

Privacy

Data minimisation

Subhashis Banerjee, Subodh Sharma

Data minimisation (DM) (aka “minimum disclosure”)

- Share only the minimum amount of data required for the purpose
 - e.g., to prove that “I am over 18 years” without disclosing my exact DOB or unique ID
 - e.g., sharing only anonymised information for statistical purposes
- Many techniques and concepts:
 1. Zero-knowledge proofs
 2. Anonymity and unlinkability: virtual identities, anonymous credentials, etc.
 3. Database anonymisation

DM1: Zero-knowledge proofs

- Techniques to prove a statement *without revealing anything other than the statement itself* (Goldwasser et al. '89)
 - e.g., to prove that “I know the secret key corresponding to a given public key”, without revealing the secret key

Sudoku in Zero Knowledge

Goal: Prover wants to prove to the verifier that it knows the solution* to the following Sudoku puzzle, without revealing the solution to the verifier.

	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

* For a correct solution to a Sudoku problem, each row, column and box must contain all the numbers from 1-9

Sudoku in Zero Knowledge

- Step 1 (**Commitment**): Prover writes the solution for each cell in one of the 81 cards placed face down over the Sudoku grid. Since the cards are numbered, the prover is *committed* to the location of each card.



Face up



Face down

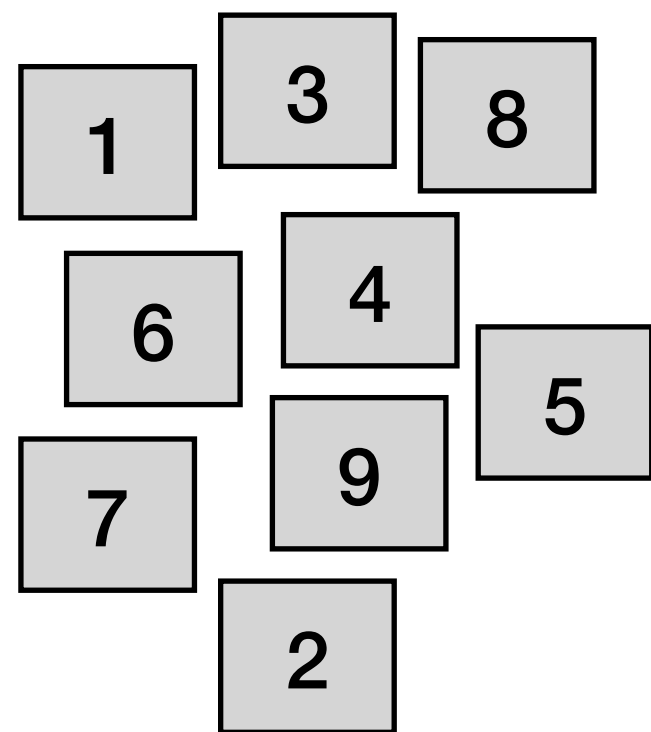
	1	2	3	4	5	6	7	8	9
A	A1	A2	A3	A4	A5	A6	A7	A8	A9
B	B1	B2	B3	B4	B5	B6	B7	B8	B9
C	C1	C2	C3	C4	C5	C6	C7	C8	C9
D	D1	D2	D3	D4	D5	D6	D7	D8	D9
E	E1	E2	E3	E4	E5	E6	E7	E8	E9
F	F1	F2	F3	F4	F5	F6	F7	F8	F9
G	G1	G2	G3	G4	G5	G6	G7	G8	G9
H	H1	H2	H3	H4	H5	H6	H7	H8	H9
I	I1	I2	I3	I4	I5	I6	I7	I8	I9

Note: Commitment is both **binding** and **hiding**!

Sudoku in Zero Knowledge

- Step 2 (**Challenge/Response**): Verifier challenges to open a random column/row/box. Prover shuffles the cards in the requested column/row/box and reveals face up. Verifier checks that all 1-9 are present and all other face-down cards are intact. Repeat k times.

Shuffled cards of the first column revealed face up!



