On (pseudo) collisions

Sebastiaan Indesteege

sebastiaan.indesteege@esat.kuleuven.be

dept. ESAT/COSIC, Katholieke Universiteit Leuven

Early Symmetric Crypto 2010
11–15 January 2010
Remich, Luxembourg

Motivation

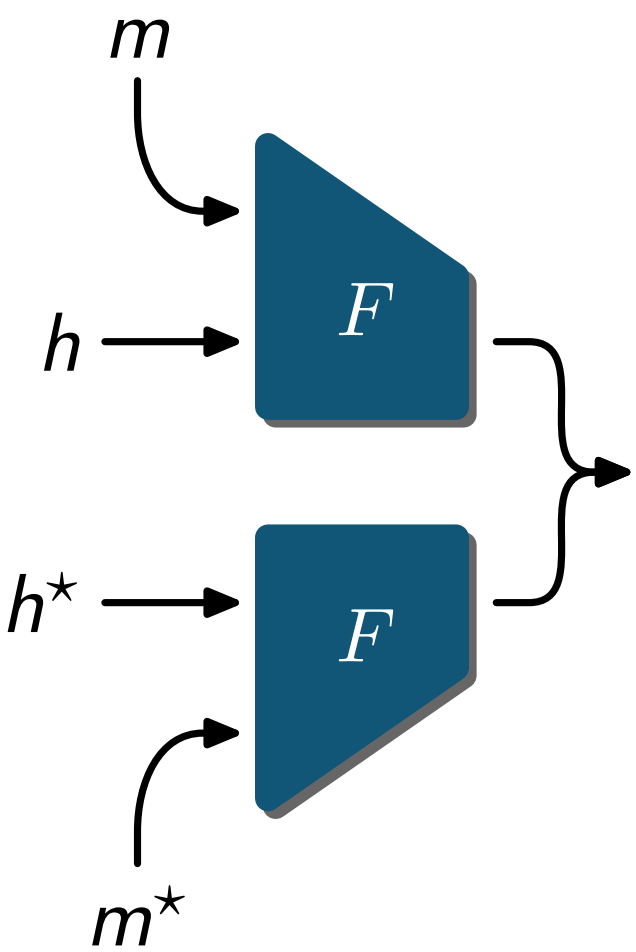
[Damgård '89], [Merkle '89]

collision resistant compression function $\Rightarrow$ collision resistant hash function

Practitioner's view

pseudo-collision attack on compression function $\not\Rightarrow$ collision attack on hash function

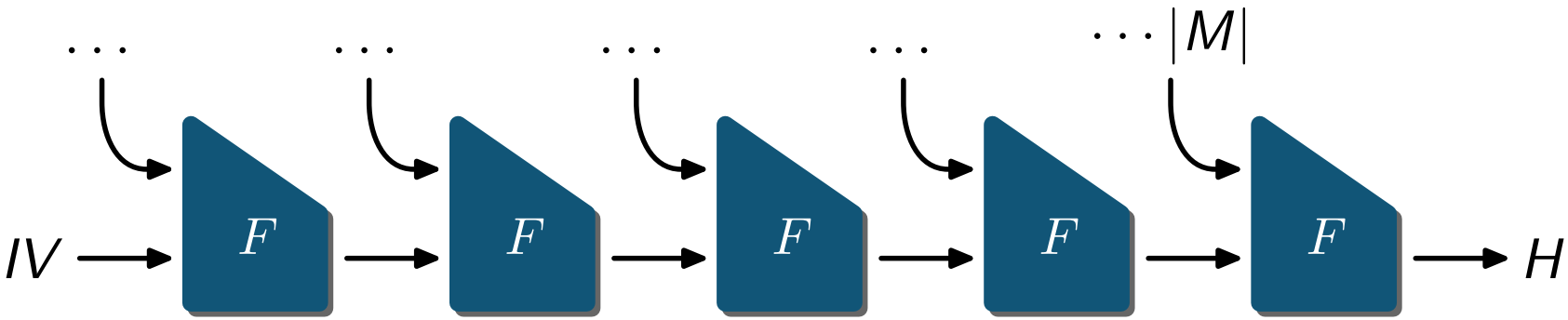
Pseudo-collisions



- Attacker choses $m, m^\star$ and $h, h^\star$
- Aka. (semi-)free start collision
- Damgård-Merkle proof no longer applies...
- But an attacker still needs to *hit* the pseudo-collision...

Review: Damgård-Merkle

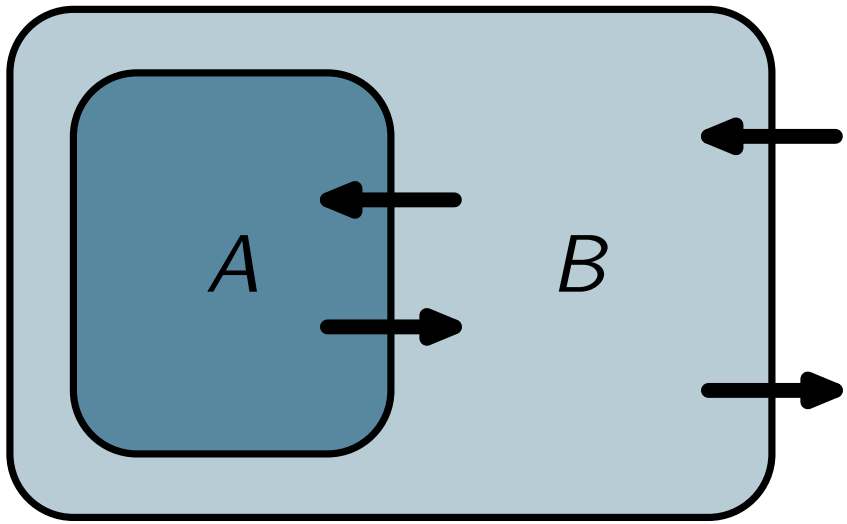
Iteration mode



- Message length $|M|$ input to last CF call

Review: Damgård-Merkle

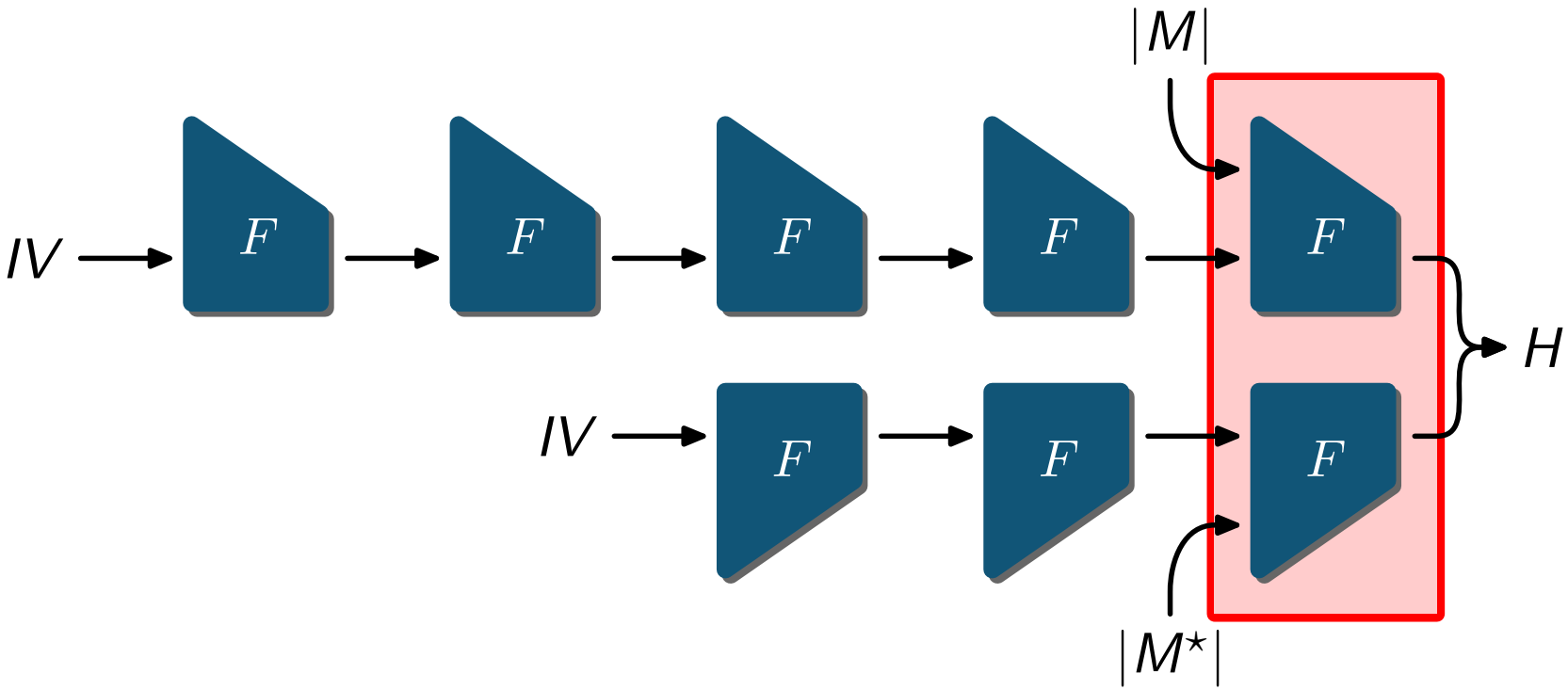
Reduction proof overview



- Given **hash function** collision adversary A
- Construct **compression function** collision adversary B
- CF collision resistance is a **sufficient** condition for hash function collision resistance.

