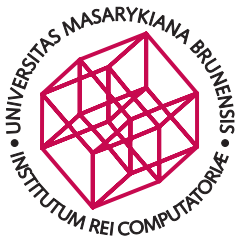
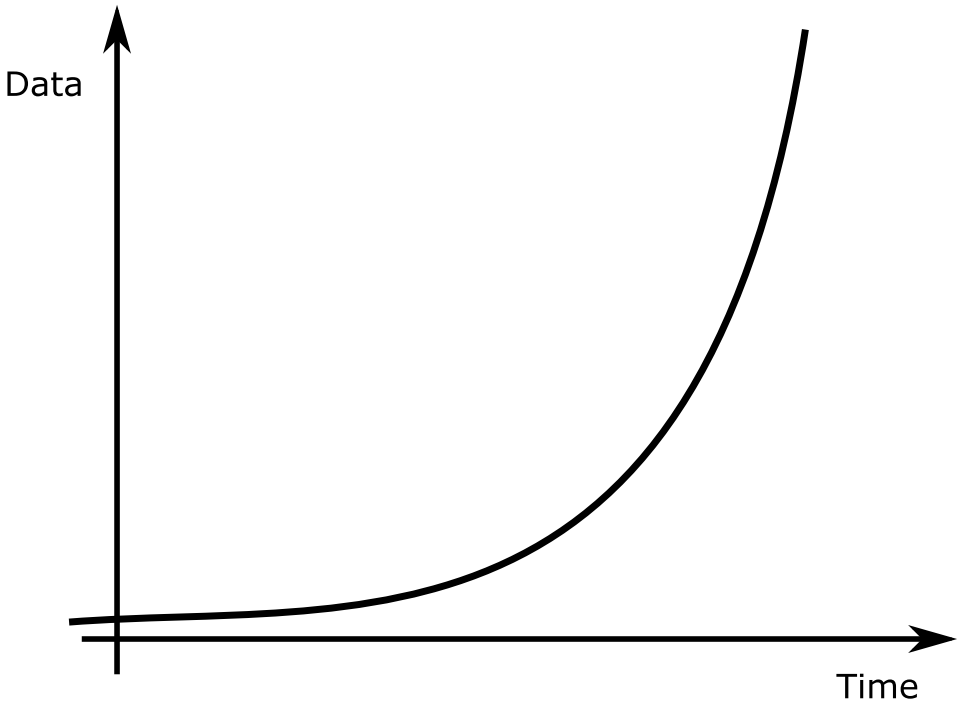
Enhancing Intrusion Detection by Correlation of Modularly Hashed Sketches



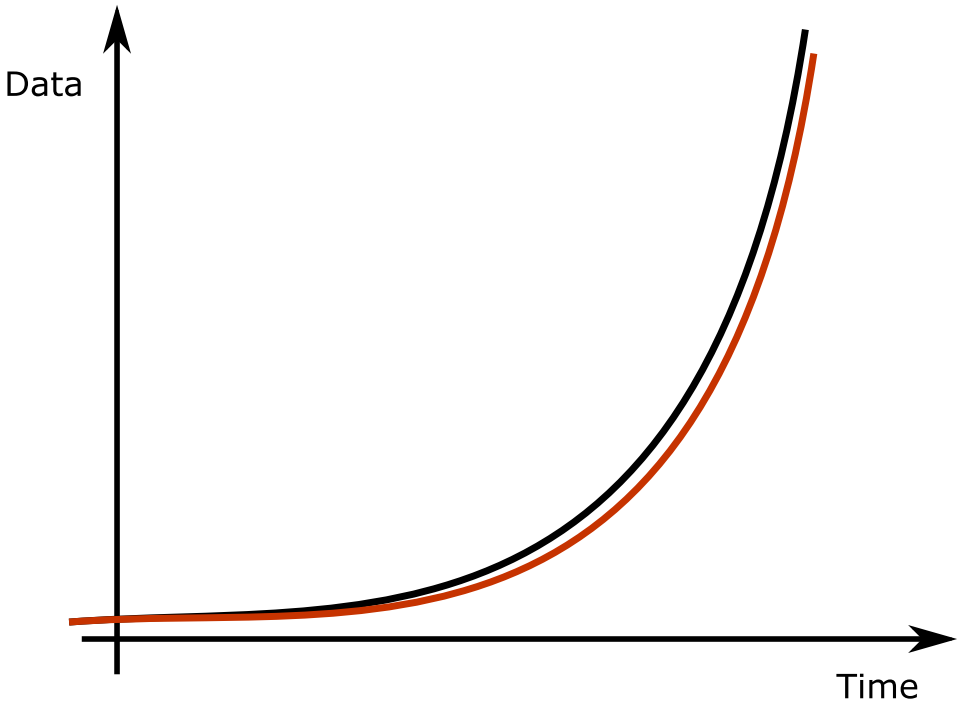
Jirsík Tomáš, Drašar Martin, Vizváry Martin