	1	2	3	4	5	6	7	8	9
A		A2	A3	A4	A5	A6	A7	A8	A9
B		B2	B3	B4	B5	B6	B7	B8	B9
C	3	C2	C3	C4	C5	C6	C7	C8	C9
D	4	D2	D3	D4	D5	D6	D7	D8	D9
E	8	E2	E3	E4	E5	E6	E7	E8	E9
F		F2	F3	F4	F5	F6	F7	F8	F9
G	9	G2	G3	G4	G5	G6	G7	G8	G9
H	7	H2	H3	H4	H5	H6	H7	H8	H9
I		I2	I3	I4	I5	I6	I7	I8	I9

Original problem

	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Sudoku in Zero Knowledge

- Step 3 (**Final Reveal**): Prover reveals all non-empty cells in the original Sudoku problem to show that he has actually solved the given problem, and not some other problem.

	1	2	3	4	5	6	7	8	9
A	A1	A2	A3	A4	A5	A6	6	8	A9
B	B1	B2	B3	B4	7	3	B7	B8	9
C	3	C2	9	C4	C5	C6	C7	4	5
D	4	9	D3	D4	D5	D6	D7	D8	D9
E	8	E2	3	E4	5	E6	9	E8	2
F	F1	F2	F3	F4	F5	F6	F7	3	6
G	9	6	G3	G4	G5	G6	3	G8	8
H	7	H2	H3	6	8	H6	H7	H8	H9
I	I1	2	8	I4	I5	I6	I7	I8	I9

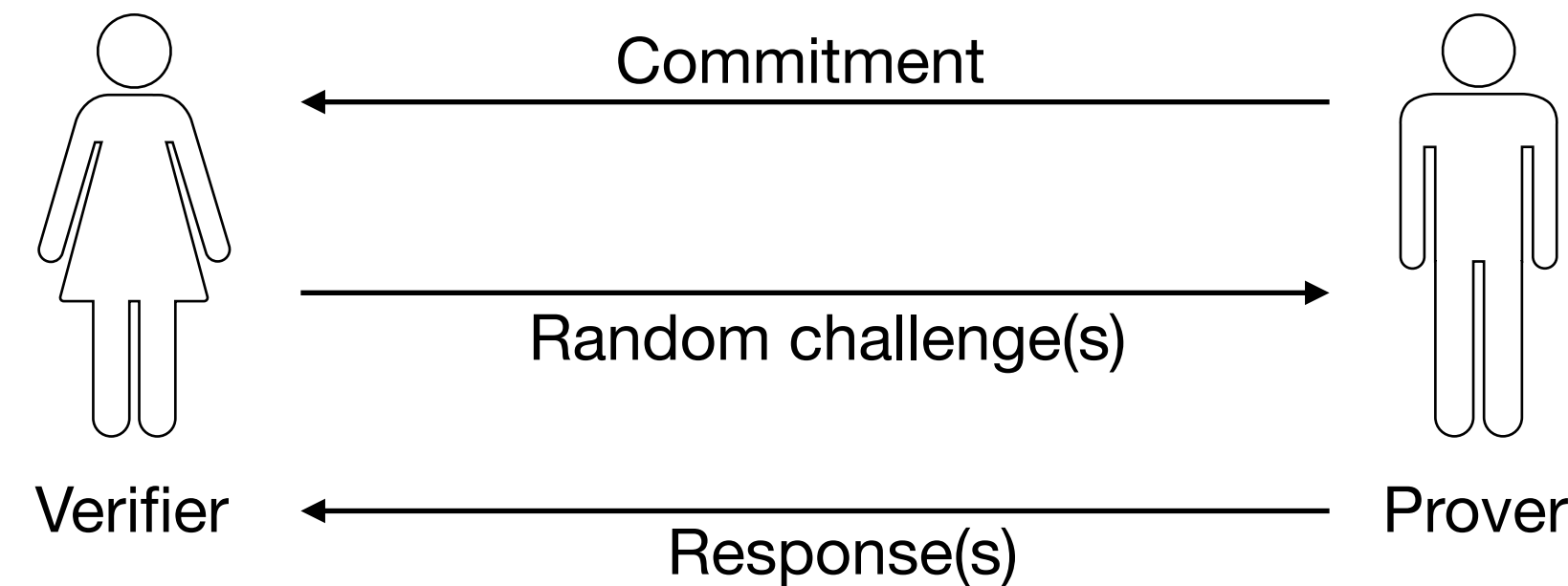
Verifier is convinced that prover knows the solution but does not learn *anything* about the solution.

