⚙️ The Skip Ratchet ⏭️

Massive Hash Chains Without All the Waiting

Or: An Encrypted Counting Scheme

https://eprint.iacr.org/2022/1078

github.com/fission-codes

Where's Quinn?

@wilton_quinn

Quinn Wilton
@wilton_quinn

It wasn't an easy decision, but I've pulled out of speaking at Strange Loop this year and @expede was gracious enough to agree to speak in my place.

I was excited to see you all, but I think it's important to avoid stressing my health right now, and I'm excited for next year!

GET WELL SOON 🙏

Brooklyn Zelenka

@expede

Brooklyn Zelenka

@expede

- Cofounder & CTO at Fission
  - https://fission.codes
  - @FissionCodes
  - Infra & SDK for edge apps
- PLT, VMs, DSys — IANYC!
- Standards: UCAN, EIPs, FVM, Multiformats, &c

Brooklyn Zelenka

@expede

- Cofounder & CTO at Fission
  - https://fission.codes
  - @FissionCodes
  - Infra & SDK for edge apps
- PLT, VMs, DSys — IANYC!
- Standards: UCAN, EIPs, FVM, Multiformats, &c

Skip Ratchet

A Hierarchical Hash System

Brooklyn Zelenka

https://eprint.iacr.org/2022/1078.pdf

Motivation

At a High Level

Motivation 💭

Uses

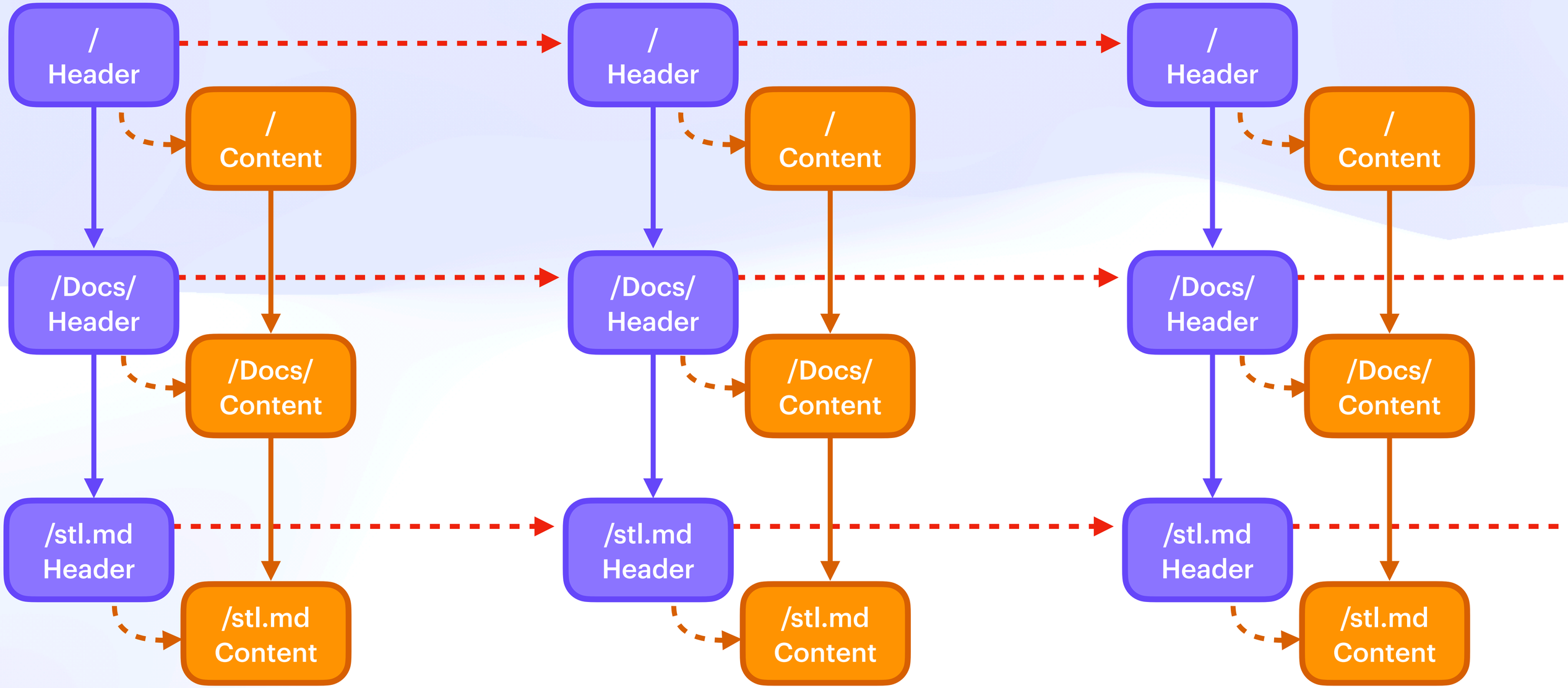
Motivation 💭

Uses

- Local-first data
- WNFS: distributed private file system
- Implemented in at least TypeScript, Rust, Golang
- Electric coins, streaming payment channels
- HD wallets (key management)
- Long-running, asymmetric channels

Motivation 💭

Deterministic Keys in WNFS



Motivation 💭

A Tale As Old as Time

Motivation 💭

A Tale As Old as Time

- PLT cross-pollination driving innovation in cryptography
- Really simple idea with lots of applications
- Interesting way of arriving at it / analogies to other areas
- Let's talk number systems & applied cryptography!

Fundamentals

Hash Chains, Lamport OTP, & More!

⛓️

Fundamentals ⛓️

Hash Chains

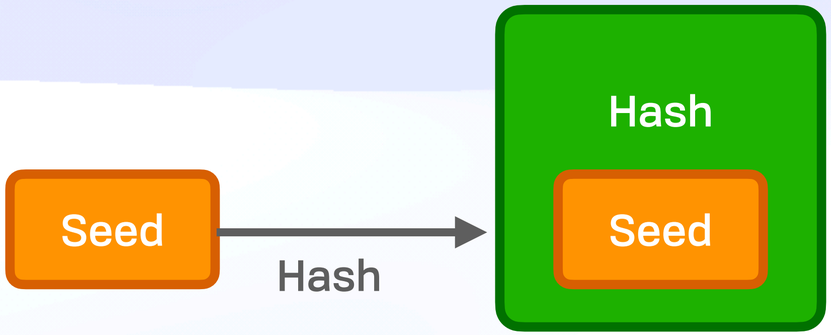
Fundamentals ⛓️

Hash Chains

Seed

Fundamentals ⛓️

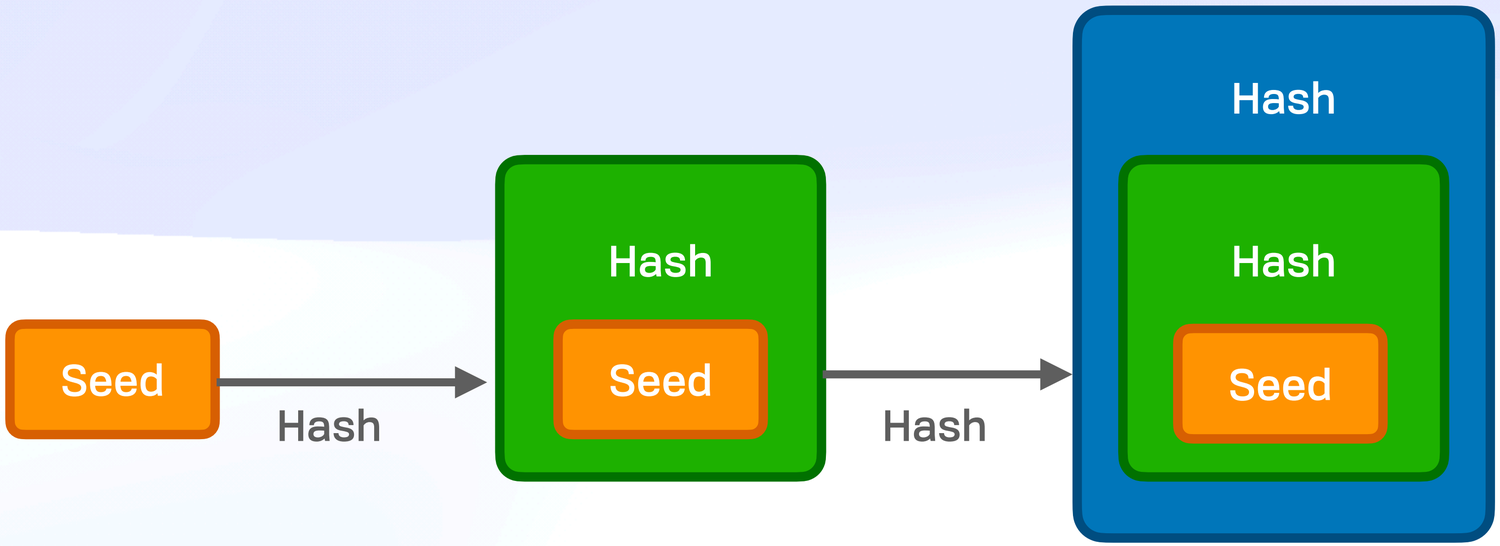
Hash Chains



Hash(seed)

Fundamentals ⛓️

Hash Chains

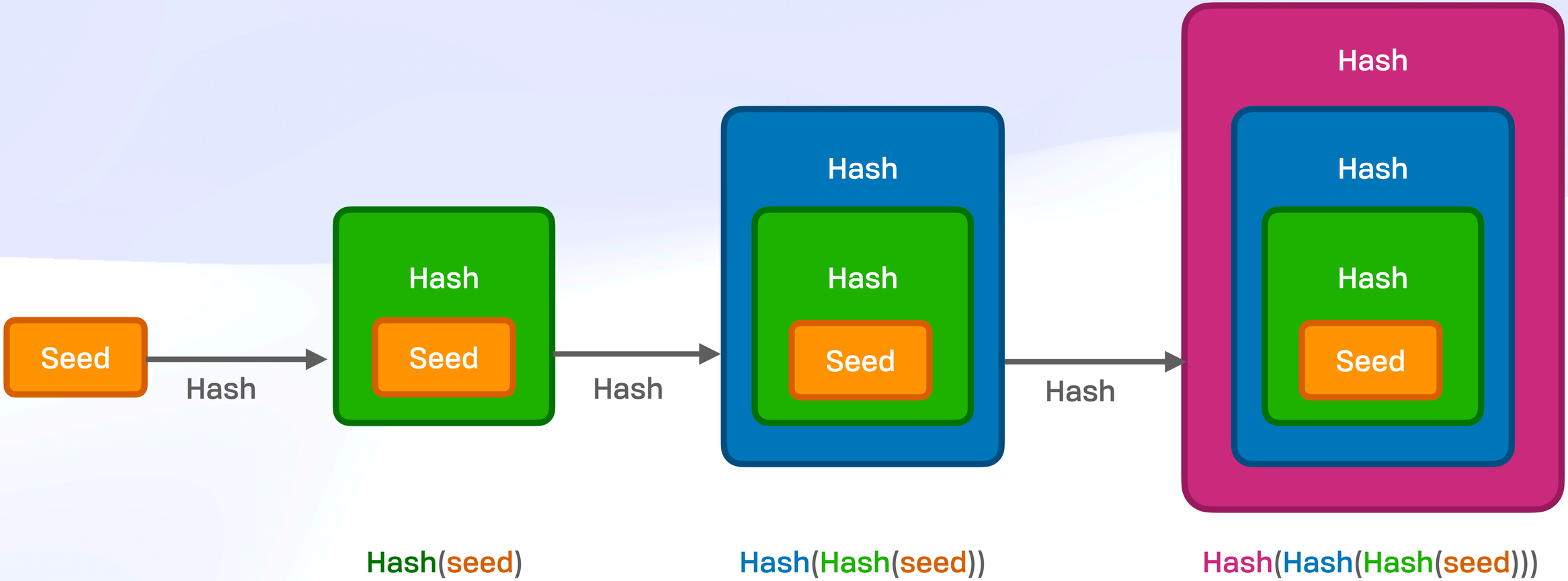


Hash(seed)

Hash(Hash(seed))

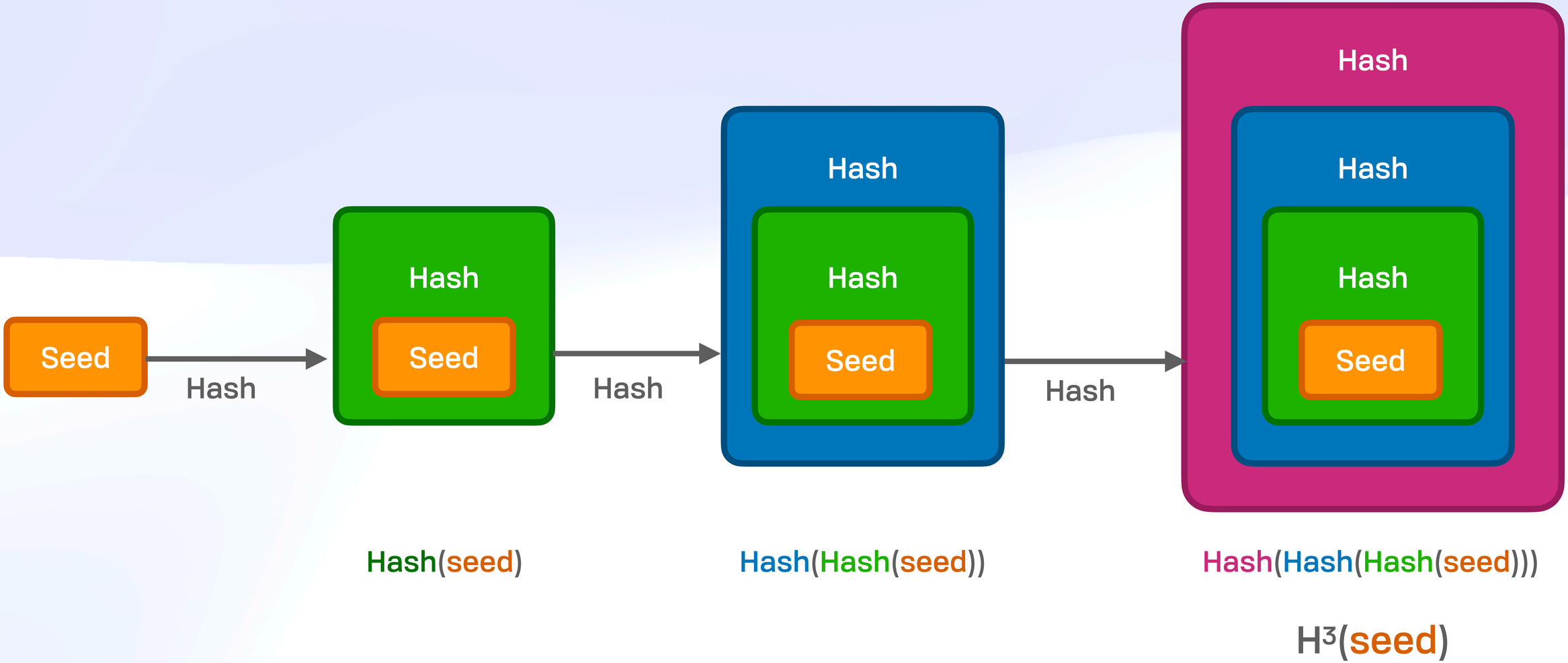
Fundamentals ⛓️

Hash Chains



Fundamentals ⛓️

Hash Chains



Fundamentals ⛓️

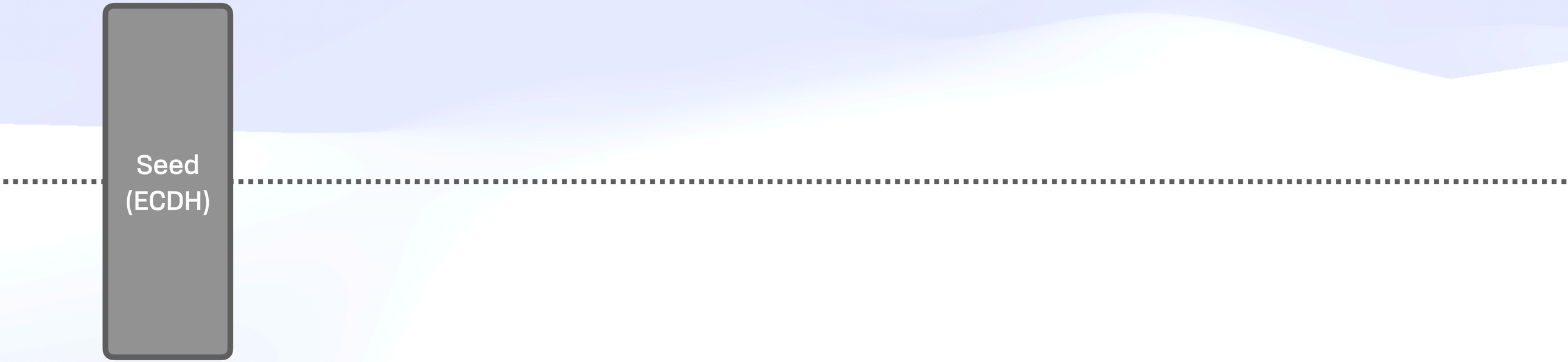
Pseudoradom Stream

Fundamentals ⛓️

Pseudoradom Stream

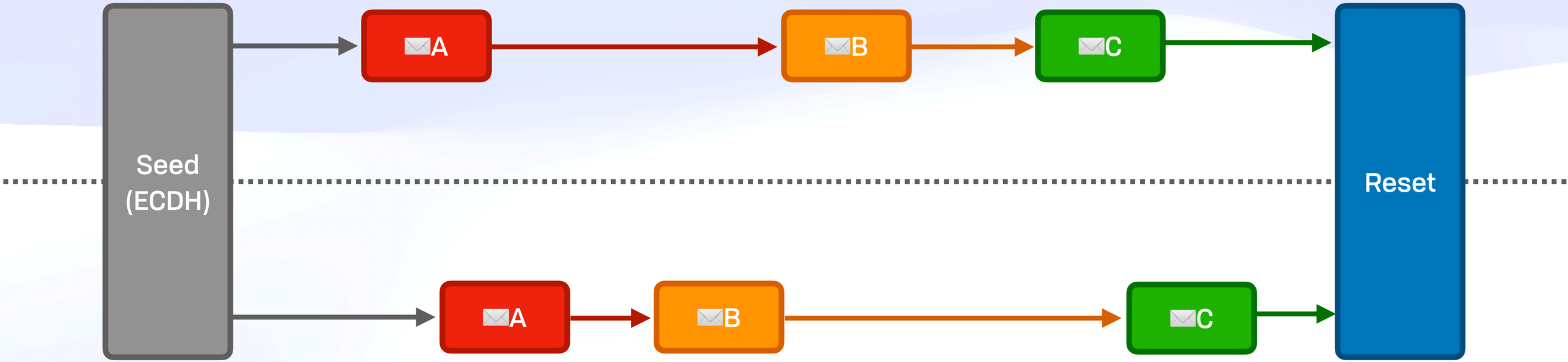
Fundamentals ⛓️

Pseudoradom Stream



Fundamentals ⛓️

Pseudoradom Stream



Fundamentals ⛓️

Lamport OTP, S/KEY

Fundamentals ⛓️

Lamport OTP, S/KEY

Fundamentals ⛓️

Lamport OTP, S/KEY

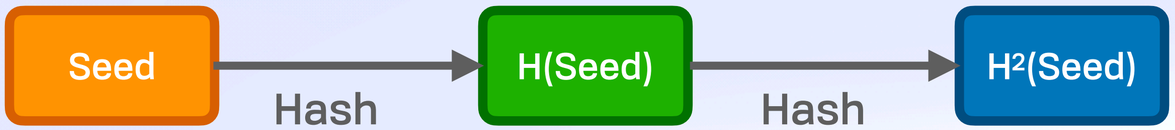
Seed

Fundamentals ⛓️

Lamport OTP, S/KEY

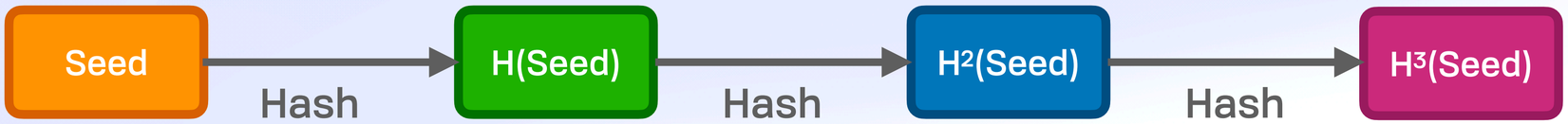
Fundamentals ⛓️

Lamport OTP, S/KEY



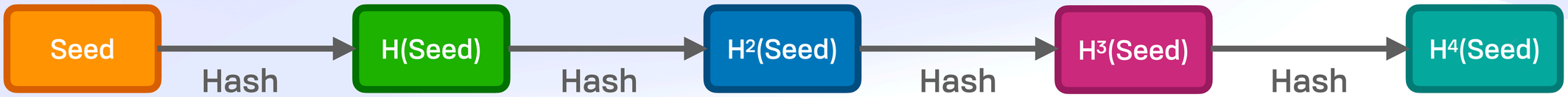
Fundamentals ⛓️

Lamport OTP, S/KEY



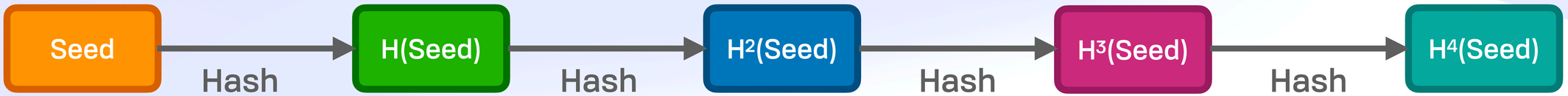
Fundamentals ⛓️

Lamport OTP, S/KEY



Fundamentals ⛓️

Lamport OTP, S/KEY

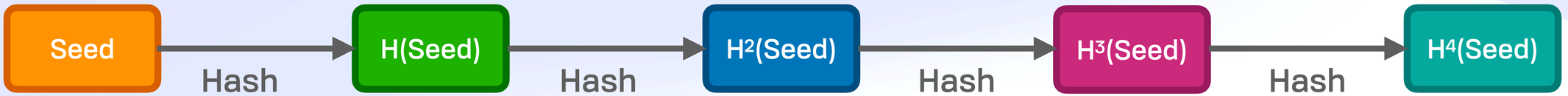


Prover

Verifier

Fundamentals ⛓️

Lamport OTP, S/KEY



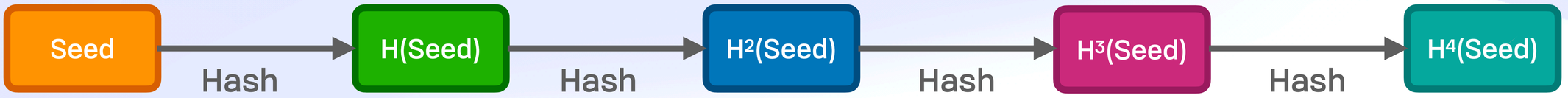
Prover

Hˣ(Seed)

Verifier

Fundamentals ⛓️

Lamport OTP, S/KEY



Prover

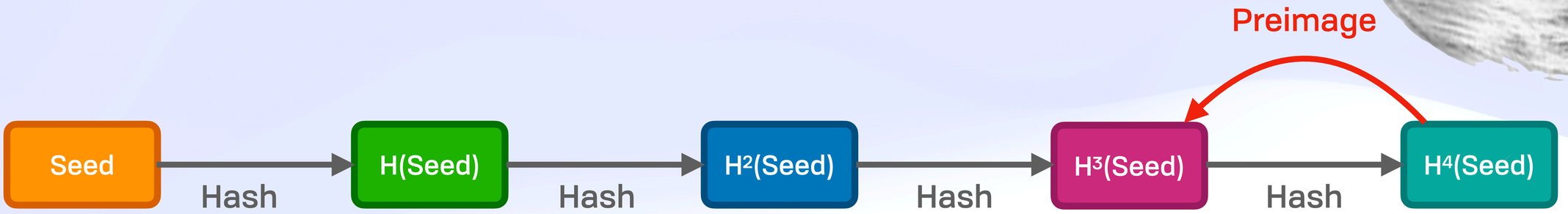
H^x(Seed)