Review: Damgård-Merkle

Proof

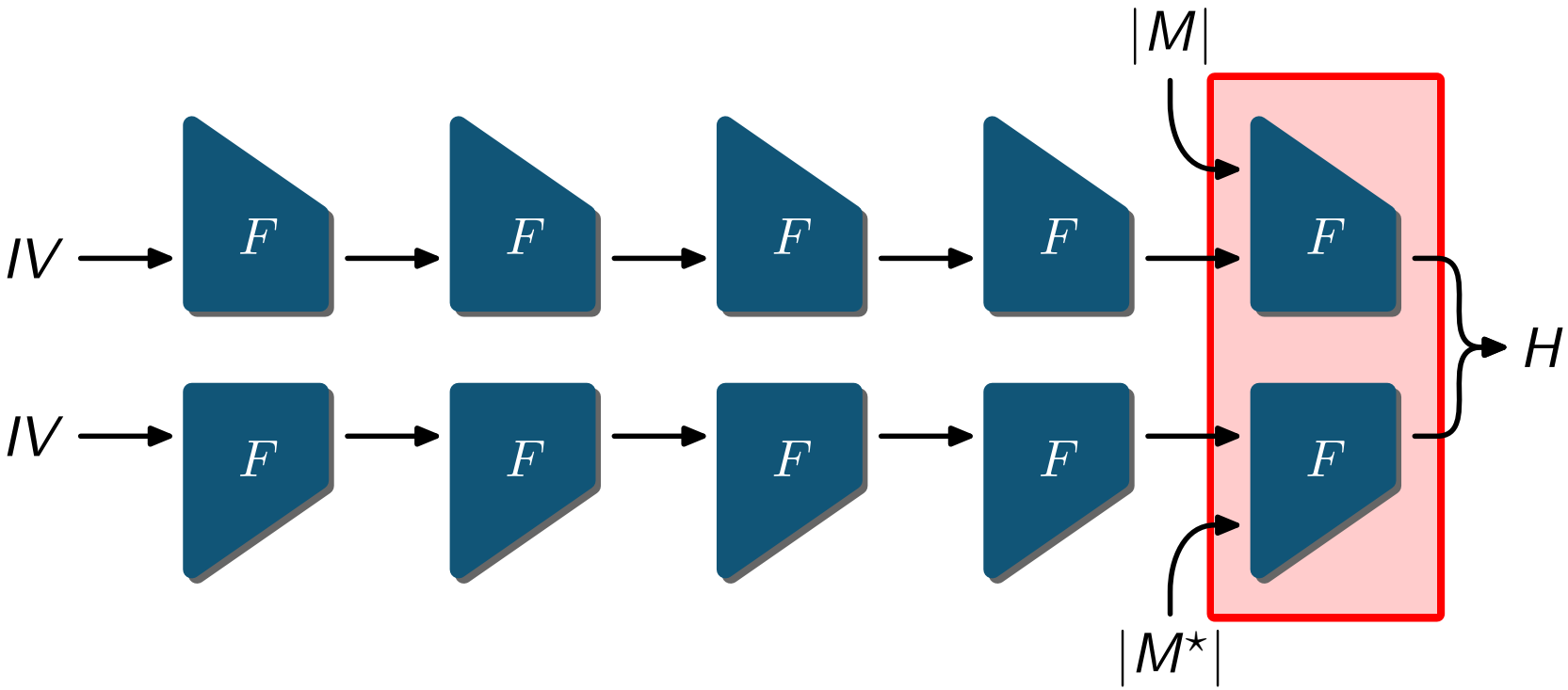


Case

- 1. $|M| \neq |M^{\star}|$

Review: Damgård-Merkle

Proof

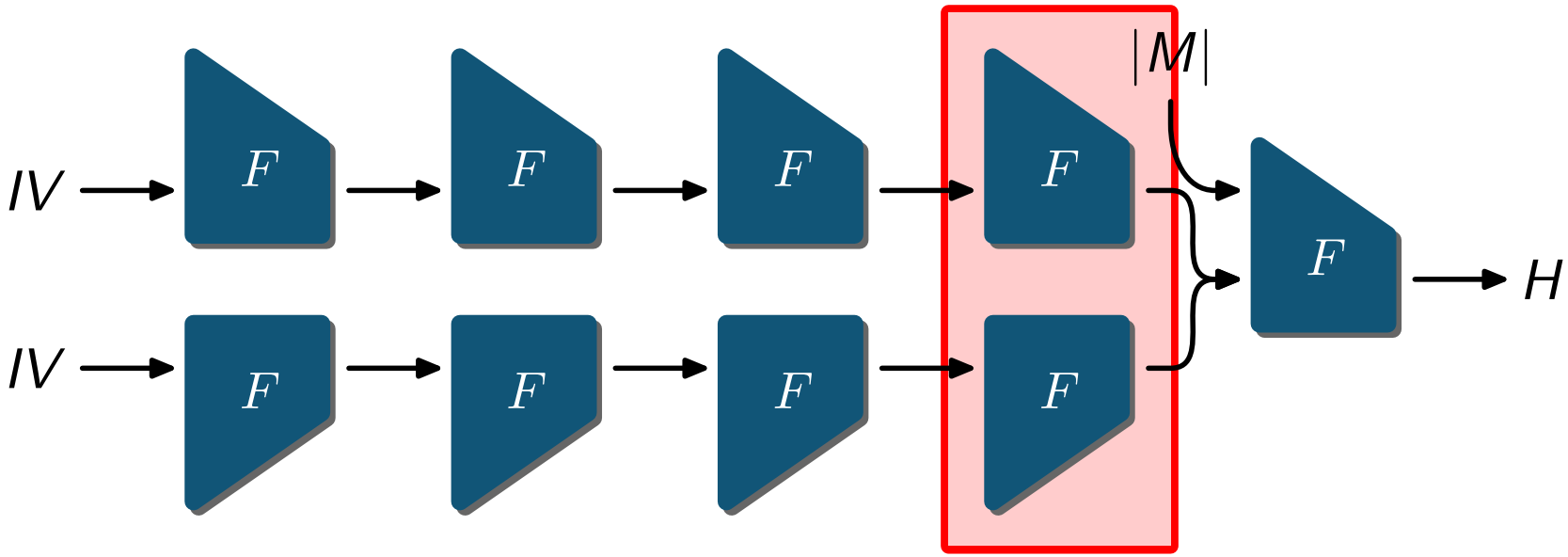


Case

- 2. $|M| = |M^{\star}|$

Review: Damgård-Merkle

Proof

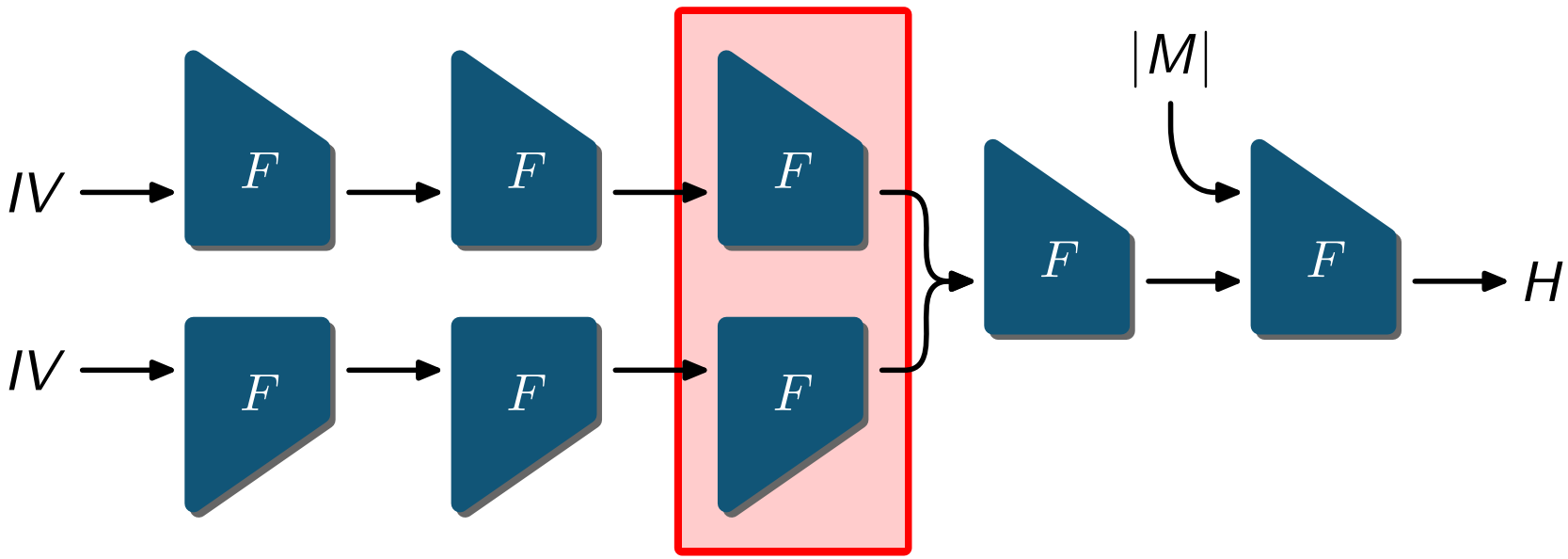


Case

- 2. $|M| = |M^\star|$

Review: Damgård-Merkle

Proof

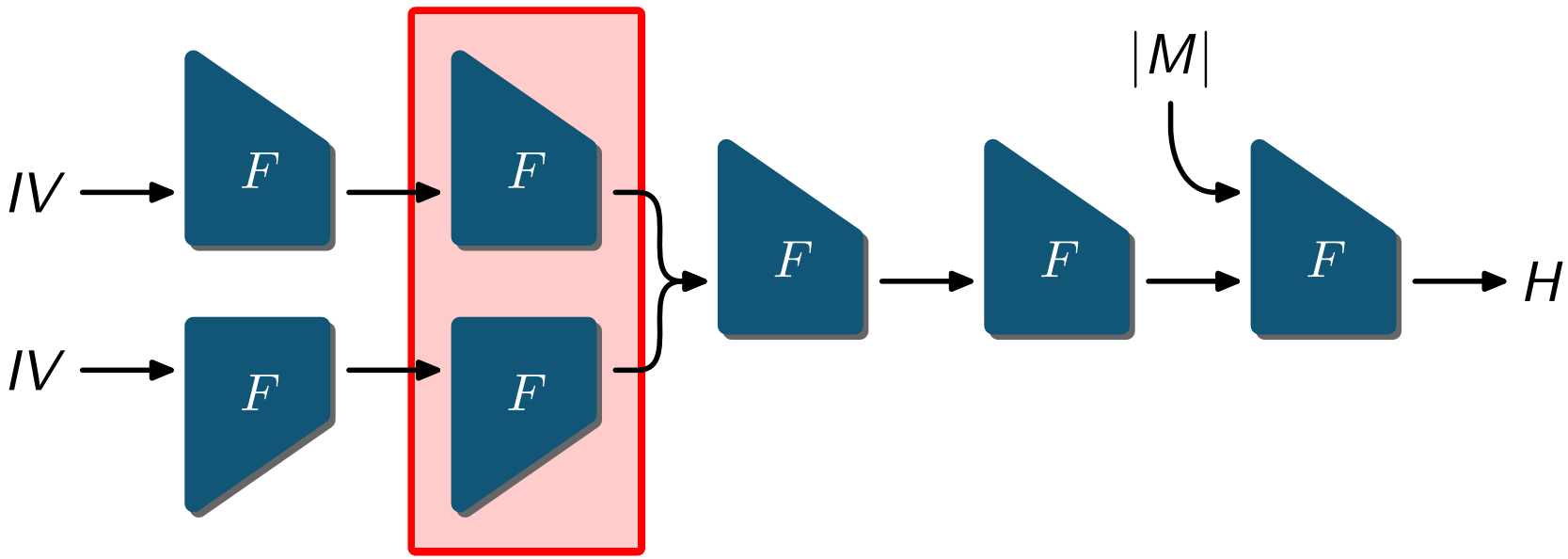


Case

- 2. $|M| = |M^{\star}|$

Review: Damgård-Merkle

Proof

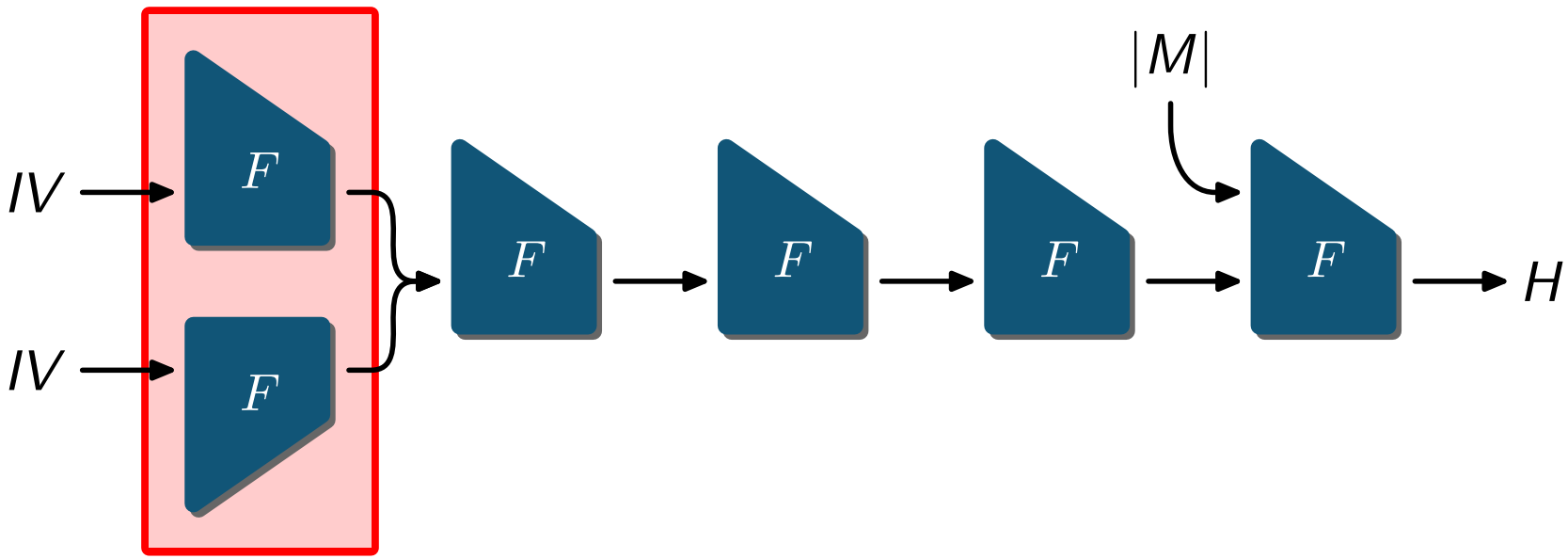


Case

- 2. $|M| = |M^{\star}|$

Review: Damgård-Merkle

Proof

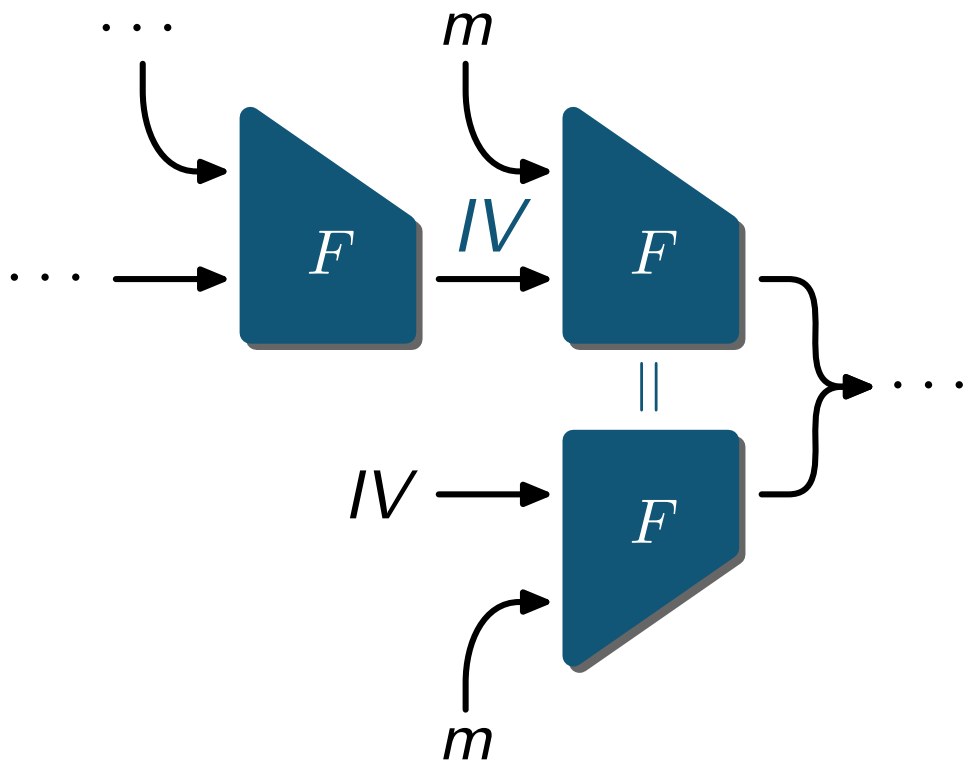


Case

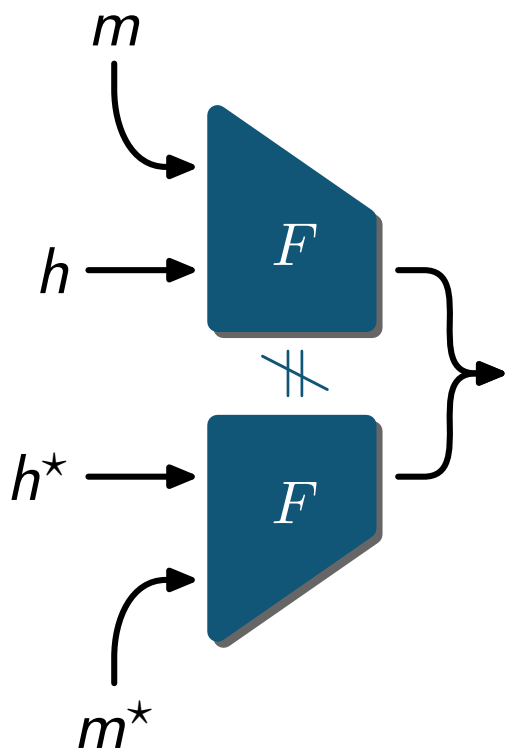