AIMS 2014, Brno, 3rd July 2014

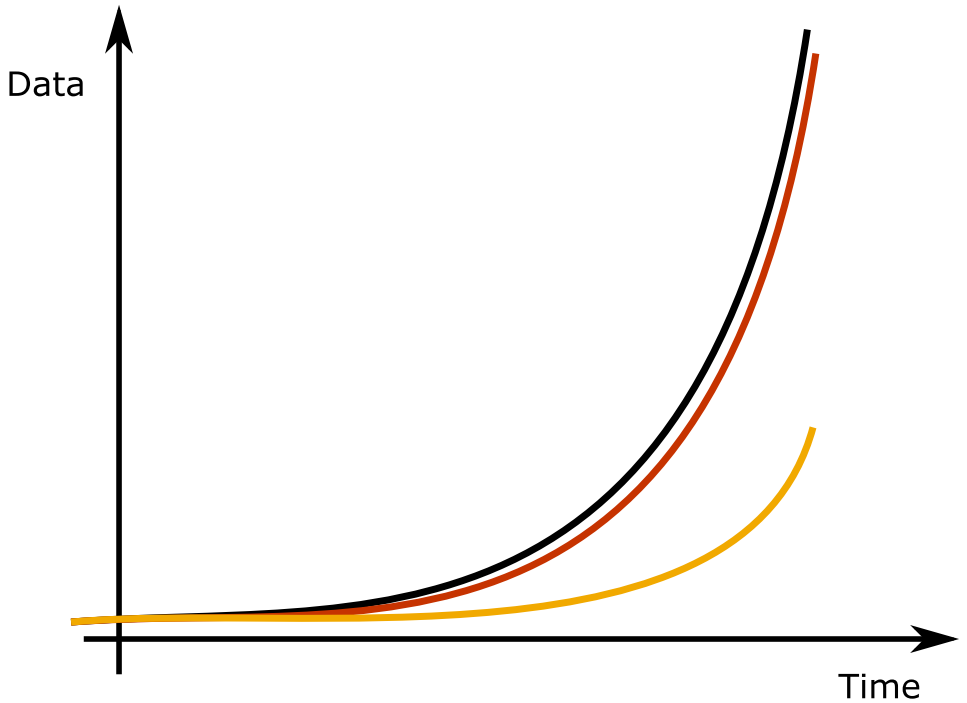
Network Traffic



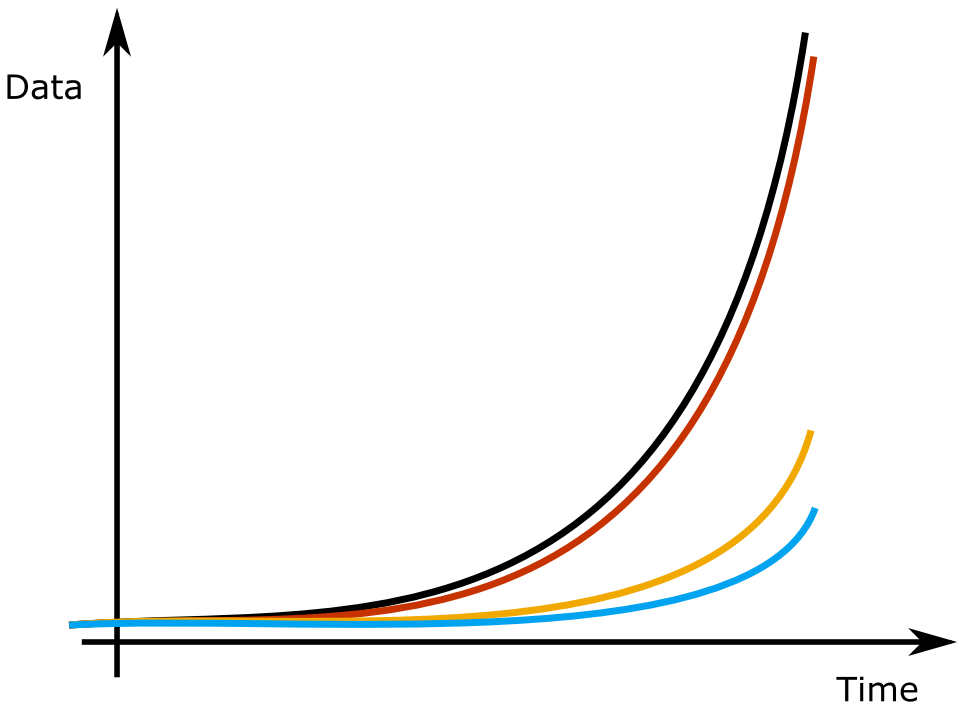
Network Traffic



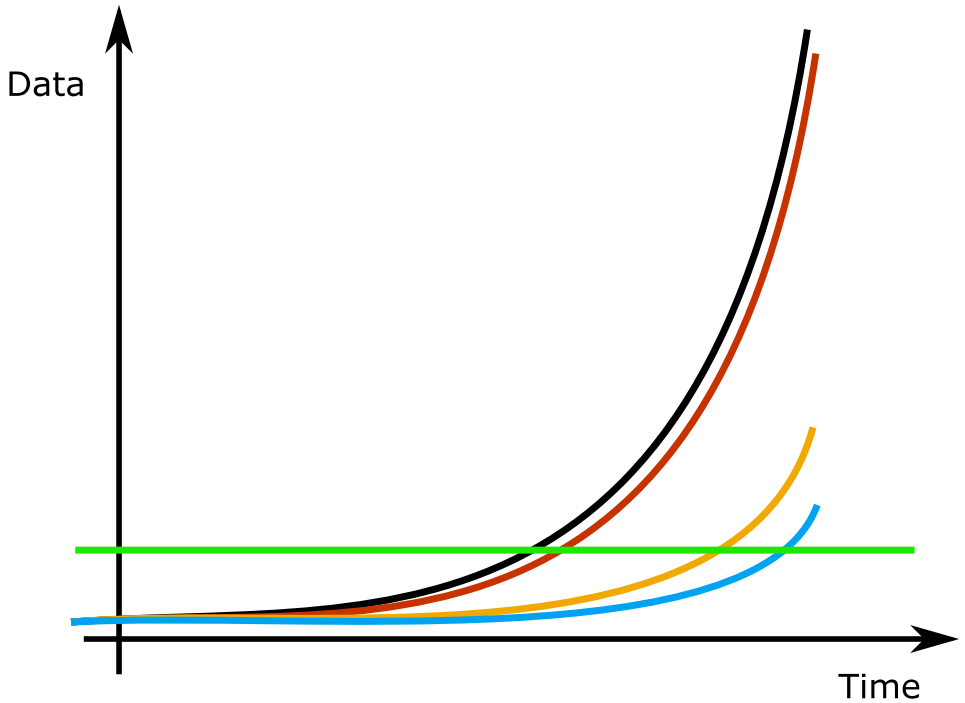
Network Traffic



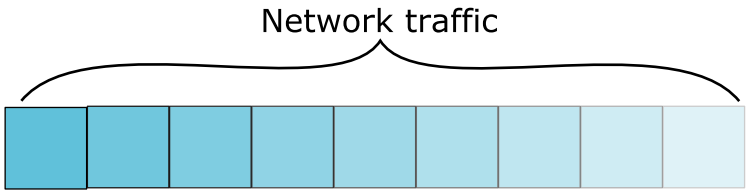
Network Traffic



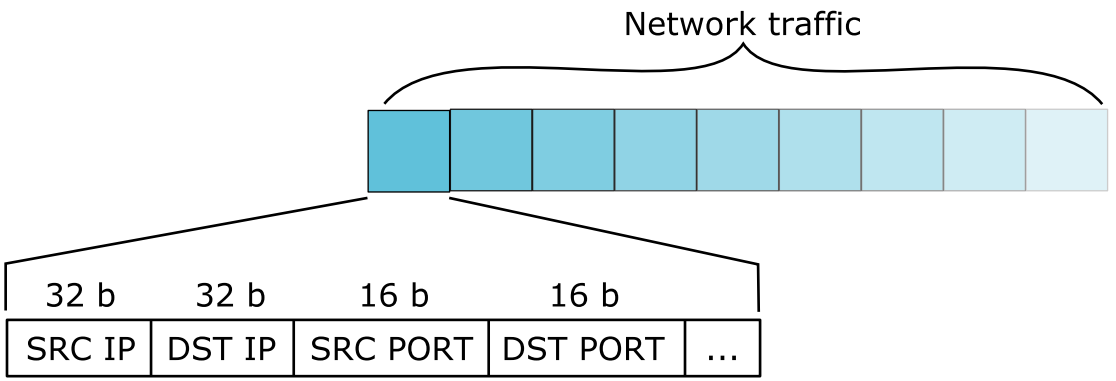
Network Traffic



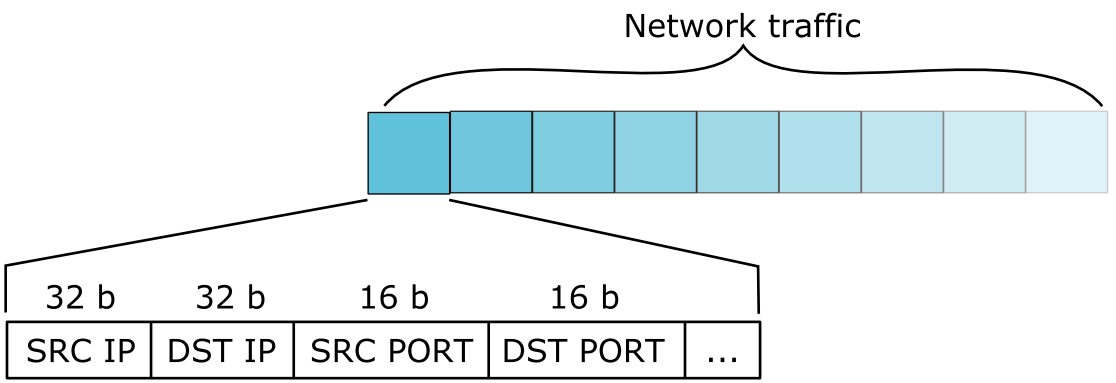
Sketch



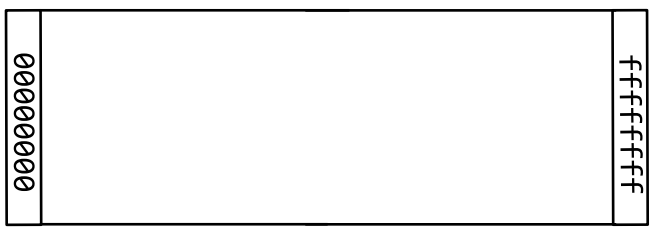
Sketch


Network traffic
32 b
32 b
16 b
16 b
SRC IP
DST IP
SRC PORT
DST PORT
...

