Witness Signatures and Non-malleable MIPs

Vipul Goyal, Aayush Jain, Dakshita Khurana

Microsoft Research Microsoft Research Microsoft Research Ucla

Motivation

Motivation

Motivation

Motivation

AGAAGGG
AGTGCAAGTC
G Disease
CATGATGTTGG
GCTGAAAAC
GATC

Witness Signature!

Witness Signatures

- Sign(x,w,m) -> $\sigma_{m,}$ s. t. Verify(x, m, σ_m) = 1
- There exists a black-box extractor that extracts a witness from any efficient forger F that outputs σ', s.t. Verify(x, m, σ') = 1.
- Related to:
    - Non-malleable NIZKPoK
    - Signatures of Knowledge [Chase-Lysyanskaya06]
    - Both require CRS

Witness Signatures

- Goal of witness-based crypto: Avoid central setup like CRS/RO

- Assume tamper-proof hardware tokens

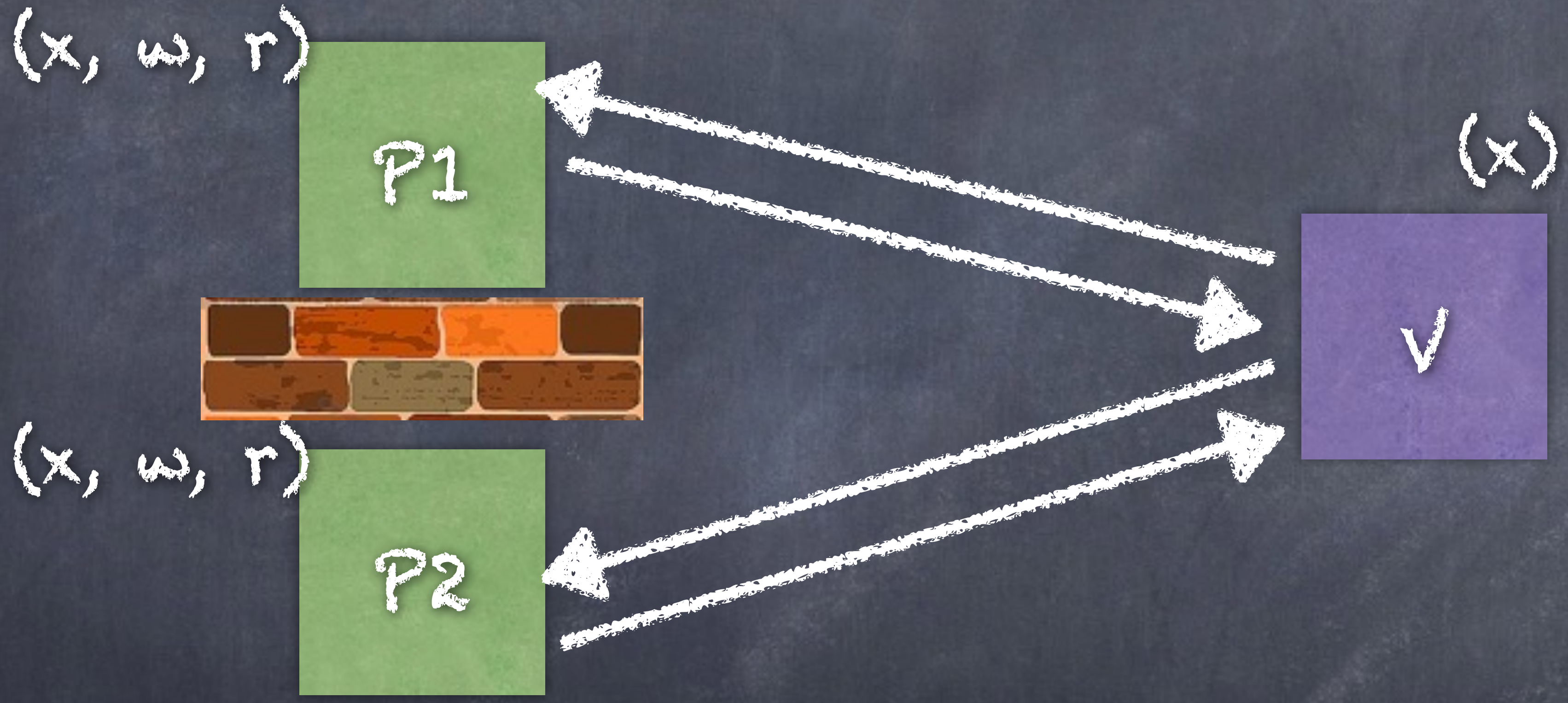
- Information theoretic efficient construction with stateful tokens

