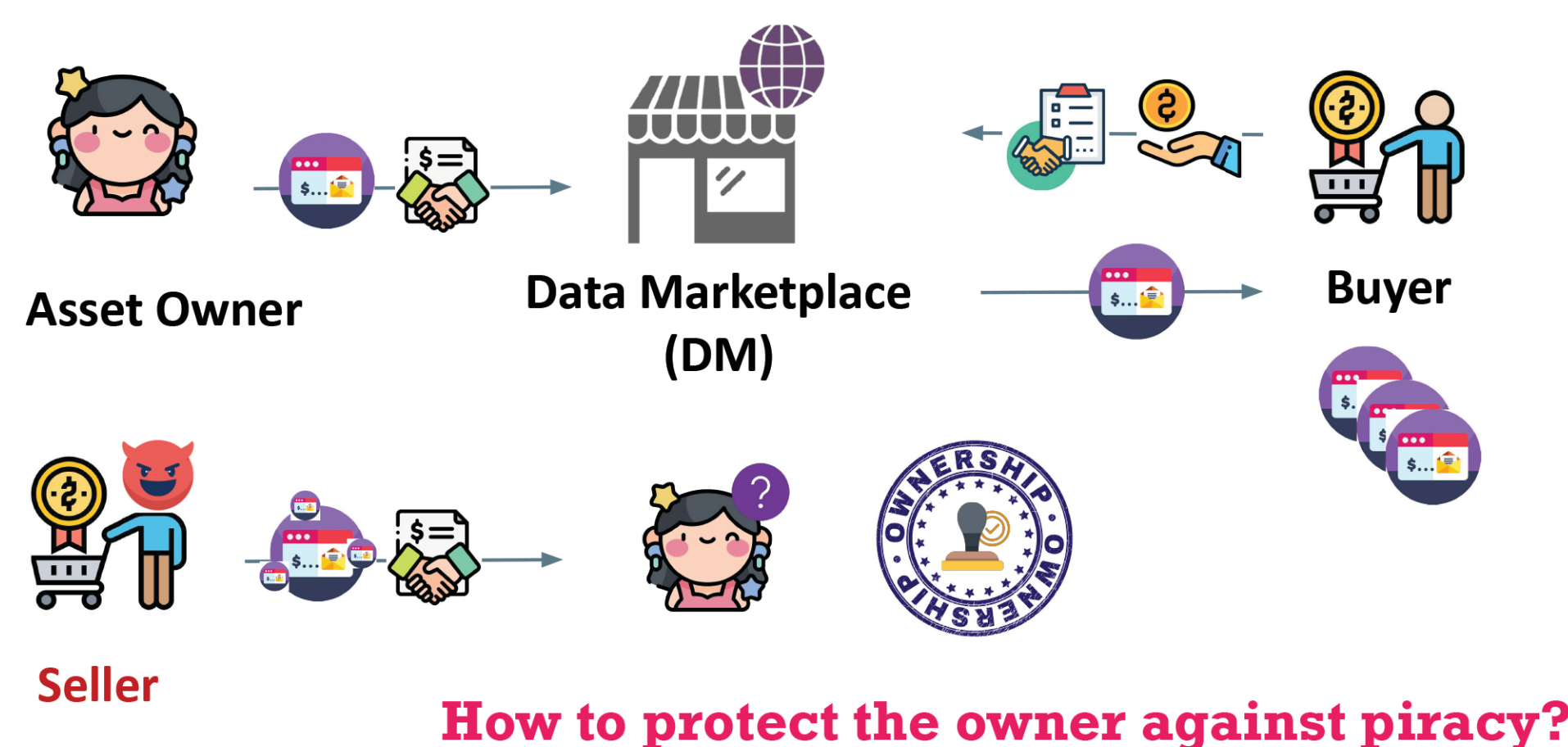
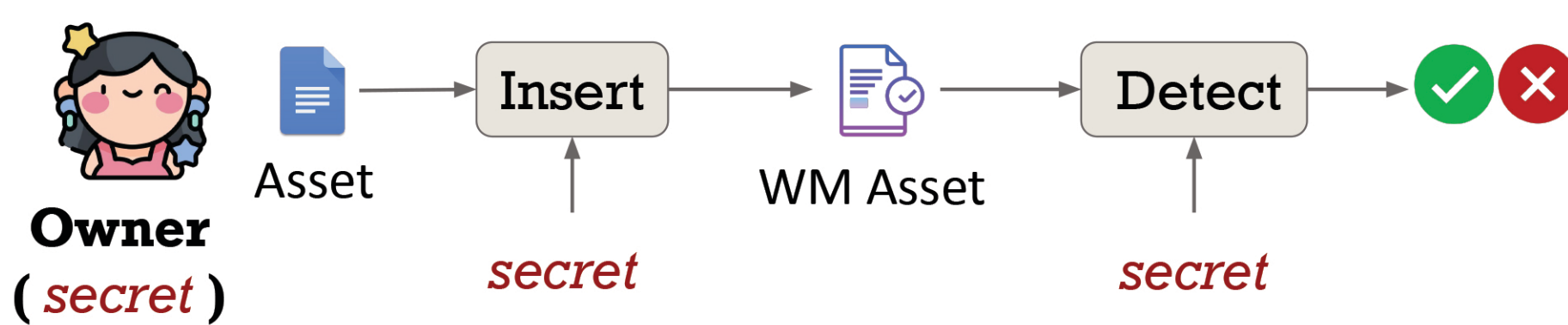


