Beyond $2^{c/2}$ Security in Sponge-Based Authenticated Encryption Modes

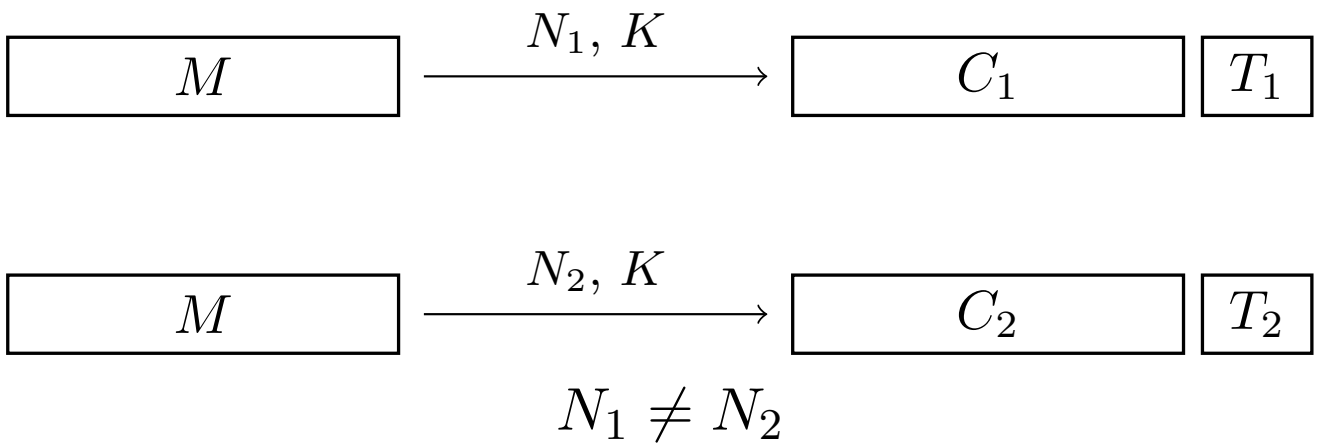
Philipp Jovanovic[1], Atul Luykx[2], and Bart Mennink[2]

[1] Universität Passau [2] KU Leuven

ASIACRYPT 2014 — December 8, 2014

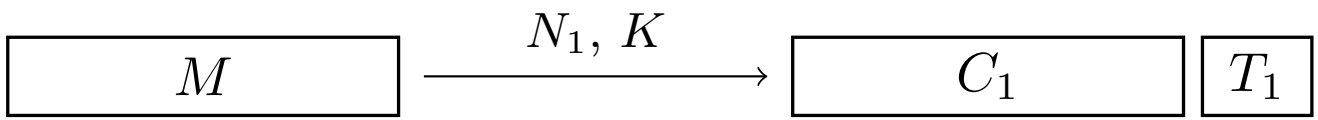
Authenticated Encryption

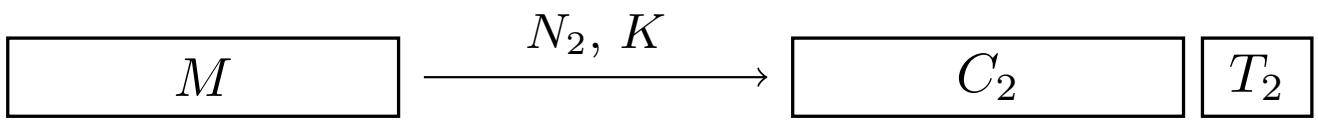
Encryption



Authenticated Encryption

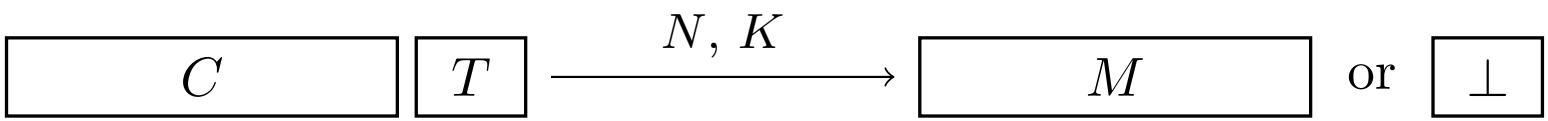
Encryption





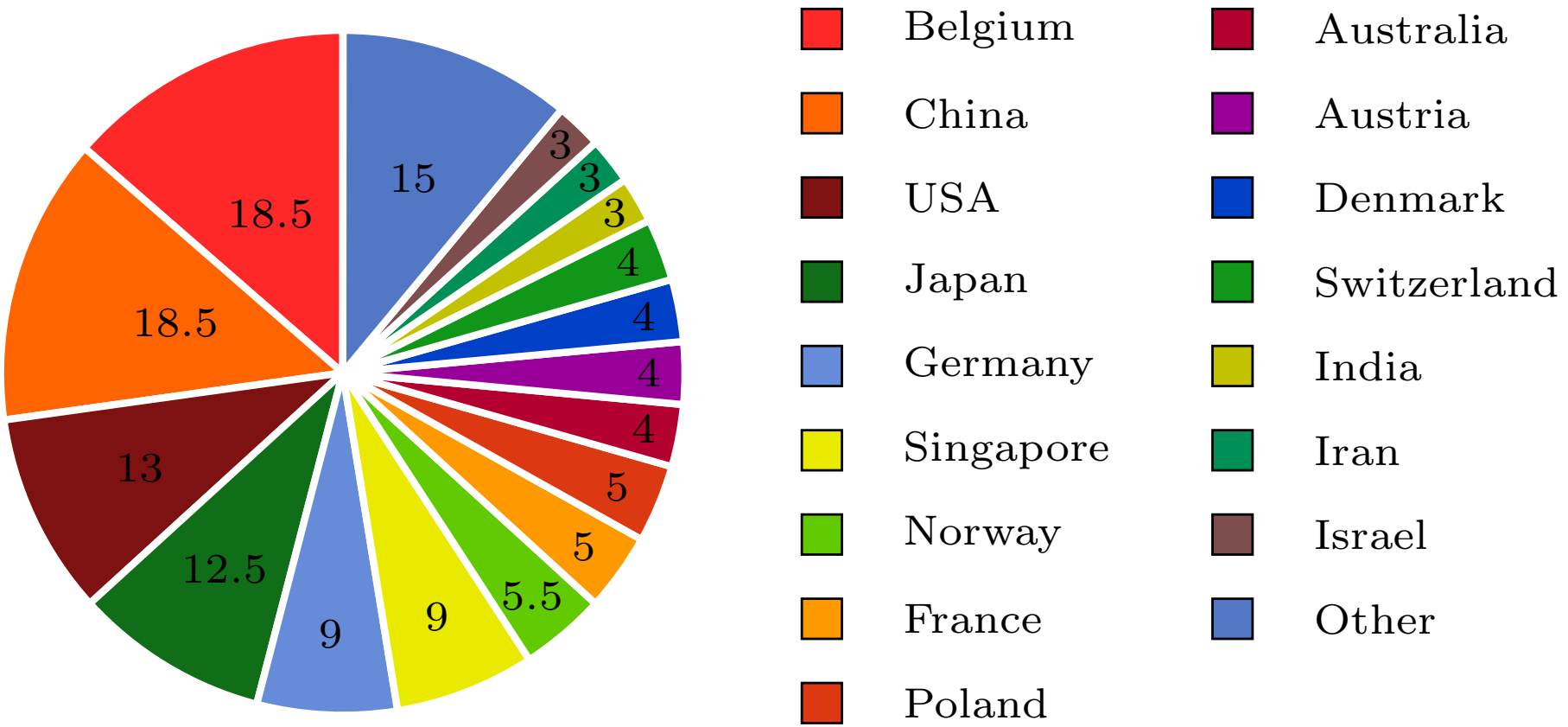
$N_1 \neq N_2$

Decryption



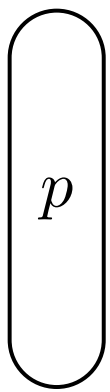
N free

Affiliations of CAESAR Submitters



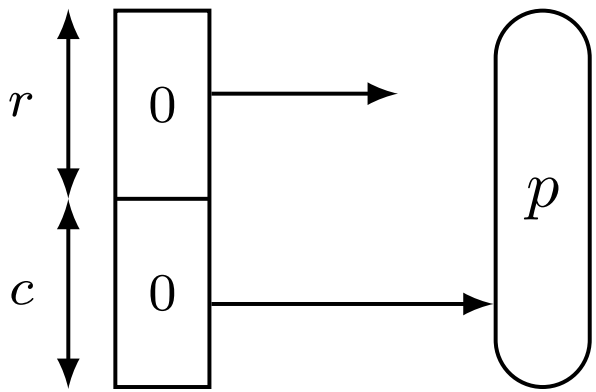
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)