- Construct (tag-based) non-malleable ZK-MIP

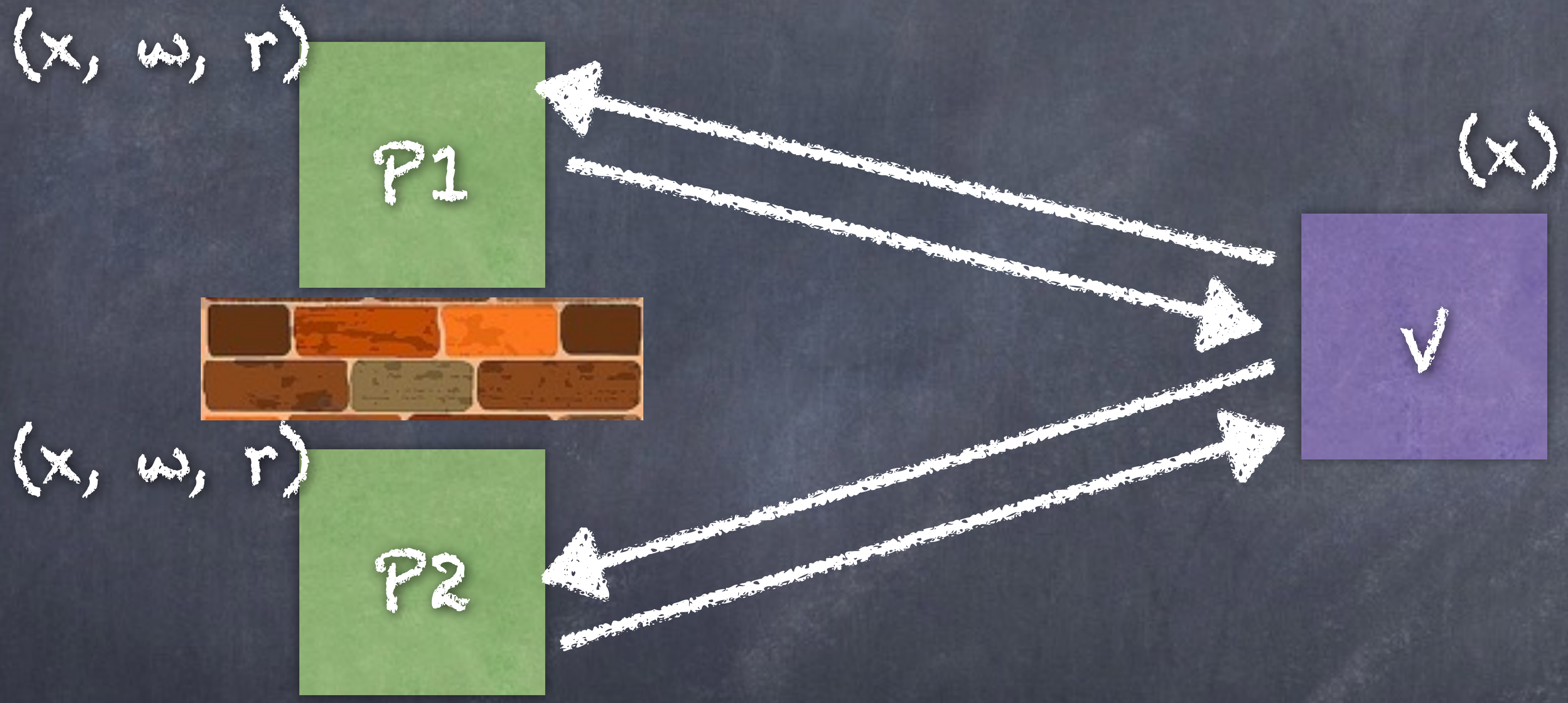
Our results

- Initiate study of non-malleable MIPs
- Obtain unconditional construction via non-malleable codes
- Use this to obtain witness signatures in the stateful token model
    - Unforgeability from non-malleability