Original problem

	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Zero-knowledge proofs: Summary

- Typical structure

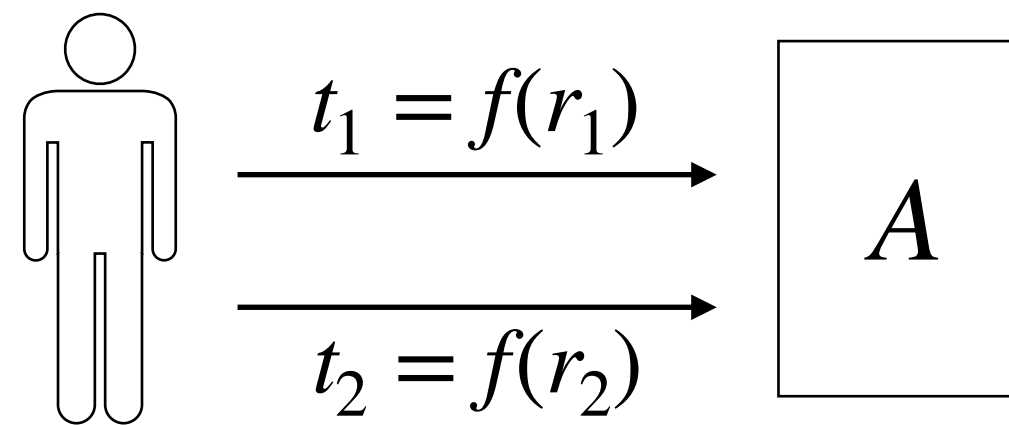


- Commitment with binding+hiding properties is a cryptographic construct too ([Pedersen '91](#))
- Interactive ZKPs can be made non-interactive using one-way hash functions instead of random challenges ([Fiat & Shamir '86](#))
- **All practical statements* can be proved in zero knowledge with overwhelming probability** ([Goldreich et al. '91](#))

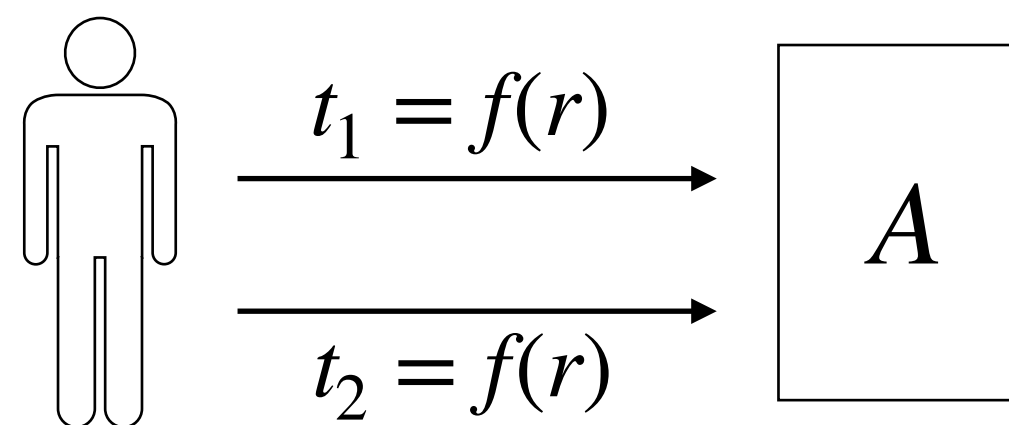
* All NP statements, i.e., which can be verified in polynomial time

DM2: Anonymity and unlinkability

- *Anonymity*: The state of not being identifiable in a set of individuals
- *Unlinkable anonymity*: Transactions do not reveal individuals' true identities and even multiple transactions by the same individual are unlinkable