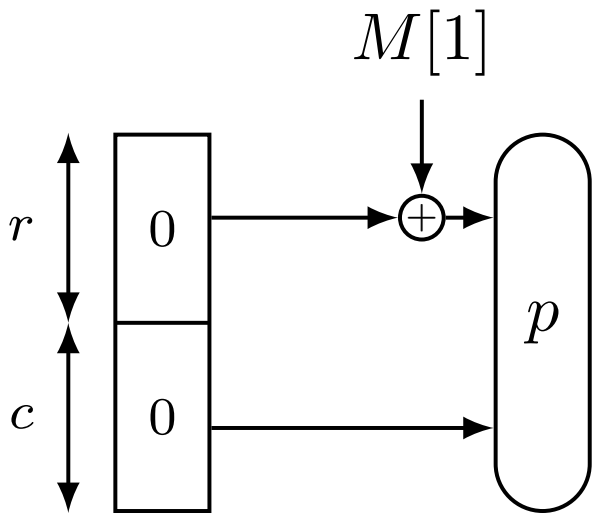
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)



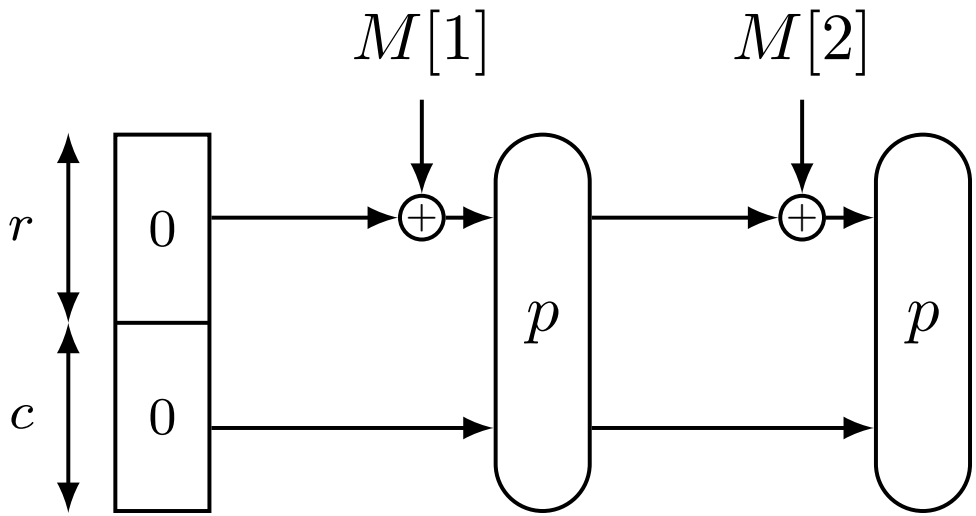
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)



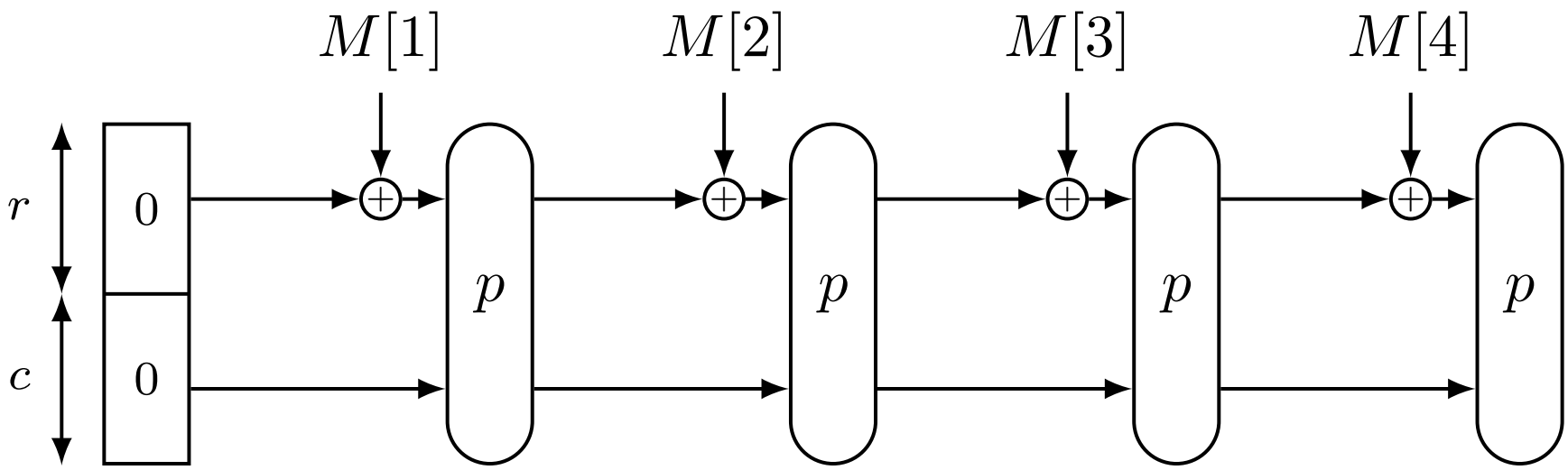
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)



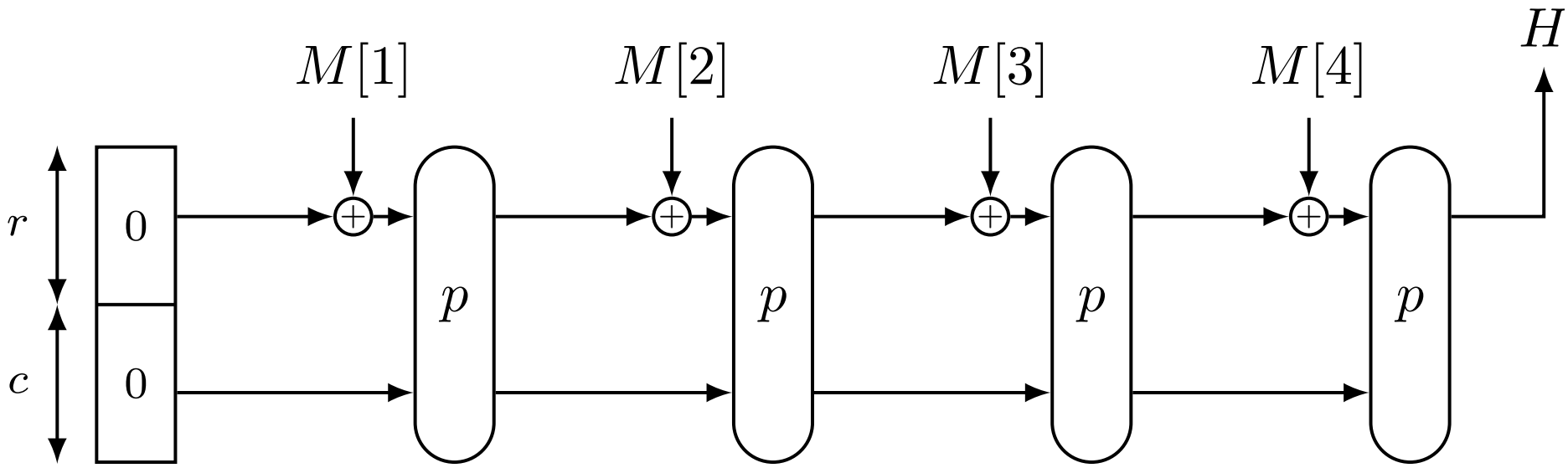
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)



