Unconditionally Secure Authenticated Encryption with Shorter Keys

Basel Alomair and Radha Poovendran

Network Security Lab
Electrical Engineering Department
University of Washington

Abstract. Confidentiality and integrity are two main objectives of security systems and the literature of cryptography is rich with proposed techniques to achieve them. To satisfy the requirements of a wide range of applications, a variety of techniques with different properties and performances have appeared in the literature. In this work, we address the problem of confidentiality and integrity in communications over public channels. We propose an unconditionally secure authenticated encryption that requires shorter key material than current state of the art. By combining properties of the integer field $\mathbb{Z}_p$ with the fact that the message to be authenticated is unknown to adversaries (encrypted), message integrity is achieved using a single modular multiplication. Against an adversary equipped with a single antenna, the adversary's probability of modifying a valid message in a way undetected by the intended receiver can be made an absolute zero.
After the description of the basic scheme and its detailed security analysis are completed, we describe an extension to the main scheme that can substantially reduce the required amount of key material.

1 Introduction and Related Work

When a secret message is to be transmitted through a public channel, the message must not be transmitted in clear text; otherwise, unintended receivers listening to the channel can infer the communicated secret. Fortunately, however, the problem of communicating secretly over public channels has been studied extensively, with a variety of good solutions available. The literature of cryptography is rich with proposed ciphers that transform plaintext messages into ciphertexts for the purpose of making the illegitimate receivers' task of breaking the confidentiality of the transmitted messages more challenging. Of course, the level of secrecy that can be achieved by different ciphers varies according to their specifications.

There are three main components in any cipher: a plaintext message to be communicated secretly, a ciphertext to be transmitted through the public channel, and a key that is used to transform the plaintext message into its corresponding ciphertext. The properties of the cipher that transforms plaintext messages into ciphertexts determine the level of secrecy that can be achieved. In his celebrated work, Shannon [1] put forth the notion of perfect secrecy and derived the necessary conditions to achieve it. Shannon proved that only one class of ciphers can achieve perfect secrecy, namely one-time pad (OTP) ciphers.

Alomair B. and Poovendran R. (2009).
Unconditionally Secure Authenticated Encryption with Shorter Keys.
In *Proceedings of the 7th International Workshop on Security in Information Systems*, pages 3-15
DOI: 10.5220/0002169600030015

Confidentiality, however, is only one objective of security systems; integrity is another one (integrity and authenticity will be used interchangeably throughout the rest of the paper). Therefore, in applications where adversaries can actively modify the transmitted message, encrypted messages are to be protected with mechanisms to ensure their integrity. Message authentication codes (MACs) are cryptographic primitives designed specifically to ensure message integrity. In authentication schemes, the term unconditional security is analogs to the term perfect secrecy in encryption scheme; they both imply security against computationally unbounded adversary. The first unconditionally secure authentication codes were invented by Gilbert *et al.* in [2]. The use of universal hash functions for the purpose of designing unconditionally secure authentication codes was introduced by Wegman and Carter [3]. Universal hash families were also used for the design of computationally secure MACs, as per Black *et al.* [4]. Other computationally secure MACs include, but are not limited to, CBCMAC [5], XORMAC [6], HMAC [7], and PMAC [8].

In this work, we address the problem of *authenticated encryption*. In authenticated encryption schemes, systems that combine message encryption and authentication are constructed. A generic technique to achieve authenticated encryption is to compose a system by combining an encryption scheme and an authentication scheme. There are three different approaches to construct generic authenticated encryption schemes, *encrypt and authenticate* ($E\&A$), *authenticate then encrypt* (AtE), and *encrypt then authenticate* (EtA). The transport layer of SSH uses a variant of $E\&A$ [9], SSL uses a variant of AtE [10], while IPSEC uses a variant of EtA [11]. Detailed discussions about generic constructions and their security relations can be found in [12, 13].

Dedicated authenticated encryption schemes are those designed to achieve the two goals directly, as opposed to combining two schemes in the generic construction. Proposals that use simple checksum or manipulation detection code have appeared in [14–16]. Such simple schemes, however, are known to be vulnerable to attacks [17]. Other block ciphers that combine encryption and message authenticity include [17–22]. In [17], Jutla proposed the integrity aware parallelizable mode (IAPM), an encryption scheme with authentication. The authenticated encryption requires a total of $m + 2$ block cipher evaluation for a message of m blocks. Gligor and Donescu proposed the XECB-MAC [18]. Rogaway *et al.* [19] proposed OCB: a block-cipher mode of operation for authenticated encryption.