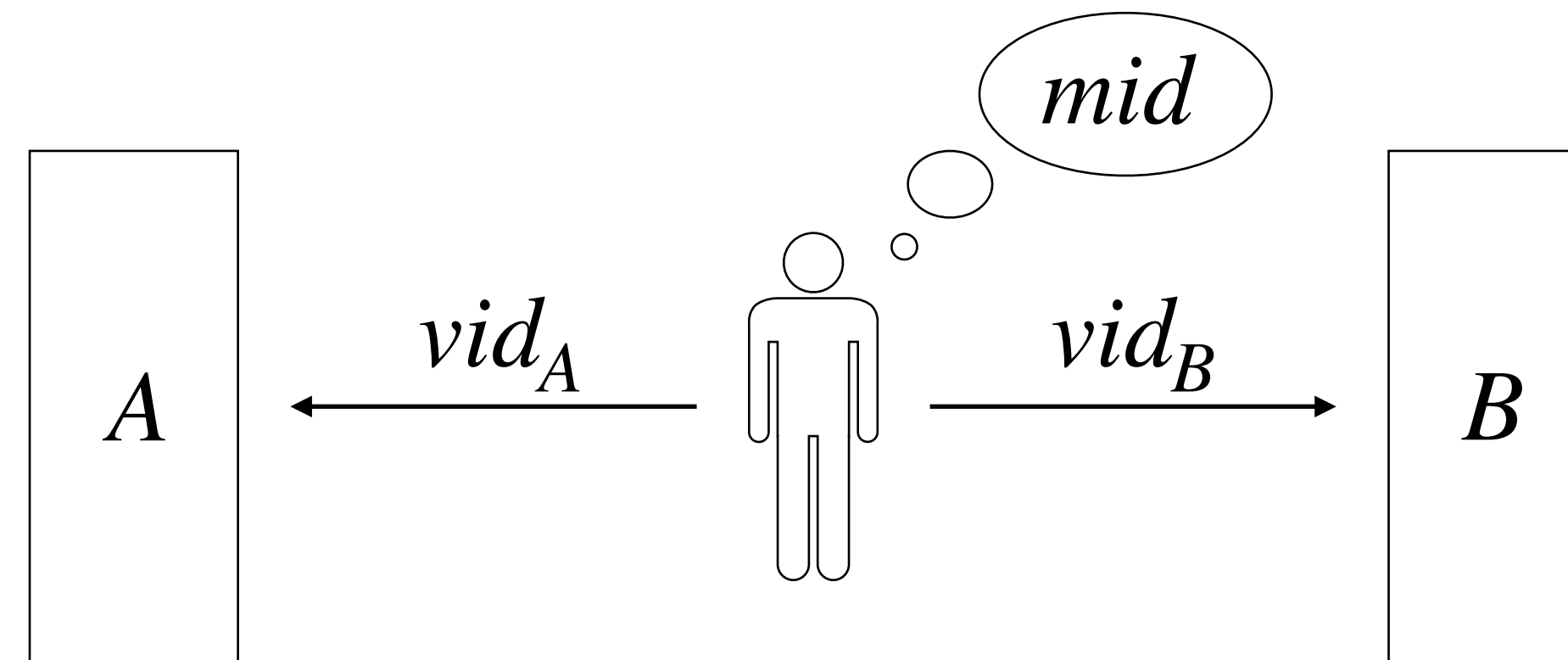


- *Linkable anonymity*: Transactions do not reveal individuals' true identities but multiple transactions by the same individual are linkable