- 2. $|M| = |M^\star|$

Review: Damgård-Merkle

- Why include $|M|$?

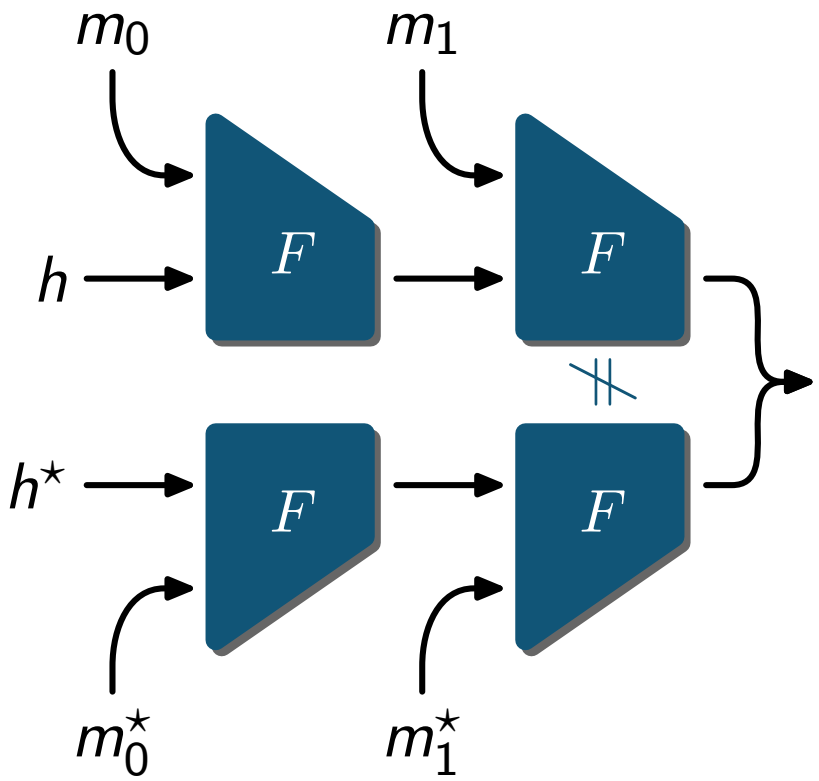


Towards two-step CF collisions



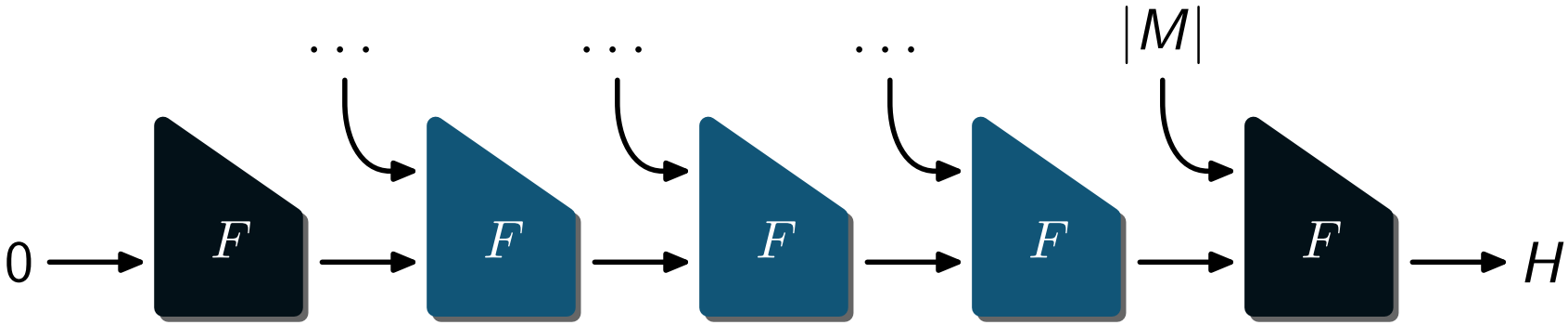
- CF **collision**: $\langle h, m, h^\star, m^\star \rangle$ s.t.
  - Collision: $F(h, m) = F(h^\star, m^\star)$
  - Active: $h||m \neq h^\star||m^\star$

Towards two-step CF collisions



- CF **two-step collision**: $\langle h, m_0, m_1, h^\star, m_0^\star, m_1^\star \rangle$ s.t.
  - Collision: $F\left(F\left(h, m_0\right), m_1\right) = F\left(F\left(h^\star, m_0^\star\right), m_1^\star\right)$
  - Second CF active: $F(h, m_0)||m_1 \neq F(h^\star, m_0^\star)||m_1^\star$