Unconditional secrecy (for encryption) and unconditional security (for authentication), were not criteria of any of the previously proposed dedicated authenticated encryption schemes [17–22]. This is due to the necessary condition that the key must not be used for more than once to have a chance for unconditional secrecy/security. Using the same secret key more than once, however, imposes one more requirement on the system. That is, in addition to the desired confidentiality and integrity goals, the key must remain secret since it will be used for future operations. Consequently, classic MACs (e.g., [3, 5–7, 4, 8]) and authenticated encryption schemes (e.g., [17–22]) usually involve carefully designed iterations of complicated operations to provide the extra protection against key exposure due to multiple use of the same key.

In this paper, we construct an unconditionally secure authenticated encryption scheme. The proposed scheme is a one-time pad cipher that carries its own MAC in a way

that preserves perfect secrecy and provide unconditionally secure authenticity. By taking advantage of the fact that the message to be authenticated is secret, the authentication code is computed using a single multiplication operation. The security of the proposed scheme relies on properties of the integer field, $\mathbb{Z}_p$. Another unique property of the proposed scheme is that, against an adversary launching a man in the middle attack and equipped with a single antenna, message integrity can be guaranteed with probability one. Since the amount of key material in one-time pad systems is of special importance in practice, we propose an alternative approach that can substantially reduce the amount of required key material.

The rest of the paper is organized as follows. Section 2 provides a detailed description of our security definitions and assumptions about the adversary's knowledge and resources, along with a list of used notations and the simple preliminaries about the finite ring $\mathbb{Z}_p$ that will be used for our security analysis. Section 3 is dedicated to describing the details of the proposed authenticated encryption scheme. The security analysis of the proposed scheme is provided in Section 4. In Section 5 we compare our scheme to existing techniques and discuss some examples of potential applications of our scheme. Section 6 details our alternative approach that can reduce the amount of required key material. The paper is concluded in Section 7.

2 Notations and Communication Model

2.1 Notations

The following notations will be used throughout the rest of the paper.

- Throughout the rest of the paper, random variables will be represented by bold font symbols, whereas the corresponding non-bold font symbols represent specific values that can be taken by these random variables.
- For two sets $A \subset B$, we denote by $B \backslash A$ the set of elements in B that are not in A.
- For the set $\mathbb{Z}_p \stackrel{\text{def}}{=} \{0, 1, ..., p-1\}$, the set $\mathbb{Z}_p^*$ is defined to be the set of integers relatively prime (co-prime) to p.
- For an integer n, the set $n\mathbb{Z}$ will denote the set of integers that are multiples of n.
- For any two strings a and b, $(a \mid\mid b)$ denotes the concatenation operation.
- For the rest of the paper, $(+)$ and $(\times)$ represent addition and multiplication over $\mathbb{Z}_p$, even if the $(\mathrm{mod}\ p)$ part is dropped for simplicity.
- For any two integers a and b, $\gcd(a, b)$ is the greatest common divisor of a and b.
- For an element a in a ring R, the element a^{-1} denotes the multiplicative inverse of a in R, if it exists.

2.2 Model Assumptions and Security Goals

We assume the legitimate receiver and the adversary are listening to the same channel and the adversary has access to all bits transmitted in this channel. Furthermore, we assume the adversary has complete control over the communication channel. That is, we assume the adversary's ability to purposely flip transmitted bits at any position of

her choice. Legitimate users are assumed to share a secret key that allows them to communicate secretly as long as this key has not been exposed.

The proposed cipher is designed to achieve two goals. The first goal is perfect secrecy (in Shannon's sense). The cipher is perfectly secret if the ciphertext gives no information about the plaintext; i.e., the ciphertext and the plaintext are statistically independent. Formally, perfect secrecy is defined as [23]:

Definition 1 (Perfect Secrecy). *For a plaintext m and its corresponding ciphertext φ, the cipher is said to achieve perfect secrecy if $\Pr(\boldsymbol{m} = m|\boldsymbol{\varphi} = \varphi) = \Pr(\boldsymbol{m} = m)$ for all plaintext m and all ciphertext φ. That is, the a posteriori probability that the plaintext is m, given that the ciphertext φ is observed, is identical to the a priori probability that the plaintext is m.*

This definition implies that, given the ciphertext, a *computationally unbounded* adversary cannot do better than randomly guessing the plaintext. Throughout the rest of the paper, perfect secrecy, unconditional secrecy, and information-theoretic security will be used synonymously.

The second goal of our design is to provide message integrity by achieving resilience to active or message corruption attacks. To formally define resilience to active attacks we start with the definition of negligible functions [24]. A function $\gamma : \mathbb{N} \rightarrow \mathbb{R}$ is said to be negligible if for any nonzero polynomial p, there exists N_0 such that for all $N > N_0$, $|\gamma(N)| < \frac{1}{|p(N)|}$. That is, the function is said to be negligible if it converges to zero faster than the reciprocal of any polynomial function.

