P4Chaskey: An Efficient MAC Algorithm for PISA Switches

Martim Francisco*, Bernardo Ferreira*, Fernando M. V. Ramos†, Eduard Marin†, Salvatore Signorello ‡*

*LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal

†INESC-ID, Instituto Superior Técnico, University of Lisbon

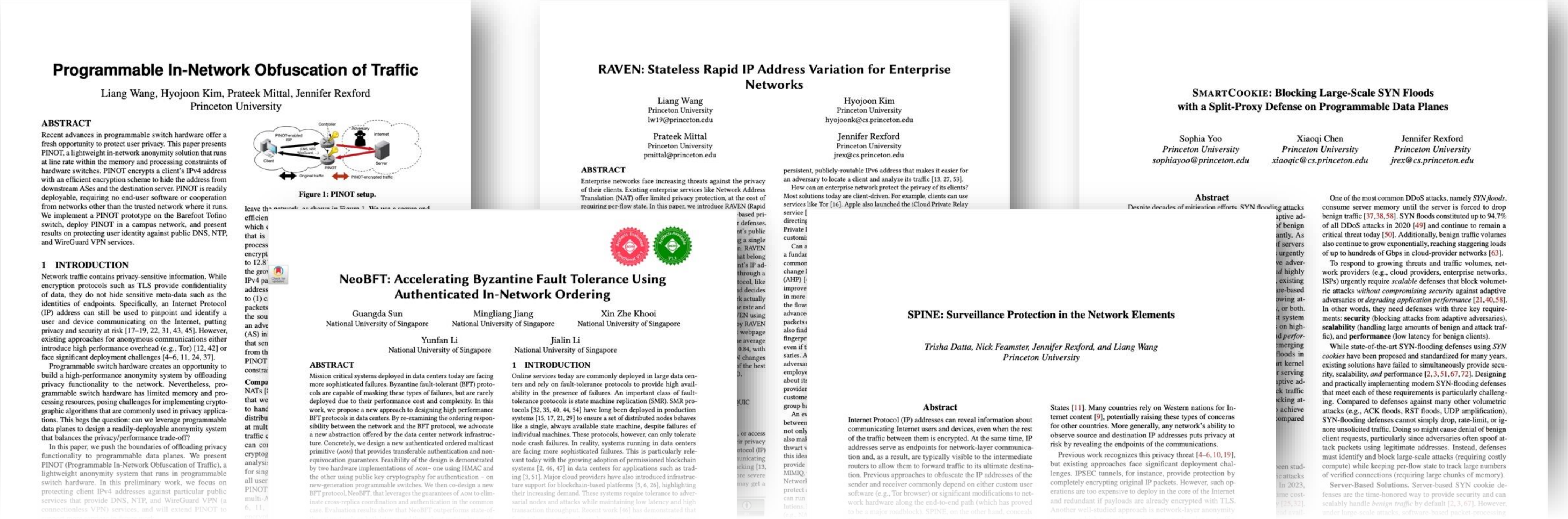
‡Telefonica Research, Spain

7th European P4 Workshop – EuroP4'24

October 28, 2024 – Charleroi, Belgium

In-Network Cryptography

The use of cryptography in the data plane has shown potential to improve anonymity, DDoS defense and BFT protocol design.



In-Network Cryptography for SCION

contributed articles

DOI:10.1145/3085591

Adhering to the end-to-end principle even more than the current Internet yields highly available point-to-point communication.

BY DAVID BARRERA, LAURENT CHUAT, ADRIAN PERRIG, RAPHAEL M. REISCHUK, AND PAWEL SZALACHOWSKI

The SCION Internet Architecture

THE INTERNET HAS been successful beyond even the most optimistic expectations. It permeates almost every aspect of our society and economy worldwide. This success has created universal dependence on communication, as many of the processes underpinning modern society would grind to a halt if it were unavailable. However, the state of the safety and availability of the Internet is far from commensurate with its importance.

Although we cannot conclusively determine what the impact of even a one-minute outage of Internet connectivity would be, anecdotal evidence suggests that even a brief outage would have a profound negative effect on governmental, economic, and societal operations.[11] Making matters worse, the Internet is not designed primarily for high availability

» key insights

- Patching the current Internet is an undesirable long-term solution; a clean-slate redesign of inter-domain routing would provide many benefits and is surprisingly simple to deploy using legacy protocols for intra-domain communication.
- SCION's isolation domains offer control-plane isolation and scoped trust; rather than restrict communication, they provide transparency for path selection, packet forwarding, and authentication.
- SCION's packet-carried forwarding state eliminates the need for inter-domain routing table lookups, improves

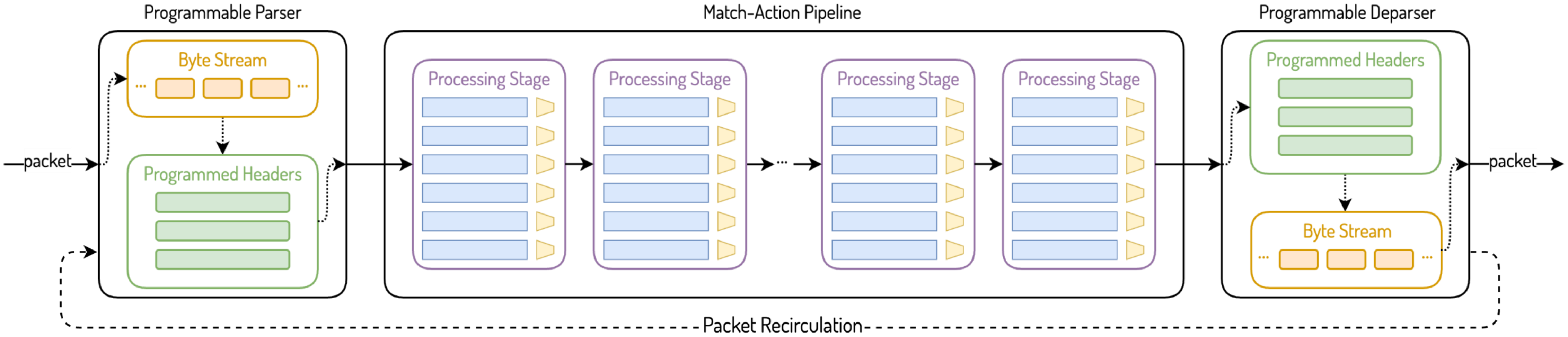
Emerging Internet architecture designs advocate for per-packet cryptographic verifications.

