Zero-Knowledge Middleboxes

Paul Grubbs, Arasu Arun, Ye Zhang, Joseph Bonneau, Michael Walfish
NYU Department of Computer Science, Courant Institute

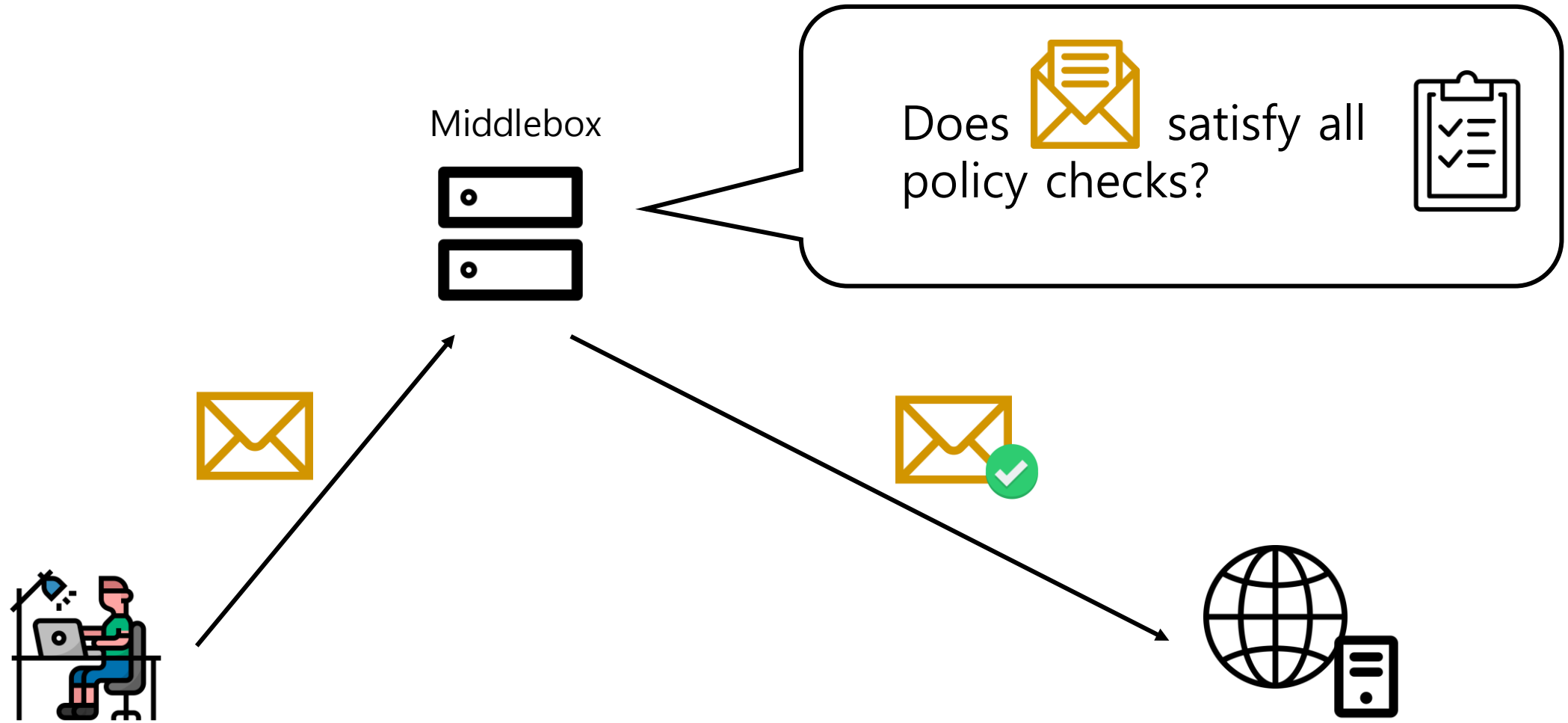
USENIX Security Symposium '22

2023.03.23.