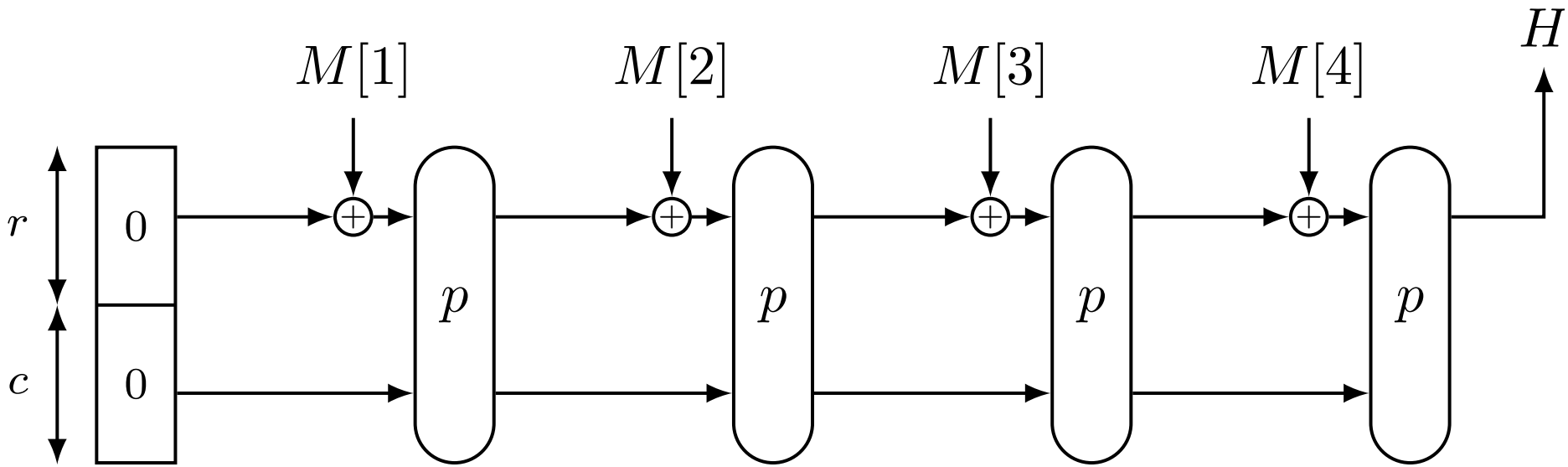
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)



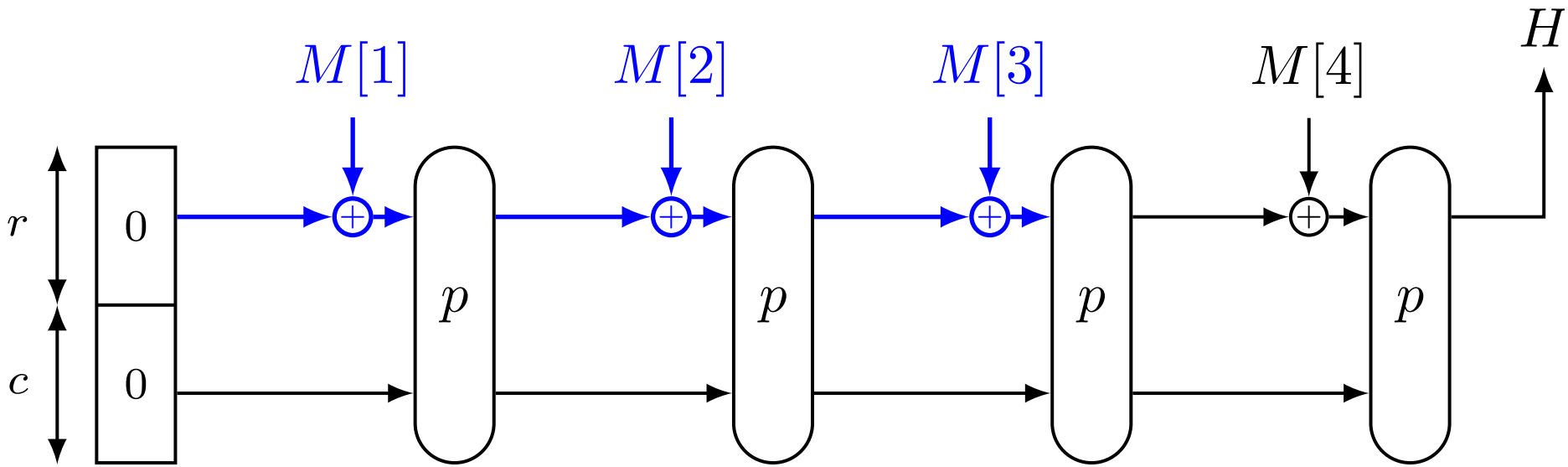
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)
- $2^{c/2}$ queries $\rightarrow$ $\frac{c}{2}$ bits security



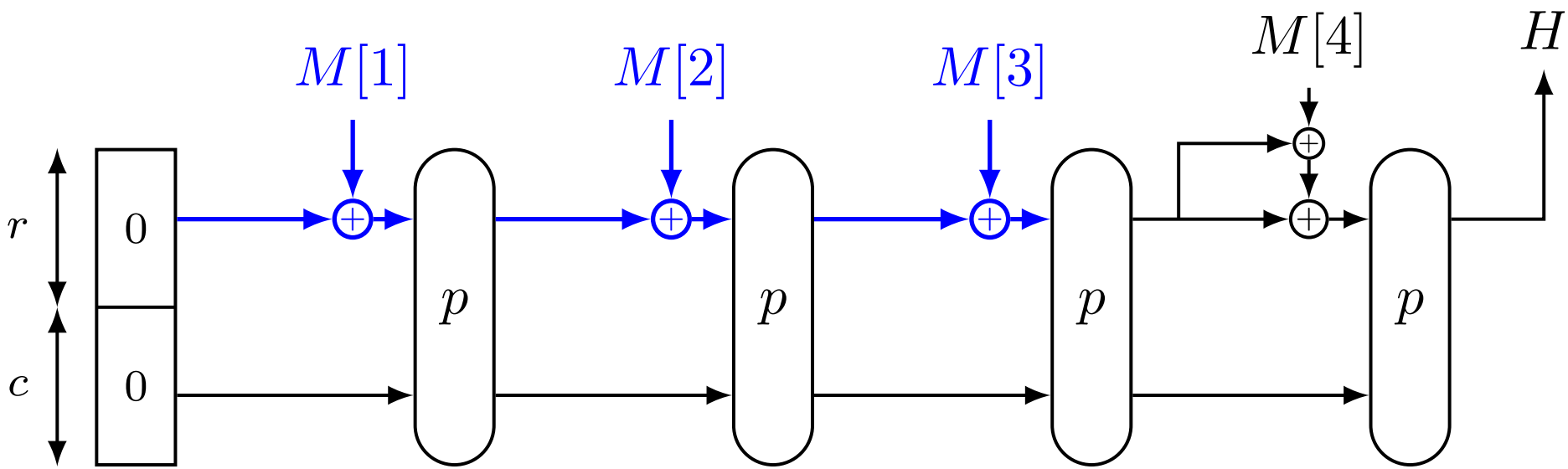
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)
- $2^{c/2}$ queries $\rightarrow$ $\frac{c}{2}$ bits security



