IEEE P802.11
Wireless LANs

Some Comments on WHF Mode

Date: March 6, 2002

Author: **Phil Rogaway**

Department of Computer Science
Engineering II Bldg, #3063
University of California
Davis, California 95616 USA

Phone: +1 530 753 0987
Email: rogaway@cs.ucdavis.edu
WWW: http://www.cs.ucdavis.edu/~rogaway

Abstract

WHF mode [WHF02] is a block-cipher mode of operation developed for 802.11 as an alternative to OCB [OCB01]. The main advantage of WHF mode—perhaps the only significant advantage—is that it is subject to no known IP. But this advantage is paid for at significant cost:

a) The mode uses roughly twice the number of block-cipher calls.

b) The mode is highly ad hoc, designed specifically for 802.11. Indeed [WHF02] does not even make clear where the mode-definition ends and the 802.11-specific choices associated to the use of this mode begin.

c) There is no proof of security for WHF mode. A proof has been promised, but there will be major technical difficulties in constructing any valid proof for this mode.

d) The mode is new and has not previously been analyzed or published in the research literature.

Document [Fe02] shows that the authenticity bound of [OCB01] is tight, up to a small constant. In other words, [Fe02] exhibits an attack on OCB's authenticity that has efficacy $\Omega(m^2/2^n)$ where m is the number of n-bit ciphertext blocks available to the adversary. That OCB admits such attacks is simple and well known, and is equally true of all other popular modes, like the CBC MAC. Such attacks are of little or no significance in a context like that of 802.11, where n=128 and $m<2^{38}$.

We believe that if one wants a patent-unencumbered alternative to OCB, then generic composition, as described and analyzed by [BN00], makes more sense then WHF. Based on the best currently known results, one would select encrypt-then-mac generic composition (rather than WHF's mac-then-encrypt approach), taken over CTR-mode encryption and a proven-secure variable-input-length version of the CBC MAC. Generic composition is the approach taken in other standards, such as IPsec.

It is our opinion that 802.11 needs to use only published and general cryptographic techniques, and should not get involved in the design of any new cryptographic mechanisms.

1 Background

The draft 802.11i standard makes use of OCB-AES [OCB01] to achieve both privacy and authenticity. OCB is a relatively new mode of operation, but one that uses modern cryptography (namely, reduction-based proofs) in order to establish security. OCB uses roughly half the number of block-cipher calls as a conventional privacy+authenticity method would use. OCB was follow-on work to what got published as [Ju01].

OCB is a general-purpose cryptographic mechanism. It was not designed for use in 802.11; that is simply one place where its use makes sense.

Over the last several months there has emerged some voices in 802.11 that would supplement or replace OCB within the draft standard. The documents that embody this sentiment are:

> **[FHW01]** – a Nov 2001 presentation by Ferguson, Housley, and Whiting.
>
> **[WHF02]** – a Jan 2002 proposal, by the same authors, for a new mode of operation which we call WHF mode.
>
> **[Fe02]** – a Feb 2002 manuscript, again by Ferguson, in which the author describes an attack on OCB having the customary effectiveness for attacking a block-cipher mode of operation.

This note is in response to some of the criticisms put forth in the above three references.

2 Authenticated Encryption Patent Status

The real agenda underlying [FHW01,WHF02,Fe02] would appear to be patent avoidance. Ferguson et al. are quite clear about this:

> "IEEE 802 has long history with patents - Bottom line: Avoid patents when there are viable unencumbered alternatives" [FHW01, slide 5]
>
> "Fair, non-discriminatory, and non-onerous are subjective (especially after [the] standard is done)" [FHW01, slide 5]
>
> "...OCB mode has been patented ... [This] has been the main reason for the author, and several other reputable cryptanalysts he has spoken to, not to spend any time on OCB. Spending time on OCB will only help the patent-holders sell their licenses without any further compensation to the cryptanalyst. ... Given that OCB's computational advantage over patent-free modes is at most a factor of 2 ... [we] expect OCB only to be used in niche applications." [Fe02, pp. 1-2]

The facts are considerably less threatening:

a) Rogaway, IBM, and VDG Inc., the three parties who could come to hold patents in this domain, have all sent in their patent-assurance letters to the IEEE.

b) It is in the interest of none of us to make licensing difficult or expensive. Quite the opposite; the hope is for authenticated encryption to become a pervasive technique, employed in multiple, general, widely-used standards. OCB will catch on beyond 802.11 only if licensing is seen to be easy and inexpensive. All of us understand this fact.

c) OCB has already been licensed, and it has not been a difficult or costly matter for anyone concerned. It is licensed for a small, fixed, one-time fee.

d) I, for one, have never been contacted by Ferguson or his identified client to discuss licensing OCB. It seems odd to suggest that things could be "onerous" without even bothering to have sent an email.