Sketch

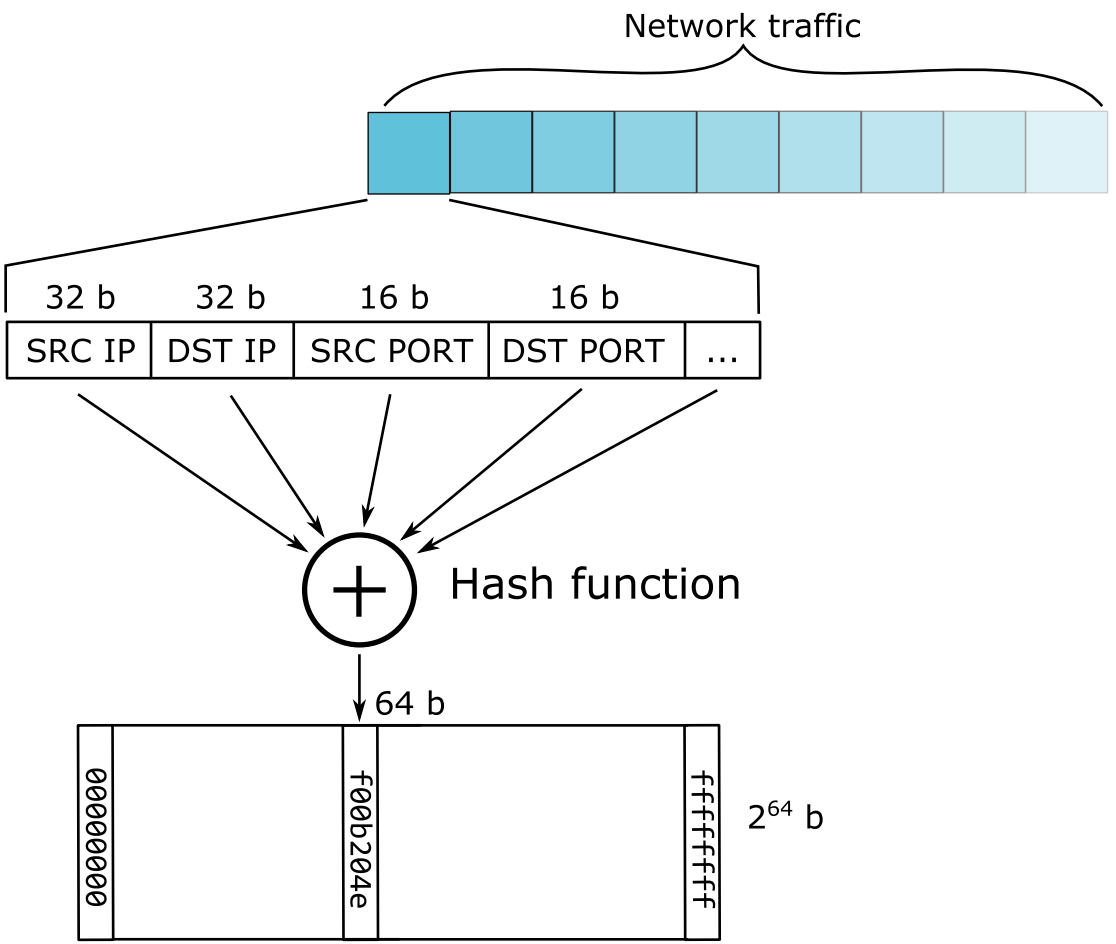


Hash function

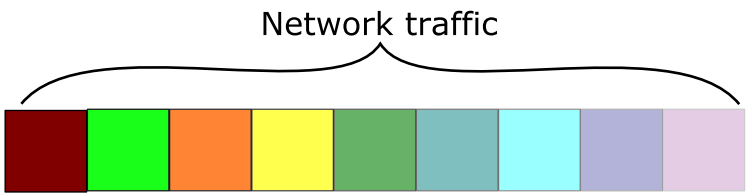


2^{64} b

Sketch

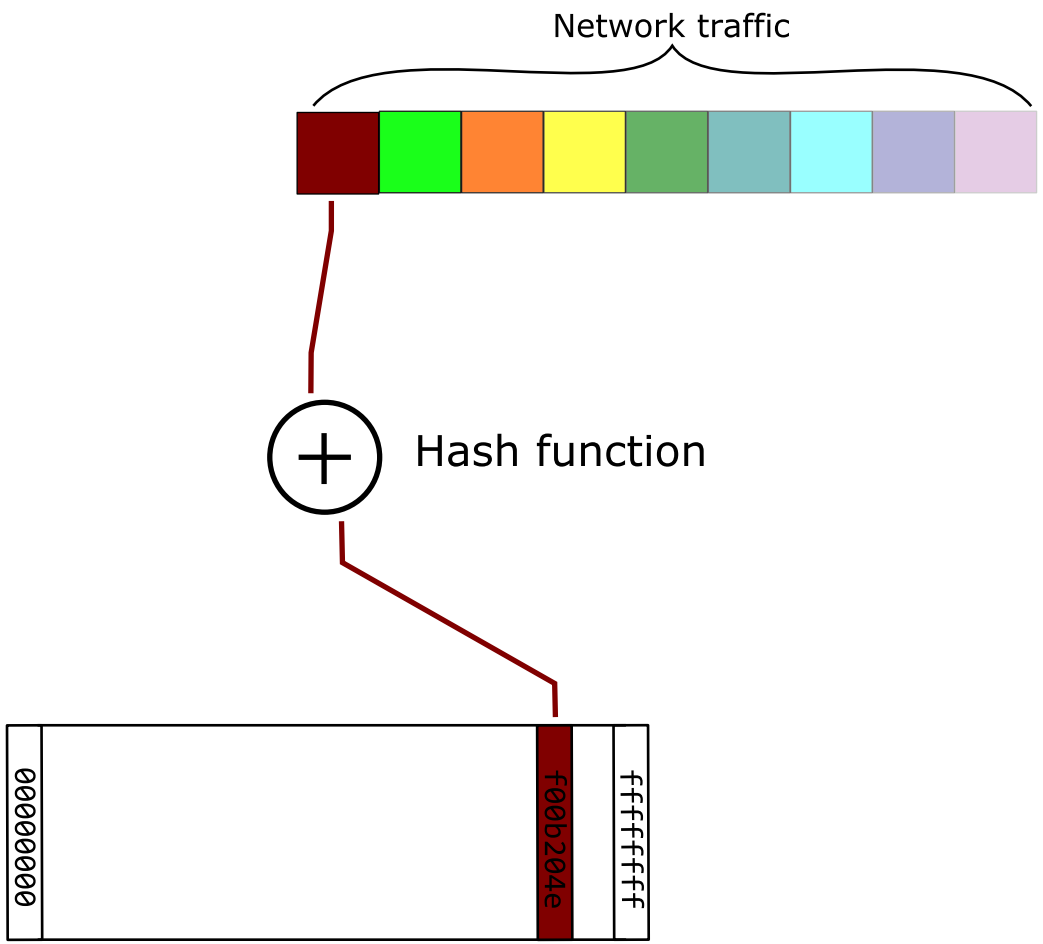

Network traffic
32 b
32 b
16 b
16 b
SRC IP
DST IP
SRC PORT
DST PORT
...
Hash function
64 b
00000000
f00b204e
ffffffff
2^{64} b