The lack of cryptographic accelerators in networking hardware has precluded cryptographic computations in the network core.

Architectures such as SCION are restricted to implementations in software with throughputs of tens of Gbps at best.

Programmable Terabit Switching Architecture

Terabit speed programmable switching architectures, such as PISA, offer a clear opportunity to implement cryptographic primitives in the data plane.



Cryptographic Primitives on PISA Switches

Minimum number of pipeline stages for a 128-bit input

Algorithm	Key Size (Bits)	# of Rounds	Stages per Round	Total Stages
ASCON[1]	128	24	8	192
AES - CMAC[2]	128	10	5	50
SipHash[3]	128	10	6	60
HalfSipHash[4]	64	14	4	56

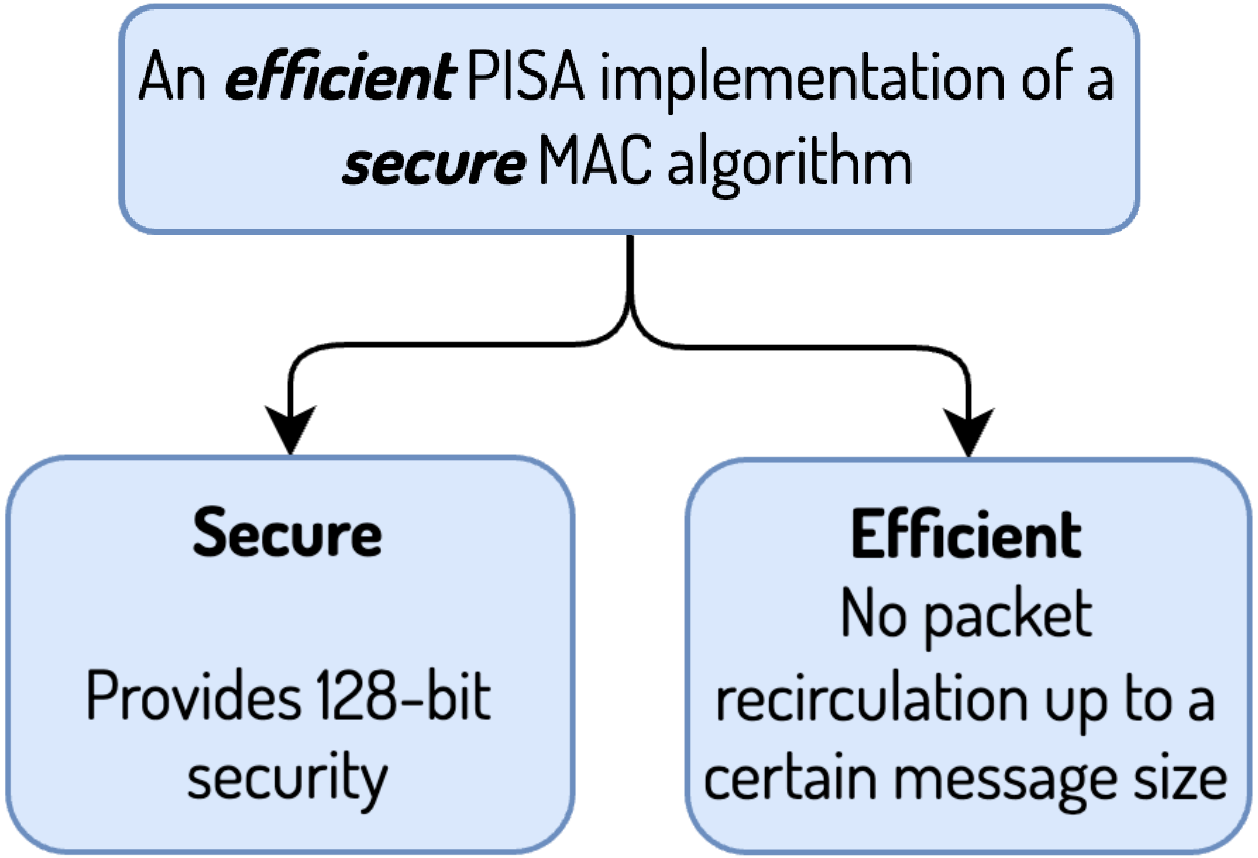
[1] Archit Bhatnagar, Xin Zhe Khooi, Cha Hwan Song, Mun Choon Chan. 2023. P4EAD: Securing the In-band Control Channels on Commodity Programmable Switches;

[2] Lars-Christian Schulz, Robin Wehner, David Hausheer. 2023. Cryptographic Path Validation for SCION in P4;

[3] Yutaro Yoshinaka, Mio Kochiyama, Yuki Koizumi, Junji Takemasa, Toru Hasegawa. 2024. A Lightweight Anonymity Protocol at Terabit Speeds on Programmable Switches;

[4] Sophia Yoo, Xiaoqi Chen. 2021. Secure Keyed Hashing on Programmable Switches.