3 An Absent Abstraction Boundary: Where's the Mode in [WHF02]?

The [WHF02] note does not explicitly specify any general block-cipher mode of operation; instead, [WHF02] describes a way to use AES that is specific to the 802.11 context. This commingling of a new mode of operation with its intended use is a major obstacle in trying to analyze the [WHF02] scheme.

The blurring together of the encryption mode and its intended use means that an analysis of [WHF02] must begin by trying to reverse-engineer a mode from the spec; one has to draw a suitable abstraction boundary or else it will not

even be clear what type of object one is analyzing or what is its intended notion of security. The abstracting out of a mode from [WHF02] turns out to be nontrivial and somewhat subjective.

It is our opinion that the "type" of object implicit in [WHF02] is a "nonce-based authenticated-encryption scheme permitting associated data". We regard [WHF02] as implicitly defining such an object. In the subject mode the associated data is 69 bits plus an additional 0 to 255 bytes. The message to be encrypted is a byte string of 0 to 65,520 bytes. The nonce is 32 bits. We consider it to part of the use of the mode, and not a part of the mode itself, that the associated data is the concatenation of what [WHF02] call RA, TA, M, and p_0,..., p_{H-1}.

To minimize technical details in the body of this note, we place in Appendix A the definition of WHF mode, as extracted from [WHF02].

4 WHF Mode is a New Mode of Operation

The [WHF02] write-up would lead one to believe that WHF mode is not a new mode of operation but a simple combination of existing modes:

> "A combination of counter mode encryption and CBC-MAC authentication is proposed here. These modes have been used and studied for a long time, with well-understood cryptographic properties, and no known patent encumbrances". [WHF02, p.1]

The above statement is extremely misleading. It is true that counter mode encryption (CTR) and the CBC MAC have been around a long time and have pretty well understood security properties; see [BDJR97] and [BKR00] for analysis of these modes. But WHF mode is not CTR mode nor the CBC MAC nor any standard way to glue these things together. WHF mode can only be studied as a new object whose security in no way follows from known results.

Studying this new cryptographic object will present major challenges. A substantial amount of "crypto engineering" has gone into the design of WHF. In particular:

- The message authentication code (MAC) that is "inside" of WHF mode is a length-prepend variant of the basic CBC-MAC. No proof of security for such a MAC has appeared. In [BKR00] it was suggested, in passing, that a particular length-prepend CBC-MAC should be provably secure, as a MAC. No proof of this statement was given, and [BKR00] specifically warned that we know of no proof approach for a length-prepend CBC MAC that would follow any line other than modifying the internals of the extremely difficult proof in our work [BKR00]. Because of this, and the fact that length-prepend MACs are not "on-line", subsequent works on arbitrary-input-length MACs abandoned the length-prepend approach [PR00,BR00].

  The situation is actually worse than the paragraph above would suggest. First, the MAC buried inside of WHF mode is even more complex than the unanalyzed form of the length-prepend CBC MAC mentioned in [BKR00]: in WHF mode the length information is intermingled with data that is being authenticated instead of being put in its own block. Beyond this, one would not be proving the security of the [WFH02] MAC in trying to establish the security of WHF mode; one would be trying to establish the security of a more complex construction, WHF mode itself, with respect to a more complex and subtle definition (that of an authenticated-encryption scheme permitting associated data).

- WHF mode roughly follows the mac-then-encrypt approach. As shown in [BN00] and then [Kr01], the mac-then-encrypt approach does not, in general, provide a mechanism that meets the "right" notion of security (ie, authenticity of ciphertexts). It is possible that WHF mode nonetheless achieves authenticity of ciphertexts, but one will not be able to establish such a result by appealing to existing work about composing encryption schemes and MACs.