Sketch

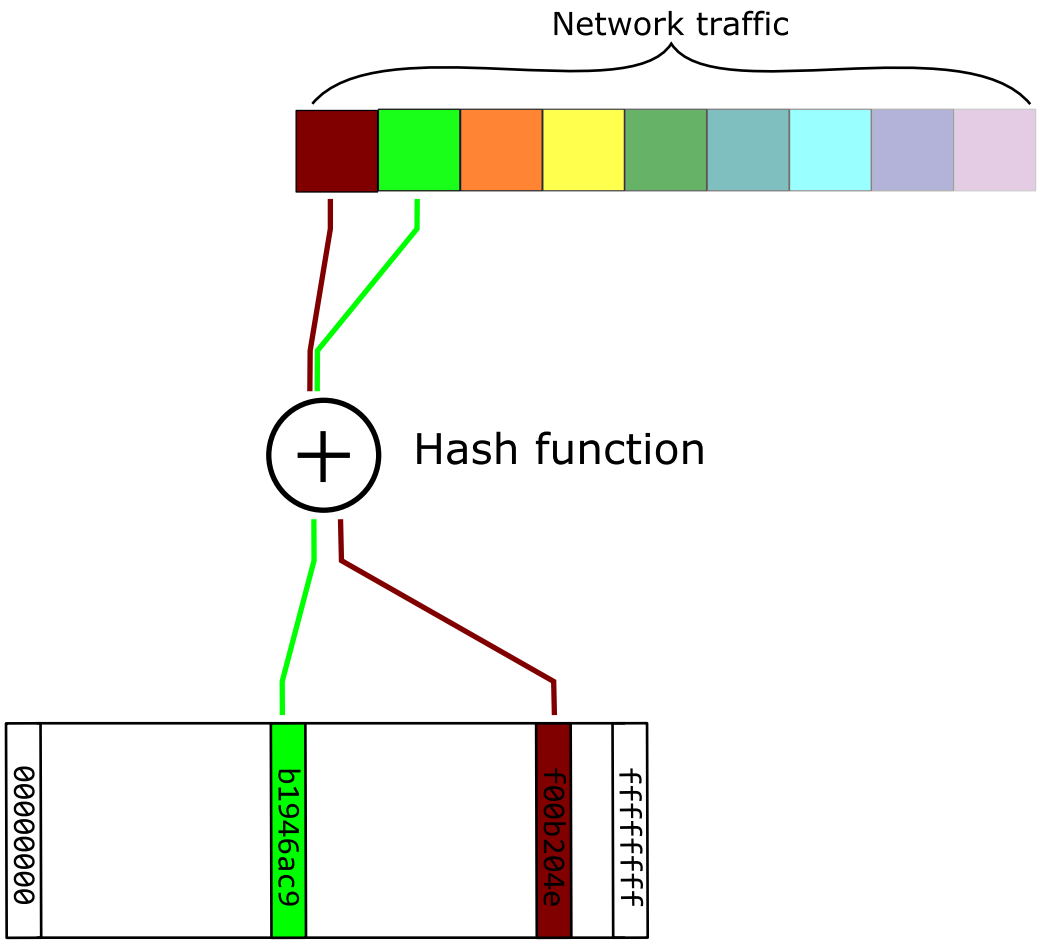


Hash function

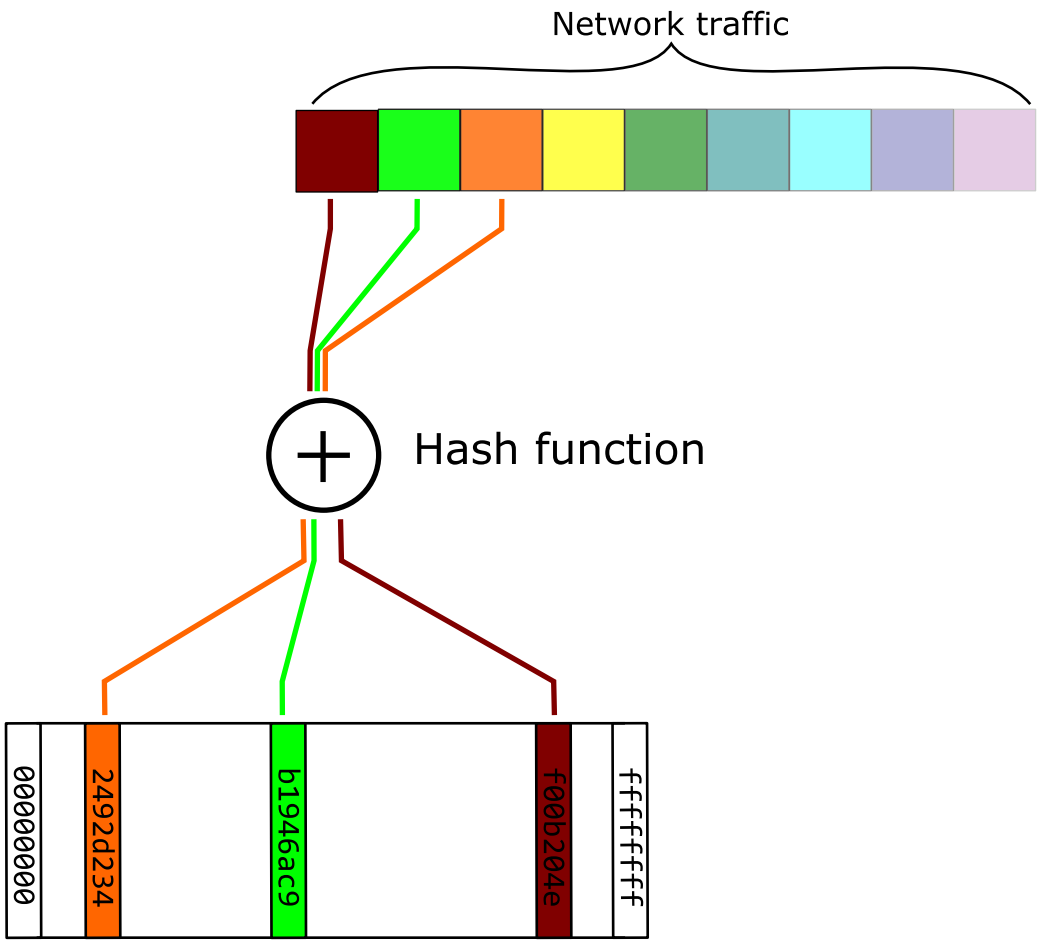
Sketch


Network traffic
Hash function
00000000
f00b204e
ffffffff

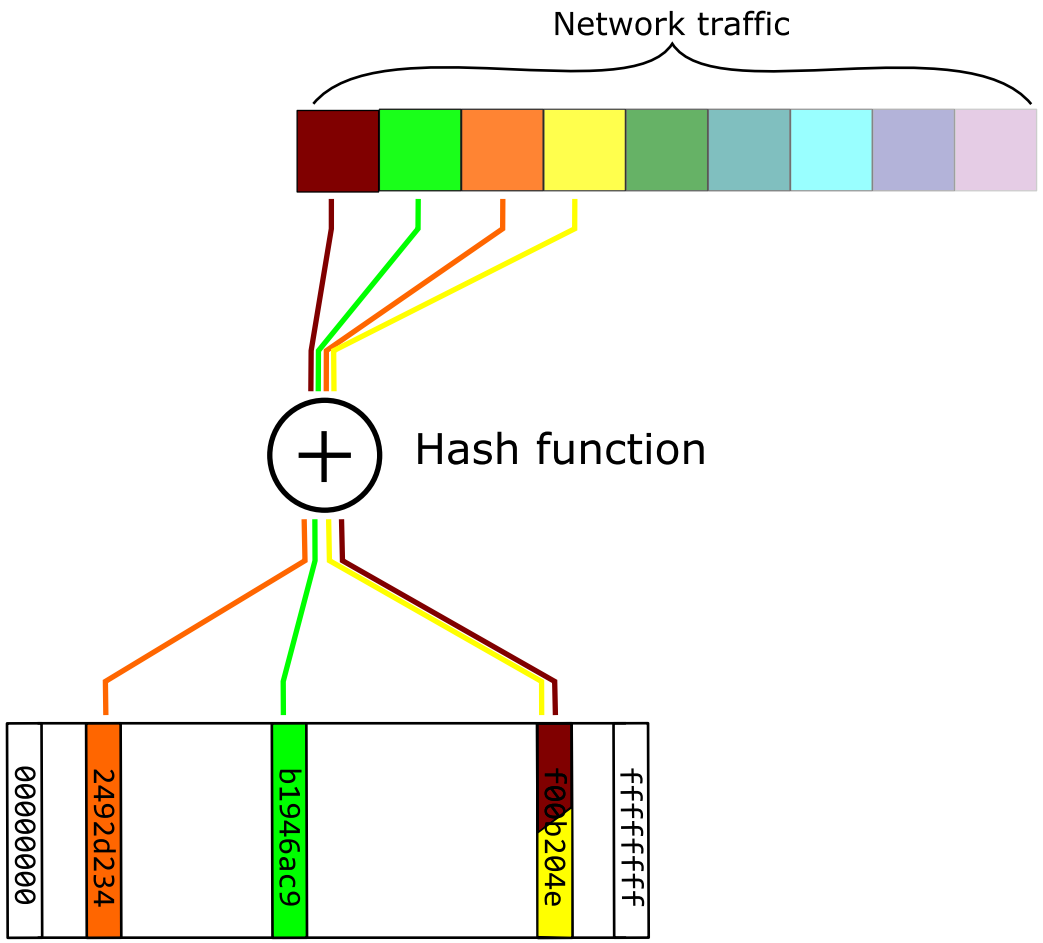
Sketch


Network traffic
Hash function
00000000
b1946ac9
f00b204e
ffffffff

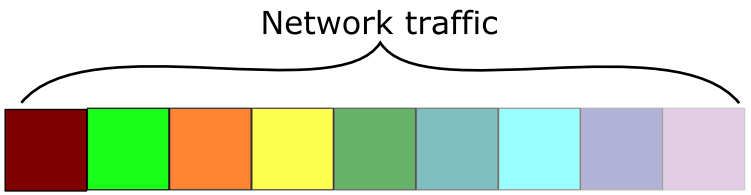
Sketch

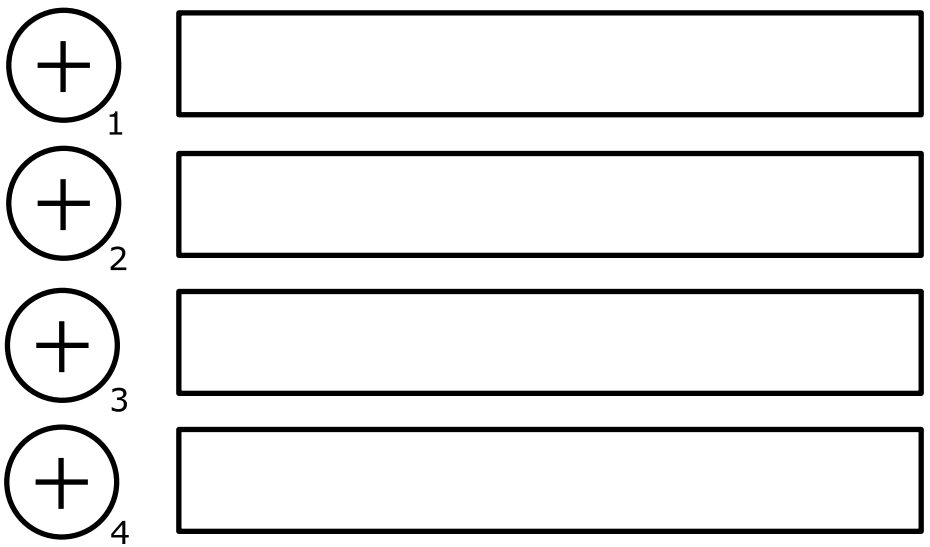

Network traffic
Hash function
00000000
2492d234
b1946ac9
f00b204e
ffffffff

Sketch

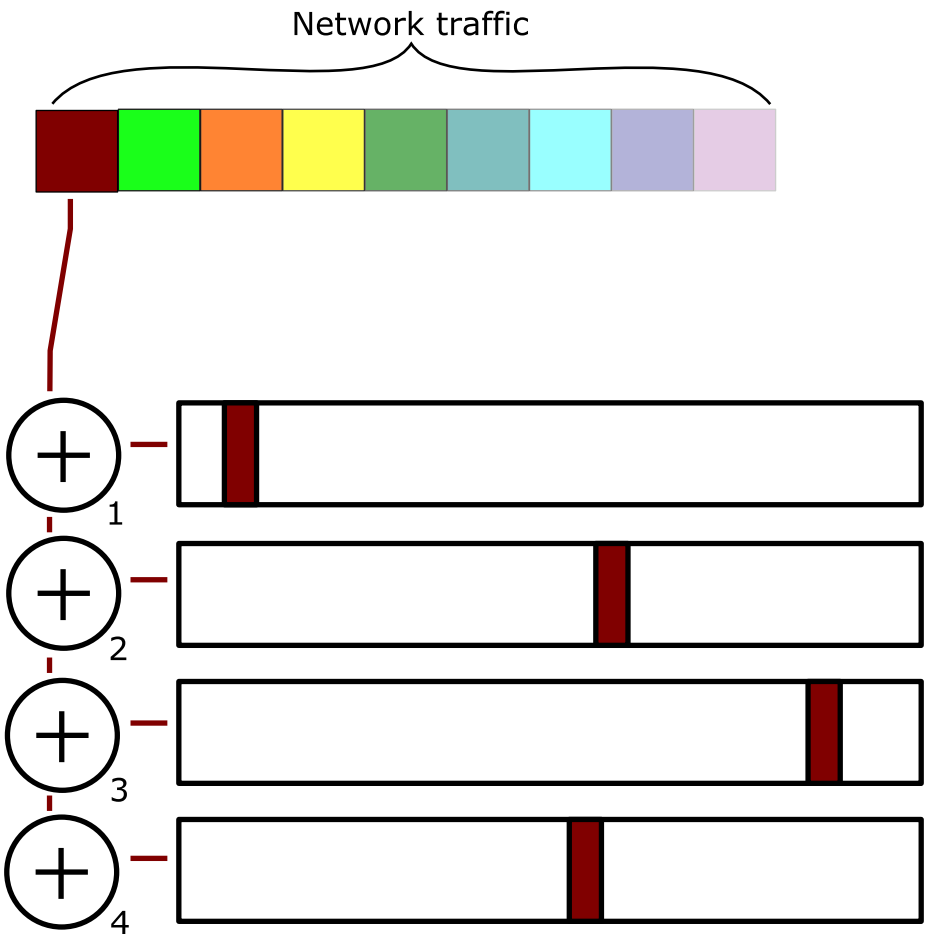

Network traffic