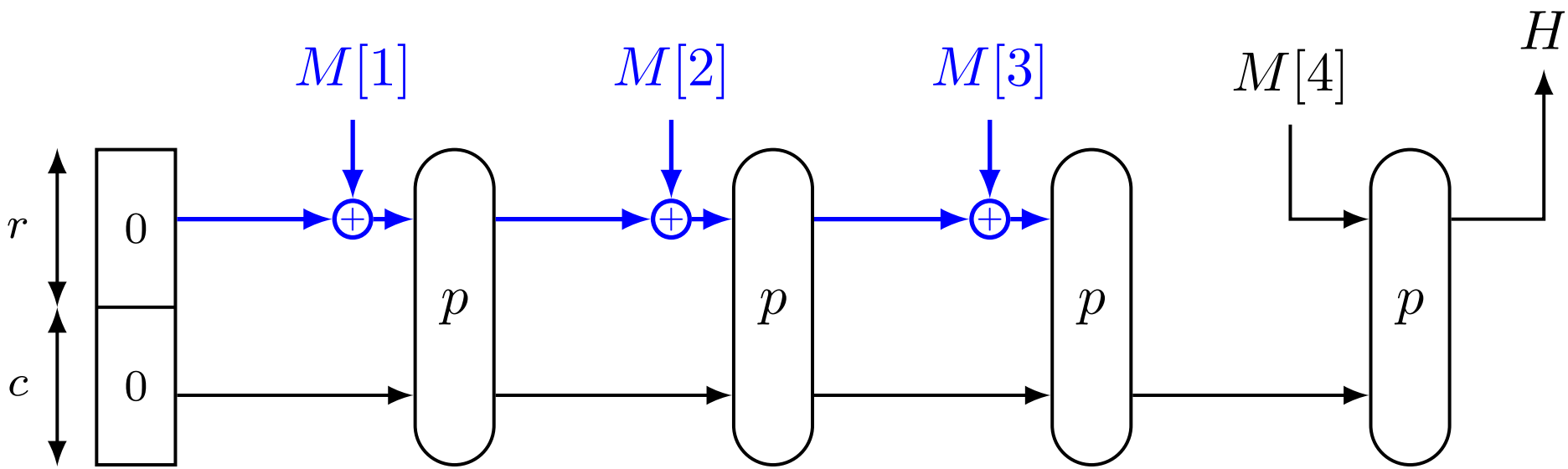
Sponge Functions

- Bertoni, Daemen, Peeters, and Van Assche (2007)
- $2^{c/2}$ queries $\rightarrow$ $\frac{c}{2}$ bits security

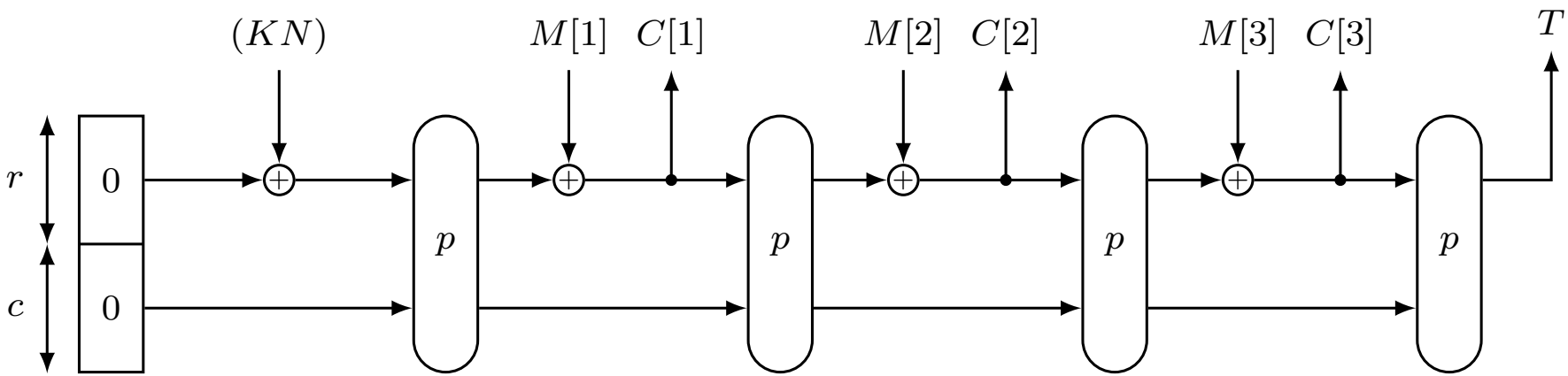


Sponge Functions

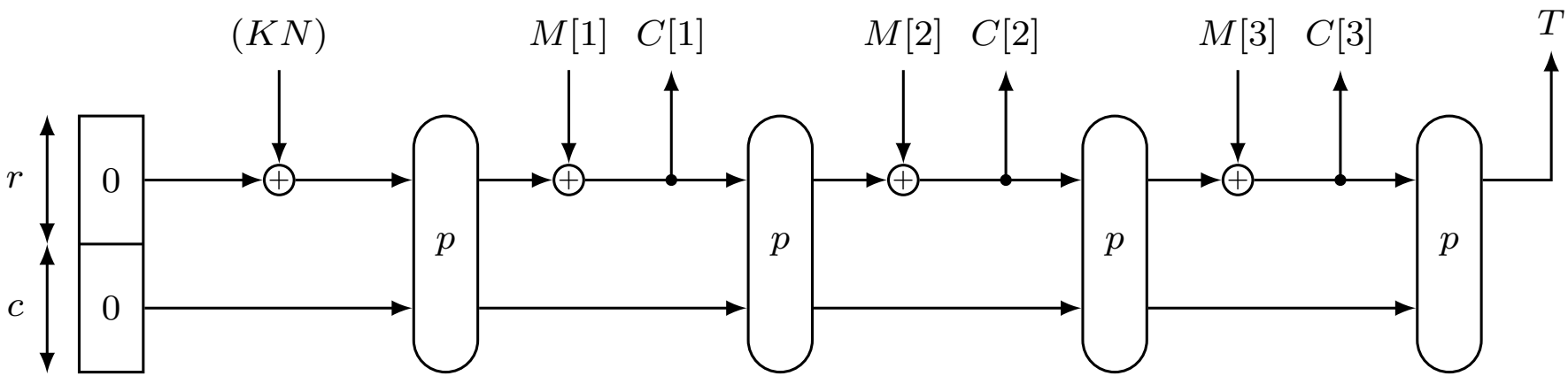
- Bertoni, Daemen, Peeters, and Van Assche (2007)
- $2^{c/2}$ queries $\rightarrow$ $\frac{c}{2}$ bits security



SpongeWrap



SpongeWrap

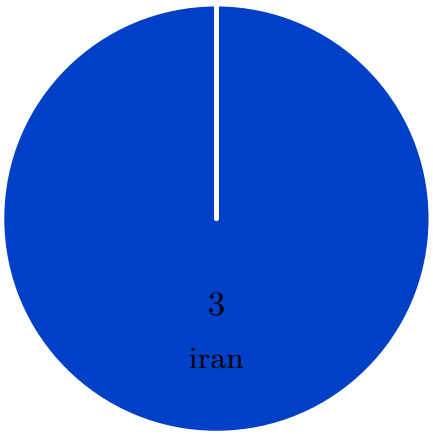


Privacy	$\min\left\{\frac{c}{2}, \kappa\right\}$ bits
Integrity	$\min\left\{\frac{c}{2}, \kappa, \tau\right\}$ bits