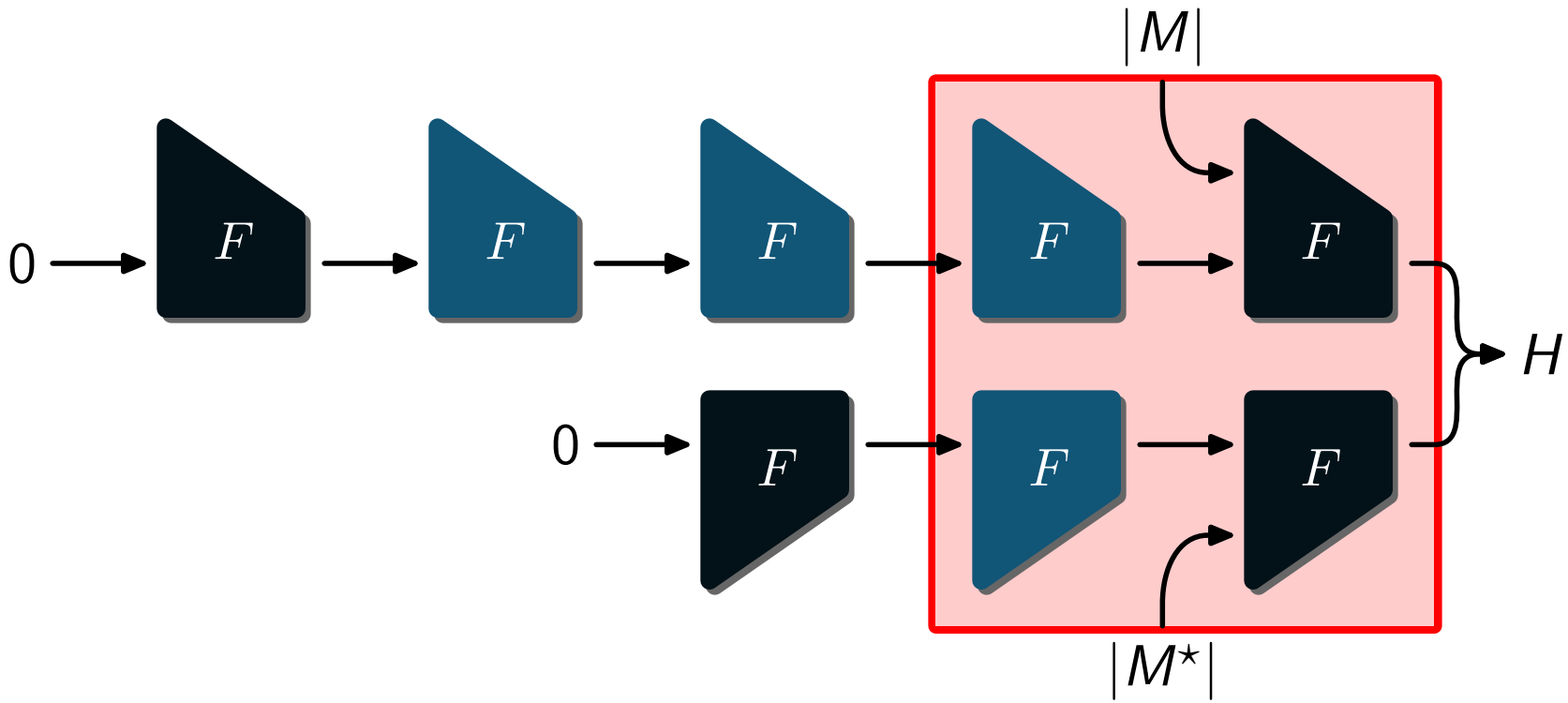
A simple iteration mode



- IV derivation using CF
- Output transformation using CF
- Message length $|M|$ input to output transformation
- Simplifies what follows...