Verifier

H^x

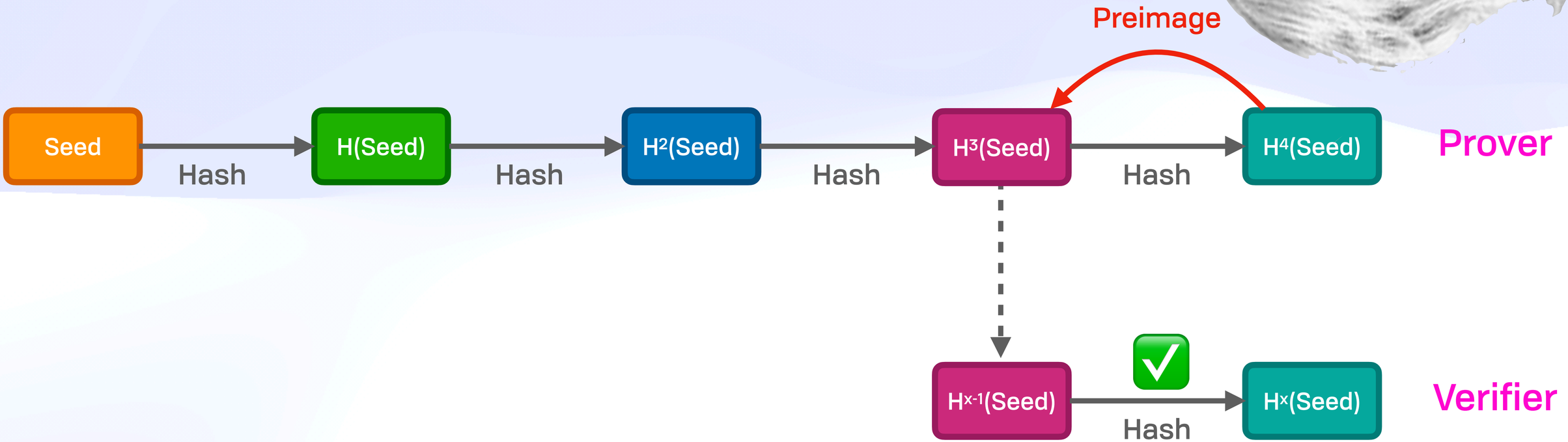
Fundamentals ⛓️

Lamport OTP, S/KEY



Fundamentals ⛓️

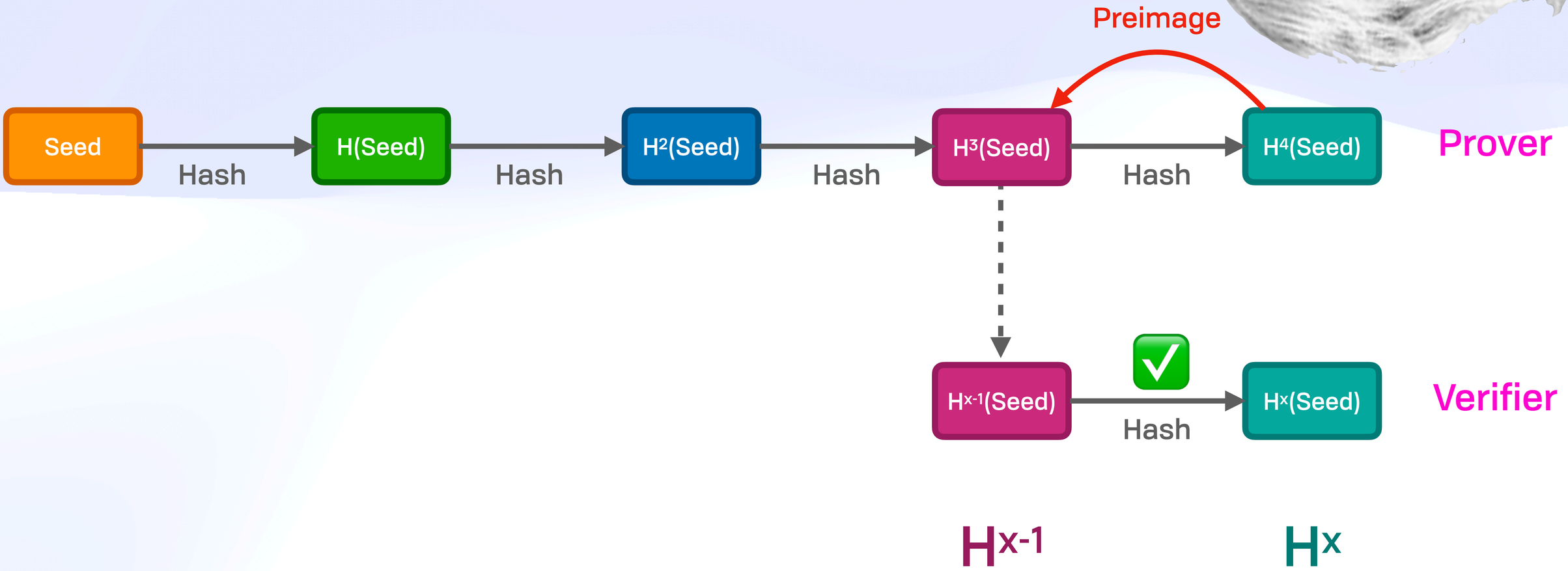
Lamport OTP, S/KEY



H^x

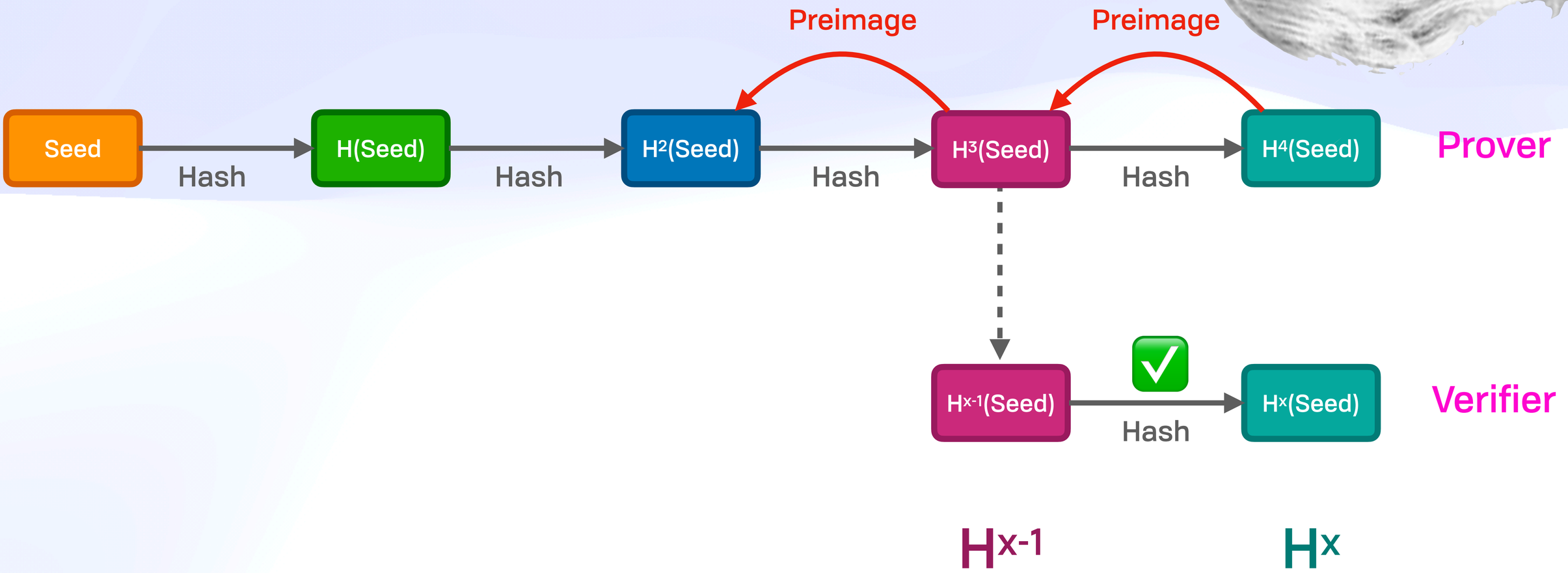
Fundamentals ⛓️

Lamport OTP, S/KEY



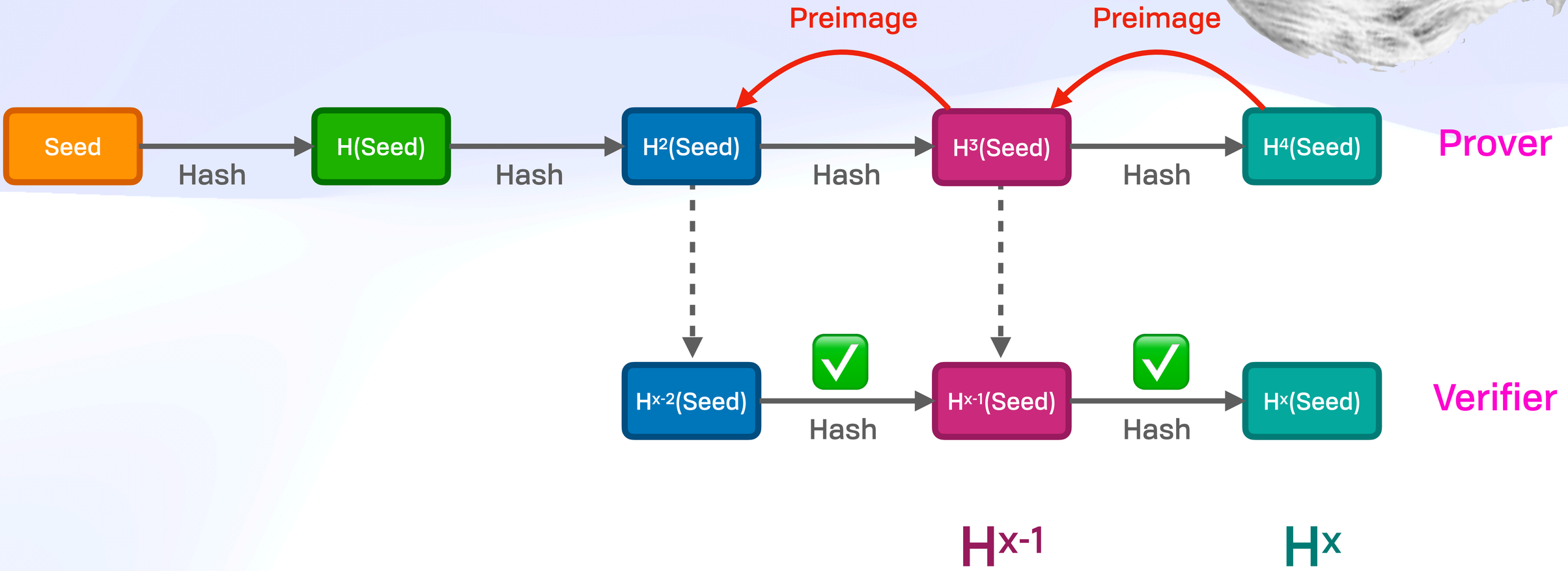
Fundamentals ⛓️

Lamport OTP, S/KEY



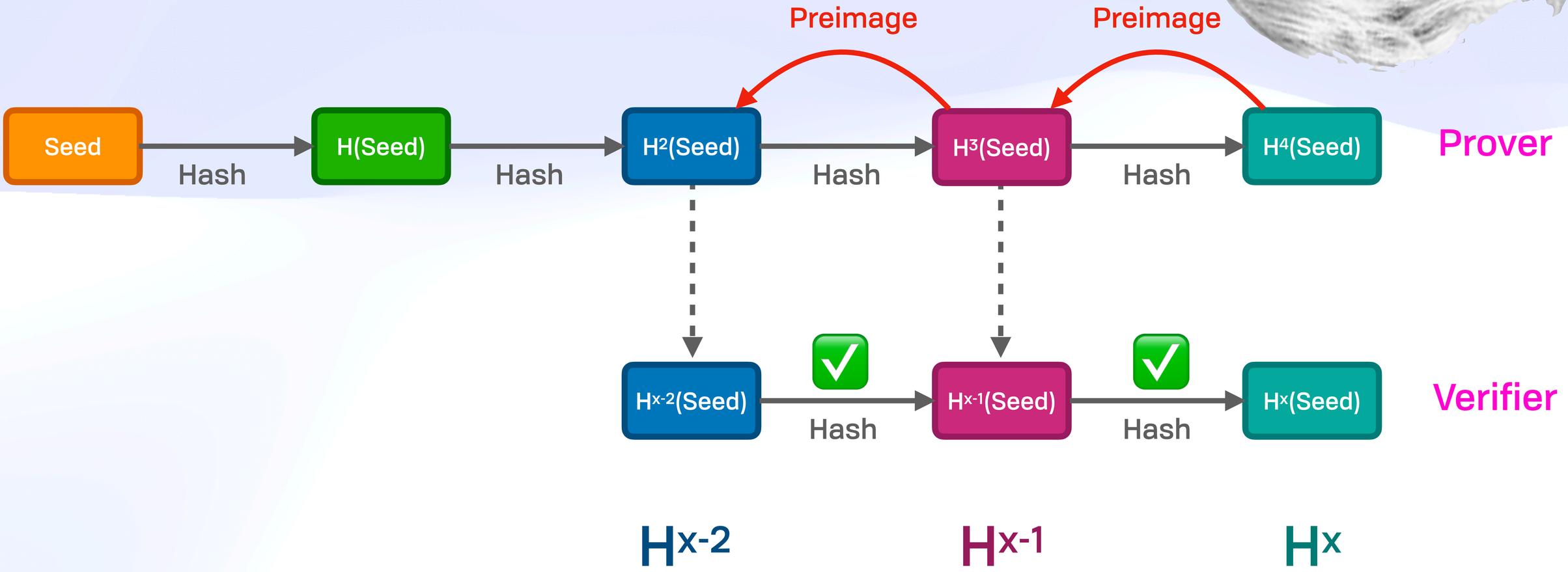
Fundamentals ⛓️

Lamport OTP, S/KEY



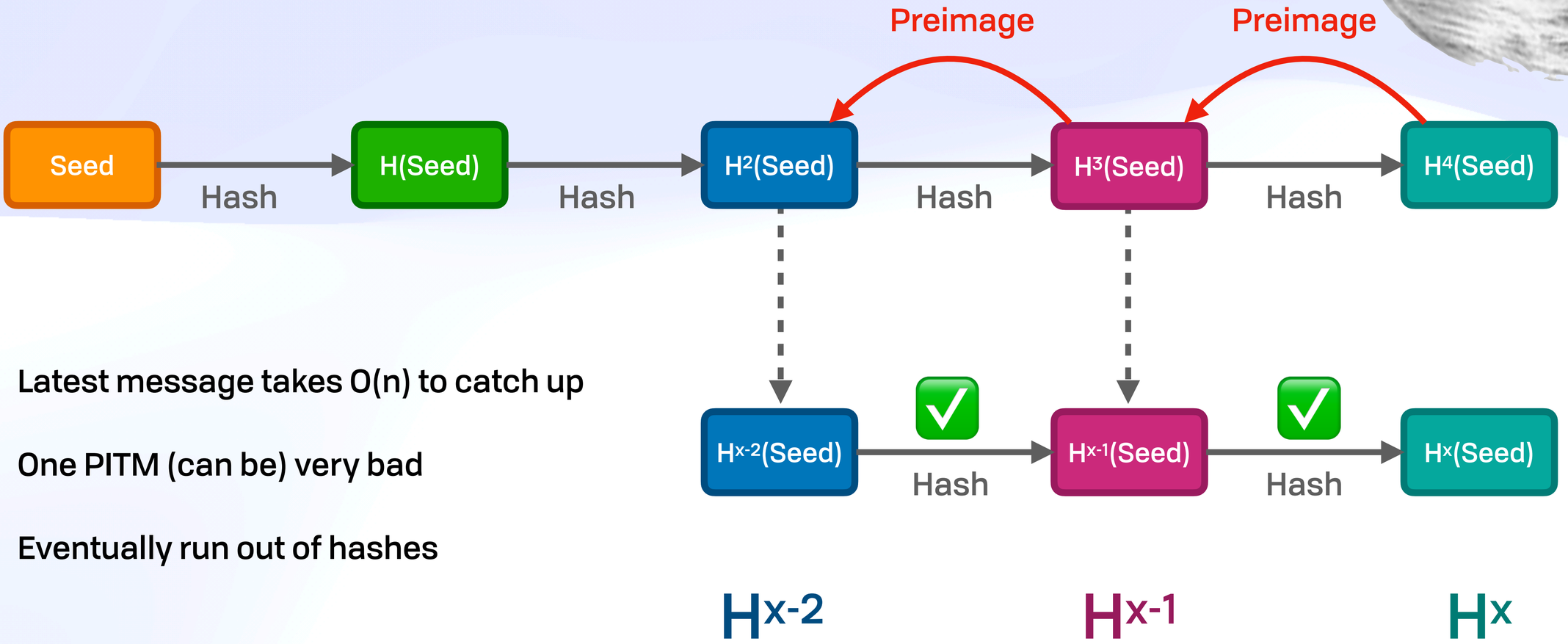
Fundamentals ⛓️

Lamport OTP, S/KEY



Fundamentals ⛓

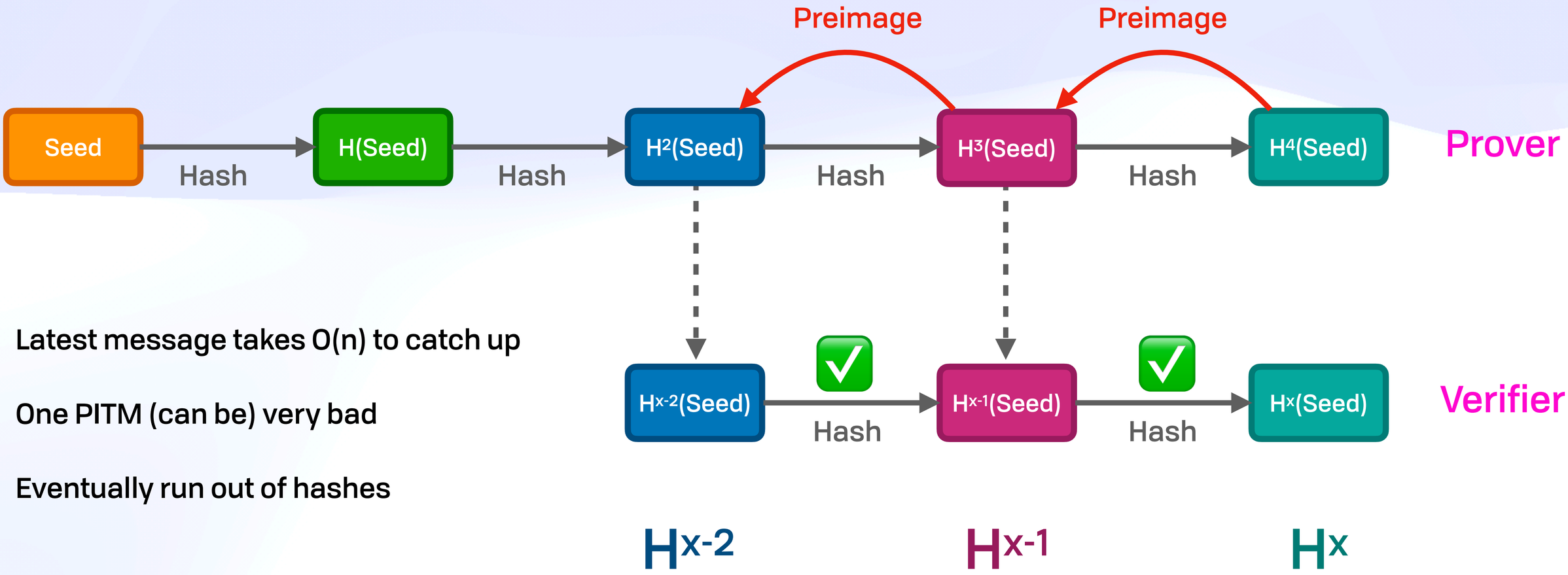
Lamport OTP, S/KEY



- Latest message takes O(n) to catch up
- One PITM (can be) very bad
- Eventually run out of hashes

Fundamentals ⛓️

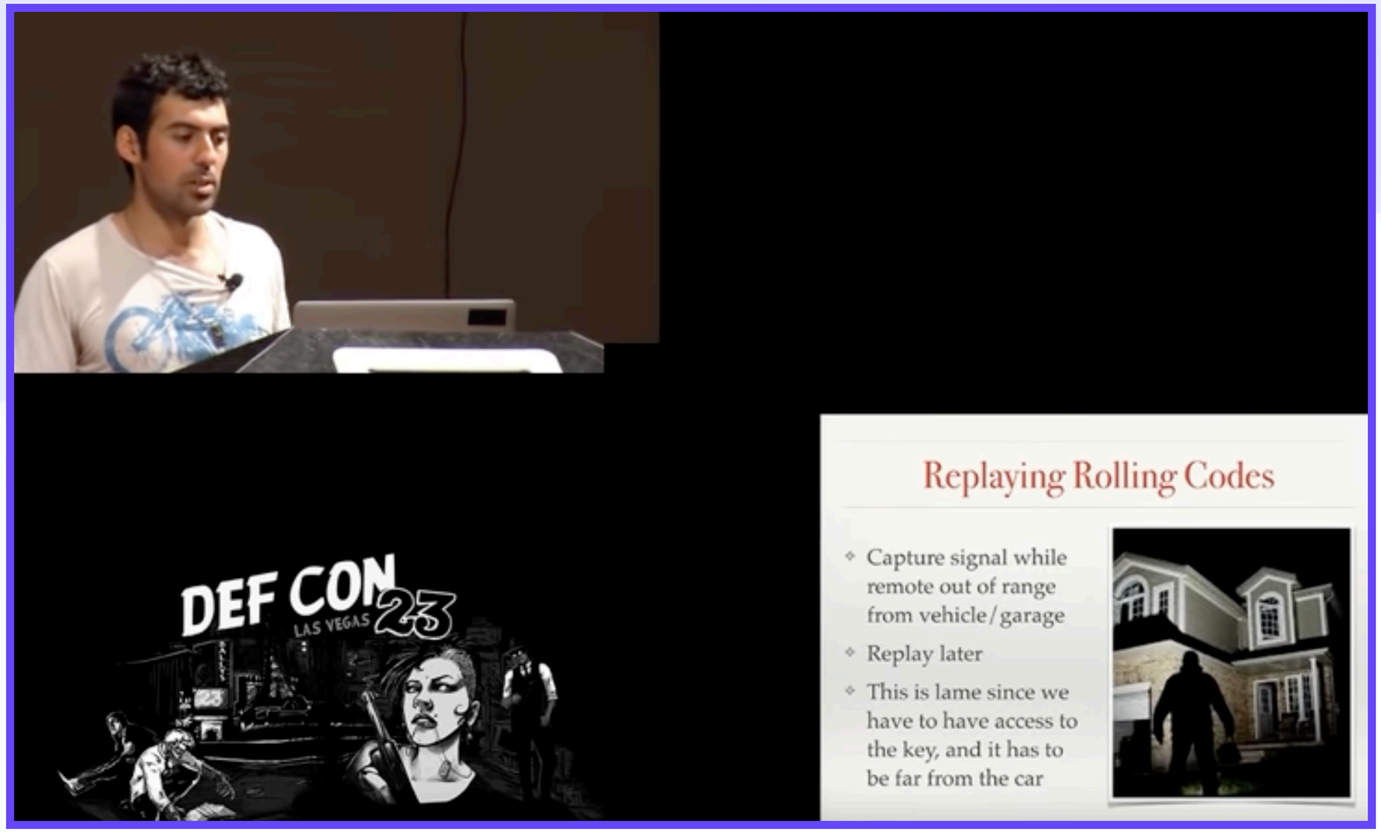
Lamport OTP, S/KEY



- Latest message takes O(n) to catch up
- One PITM (can be) very bad
- Eventually run out of hashes

Fundamentals ⛓️

Samy Kamkar's Drive it like you Hacked it



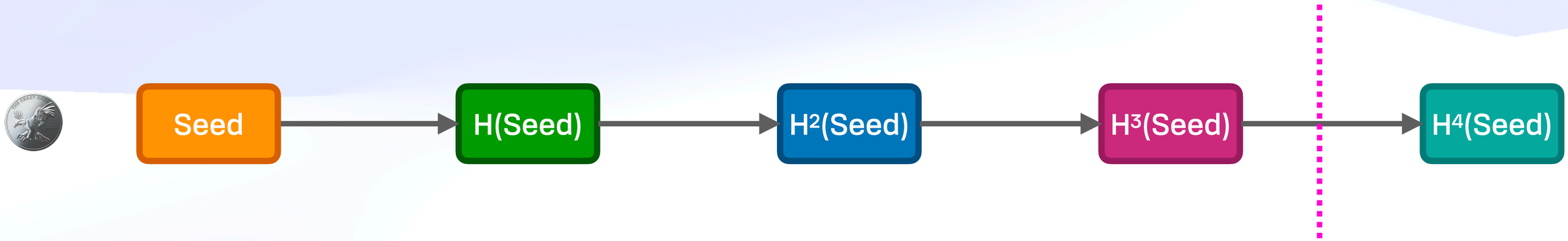
https://www.youtube.com/watch?v=UNgvShN4USU

Fundamentals ⛓️

Micropayments (Simplified PayWord)

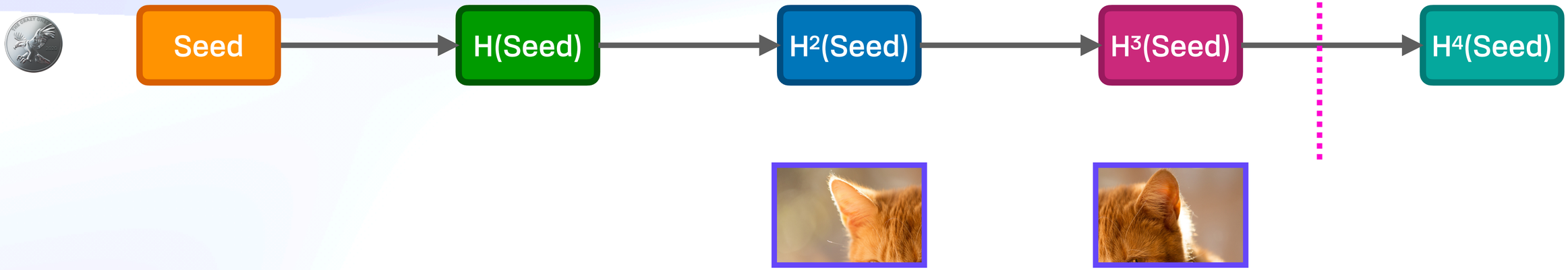
Fundamentals ⛓️

Micropayments (Simplified PayWord)



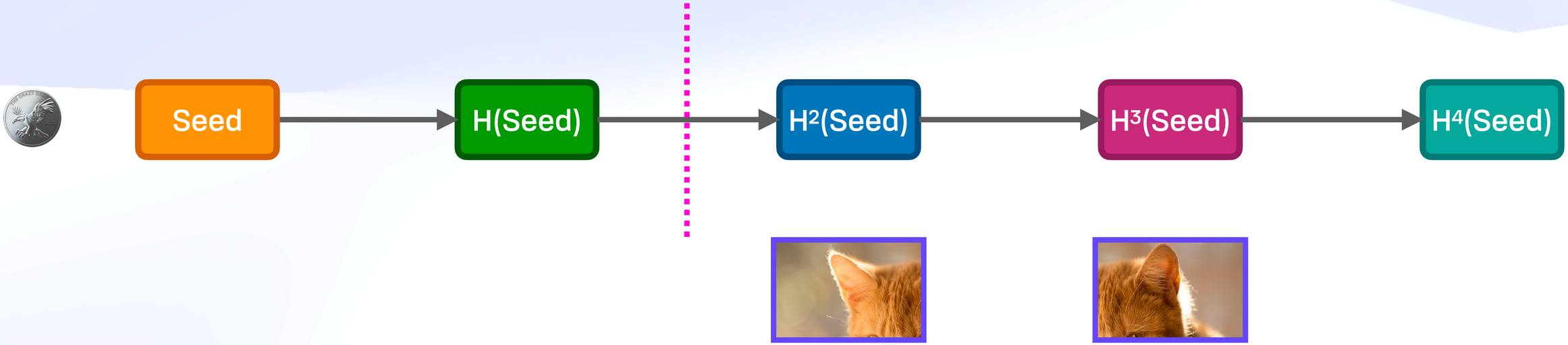
Fundamentals ⛓️

Micropayments (Simplified PayWord)



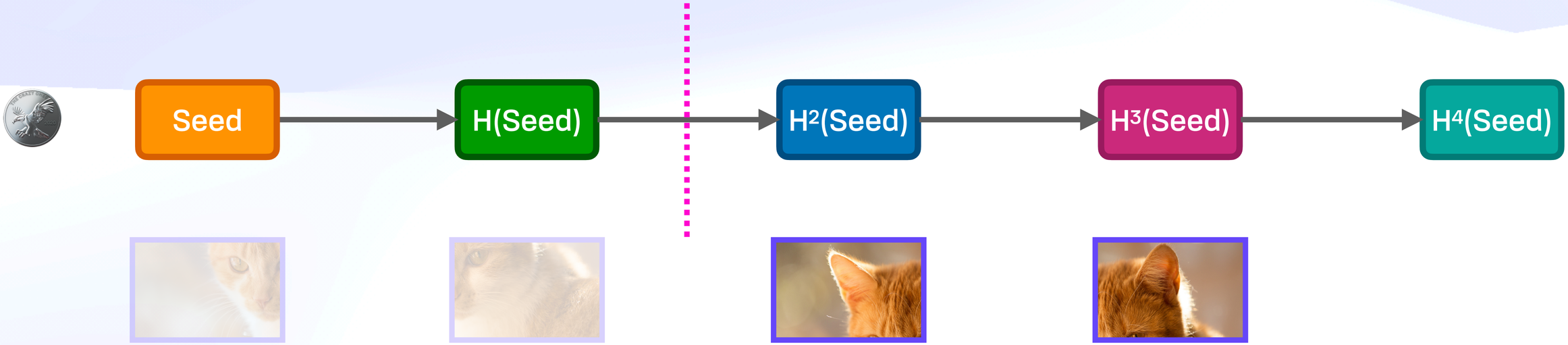
Fundamentals ⛓️

Micropayments (Simplified PayWord)



Fundamentals ⛓️

Micropayments (Simplified PayWord)



Analogy From Counting

One Hash, Two Hash...

"Can you do Addition?" the White Queen said.
"What's one and one and one and one and one and one and one and one and one and one?"

"I don't know," said Alice. ***"I lost count."***

"She can't do Addition," the Red Queen interrupted.

— **Lewis Carroll, Through the Looking Glass**

Analogy From Counting 🔢

The Ishango Bone

Ishango Bone
Congo
~20,000 years

Lebombo Bone
South Africa
~44,000 years

Joeykentin CC-BY-SA 4.0
https://commons.wikimedia.org/wiki/File:Ishango_bone.jpg

🌾 Agriculture ~ 11.5k years
🐷 Herding ~ 10k years

Analogy From Counting 🔢

Unary Counting

Analogy From Counting 🔢

Unary Counting

Analogy From Counting 🔢

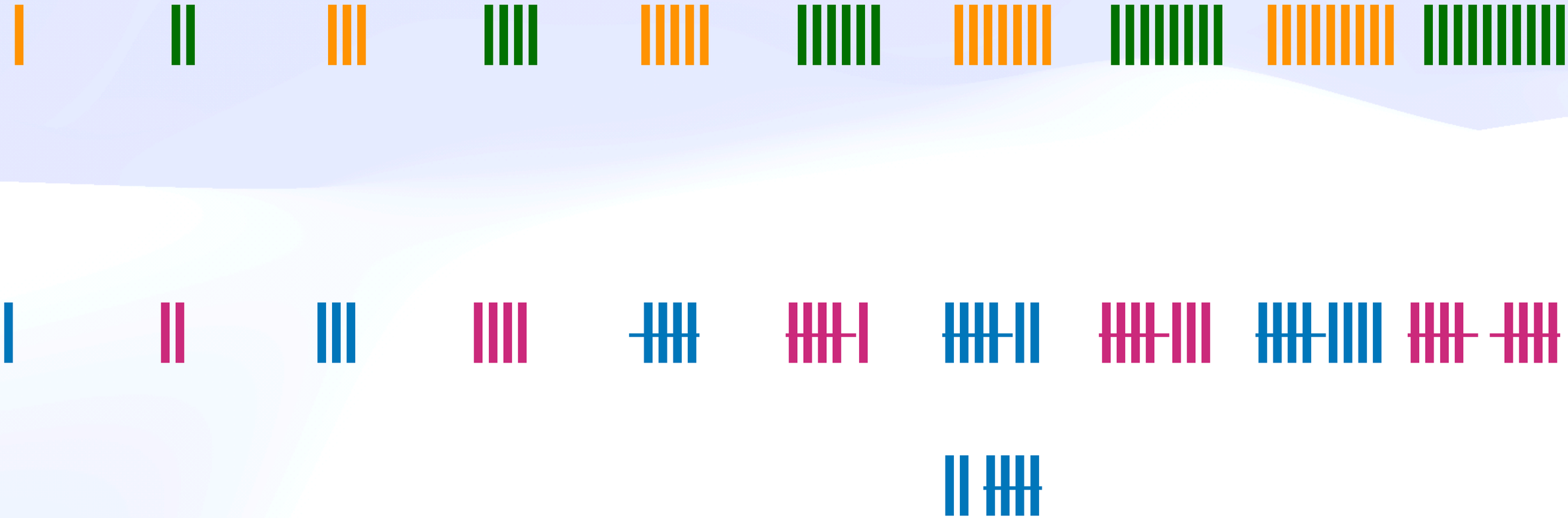
Unary Counting

Analogy From Counting 🔢

Unary Counting

Analogy From Counting 🔢

Unary Counting



Analogy From Counting 🔢

Unary Constructors

```
data Peano = Zero | Succ Peano
```

Analogy From Counting 🔢

Unary Constructors

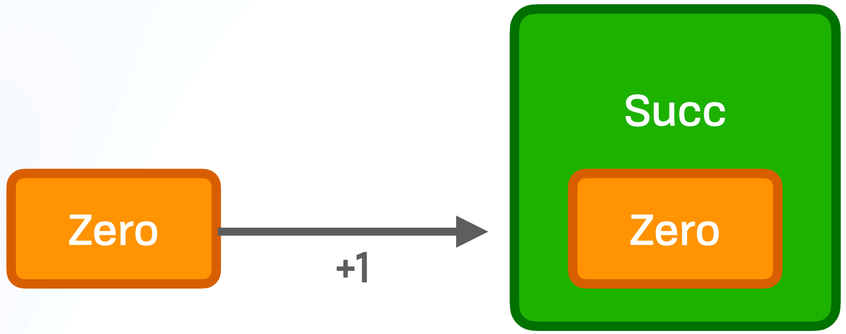
```
data Peano = Zero | Succ Peano
```

Zero

Analogy From Counting 🔢

Unary Constructors

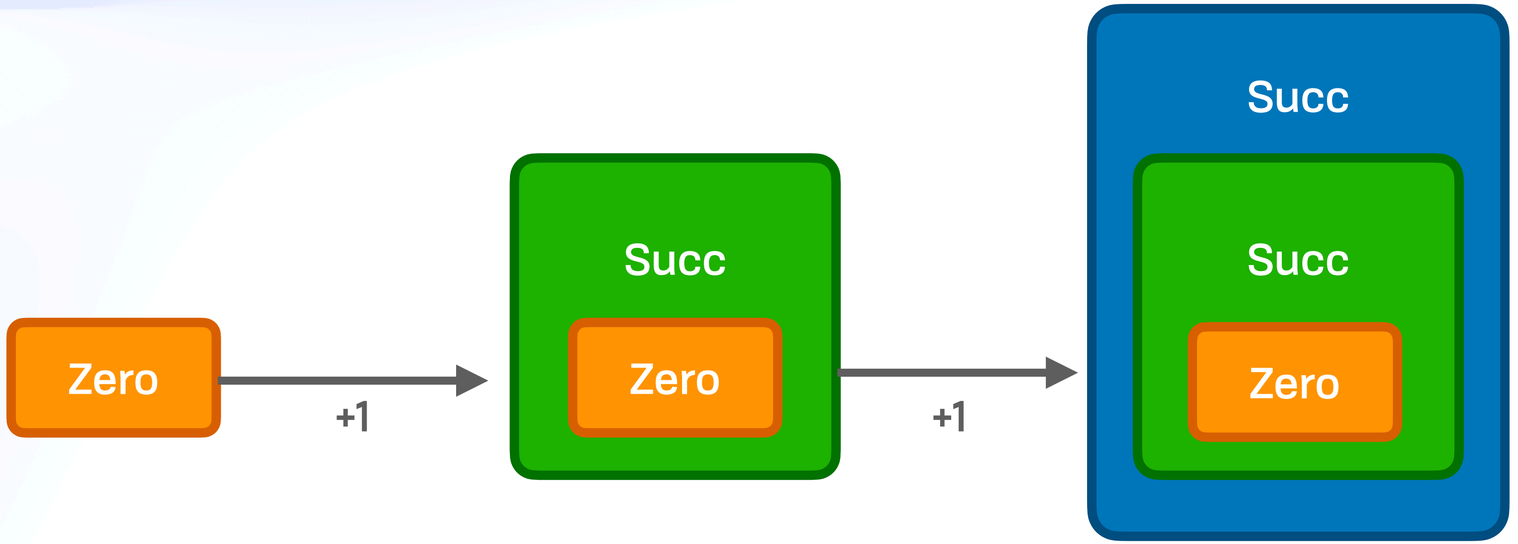
```
data Peano = Zero | Succ Peano
```



Analogy From Counting 🔢

Unary Constructors

```
data Peano = Zero | Succ Peano
```



Analogy From Counting 🔢

From Constructors to Functions

```
0    λf x → x
```

Analogy From Counting 🔢

From Constructors to Functions

```
0    λf x → x

1    λf x → f x
```

Analogy From Counting 🔢

From Constructors to Functions

```
0    λf x → x
1    λf x → f x
2    λf x → f (f x)
```

Analogy From Counting 🔢

From Constructors to Functions

```
0    λf x → x
1    λf x → f x
2    λf x → f (f x)
3    λf x → f (f (f x))
```

Analogy From Counting 🔢

From Constructors to Functions

```
0    λf x → x
1    λf x → f x
2    λf x → f (f x)
3    λf x → f (f (f x))
```

Analogy From Counting 🔢

From Constructors to Functions

```
0    λf x → x
1    λf x → f x
2    λf x → f (f x)
3    λf x → f (f (f x))
h³       x → h (h (h x))
```

Analogy From Counting 🔢

Naive

|||

```
Succ (Succ (Succ Zero))
```

```
λf x → f (f (f x))
```

```
h (h (h x))
```

Positional Numerals

Abstraction By Symbolic Juxtaposition 

Mathematics is only the art of saying the ***same thing in different words***

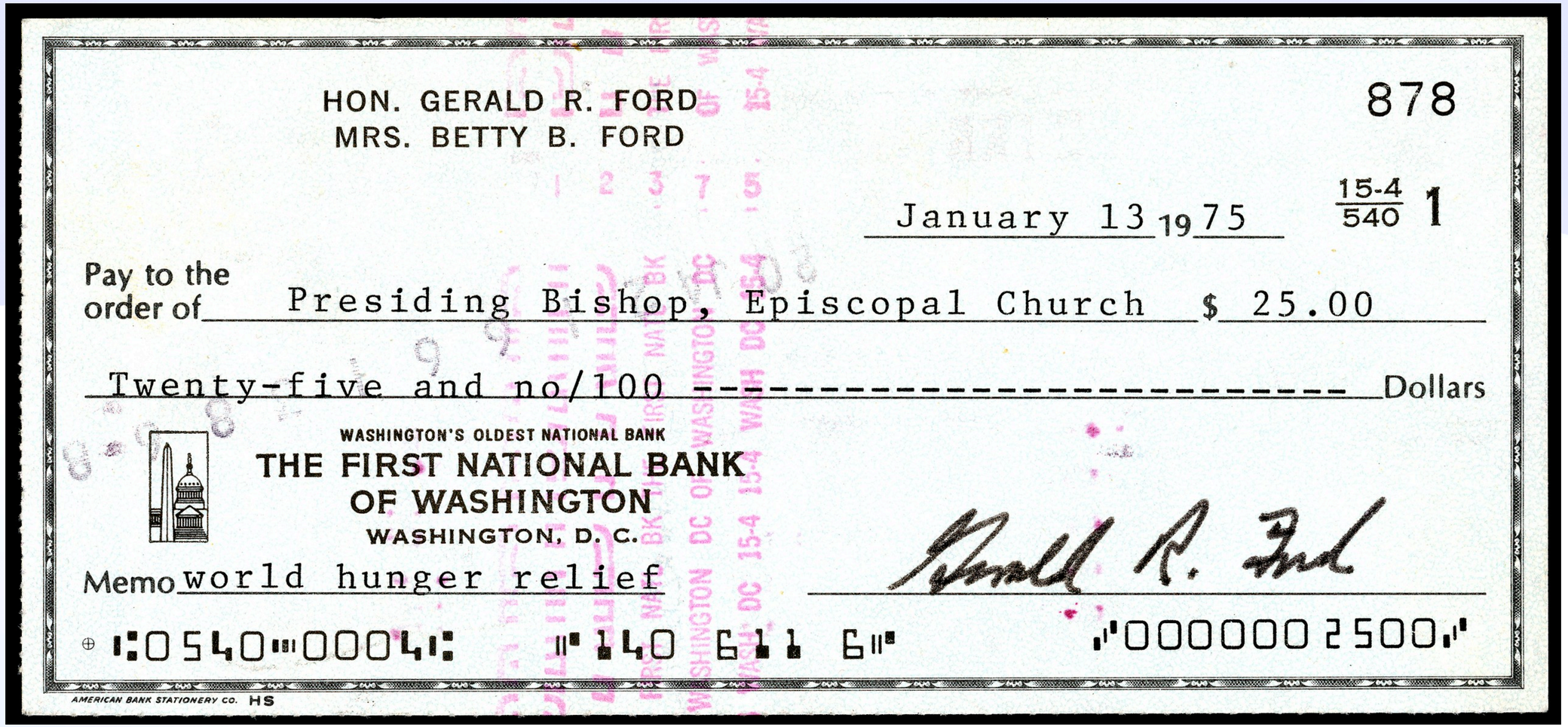
— Bertrand Russell

Positional Numerals 🧮

Positional Systems

Positional Numerals 🧮

Positional Systems



HON. GERALD R. FORD
MRS. BETTY B. FORD

878

January 13 1975

15-4
540 1

Pay to the order of Presiding Bishop, Episcopal Church $ 25.00

Twenty-five and no/100 ---------- Dollars

WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK OF WASHINGTON
WASHINGTON, D. C.

