The SIV Mode of Operation for Deterministic Authenticated-Encryption (Key Wrap) and Misuse-Resistant Nonce-Based Authenticated-Encryption

Version 2.4 — Aug 8, 2007

Phillip Rogaway
University of California, Davis

Thomas Shrimpton
Portland State University

1 Introduction

The SIV mode of operation specifies a way for using a blockcipher to encrypt. Encryption under SIV (which stands for "Synthetic IV") takes as input a key, a plaintext, and a header, the header being a sequence of zero or more strings. It produces, deterministically, an associated ciphertext. The ciphertext protects the privacy of the plaintext and the authenticity of both the ciphertext and header. SIV can be based on an arbitrary blockcipher, such as AES or TDEA. Depending on how it is used, SIV solves both the key-wrap problem (deterministic authenticated-encryption) and the problem of conventional (two-pass, nonce-based) authenticated-encryption. This document is a compact specification for SIV mode; the theory underlying it is described elsewhere [5].

The American Standards Committee Working Group X9F1 has proposed four key-wrap schemes in a draft standard known as ANS X9.102 [1]. The algorithms are called AESKW, TDKW, AKW1, and AKW2. Compared to these modes, SIV has advantages in terms of efficiency, generality, and assurance. Compared to CCM [4], a nonce-based scheme, SIV has advantages in terms of efficiency, generality, and resistance to nonce misuse. Like all of these algorithms, SIV is not covered by any known intellectual property.

2 Notation

Throughout this specification we fix a blockcipher $E\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ for some block length $n \geq 64$. We write $E_K(X) = E(K, X)$ for the result of applying E with key $K \in \mathcal{K}$ to plaintext block $X \in \{0,1\}^n$.

All strings in this note are finite binary strings. When $M \in \{0,1\}^*$ is a string we let $|M|$ denote its length, in bits, and we let $M10^* = M10^i$ where $i \geq 0$ is the least number such that $|M| + 1 + i$ is divisible by n. The empty string is denoted ε. By $M[i..j]$ we mean the substring of M running from characters i to j (indexing begins at 1) whenever $1 \leq i \leq j \leq |M|$, and ε otherwise. For strings $S \in \{0,1\}^n$ and $M \in \{0,1\}^m$ where $m \geq n$ let $S \oplus_{\text{end}} M = (0^{m-n}S) \oplus M$. Let $\mathbf{0} = 0^n$. Let $\mathrm{msb}(S)$ be the first bit of S and let $S{\ll}1$ be S stripped of its first bit and with a zero bit appended to the end. When $S \in \{0,1\}^n$ let $\mathbf{dbl}(S) \in \{0,1\}^n$ be the product of S and $2 = 0^{n-2}10$ in the finite field with 2^n elements, this field represented in the usual way using the lexicographically first minimum-weight primitive polynomial. Doubling can be implemented with a left shift followed by a conditional xor; in particular, for $|S| = n = 128$ we have that

$$\mathbf{dbl}(S) \quad = \quad \begin{cases} S{\ll}1 & \text{if } \mathrm{msb}(S) = 0, \text{ and} \\ (S{\ll}1) \oplus 0^{120}10000111 & \text{otherwise} \end{cases}$$

and for $|S| = n = 64$ we have that $\mathbf{dbl}(S)$ is $S{\ll}1$ if $\mathrm{msb}(S) = 0$, and $(S{\ll}1) \oplus 0^{59}11011$ otherwise.

Algorithm SIV-Encrypt$^{H_1,\ldots,H_t}_{K1\,K2}(M)$
if $t \geq n-1$ **then return** $\perp$
$\mathrm{IV} \leftarrow \mathrm{CMAC}^*_{K1}(H_1, \ldots, H_t, M)$
$\mathbb{C} \leftarrow \mathrm{CTR}_{K2}(IV, M)$
return $\mathrm{IV} \parallel C$

Algorithm $\mathrm{CMAC}^*_K(X_1, \ldots, X_m)$
$S \leftarrow \mathrm{CMAC}_K(\mathbf{0})$
for $i \leftarrow 1$ **to** $m-1$ **do** $S \leftarrow \mathbf{dbl}(S) \oplus \mathrm{CMAC}_K(X_i)$
if $|X_m| \geq n$
 then return $\mathrm{CMAC}_K(S \oplus_{\text{end}} X_m)$
 else return $\mathrm{CMAC}_K(\mathbf{dbl}(S) \oplus X_m 10^*)$