Two-step CF collisions

Proof for example iteration

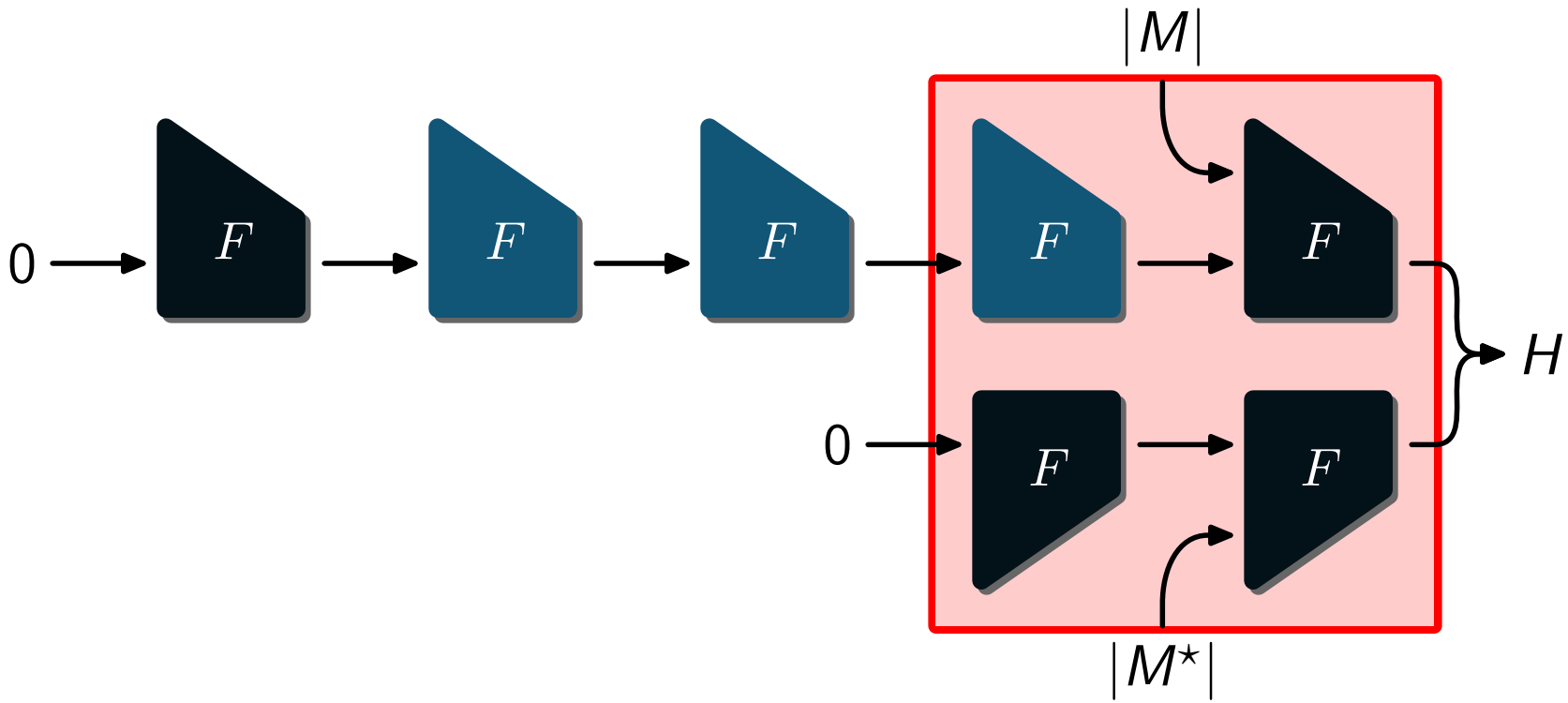


Case

- 1. $|M| \neq |M^{\star}|$

Two-step CF collisions

Proof for example iteration

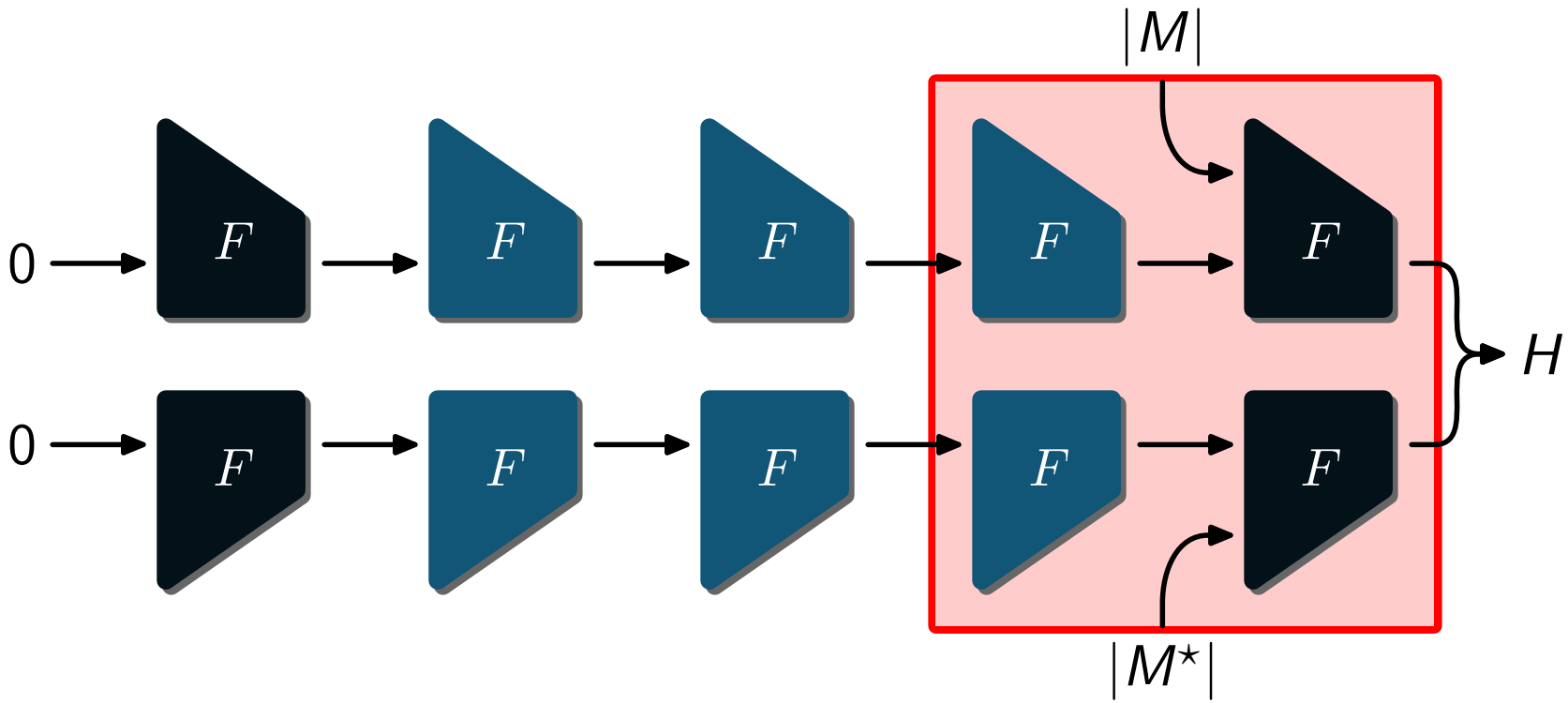


Case

- 1. $|M| \neq |M^{\star}|$

Two-step CF collisions

Proof for example iteration

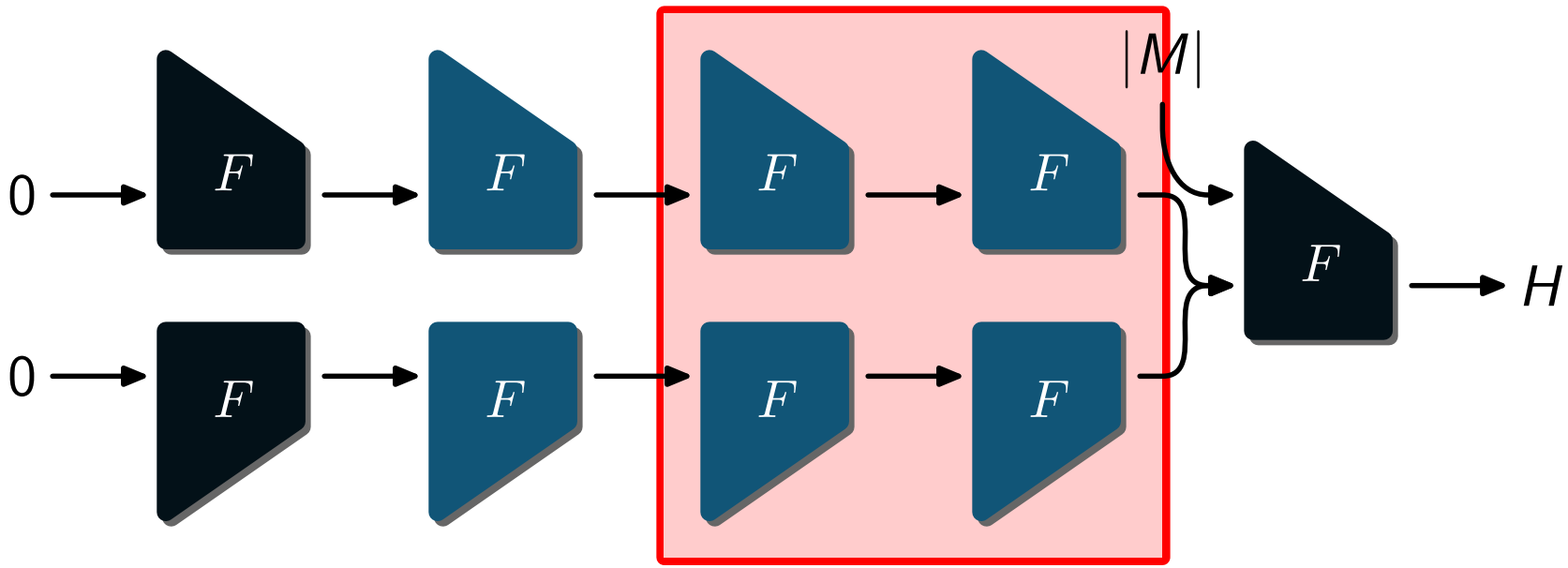


Case

- 2. $|M| = |M^{\star}|$

Two-step CF collisions

Proof for example iteration

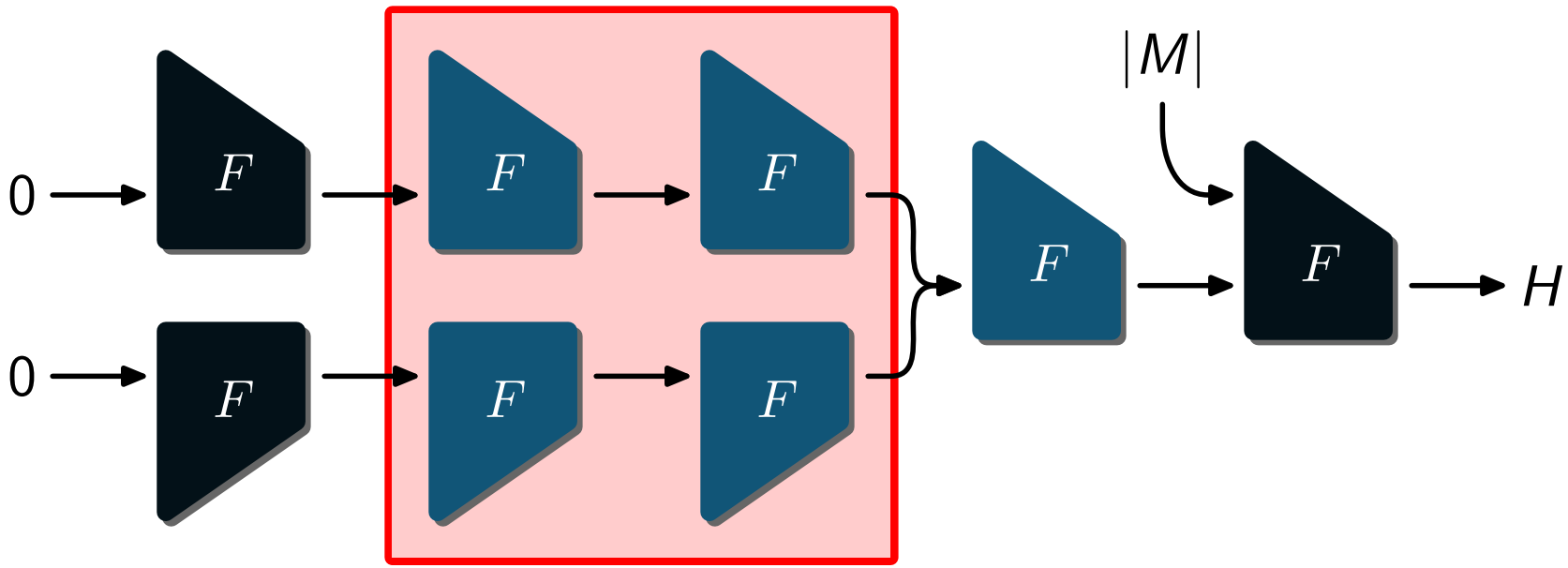


Case

- 2. $|M| = |M^{\star}|$

Two-step CF collisions

Proof for example iteration

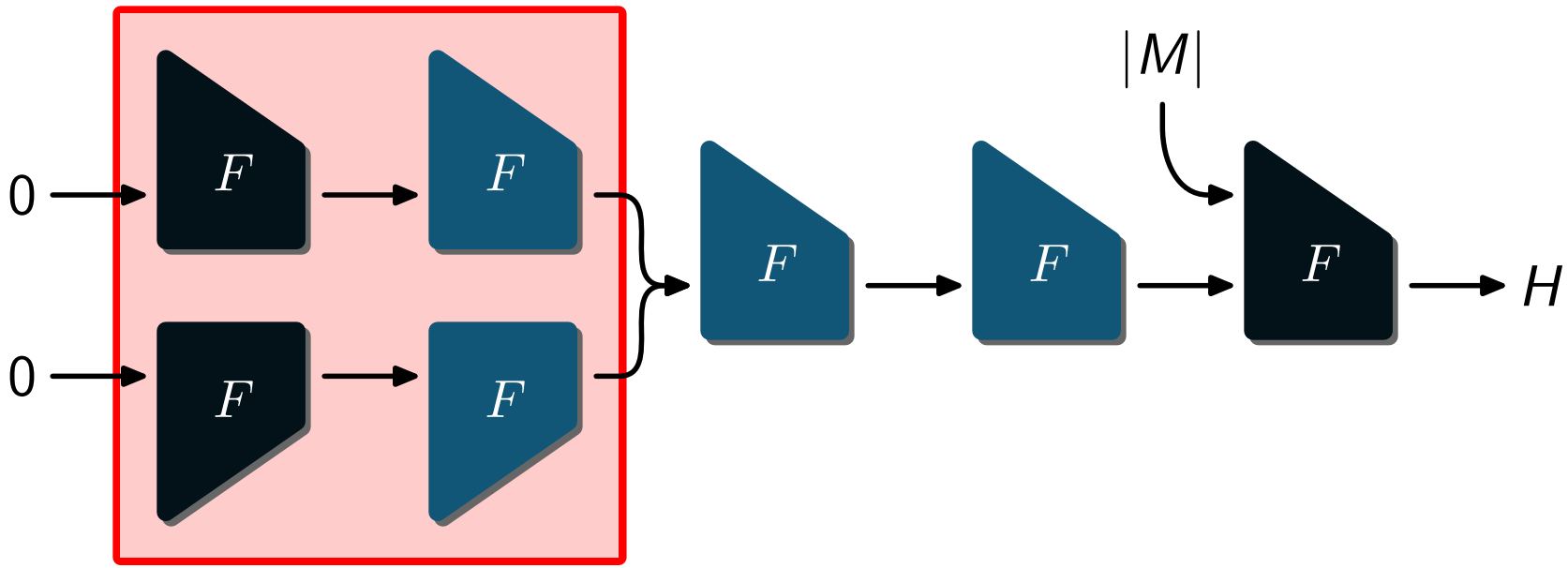


Case

- 2. $|M| = |M^{\star}|$

Two-step CF collisions

Proof for example iteration

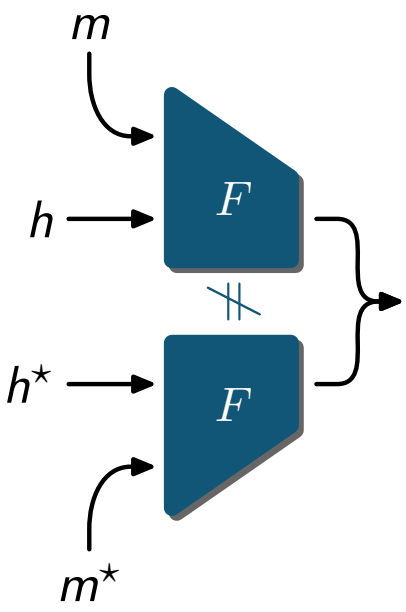


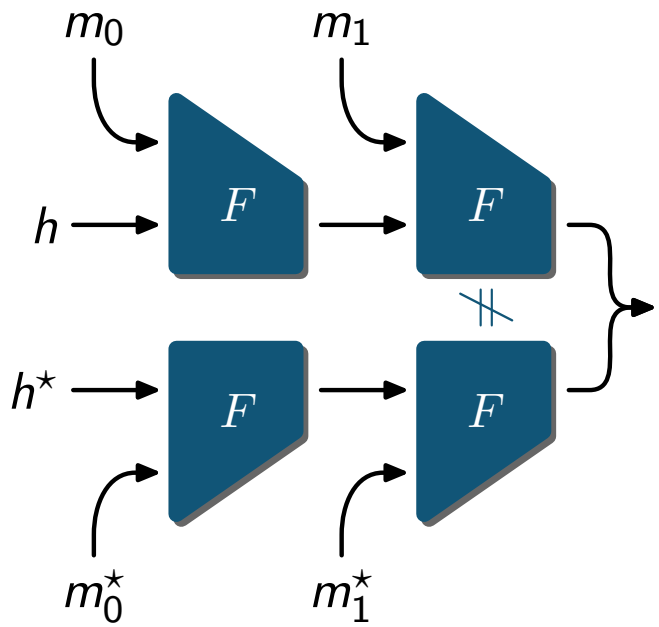
Case

- 2. $|M| = |M^{\star}|$

Two-step CF collisions

A trivial theorem



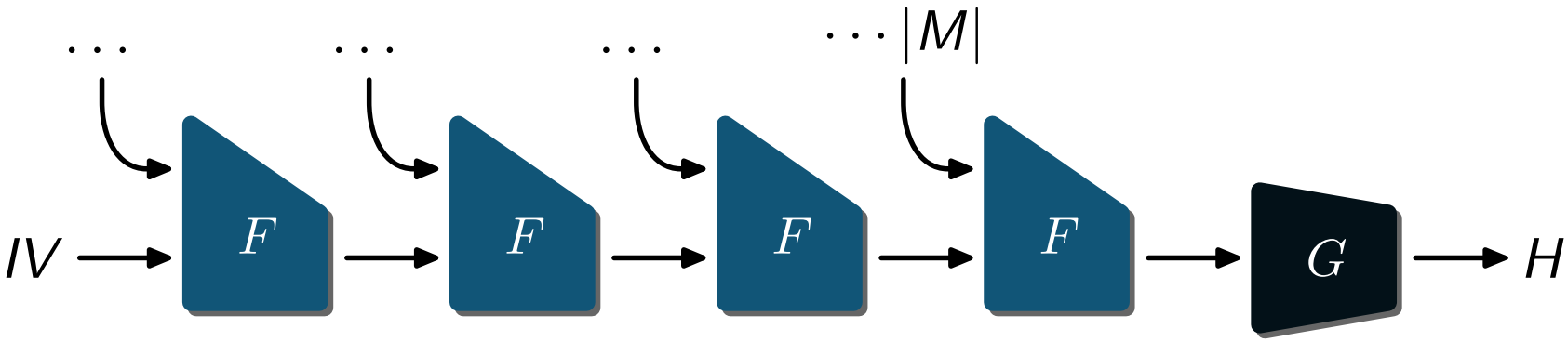


Theorem

Collision secure compression function $\Rightarrow$ Two-step collision secure compression function

Proof: trivial.