- One sense in which WHF mode does not follow the mac-then-encrypt paradigm is that the same key is used internally for both the MAC-generation and the CTR-mode encryption. Such intermingling of keys is often disastrous. It might turn out that WFH mode is OK in this regard; the 3-bit "CBC-MAC" vs. "Encryption" markers used inside of WHF mode were obviously designed to "separate" these two internal tasks. But it is not clear that a proof can be pushed through, and the use of a single key will make any proof for this mode highly complex and non-modular, as it destroys the only obvious abstraction boundary inside of the mode's definition.

5 Is WHF Secure?

The short answer to this is that we do not know. WHF mode is very complex and a few days of studying it have not yielded an attack or proof.

We have made progress. As I said, the mode definition was reverse-engineered out of the [WHF02] write-up. This was a necessary first step. The mode definition is given in Appendix A.

The definition of security that one wants from the type of object that WHF mode represents is given in Appendix B. The privacy notion is a form of indistinguishability from random bits. The authenticity notion is a form of authenticity of ciphertexts. Both notions must be lifted to account for the usage of the nonce and the associated data. The desired complexity assumption would be that the block cipher is good as a pseudorandom permutation (PRP) or as a strong PRP.

In spite of hopeful statements in [Fe02], we are skeptical about the prospects of proving WHF mode secure. The complexity of a valid proof for the mode would almost certainly exceed the complexity of the [BKR00] proof, since WHF has "within it" something more complex than what [BKR00] analyzed. The complexity of a valid proof for [WHF02] would likely exceed that of [OCB01] as well. Handling adversarial adaptivity is always a major problem in a setting like this. Both [BKR00] and [OCB01] took our team months of time, and any claim that WFH mode has been proven secure should be carefully verified. There are very few people in the world who would be able to prove this mode secure, if it is possible to do at all.

6 OCB's Security Bound

The only known way to have good confidence in a block-cipher mode of operation is to have a proof of security for it. The proof establishes that IF one could break the mode of operation THEN one could break the underlying block cipher. "Breaking" (for both the encryption mode and the block cipher) are defined by well-accepted notions. OCB mode has such a reduction-based proof [OCB01]. It has been carefully executed, published in a respectable venue, and verified by my peers. WHF mode does not have any proof. From this perspective, assurance is overwhelmingly in OCB's favor.

The full story is somewhat more complex. Cryptographic security is not an all-or-nothing phenomenon, and our theory strongly reflects this. When giving a concrete-security proof of a mode of operation, there will be bounds, summarizable by formulas, which tell you how good is the proven security. The actual security might be better than the proven security bounds suggest, but it cannot be worse. One should always be pessimistic and assume that the actual security is no better than the proven security.

In the case of OCB, the bound works like this. Let's suppose that an adversary A is able, during the course of an attack, to obtain m blocks worth of plaintexts and their OCB-AES encrypted ciphertexts. For ease of explanation, suppose that there are essentially no defects in AES. (Of course the actual results in [OCB01] are devoid of such vague statements.) Then OCB's security theorems tell us that the adversary won't be able to glean information about plaintexts, nor will the adversary be able to forge new ciphertexts, with success probability ("advantage") exceeding around

$$1.5\, m^2 / 2^{128} \qquad (*)$$

As a couple of numerical examples:

a) An adversary who obtains 2^{30} bytes of data can't break privacy or authenticity with advantage exceeding $2^{2\cdot 26} / 2^{-127} = 2^{-75}$ (the 26 is $30 - 4$; one has to turn bytes into blocks)

b) An adversary who obtains $2^{41.2} > 2^{30} \times 2312$ bytes of data—more than the maximum possible in the context of 802.11—can't violate privacy or authenticity with advantage exceeding $1.5 \times 2^{2(37.2)} / 2^{-128} < 2^{-53}$

The contribution of [Fe02] is to point out that formula (*) is nearly tight: there IS an adversary that does almost as well in breaking authenticity as formula (*) allows. In fact, there are adversaries that nearly match bound (*) for attacking privacy, too.