(Stand-alone) MIP: Setting

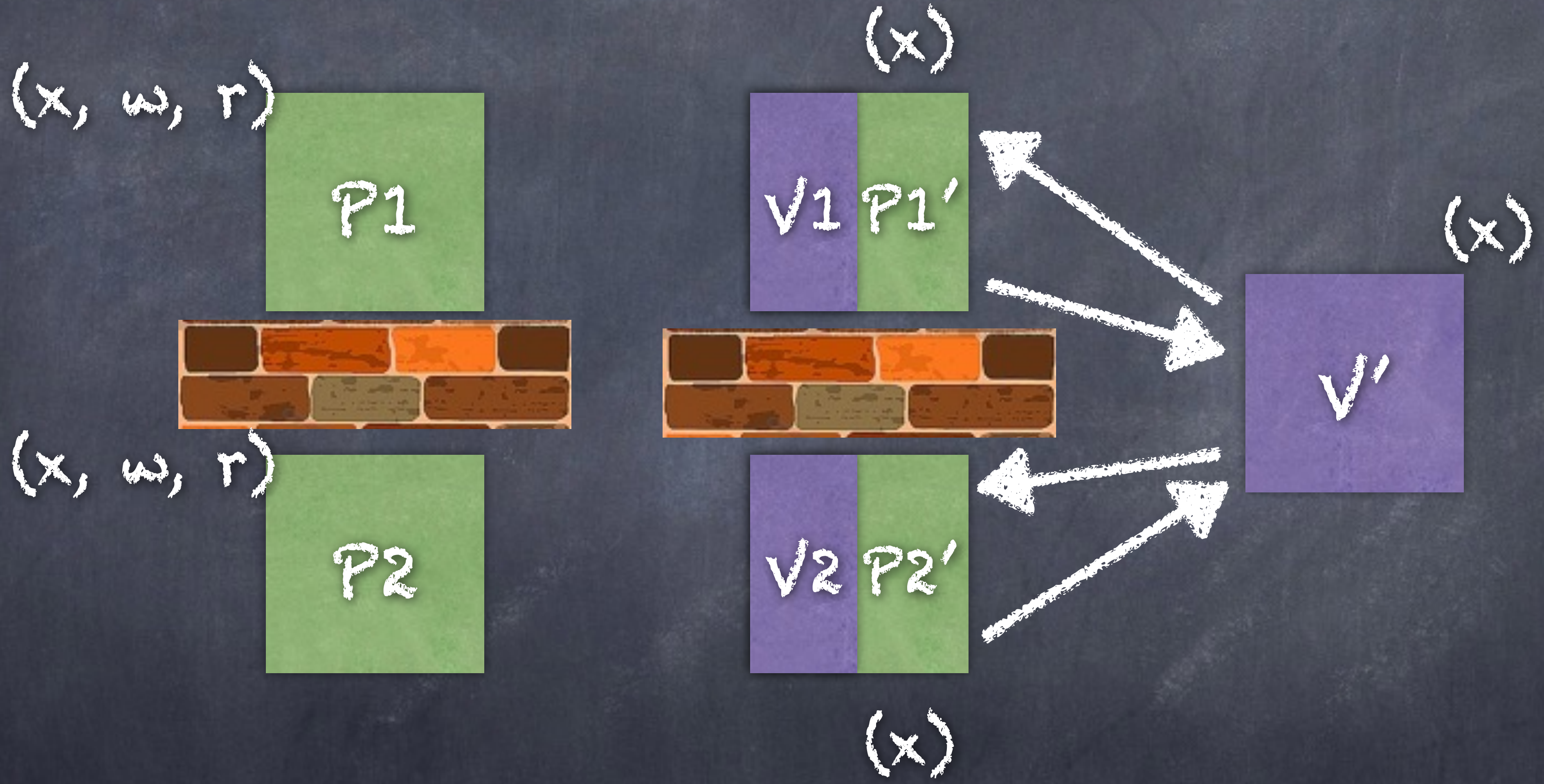


(Stand-alone) MIP