A more generic iteration mode

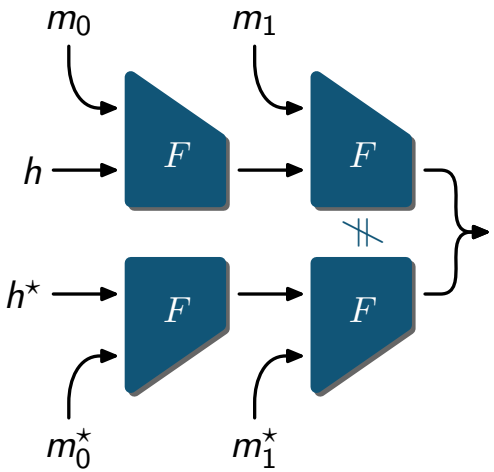


- Output transformation G
- Message length $|M|$ input to last CF call
- NOTE: Damgård-Merkle proof needs to be adapted here anyway, to deal with collisions in G...

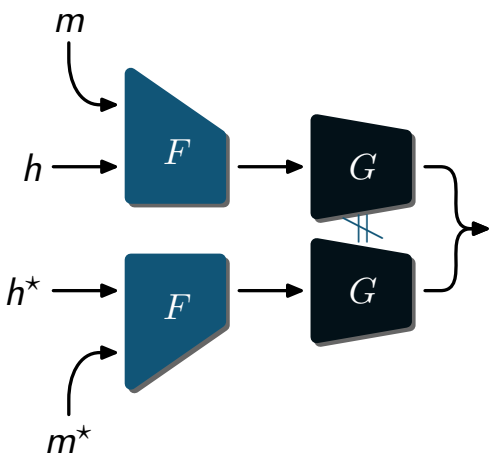
Two-step CF collisions

Updated definition

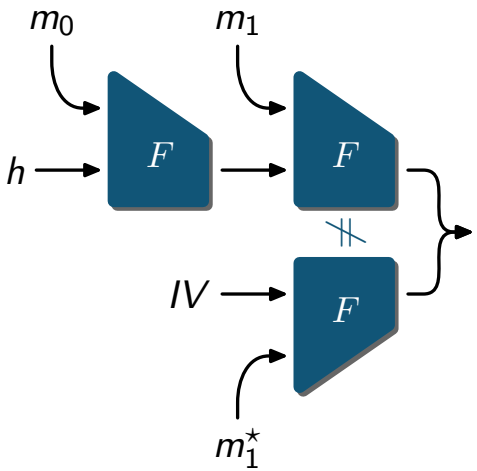
a.



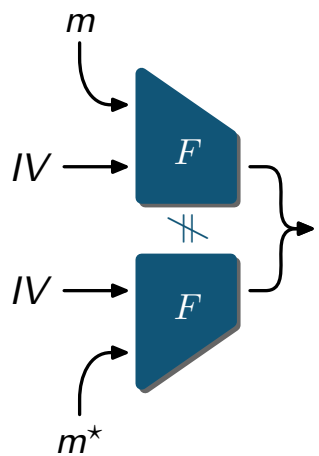
b.



c.

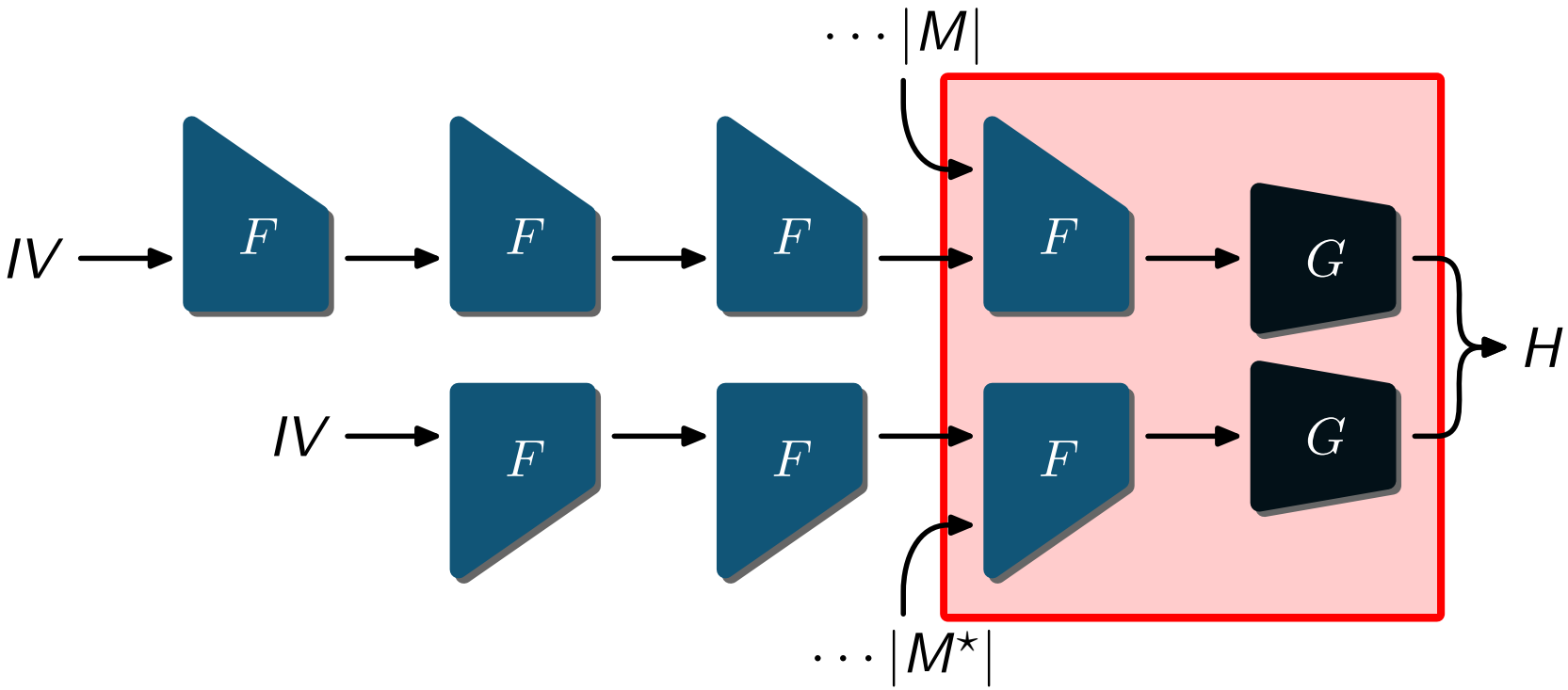


d.