Target Properties for a MAC on PISA



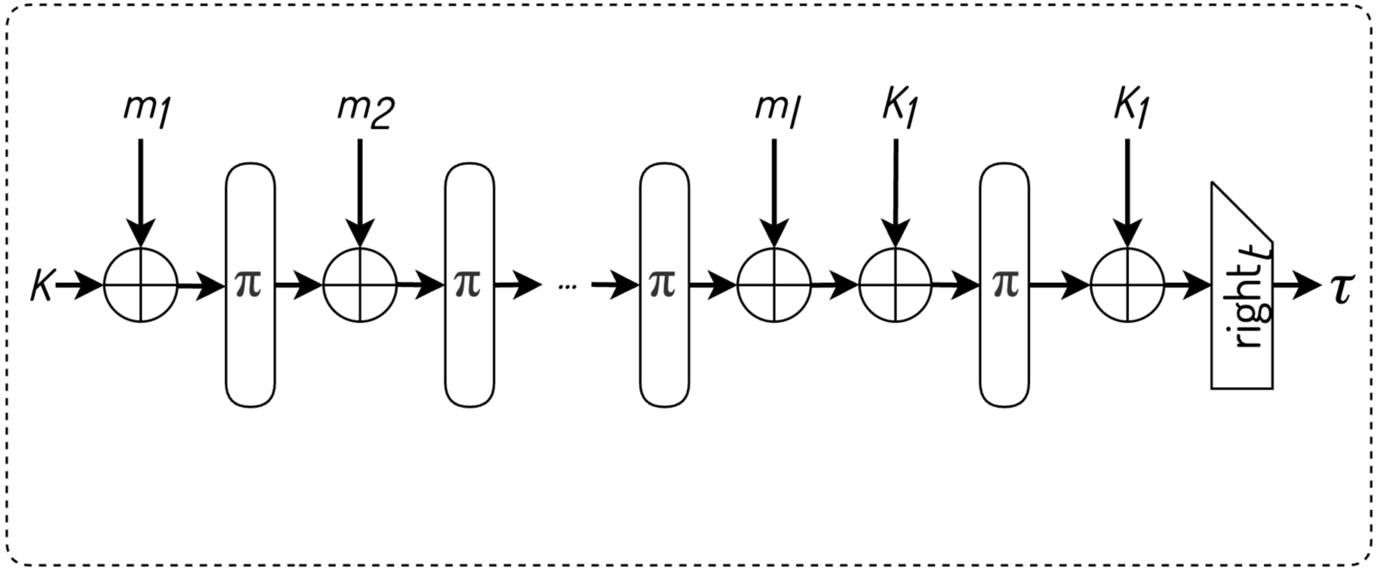
Our answer is P4Chaskey!

The Chaskey MAC Algorithm

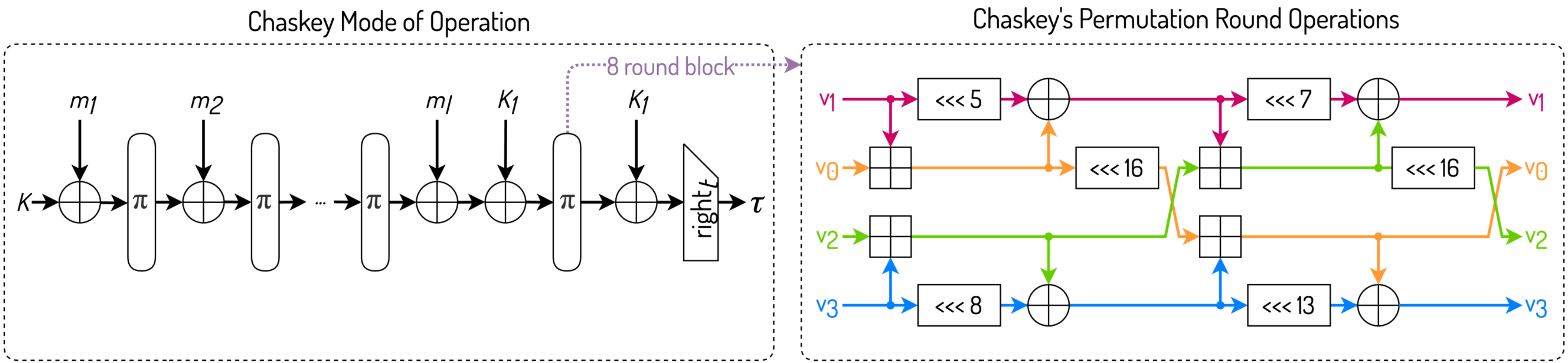
Permutation-based MAC algorithm for 32-bit microcontrollers:

- Processes a message *m* into *l* blocks of $n = 128$ bits each through π permutation rounds.