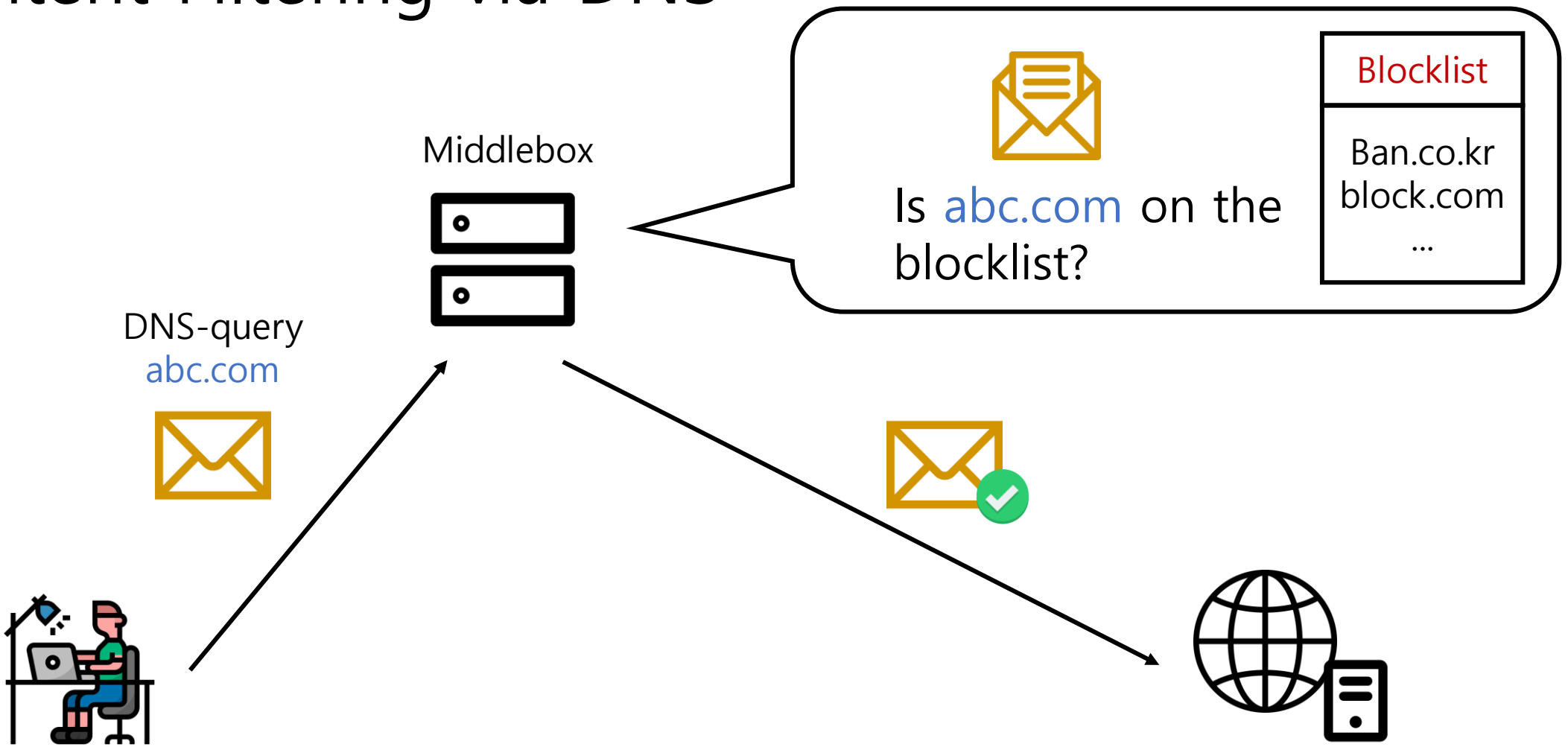
GyeongHeon Jeong(ghjeong@mmlab.snu.ac.kr)