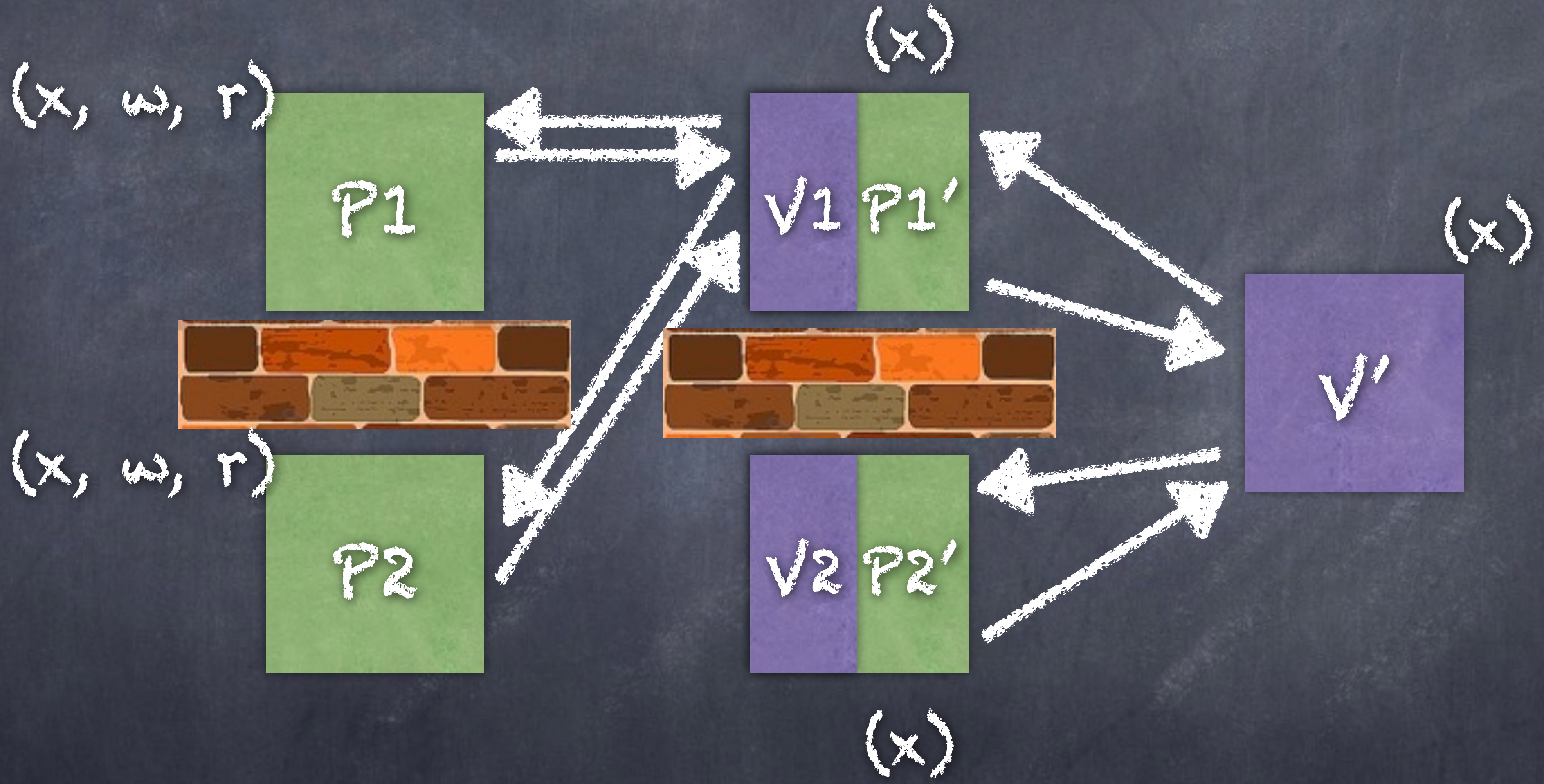


ZK-MIPs for all NP, also PoK
[BenOr-Goldwasser-Kilian-Wigderson88,
Lapidot-Shamir90]