Memo world hunger relief

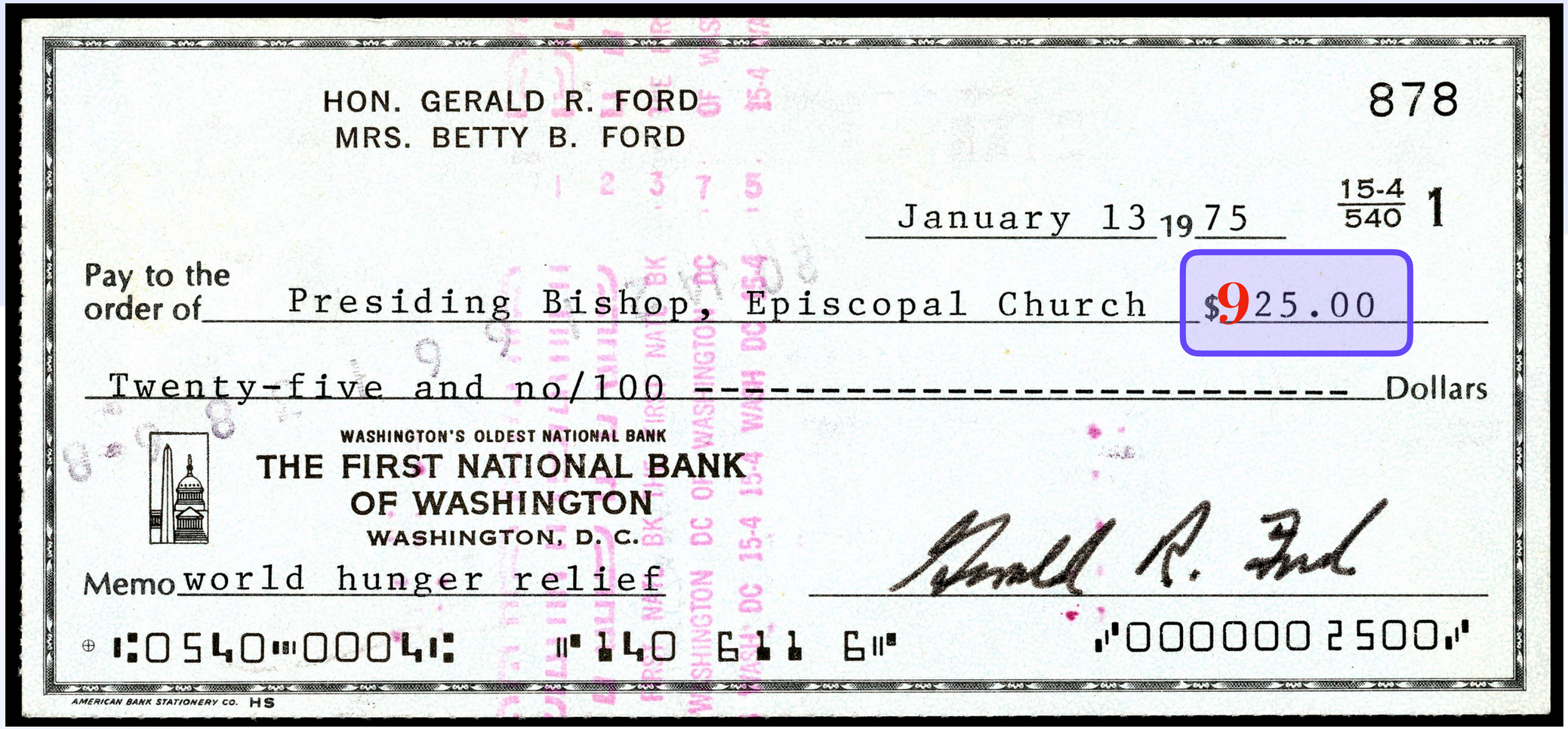
Gerald R. Ford

⑈0540⑈00041⑈ ⑈140 611 6⑈ ⑆000002500⑆

AMERICAN BANK STATIONERY CO. HS

Image Credit: National Numismatic Collection at the Smithsonian Institution, CC BY-SA 3.0

Positional Systems



HON. GERALD R. FORD
MRS. BETTY B. FORD

878

January 13 1975

15-4
540 1

Pay to the order of Presiding Bishop, Episcopal Church $925.00

Twenty-five and no/100 ---------- Dollars

WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK OF WASHINGTON
WASHINGTON, D. C.

Memo world hunger relief

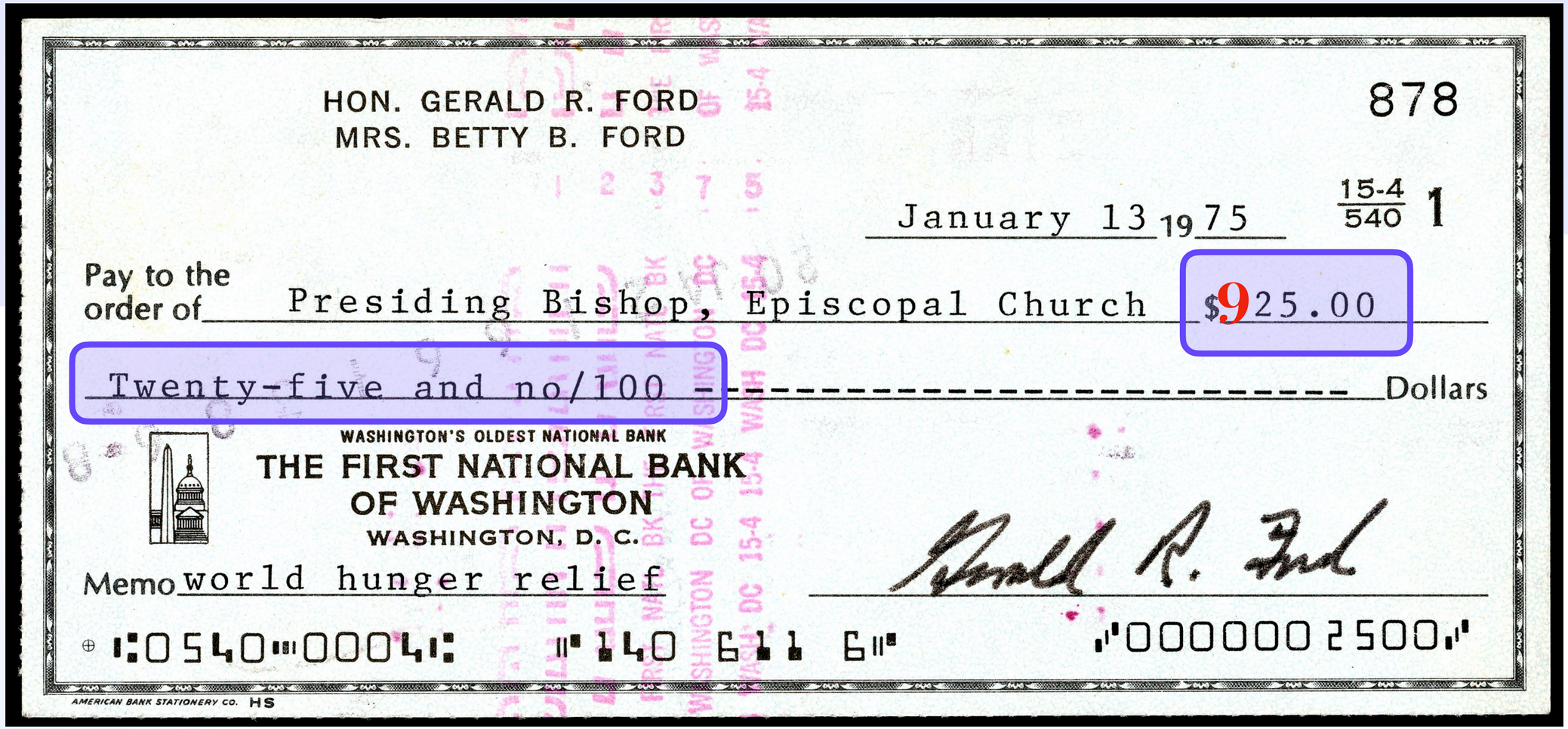
Gerald R. Ford

⑆054000041⑆ ⑈140 611 6⑈ ⑆000002500⑆

AMERICAN BANK STATIONERY CO. HS

Image Credit: National Numismatic Collection at the Smithsonian Institution, CC BY-SA 3.0

Positional Systems



HON. GERALD R. FORD
MRS. BETTY B. FORD

878

15-4
540 1

January 13 1975

Pay to the order of Presiding Bishop, Episcopal Church $925.00

Twenty-five and no/100 ---------- Dollars

WASHINGTON'S OLDEST NATIONAL BANK
THE FIRST NATIONAL BANK OF WASHINGTON
WASHINGTON, D. C.

Memo world hunger relief

Gerald R. Ford

⑈054000041⑈ ⑆140 611 6⑆ ⑈000002500⑈

AMERICAN BANK STATIONERY CO. HS

Image Credit: National Numismatic Collection at the Smithsonian Institution, CC BY-SA 3.0

Positional Numerals 🧮

Positional Systems

100 ↔ 壹佰
1000 ↔ 壹仟

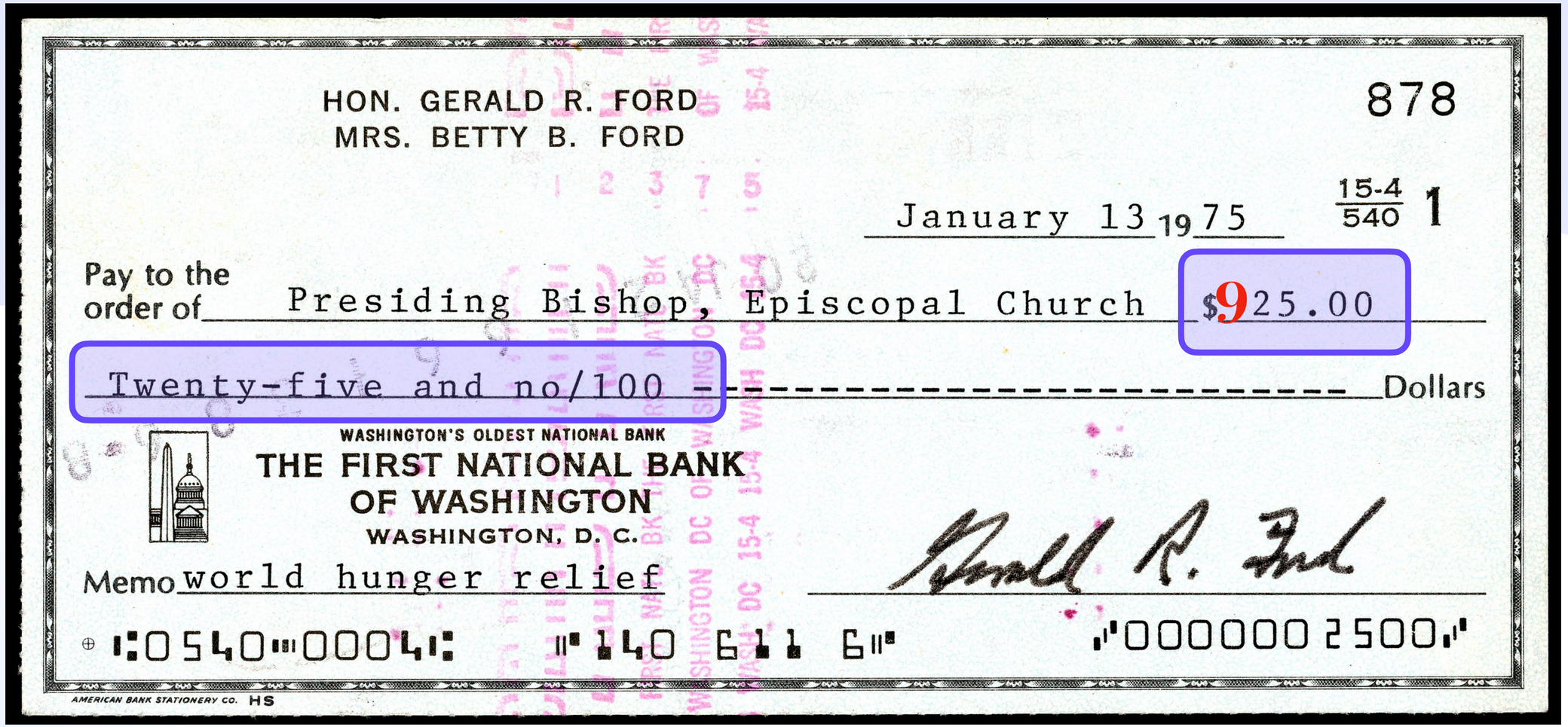


Image Credit: National Numismatic Collection at the Smithsonian Institution, CC BY-SA 3.0

Positional Numerals 🧮

Positional Digits

Positional Numerals 🧮

Positional Digits

Numeral	X 100	X 10	X 1

Positional Numerals 🧮

Positional Digits

Numeral	X 100	X 10	X 1
0	0	0	0

Positional Numerals 🧮

Positional Digits

Numeral	X 100	X 10	X 1
0	0	0	0
11	0	1	1

Positional Numerals 🧮

Positional Digits

Numeral	X 100	X 10	X 1
0	0	0	0
11	0	1	1
582	5	8	2

Positional Numerals 🧮

Positional Digits

Numeral	X 100_{10}	X 10_{10}	X 1_{10}
0	0	0	0
11	0	1	1
582	5	8	2

Positional Numerals 🧮

Mixed-Radix 😜

Numeral	X 12_{111}	X 4_{12}	X 1_{4}
0	0	0	0
11	0	2	3
582	44	1	2

Positional Numerals 🧮

Mixed-Radix

Positional Numerals 🧮

Mixed-Radix

- 2022 Sept 22 11:22:03.987
- 60 minutes / hour
- 24 hours / day
- 7 days / week
- 52 weeks / year

Positional Numerals 🧮

Mixed-Radix

- 2022 Sept 22 11:22:03.987
- 60 minutes / hour
- 24 hours / day
- 7 days / week
- 52 weeks / year

Positional Numerals 🧮

Compound Hash

Positional Numerals 🧮

Compound Hash

Numeral	"hundreds"	"tens"	"ones"

Positional Numerals 🧮

Compound Hash

Numeral	"hundreds"	"tens"	"ones"
`X + 0`	`"hundreds"`	`"tens"`	`"ones"`

Positional Numerals 🧮

Compound Hash

Numeral	"hundreds"	"tens"	"ones"
X + 0	"hundreds"	"tens"	"ones"
X + 11	"hundreds"	h("tens") 523c079f58465edb79c834fbf4608099cf864039bb511c072beb35c568c80edf	h("ones") d413f65286221536df21b59e5d29215e2817d8cc70a1d6ef4273e7c63c6b1a08

Positional Numerals 🧮

Compound Hash

Numeral	"hundreds"	"tens"	"ones"
X + 0	"hundreds"	"tens"	"ones"
X + 11	"hundreds"	h("tens") 523c079f58465edb79c834fbf4608099cf864039bb511c072beb35c568c80edf	h("ones") d413f65286221536df21b59e5d29215e2817d8cc70a1d6ef4273e7c63c6b1a08
X + 582	h^5("hundreds") b7fee5aff5d93be282a3826766c8f4a3af7a35e620e78b300c5a8fd8791e77cb	h^8("tens") 6d00cd80a2f03d126077401fa4b95129d4e79ec3f4ea7ae36099af5a39478ef7	h^2("ones") e6f92be646346875e815ebd95fbc0e3b2412e2d630b2325decdbdb4a0eeb3401

Positional Numerals 🧮

Compound Hash

Numeral	"hundreds"	"tens"	"ones"
X + 0	"hundreds"	"tens"	"ones"
X + 11	"hundreds"	h("tens") 523c079f58465edb79c834fbf4608099cf864039bb511c072beb35c568c80edf	h("ones") d413f65286221536df21b59e5d29215e2817d8cc70a1d6ef4273e7c63c6b1a08
X + 582	h^5("hundreds") b7fee5aff5d93be282a3826766c8f4a3af7a35e620e78b300c5a8fd8791e77cb	h^8("tens") 6d00cd80a2f03d126077401fa4b95129d4e79ec3f4ea7ae36099af5a39478ef7	h^2("ones") e6f92be646346875e815ebd95fbc0e3b2412e2d630b2325decdbdb4a0eeb3401

```
» echo -n "hundreds" | sha256sum | sha256sum | sha256sum | sha256sum | sha256sum
b7fee5aff5d93be282a3826766c8f4a3af7a35e620e78b300c5a8fd8791e77cb  -
```