c = capacity $\quad$ κ = key size $\quad$ τ = tag size

Sponge-Based CAESAR Modes

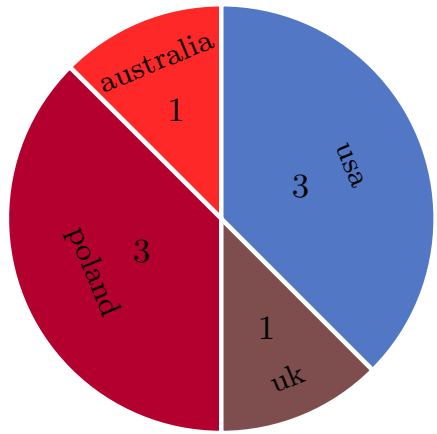
Artemia



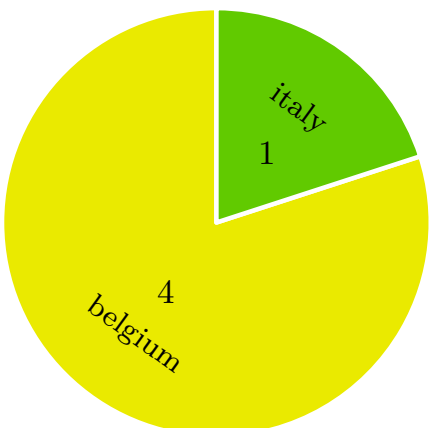
Ascon

CBEAM&STRIBOB

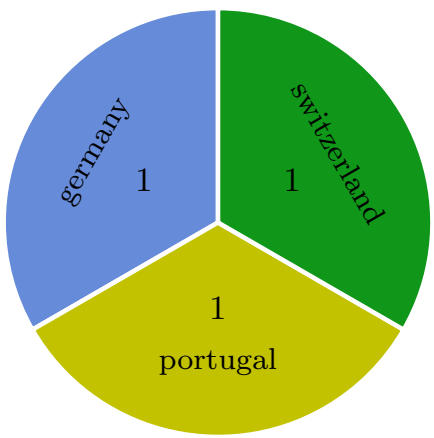
ICEPOLE



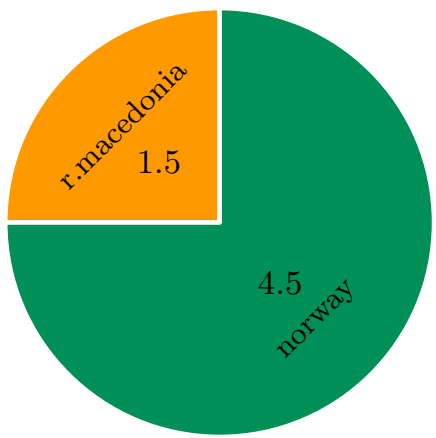
Ketje&Keyak



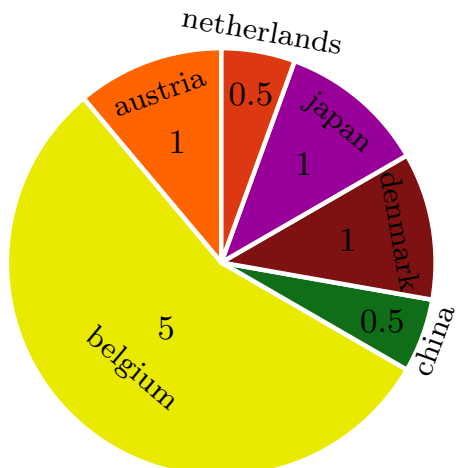
NORX



π-Cipher



PRIMATEs



Sponge-Based CAESAR Modes

nonce-dependent	**security against nonce-reuse**
Artemia	APE[2,3]
Ascon	
CBEAM/STRIBOB[1]	
ICEPOLE	
Ketje	
Keyak	
NORX	
π-Cipher	
GIBBON/HANUMAN[2]	

[1] CBEAM and STRIBOB use BLNK sponge mode

[2] PRIMATEs = {GIBBON, HANUMAN, APE}

[3] also used in submission Prøst

Sponge-Based CAESAR Modes

nonce-dependent	**security against nonce-reuse**
Artemia	APE[2,3]
Ascon	
CBEAM/STRIBOB[1]	
ICEPOLE	
Ketje	
Keyak	
NORX	
π-Cipher	
GIBBON/HANUMAN[2]	

$\frac{c}{2}$ bit security (tight)

[1] CBEAM and STRIBOB use BLNK sponge mode

[2] PRIMATEs = {GIBBON, HANUMAN, APE}

[3] also used in submission Prøst

Sponge-Based CAESAR Modes

nonce-dependent	security against nonce-reuse
Artemia	APE[2,3]
Ascon	
CBEAM/STRIBOB[1]	
ICEPOLE	
Ketje	
Keyak	
NORX	
π-Cipher	
GIBBON/HANUMAN[2]	

parameters based on $\frac{c}{2}$ results

$\frac{c}{2}$ bit security (tight)

[1] CBEAM and STRIBOB use BLNK sponge mode

[2] PRIMATEs = {GIBBON, HANUMAN, APE}

[3] also used in submission Prøst

Sponge-Based CAESAR Modes

	b	c	r	κ	**security**
Ascon	320	192	128	96	**96**
	320	256	64	128	**128**
CBEAM	256	190	66	128	**128**
ICEPOLE	1280	254	1026	128	**128**
	1280	318	962	256	**256**
Keyak	800	252	548	128	**128**
	1600	252	1348	128	**128**
NORX	512	192	320	128	**128**
	1024	384	640	256	**256**
GIBBON/ HANUMAN	200	159	41	80	**80**
	280	239	41	120	**120**
STRIBOB	512	254	258	192	**192**

Sponge-Based CAESAR Modes

	b	c	r	κ	**security**
Ascon	320	192	128	96	**96**
	320	256	64	128	**128**
CBEAM	256	190	66	128	**128**
ICEPOLE	1280	254	1026	128	**128**
	1280	318	962	256	**256**
Keyak	800	252	548	128	**128**
	1600	252	1348	128	**128**
NORX	512	192	320	128	**128**
	1024	384	640	256	**256**
GIBBON/ HANUMAN	200	159	41	80	**80**
	280	239	41	120	**120**
STRIBOB	512	254	258	192	**192**

Nonce changes everything

Mode Security Improvement

Privacy

$\min\left\{\frac{b}{2}, c, \kappa\right\}$ security

Integrity

$\min\left\{\frac{b}{2}, c, \kappa, \tau\right\}$ security

Mode Security Improvement

Privacy

$\min\left\{\frac{b}{2}, c, \kappa\right\}$ security

Integrity

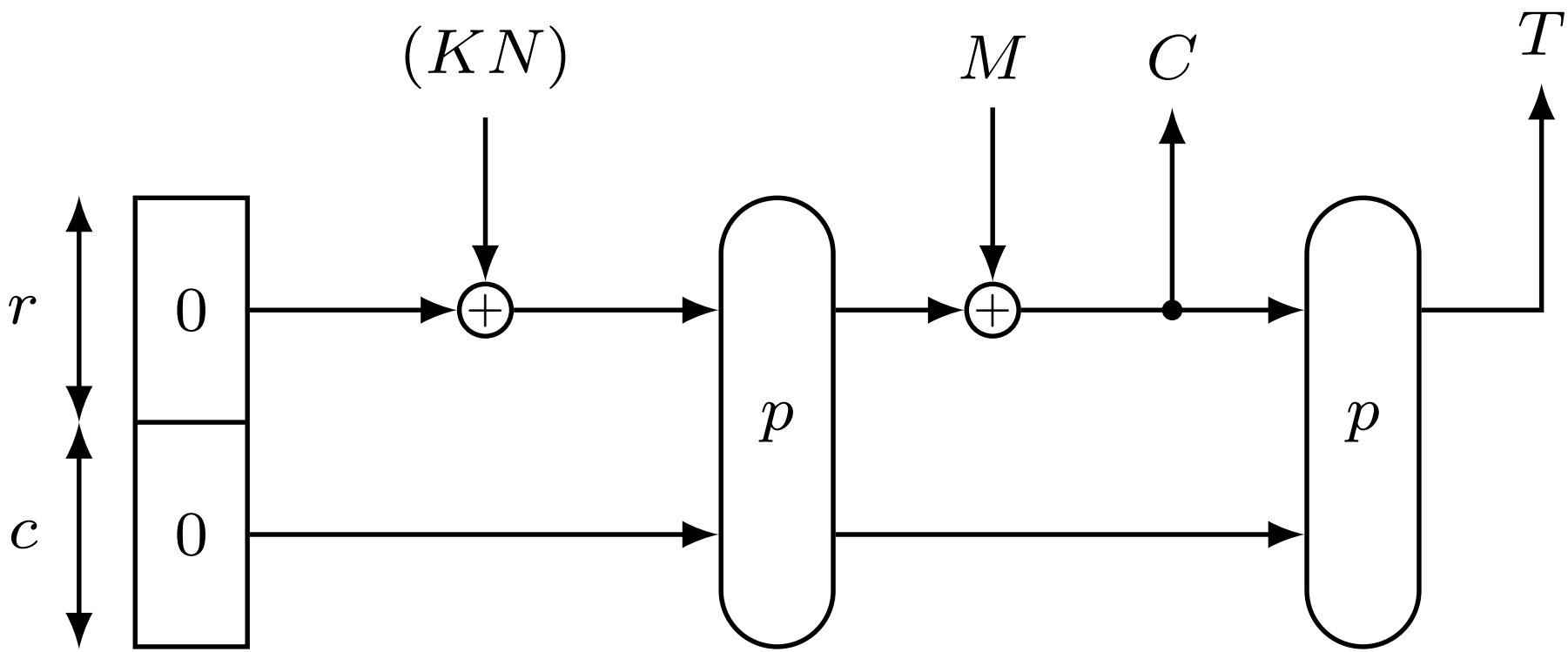
$\min\left\{\frac{b}{2}, c, \kappa, \tau\right\}$ security