That OCB admits attacks that nearly match our security bounds is something well known to the authors of OCB. (In fact, it is obvious to anyone who has thought seriously about our construction.) In [OCB01] we did not describe attacks achieving advantage $\Omega(m^2/2^n)$, where n is the block size, because every standard mode of operation has

been susceptible to attacks of this (in)severity. It is what everyone expects. And the whole point of provable-security is to not have to look at attacks like this in order to know how secure is your construction.

The above is not to imply that getting better bounds for schemes is not a nice area of research. Indeed, for several years the cryptographic community has paid attention to the design and analysis of encryption and MAC schemes that support proven security bounds better than $\Omega(m^2/2^n)$. [BGR95] and [BGK99] were motivated by this issue.

But the truth is, finding block-cipher modes with improved bounds was seen as more important when the prevailing blocksize was n=64 bits. Now that one imagines using a block cipher with a blocksize of n=128, the usual $\theta(m^2/2^n)$ bounds seem perfectly fine to most researchers. This is particularly true for 802.11, where there is a well understood and moderate maximum number of message blocks sent on a given key; see calculation (b) above. Note that 2^{-53} is a miniscule forgery probability (2^{-32} has been the norm for retail banking); do not confuse this number with some sort of inverse running time, for example.

[Fe02] does raise an interesting possibility: that mac-then-encrypt authenticated encryption, when suitably instantiated, may achieve a better security bound than that achieved by encrypt-then-mac. It is possible. It turns out that Mihir Bellare has recently been investigating this question, though no results in this direction have appeared. Ferguson indicates that he knows of no attack on WHF mode that achieves $\Omega(m^2/2^n)$ forgery probability. (Breaking WHF privacy with $\Omega(m^2/2^n)$ advantage is easy.) We, likewise, do not see such an attack right off. Proving a subquadratic security bound for a mac-then-encrypt scheme is an interesting research problem. But the author finds none of this discussion relevant to 802.11, where the state of the art—proven bounds of $\theta(m^2/2^n)$—is perfectly fine.

7 Alternatives to the Alternative

Despite the criticism of WHF mode given here, there are reasonable alternatives to OCB mode. In my July 2001 talk at 802.11 [Ro01], and in information on the OCB web site (www.cs.ucdavis.edu/~rogaway/ocb ; see question 20 of the OCB FAQ), I have explained that generic composition makes a reasonable alternative to OCB. Generic composition entails that one separately encrypts and computes a MAC, using different keys. To make a scheme with good assurance, both modes being glued together need to be proven secure and the combining of the modes must be done with care [BN00, Kr01]. Using CTR mode and a proven-secure version of the CBC MAC, one would pay a factor of two in block cipher calls compared to OCB. One would pay in increased key length as well. But, as with OCB, one gets provable security, and with the same security bound. The ciphertext length is also unchanged. It is possible that WHF mode began as an attempt to do generic composition but took a wrong turn somewhere along the way.

8 Acknowledgements

Many thanks for the comments and useful feedback from Mihir Bellare (UC San Diego), Nancy Cam-Winget (CMC), David Wagner (UC Berkeley), and Jesse Walker (Intel).

9 References

[BDJR97] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation. Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS 97), IEEE Press, 1997. http://www.cs.ucdavis.edu/~rogaway

[BGK99] M. Bellare, O. Goldreich, and H. Krawczyk. Stateless evaluation of pseudorandom functions: Security beyond the birthday barrier. CRYPTO 99. LNCS v. 1666, Springer-Verlag, 1999. http://www-cse.ucsd.edu/users/mihir/

[BGR95] M. Bellare, R. Guerin, and P. Rogaway. XOR MACs: New methods for message authentication using finite pseudorandom functions. CRYPTO '95. LNCS vol. 963, Springer-Verlag, 1995. http://www.cs.ucdavis.edu/~rogaway

[BKR00] M. Bellare, J. Kilian, and P. Rogaway. The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences (JCSS), vol. 61, no. 3, Dec 2000, pp. 362-399. Earlier version in CRYPTO '94. http://www.cs.ucdavis.edu/~rogaway

[BN00] M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. ASIACRYPT 2000, LNCS vol. 1976, Springer-Verlag, 2000. http://www-cse.ucsd.edu/users/mihir/