Positional Numerals 🧮

Denominated PayWord

https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Positional Numerals 🧮

Denominated PayWord

https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

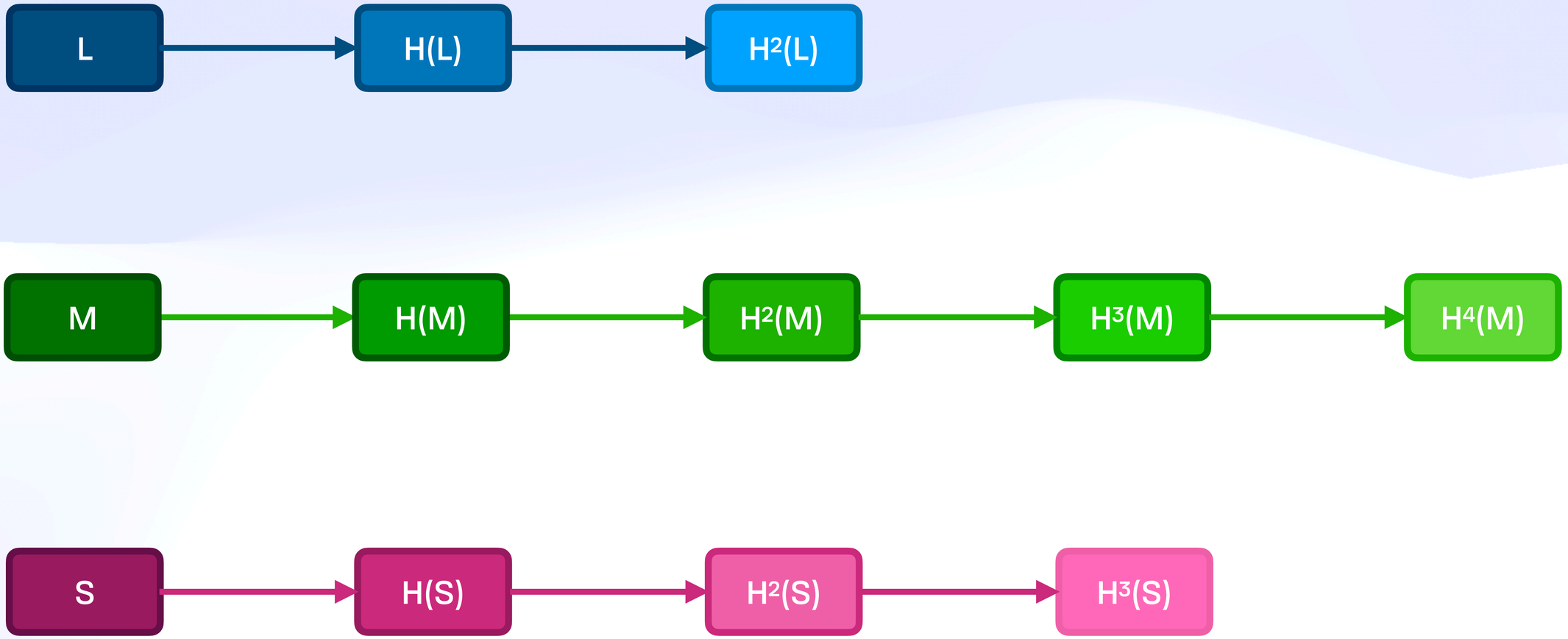
Positional Numerals 🧮

Denominated PayWord

https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Positional Numerals 🧮

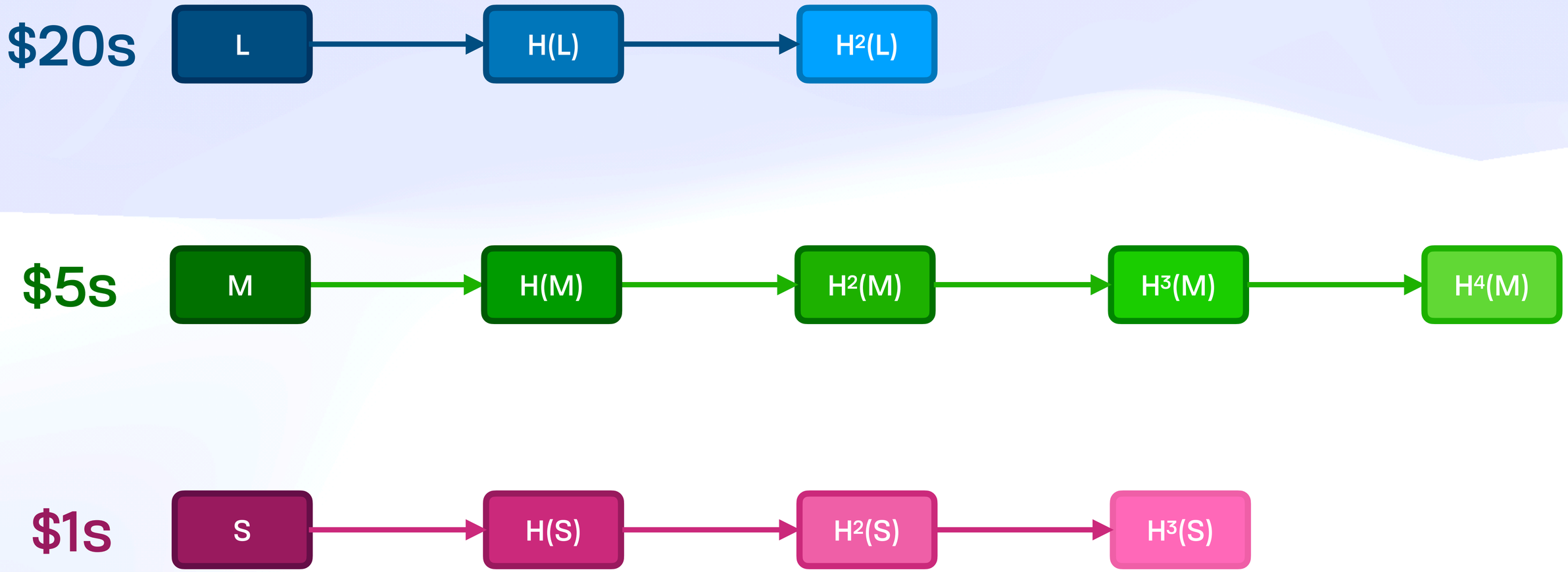
Denominated PayWord



https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Positional Numerals 🧮

Denominated PayWord

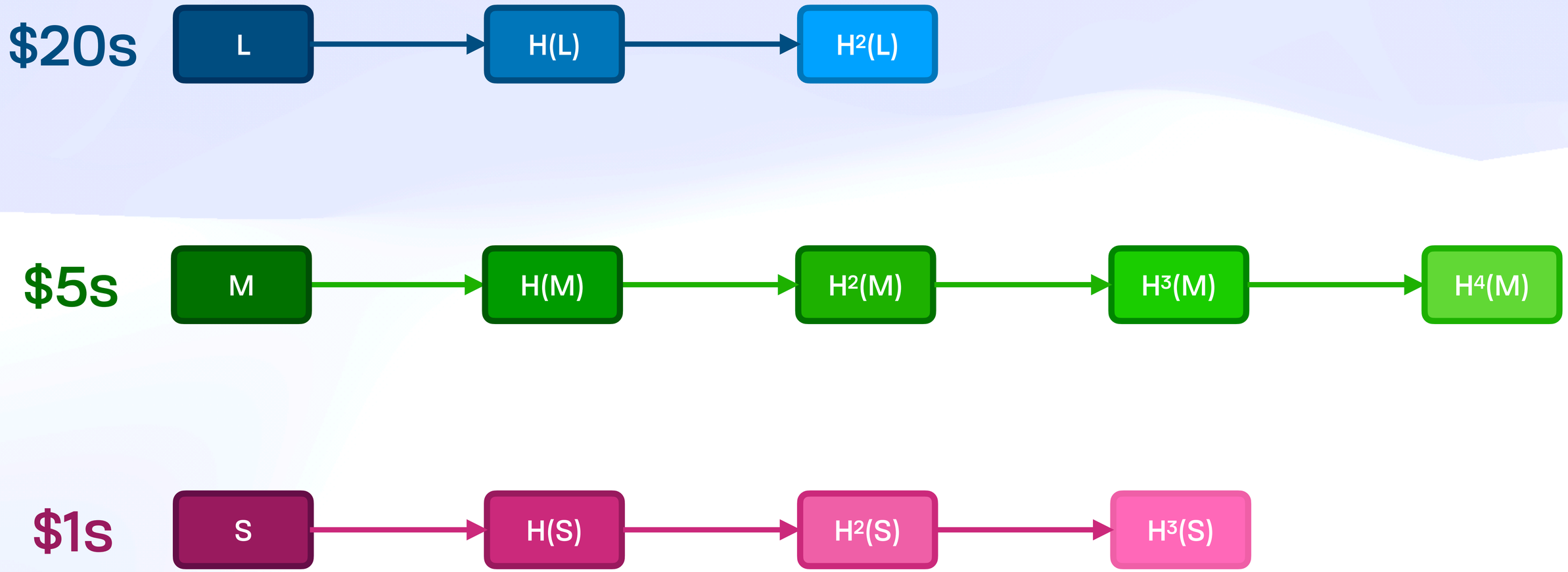


https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Positional Numerals 🧮

Denominated PayWord

🙈 👀



https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

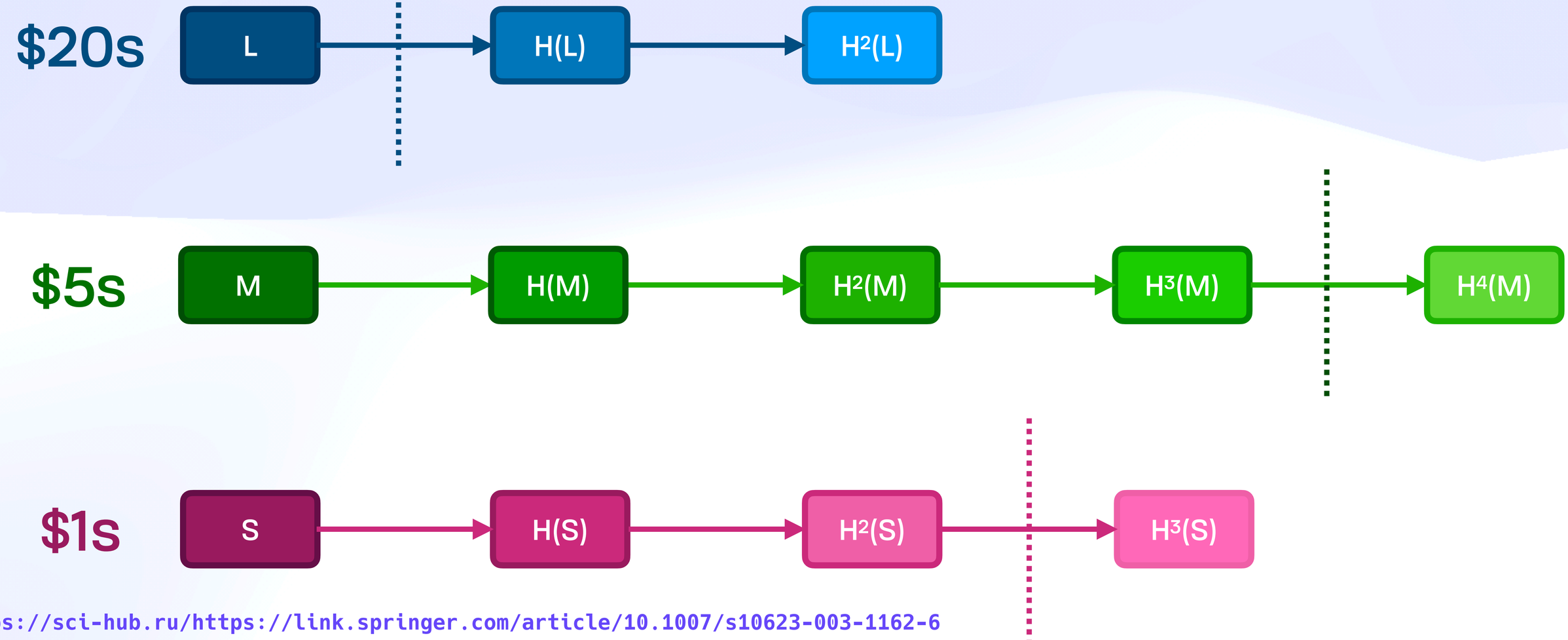
Positional Numerals 🧮

Denominated PayWord

https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Positional Numerals 🧮

Denominated PayWord

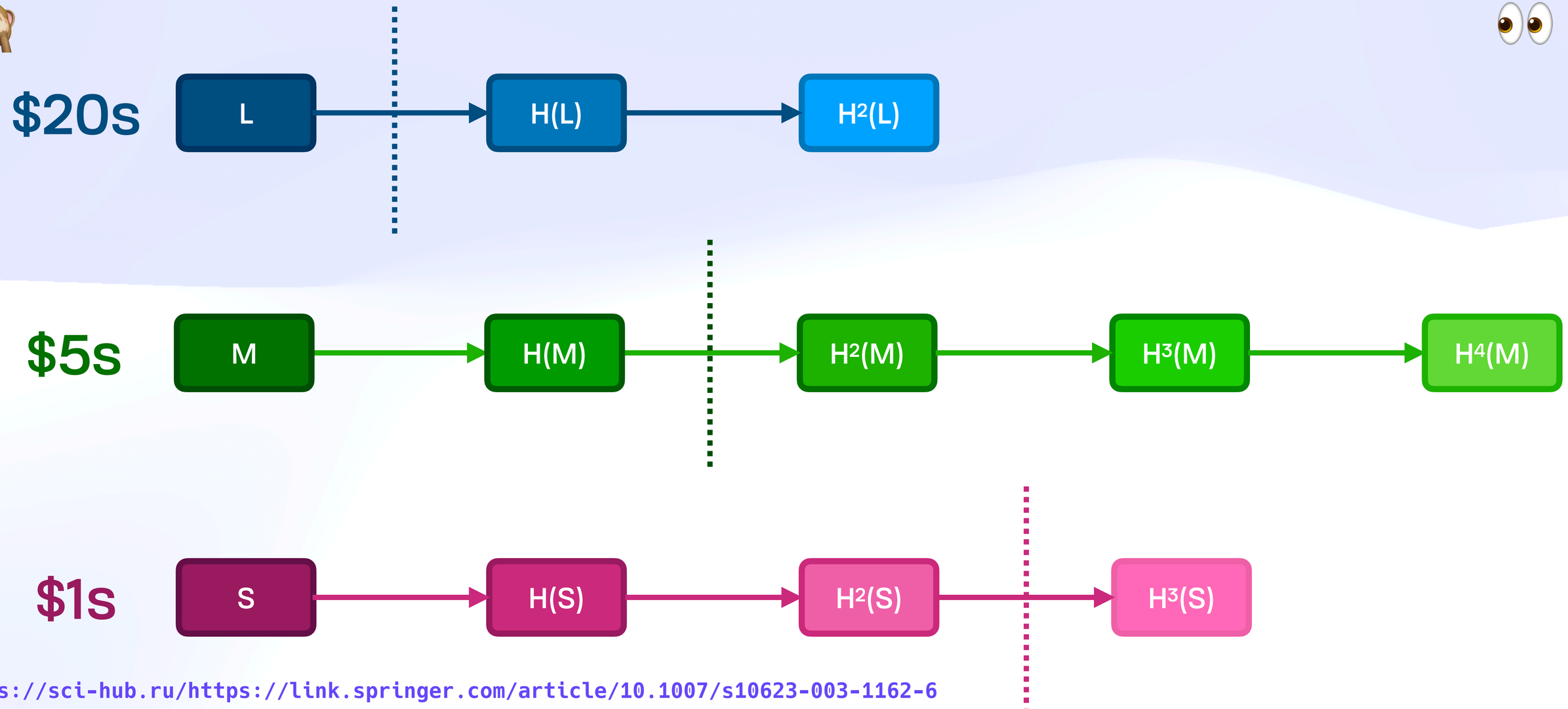


https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Positional Numerals 🧮

Denominated PayWord

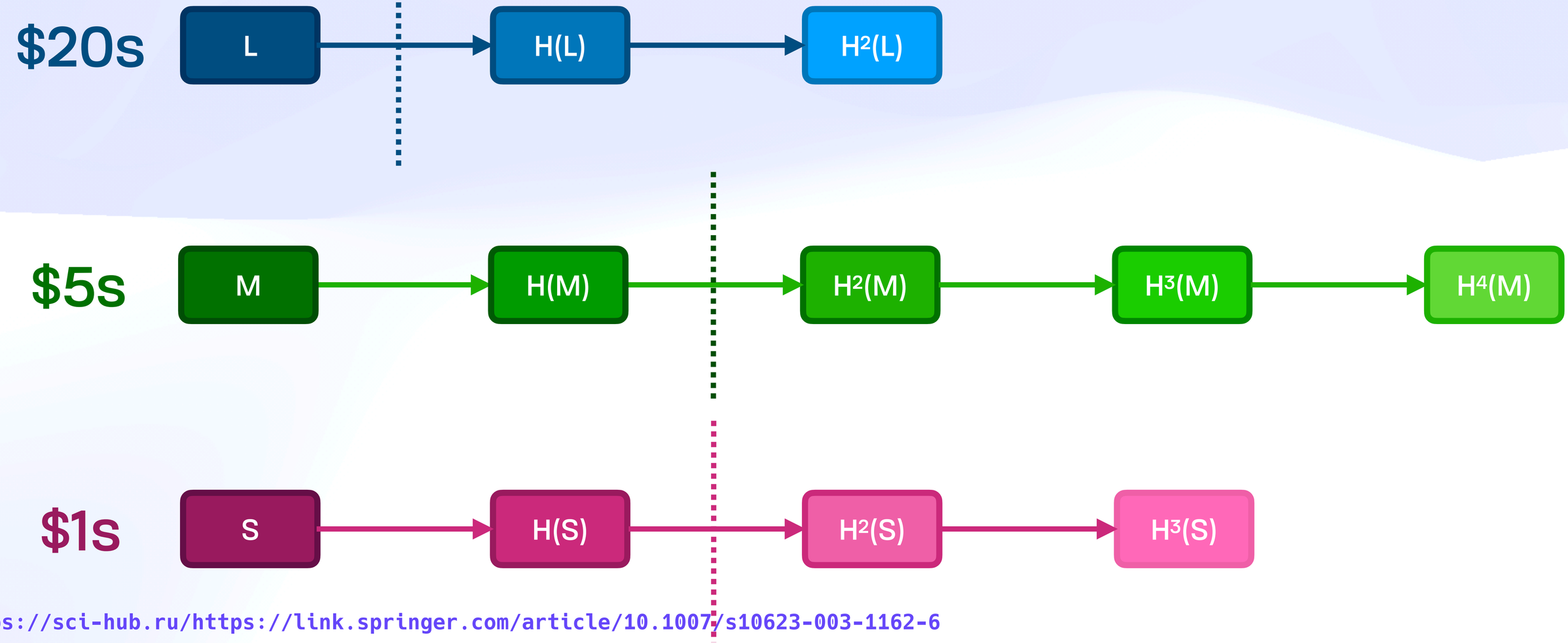
🙈 👀



https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Positional Numerals 🧮

Denominated PayWord



https://sci-hub.ru/https://link.springer.com/article/10.1007/s10623-003-1162-6

Analogy From Data Structures

Who Doesn't Love DAGs In Their Crypto?

Analogy From Data Structures 🌲

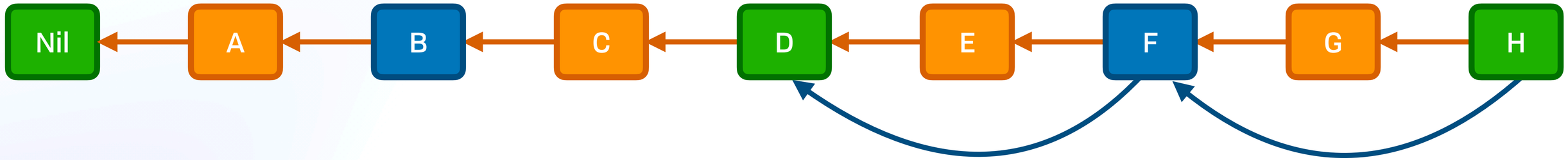
Deterministic Skip List

Analogy From Data Structures 🌲

Deterministic Skip List

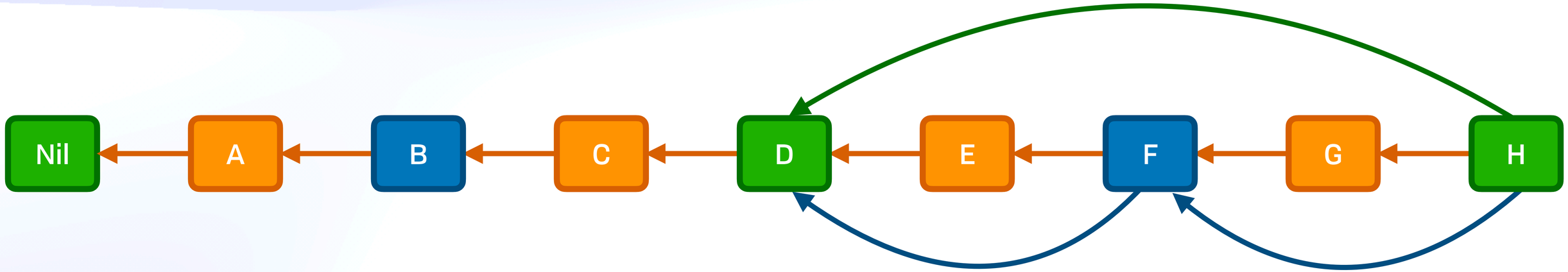
Analogy From Data Structures 🌲

Deterministic Skip List



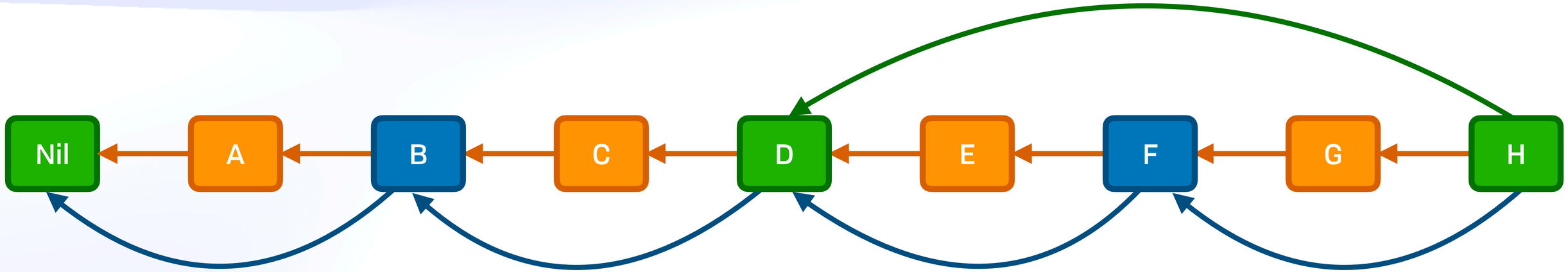
Analogy From Data Structures 🌲

Deterministic Skip List



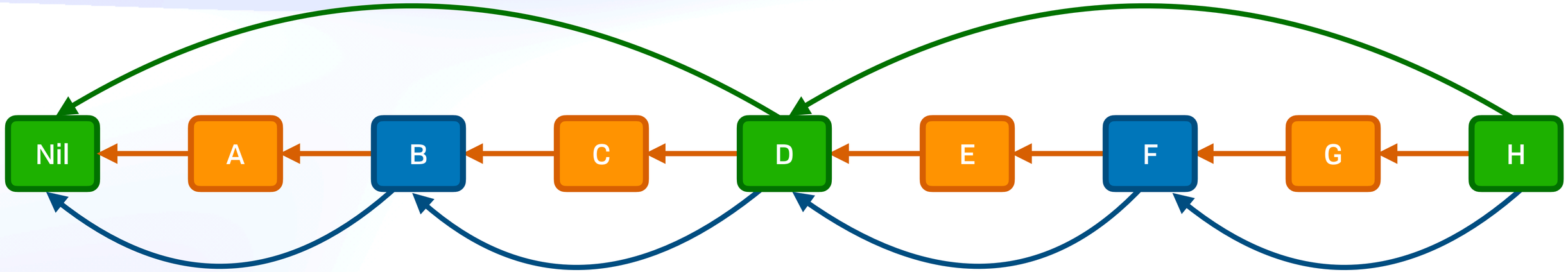
Analogy From Data Structures 🌲

Deterministic Skip List



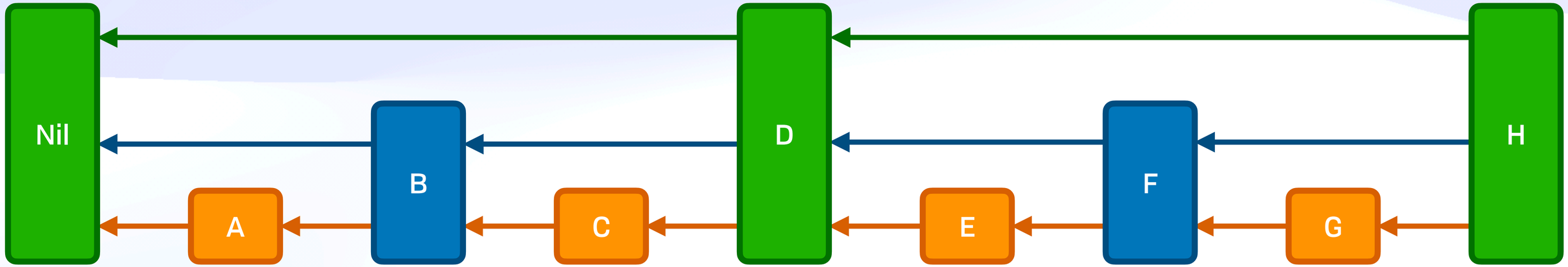
Analogy From Data Structures 🌲

Deterministic Skip List



Analogy From Data Structures 🌲

Deterministic Skip List

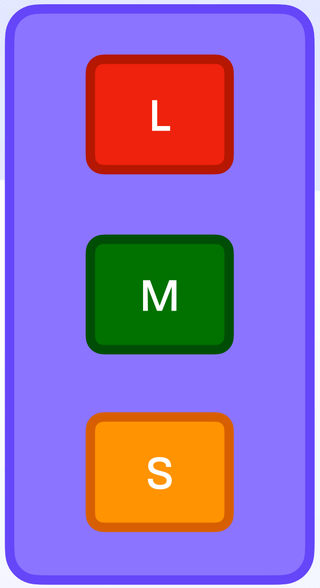


Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet

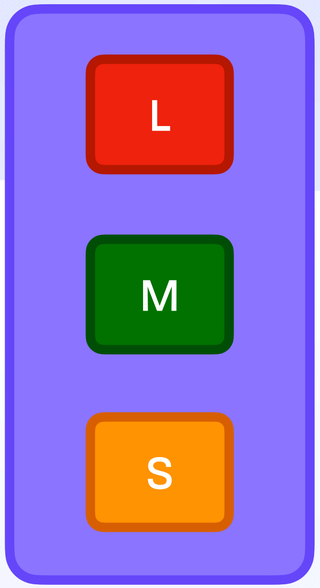
Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet



Analogy From Data Structures 🌲

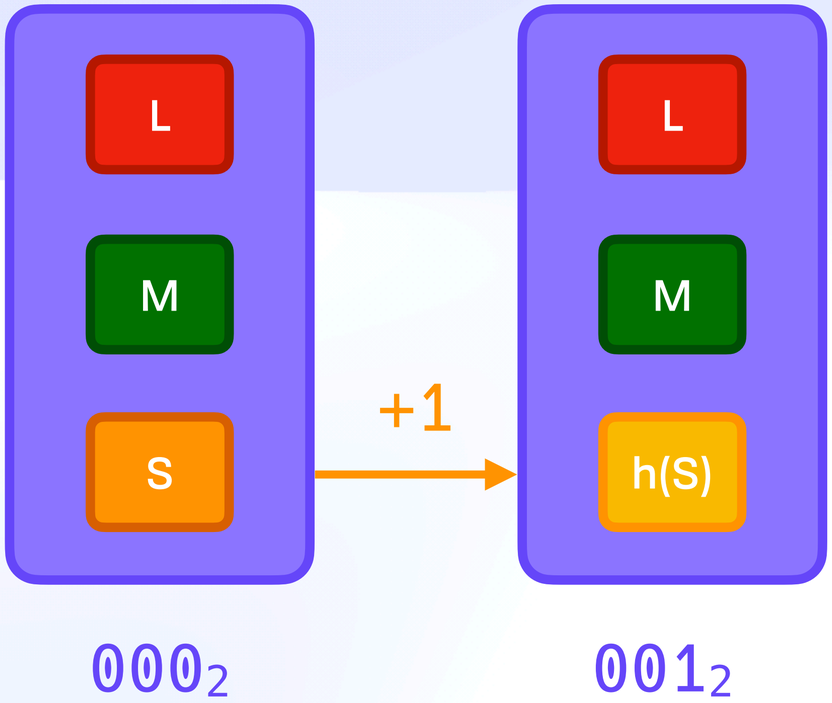
Simplified Binary Skip Ratchet



000_2

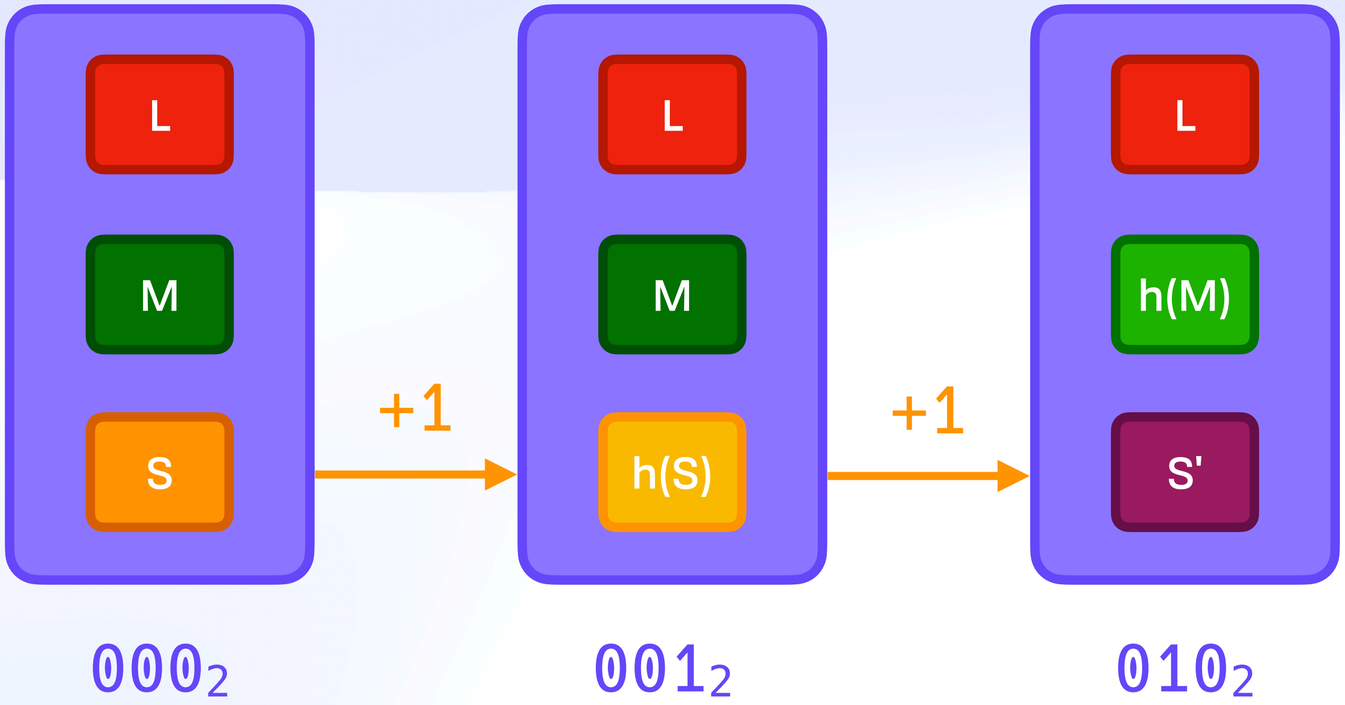
Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet



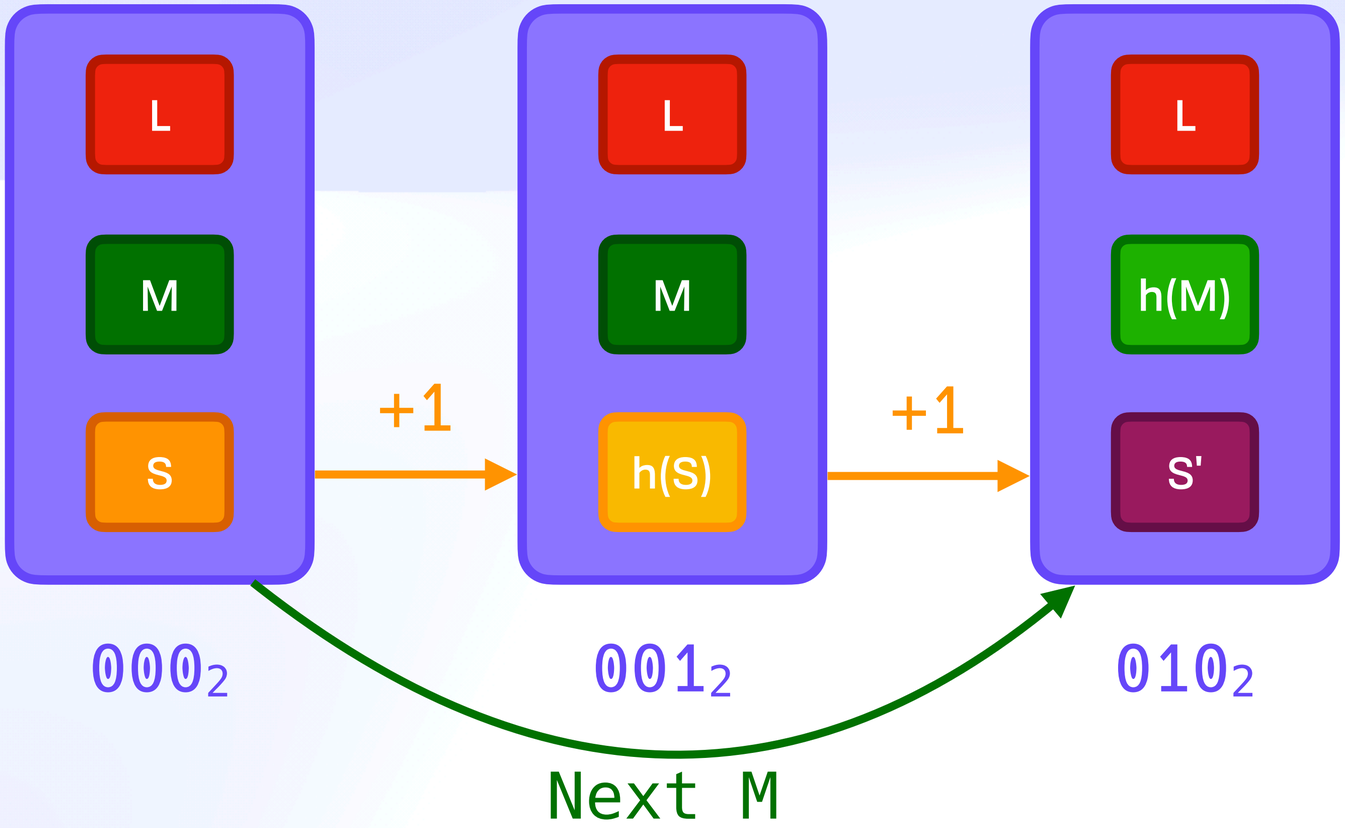
Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet



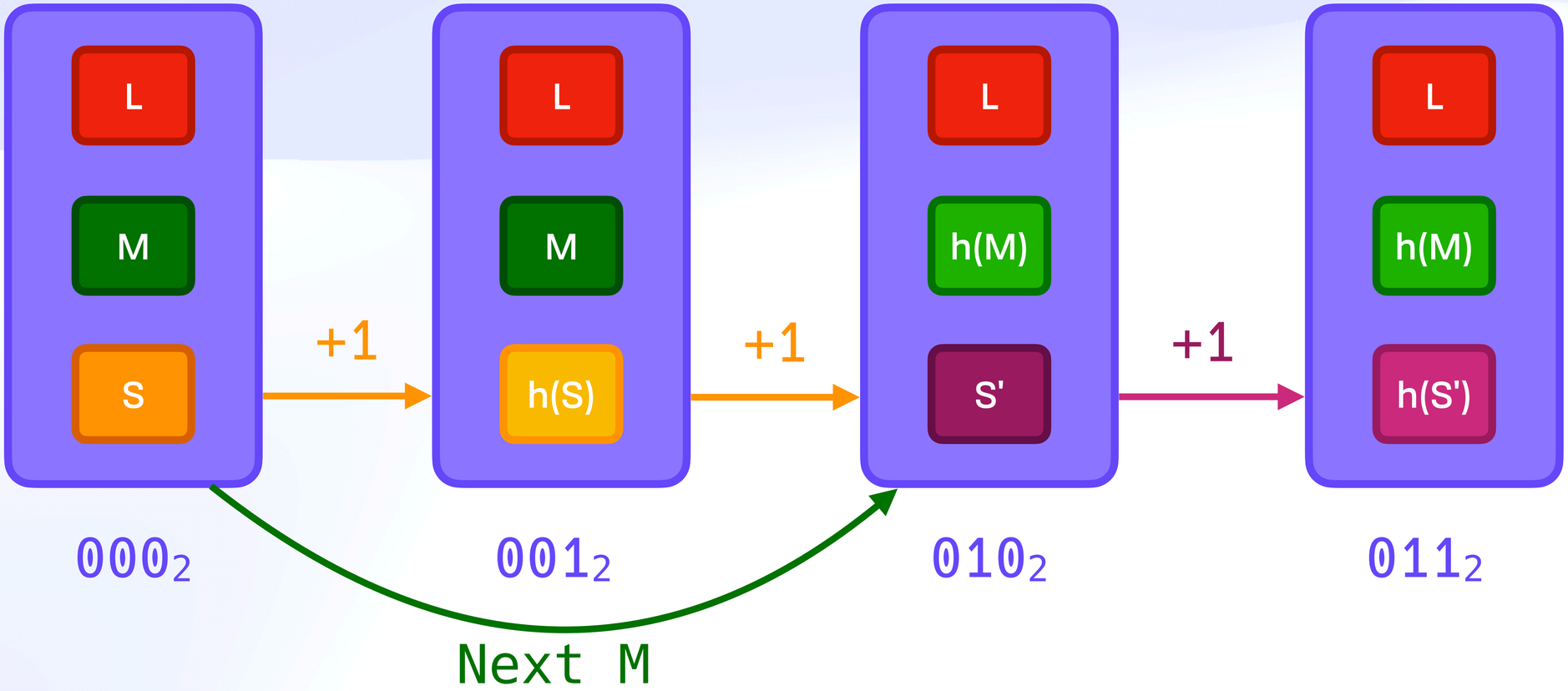
Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet



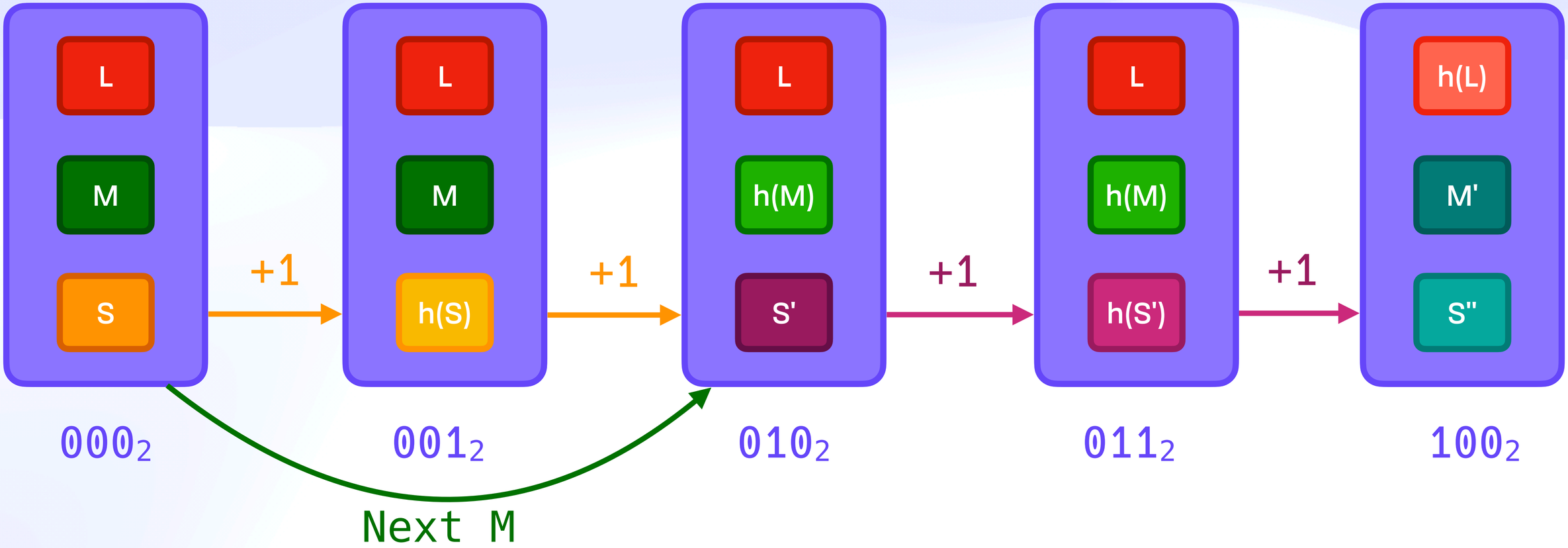
Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet



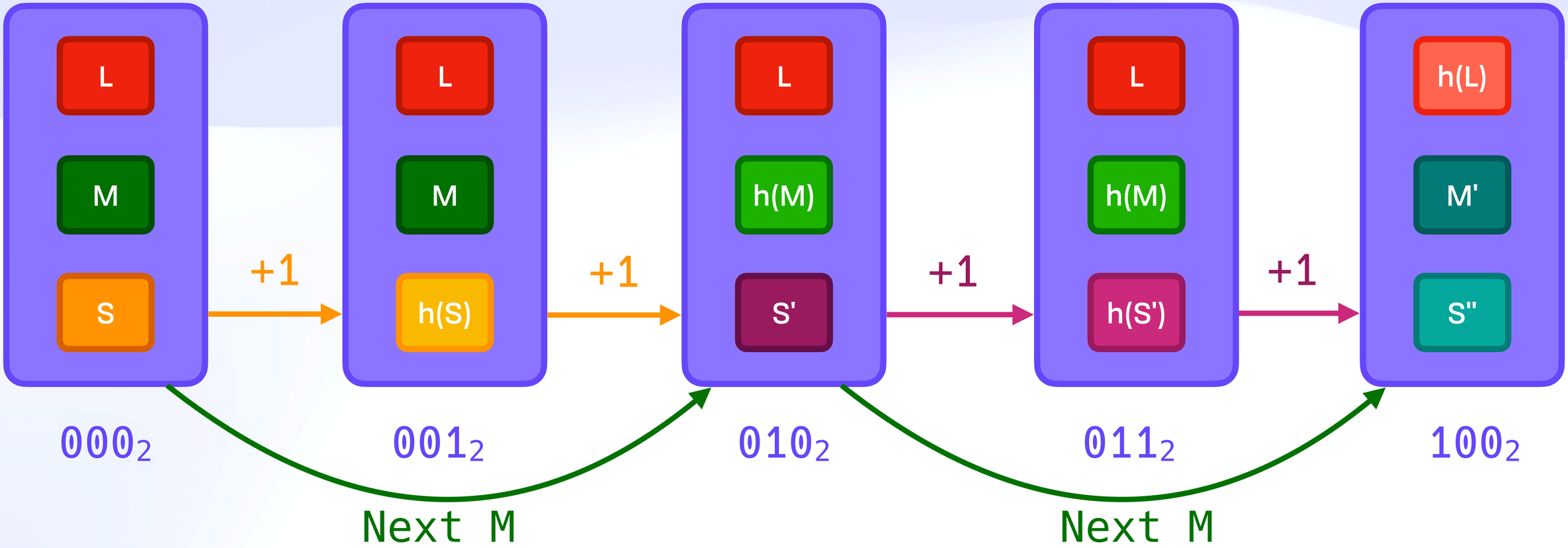
Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet



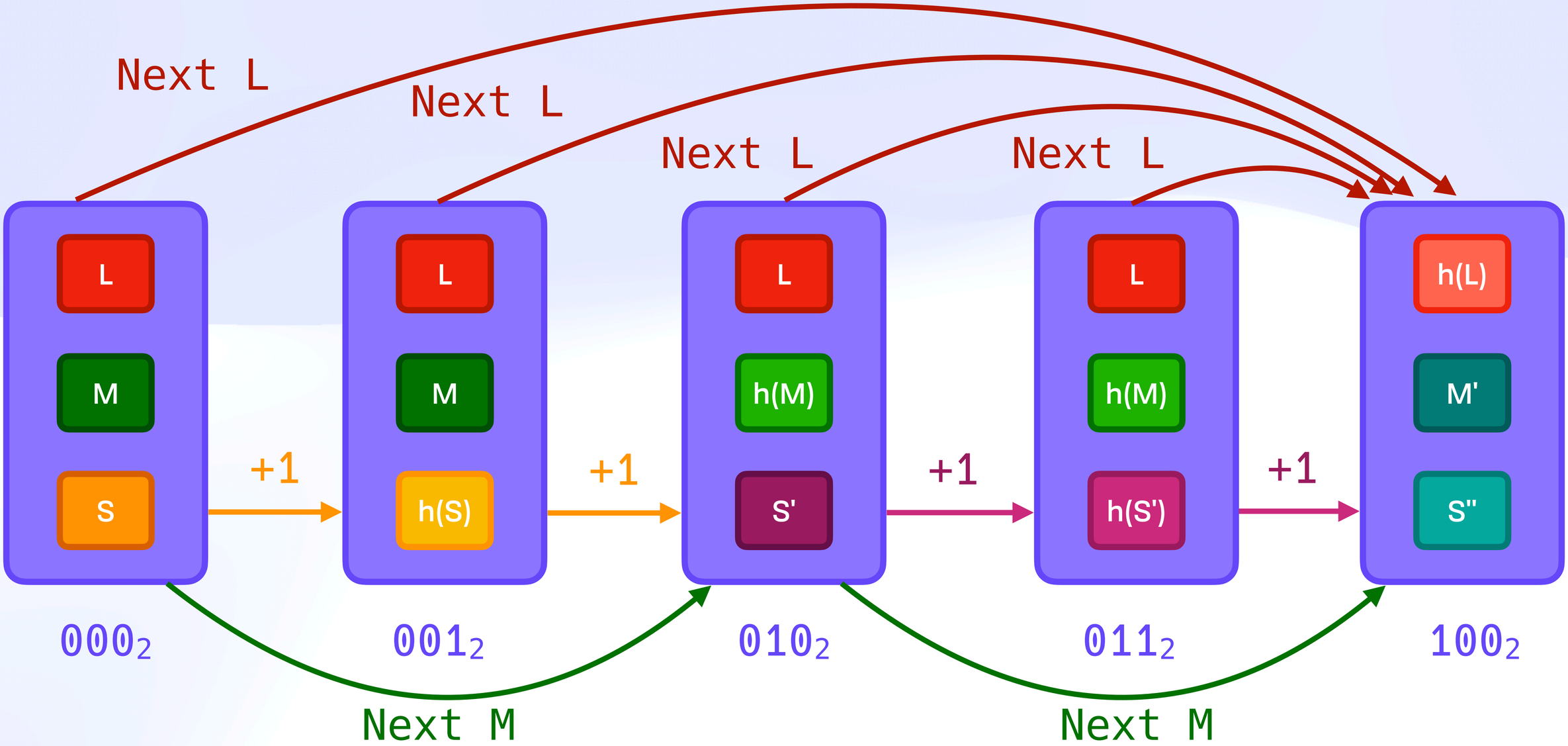
Analogy From Data Structures 🎄

Simplified Binary Skip Ratchet



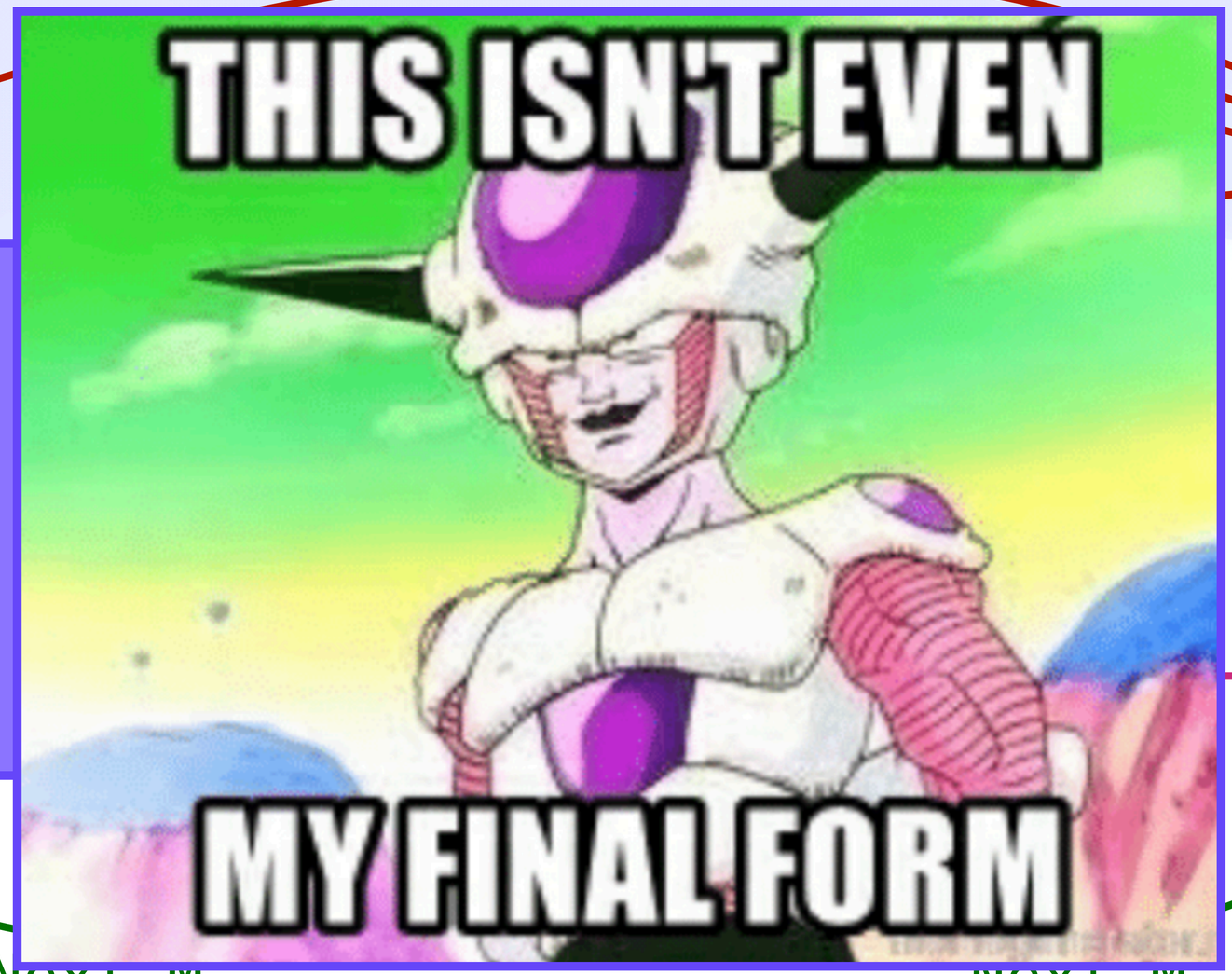
Analogy From Data Structures 🌲

Simplified Binary Skip Ratchet



Analogy From Data Structures 🎄

Simplified Binary Skip Ratchet



Next L

L

M

S

+1

000_2

h(L)

M'

S''

+1

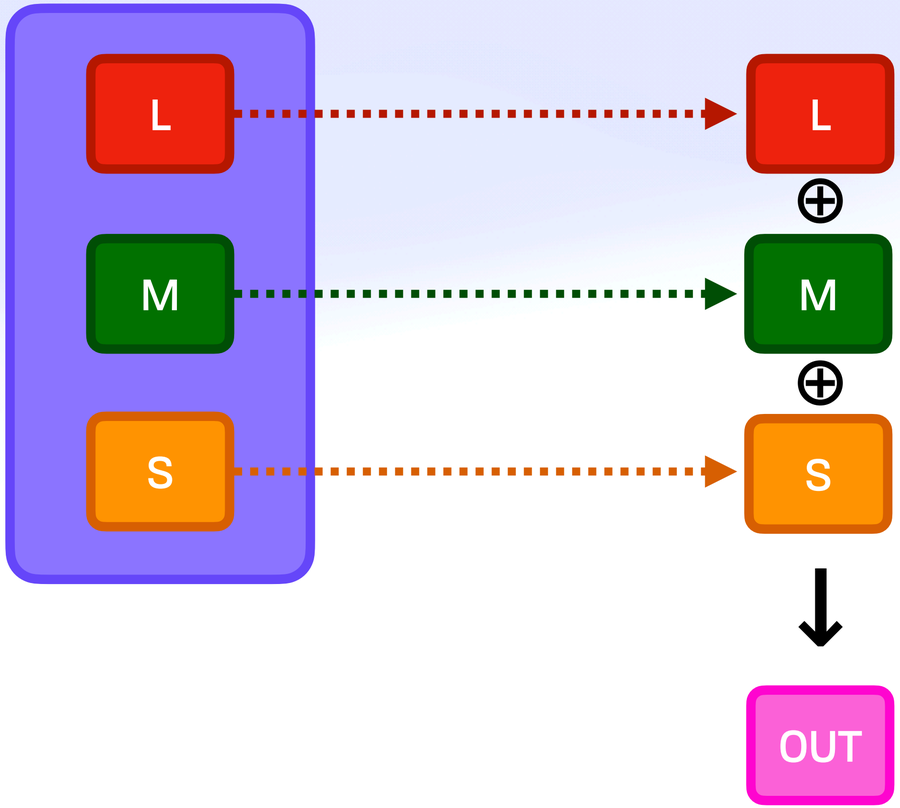
100_2

Next M

Next M

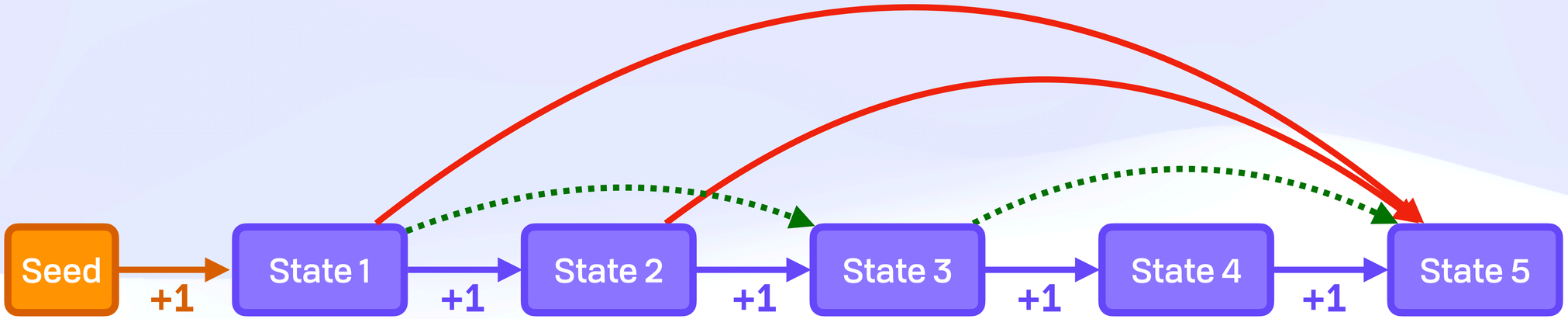
Analogy From Data Structures 🌲

Deriving Secrets



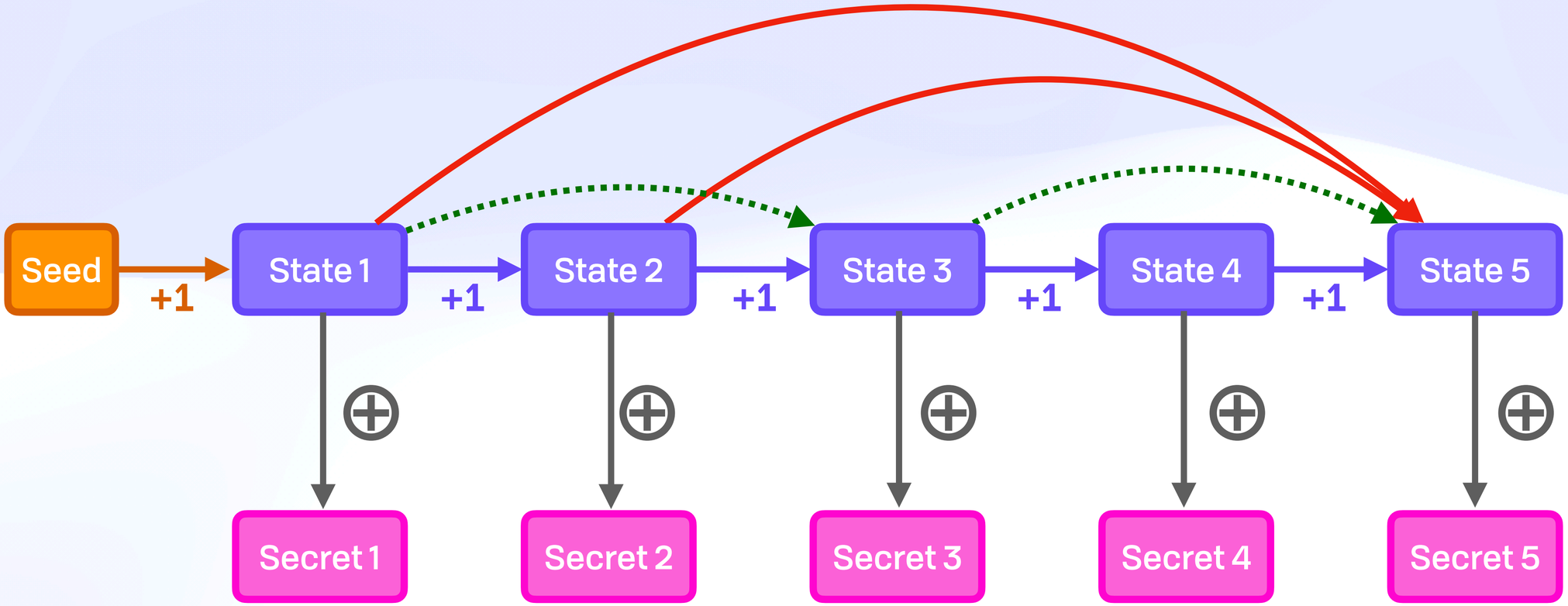
Analogy From Data Structures 🌲

Deriving Secrets With Secrets



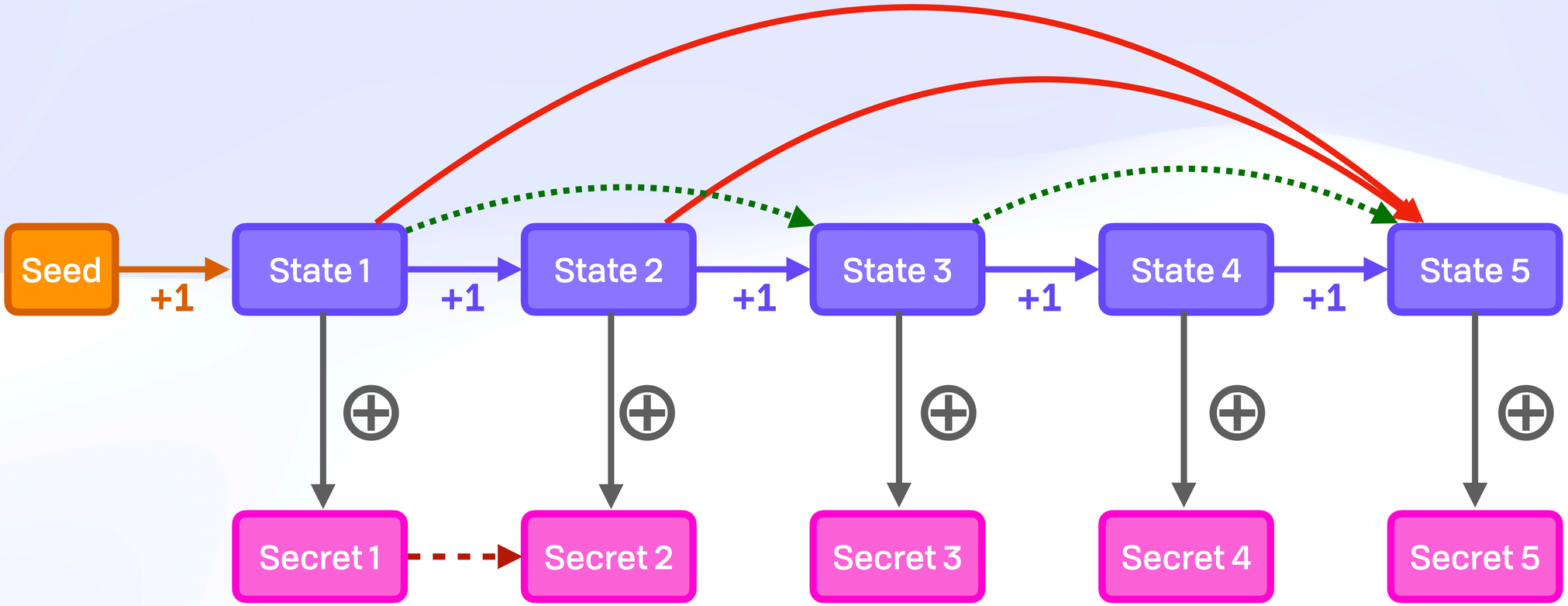
Analogy From Data Structures 🌲

Deriving Secrets With Secrets



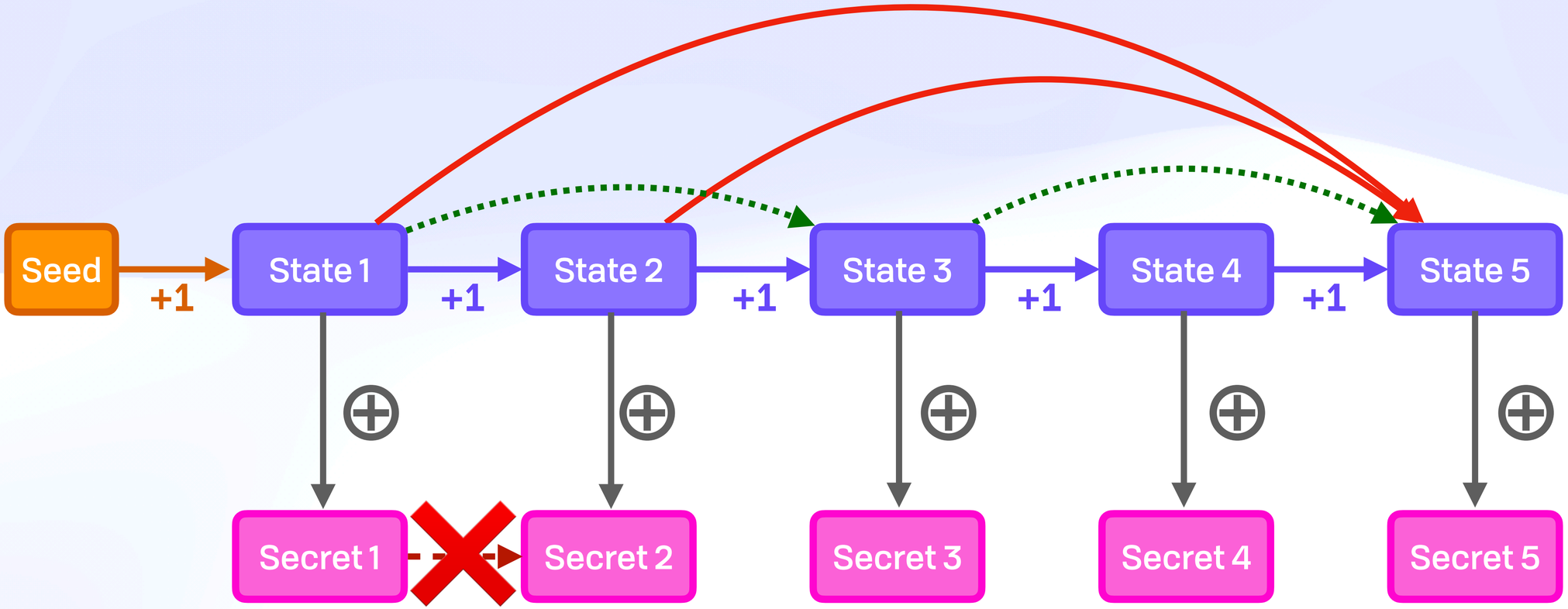
Analogy From Data Structures 🌲

Deriving Secrets With Secrets



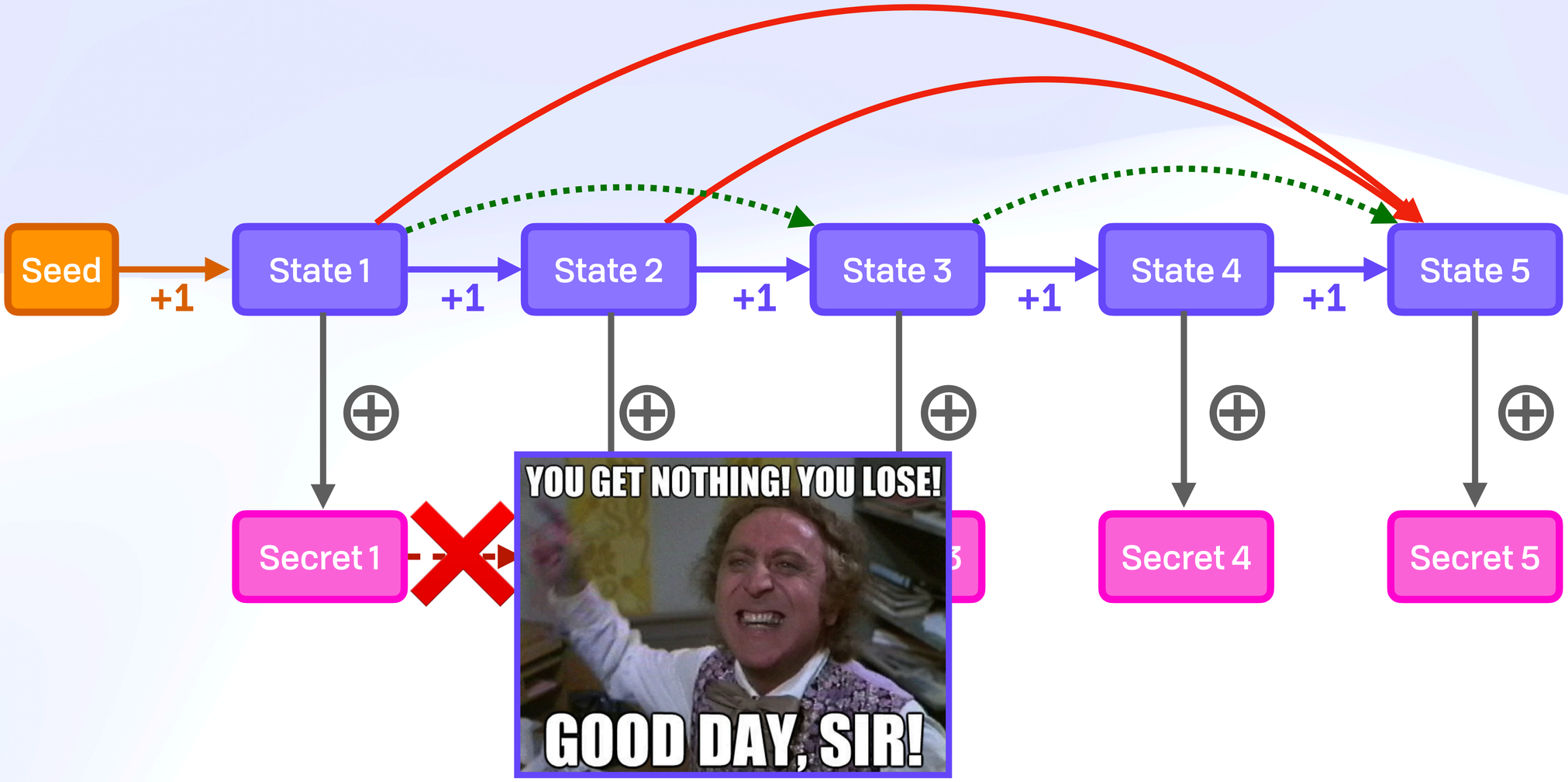
Analogy From Data Structures 🌲

Deriving Secrets With Secrets



Analogy From Data Structures 🌲

Deriving Secrets With Secrets



Security

Who Hashes the Hashers?

Security 🔐

Zeroing & Epochs

Security 🔐

Zeroing & Epochs

10

11

...

18

19

20

21

22

...

Security 🔐

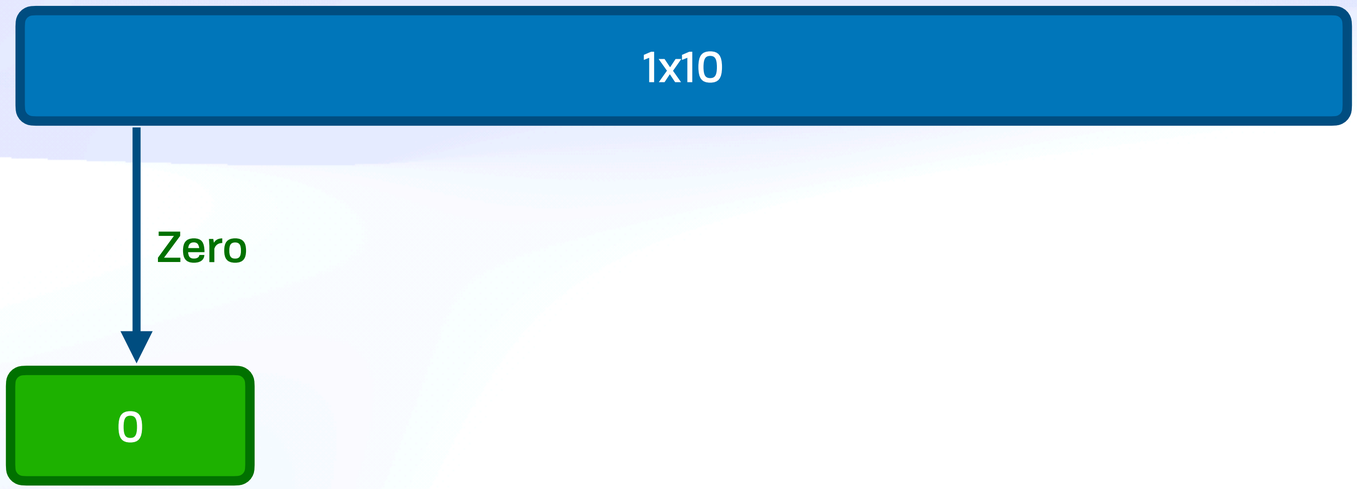
Zeroing & Epochs

10
11
...
18
19
20
21
22
...

Security 🔐

Zeroing & Epochs

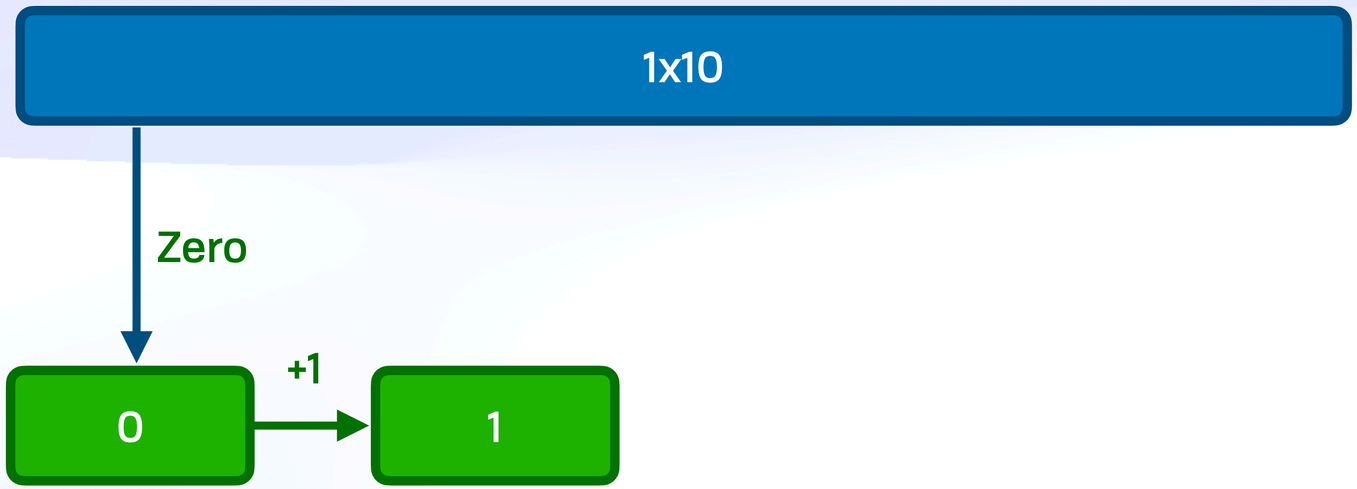
10
11
...
18
19
20
21
22
...



Security 🔐

Zeroing & Epochs

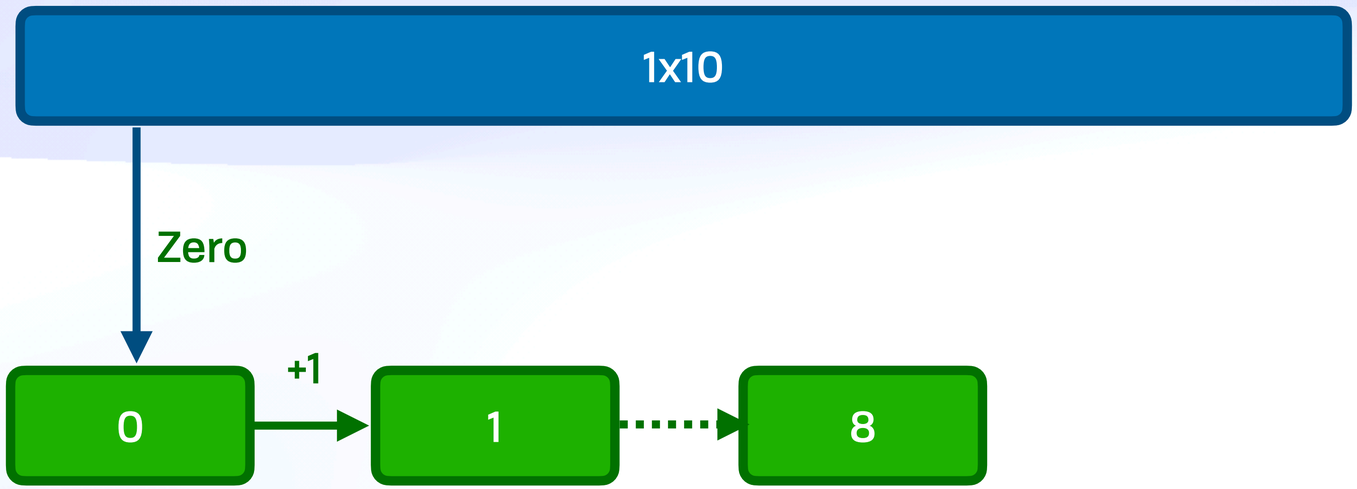
10
11
...
18
19
20
21
22
...