(In Submission)

Introduction



Ownership via Watermarking



Limitation: Public Verifiability

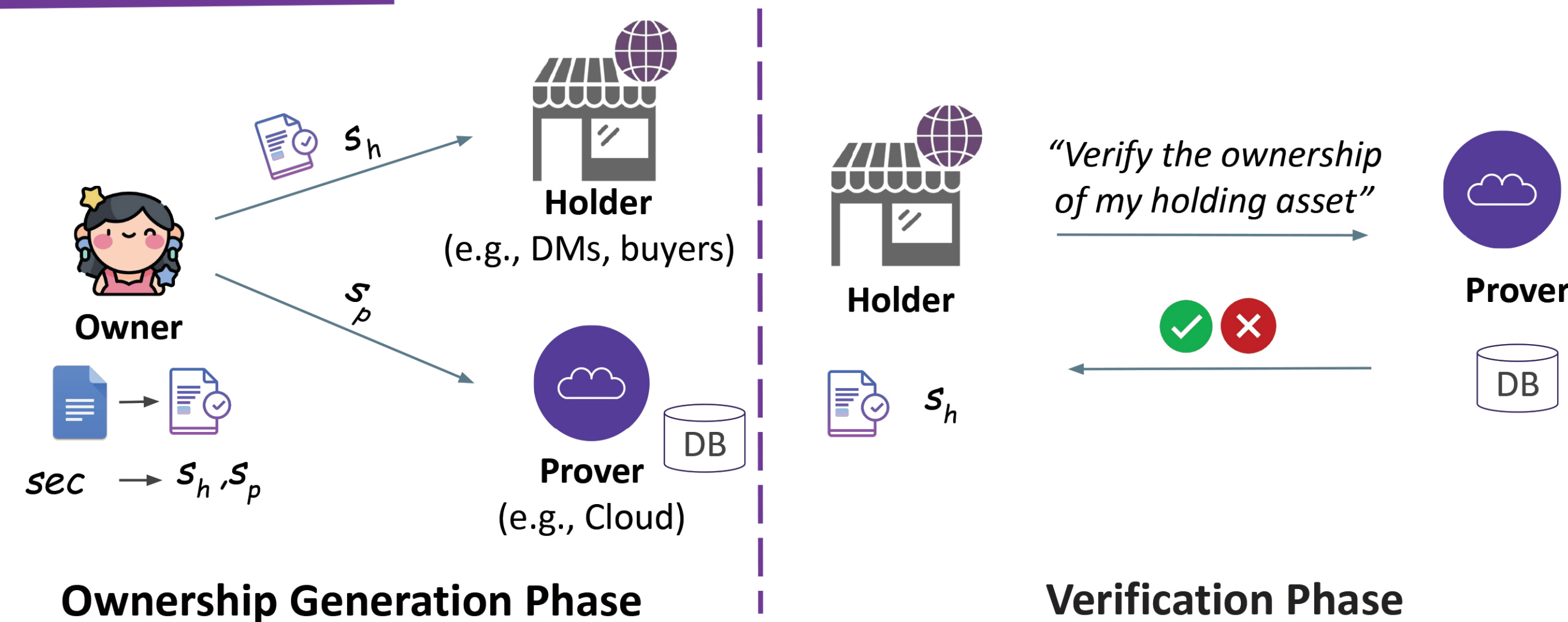
- Scenario :** To detect a watermark on an asset,
- Owner **has to reveal** the watermarking secret;
 - **Only** the intended party (e.g., DM) can run the detection algorithm and verify the claim; and
 - Public verification can be done **only once**.