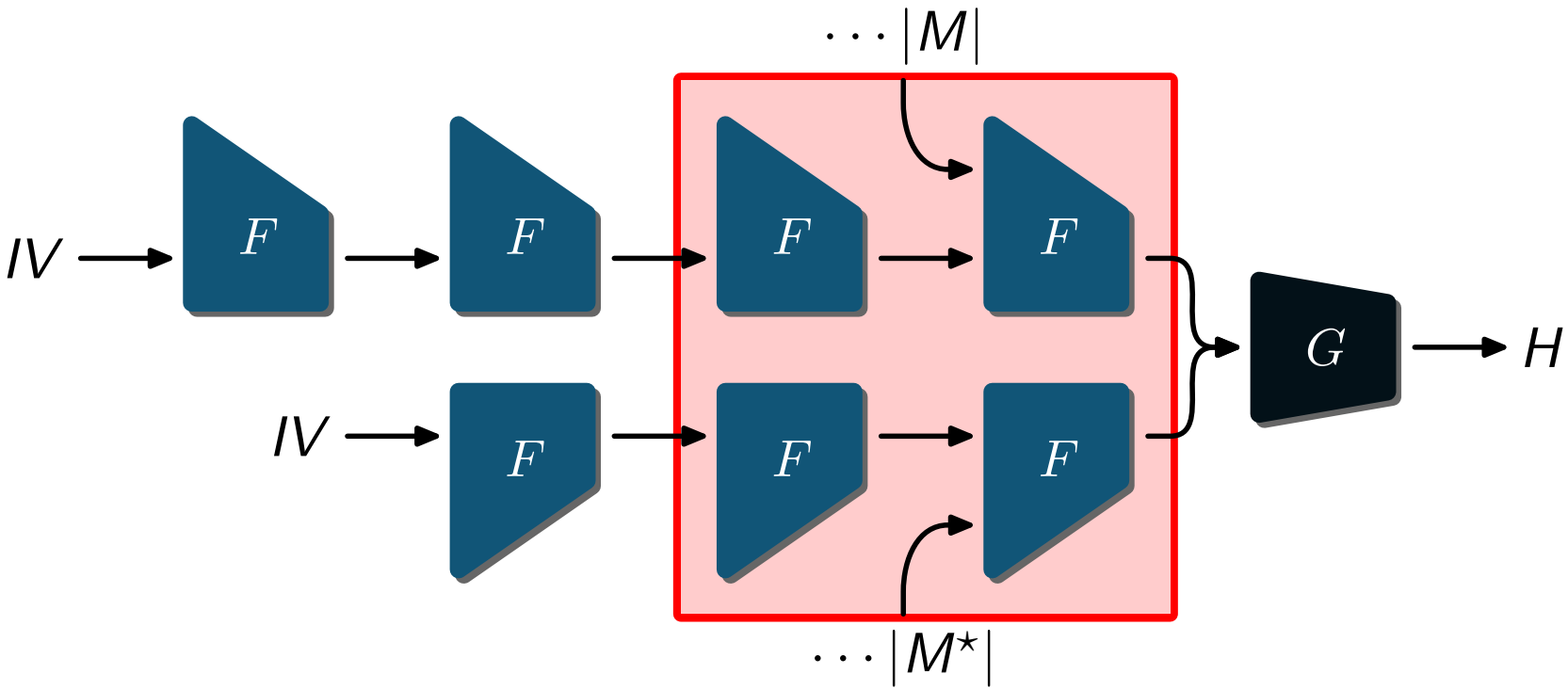
Two-step CF collisions

Proof for generic iteration



Two-step CF collisions

Proof for generic iteration

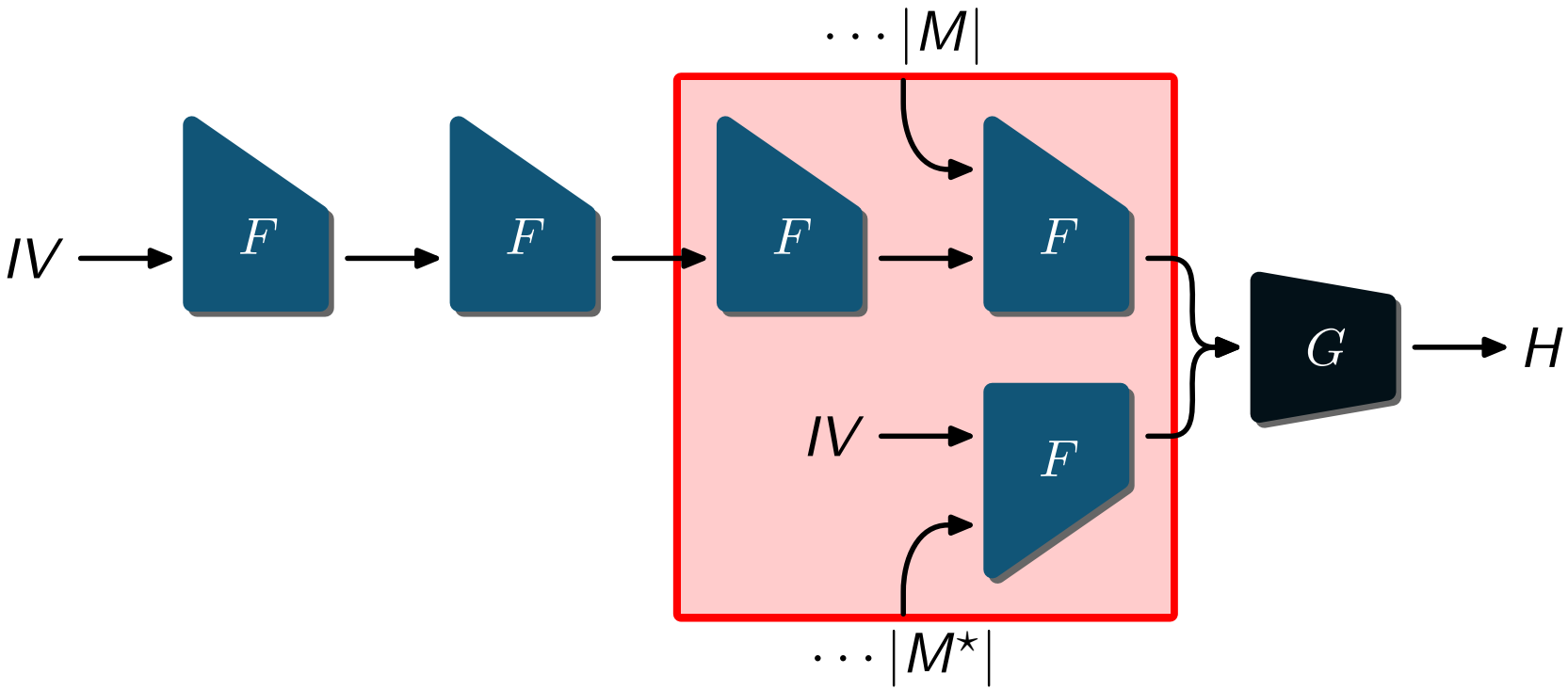


Case

- 1. $|M| \neq |M^\star|$

Two-step CF collisions

Proof for generic iteration

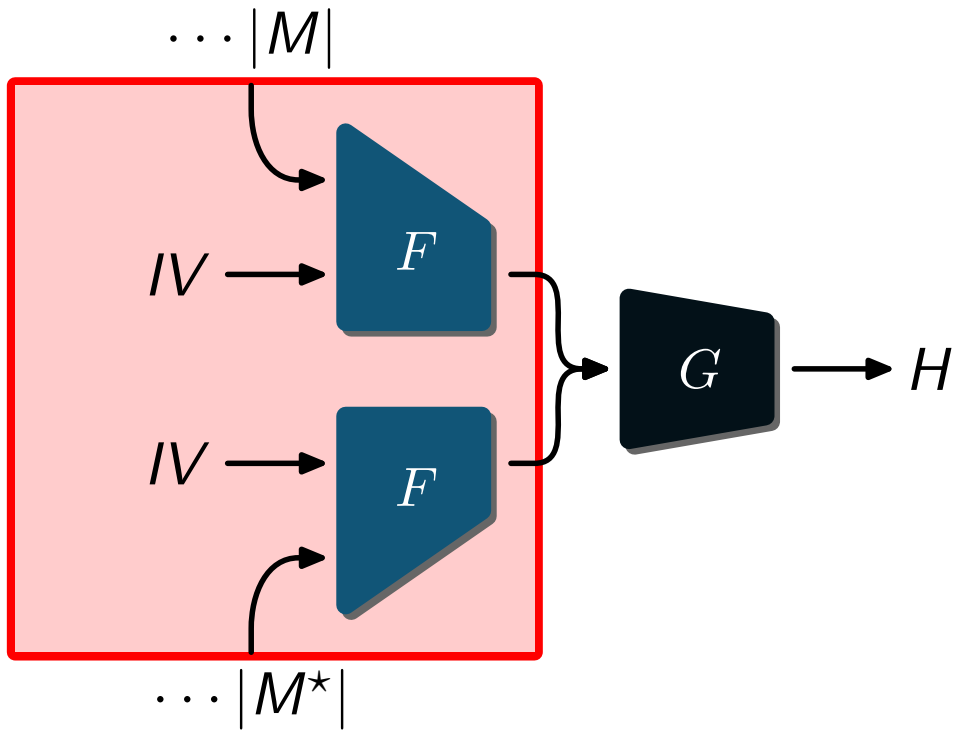


Case

- 1. $|M| \neq |M^\star|$

Two-step CF collisions

Proof for generic iteration

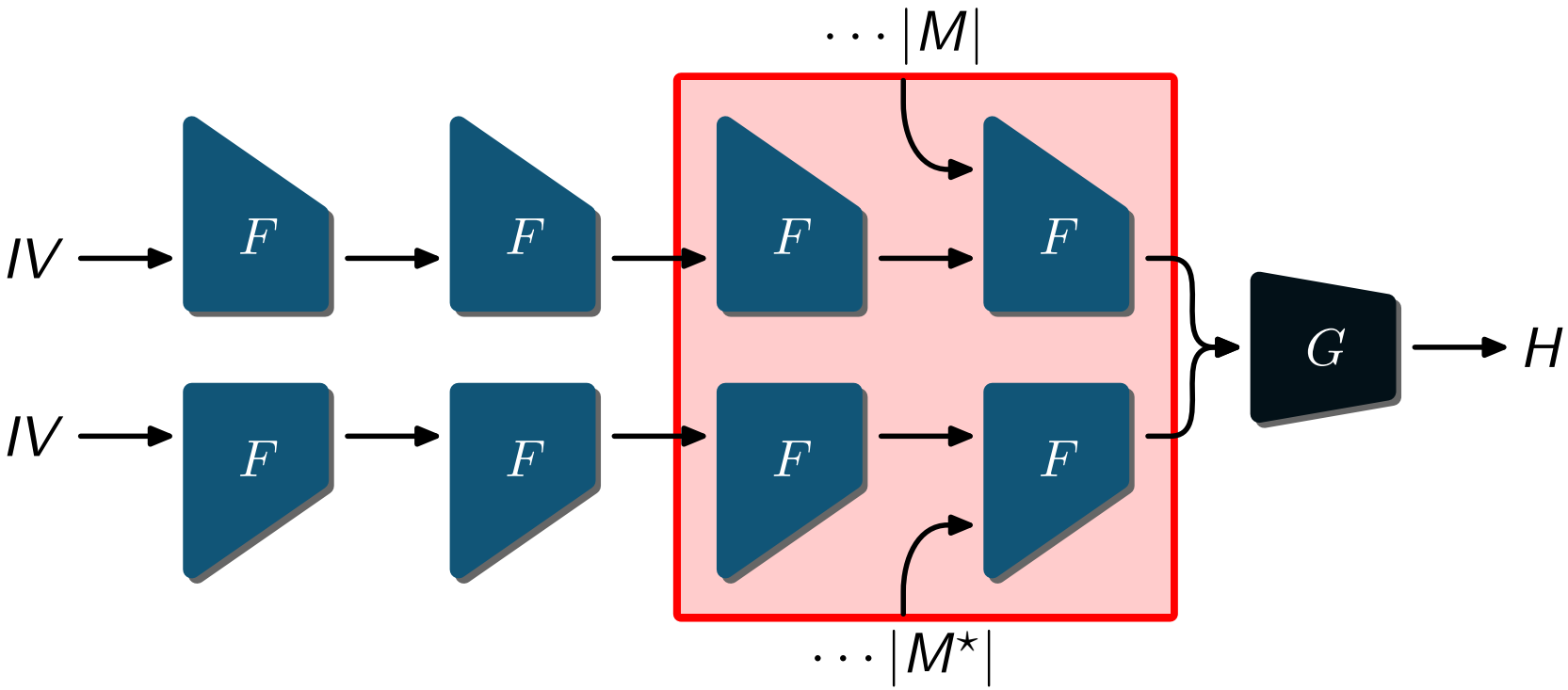


Case

- 1. $|M| \neq |M^\star|$

Two-step CF collisions

Proof for generic iteration

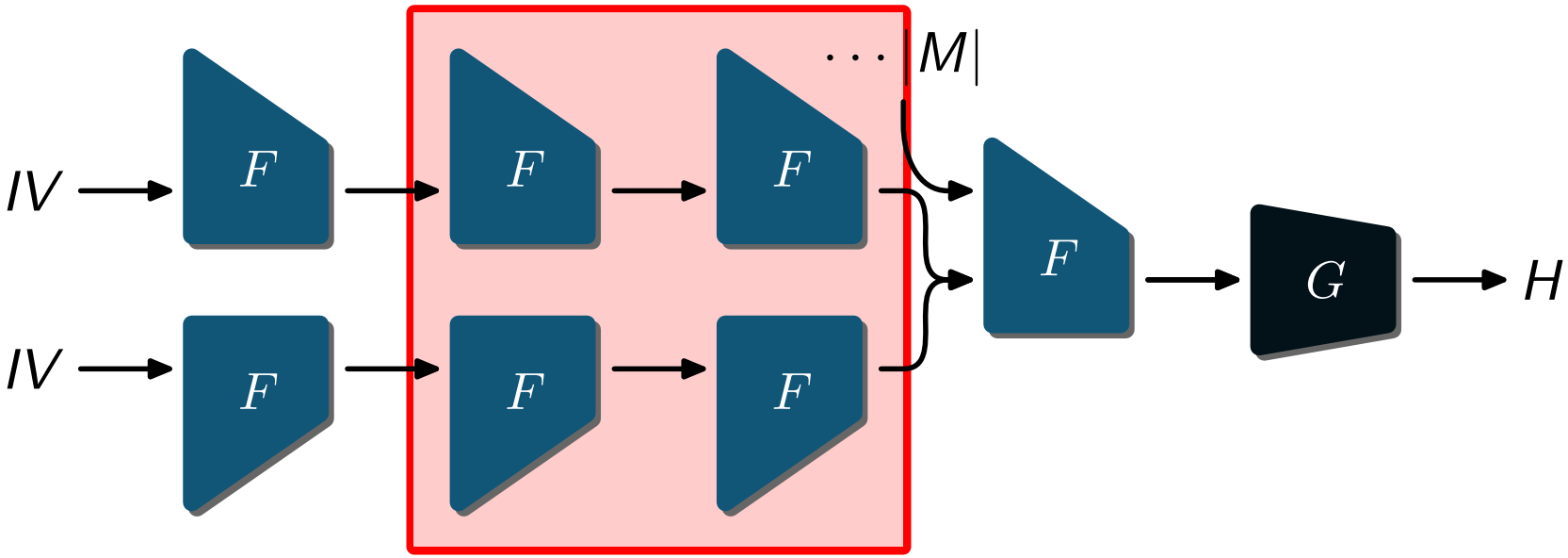


Case

- 2. $|M| = |M^\star|$

Two-step CF collisions

Proof for generic iteration

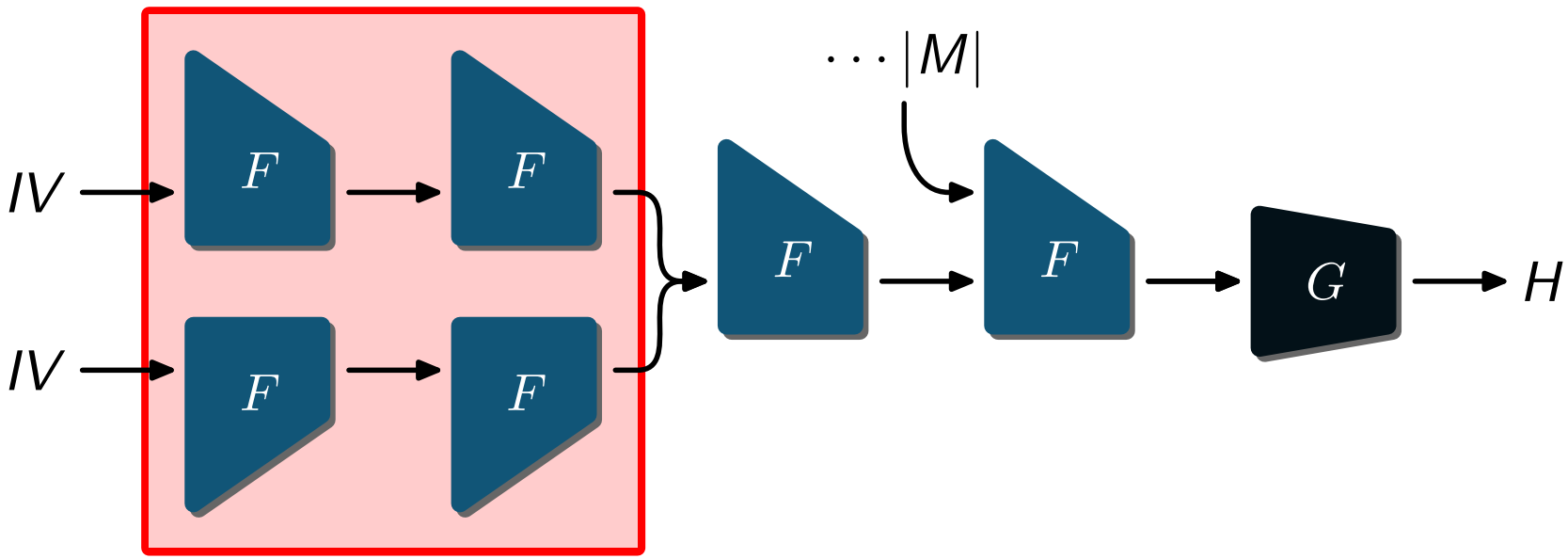


Case

- 2. $|M| = |M^\star|$

Two-step CF collisions

Proof for generic iteration

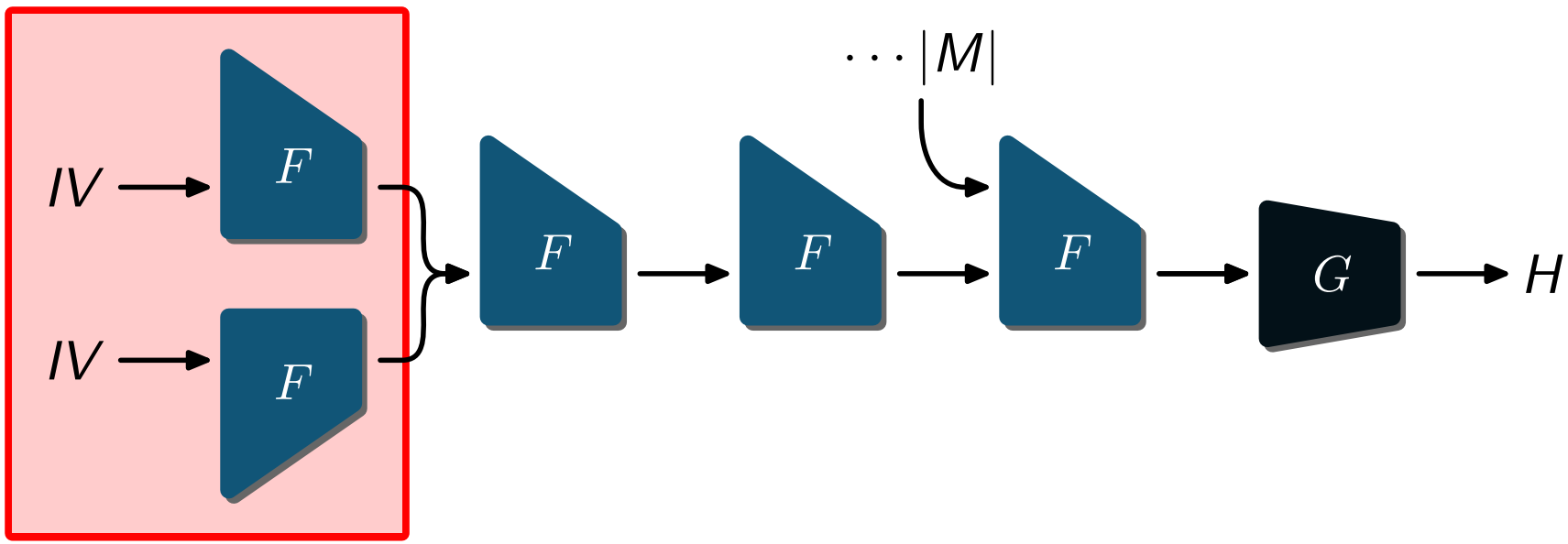


Case

- 2. $|M| = |M^\star|$

Two-step CF collisions

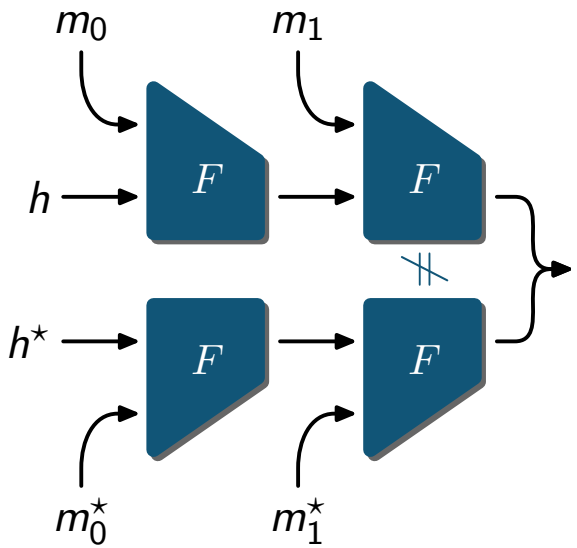
Proof for generic iteration



Case

- 2. $|M| = |M^\star|$

Conclusion



- Resistance against two-step compression function collisions is a **sufficient condition** for hash function collision resistance.
- But still not a **necessary condition** (*e.g.* permutation sponges)

Conclusion

Discussion: Do pseudo-collisions *really* matter?

- Pseudo-collisions are still special, like near-collisions, distinguishers, . . .

Conclusion

Discussion: Do pseudo-collisions *really* matter?

- Pseudo-collisions are still special, like near-collisions, distinguishers, . . .
  - Yes, they are.
- And how about multi-block collision attacks, *cf.* SHA-1?

Conclusion

Discussion: Do pseudo-collisions *really* matter?

- Pseudo-collisions are still special, like near-collisions, distinguishers, ...
  - Yes, they are.
- And how about multi-block collision attacks, *cf.* SHA-1?