Security 🔐

Zeroing & Epochs

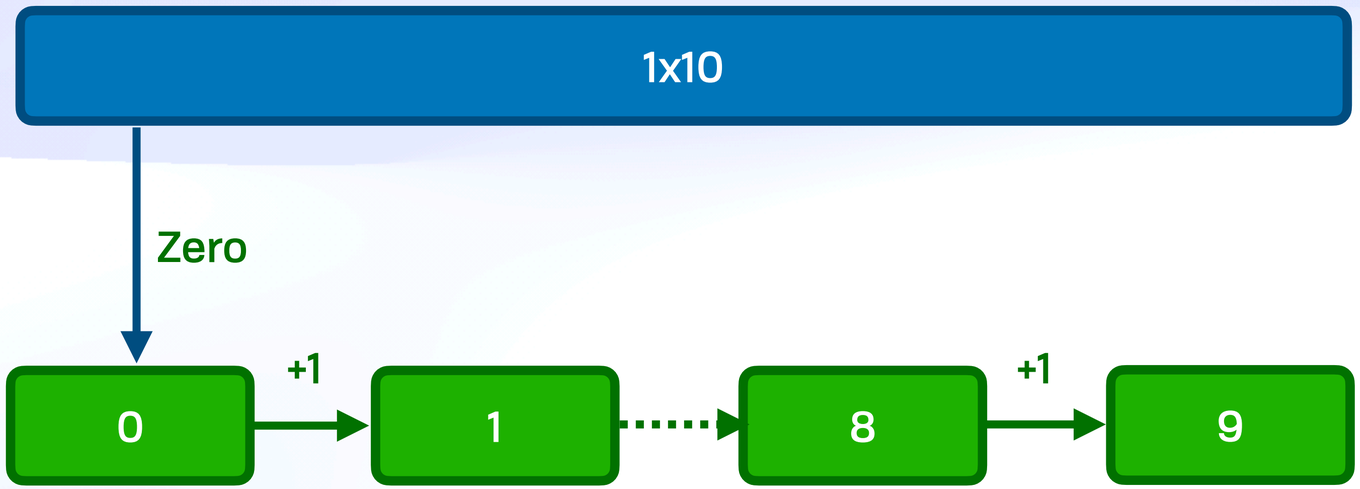
10
11
...
18
19
20
21
22
...



Security 🔐

Zeroing & Epochs

10
11
...
18
19
20
21
22
...



Security 🔐

Zeroing & Epochs

10

11

...

18

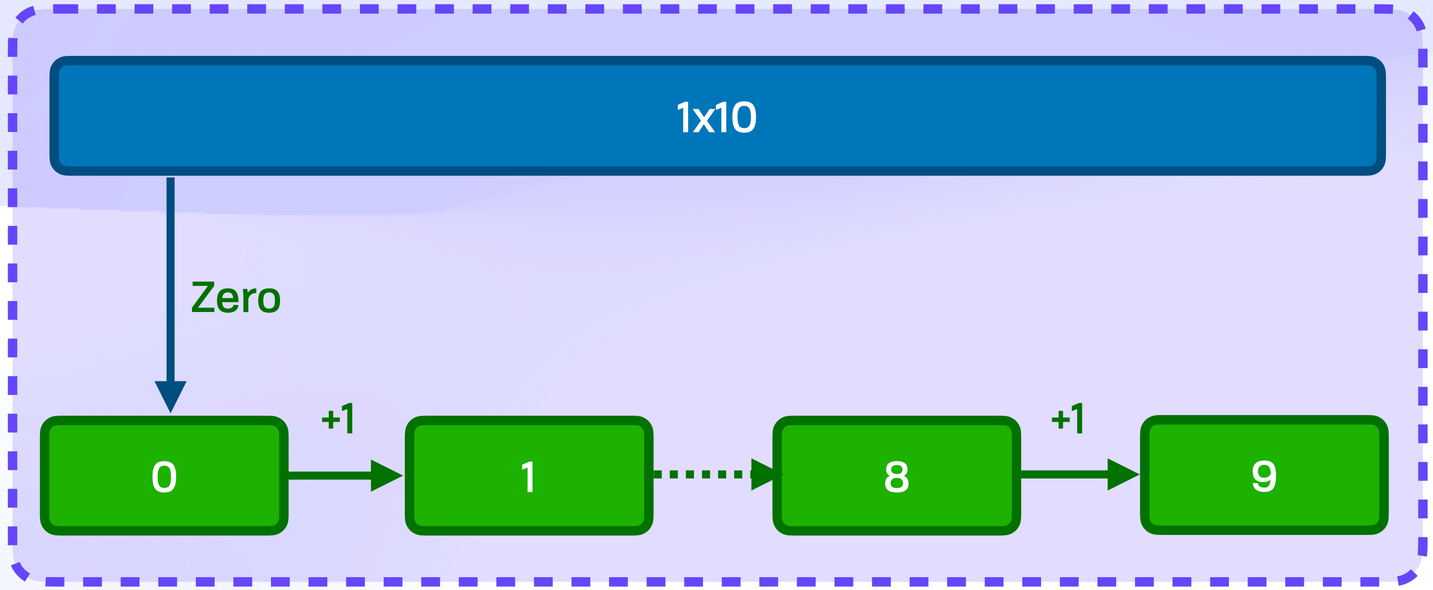
19

20

21

22

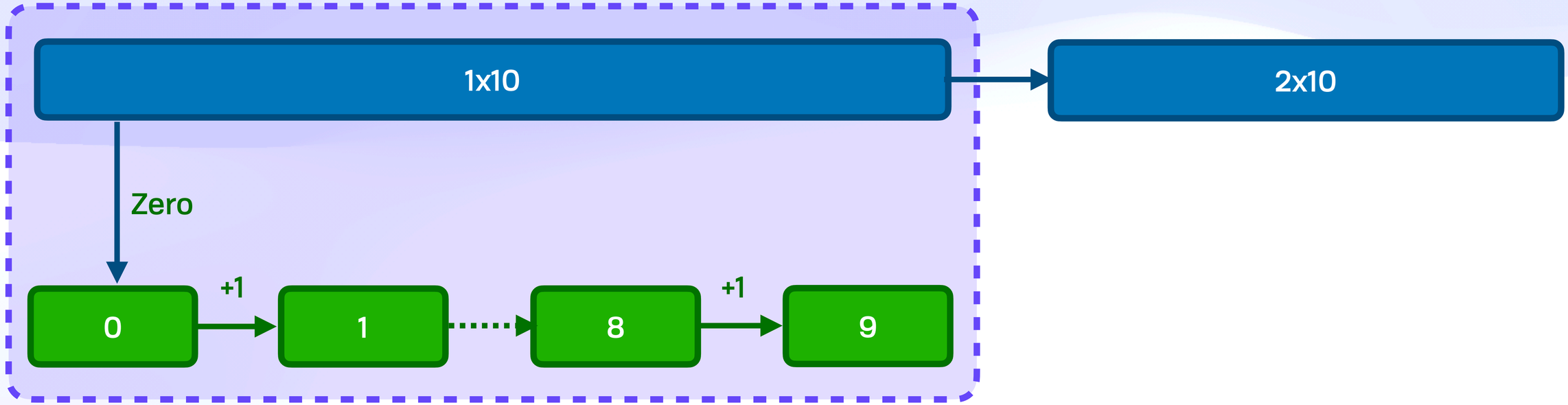
...



Security 🔐

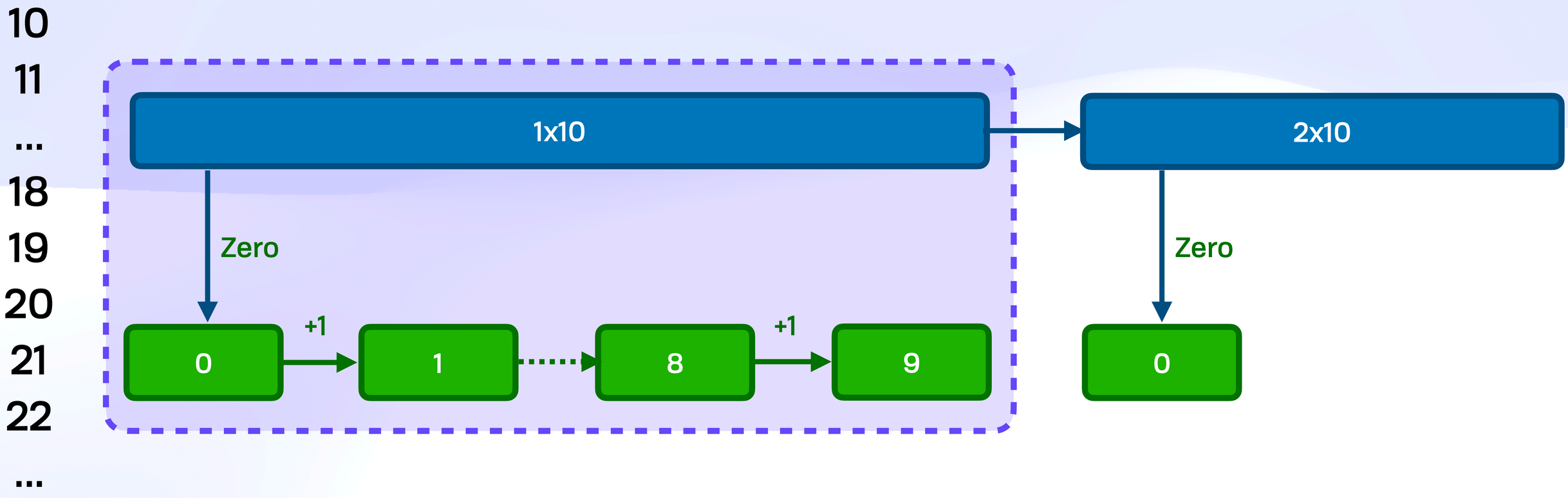
Zeroing & Epochs

10
11
...
18
19
20
21
22
...



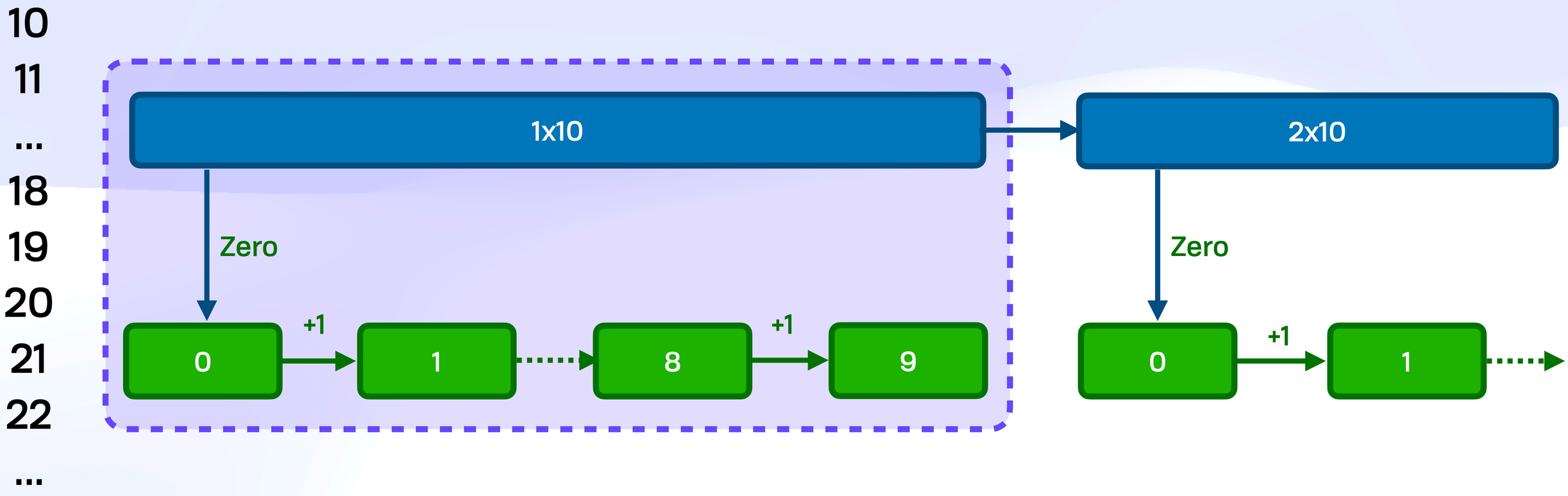
Security 🔐

Zeroing & Epochs



Security 🔐

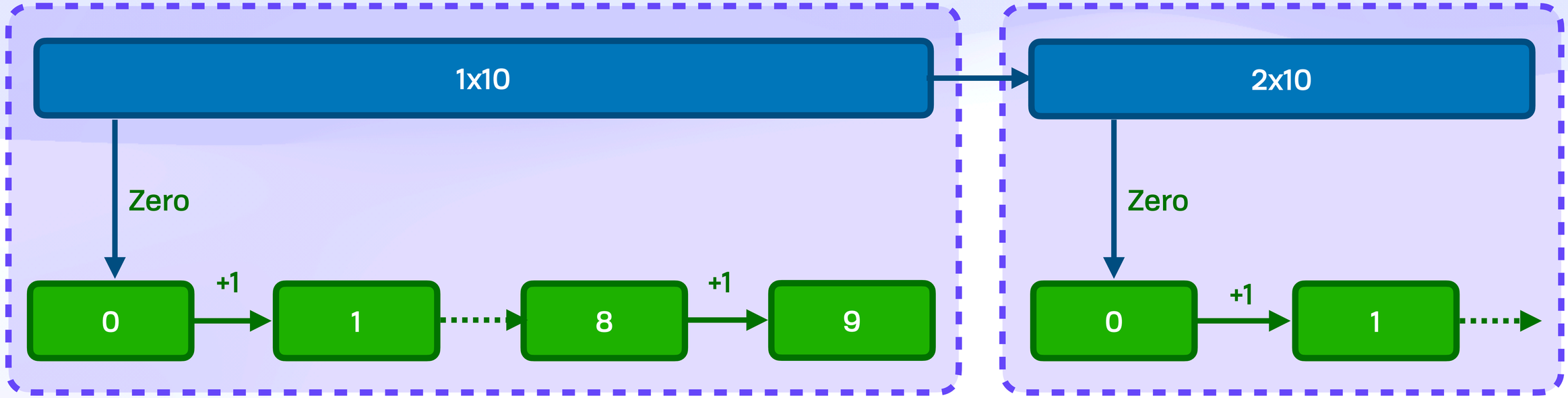
Zeroing & Epochs



Security 🔐

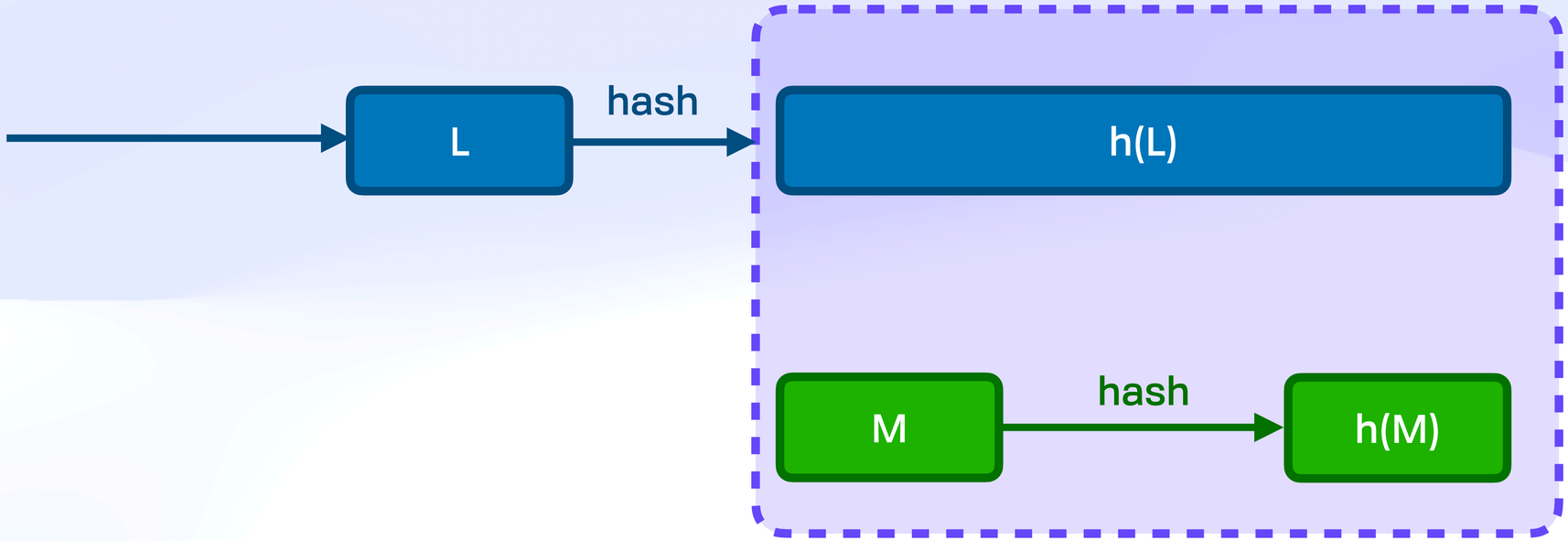
Zeroing & Epochs

10
11
...
18
19
20
21
22
...