Index

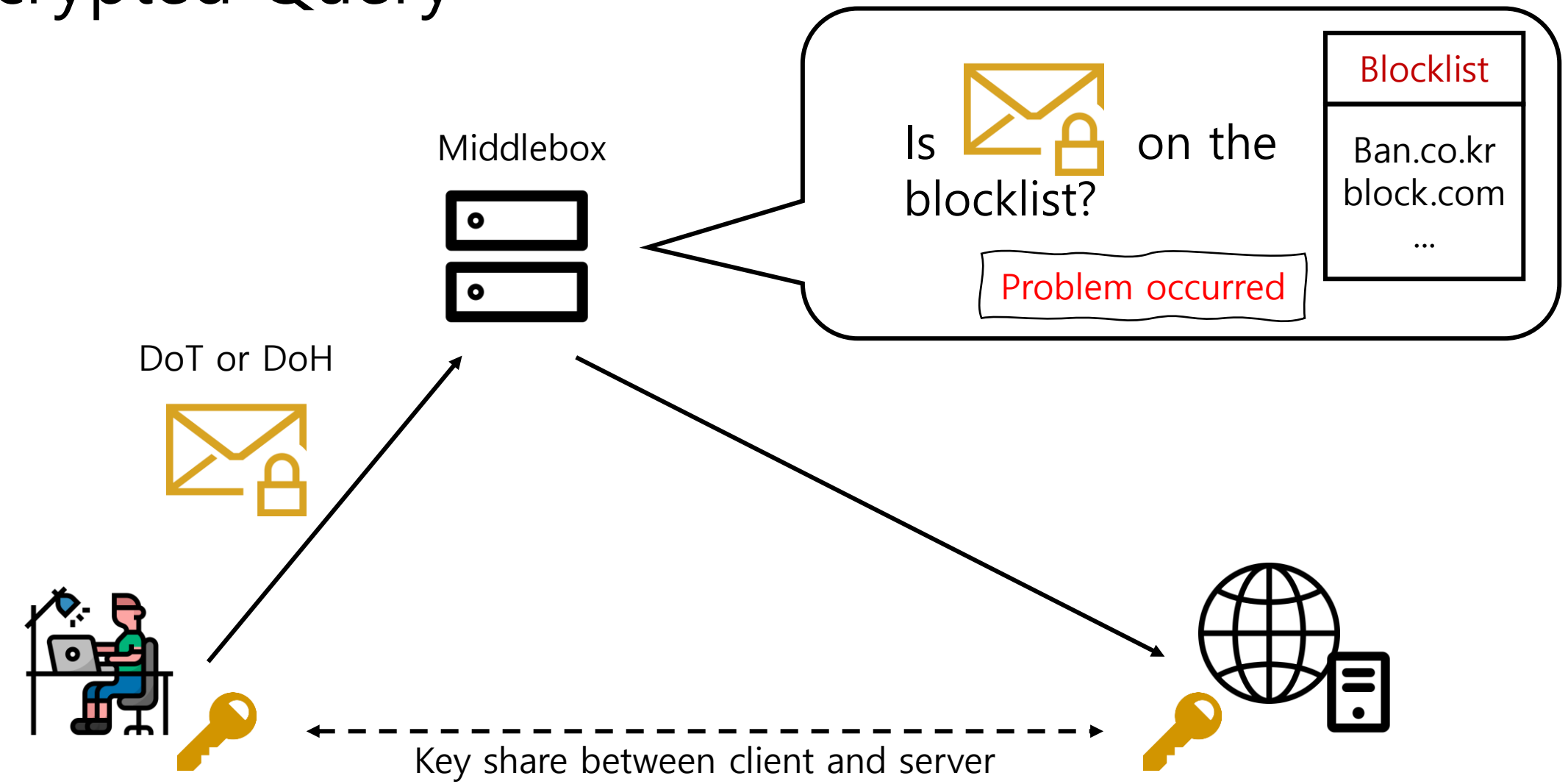
Middlebox inspects traffic



Content Filtering via DNS



Encrypted Query

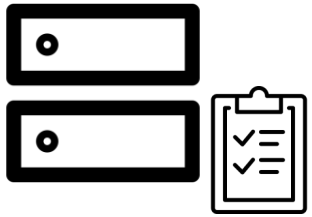


Motivation

Client

Want to keep own **Privacy**

Middlebox



Want to imforce own **Policy**

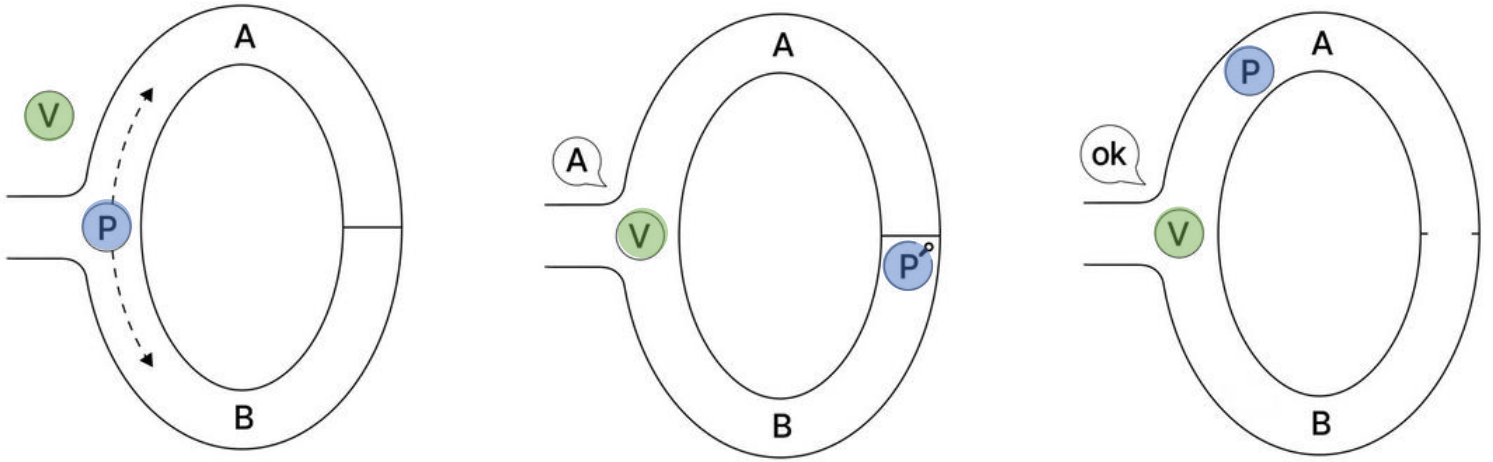
Compatible Solution

Zero-Knowledge Proofs

Background – Zero Knowledge Proofs

- Procedure in cryptography that ensures that when someone proves to another that a statement is true, they do not reveal anything except whether the statement is true or false
- The way to prove the validity of information without revealing any information

