The SIV Mode of Operation
IP Statement

Phillip Rogaway
University of California, Davis

Thomas Shrimpton
Portland State University

The inventors of SIV mode [1, 2] claim no IP rights associated to the algorithm, and are unaware of any relevant IP held by others: to the best of our knowledge, the algorithm is entirely in the public domain.

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. The full version is titled "Deterministic authenticated-encryption: a provable-security treatment of the key-wrap problem" and appears as ePrint Report 2006/221.

[2] P. Rogaway and T. Shrimpton. The SIV mode of operation for deterministic authenticated-encryption (key wrap) and misuse-resistant nonce-based authenticated-encryption. Unpublished specification document corresponding to the above. August 2007.