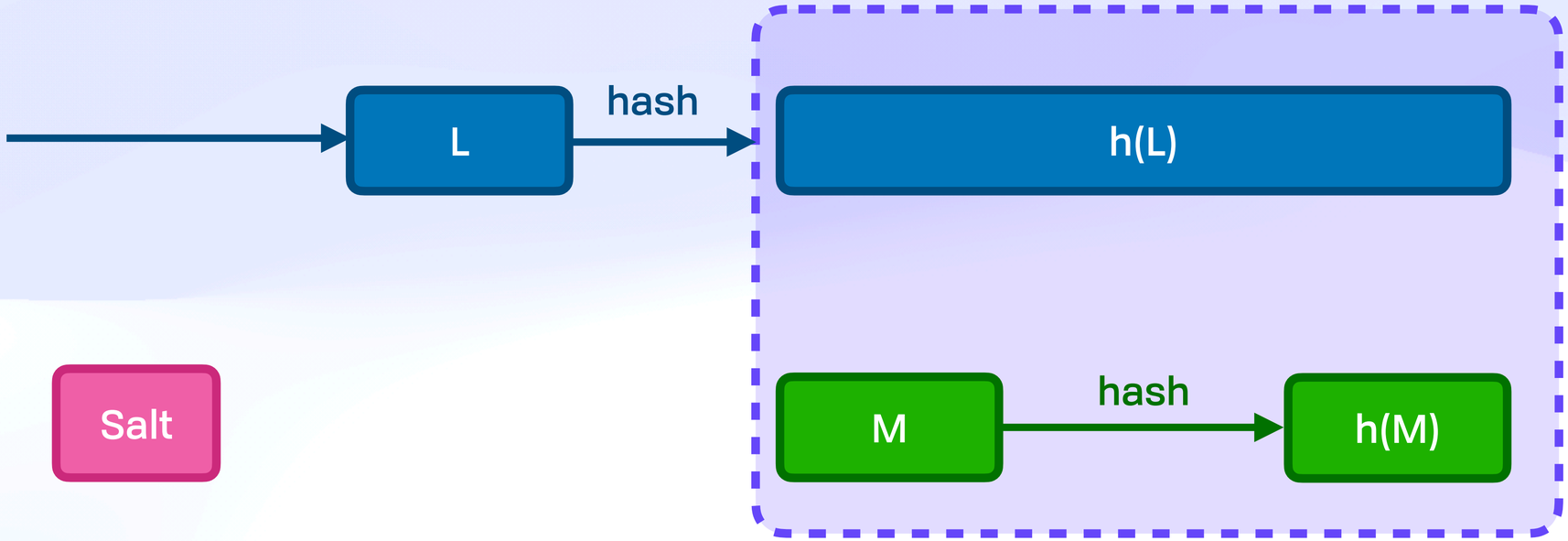
Security 🔐

Zeroing & Epochs



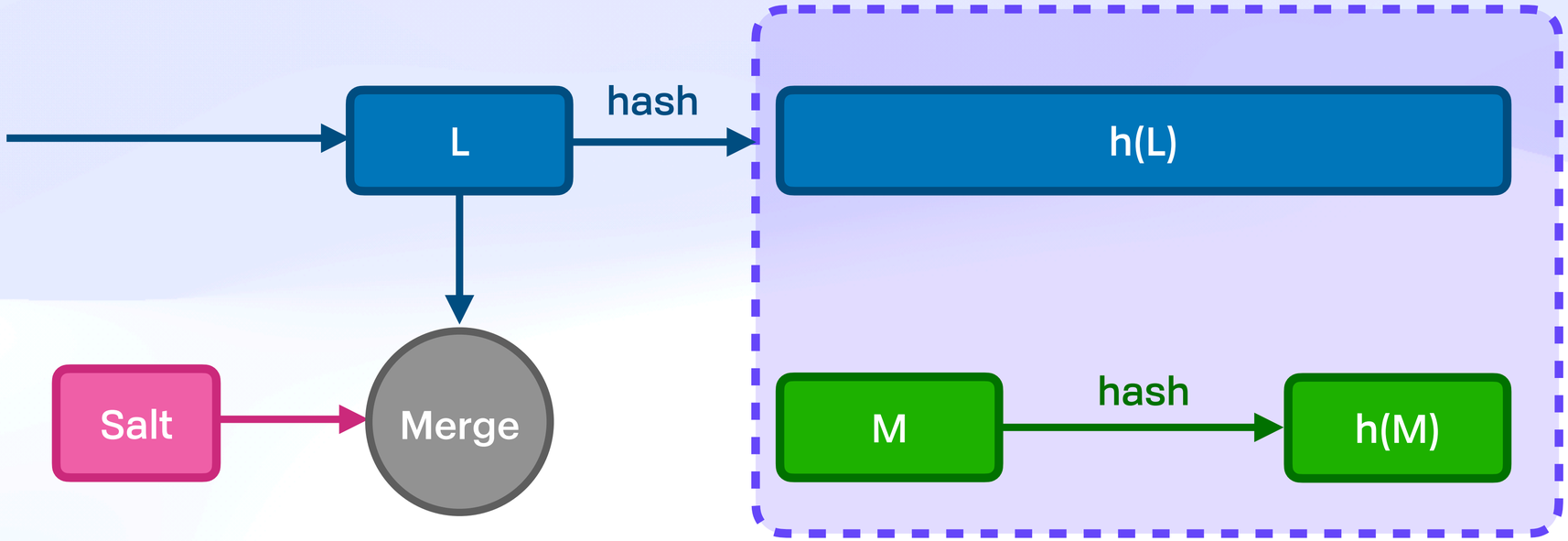
Security 🔐

Zeroing & Epochs



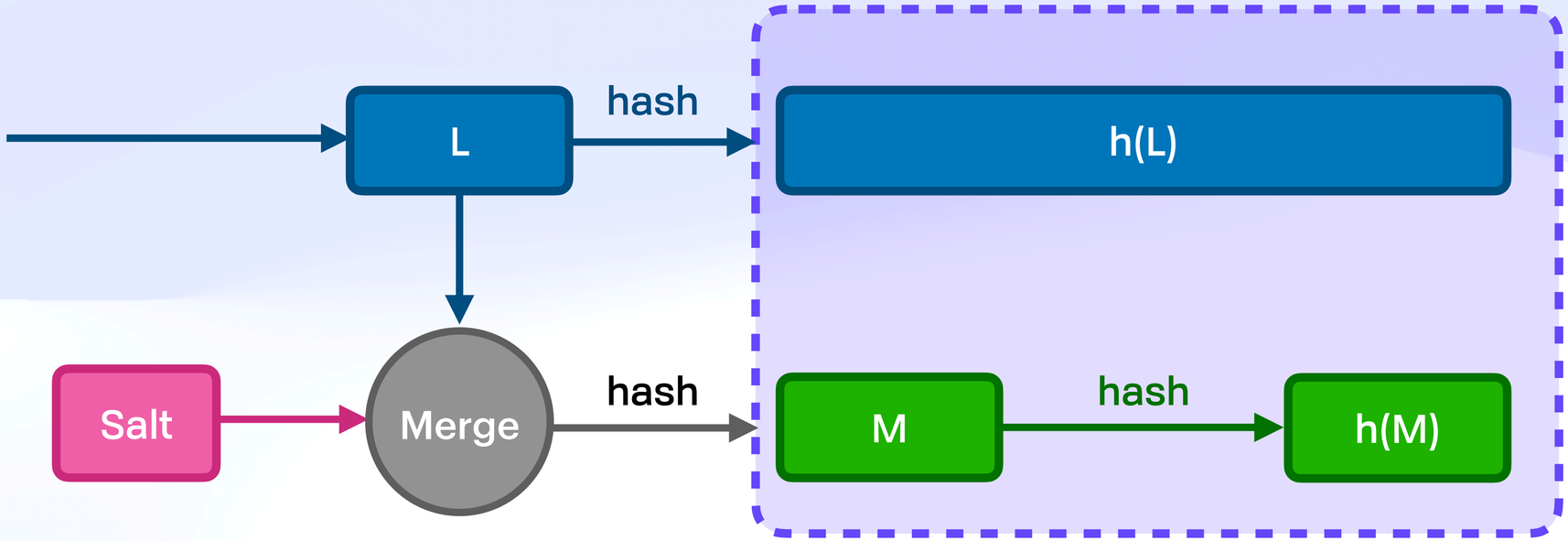
Security 🔐

Zeroing & Epochs



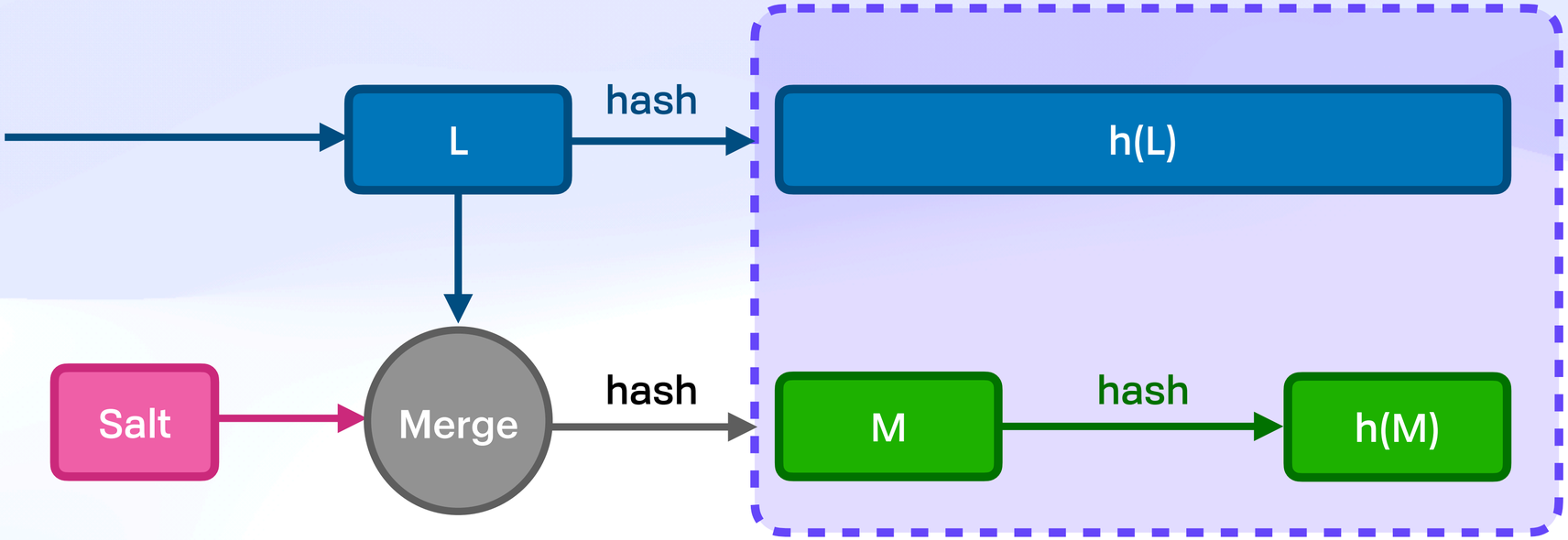
Security 🔐

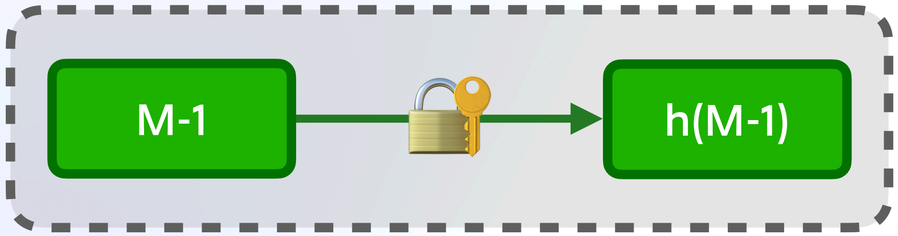
Zeroing & Epochs



Security 🔐

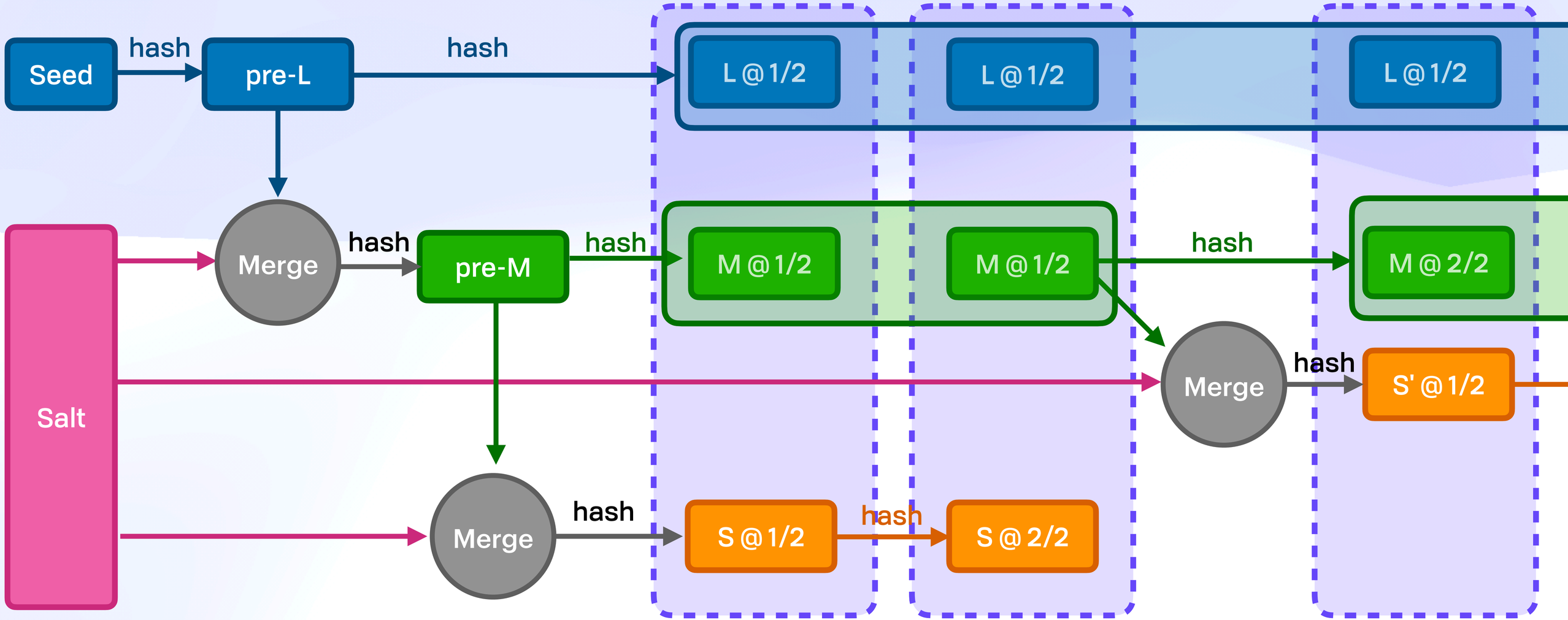
Zeroing & Epochs





Security 🔐

Setup



Security 🔐

Random Start 🙈🎲

Security 🔐

Random Start 🙈🎲

L

Security 🔐

Random Start 🙈🎲

Security 🔐

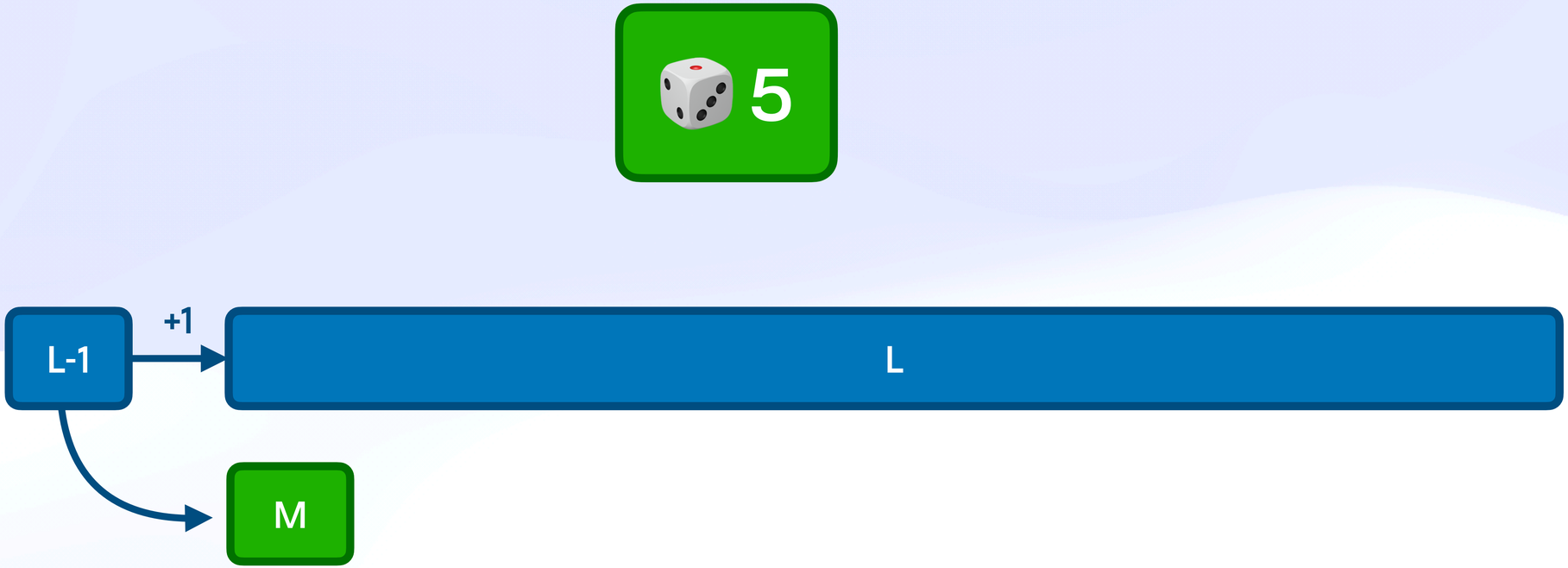
Random Start 🙈🎲

Security 🔐

Random Start 🙈🎲

Security 🔐

Random Start 🙈🎲



Security 🔐

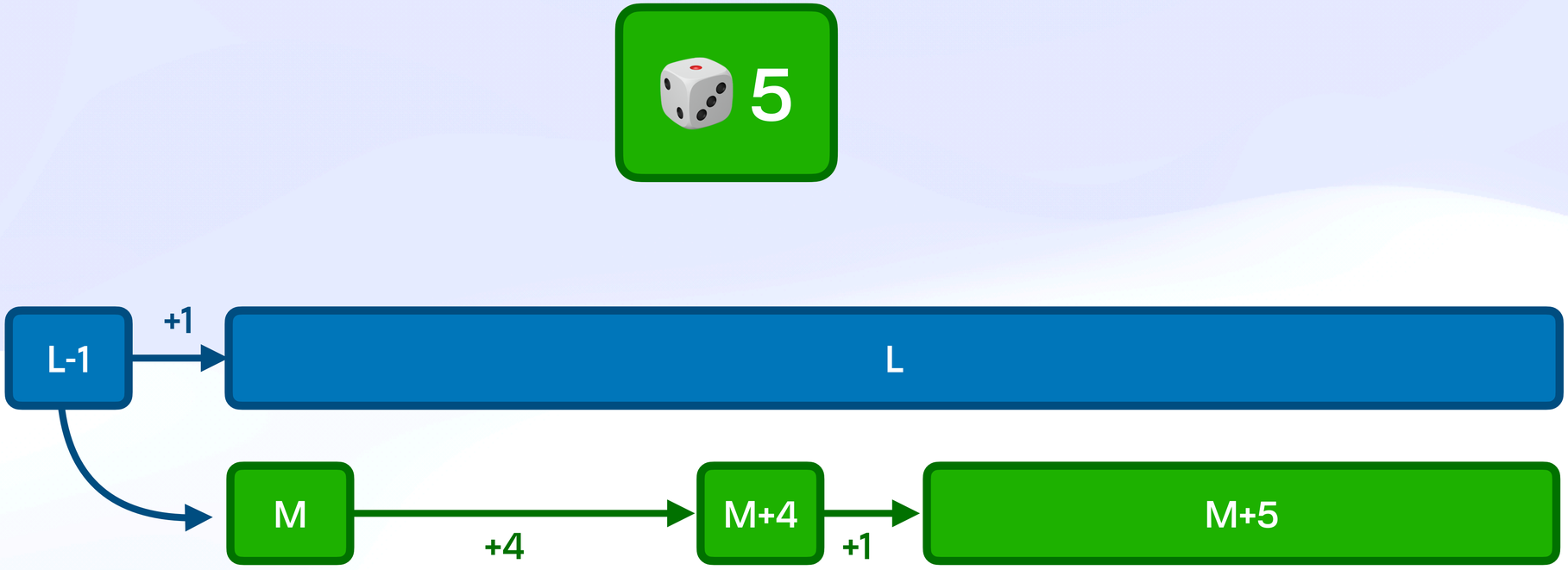
Random Start 🙈🎲

Security 🔐

Random Start 🙈🎲

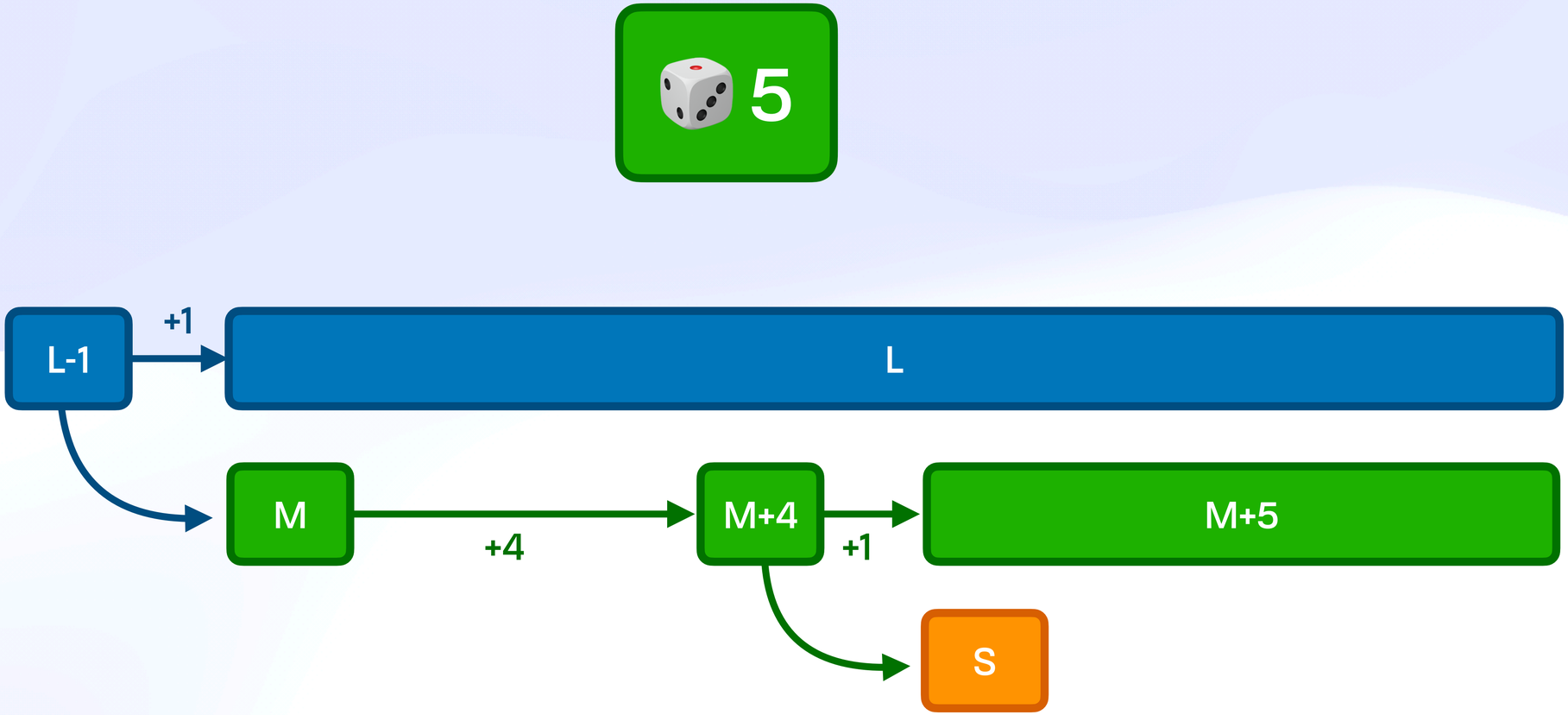
Security 🔐

Random Start 🙈🎲



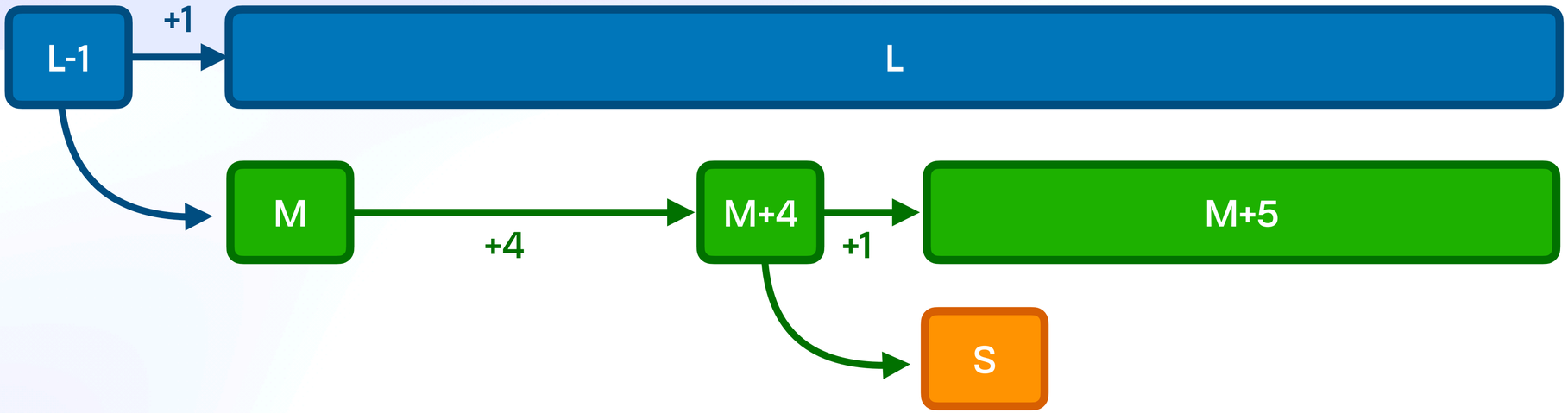
Security 🔐

Random Start 🙈🎲



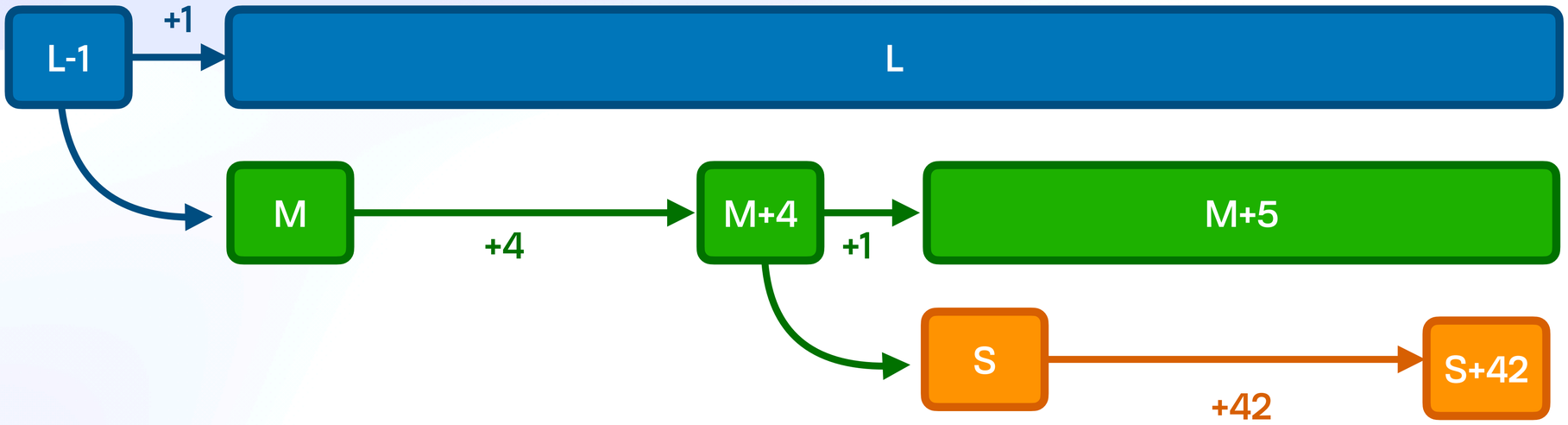
Security 🔐

Random Start 🙈🎲



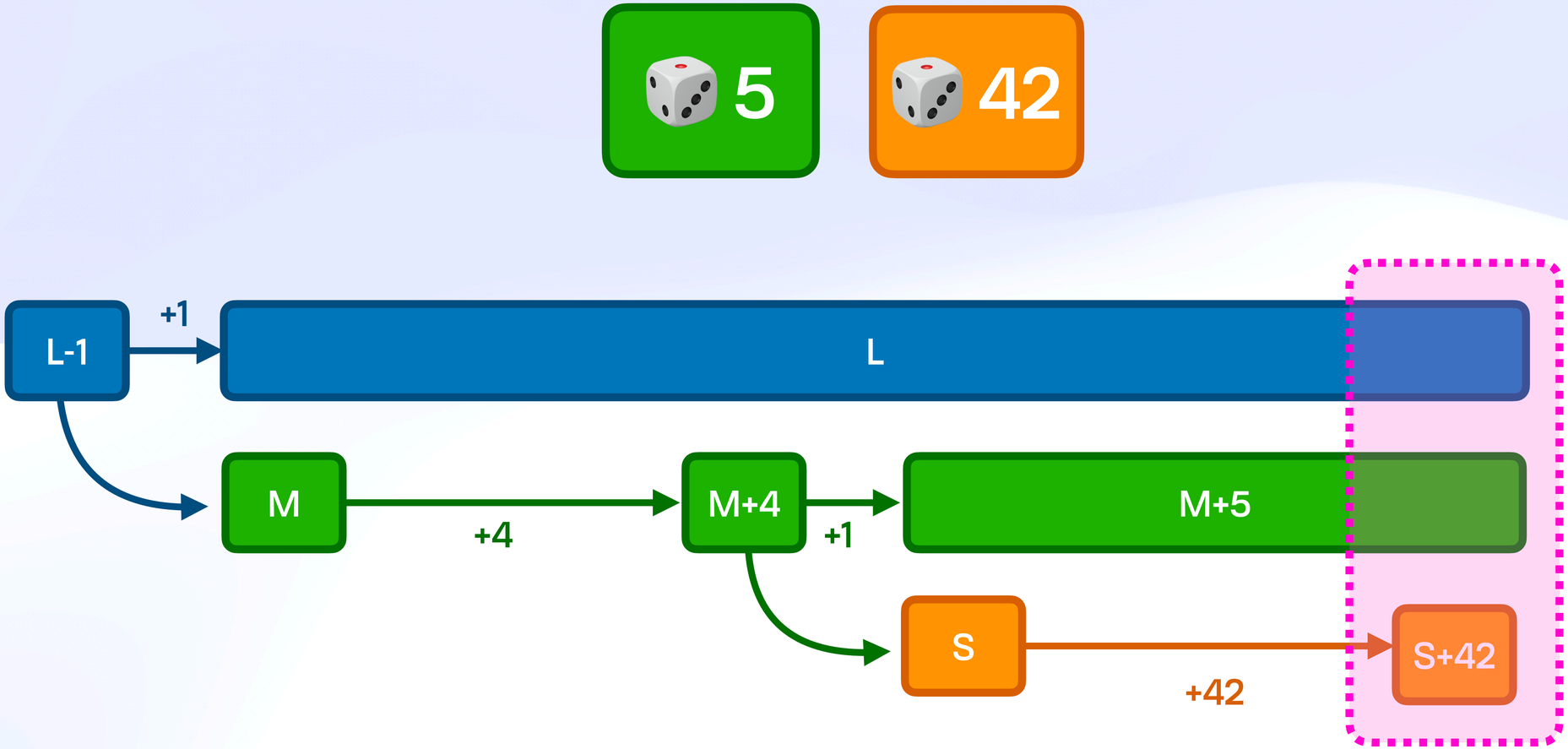
Security 🔐

Random Start 🙈🎲



Security 🔐

Random Start 🙈🎲

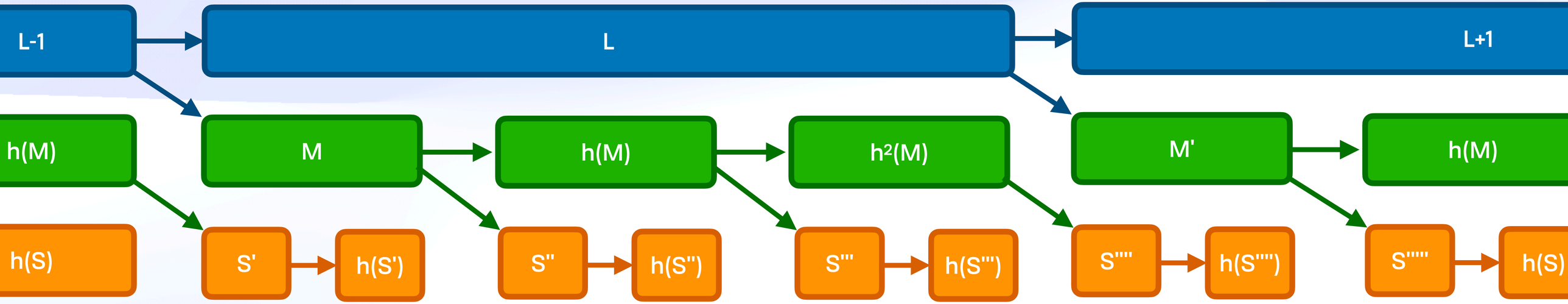


Security 🔐

Unary + Positional

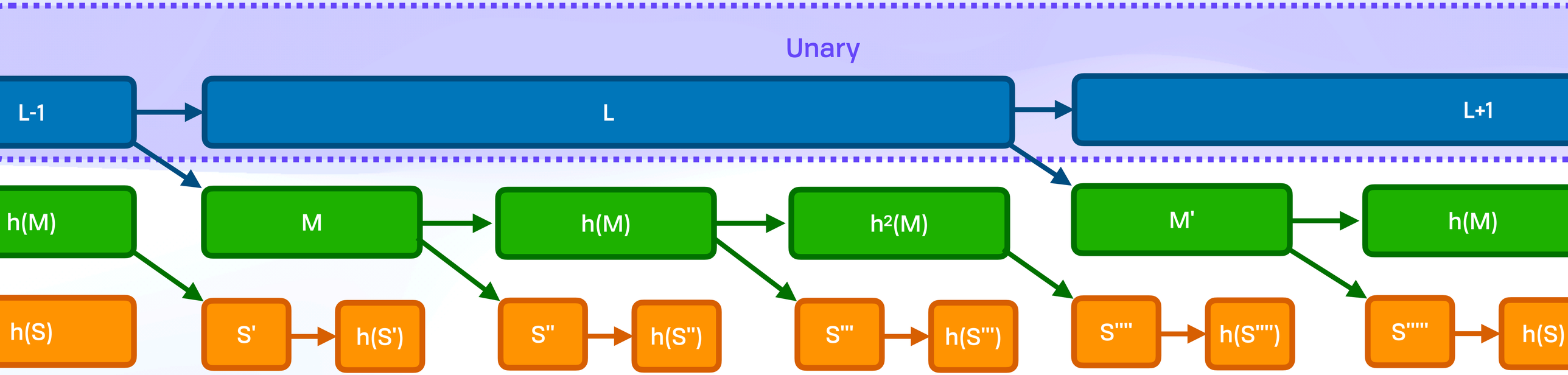
Security 🔐

Unary + Positional



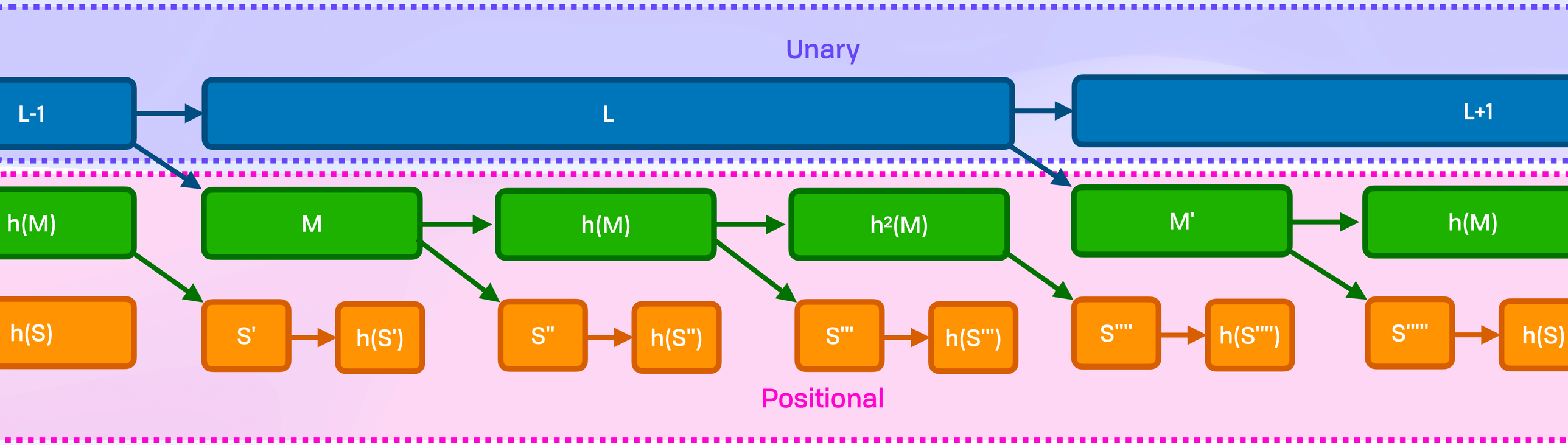
Security 🔐

Unary + Positional



Security 🔐

Unary + Positional

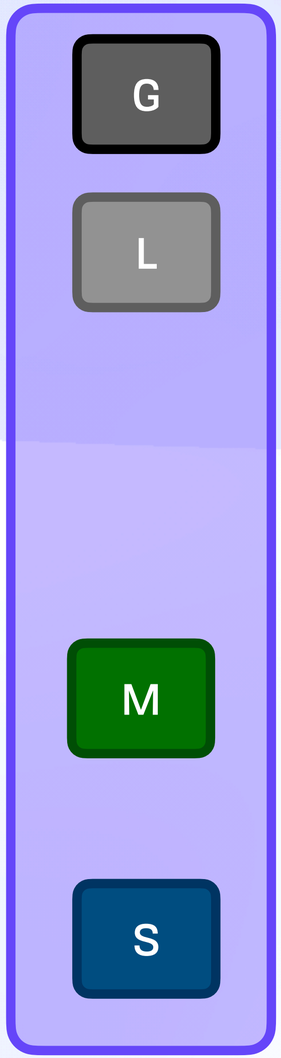


Security 🔐

Limiting Ranges 🗜️

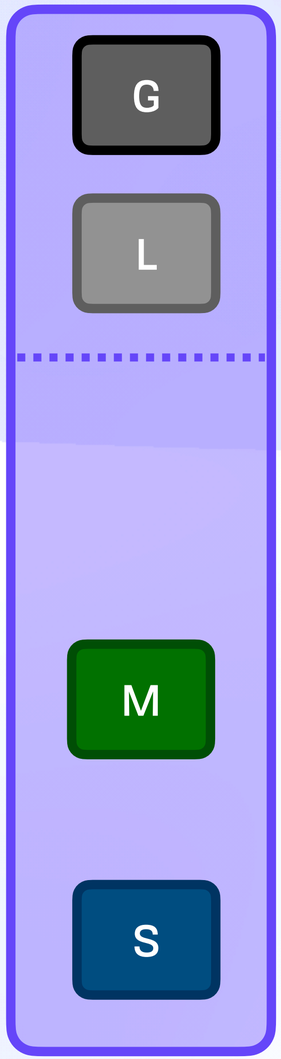