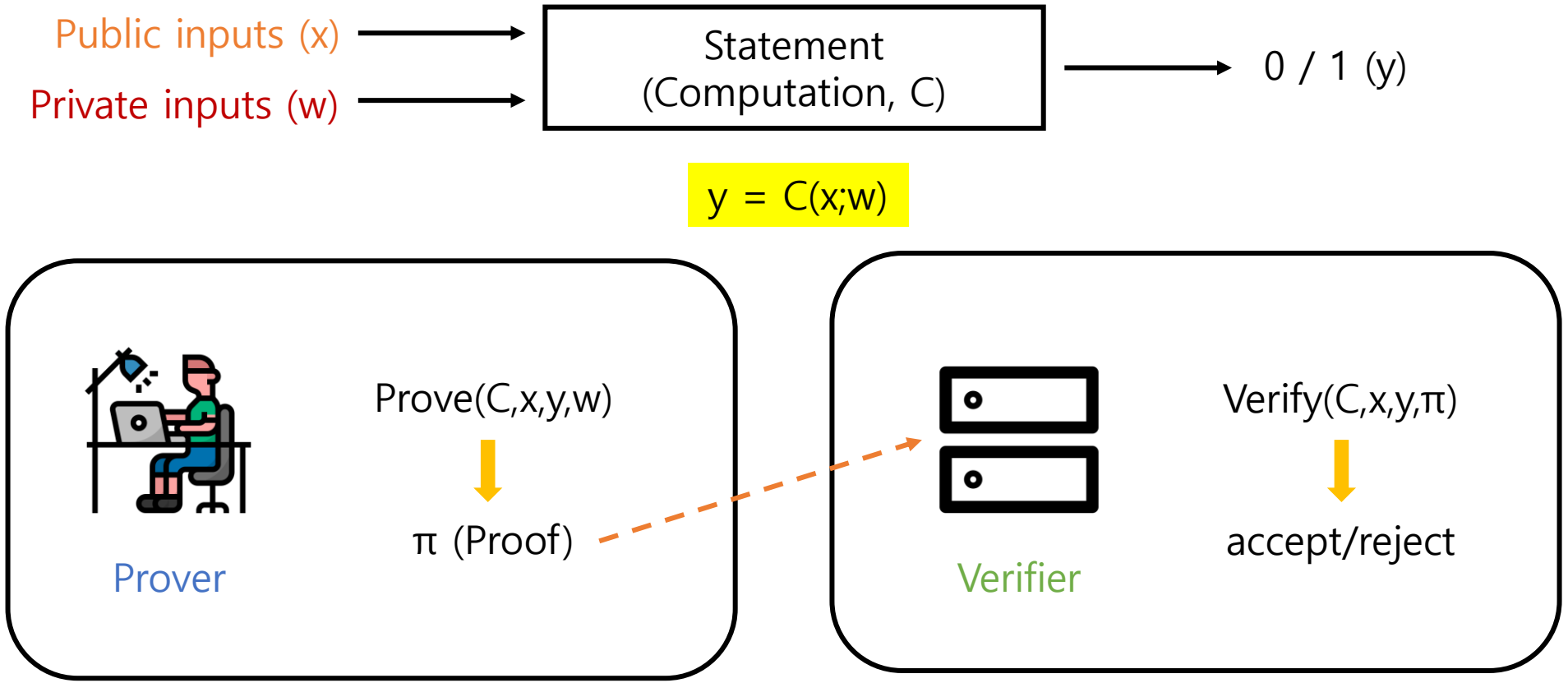
- **Prover** prove to the **Verifier** that it knows the **Secret** without revealing it