Algorithm SIV-Decrypt$^{H_1,\ldots,H_t}_{K1\,K2}(\mathbb{C})$
if $t \geq n-1$ **or** $|\mathbb{C}| < n$ **then return** $\perp$
$\mathrm{IV} \leftarrow \mathbb{C}[1\,..\,n],\ C \leftarrow [n+1\,..\,|\mathbb{C}|]$
$M \leftarrow \mathrm{CTR}_{K2}(\mathrm{IV},\ C)$
$\mathrm{IV}' \leftarrow \mathrm{CMAC}^*_{K1}(H_1, \ldots, H_t, M)$
if $\mathrm{IV} = \mathrm{IV}'$ **then return** M **else return** $\perp$

Algorithm $\mathrm{CTR}_K(\mathrm{IV}, M)$
$S \leftarrow \mathrm{IV},\ \ m \leftarrow \lceil |M|/n \rceil,\ \ Pad \leftarrow \varepsilon$
for $i \leftarrow 1$ **to** m **do** $S \leftarrow \mathbf{dbl}(S)$
 $Pad \leftarrow Pad \parallel E_K(S)$ **od**
return $M \oplus Pad\,[1..|M|]$

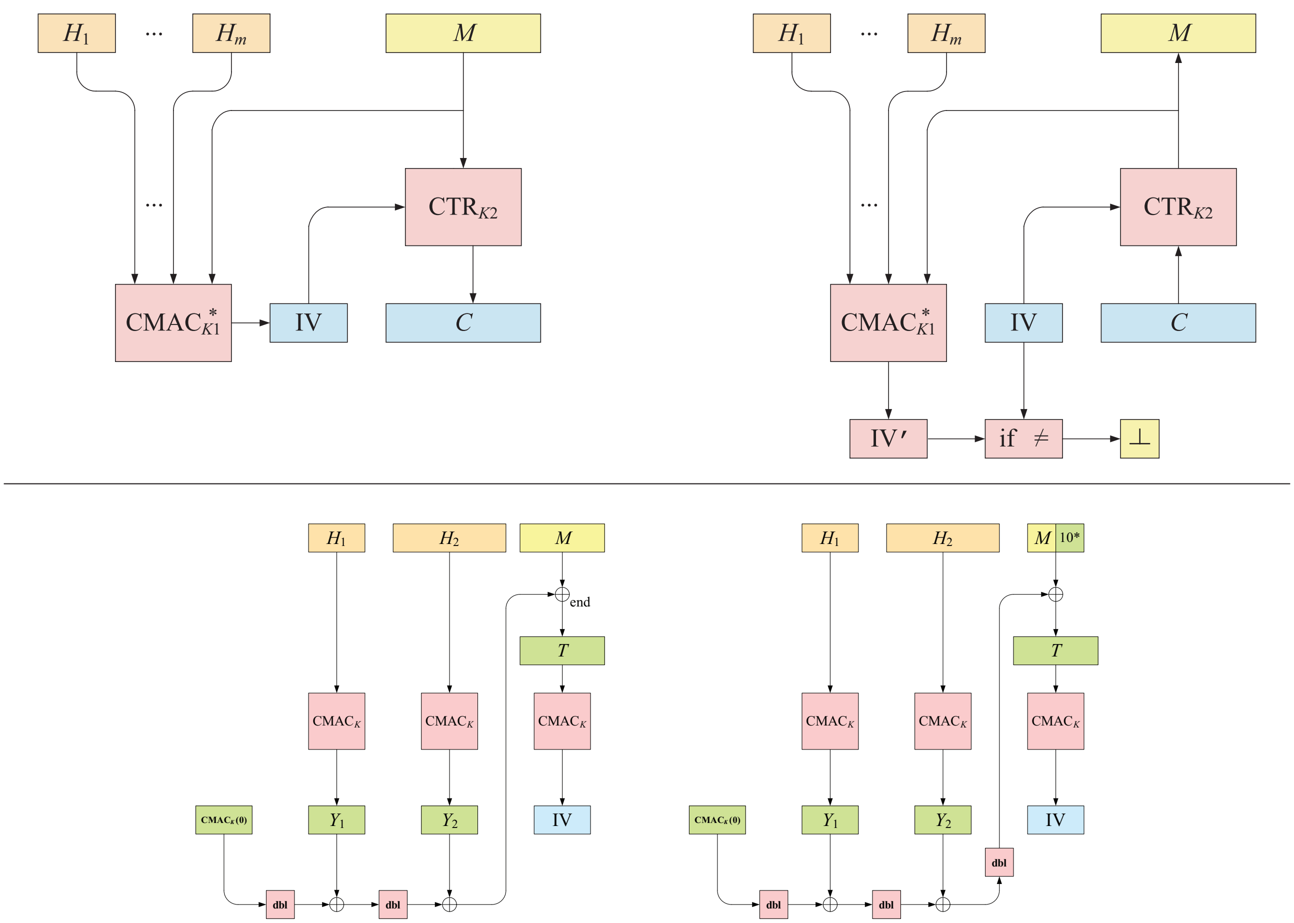

Figure 1: **Top:** Definition of SIV mode. **Middle:** Illustration of encryption (left) and decryption (right). **Bottom:** Illustration of CMAC^* when the final argument has n or more bits (left) and when it does not (right).

3 Definition of the mode

SIV mode is defined at the top of Figure 1. A key for the encryption scheme is a pair of keys $(K1, K2)$ for the underlying blockcipher. A return value of $\perp$ indicates that the input is invalid. See the CMAC specification [3] for a description of that algorithm. CMAC is understood to be taken over the same blockcipher E.

4 Comments

To achieve the key-wrap goal SIV is used "as is"; to achieve nonce-based authenticated-encryption, regard one component of the header (the j^{th} component, for some fixed j; or the last component) as holding a user-supplied nonce. This value should be chosen as something new with each message encrypted under a given key. But SIV has strong privacy and authenticity properties even if this nonce should somehow get reused: even then, new (header, ciphertext) pairs cannot be forged, and privacy will be compromised only to the extent that an adversary can detect repetitions in (header, plaintext) pairs. This property is called *misuse resistance* [5].

Prominent characteristics of SIV include: (1) The message space is all of $\{0,1\}^*$; an arbitrary string can be encrypted. (2) A header may be authenticated along with the message, the header being a vector of any reasonable number of strings (including zero), each of these strings arbitrary. (3) Message expansion is independent of header and message length: it is always n bits. (4) The contribution of any component of the header can be pre-processed