ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

*INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING*

*National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)*

*Alva's Institute of Engineering and Technology, Moodbidri*

*Vol. 3, Special Issue 1, April 2015*

# For Mobile and Pervasive Computing Providing Efficient Authentication

**Sreekanth. K**

M.Tech Student, Department of Computer Science and Engineering, Shree Devi Institute of Technology, Mangalore, Karnataka, India

**Abstract:** With today's technology, many applications rely on the existence of small devices that can exchange information and form communication networks. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this work, we propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives.

**Index Terms:** Authentication, unconditional security, computational security, universal hash-function families, pervasive computing.

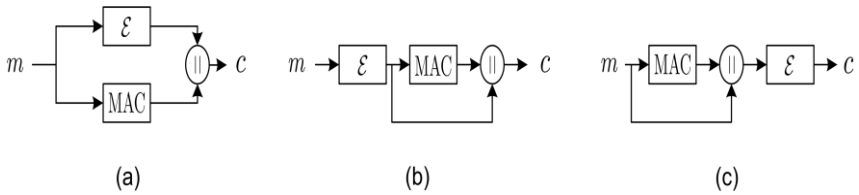


Fig. 1. A schematic of the three generic compositions; (a) Encrypt-and-Authenticate (E&A), (b) Encrypt-then Authenticate (EtA), and (c) Authenticate-then-Encrypt (AtE).

## I. INTRODUCTION

PRESERVING the integrity of messages exchanged over public channels is one of the classic goals in cryptography and the literature is rich with message authentication code (MAC) algorithms that are designed for the sole purpose of preserving message integrity. Based on their security, MACs can be either unconditionally or computationally secure. Unconditionally secure MACs provide message integrity against forgers with unlimited computational power. On the other hand, computationally secure MACs are only secure when forgers have limited computational power. One of the main differences between unconditionally secure MACs based on universal hashing and computationally secure MACs based on universal hashing is the requirement to process the compressed image with a cryptographic primitive in the latter class of MACs. This round of computation is necessary to protect the secret key of the universal hash function. That is, since universal hash functions are not cryptographic functions, the observation of multiple message-image pairs can reveal the value of the hashing key. Since the hashing key is used repeatedly in computationally secure MACs, the exposure of the hashing key will lead to breaking the security of the MAC. Thus, processing the compressed image with a cryptographic primitive is necessary for the security of this class of MACs. This implies that unconditionally secure MACs based on universal hashing are more efficient than computationally secure ones. On the negative side, unconditionally secure universal hashing based MACs are considered impractical in most modern applications, due to the difficulty of managing one-time keys.

There are two important observations to make about existing MAC algorithms. First, they are designed independently of any other operations required to be performed on the message to be authenticated. For instance, if the authenticated message must also be encrypted, existing MACs are not designed to utilize the functionality that can be provided by the underlying encryption algorithm. Second, most existing MACs are designed for the general computer communication systems, independently of the properties that messages can possess. For example, one can find that most existing MACs are inefficient when the messages to be authenticated are short.

## II. CONTRIBUTIONS

In this work, we pose the following research question: if there is an application in which messages that need to be exchanged are short and both their privacy and integrity

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

*INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING*

*National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)*

*Alva's Institute of Engineering and Technology, Moodbidri*

*Vol. 3, Special Issue 1, April 2015*

need to be preserved, can one do better than simply encrypting the messages using an encryption algorithm and authenticating them using standard MAC algorithm? We answer the question by proposing two new techniques for authenticating short encrypted messages that are more efficient than existing approaches. In the first technique, we utilize the fact that the message to be authenticated is also encrypted, with any secure encryption algorithm, to append a short random string to be used in the authentication process. Since the random strings used for different operations are independent, the authentication algorithm can benefit from the simplicity of unconditional secure authentication to allow for faster and more efficient authentication, without the difficulty to manage one-time keys. In the second technique, we make the extra assumption that the used encryption algorithm is block cipher based to further improve the computational efficiency of the first technique. The driving motive behind our investigation is that using a general purpose MAC algorithm to authenticate exchanged messages in such systems might not be the most efficient solution and can lead to waste of resources already available, namely, the security that is provided by the encryption algorithm.

## III. AUTHENTICATING SHORT ENCRYPTED MESSAGES

In this section, we describe our first authentication scheme that can be used with any IND-CPA secure encryption algorithm. An important assumption we make is that messages to be authenticated are no longer than a predefined length. This includes applications in which messages are of fixed length that is known a priori, such as RFID systems in which tags need to authenticate their identifiers, sensor nodes reporting events that belong to certain domain or measurements within a certain range, etc. The novelty of the proposed scheme is to utilize the encryption algorithm to deliver a random string and use it to reach the simplicity and efficiency of one-time pad authentication without the need to manage impractically Long keys.