[BR00] J. Black and P. Rogaway. CBC MACs for arbitrary-length messages: The three-key constructions. CRYPTO '00, LNCS vol. 1880, Springer-Verlag, 2000. http://www.cs.ucdavis.edu/~rogaway

[Fe02] N. Ferguson, Collision attacks on OCB. Unpublished manuscript. Feb 11, 2002. http://www.cs.ucdavis.edu/~rogaway/ocb/fe02.pdf

[FHW01] N. Ferguson, R. Housley, and D. Whiting. AES mode choices—OCB vs counter mode with CBC-MAC. Presentation to 802.11, doc.:IEEE 802.11-01/634r1. November 2001. http://www.cs.ucdavis.edu/~rogaway/ocb/fhw01.pdf

[Ju01] C. Jutla. Encryption modes with almost free message integrity. EUROCRYPT 2001. LNCS vol. 2045, Springer-Verlag, 2001. NIST submission csrc.nist.gov/encryption/modes/proposedmodes/

[Kr01] H. Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is SSL?). CRYPTO 2001, Springer-Verlag, 2001. http://eprint.iacr.org/2001/045/

[OCB01] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. A block-cipher mode of operation for efficient authenticated encryption. Eighth ACM Conference on Computer and Communications Security (CCS-8), ACM Press, pp. 196-205, 2001. http://www.cs.ucdavis.edu/~rogaway

[PR00] E. Petrank and C. Rackoff. CBC MACs for real-time data sources. J. of Cryptology, vol.13, no.13, pp. 315-338, 2000. Earlier version as http://eprint.iacr.org/1997/010/

[Ro01] P. Rogaway. OCB mode. doc:IEEE 802.11-01/378. July 01. www.cs.ucdavis.edu/~rogaway/ocb/talks.htm

[WHF02] D. Whiting, R. Housley, and N. Ferguson. AES encryption & authentication using CTR Mode & CBC-MAC. Unpublished manuscript, doc.:IEEE 802.11-02/001r0. January 15, 2002. http://www.cs.ucdavis.edu/~rogaway/ocb/whf02.pdf

A. Appendix – Abstracting out the Mode from [WHF02]

NOTATION. Let [...] denote an encoding of the specified arguments into a 128-bit string. Let *len*(*x*) be the bit length of string *x* and let *LEN*(*x*) be the byte length of byte-string *x*. Fix a block cipher E: $\{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$.

DEFINITION OF THE WHF SCHEME. The WHF encryption scheme is the triple *WHF* = (*WHF_Key*, *WHF_Encrypt*, *WHF_Decrypt*) where each component algorithm is specified below. WHF mode is parameterized by the block cipher *E*.

DEFINITION OF THE KEY-GENERATION ALGORITHM. Key-generation algorithm *WHF_Key* chooses a random key *K* for the underlying block cipher *E* and returns *K* as the key for the encryption scheme.

DEFINITION OF THE ENCRYPTION ALGORITHM. We define WHF encryption as follows.

```
WHF_Encrypt ( K         - 16-byte string (the key)
              N         -  4-byte string (the nonce)
              AD        - string of 69 + 8H bits where 0 ≤ H ≤ 255
              Message   - byte string, LEN(Message) ≤ 65,520 − H
      )
begin
      ad || Header = AD where len(ad) = 69
      H  = LEN(Header)
      L = HL + LEN(Message)
      P = Header || Message
      P* = P || 0^i with i minimal s.t. 128 |len(P*)
      Z[0] = E(K, [N, H, L, ad, "MIC"])
      X[1] || ... || X[m] = P* where LEN(X[i])=16 for I < m and
                                     1 ≤ len(X[m]) ≤ 128
      for i = 1 to m do
            Z[i] = E (K, Z[i−1] xor X[i])
      Tag = first 8 bytes of Z[m]

      MessageTag = Message || Tag
      Pad = the first LEN(MessageTag) bytes of
            E(K, <N, H, 0, ad, "ENC"> ||
            E(K, <N, H, 1, ad, "ENC"> ||
            E(K, <N, H, 2, ad, "ENC"> ||  ...

      Ciphertext = MessageTag xor Pad
      return Ciphertext  // byte string of LEN(Plaintext) + 8 bytes
end
```