Existing Solutions

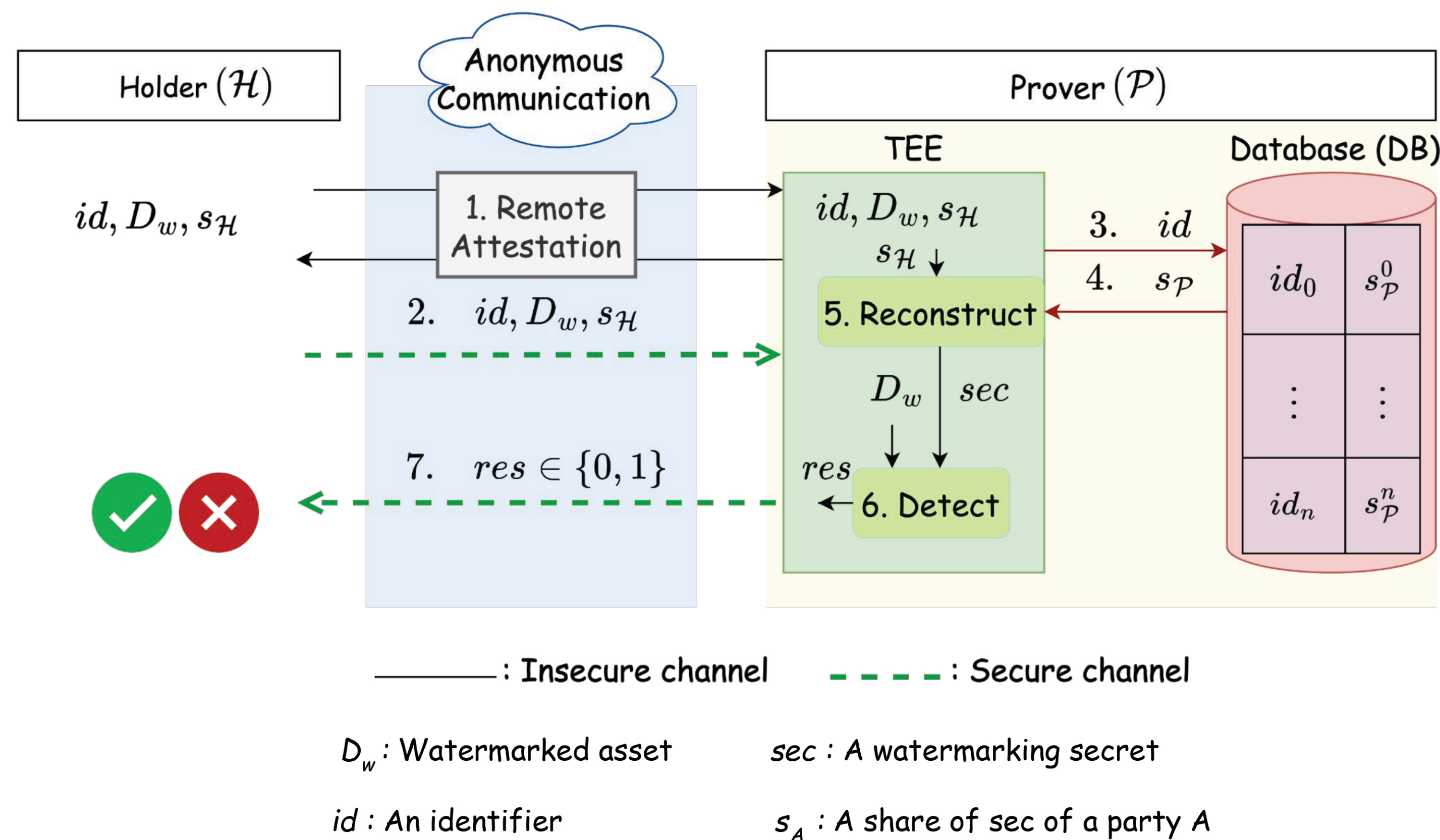
- Via a Certificate authority → Trusted Third Party needed
- Adding multiple watermarks on an asset → Limited # of detections
- Via Zero Knowledge Proof → Requires online Owner

Is it possible to convert any symmetric watermarking schemes into publicly verifiable ones without incurring any of these shortcomings?

Puppy Overview



Puppy-TEE



Evaluation

Session Establishment: w/ SGX ~6.50 ms and w/o ~2.20 ms.
 Session Termination: w/ SGX ~0.10 ms and w/o ~0.03 ms.

WM Type	SGX	Receive Data	Reconstruct Secret	Detect WM
FreqyWM Dataset	✓	0.53	0.03	0.06
	✗	0.31	0.01	0.02
OBT-WM Num. Database	✓	0.40	0.01	0.05
	✗	0.20	0.0001	0.02
Image-WM	✓	14.7	0.04	1.26
	✗	1.44	0.01	0.70
DNN-WM	✓	5040	4773	10333
	✗	358	925	426.6

***All measurement units are in milliseconds (ms).

Conclusion

- **[Unlimited Verification]** Puppy enables holders to verify a watermarked asset an unlimited number of times.
- **[Owner-free Verification]** Puppy does not require owners' online participations.
- **[Watermarking Secret Protection]** Puppy protect watermarking secret known only by the owner.
- **[Watermarked Asset Protection]** No other party learns the watermarked asset.
- **[Privacy]** All communication history between an owner and a holder is kept private.