## IV. THE PROPOSED SYSTEM

Let N  1 be an upper bound on the length, in bits, of exchanged messages. That is, messages to be authenticated can be no longer than (N  1)-bit long. Choose p to be an N-bit long prime integer. (If N is too small to provide the desired security level, p can be chosen large enough to satisfy the required security level.) Choose an integer ks uniformly at random from the multiplicative group Z_ p; ks is the secret key of the scheme. The prime integer, p, and the secret key, ks, are distributed to legitimate users and will be used for message authentication. Note that the value of p need not be secret, only ks is secret. Let E be any IND-CPA secure encryption algorithm. Let m be a short messages (N  1 bit or shorter) that is to be transmitted to the intended receiver in a confidential manner (by encrypting it with E). Instead of authenticating the message using a traditional MAC algorithm, consider the following procedure. On input a message m, a random nonce r 2 Zp is chosen. (We overload m to denote both the binary string representing the message, and the integer representation of the message as an element of Zp. The same applies to ks and r. The distinction between the two representations will be omitted when it is clear from the context.) We assume that integers representing distinct messages are also distinct, which can be achieved by appropriately encoding messages. Now, r is appended to the message and the resulting m k r, where "k" denotes the concatenation operation, goes to the encryption algorithm as an input.

**Security Model:**

A message authentication scheme consists of a signing algorithm S and a verifying algorithm V. The signing algorithm might be probabilistic, while the verifying one is usually not. Associated with the scheme are parameters and N describing the length of the shared key and the resulting authentication tag, respectively. On input an `-bit key k and a message m, algorithm S outputs an N-bit string called the authentication tag, or the MAC of m. On input an `-bit key k, a message m, and an N-bit tag , algorithm V outputs a bit, with 1 standing for accept and 0 for reject. We ask for a basic validity condition, namely that authentic tags are accepted with probability one.) for a random but hidden choice of k. A can query S to generate a tag for a plaintext of its choice and ask the verifier V to verify that _ is a valid tag for the plaintext. Formally, A's attack on the scheme is described by the following experiment:

1) A random string of length ` is selected as the shared secret.
2) Suppose A makes a signing query on a message m. Then the oracle computes an authentication tag _ = S (k; m) and returns it to A. (Since S may be probabilistic, this step requires making the necessary underlying choice of a random string for S, anew for each signing query.)
3) Suppose A makes a verify query (m; _). The oracle computes the decision d = V (k; m; _) and returns it to A.

**Security of the Authenticated Encryption Composition:**

In this module, it defined two notions of integrity for authenticated encryption systems: the first is integrity of plaintext (INT-PTXT) and the second is integrity of cipher text (INT-CTXT). Combined with encryption algorithms that provide in-distinguish ability under chosen plaintext attacks (IND-CPA), the security of different methods for constructing generic compositions is analyzed.

Note that our construction is an instance of the Encrypt-and-Authenticate (E&A) generic composition since the plaintext message goes to the encryption algorithm as an input, and the same plaintext message goes to the authentication algorithm as an input.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

*INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING*

*National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)*

*Alva's Institute of Engineering and Technology, Moodbidri*

*Vol. 3, Special Issue 1, April 2015*

## V. FROM WEAK TO STRONG UNFORGEABILITY

There are two notions of unforgeability in authentication codes. Namely, a MAC algorithm can be weakly unforgeable under chosen message attacks (WUF-CMA), or strongly unforgeable under chosen message attacks (SUFCMA). A MAC algorithm is said to be SUF-CMA if, after launching chosen message attacks, it is infeasible to forge a message-tag pair that will be accepted as valid regardless of whether the message is "new" or not, as long as the tag has not been previously attached to the message by an authorized user. If it is only hard to forge valid tags for "new" messages, the MAC algorithm is said to be WUF-CMA.

The authentication code, as described in Section 3, is only WUF-CMA. To see this, let E works as follows. On input a message m, generate a random string s, compute PRFx(s), where PRFx is a pseudorandom function determined by a secret key x, and transmit c = (s; PRFx(s) _ m) as the cipher text. Then, E is an IND-CPA secure encryption.

## VI. ENCRYPTING WITH PSEUDORANDOM PERMUTATIONS

(BLOCK CIPHERS)

In this section, we describe a message authentication approach that is faster than the one described in previous sections. The main idea of this approach is that the input-output relation of the used encryption operation can be realized as a pseudorandom permutation. In what follows, we will show how to utilize the pseudo randomness of block ciphers in a novel way to further improve the efficiency of the authentication algorithm. Message Encryption Let m be a short message that is to be transmitted to the intended receiver in a confidential manner. For every message to be transmitted, a random nonce r 2 Z2N is chosen.