DEFINITION OF THE DECRYPTION ALGORITHM. We define WHF decryption as follows. Note that decryption returns either a string or the distinguished value INVALID. Though we do not explicitly say so in the pseudocode, it is understood that INVALID must be returned when one tries to decrypt any point outside of the specified domain.

```
WHF_Decrypt ( K          - 16-byte string (the key)
              N          -  4-byte string (the nonce)
              AD         - string of 69 + 8H bits where 0 ≤ H ≤ 255
              Ciphertext - byte string, 8 ≤ LEN(Ciphertext) ≤ 65520 - H
      )
begin
      ad || Header = AD where len(ad) = 69
      H  = LEN(Header)
      L = H + LEN(CIPHERTEXT) − 8

      Pad = the first LEN(Ciphertext) bytes of
            E(K, <N, H, L, 0, "ENC"> ||
            E(K, <N, H, L, 1, "ENC"> ||
            E(K, <N, H, L, 2, "ENC"> ||  ...
      MessageTag = Ciphertext xor Pad
      Message || Tag = MessageTag where LEN(Tag)=8

      P = Header || Message
      P* = P || 0^i with i minimal s.t. 128 |len(P*)

      X[0] = [N, H, L, ad, "MIC"]
      X[1] || ... || X[m] = P* where LEN(X[i])=16 for i < m and

      for i = 1 to m do
            Z[i] = E (K, Z[i−1] xor X[i])
      Tag' = first 8 bytes of Z[m]

      if Tag = Tag' then return Message
      else return INVALID
end
```

B. Appendix – A Security Definition Appropriate to [WHF02]

PRIVACY. Let *WFH*[*E*] be the specified encryption scheme for some block cipher *E*. Consider an adversary *A* that is given an oracle ORACLE(*N*, *AD*, *Message*). The adversary asks of this oracle, adaptively, a sequence of queries (*N*_1, *AD*_2, *M*_1), ..., (*N_q*, *AD_q*, *M_q*), obtaining as a result of these queries *C*_1, ..., *C_q*. The values *N*_1, ..., *N_q* that the adversary asks during this stage must be distinct. Consider answering *A*'s queries in one of the following two ways:

Real Query (*N*,*AD*,*Message*) returns *E*(*K*,*N*,*AD*,*Message*) for a random *K* (chosen at the beginning of the experiment by running *WHF_Key*).

$ Query (*N*,*AD*,*Message*) returns a random string of *LEN*(*Message*) + 8 bytes.

Define $\mathbf{Adv}^{\text{priv}}(A) = \mathbf{Pr}[A^{\text{Real}} = 1] - \mathbf{Pr}[A^{\$} = 1]$ and define $\mathbf{Adv}^{\text{priv}}(q,m)$ as the maximum value of $\mathbf{Adv}^{\text{priv}}(A)$ over all adversaries *A* that ask messages *M*_1, ..., *M_q* that sum to *mn* bits.

Intuitively, the privacy goal is for $\mathbf{Adv}^{\text{priv}}(q,m)$ to be small when *E* is secure in the usual sense of being a good pseudorandom permutation. One needs a theorem to establish such a claim.

AUTHENTICITY. Provide an adversary *A* with a **Real** oracle, as specified above. When running adversary *A* with such an oracle *E*(*K*,?,?,?), say that *A forges* if it outputs (*N*, *AD*, *C*) where *WHF_Decrypt*(*K*,*N*,*AD*,*C*) is not INVALID and *A* made no earlier oracle query (*N*,*AD*,*) the resulted in a response *C*. Let $\mathbf{Adv}^{\text{auth}}(A)$ be the probability that *A* forges. Let $\mathbf{Adv}^{\text{auth}}(q,m)$ be the maximum value of $\mathbf{Adv}^{\text{auth}}(A)$ over all adversaries *A* that ask queries *M*_1, ..., *M_q* and then produce an output *C* that totals *mn* bits.

Intuitively, the authenticity goal is for $\mathbf{Adv}^{\text{auth}}(q,m)$ to be small when *E* is secure in the usual sense of being a strong pseudorandom permutation. One needs a theorem to establish such a claim.