Main Implication

putting $c = \kappa$ does not decrease mode security level

Privacy Intuition

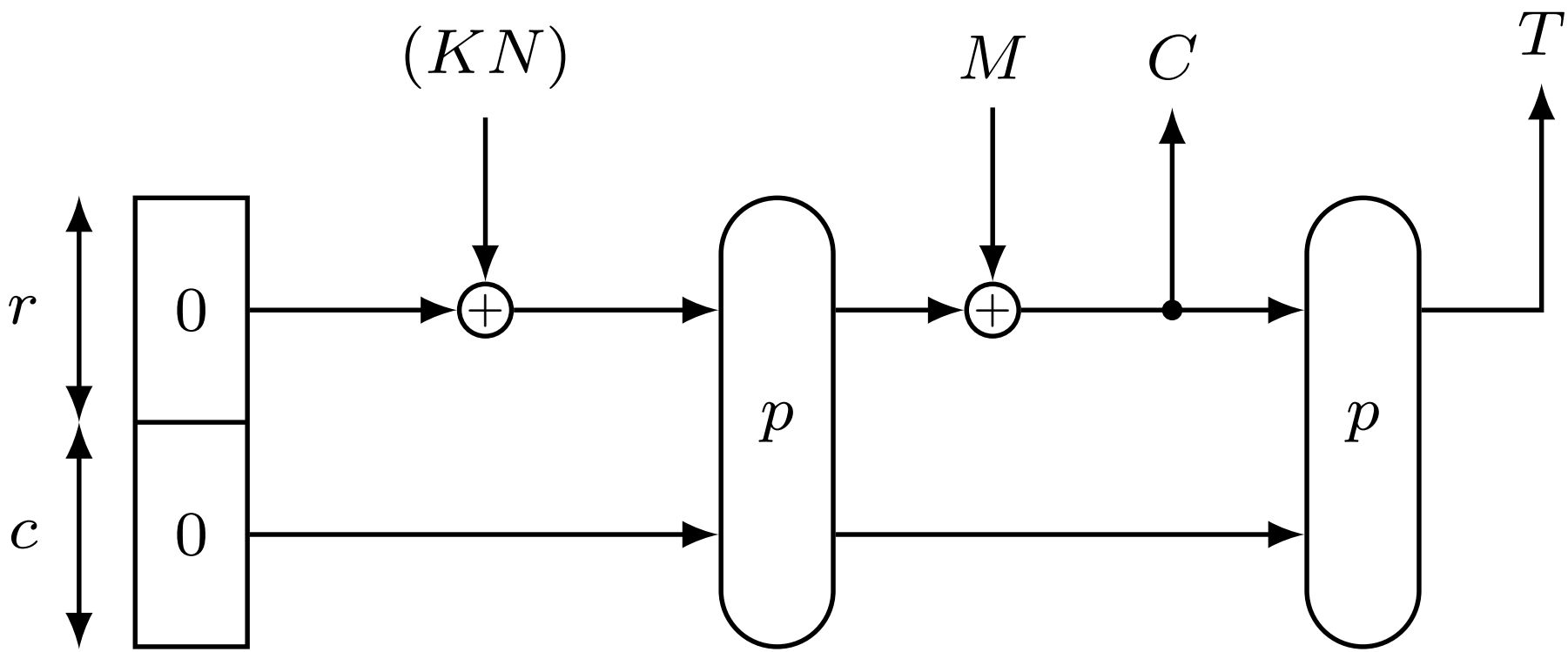
$\min\left\{\frac{b}{2}, c, \kappa\right\}$ security