Security 🔐

Limiting Ranges 🗜️



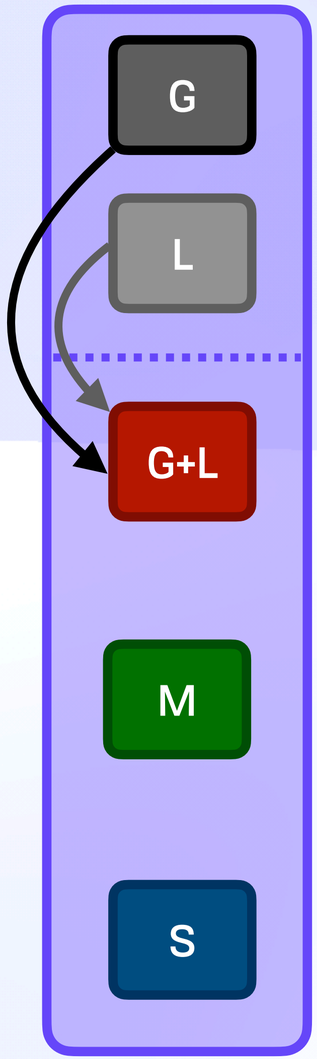
Security 🔐

Limiting Ranges 🗜️



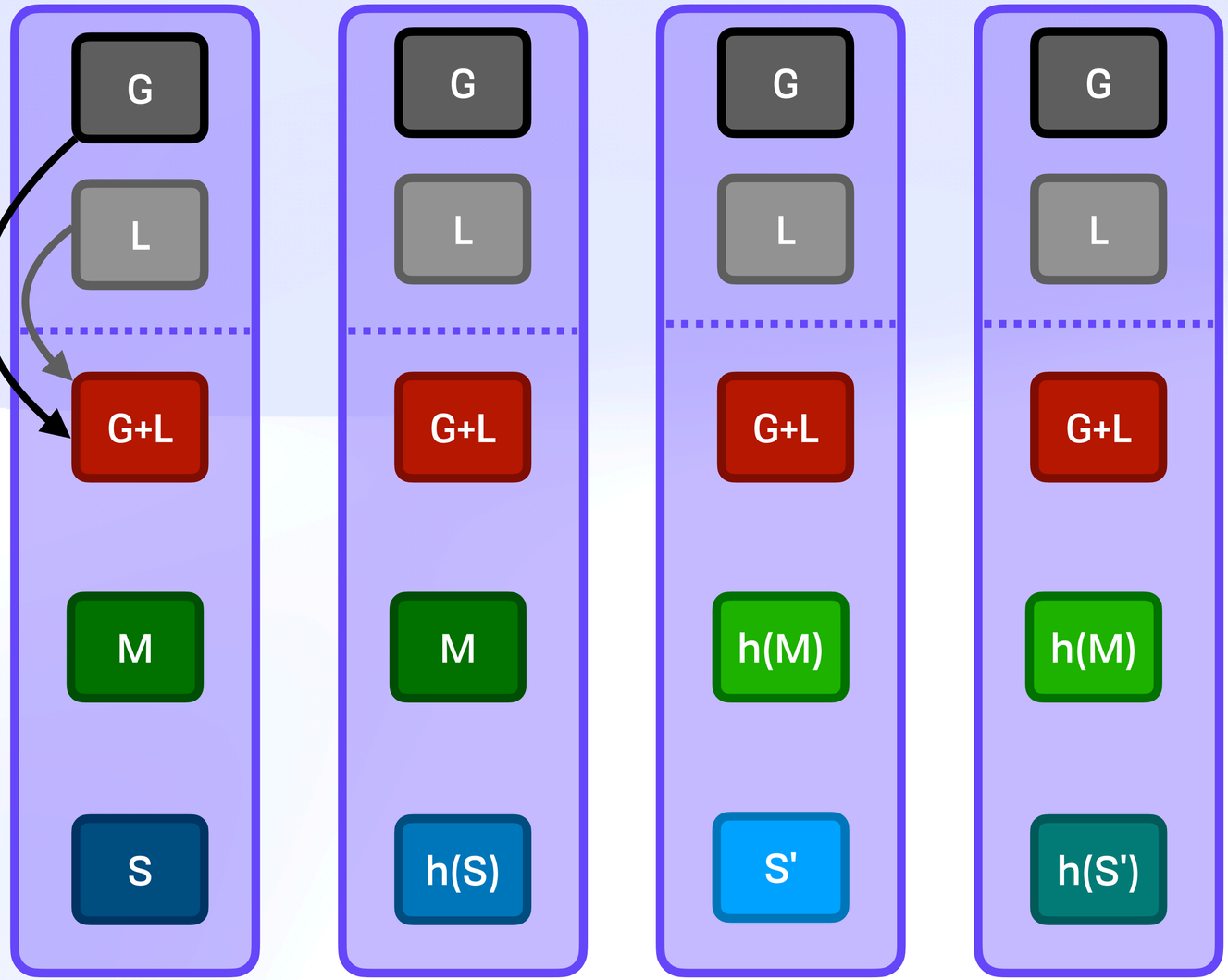
Security 🔐

Limiting Ranges 🗜️



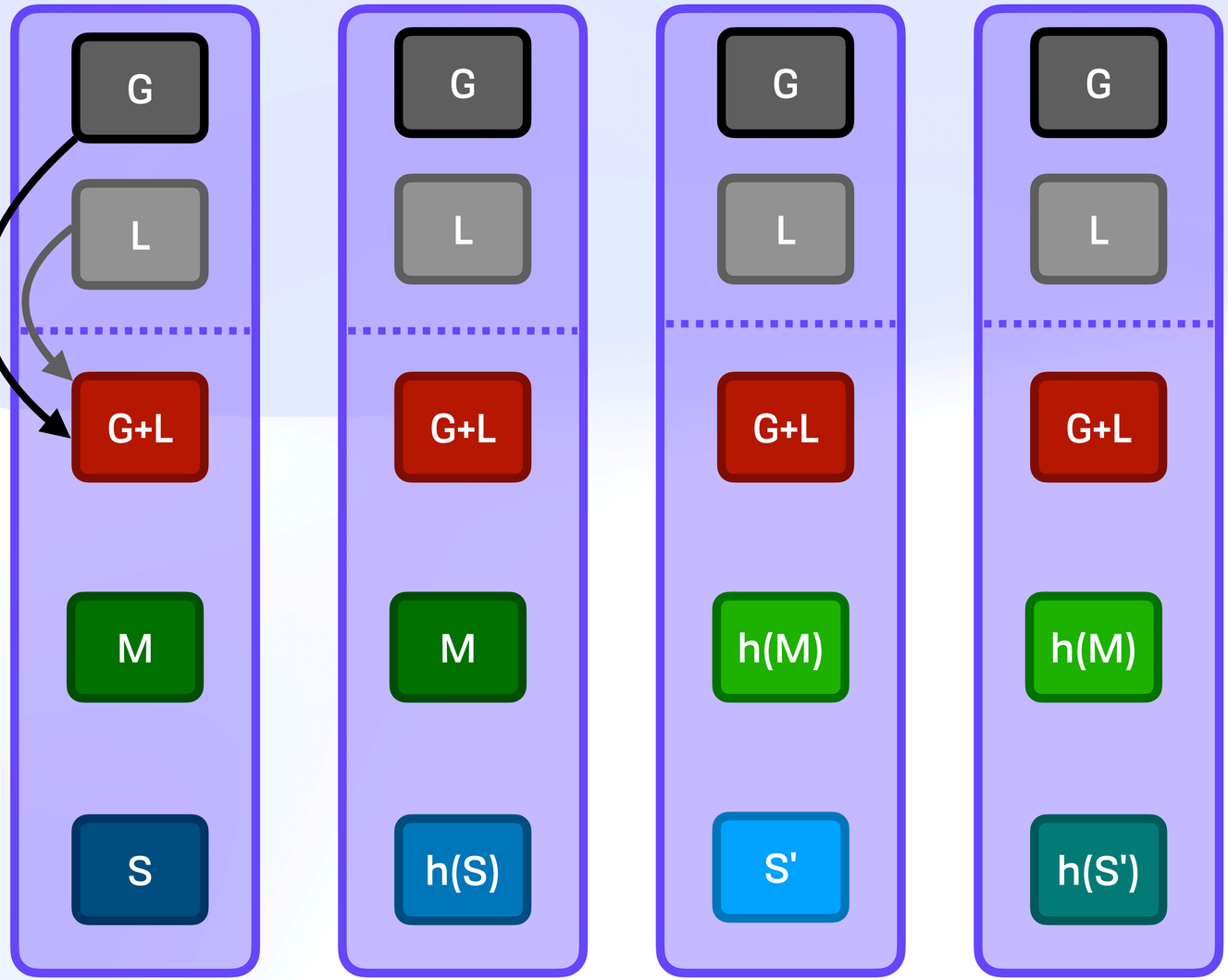
Security 🔐

Limiting Ranges 🗜️



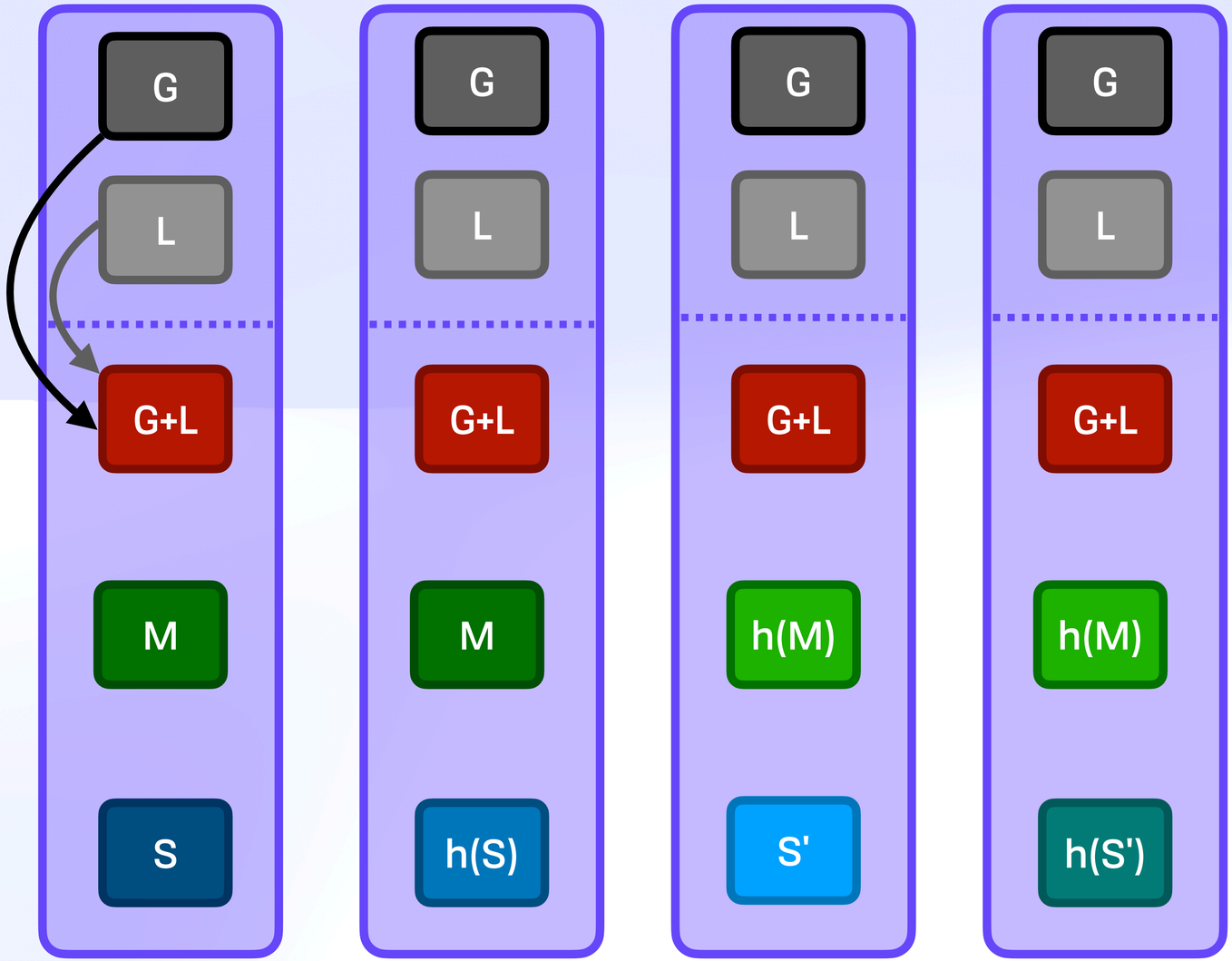
Security 🔐

Limiting Ranges 🗜️



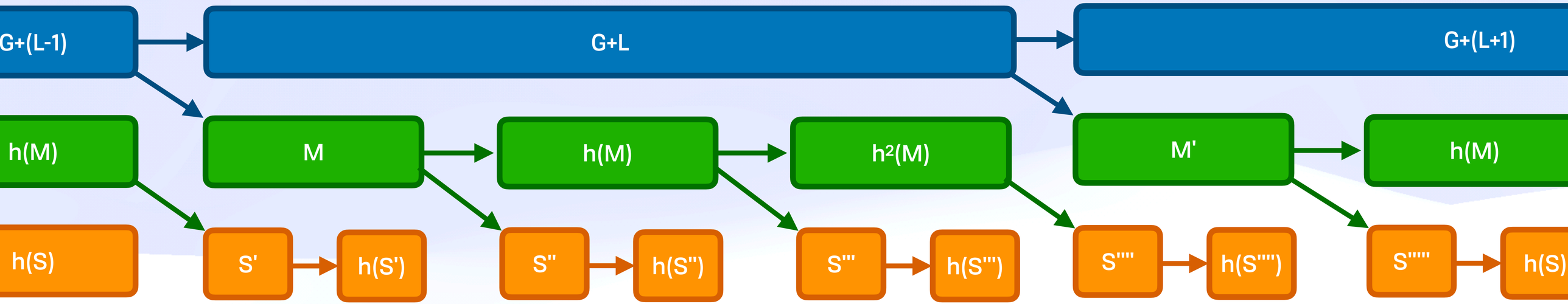
Security 🔐

Limiting Ranges 🗜️



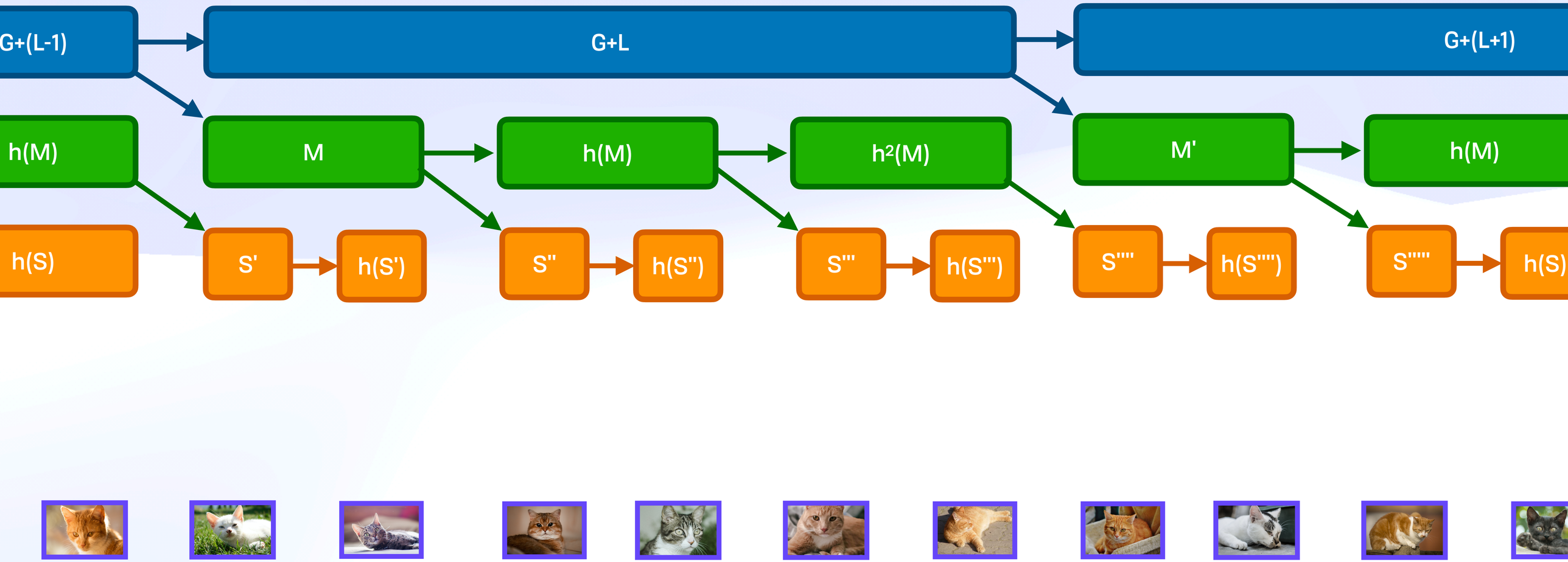
Security 🔐

Range Access



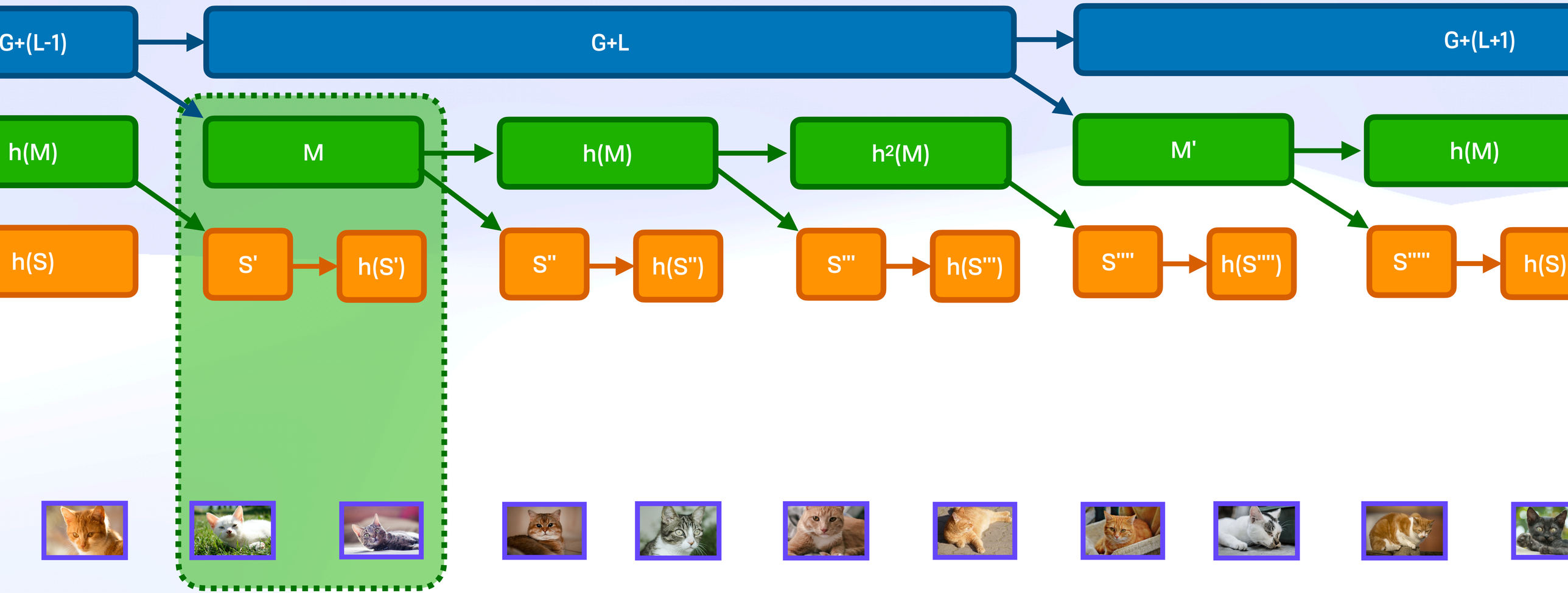
Security 🔐

Range Access



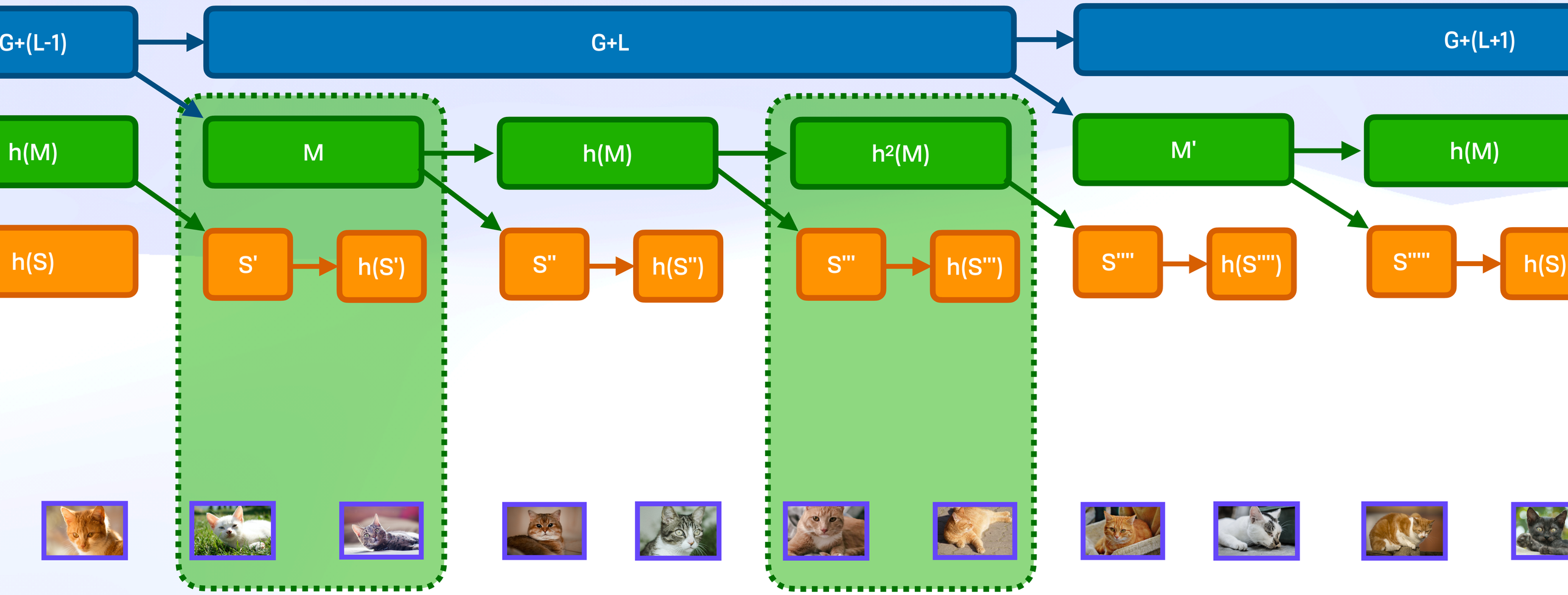
Security 🔐

Range Access



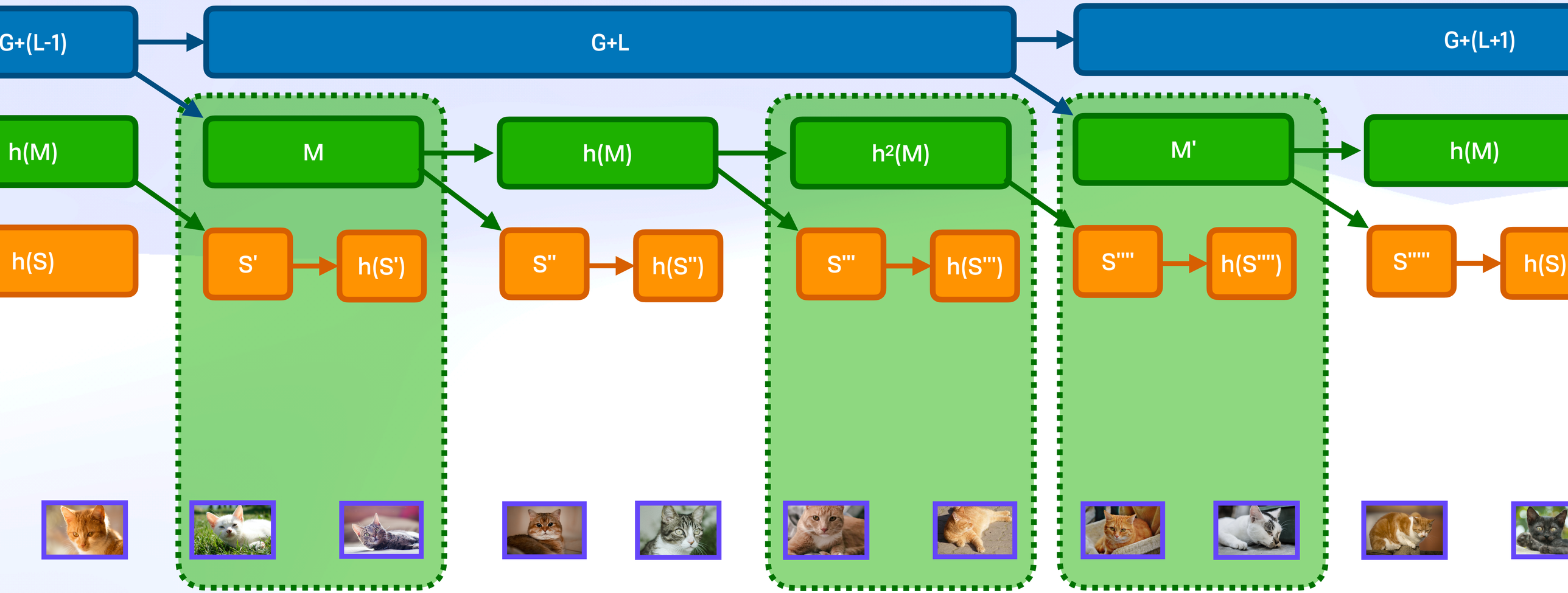
Security 🔐

Range Access



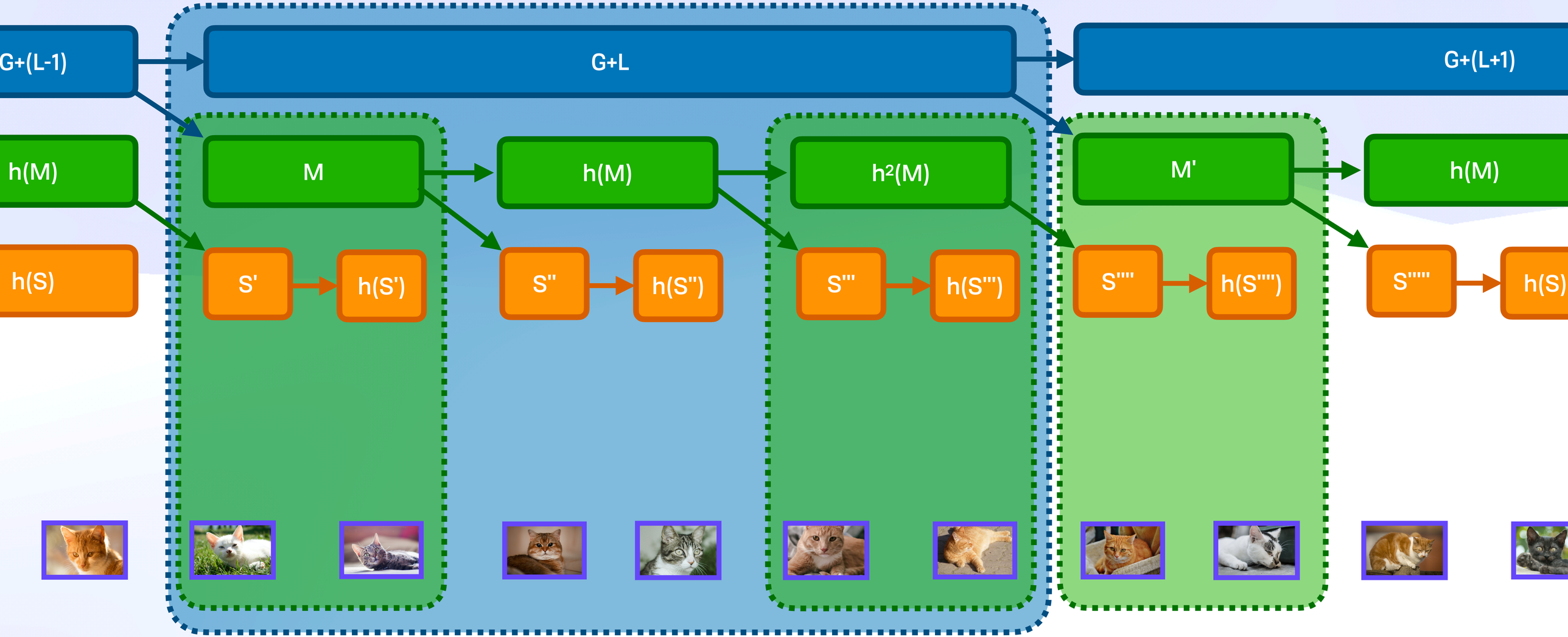
Security 🔐

Range Access



Security 🔐

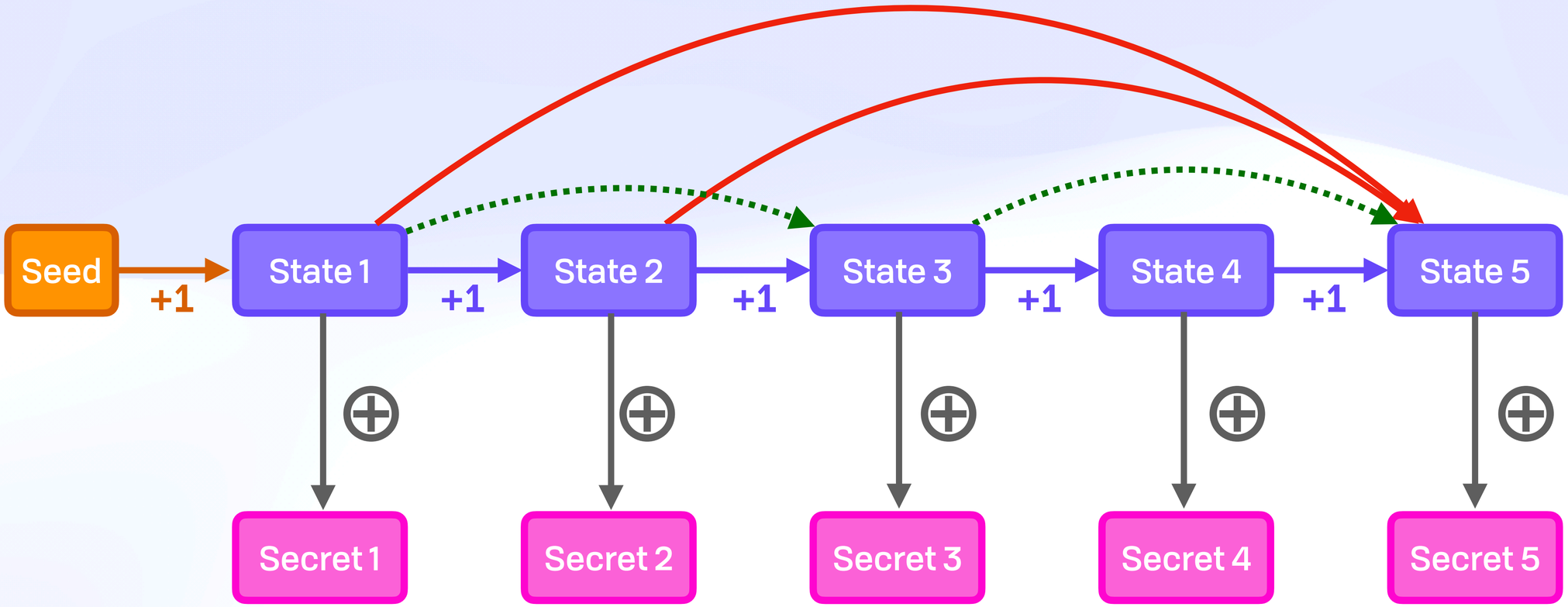
Range Access



Wrap Up

Wrap Up 🎁

Skip Ratchet



Wrap Up 🎁

Takeaways

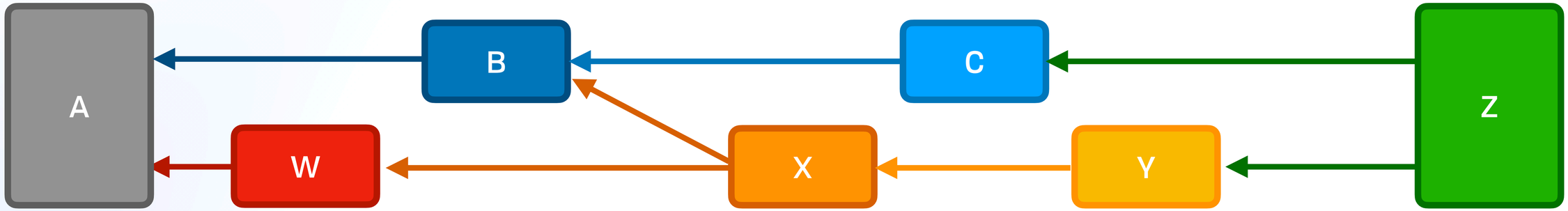
Wrap Up 🎁

Takeaways

- Really fast secrets thanks to positional structure
- In production in several systems, still finding more uses
- Very disparate ideas share some common core
- Many ways to tackle a problem
- There's still tons of low hanging fruit out there!

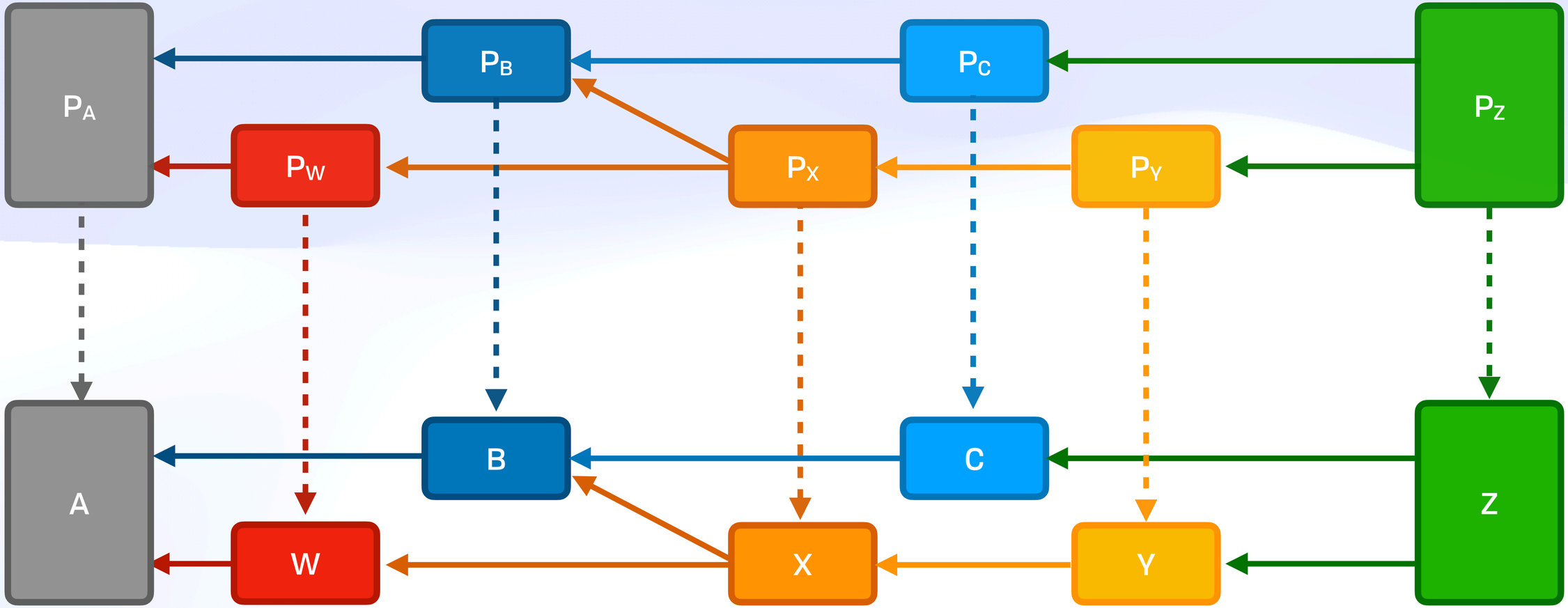
Wrap Up 🎁

WNFS: Skip Ratchet In Situ



Wrap Up 🎁

WNFS: Skip Ratchet In Situ



🎉 Thank You, Strange Loop ♾️

@expede
brooklyn@fission.codes
https://eprint.iacr.org/2022/1078.pdf