Chaskey Mode of Operation

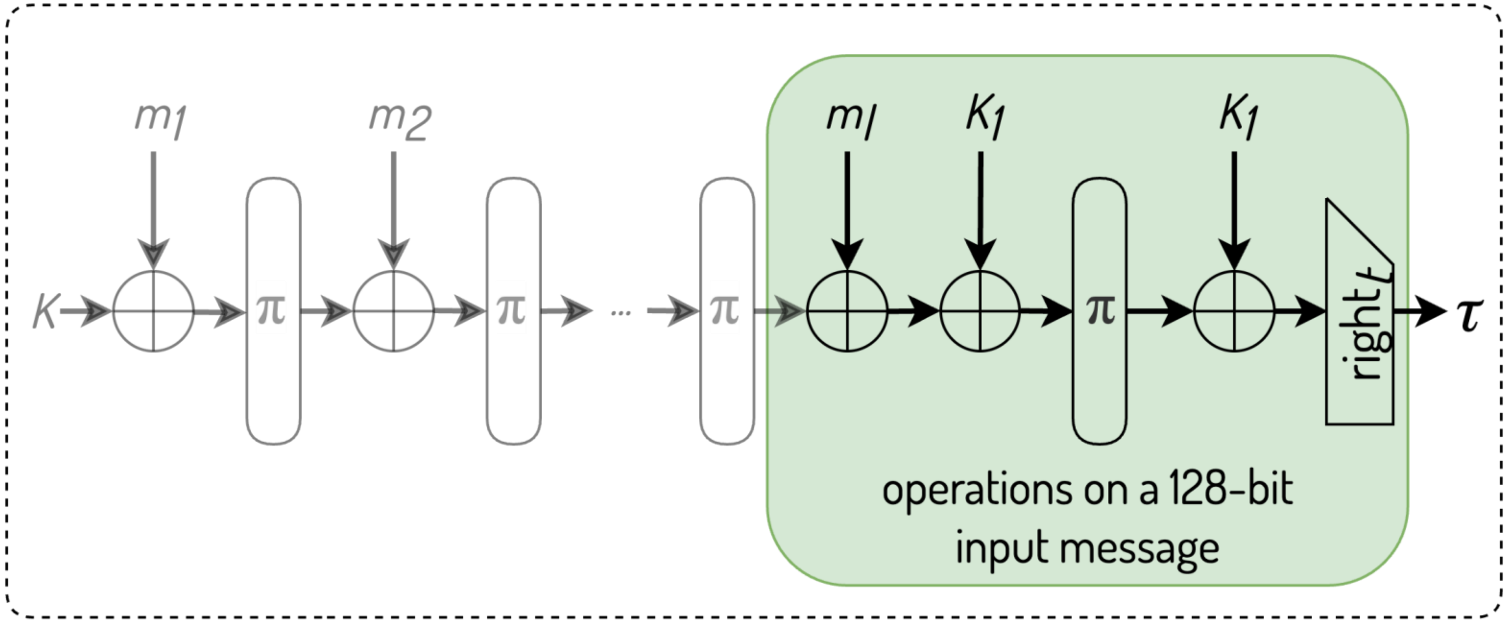


Chaskey's Operations



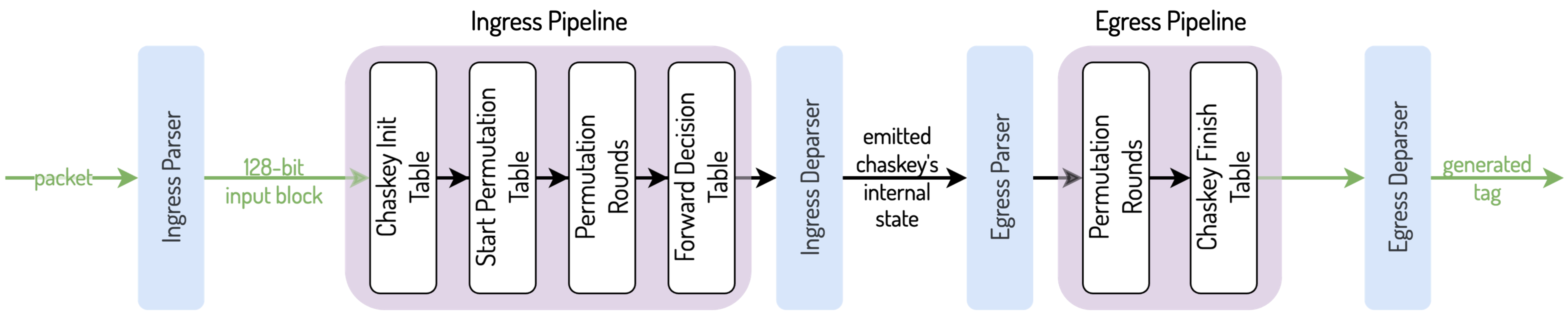
Chaskey for a 128-bit Input Message

Chaskey Mode of Operation



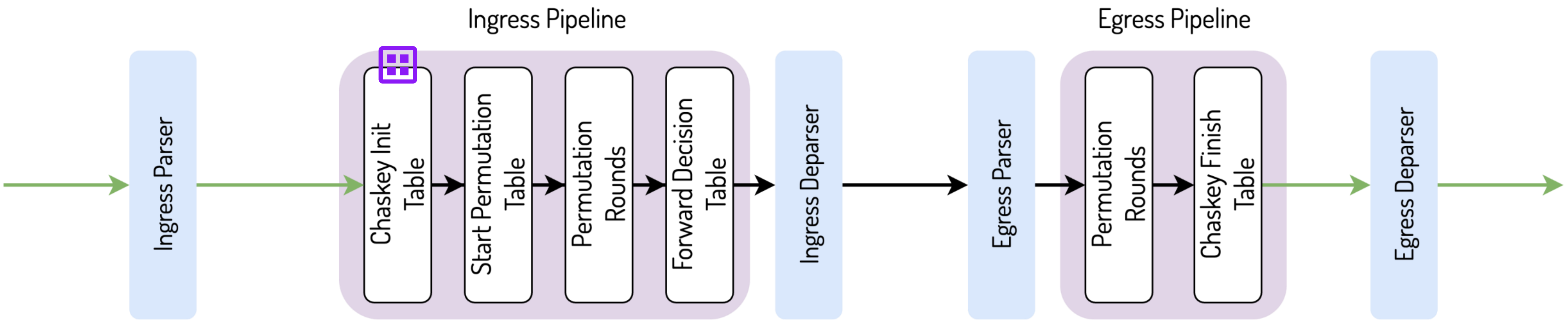
P4Chaskey Design & Implementation

P4Chaskey Design



P4Chaskey Control Flow

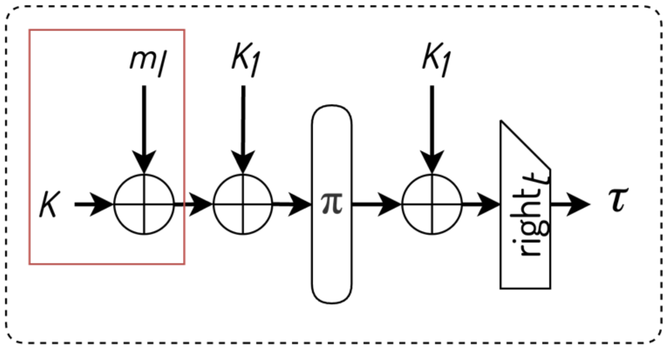
Current Round: 0



Chaskey Init Table

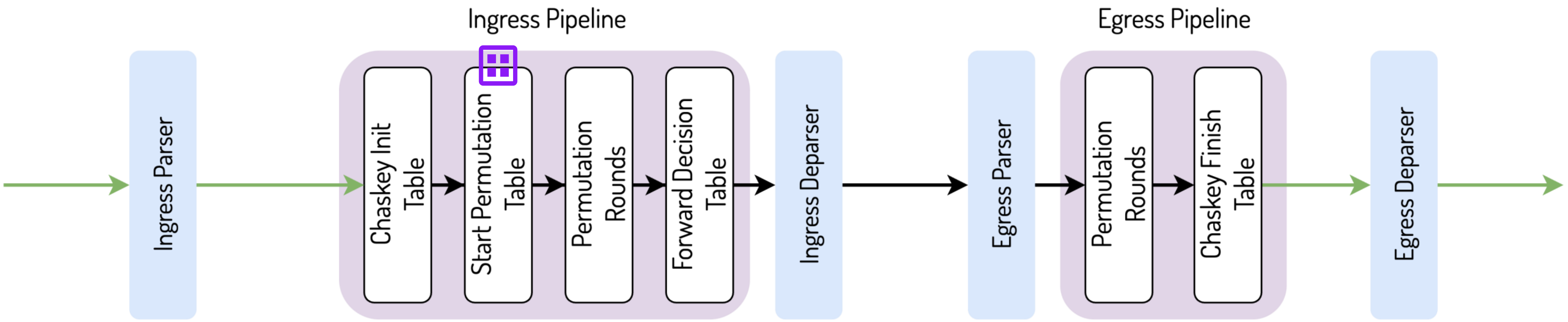
