Key Rap

P. ROGAWAY* T. SHRIMPTON†

4 October 2006

Mihir Bellare was the first to ask why *key wrap* needs that apparently superfluous *w*, inspiring this exposition. It formerly appeared as Appendix F of *Deterministic authenticated-encryption: a provable-security treatment of the key-wrap problem* (ePrint Report 2006/221, June 2006), which is the full version of [1].

Yo! We'z gonna' take them keys
an' whatever you pleaze
We gonna' wrap 'em all up
looks like some ran'om gup
Make somethin' gnarly and funky
won't fool no half-wit junkie
So the game's like AE
but there's one major hitch
No coins can be pitched
there's no state to enrich
the IV's in a ditch
dead drunk on cheap wine

Now NIST and X9
and their friends at the fort
suggest that you stick it
in a six-layer torte
S/MIME has a scheme
there's even one more
So many ways
that it's hard to keep score
And maybe they work
and maybe they're fine
but I want some proofs
for spendin' my time

After wrappin' them keys
gonna' help out some losers
chronic IV abusers
don't read the directions
risk a deadly infection
If a rusty IV's drippin' into yo' veins
and ya never do manage
to get it exchanged
Then we got ya somethin'
and it comes at low cost
When you screw up again
not all 'ill be lost

References

[1] P. Rogaway and T. Shrimpton. A provable-security treatment of the key-wrap problem. *Advances in Cryptology – Eurocrypt '06*, LNCS vol. 4004, Springer, pp. 373–390, 2006.

* Dept. of Computer Science, University of California at Davis, Davis, California 95616, USA; and Dept. of Computer Science, Faculty of Science, Chiang Mai University, Chiang Mai 50200, Thailand.

† Department of Computer Science, Portland State University, Portland, Oregon 97201, USA