Definition 2 (Resilience to Active Attacks). *The cipher is said to be resilient to active attacks if and only if the probability of legitimate receivers accepting a corrupted ciphertext is a negligible function of the security parameter.*

The cipher is said to provide message integrity if it is resilient to active attacks. Unconditionally secure MACs demands more than resilience to active attacks. Just like perfect secrecy, unconditionally secure authentication implies security against computationally unbounded adversaries.

2.3 Preliminaries

An important property of prime integers is that, for any prime p, the integer ring $\mathbb{Z}_p$ is a field. Moreover, the fact that any field is an integral domain is critical for the integrity of our system.

Lemma 1. *Let p be a prime integer. Then, given an integer $k \in \mathbb{Z}_p^*$, for an r uniformly distributed over $\mathbb{Z}_p$, the value $\delta \equiv r \times k \pmod{p}$ is uniformly distributed over $\mathbb{Z}_p$.*

Lemma 1 is a direct consequence of the fact that, for a prime integer p, the ring, $\mathbb{Z}_p$, is a field.

3 The Simple Authenticated Encryption Scheme

Let p be a prime integer that the legitimate users have pre-agreed upon based on required security performance. The security parameter, ℓ, is the length of p in bits. Let

the legitimate users share a key $k = k_1||k_2$, where k_1 and k_2 are secret and chosen *independently* and *uniformly* from the sets $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively.

For any nonzero message $m \in \mathbb{Z}_p\backslash\{0\}$, define two functions $\varphi_{k_1}(m) : \mathbb{Z}_p\backslash\{0\} \rightarrow \mathbb{Z}_p$ and $\varphi_{k_2}(m) : \mathbb{Z}_p\backslash\{0\} \rightarrow \mathbb{Z}_p^*$ as follows:

$$\varphi_{k_1}(m) \equiv k_1 + m \pmod{p}, \tag{1}$$

$$\varphi_{k_2}(m) \equiv k_2 \times m \pmod{p}. \tag{2}$$

Then, the ciphertext of the plaintext message, m, is the concatenation of $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$. That is,

$$\varphi_k(m) = \varphi_{k_1}(m) \,||\, \varphi_{k_2}(m). \tag{3}$$

(Equivalently, the exclusive-or operation can be used instead of the addition operation in equation (1) without affecting the cipher's security properties).

Upon receiving the ciphertext, $\varphi'_k(m)$, the receiver extracts a plaintext, m', as follows:

$$m' = \varphi'_{k_1}(m) - k_1 \pmod{p}. \tag{4}$$

The integrity of the extracted m' is verified by the following check:

$$m' \times k_2 \stackrel{?}{\equiv} \varphi'_{k_2}(m) \pmod{p}. \tag{5}$$

The notations $\varphi'_k(m)$ and m' are to reflect the possibility of receiving a modified ciphertext. The ciphertext is considered valid if and only if the integrity check of equation (5) is passed. Wherever is convenient, $\varphi_{k_2}(m)$ will be referred to as the MAC of m (since its purpose is to provide message integrity).

4 Security Analysis

Since resilience to active attacks is the main contribution of the our scheme, we will first show that φ_{k_2} serves as a secure MAC for the plaintext m. More precisely, we will show that if the extracted message, m', passes the integrity check of equation (5), then the probability that $m' \neq m$ is negligible in the security parameter, ℓ.

Theorem 1. *Under Definition 2, the proposed authenticated encryption scheme is resilient to active attacks.*

Proof. There are two cases to be considered here, modifying φ_{k_1} alone, and modifying both φ_{k_1} and φ_{k_2}. Modifying φ_{k_2} alone, since it serves as a MAC, does not lead to extracting a modified plaintext.

Assume that only φ_{k_1} has been modified to φ'_{k_1}. Since k_1 is known to the receiver, this modification will lead to the extraction of an m' that is different than the transmitter's generated m; that is, $m' \equiv \varphi'_{k_1} - k_1 \pmod{p}$. Let $m' \equiv m + \delta \pmod{p}$, for some $\delta \in \mathbb{Z}_p\backslash\{0\}$. To be accepted by the receiver, m' must satisfy the following integrity check:

$$m' \times k_2 \equiv (m + \delta) \times k_2 \equiv (m \times k_2) + (\delta \times k_2) \stackrel{?}{\equiv} \varphi_{k_2} \equiv m \times k_2 \pmod{p}. \tag{6}$$

That is, m' will be accepted as a valid message only if the following condition holds:

$$\delta \times k_2 \equiv 0 \pmod{p}. \tag{7}$$

Since $\mathbb{Z}_p$ is an integral domain, k_2 is chosen from $\mathbb{Z}_p \backslash \{0\}$, and $\delta \not\equiv 0 \pmod{p}$ by assumption (since $\delta \equiv 0 \pmod{p}$ implies that the message has not been modified), equation (7) can never be satisfied. Consequently, any modification of φ_{k_1} "alone" will be detected by φ_{k_2} with probability *one*.