if that component is held fixed. This can save a significant amount of time when some or all header information is static. (5) After initial preprocessing, the number of blockcipher calls to encrypt a nonempty message M with header $H_1, \ldots, H_t$ is $2m + h$, where $m = \lceil |M|/n \rceil$ and $h = \sum_i \lceil |H_i|/n \rceil$. The second addend may sometimes be reduced, as just described. (6) The proven security of SIV falls off in $\sigma^2/2^n$ where σ is the total number of blocks acted on. The underlying assumption is that the blockcipher is secure as a pseudorandom permutation. (7) No (invariably ad hoc) method is employed is encode various strings into one. (8) SIV never uses the inverse of the blockcipher (convenient for a blockcipher like AES).

We realize the incrementing function in CTR mode by way of doubling in a finite field, not by adding one. This choice is made for economy of techniques: doubling was already used within the mode but integer addition was not. NIST Recommendation 800-38A allows for CTR mode to use such an incrementing function [2]. The mode remains correct if other ways to increment S are used.

Acknowledgments

Many thanks to Jesse Walker, who provided much valuable feedback on this project, and to Susan Langford, who pointed out an error in an earlier version. Phil Rogaway was supported in this work by NSF 0208842 and a gift from Intel Corp.

References

[1] M. Dworkin. Request for review of key wrap algorithms. Cryptology ePrint report 2004/340, 2004. Contents are excerpts from a draft standard of the Accredited Standards Committee, X9, entitled *ANS X9.102 — Wrapping of Keys and Associated Data.*

[2] National Institute of Standards and Technology, M. Dworkin, author. Recommendation for block cipher modes of operation, methods and techniques. NIST Special Pub. 800-38A, 2001.

[3] National Institute of Standards and Technology, M. Dworkin, author. Recommendation for block cipher modes of operation: the CMAC mode for authentication. NIST Special Pub. 800-38B, May 2005.

[4] National Institute of Standards and Technology, M. Dworkin, author. Recommendation for block cipher modes of operation: the CCM mode for authentication and confidentiality. NIST Special Pub. 800-38C, May 2004.

[5] P. Rogaway and T. Shrimpton. A provable-security treatment of the key-wrap problem. *Advances in Cryptology – EUROCRYPT 2006.* LNCS vol. 4004, Springer, pp. 373–390, 2006.