MAC1271

D. J. Bernstein
University of Illinois at Chicago

NSF ITR–0716498
Better universal hashing

<table>
<thead>
<tr>
<th>#vars</th>
<th>#mults</th>
<th>authenticators</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>$n$</td>
<td>1974; “MMH” etc.</td>
</tr>
<tr>
<td>1</td>
<td>$n$</td>
<td>1993; “GCM” etc.</td>
</tr>
<tr>
<td>$n$</td>
<td>$n/2$</td>
<td>1997; “UMAC” etc.</td>
</tr>
<tr>
<td>1</td>
<td>$n/2$</td>
<td>new</td>
</tr>
</tbody>
</table>

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 \( \mathbb{Z}/(2^{127} - 1) \) 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.