MAC1271

D. J. Bernstein
University of Illinois at Chicago

NSF ITR–0716498

Better universal hashing

#vars	#mults	authenticators
n	n	1974; “MMH” etc.
1	n	1993; “GCM” etc.
n	$n/2$	1997; “UMAC” etc.
1	$n/2$	new

Small #mults has
obvious speed benefits.

Small #vars allows
short keys, no expansion,
good cache use, small circuits.

`cr.yp.to/papers.html#pema`

One MAC to rule them all

Choose field $\mathbf{Z}/(2^{127} - 1)$
for implementation flexibility.
Encode messages carefully.

Use the new hashes.

Derive hash key from nonce.
This *saves* time!

Discard old nonces (in receiver)
to eliminate “re-forgeries.”

Apply output filter
to protect against idiots.