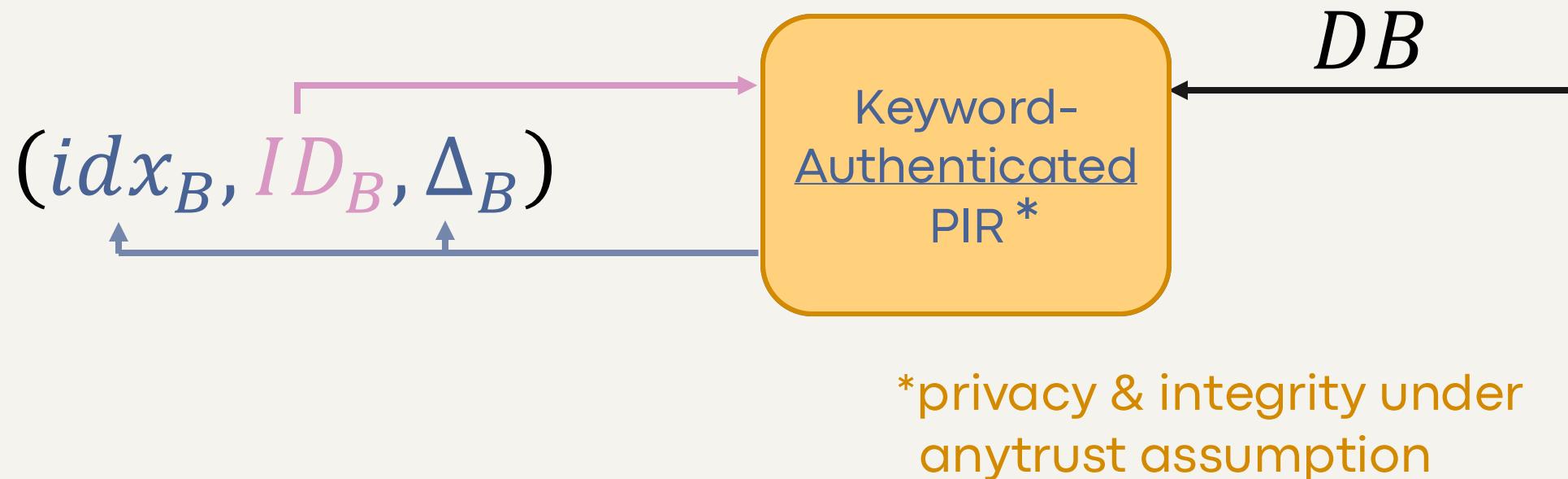
Sender Retrieval



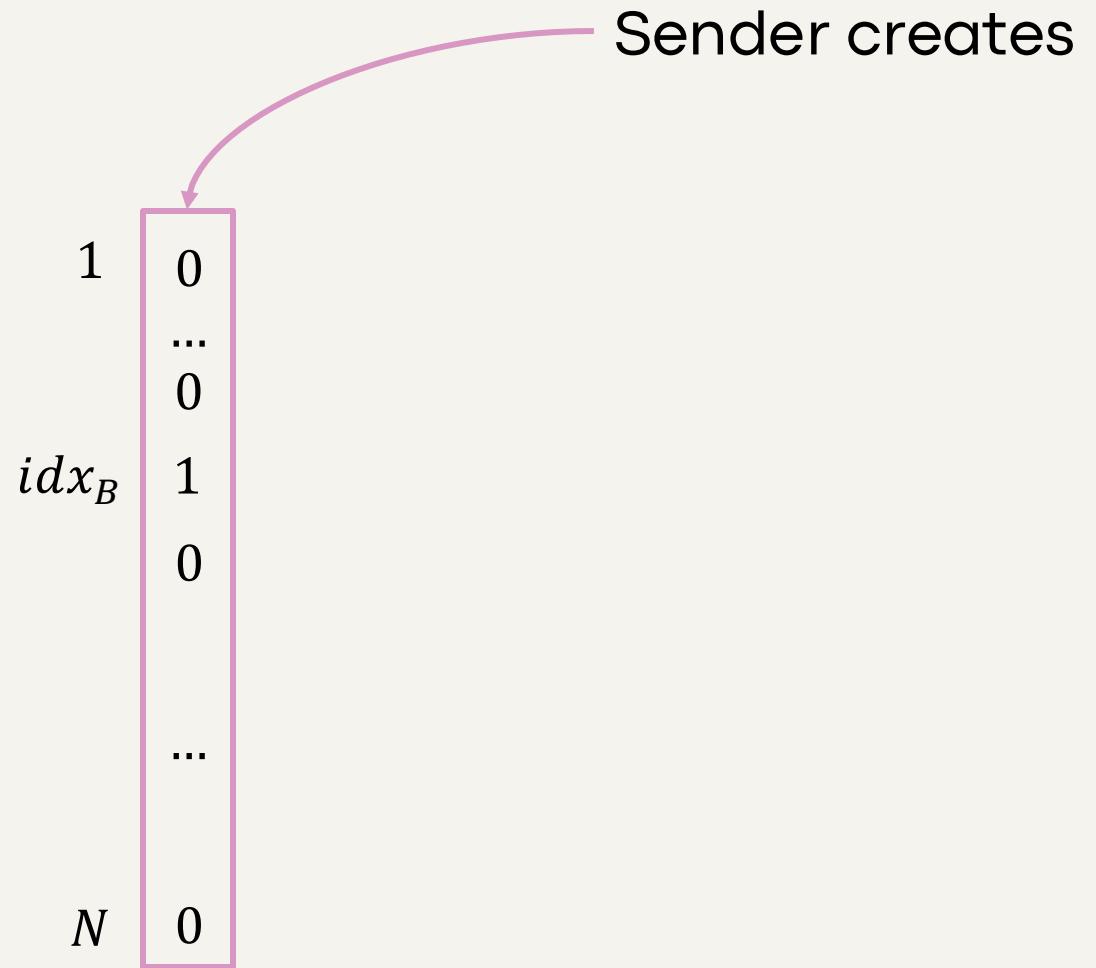
Sender Retrieval



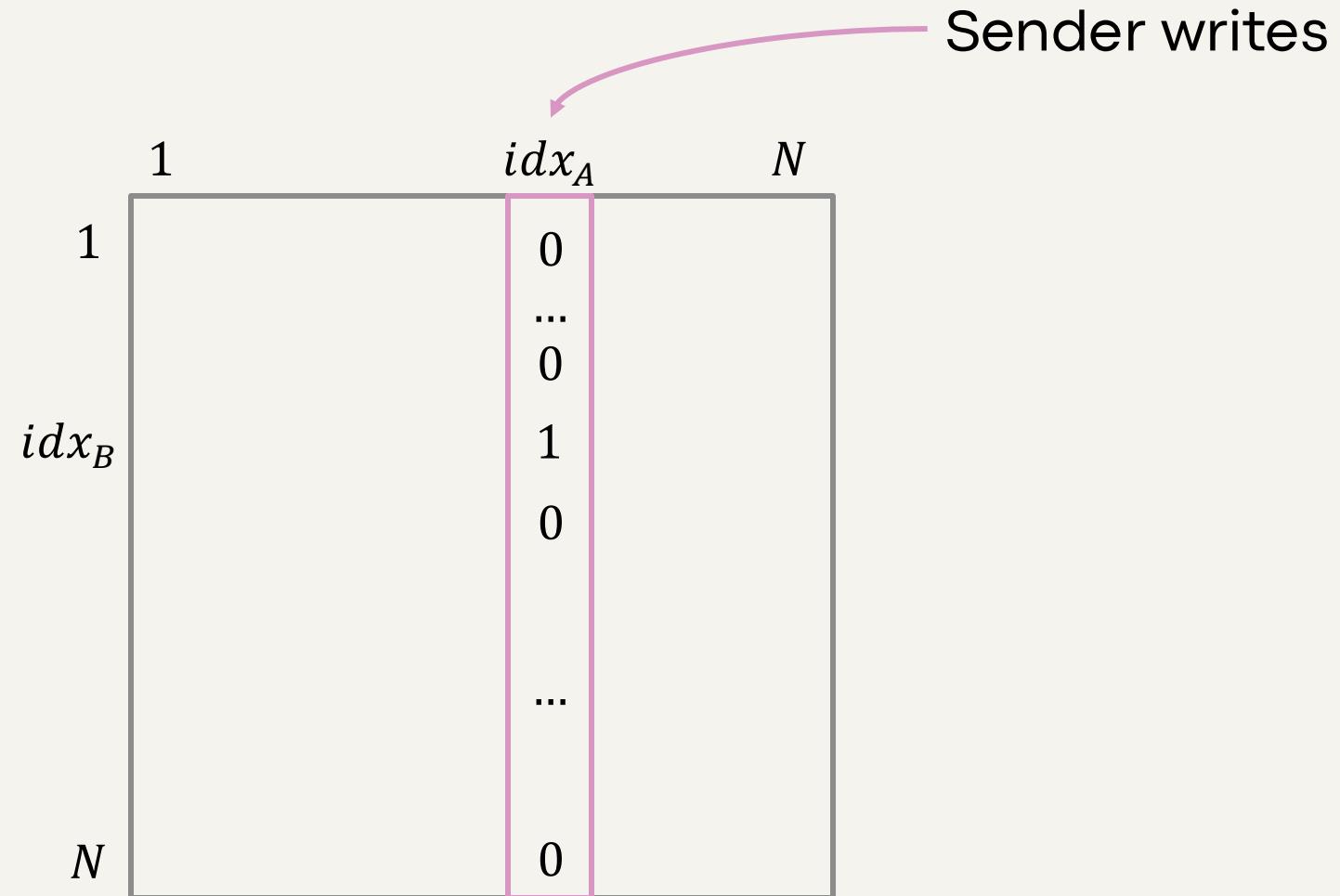
Sender Retrieval