Chaskey Meta Hdr	Operation
isValid = false	Setup internal state v (m ⊕ k)

Position in Chaskey's Algorithm

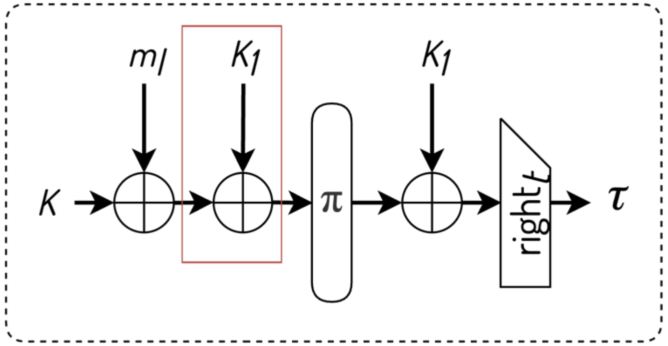


P4Chaskey Control Flow

Current Round: 0



Position in Chaskey's Algorithm

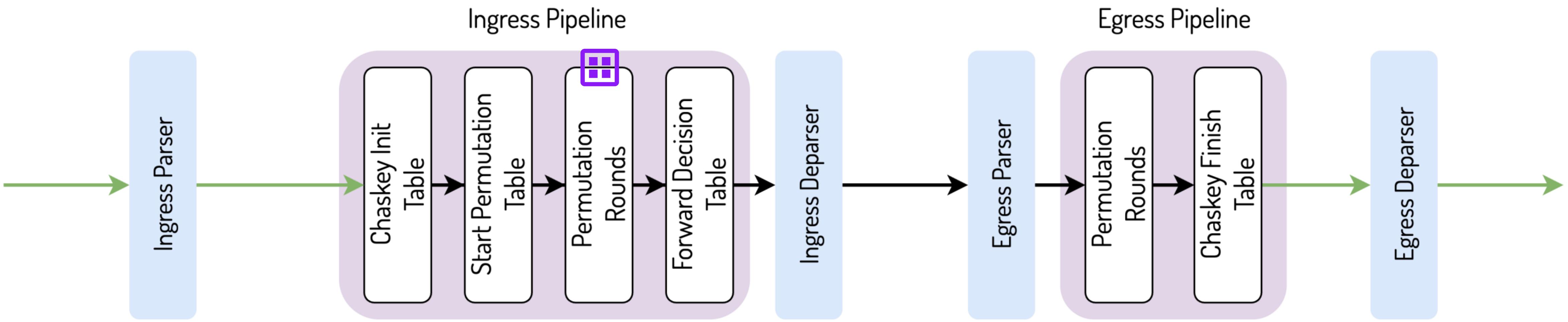


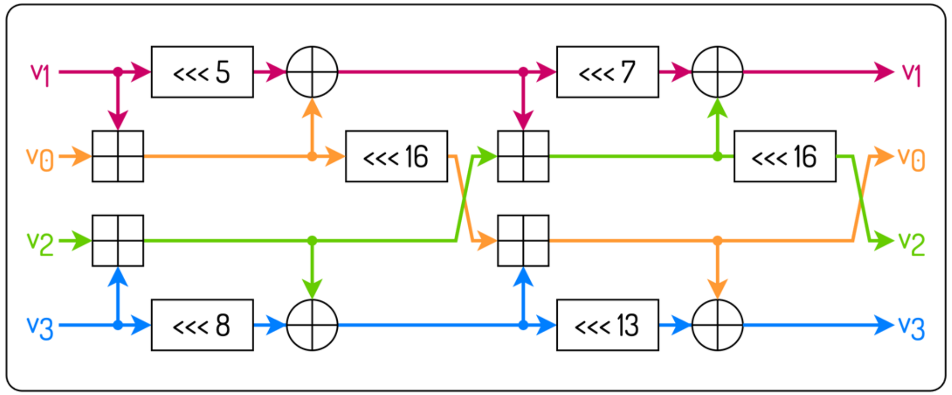
Start Permutation Table

Current Round	Operation
0	Setup (Final) Permutation ($v \oplus k_1$)

