The JMAC MAC

P. KARPMAN
B. MENNINK

CRYPTO 2017

New at CRYPTO'17: ZMAC

ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication

Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, Yannick Seurin

Last in a long series of imaginatively named MACs

Such as: HMAC, NMAC, PMAC, UMAC, VMAC…

Some other famous MACs:

MAC

MAC

Definitely a pattern going on…

W.h.p., a MAC must be named xMAC, x ∈ {A,…Z, Pelican, Sandwich}

=> The design space is getting smaller

Which names are taken???

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	Pelican	Sandwich

The Bingo game goes on…

AMAC (Bellare, Bernstein & Tessaro, EC'16)

QMAC (Fehr & Salvail, EC'17)

OMAC (Iwata & Kurosawa, FSE'03)

FMAC (Hirose, SECITC'06)

XMAC (Black & Rogaway, CR'00)

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	Pelican	Sandwich

And on…

RMAC (Jaulmes, Joux & Valette, FSE'02)

MMAC (Boneh, Durfee & Franklin, EC'01)

KMAC (Kelsey, Chang & Perlner, NIST'16)

CMAC (Dworkin, NIST'05)

LMAC (Chowdhury & DasBit, GLOBECOM'15)

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	Pelican	Sandwich

And on…

BMAC (Abdalla, Namprempre & Neven, CT-RSA'06)

IMAC (Zeng, Yu & Lin, 2006)

TMAC (Kurosawa & Iwata, CT-RSA'03)

SMAC (Dent & Mitchell, 2004)

DMAC (Petrank & Rackoff, EP'97)

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	Pelican	Sandwich

And on…

WMAC (Black & Cochran, FSE'09)

EMAC (Bosselaers & Preneel, RIPE'95)

GMAC (Dworkin, IST SP'07)

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	Pelican	Sandwich

Two letters still available?

JMAC, YMAC, open to the highest bidder

But…

Kan Yasuda designed so many MACs, thus:

Definition [YMAC]:
PMAC+ (by Kan Yasuda)

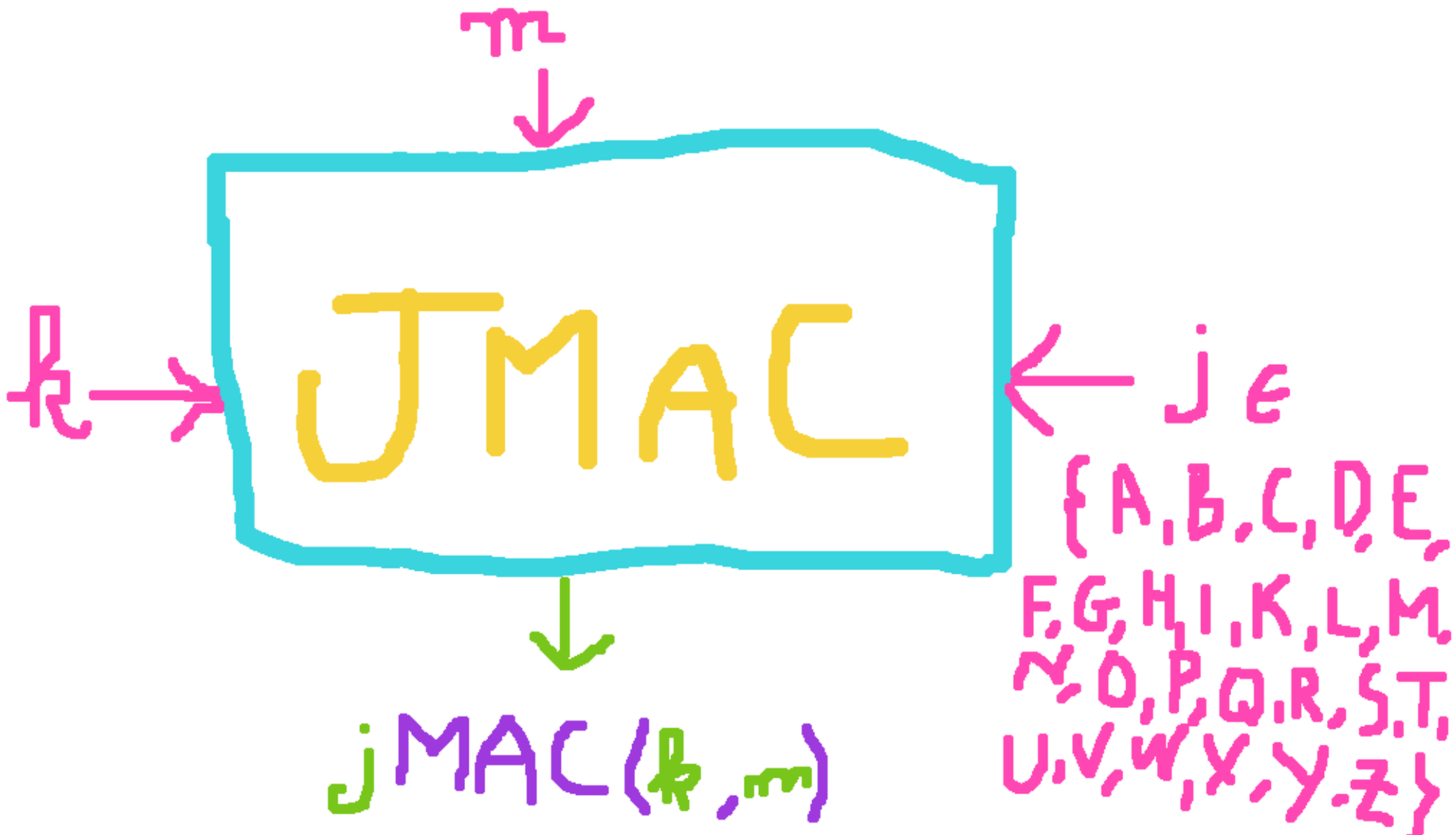
A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	Pelican	Sandwich

The True Last MAC

Finally, only one more to go!

Insert your Lord of the Rings/Highlander/Pokémon reference here

The JMAC MAC



The joke's over (thanks for enduring)!