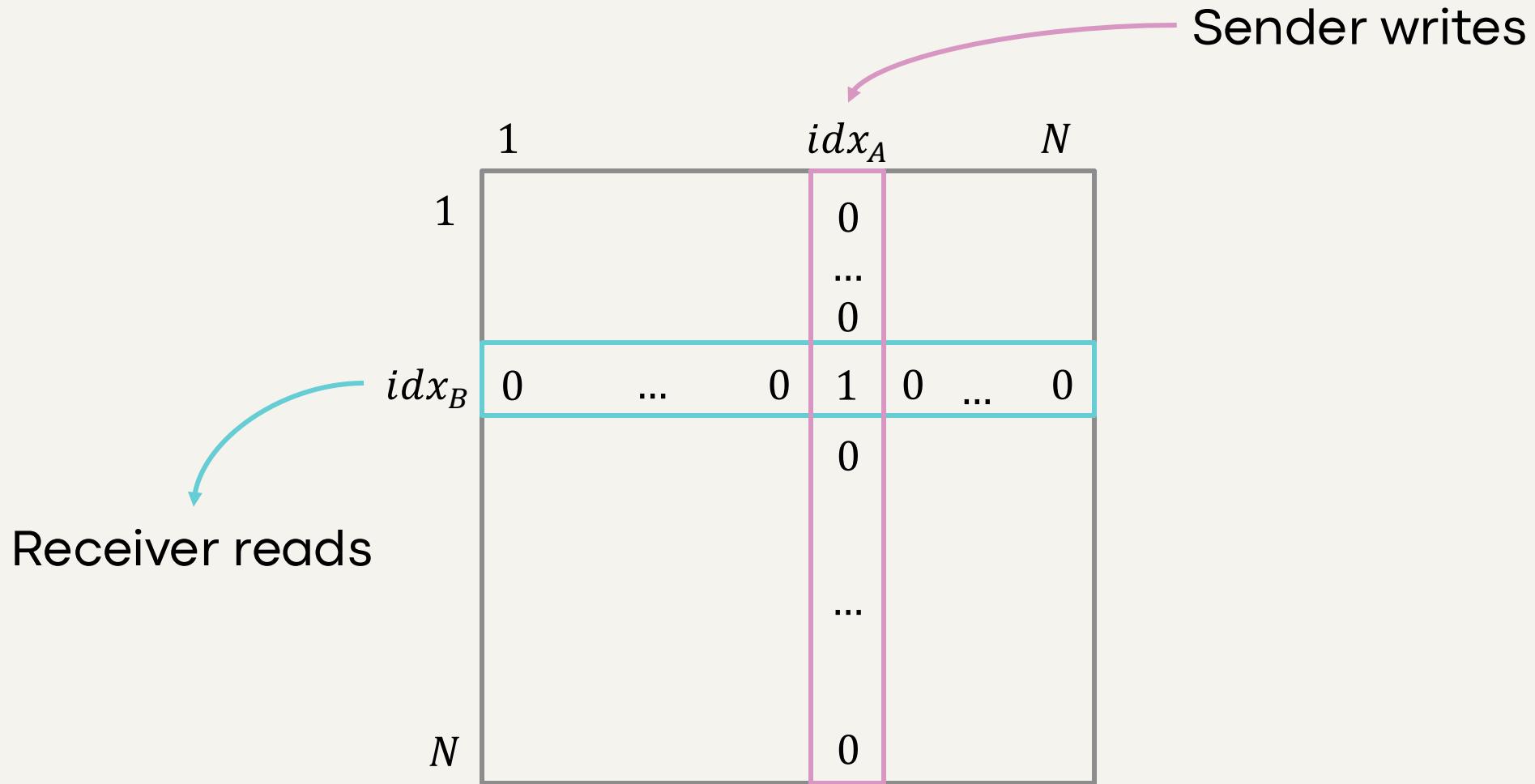
Notification



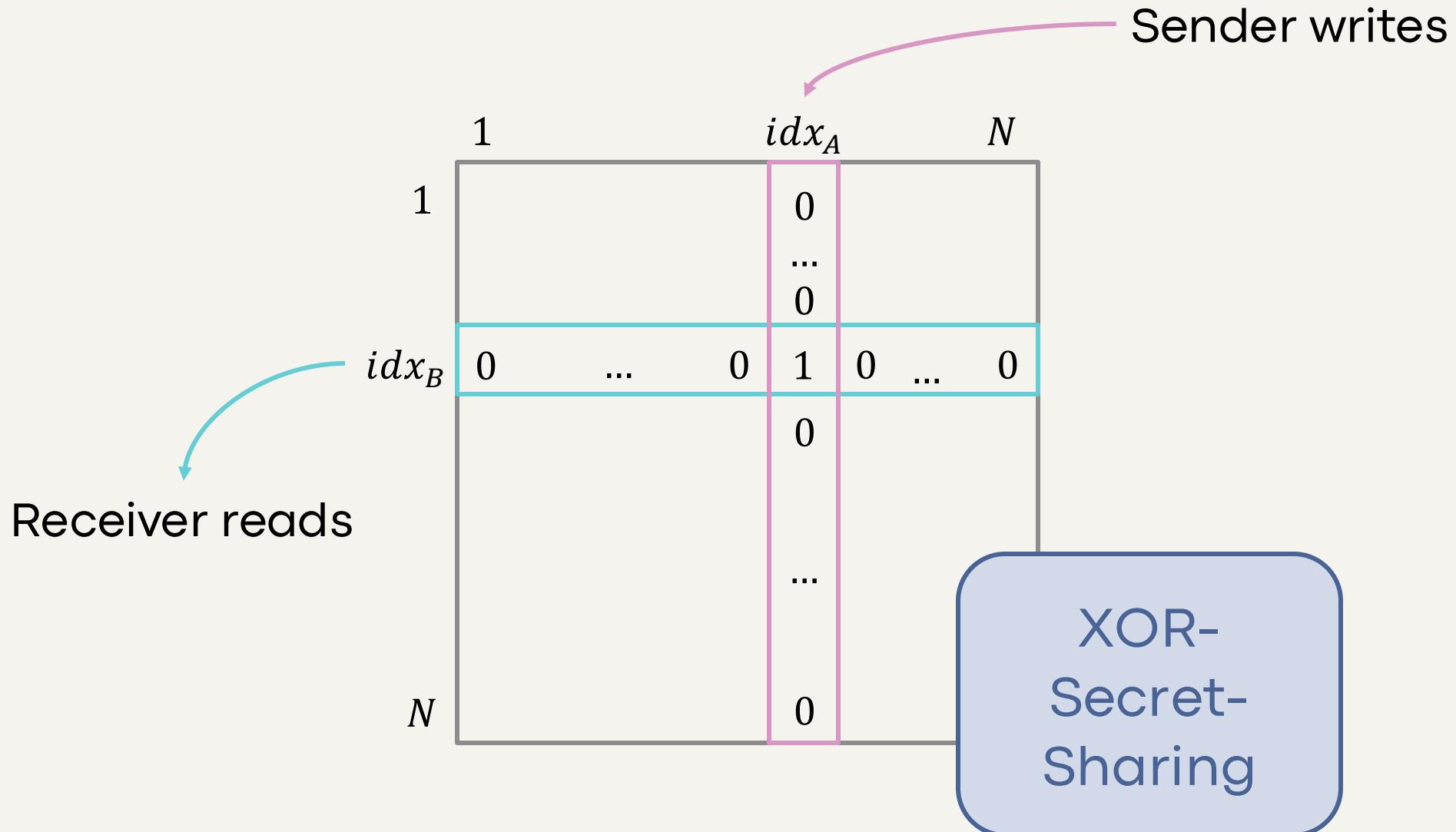
Notification



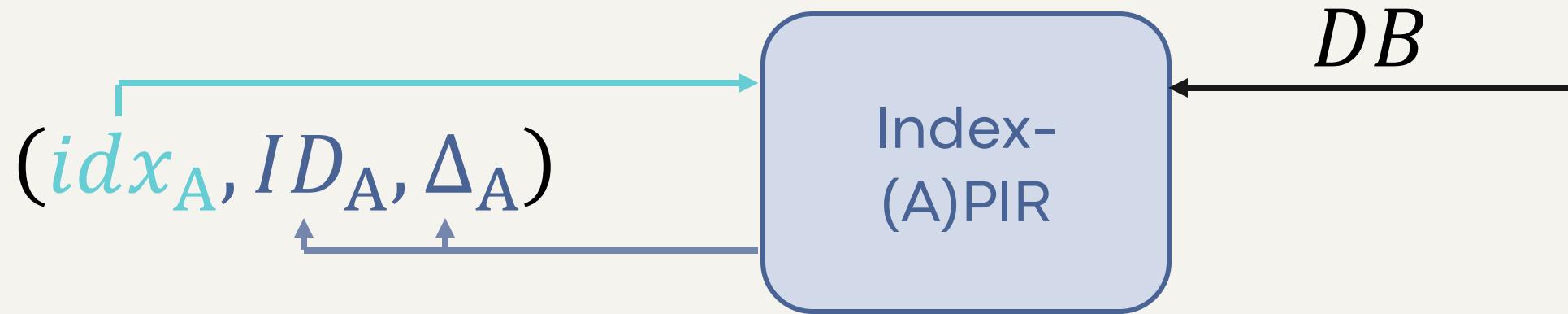
Notification



Notification



Receiver Retrieval



EVALUATION

Bandwidth Comparison



	Number of clients		
	2^{14}	2^{16}	2^{18}
Alpenhorn	7.53 MiB	8.97 MiB	14.10 MiB
Pudding w/o Nym	125.57 KiB	125.57 KiB	125.57 KiB
Pudding w/ Nym	6.99 MiB	6.99 MiB	6.99 MiB

Nym is the underlying Mixnet

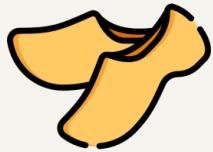
Bandwidth Comparison

	Number of clients			
	2^{14}	2^{16}	2^{18}	
	Alpenhorn	7.53 MiB	8.97 MiB	14.10 MiB
	Pudding w/o Nym	125.57 KiB	125.57 KiB	125.57 KiB
	Pudding w/ Nym	6.99 MiB	6.99 MiB	6.99 MiB

Nym is the
underlying Mixnet

→ No Mixnet,
no privacy!