P4Chaskey Control Flow

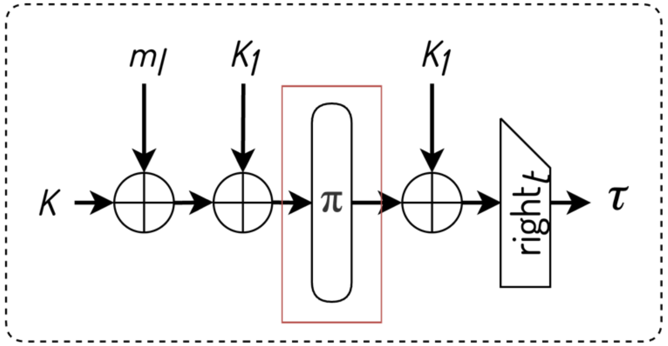
Current Round: 0





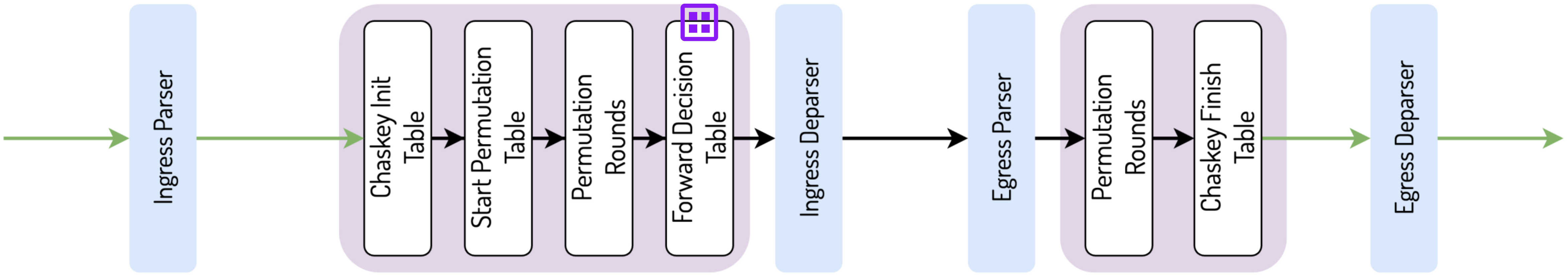
X 4

Position in Chaskey's Algorithm



P4Chaskey Control Flow

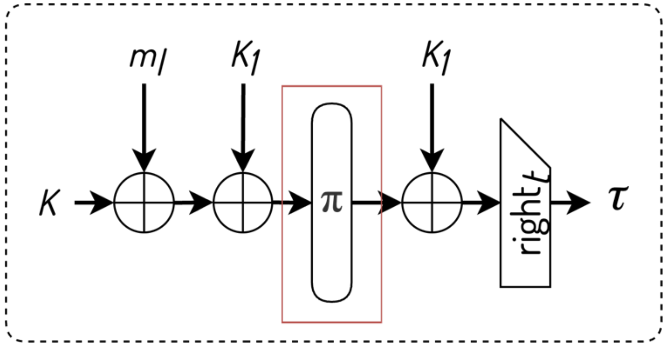
Current Round: 4



Forward Decision Table

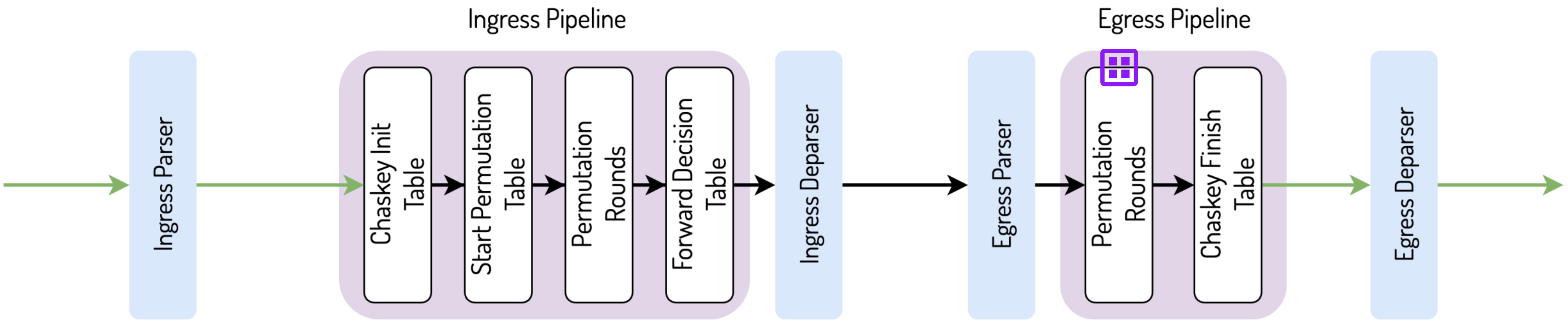
Current Round	Operation
0	Set the output port to the destination Update the current round field to 4