Hash function
00000000
2492d234
b1946ac9
f00b204e
ffffffff

Sketch

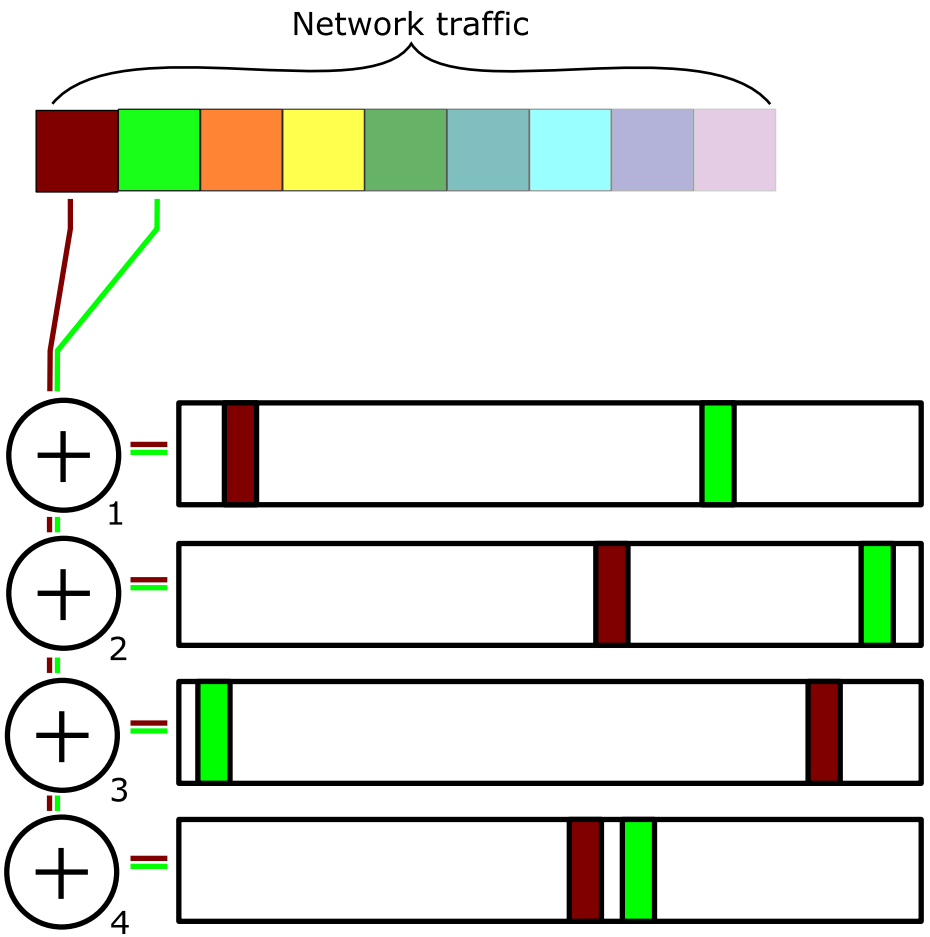




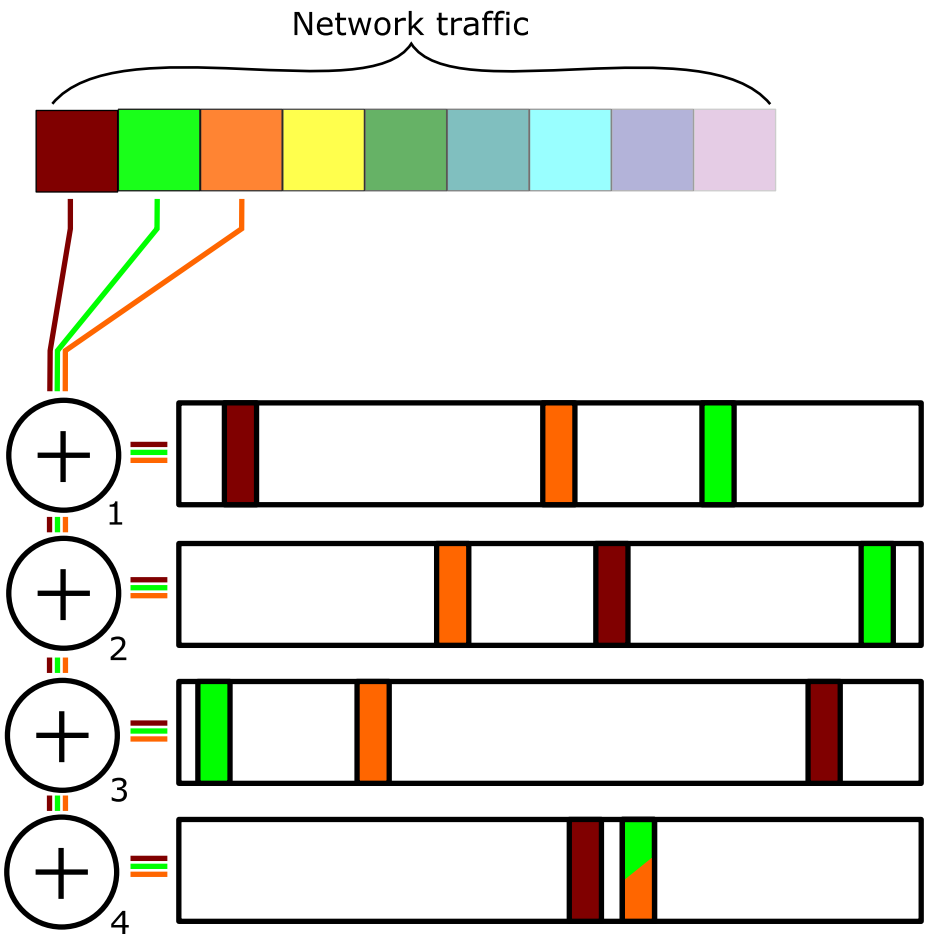
Sketch



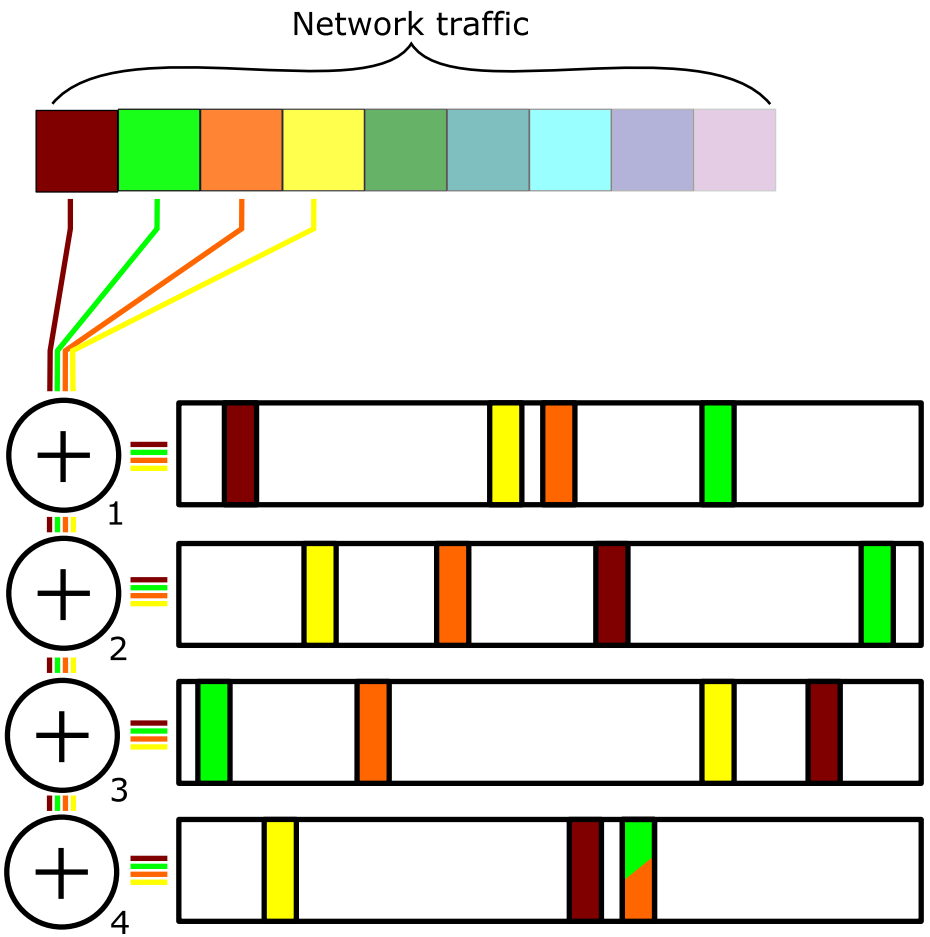
Sketch



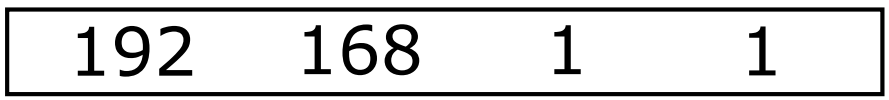
Sketch



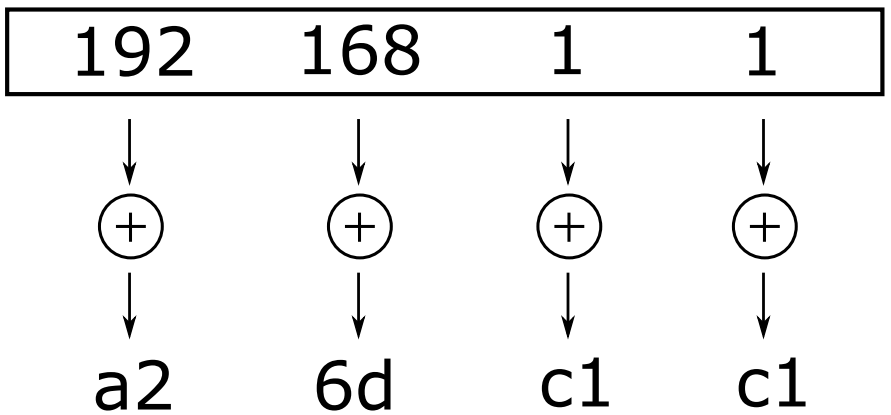
Sketch



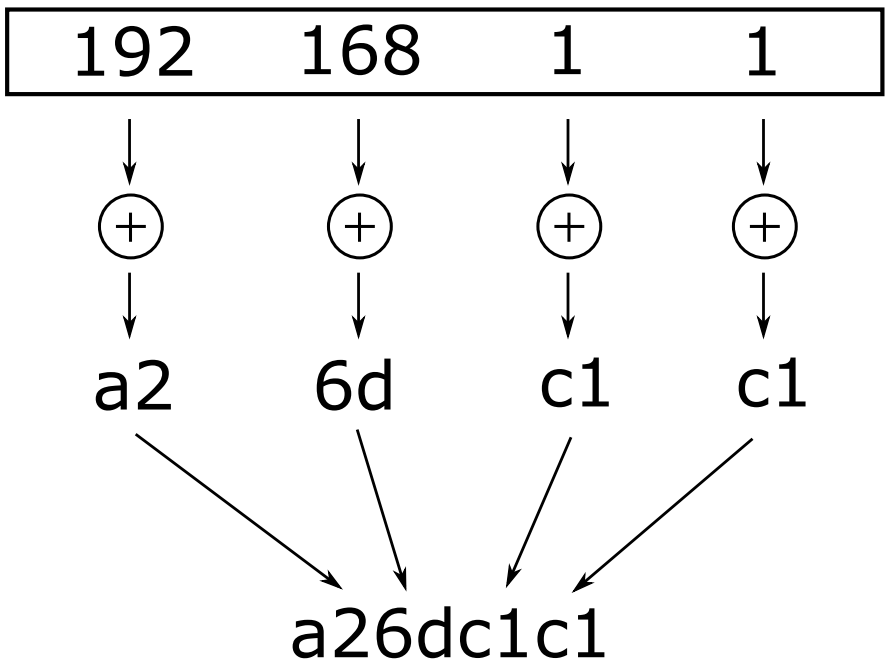
Modular Hashing



Modular Hashing

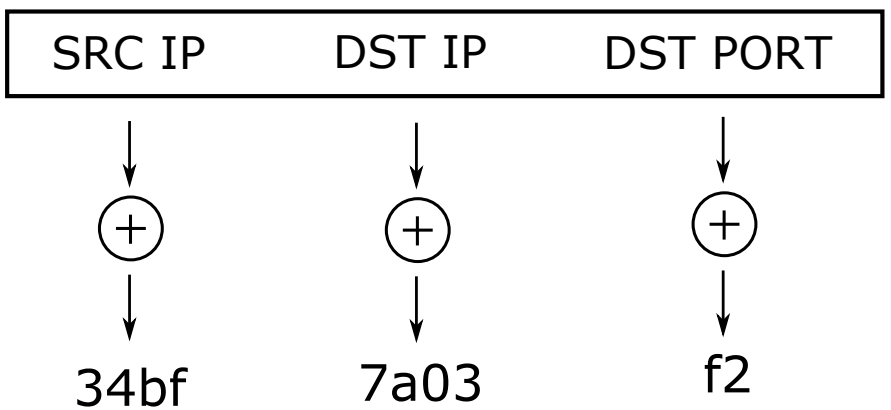


Modular Hashing

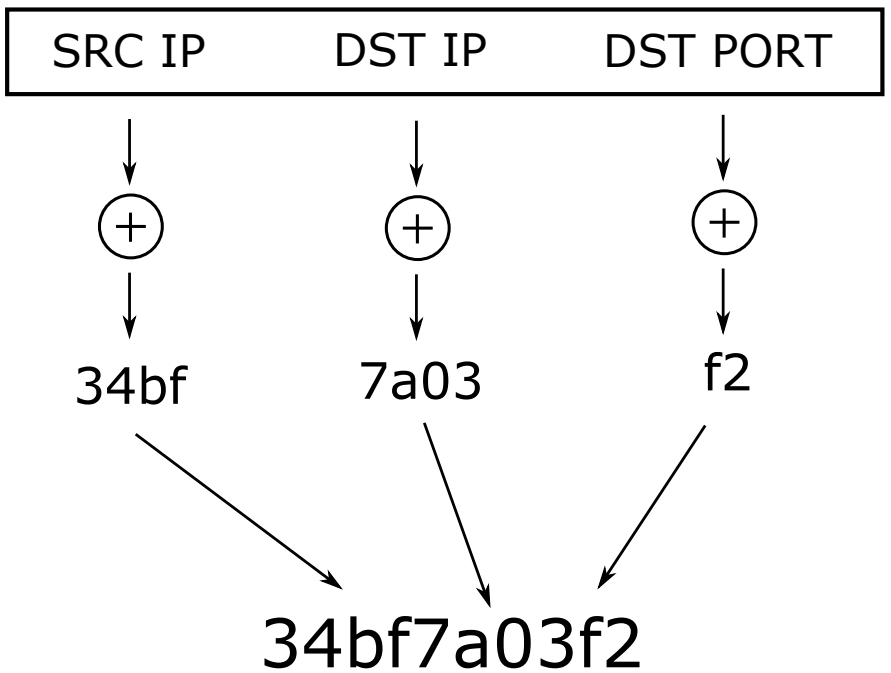


Modular Hashing

Modular Hashing