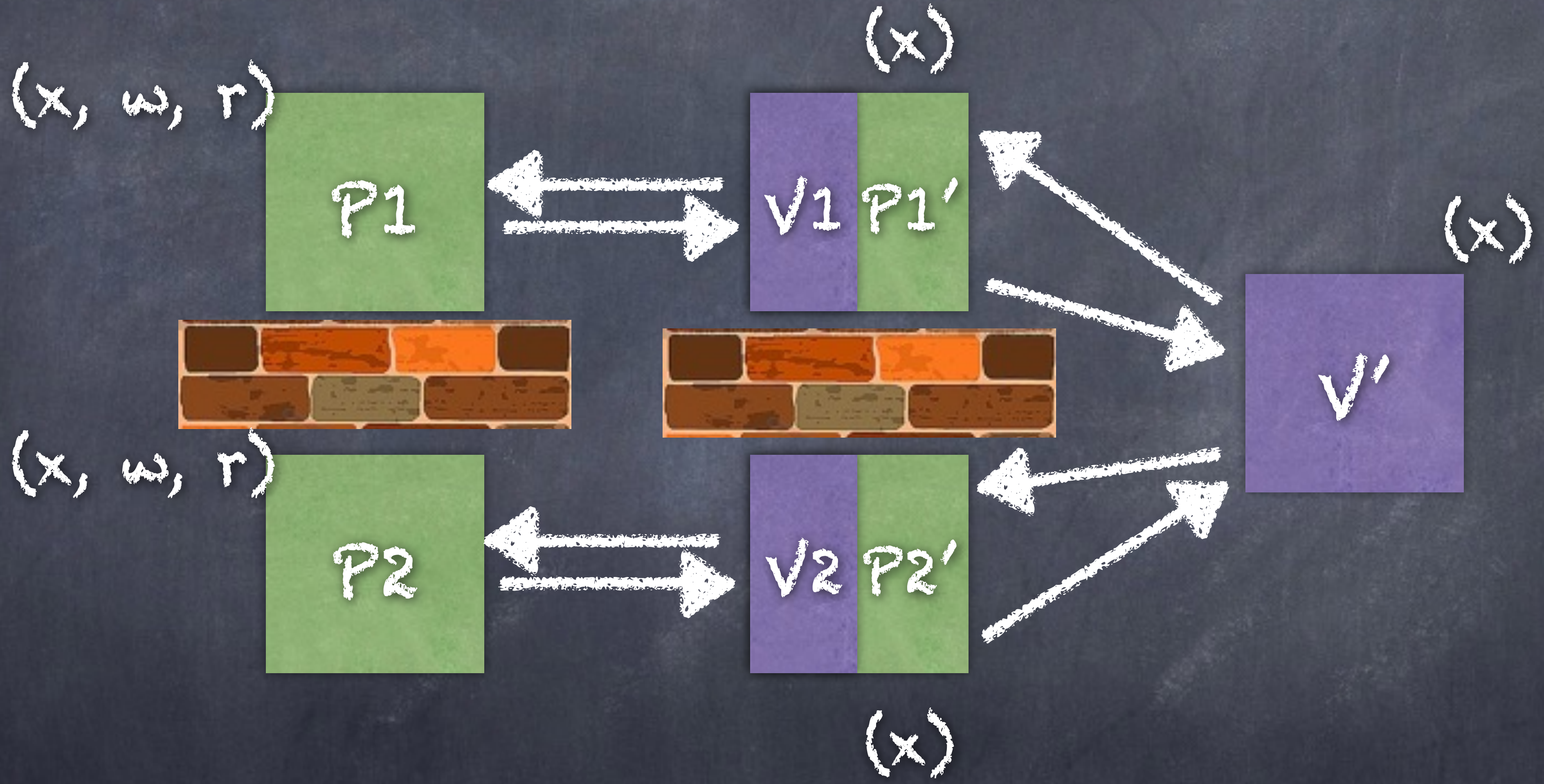
Man-in-the-middle attack



Man-in-the-middle attack



Man-in-the-middle attack



Non-malleable (SS) MIP: Construction

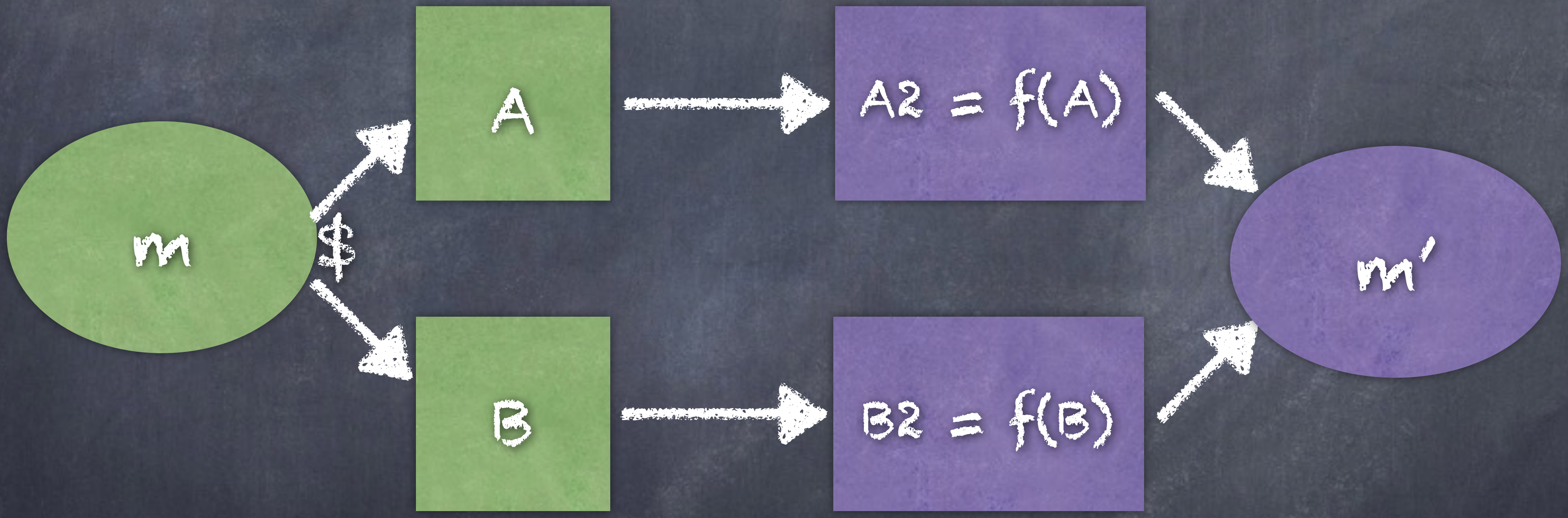
- Information theoretic
- Uses split-state non-malleable codes

Summary

- New cryptographic objects: Witness Signatures and Non Malleable MIPs
- Interesting application of non-malleable codes in the information-theoretic setting