Privacy Intuition

$\min\left\{\frac{b}{2}, c, \kappa\right\}$ security

key guess

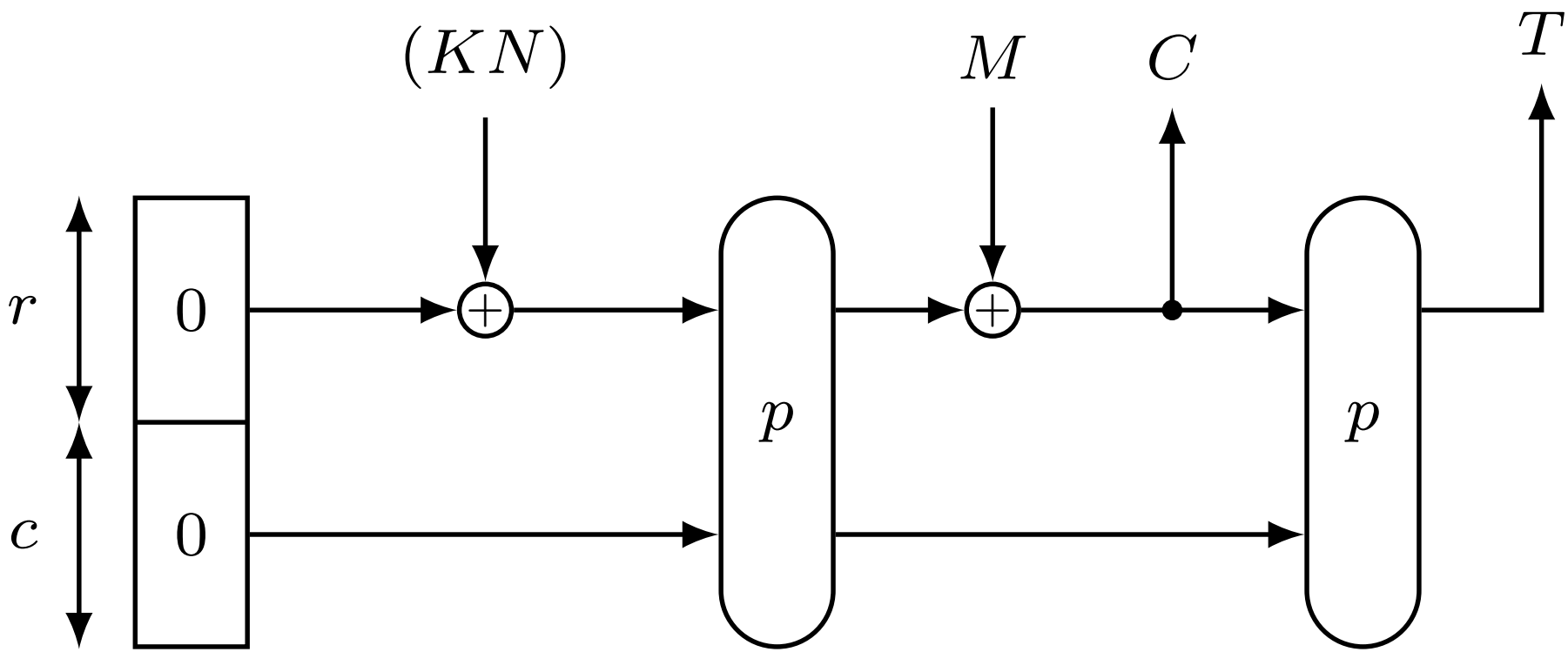


Privacy Intuition

$$\min\left\{\frac{b}{2}, c, \kappa\right\} \text{ security}$$

$\downarrow$

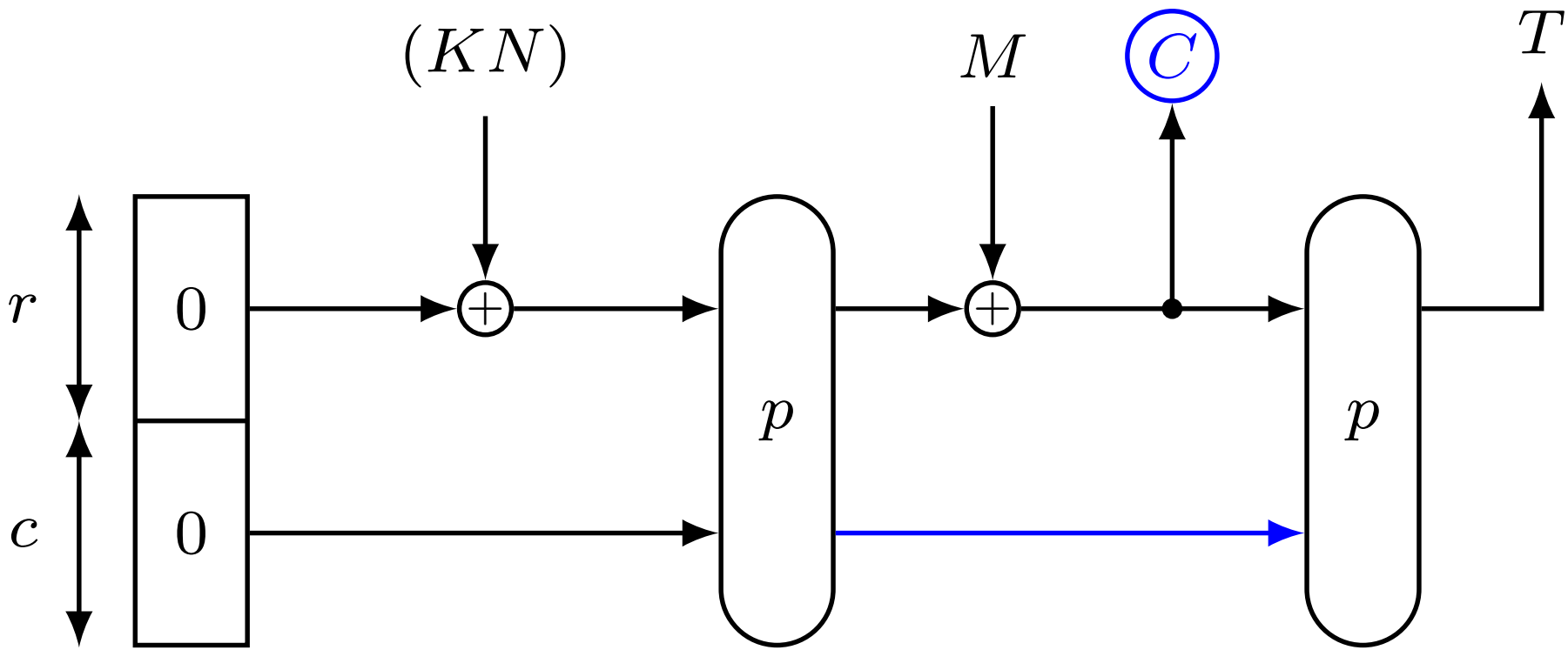
capacity guess



Privacy Intuition

$$\min\left\{\frac{b}{2}, c, \kappa\right\} \text{ security}$$

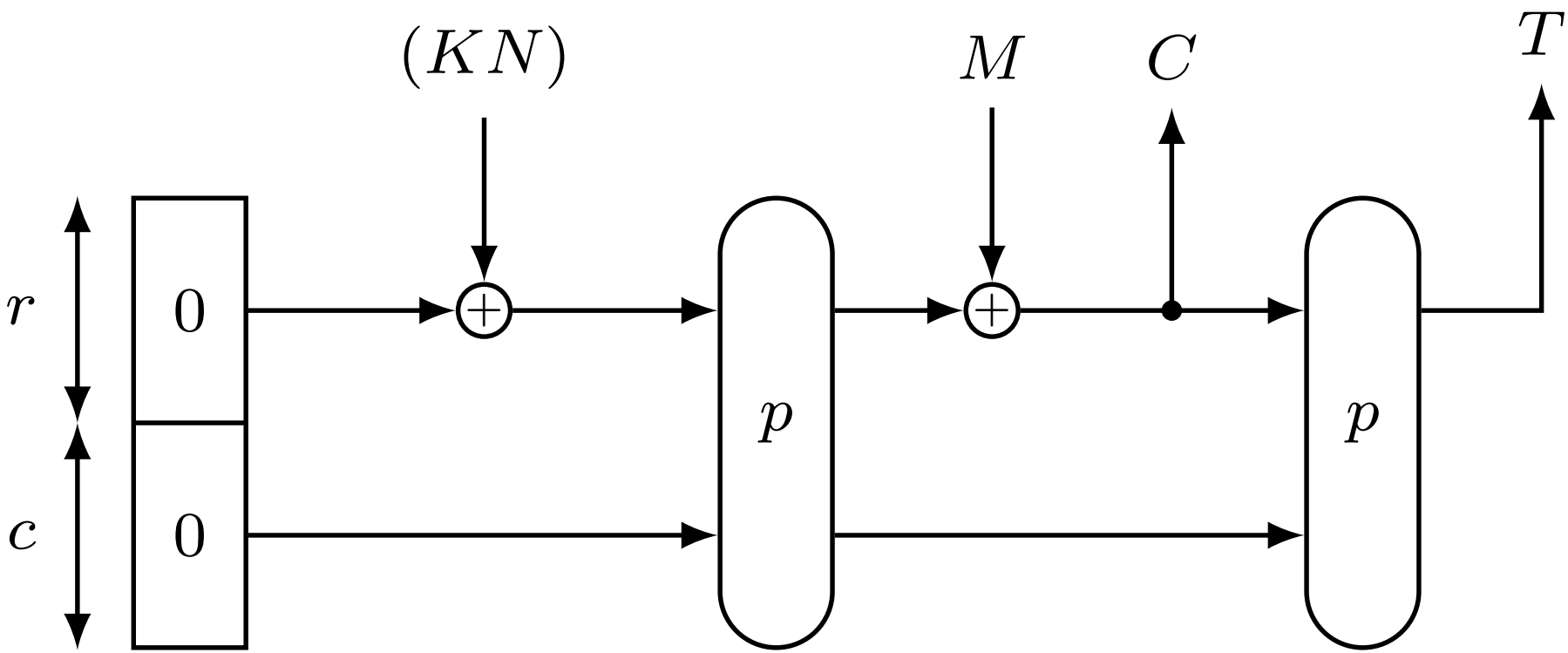
capacity guess



Privacy Intuition

$$\min\left\{\frac{b}{2}, c, \kappa\right\} \text{ security}$$

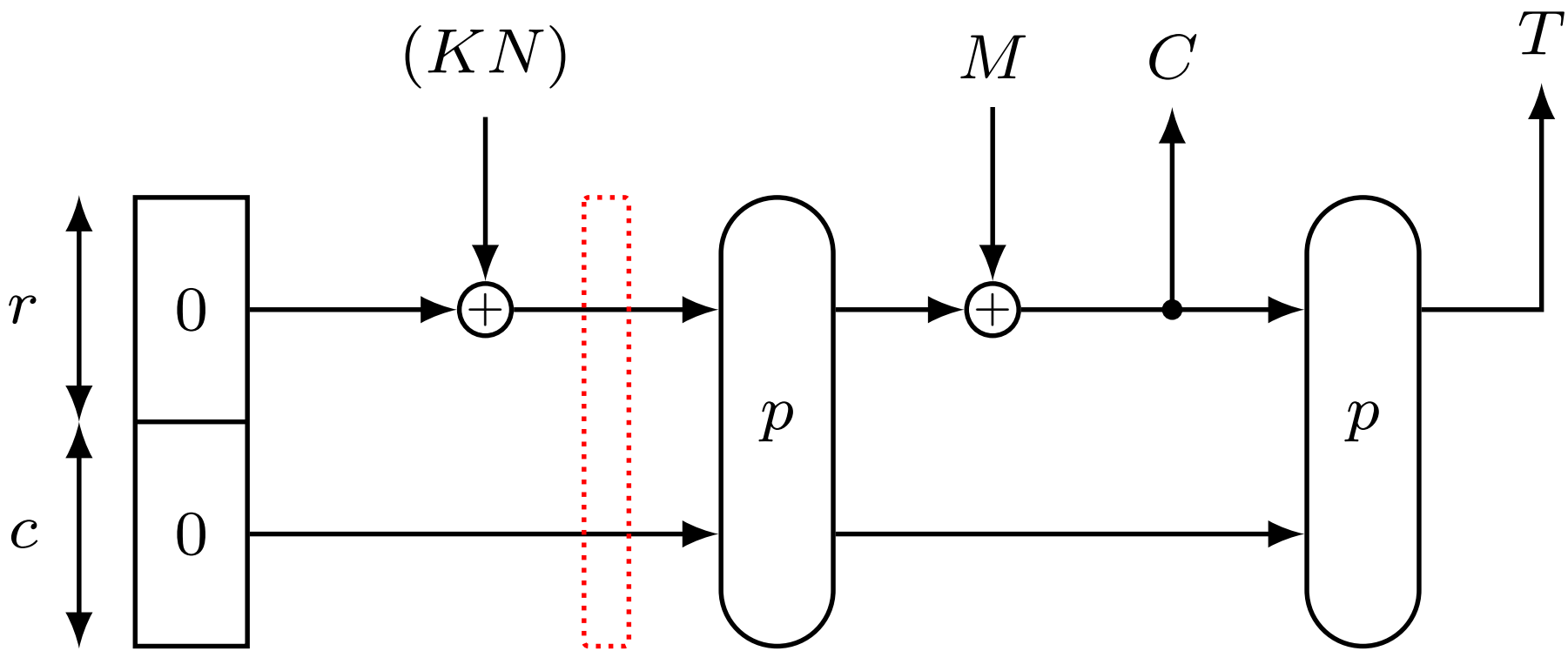
$\frac{b}{2}$ ↓ state collision



Privacy Intuition

$$\min\left\{\frac{b}{2}, c, \kappa\right\} \text{ security}$$

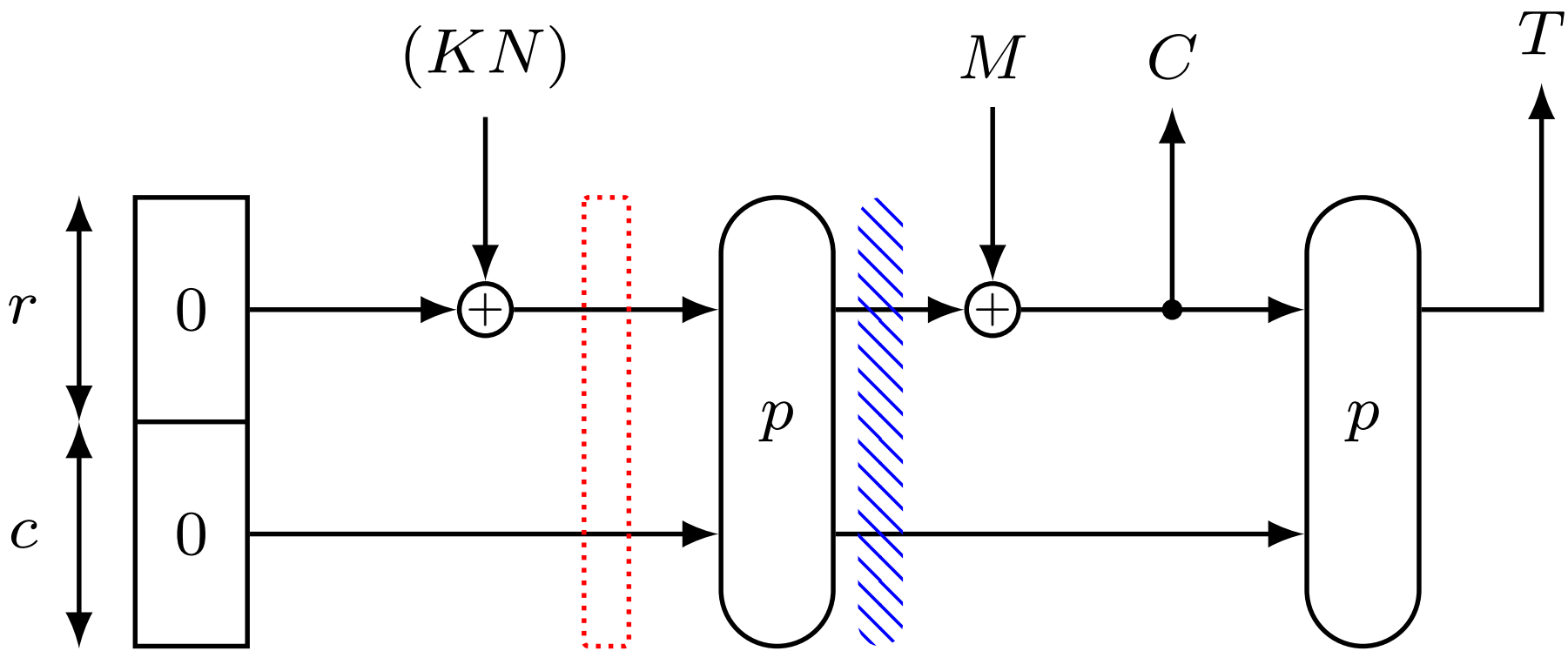
$\frac{b}{2}$ ↓ state collision



Privacy Intuition

$$\min\left\{\frac{b}{2}, c, \kappa\right\} \text{ security}$$

state collision



Integrity

$$\min\left\{\frac{b}{2}, c, \kappa, \tau\right\} \text{ security}$$

- Key guess, Tag guess

Integrity

$$\min\left\{\frac{b}{2}, c, \kappa, \tau\right\} \text{ security}$$

- Key guess, Tag guess
- Encryption queries: see privacy

Integrity

$$\min\left\{\frac{b}{2}, c, \kappa, \tau\right\} \text{ security}$$

- Key guess, Tag guess
- Encryption queries: see privacy
- Decryption queries: intuition similar to sponge function

Generalization

- Proof for NORX

Generalization

- Proof for NORX
- Generalizes to SpongeWrap and DuplexWrap

Generalization

- Proof for NORX
- Generalizes to SpongeWrap and DuplexWrap
- Generalizes to CAESAR submission modes
  - Ascon
  - BLNK (used in CBEAM and STRIBOB)
  - ICEPOLE
  - Keyak
  - GIBBON and HANUMAN (two PRIMATEs)

New Security Levels

	b	c	r	κ	**security**
Ascon	320	192	128	96	**96**
	320	256	64	128	**128**
CBEAM	256	190	66	128	**128**
ICEPOLE	1280	254	1026	128	**128**
	1280	318	962	256	**256**
Keyak	800	252	548	128	**128**
	1600	252	1348	128	**128**
NORX	512	192	320	128	**128**
	1024	384	640	256	**256**
GIBBON/ HANUMAN	200	159	41	80	**80**