Probability

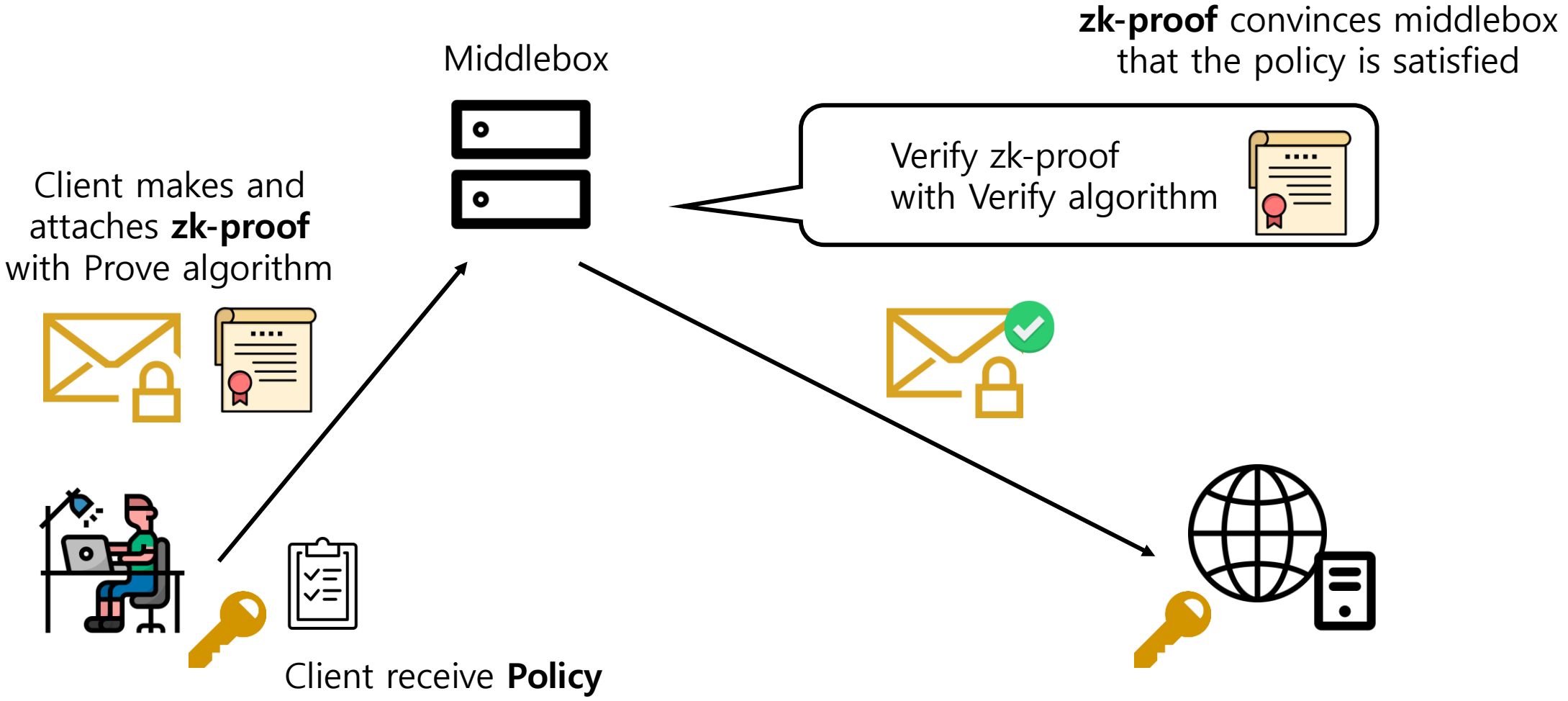
1 time: 50%
20 times: <0.0001%

Background – Zero Knowledge Proofs (cont.)



QAP-based proof protocol Groth16 (zkSNARK) which is a non-interactive zero knowledge proof (NIZK)