Bandwidth Comparison



	Number of clients	2^{14}	2^{16}	2^{18}
SABOT_h (1)				
SABOT_h (5)				
SABOT_h (10)				
SABOT_m (1)				
SABOT_m (5)				
SABOT_m (10)				
Alpenhorn		7.53 MiB	8.97 MiB	14.10 MiB
Pudding w/o Nym	125.57 KiB	125.57 KiB	125.57 KiB	
Pudding w/ Nym	6.99 MiB	6.99 MiB	6.99 MiB	



honest-but-curious
setting

malicious
setting

Nym is the
underlying Mixnet

→ No Mixnet,
no privacy!

Bandwidth Comparison



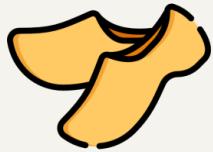
	Number of clients		
	2^{14}	2^{16}	2^{18}
SABOT_h (1)	22.00 KiB	82.28 KiB	322.57 KiB
SABOT_h (5)	5.78 KiB	18.03 KiB	66.29 KiB
SABOT_h (10)	3.73 KiB	9.97 KiB	34.22 KiB
SABOT_m (1)			
SABOT_m (5)			
SABOT_m (10)			
Alpenhorn	7.53 MiB	8.97 MiB	14.10 MiB
Pudding w/o Nym	125.57 KiB	125.57 KiB	125.57 KiB
Pudding w/ Nym	6.99 MiB	6.99 MiB	6.99 MiB

honest-but-curious
setting

malicious
setting

Nym is the
underlying Mixnet

Bandwidth Comparison



	Number of clients		
	2^{14}	2^{16}	2^{18}
SABOT _h (1)	22.00 KiB	82.28 KiB	322.57 KiB
SABOT _h (5)	5.78 KiB	18.03 KiB	66.29 KiB
SABOT _h (10)	3.73 KiB	9.97 KiB	34.22 KiB
SABOT _m (1)	25.76 KiB	86.54 KiB	327.34 KiB
SABOT _m (5)	9.18 KiB	21.89 KiB	70.59 KiB
SABOT _m (10)	7.04 KiB	13.73 KiB	38.41 KiB
Alpenhorn	7.53 MiB	8.97 MiB	14.10 MiB
Pudding w/o Nym	125.57 KiB	125.57 KiB	125.57 KiB
Pudding w/ Nym	6.99 MiB	6.99 MiB	6.99 MiB

honest-but-curious
setting

malicious
setting

Nym is the
underlying Mixnet



Summary

Summary

Anonymous
“out-of-band”
bootstrapping

Summary

Anonymous
“out-of-band”
bootstrapping

Bandwidth Efficiency

Summary

Anonymous
“out-of-band”
bootstrapping

Bandwidth Efficiency

Communication
Unobservability

Summary

Anonymous
“out-of-band”
bootstrapping

Bandwidth Efficiency

Communication
Unobservability

Formal Security Proof
in Semi-Honest Setting

Summary

Anonymous
“out-of-band”
bootstrapping

Bandwidth Efficiency

Communication
Unobservability

Formal Security Proof
in Semi-Honest Setting

Open Questions:

Summary

Anonymous
“out-of-band”
bootstrapping

Bandwidth Efficiency

Communication
Unobservability

Formal Security Proof
in Semi-Honest Setting

Open Questions:

Formal Security in
Malicious Setting?