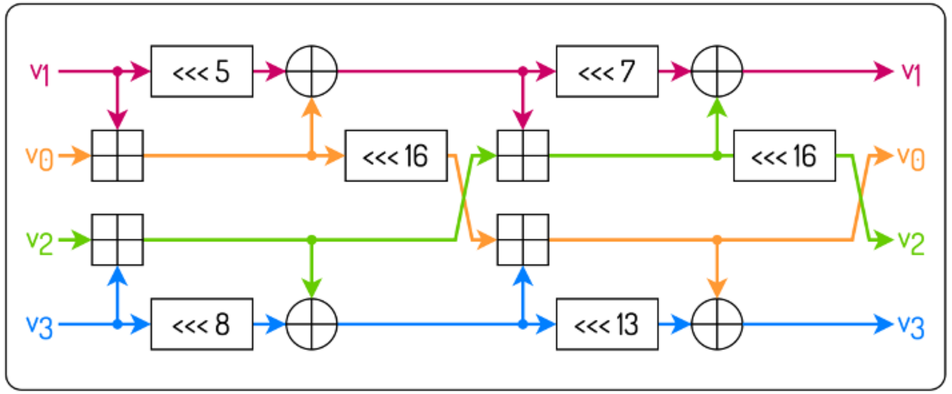
Position in Chaskey's Algorithm



P4Chaskey Control Flow

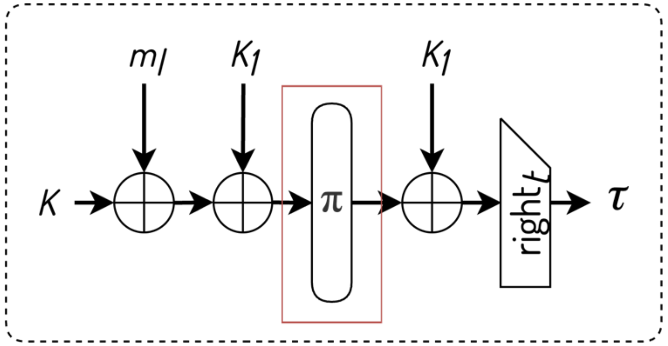
Current Round: 4





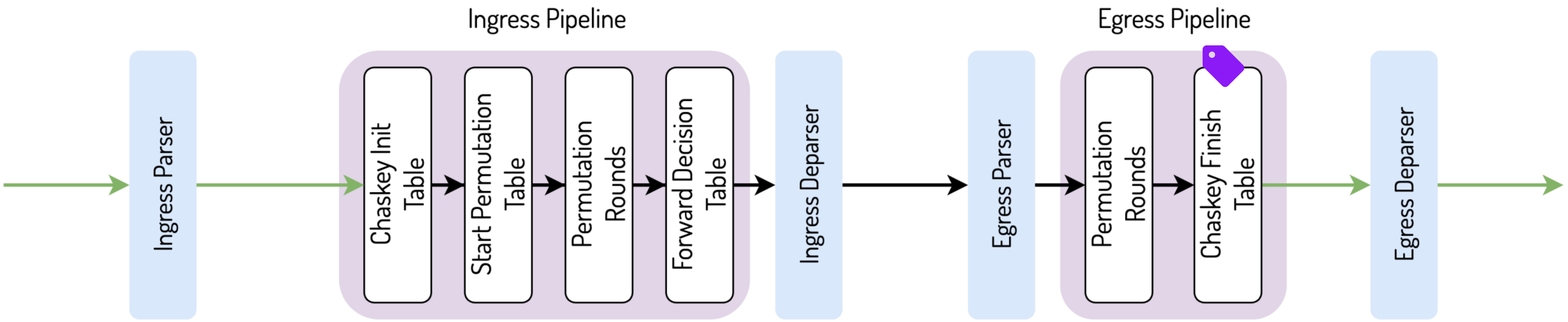
X 4

Position in Chaskey's Algorithm



P4Chaskey Control Flow

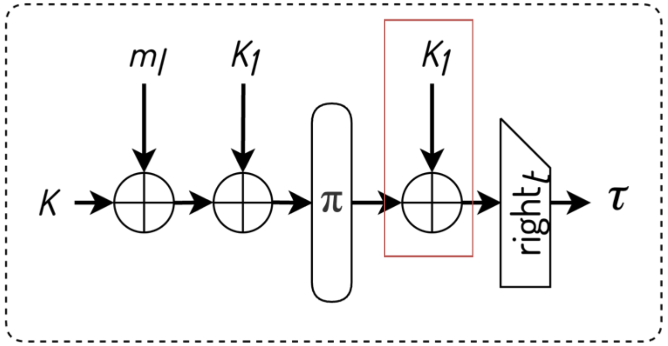
Current Round: 4



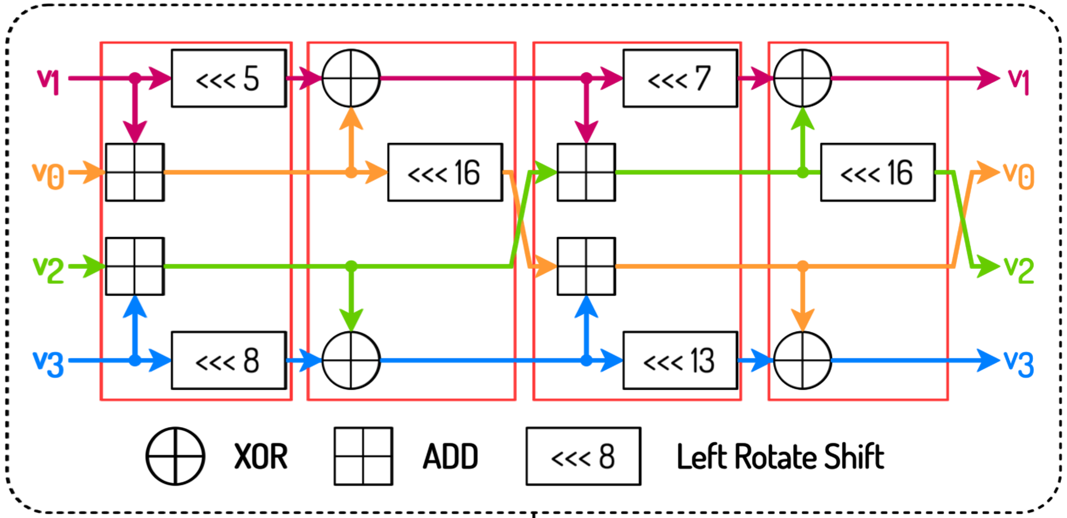
Chaskey Finish Table

Current Round	Operation
4	Final XOR Operation ($v \oplus k_1$)