The ZKMB Framework



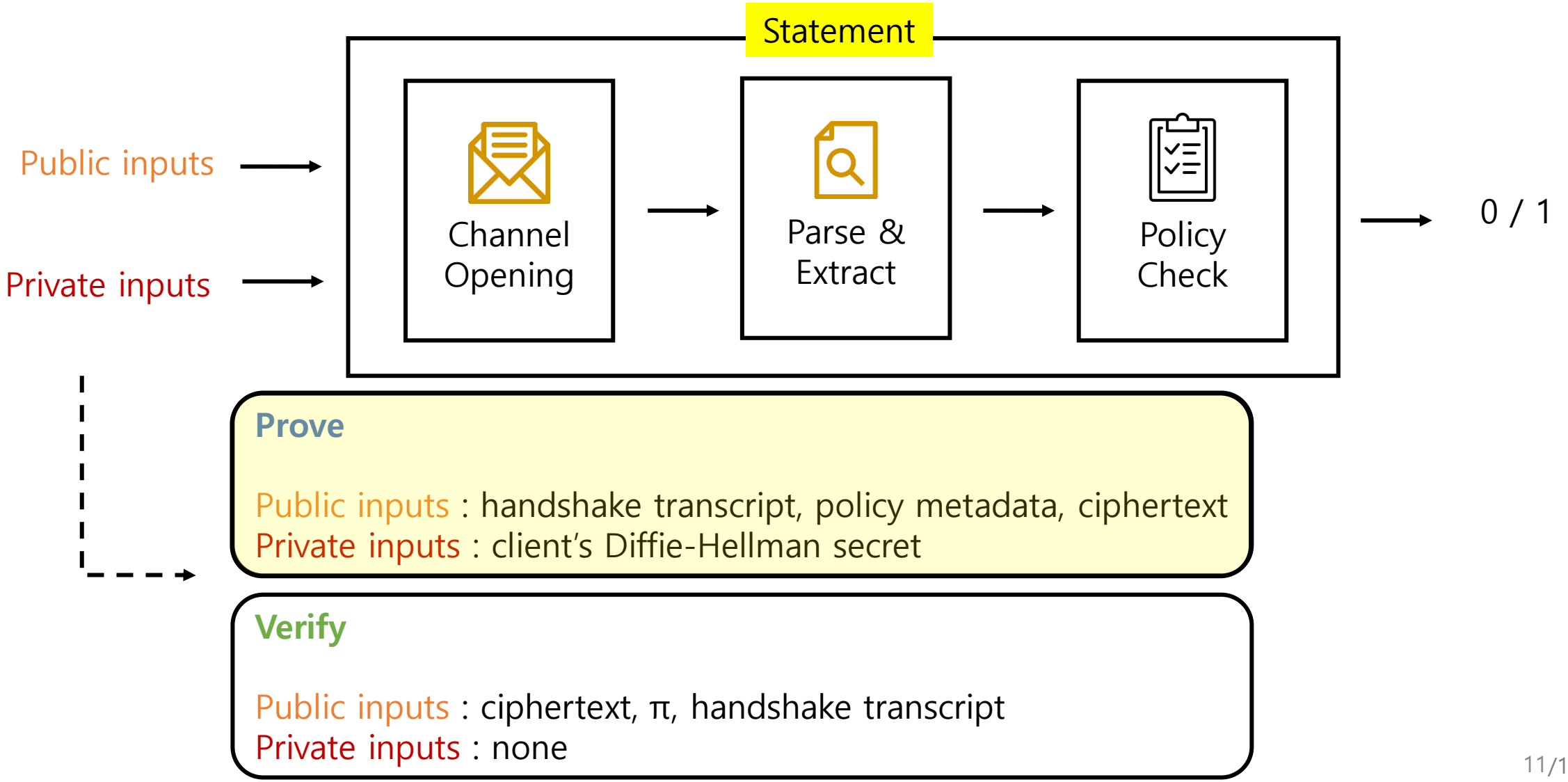
The challenge with network messages

- Many practical ZK protocols (e.g., SNARKs) are made
  - They require representing the statement as an **arithmetic circuit** over a field

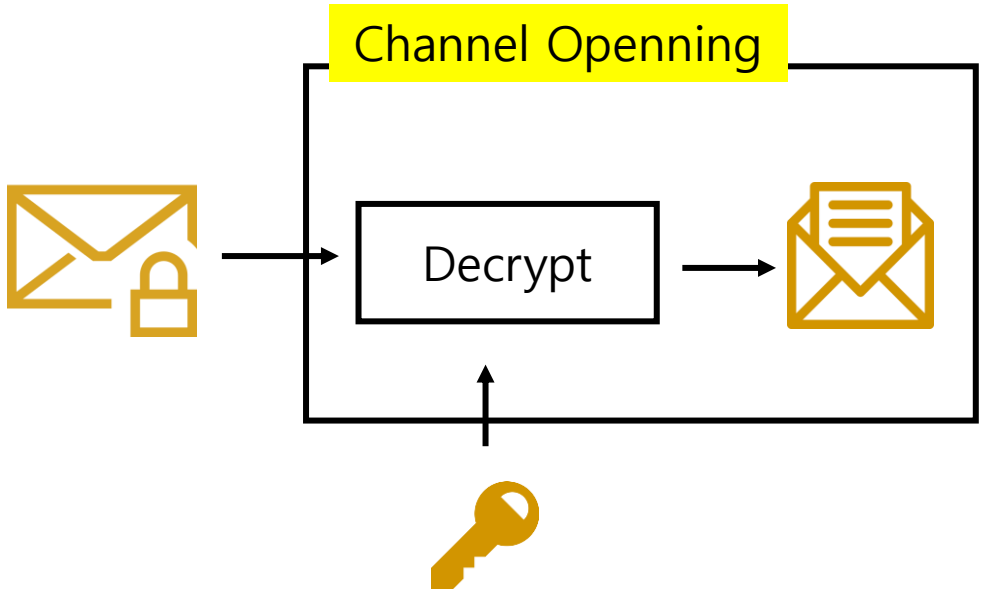
- Legacy symmetric-key functions like AES, ChaCha, SHA are very inefficient as circuits
  - Thus, they **must design proof statements** for this case

- Of course, No weakened encryption or privacy guarantees of TLS 1.3 and no server-side modification