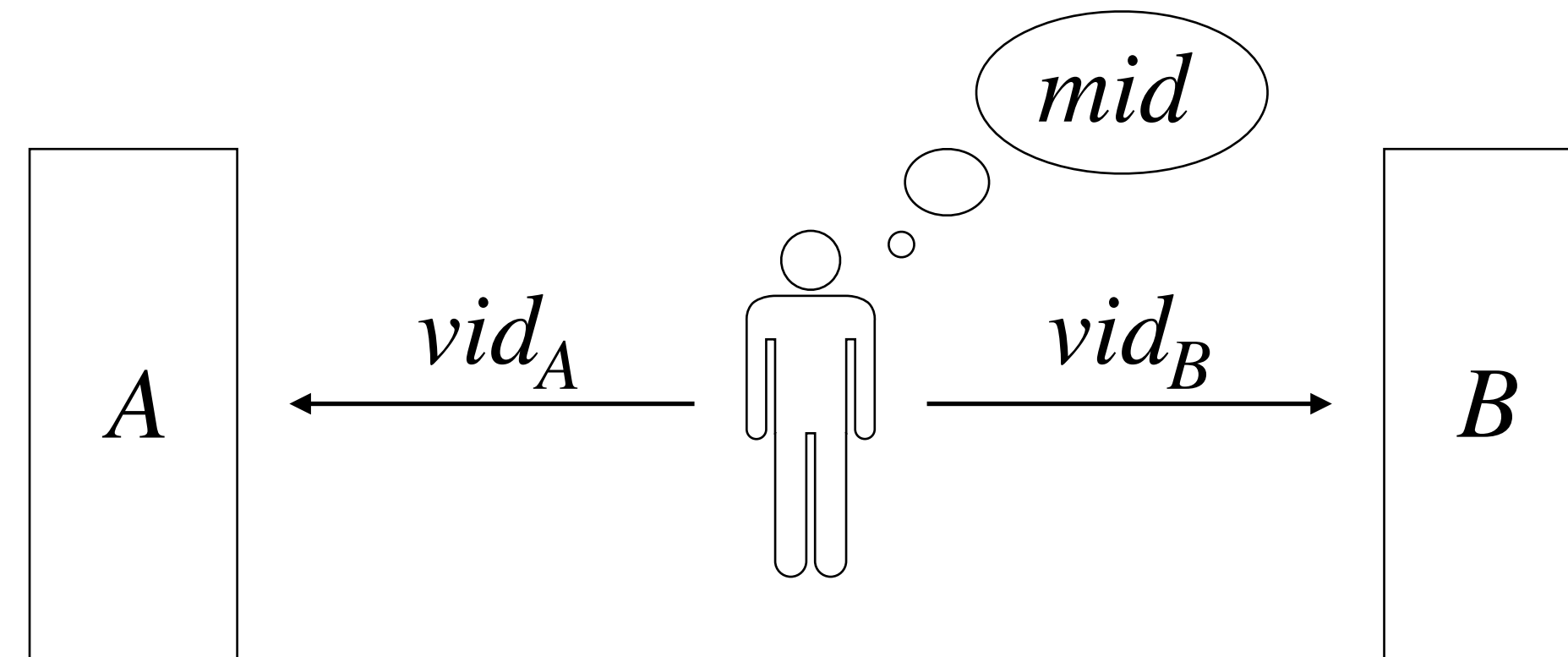
Virtual identities

- Individuals own a master identity and generate random looking, completely unlinkable virtual identities for different organisations ([Chaum '85](#))



- Unlinkable anonymity for inter-organisation transactions / linkable or unlinkable anonymity for intra-organisation transactions
- Purpose-limited linkability by a trusted authority (for genuine reasons, accountability)

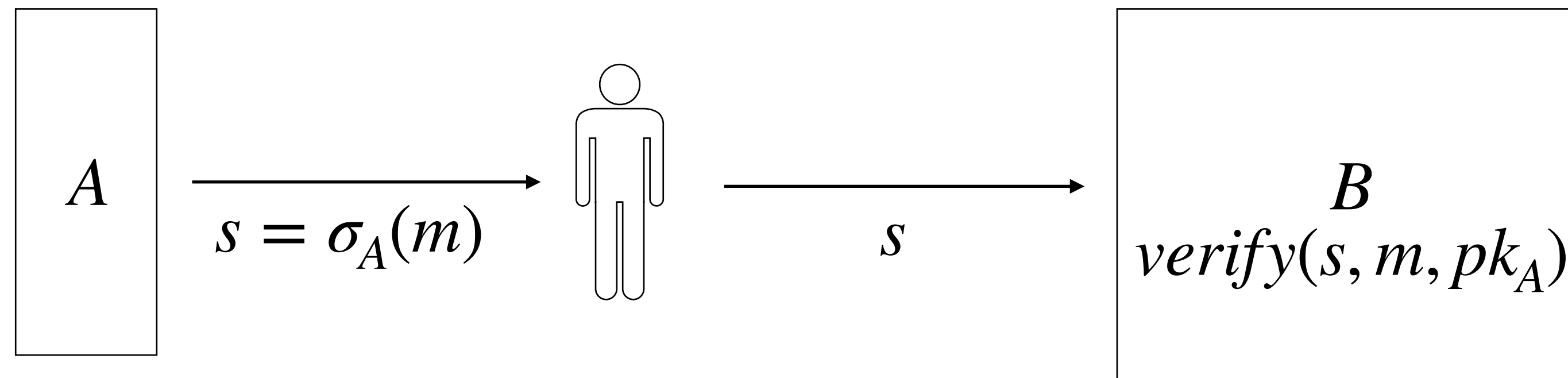
Anonymous credentials



- What if the individual wants to show some credentials obtained from A to B , without allowing A or B to link vid_A and vid_B (e.g., A =college, B =employer)?