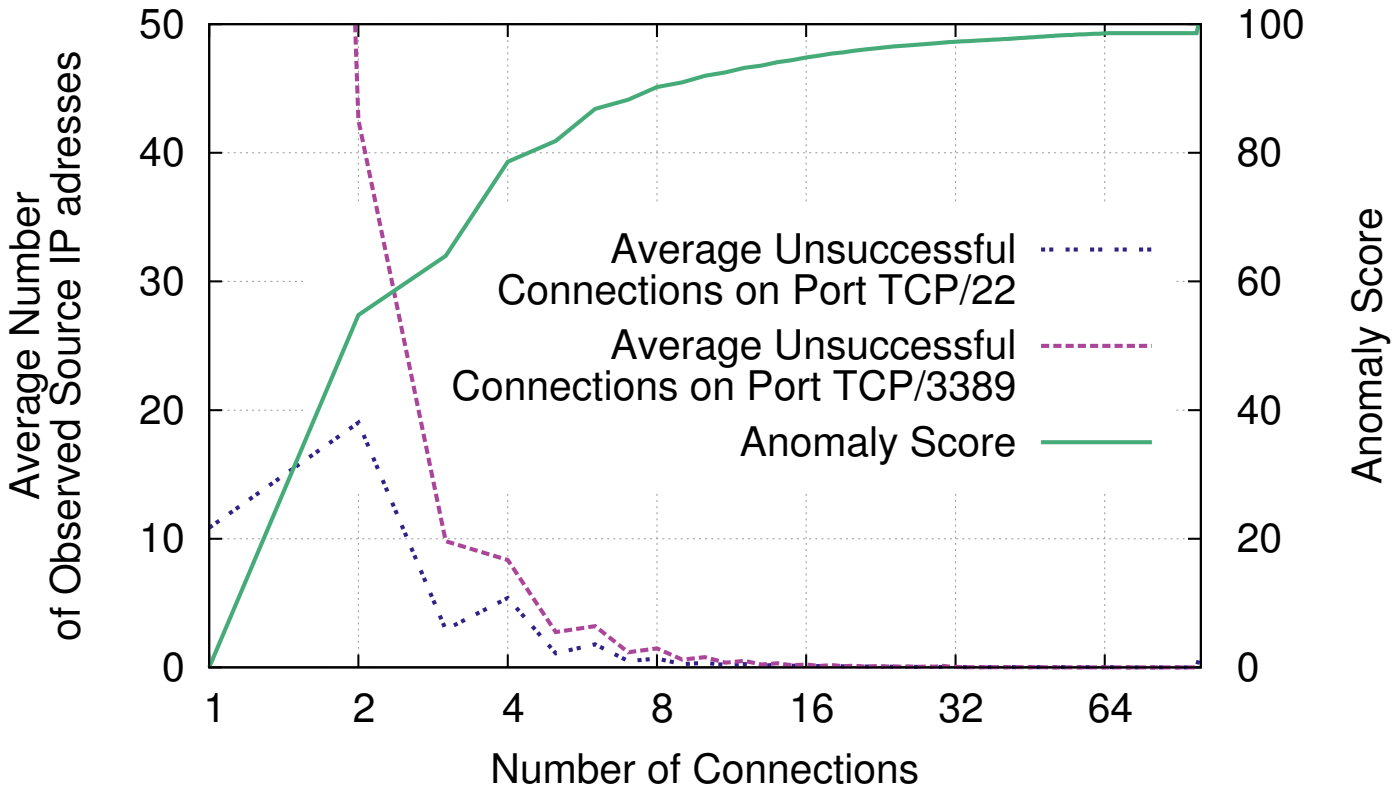


Modular Hashing



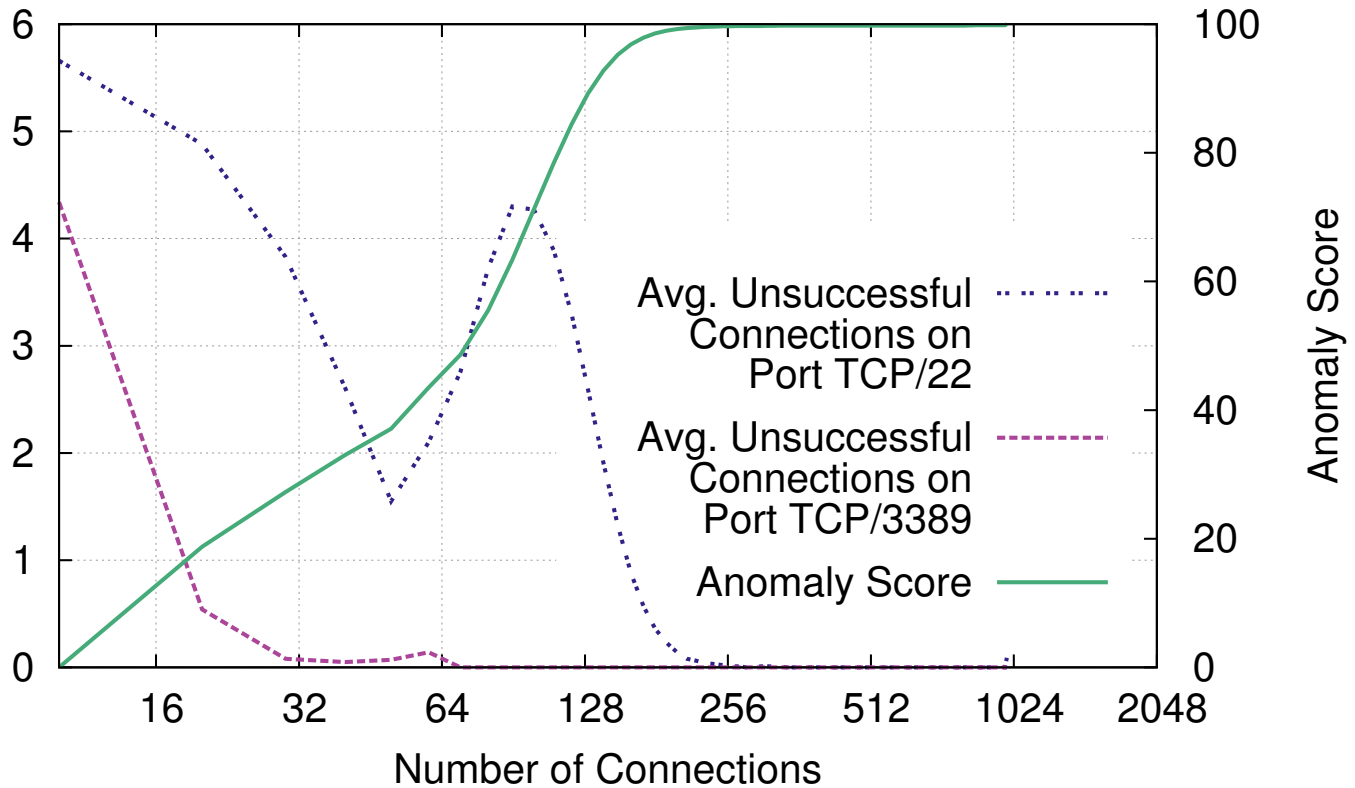
Partial detections

Source network scans



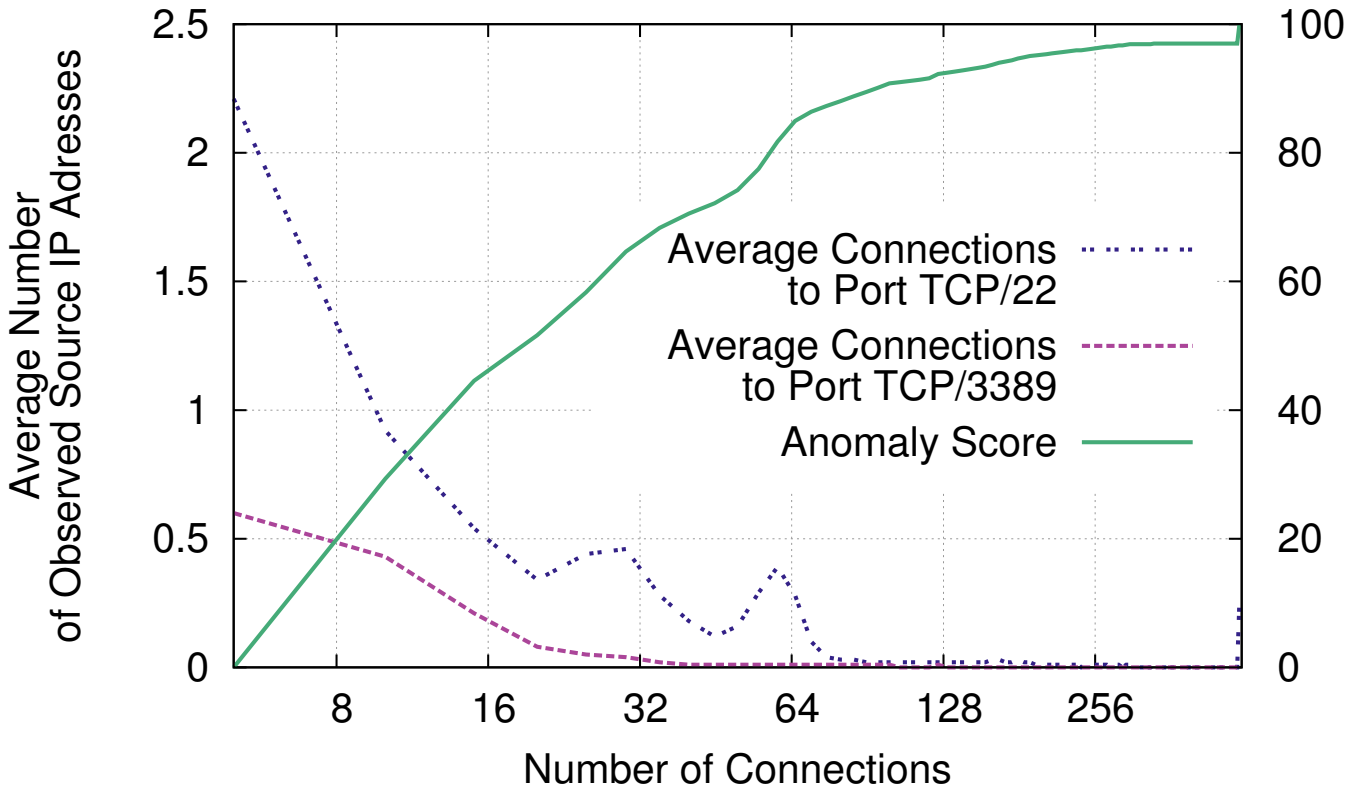
Partial detections

Destination network scans



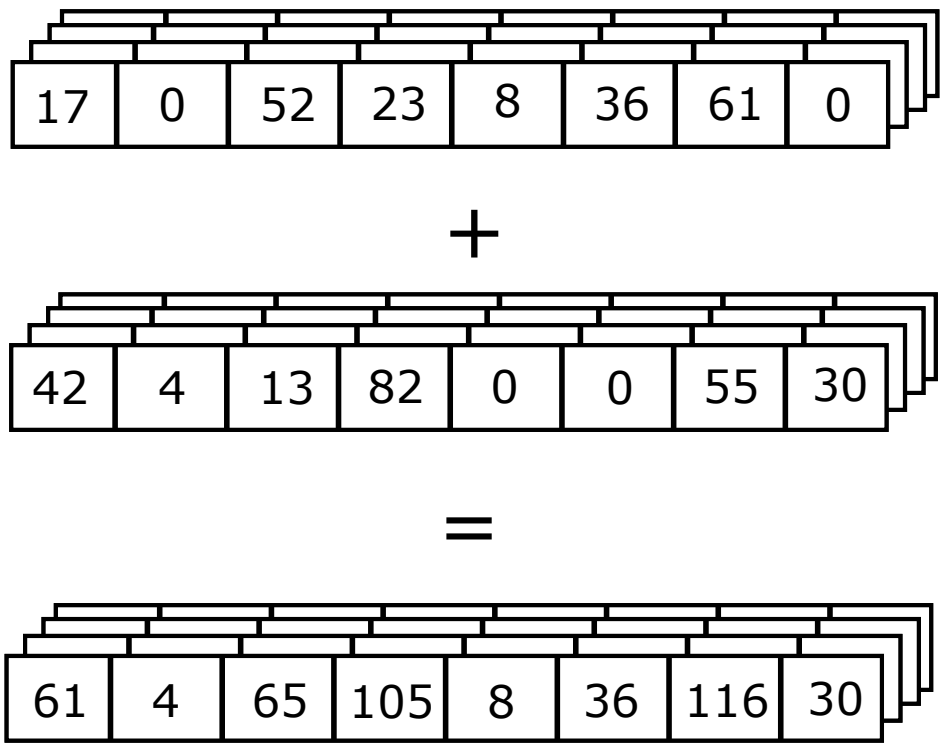
Partial detections

Number of connections



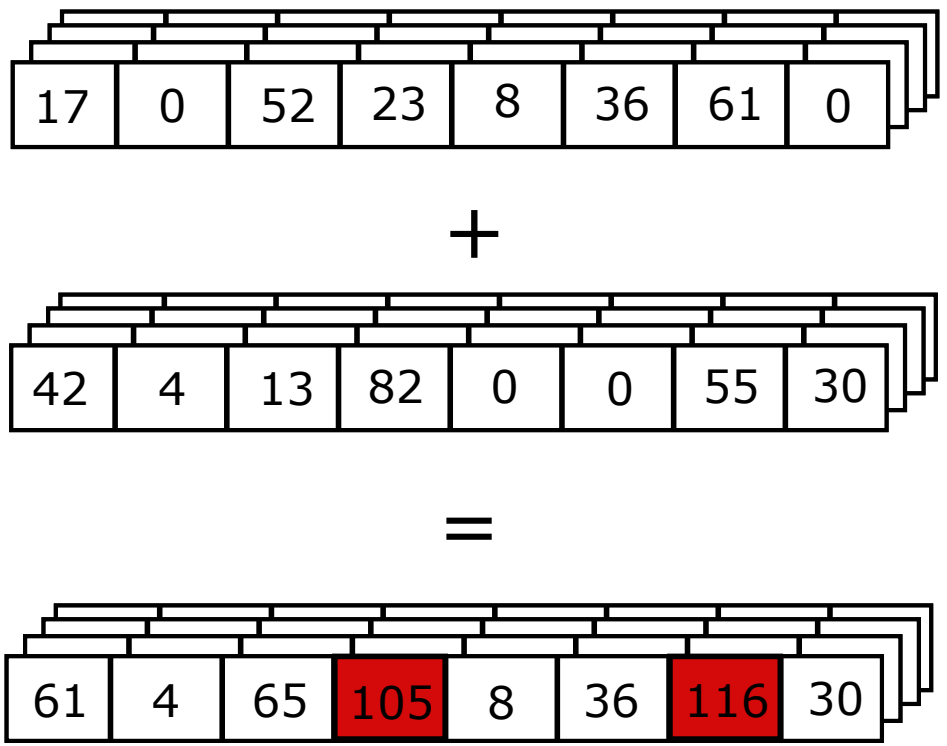
Detection algorithm

Accumulation phase



Detection algorithm

Analysis phase



Detection algorithm

Combination phase

SIP	DPORT	Value
A_1	B_1	X_1
A_1	B_2	X_2