	280	239	41	120	**120**
STRIBOB	512	254	258	192	**192**

New Security Levels

	b	c	r	$\frac{r}{r_{\text{old}}}$	κ	**security**
Ascon	320	96	224	1.75	96	**96**
	320	128	192	3	128	**128**
CBEAM	256	190	66		128	**128**
ICEPOLE	1280	254	1026		128	**128**
	1280	318	962		256	**256**
Keyak	800	252	548		128	**128**
	1600	252	1348		128	**128**
NORX	512	192	320		128	**128**
	1024	384	640		256	**256**
GIBBON/ HANUMAN	200	159	41		80	**80**
	280	239	41		120	**120**
STRIBOB	512	254	258		192	**192**

New Security Levels

	b	c	r	$\frac{r}{r_{\text{old}}}$	κ	**security**
Ascon	320	96	224	1.75	96	**96**
	320	128	192	3	128	**128**
CBEAM	256	128	128	1.94	128	**128**
ICEPOLE	1280	128	1152	1.12	128	**128**
	1280	256	1024	1.06	256	**256**
Keyak	800	128	672	1.23	128	**128**
	1600	128	1472	1.09	128	**128**
NORX	512	128	384	1.2	128	**128**
	1024	256	768	1.2	256	**256**
GIBBON/ HANUMAN	200	80	120	2.93	80	**80**
	280	120	160	3.90	120	**120**
STRIBOB	512	192	320	1.24	192	**192**

Conclusions

From $\min\left\{\frac{c}{2}, \kappa\right\}$ to $\min\left\{\frac{b}{2}, c, \kappa\right\}$

- Applies to
  - SpongeWrap and DuplexWrap
  - Modes of Ascon, CBEAM, ICEPOLE, Keyak, NORX, PRIMATEs, and STRIBOB

Conclusions

From $\min\left\{\frac{c}{2}, \kappa\right\}$ to $\min\left\{\frac{b}{2}, c, \kappa\right\}$

- Applies to
  - SpongeWrap and DuplexWrap
  - Modes of Ascon, CBEAM, ICEPOLE, Keyak, NORX, PRIMATEs, and STRIBOB
- Current parameter choices overly conservative
- Schemes can operate up to $4\times$ as fast
  without **mode security** degradation

Conclusions

From $\min\left\{\frac{c}{2}, \kappa\right\}$ to $\min\left\{\frac{b}{2}, c, \kappa\right\}$

- Applies to
  - SpongeWrap and DuplexWrap
  - Modes of Ascon, CBEAM, ICEPOLE, Keyak, NORX, PRIMATEs, and STRIBOB
- Current parameter choices overly conservative
- Schemes can operate up to $4\times$ as fast
  without **mode security** degradation

Thank you for your attention.