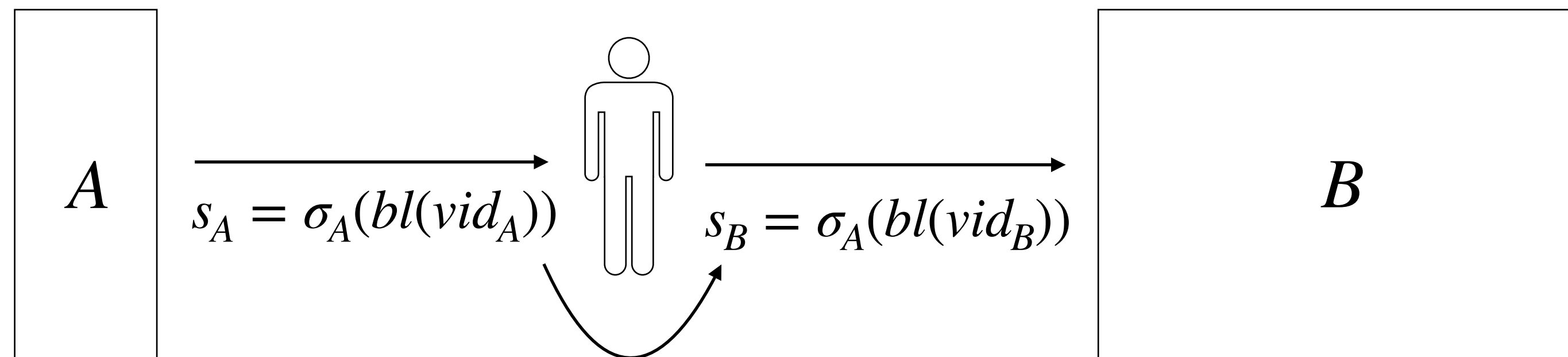
Anonymous credentials

- Regular credentials: Based on *digital signatures* that are unforgeable



No one except A can forge a signature that passes the verification

- Anonymous credentials: Often based on *blind signatures* that are transformable (Chaum '85)



No one can present a signature on a *vid* unless they obtained a signature on another *vid* they own

e.g. $s_A = \sigma_A("vid_A \text{ has degree } X") \longrightarrow s_B = \sigma_A("vid_B \text{ has degree } X")$

DM3: Database anonymisation

- Data minimisation technique to allow analytics on DBs while preserving anonymity
- Hide personally identifiable information by adding noise, suppressing info or coarsening data

Name	Age	Sex	Height	Weight	Location	HIV
Alice	15	F	5.5	84	Rohila Apartments, Pune	Yes
Bob	28	M	5.1	58	Bldg X, DLF Phase 3, GG	No
Charles	34	M	5.9	65	Sameer Bungalow, Delhi	No
David	43	M	6.1	76	55, Sunset Blvd, Mumbai	No