$\oplus$

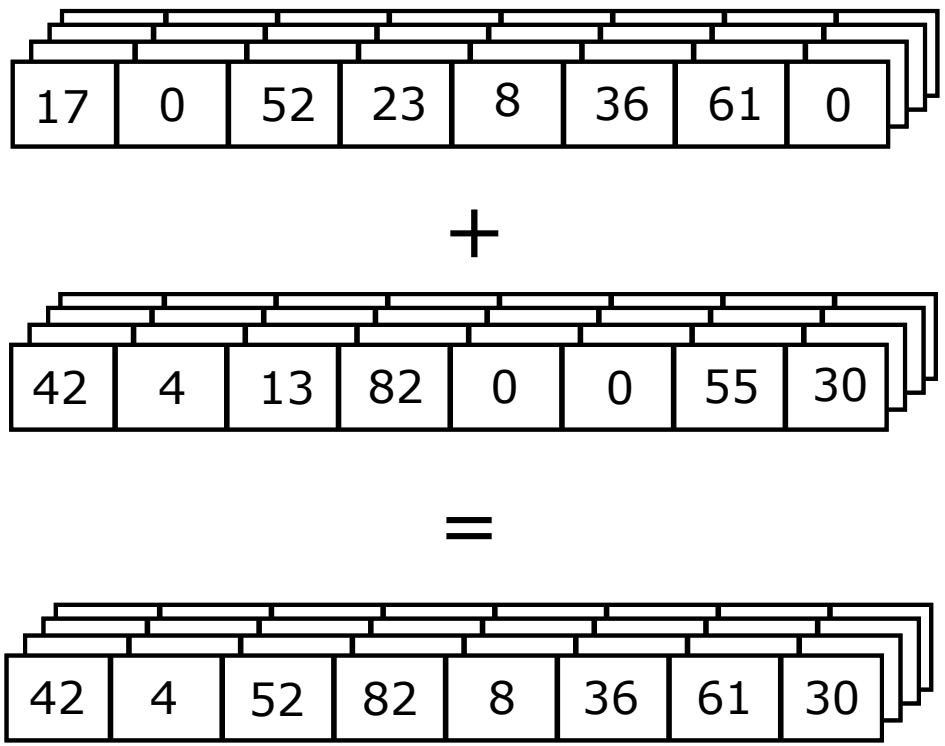
DPORT	DIP	Value
B_1	C_1	Y_1
B_1	C_2	Y_2

$=$

SIP	DIP	DPORT	Value
A_1	C_1	B_1	$X_1 + Y_1$
A_1	C_2	B_1	$X_1 + Y_2$

Detection algorithm

Aggregation phase



Evaluation

Anomalies	Connection	Accumulation	Combination	Reference methods
TCP/22	2679 (116)	10045 (264)	26408 (551)	(47)
TCP/3389	53 (20)	2175 (1079)	0	(878)

SNS	*Source Network Scan Detection*
DNS	*Destination Network Scan Detection*
Connection	*Abnormal Number of Connections Detection*
Variance	*Low Traffic Variance Detection*
Accumulation	*Accumulation of* SNS, Connection, Variance
Combination	*Combination of* SNS, DNS, Connection, Variance

Summary

- Presented algorithm based on k-ary sketches is suitable tool for correlation of events with different dimensions.
- This algorithm performs better than reference methods deployed in production.
- It does not require much processing power and a constant amount of memory.

Thank you for your attention.
I'd be happy to answer your questions.

Jirsík Tomáš, Drašar Martin,
Vizváry Martin