ZKMB proof statements

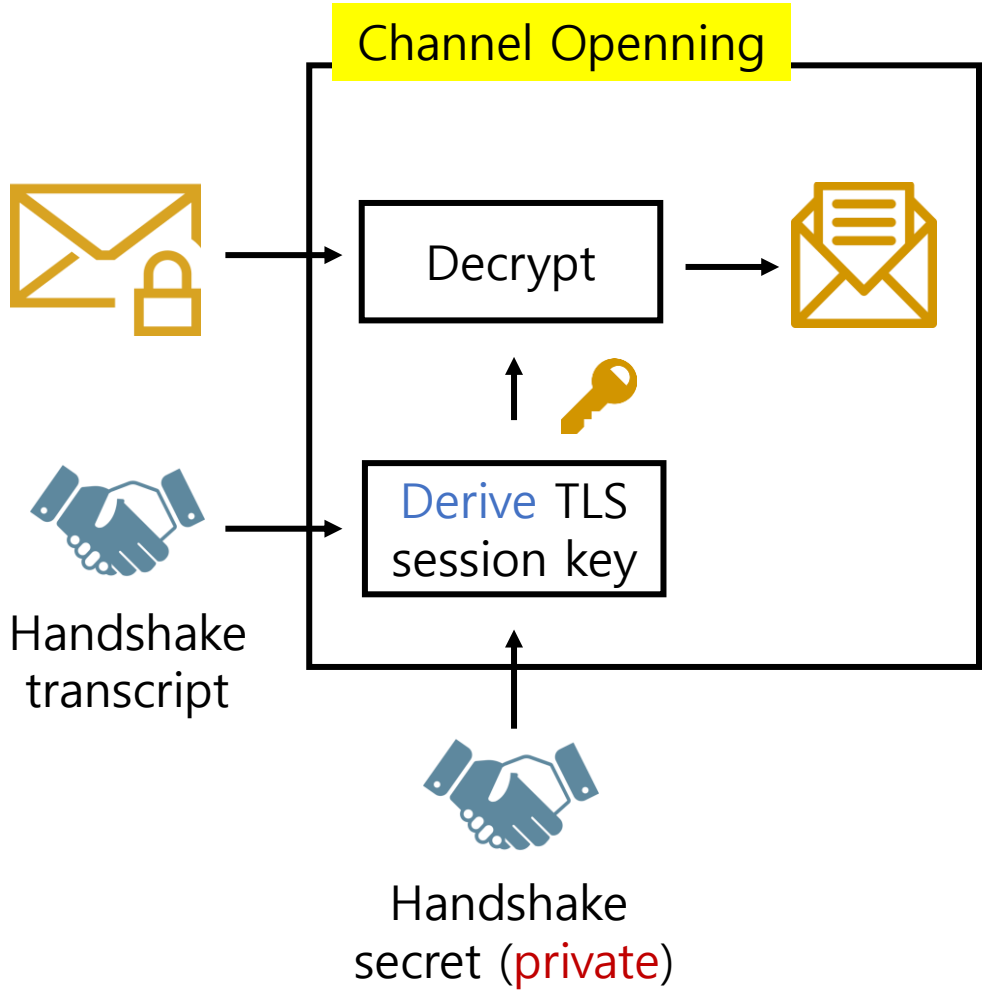


Channel Opening



Challenge

Prover may use a different key because TLS 1.3 doesn't support any "key-committing" authenticated encryption ciphers

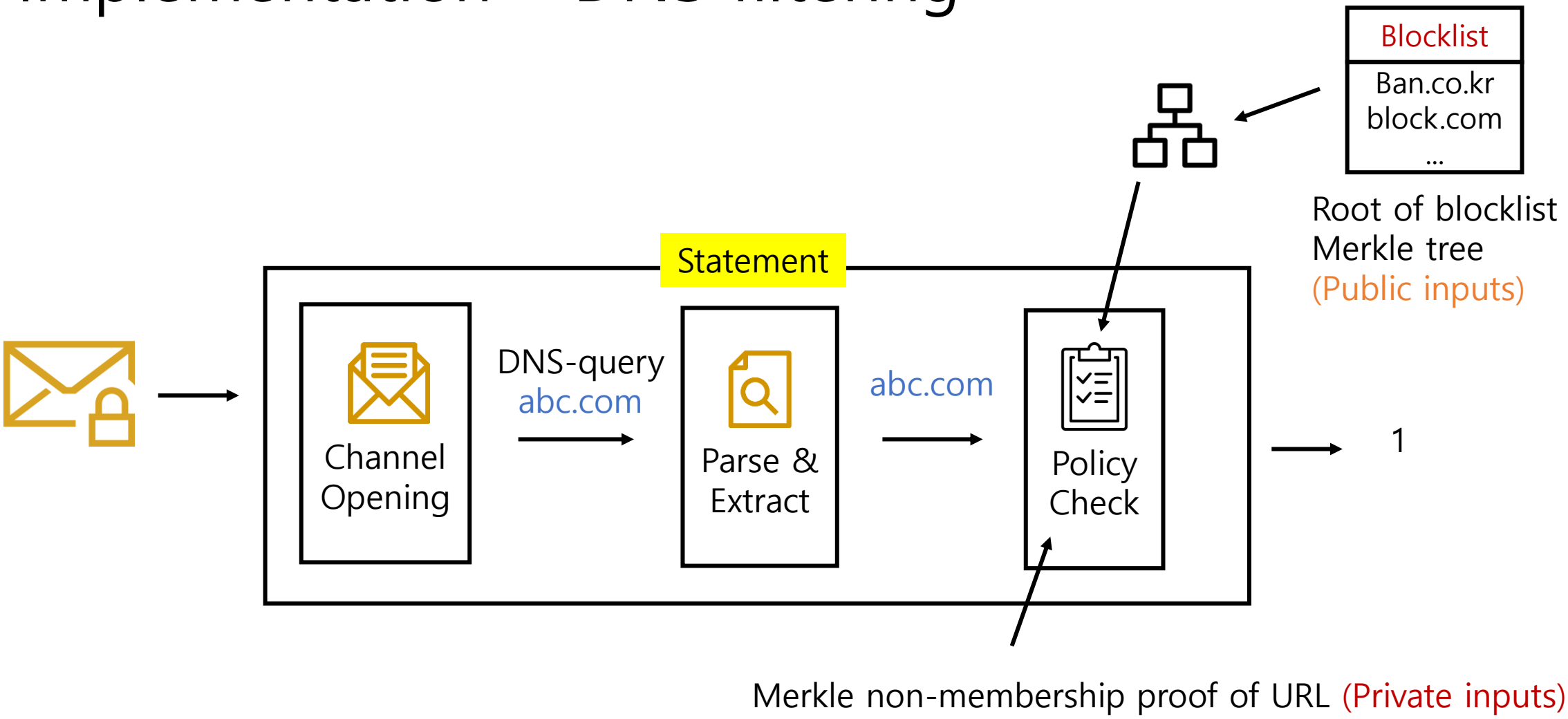


Parse & Extract and Policy Check

- Translation between the network protocol wire format of message and the input format of the policy check
  - Extract the policy-relevant substring of a network packet, while checking that some syntactic requirements
  - Operate differently depending on whether it's DoH or DoT, because they have different format of message