Medical Database

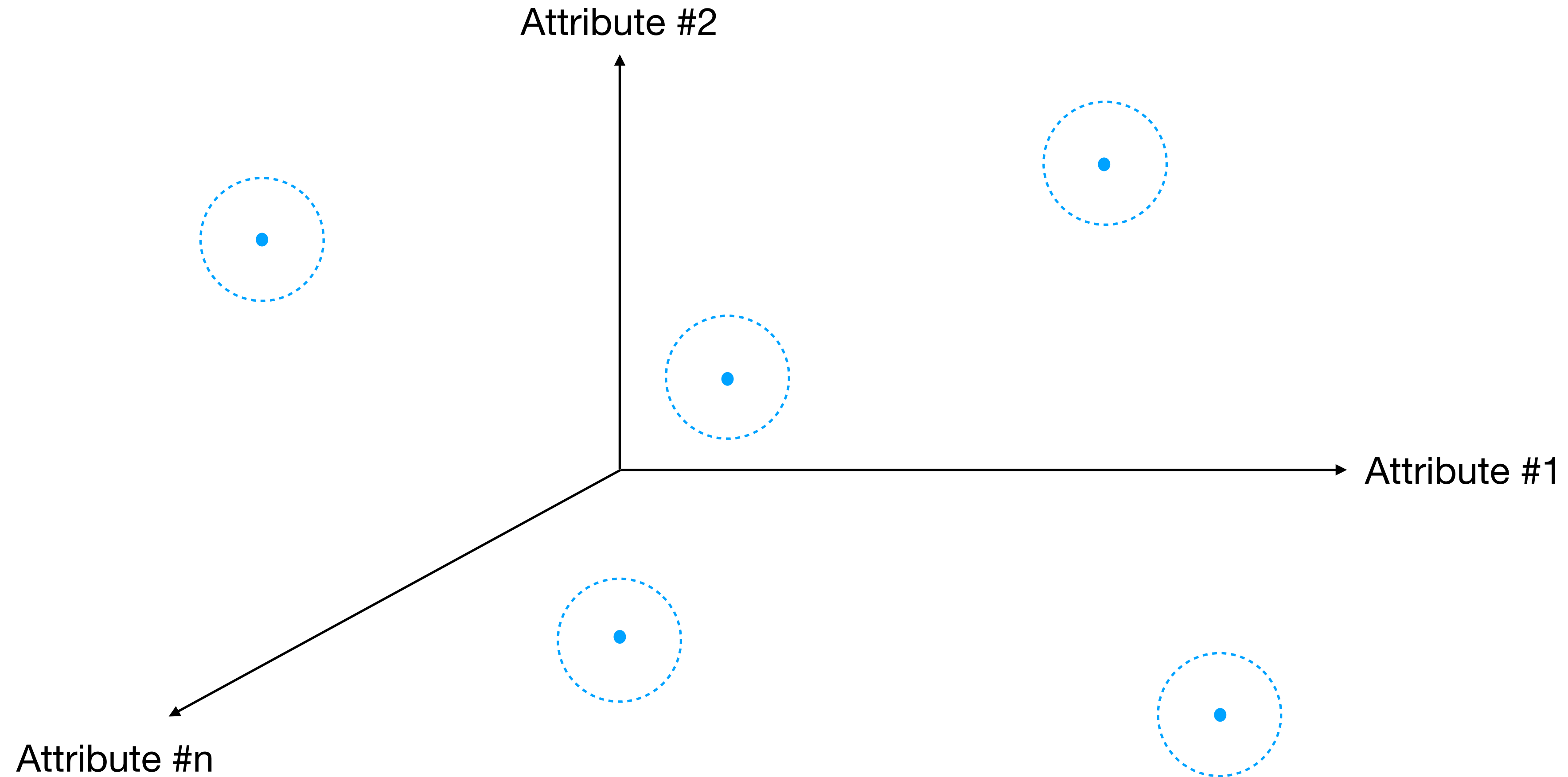


Name	Age	Sex	Height	Weight	Location	HIV Status
*	15-20	F	5.5-6.0	80-85	Pune	Yes
*	25-30	M	5.0-5.5	55-60	Gurgaon	No
*	30-35	M	5.5-6.0	60-65	Delhi	No
*	40-45	M	6.0-6.5	75-80	Mumbai	No

Anonymised Medical Database

- Many notions: k -anonymity, l -diversity, etc.

Anonymisation is a myth



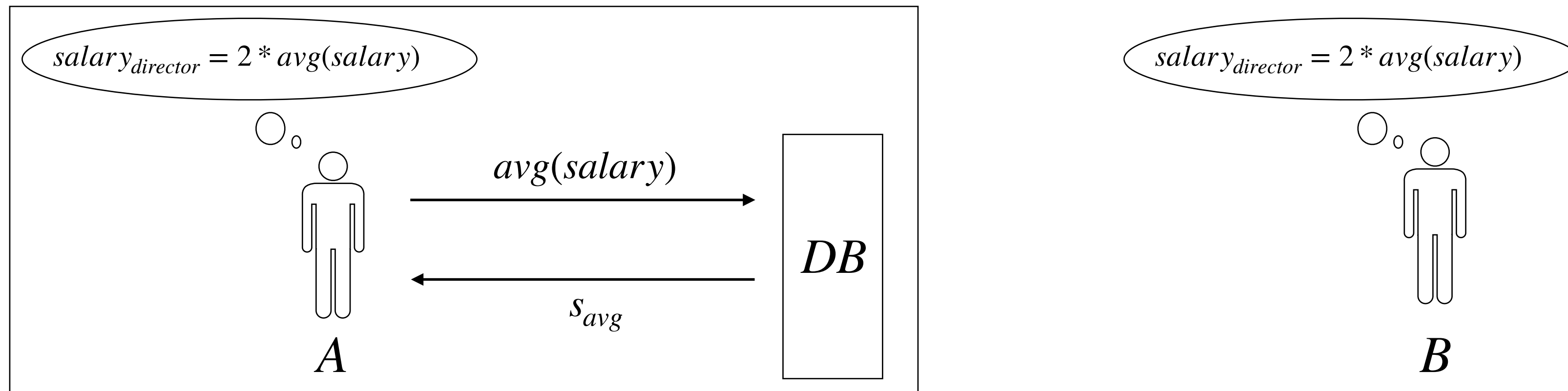
Individuals map to points in a sparse high-dimensional space where they are uniquely identifiable even after adding a lot of noise.