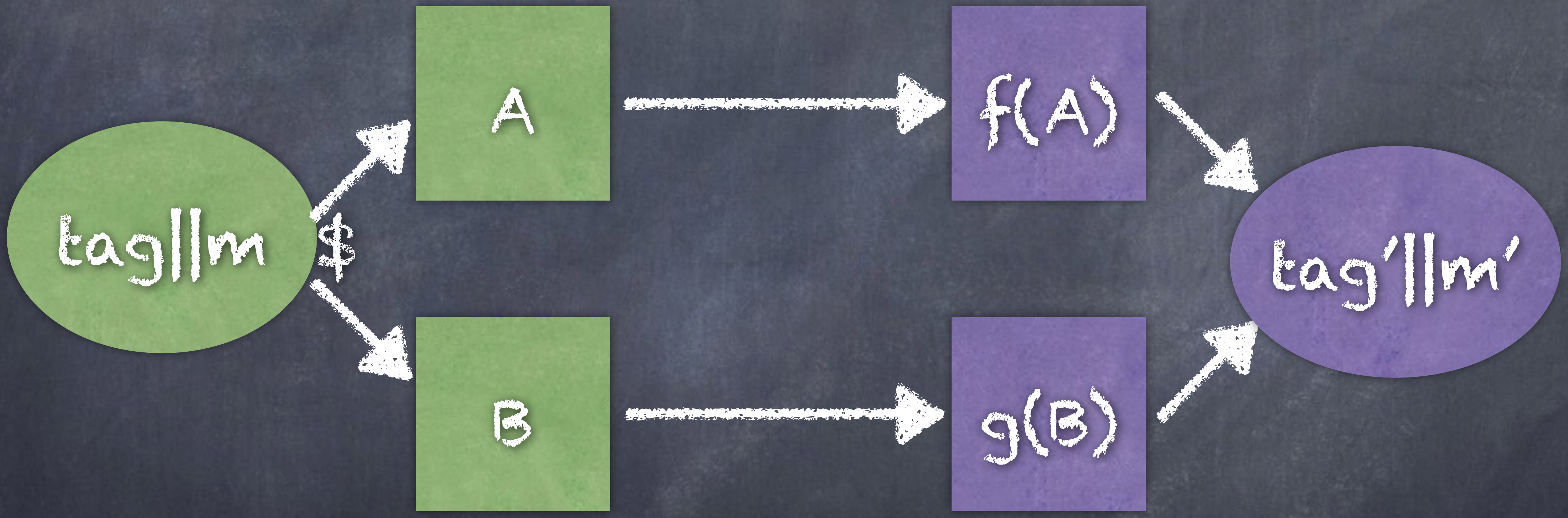
Thank you!

Split State Non-Malleable Codes



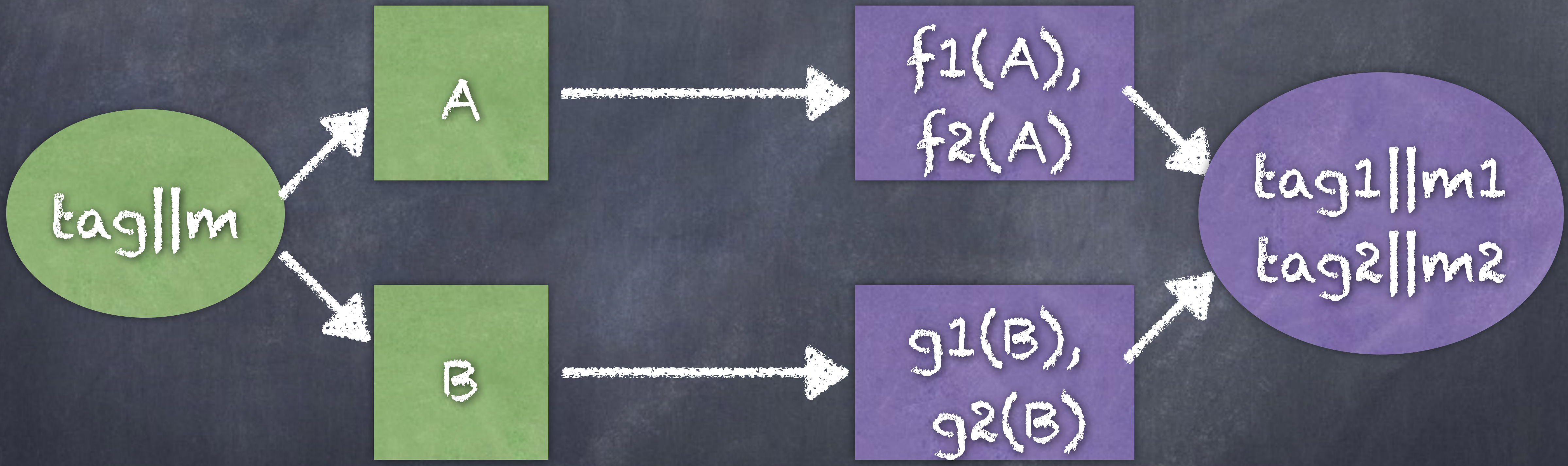
Either m'= m or they are unrelated!