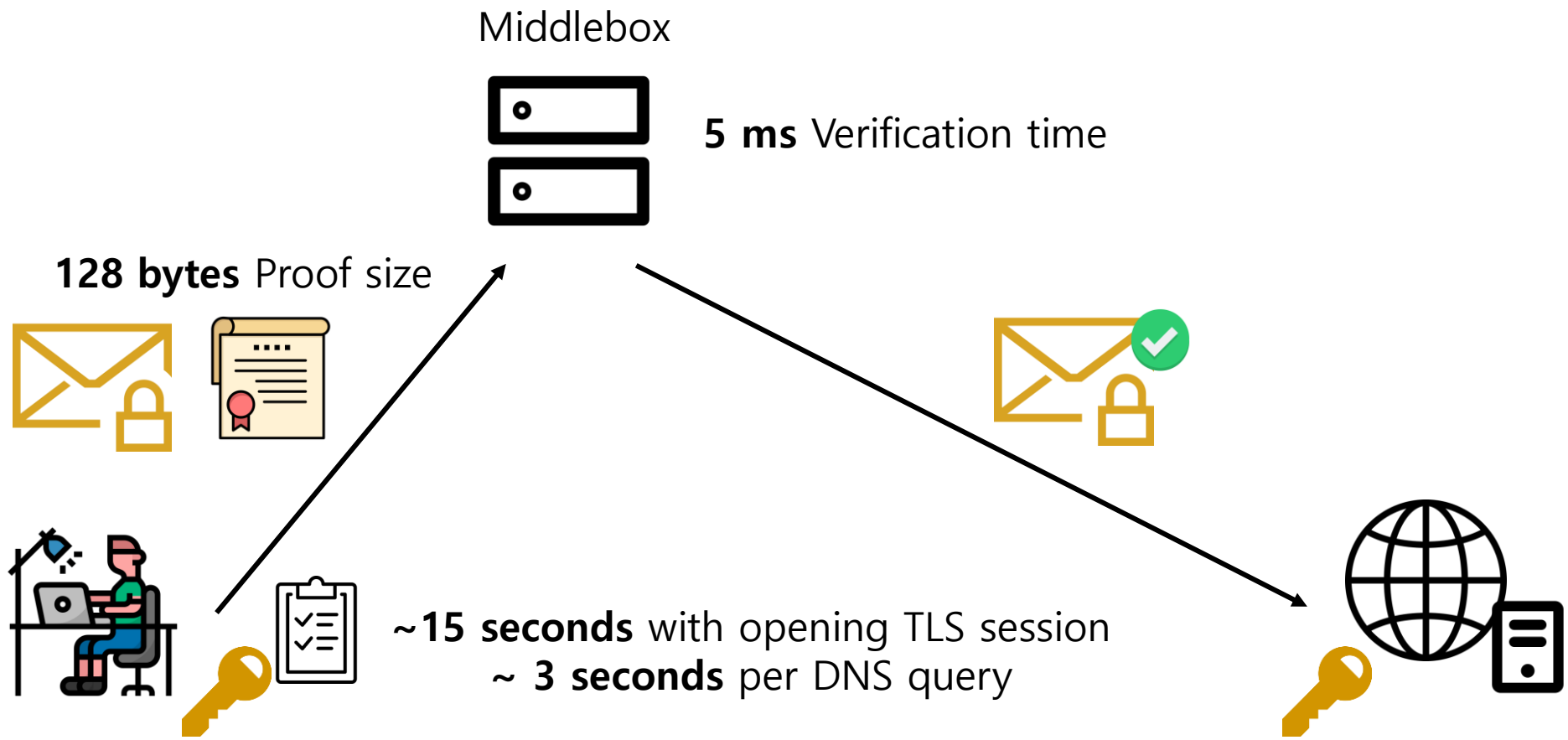
- Check that extracted message **satisfies the policy** in the policy metadata

Implementation – DNS filtering



Experiment Result

- Implemented with xJsnark library and Groth16 algorithm



Conclusion

- ZKMB is **compatible solution** for clients and middleboxes
  - Clients prove policy-compliance using zk-proof with keeping privacy
- Modular policy check
  - DNS filtering, HTTP firewall, …
- Future work
  - Low delay
  - Protocol-specific optimization
  - Not only in local network, but also in cloud network

Thank you for listening