Anonymisation is a myth

- De-anonymisation attacks on anonymised social network data, location data, writing style, source code, browser history, etc., exist. ([Narayanan et al. '19](#))
- *Theoretical bottlenecks:* Given a database with n rows, if the adversary is allowed to obtain answers to $O(n)$ subset-sum queries, it can **reconstruct the entire database** (unless you add an unacceptable amount of noise) ([Dinur & Nissim '03](#))
- *Rough intuition:* Solve a bunch of linear equations to derive individual values from aggregate answers

Impossibility of absolute privacy

Absolute privacy goal (aka inferential privacy): A should not obtain any information about an individual that B cannot obtain without access to DB

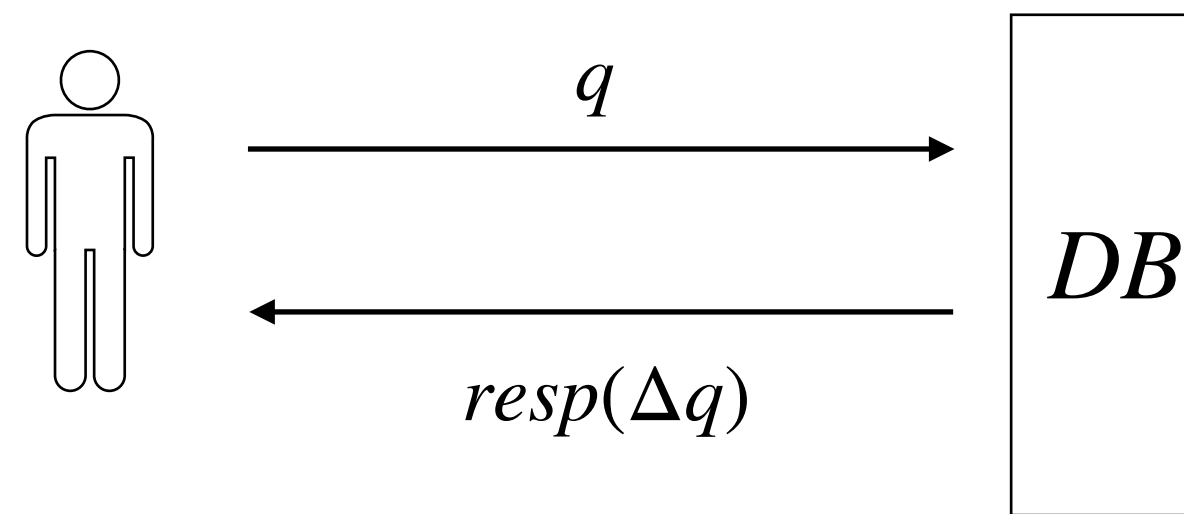


If the adversary has arbitrary side-information, above absolute privacy goal is impossible to achieve. (Dwork '05)

Observe: Privacy of director's salary is compromised even if the director is not in the DB

Changing the goalpost: differential privacy

Differential privacy goal: Database should answer such that the *additional* privacy risk any individual incurs by participating in the database is minimal.



Query q 's sensitivity Δq measures how much the answer for q can change w.r.t. changes in only one row

Interactively calibrate noise as per query sensitivity to maintain user's differential privacy

Limitations of differential privacy

- As query sensitivity increases, noise increases
- DP mechanisms for different types of queries need to be specially designed
- Cannot easily answer many many queries (although some sophisticated noise addition techniques allow answering many queries of a special type)
- How to prevent community-level profiling (cf. Cambridge Analytica)?
- Not suitable for non-statistical uses