Split State Non-Malleable Codes



tag' ≠ tag ⇒ m' and m are unrelated!

One-many split-state non-malleable codes

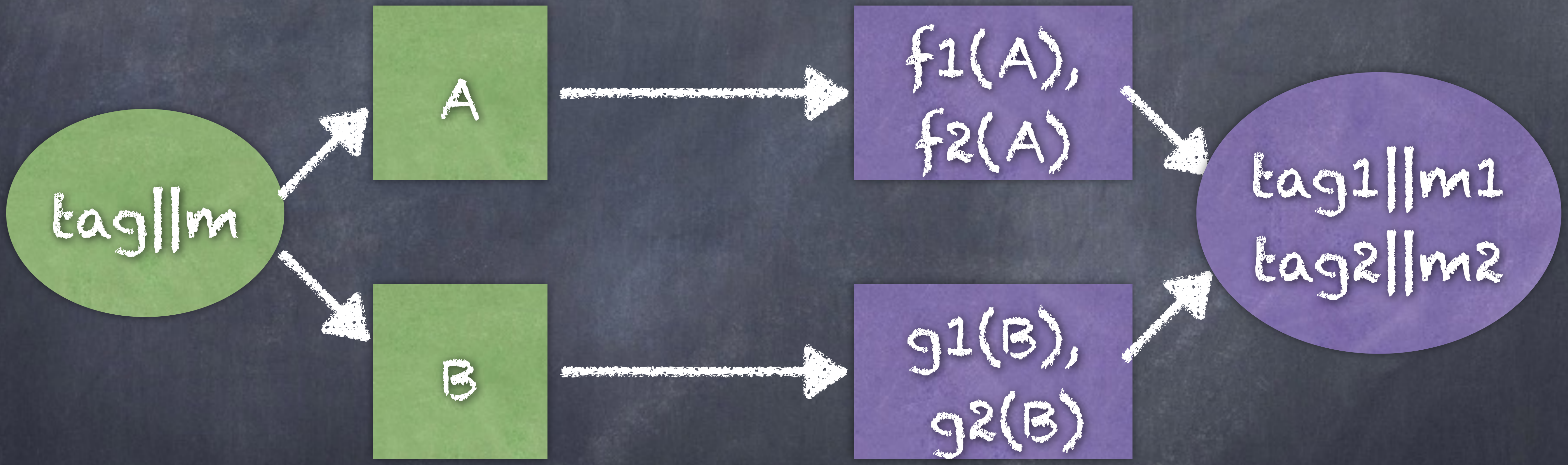


tag1 ≠ tag and tag2 ≠ tag

⇒ (m1, m2) and m are unrelated!

One-many split-state non-malleable codes

[Chattopadhyay-Goyal-Li15]



tag1 ≠ tag and tag2 ≠ tag

⇒ (m1, m2) and m are unrelated!