Position in Chaskey's Algorithm



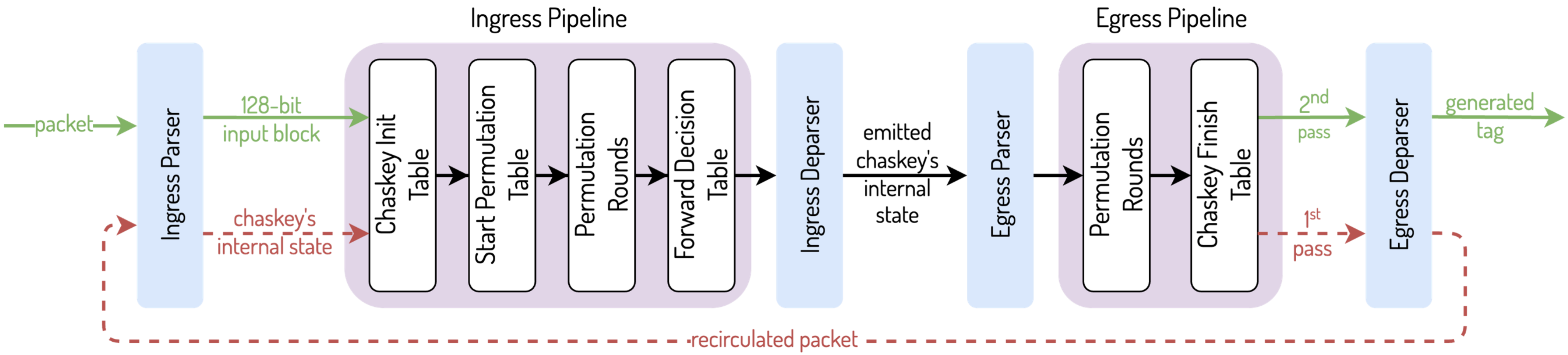
P4Chaskey Permutation Round



Group 1	Group 2	Group 3	Group 4
v1 <<<= 5 v0 += v1 v2 += v3 v3 <<<= 8	v1 ⊕= v0 v0 <<<= 16 v3 ⊕= v2	v1 <<<= 7 v2 += v1 v0 += v3 v3 <<<= 13	v1 ⊕= v2 v2 <<<= 16 v3 ⊕= v0

Stage 1	Stage 2	Stage 3	Stage 4
a1 = v1 <<< 5 a0 = v0 + v1 a2 = v2 + v3 a3 = v3 <<< 8	b1 = a1 ⊕ a0 b0 = a0 <<< 16 b3 = a3 ⊕ a2 b2 = a2	a1 = b1 <<< 7 a2 = b2 + b1 a0 = b0 + b3 a3 = b3 <<< 13	v1 = a1 ⊕ a2 v2 = a2 <<< 16 v3 = a3 ⊕ v0 v0 = a0

P4Chaskey Operation on Tofino 1



How did we evaluate P4Chaskey?

Evaluation Targets

P4Chaskey correctness was assessed by using the results obtained with Chaskey's C implementation[1].

Our evaluation has two main targets:

- Demonstrating that our design and P4 implementation of Chaskey for PISA is the first that enables computing a MAC using a 128-bit key without packet recirculation.
- Measuring the resource usage of P4Chaskey on the target switch platforms.

[1] https://mouha.be/wp-content/uploads/chaskey12.c

Comparison Against State-of-the-art Solutions

Number of pipeline passes for a 128-bit input message

Target	Algorithm	Key Size (Bits)	Block/Message Size (Bits)	Pipeline Passes
Tofino 1	HalfSipHash[1]	64	32	5
	Chaskey	128	128	2
Tofino 2	SipHash[2]	128	64	2
	AES - CMAC[3]	128	128	2
	Chaskey	128	128	1 ✓

[1] Sophia Yoo, Xiaoqi Chen. 2021. Secure Keyed Hashing on Programmable Switches;

[2] Yutaro Yoshinaka, Mio Kochiyama, Yuki Koizumi, Junji Takemasa, Toru Hasegawa. 2024. A Lightweight Anonymity Protocol at Terabit Speeds on Programmable Switches;

[3] Lars-Christian Schulz, Robin Wehner, David Hausheer. 2023. Cryptographic Path Validation for SCION in P4.

Resource usage: Tofino 1 & Tofino 2

Resource Type	Tofino 1	Tofino 2
Number of Stages	10/12	18/20
Action Data Bus Bytes	9,5%	9,5%
VLIW Instructions	8,1%	8,4%
Exact Match Input Xbar	8,6%	10,2%
Gateway	13%	15,6%
Hash Distribution Units	66,7%	80%
Logical Table ID	35,4%	41,3%
PHV Allocation	≤40%	≥40%
SRAM	0,7%	0,4%
TCAM	0%	0%

<= Pipeline Length

Moderate control flow logic

Almost no memory used

Integrating P4Chaskey With Other P4 Programs

In our public repository on github, we have provided an example of using P4Chaskey as a control block into a generic P4 program.

- Small reflector program that verifies IPv6 addresses before forwarding.

We are currently integrating P4Chaskey into the desing of a SCION border router in P4 that includes some of the EPIC[1] security extensions.

[1] Markus Legner, Tobias Klenze, Marc Wyss, Christoph Sprenger, Adrian Perrig. 2020. EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet.

Conclusion

We presented P4Chaskey, the first data plane implementation of a MAC algorithm for PISA that:

- Uses 128-bit security.
- It executes in a single pipeline pass (Tofino 2) for inputs up to 128-bits.

Our evaluation has shown that:

- It requires fewer pipeline passes than state-of-the-art implementations.
- Its resource usage allows for other data plane functionality to be executed in parallel.