(We overload m to denote both the binary string representing the message, and the integer representation of the message as an element of Z2N; the same applies to r. The distinction between the two representations will be omitted when it is clear from the context.) Now, the concatenation of r and m goes to the encryption algorithm, call it E, as an input. Ideally, we may desire E to be a strong pseudorandom permutation; however, since N can be sufficiently long (e.g., 128 or larger), constructing a block cipher that maps 2N-bit strings to 2N-bit strings can be expensive.

Therefore, we resort to the well-studied cipher block chaining (CBC) mode of operation to construct E from, Consider the CBC mode of operation. The nonce r is treated as the first plaintext block and is XORed with the initialization vector (IV) to insure IND-CPA security.

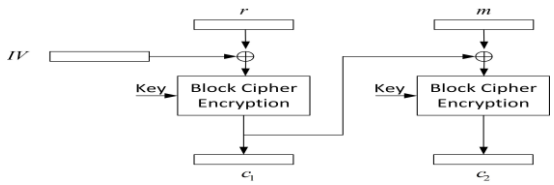


Fig. 2. The Cipher Block Chaining (CBC) mode of encryption used for message encryption. The random number, r, is treated as the first block of the plaintext.

**Security Model**

Recall signing and verifying algorithms, and challenged to generate a new massage-tag pair that will be accepted as valid, for a tag that has not been attached to the message by the signing oracle. Observe, however, that the message to be authenticated in our setup must also be encrypted. That is, what the intended user receives is a cipher text-tag pair, as opposed to plaintext-tag pair in the standard model. This implies that the adversary must come up with a valid cipher text-tag pair for a successful forgery. In what follows, we modify the standard model to address the difference between standard MACs and our MAC in which the message must be encrypted.

Let E be the underlying encryption algorithm. (We treat E as a black box that takes a plaintext message as an input and outputs its corresponding cipher text.) The signing oracle internally calls the encryption algorithm and outputs a ciphertexttag pair. That is, given an encryption algorithm E, on input a key k and a message m, the signing algorithm SE (k;m) outputs (c; _ ), where c is the cipher text corresponding to m and _ is its authentication tag.6 The verifying oracle must also be modified to properly model the system. That is, given the decryption algorithm D, on input a key k, a cipher text c, and an authentication tag _, the verifying oracle VD outputs a bit, with 1 standing for accept and 0 for reject. We ask for a basic validity condition, namely that authentic tags are accepted with probability one. That is, if (c; _) = SE (k;m), it must be the case that VD(k; c; _ ) = 1 for any encryption/decryption algorithms, key k, cipher text c, and authentication tag _ . As in the standard model, an adversary is a probabilistic polynomial time algorithm, A. The adversary is given oracle access to algorithms SE (k; _) and VD (k; _; _) for a random but hidden choice of k. A can query SE to generate a cipher text tag pair for a plaintext of her choice and ask the verifier VD to verify that (c; _) is a valid cipher text-tag pair.

## V. CONCLUSION

In this work, a new technique for authenticating short encrypted Messages is proposed. The fact that the message to be authenticated must also be encrypted is used to deliver a random nonce to the intended receiver via the cipher text. This allowed the design of an authentication code that benefits from the simplicity of unconditionally

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

*INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING*

*National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)*

*Alva's Institute of Engineering and Technology, Moodbidri*

*Vol. 3, Special Issue 1, April 2015*

secure authentication without the need to manage one-time keys. In particular, it has been demonstrated in this paper that authentication tags can be computed with one addition and a one modular multiplication. Given that messages are relatively short, addition and modular multiplication can be performed faster than existing computationally secure MACs in the literature of cryptography. When devices are equipped with block ciphers to encrypt messages, a second technique that utilizes the fact that block ciphers can be modeled as a strong pseudorandom permutation is proposed to authenticate messages using a single modular addition. The proposed schemes are shown to be orders of magnitude faster, and consume orders of magnitude less energy than traditional MAC algorithms. Therefore, they are more suitable to be used in computationally constrained mobile and pervasive devices.

## REFERENCES

[1]. J. Carter and M. Wegman, "Universal classes of hash functions," in Proceedings of the ninth annual ACM symposium on Theory of computing–STOC'77. ACM, 1977, pp. 106–112

[2]. M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," in Advances in Cryptology–CRYPTO'96, vol. 96, Lecture Notes in Computer Science. Springer, 1996, pp. 1–15.

[3]. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and Secure Message Authentication," in Advances in Cryptology– CRYPTO'99, vol. 1666, Lecture Notes in Computer Science. Springer, 1999, pp. 216–233

[4]. S. Sarma, S. Weis, and D. Engels, "RFID systems and security and privacy implications," Cryptographic Hardware and Embedded Systems- CHES 2002, pp. 1–19, 2003.

[5]. A Design Proposal of Security Architecture for Medical Body Sensor Networks Shu-Di Bao1, Yuan-Ting Zhang, Lian-Feng Shen

[6]. V. Shoup, "On fast and provably secure message authentication based on universal hashing," in Advances in Cryptology–CRYPTO'96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 313–328.