  - But those are not just any near-collision and pseudo-collision attack combined!
- But this is not a CF property, but a $2 \times$ CF property!

Conclusion

Discussion: Do pseudo-collisions *really* matter?

- Pseudo-collisions are still special, like near-collisions, distinguishers, ...
  - Yes, they are.
- And how about multi-block collision attacks, *cf.* SHA-1?
  - But those are not just any near-collision and pseudo-collision attack combined!
- But this is not a CF property, but a $2 \times$ CF property!
  - It's still *fixed length* though.
- Why not go to 3 CF's, 4 CF's?

Conclusion

Discussion: Do pseudo-collisions *really* matter?

- Pseudo-collisions are still special, like near-collisions, distinguishers, ...
  - Yes, they are.
- And how about multi-block collision attacks, *cf.* SHA-1?
  - But those are not just any near-collision and pseudo-collision attack combined!
- But this is not a CF property, but a $2 \times$ CF property!
  - It's still *fixed length* though.
- Why not go to 3 CF's, 4 CF's?
  - Possible, but little gain and much more mess!
- But my pseudo-collision attack *does* extend to the hash function!

Conclusion

Discussion: Do pseudo-collisions *really* matter?

- Pseudo-collisions are still special, like near-collisions, distinguishers, ...
  - Yes, they are.
- And how about multi-block collision attacks, *cf.* SHA-1?
  - But those are not just any near-collision and pseudo-collision attack combined!
- But this is not a CF property, but a $2 \times$ CF property!
  - It's still *fixed length* though.
- Why not go to 3 CF's, 4 CF's?
  - Possible, but little gain and much more mess!
- But my pseudo-collision attack *does* extend to the hash function!
  - Perhaps, if they are very efficient and/or there is a good way to *hit* the pseudocollision. This is exactly what this notion captures.
- ...