Summary

Anonymous
“out-of-band”
bootstrapping

Bandwidth Efficiency

Communication
Unobservability

Formal Security Proof
in Semi-Honest Setting

Open Questions:

Formal Security in
Malicious Setting?

Authenticity without
Membership Leakage?

Summary

Anonymous
“out-of-band”
bootstrapping

Bandwidth Efficiency

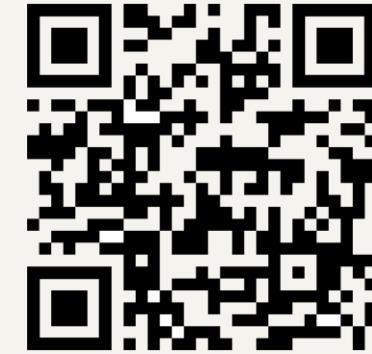
Communication
Unobservability

Formal Security Proof
in Semi-Honest Setting

Open Questions:

Formal Security in
Malicious Setting?

Authenticity without
Membership Leakage?



ia.cr/2025/971

Get in touch:

laura.hetz@inf.ethz.ch

References

- [1] Jelle van den Hooff, David Lazar, Matei Zaharia, and Nickolai Zeldovich. 2015. Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis. In SOSP 2015. ACM.
- [2] Sebastian Angel and Srinath T. V. Setty. Unobservable Communication over Fully Untrusted Infrastructure. In OSDI 2016. USENIX Association.
- [3] Nirvan Tyagi, Yossi Gilad, Derek Leung, Matei Zaharia, and Nickolai Zeldovich. Stadium: A Distributed Metadata-Private Messaging System. In SOSP 2017. ACM.
- [4] David Lazar, Yossi Gilad, and Nickolai Zeldovich. Karaoke: Distributed private messaging immune to passive traffic analysis. In OSDI 2018. USENIX Association.
- [5] Albert Kwon, David Lu, and Srinivas Devadas. XRD: Scalable Messaging System with Cryptographic Privacy. In NSDI 2020. USENIX Association.
- [6] Ludovic Barman, Moshe Kol, David Lazar, Yossi Gilad, and Nickolai Zeldovich. Groove: Flexible Metadata-Private Messaging. In OSDI 2022. USENIX Association.
- [7] Henry Corrigan-Gibbs and Bryan Ford. Dissent: Accountable Anonymous Group Messaging. In CCS 2010. ACM.
- [8] Henry Corrigan-Gibbs, David Isaac Wolinsky, and Bryan Ford. Proactively Accountable Anonymous Messaging in Verdict. In USENIX Security 2013. USENIX Association.
- [9] Ania M. Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. The Loopix Anonymity System. In USENIX Security 2017. USENIX Association.
- [10] Nikolaos Alexopoulos, Aggelos Kiayias, Riivo Talviste, and Thomas Zacharias. MCMix: Anonymous Messaging via Secure Multiparty Computation. In USENIX Security 2017. USENIX Association.
- [11] Saba Eskandarian and Dan Boneh. 2022. Clarion: Anonymous Communication from Multiparty Shuffling Protocols. In NDSS 2022. The Internet Society.

References

- [12] Adithya Vadapalli, Kyle Storrier, and Ryan Henry. Sabre: Sender Anonymous Messaging with Fast Audits. In IEEE SP 2022. IEEE.
- [13] Saba Eskandarian, Henry Corrigan-Gibbs, Matei Zaharia, and Dan Boneh. Express: Lowering the Cost of Metadata-hiding Communication with Cryptographic Privacy. In USENIX Security 2021. USENIX Association.
- [14] David Lazar and Nickolai Zeldovich. Alpenhorn: Bootstrapping Secure Communication without Leaking Metadata. In OSDI 2016. USENIX Association.
- [15] Ceren Kocaoğullar, Daniel Hugenroth, Martin Kleppmann, and Alastair R Beresford. Pudding: Private User Discovery in Anonymity Networks. In IEEE SP 2024. IEEE.

This presentation has been designed using resources from PowerPoint and icons made by Freepik from www.flaticon.com.