We now examine the case where both φ_{k_1} and φ_{k_2} are modified so that a false message will be validated. Assume that φ_{k_1} has been modified so that the extracted message becomes $m' = m + \delta \pmod{p}$, for some $\delta \in \mathbb{Z}_p \backslash \{0\}$. Also, assume that φ_{k_2} has been modified to $\varphi'_{k_2} = \varphi_{k_2} + \epsilon \pmod{p}$, for some $\epsilon \in \mathbb{Z}_p \backslash \{0\}$. The integrity of m' is verified using the received φ'_{k_2} as follows:

$$\varphi_{k_2} + \epsilon \equiv \varphi'_{k_2} \stackrel{?}{\equiv} m' \times k_2 \equiv (m + \delta) \times k_2 \equiv (m \times k_2) + (\delta \times k_2) \equiv \varphi_{k_2} + (\delta \times k_2) \pmod{p}. \tag{8}$$

By examining equation (8), the condition for validating the modified m' can be reduced to $\epsilon \equiv \delta \times k_2 \pmod{p}$. That is, the adversary's probability of successful forgery becomes:

$$\Pr(\text{successful forgery}) = \Pr\{\delta^{-1} \times \epsilon \equiv k_2 \pmod{p}\} \tag{9}$$

If k_2 is known, it is trivial to find two integers δ and ϵ that satisfy equation (9). However, since k_2 is unknown and uniformly distributed over $\mathbb{Z}_p^*$, by Lemma 1, the adversary's probability of successful forgery by modifying "both" φ_{k_1} and φ_{k_2} is equivalent to randomly guessing the value of k_2, which is equal to $1/(p-1)$.

Since an adversary modifying the ciphertext φ_{k_1} alone will be successful with probability *zero*, and an adversary modifying both ciphertexts φ_{k_1} and φ_{k_2} will be successful with probability $1/(p-1)$, for an ℓ-bit prime p, the adversary's probability of success is at most $1/2^{\ell-1}$, a negligible function in the security parameter ℓ. Therefore, by Definition 2, the proposed scheme is resilient to active attacks. □

Theorem 1 implies that the first requirement of our design, namely message integrity, is satisfied. Observe that not only the proposed scheme is resilient to active attacks, the adversary cannot do better than guessing the value of k_2 to forge a valid MAC, regardless of how much computational power she possesses. Otherwise stated, the integrity of the proposed scheme is unconditionally secure.

The next theorem addresses the second requirement of our design, confidentiality.

Theorem 2. *The proposed scheme achieves perfect secrecy (in Shannon's sense).*

Proof. Let $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ be uniform, independent random variables distributed over $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively. By equation (1), for any given plaintext $m \in \mathbb{Z}_p \backslash \{0\}$, as a result of the uniform distribution of $\boldsymbol{k_1}$ over $\mathbb{Z}_p$, the resulting $\boldsymbol{\varphi_{k_1}}$ is uniformly distributed over $\mathbb{Z}_p$. Similarly, as a result of the uniform distribution of $\boldsymbol{k_2}$ over $\mathbb{Z}_p^*$, by Lemma 1, the resulting $\boldsymbol{\varphi_{k_2}}$ is uniformly distributed over $\mathbb{Z}_p^*$. Consequently, for any arbitrary

$\varphi_{k_1} \in \mathbb{Z}_p$ and an arbitrary $\varphi_{k_2} \in \mathbb{Z}_p^*$, the probabilities $\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1})$ and $\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2})$ are $1/p$ and $1/(p-1)$, respectively.

Now, given a specific value of a plaintext message, $\boldsymbol{m} = m$, the probability that the ciphertext $\boldsymbol{\varphi_{k_1}}$ takes a specific value φ_{k_1} is:

$$\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1} | \boldsymbol{m} = m) = \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m) = 1/p = \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}). \quad (10)$$

Similarly, for a specific $\boldsymbol{m} = m$, the probability that the ciphertext $\boldsymbol{\varphi_{k_2}}$ takes a specific value φ_{k_2} is:

$$\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2} | \boldsymbol{m} = m) = \Pr(\boldsymbol{k_2} = \varphi_{k_2} \times m^{-1}) = \frac{1}{p-1} = \Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2}). \quad (11)$$

Equations (10) and (11) hold since, by design, $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ are uniformly distributed over $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively. The existence of m^{-1}, the multiplicative inverse of the message m modulo p, is a direct consequence of the fact that $m \in \mathbb{Z}_p^*$.

Now, Bayes' theorem, combined with equations (10) and (11), can be used to show that:

$$\Pr(\boldsymbol{m} = m | \boldsymbol{\varphi_{k_1}} = \varphi_{k_1}) = \frac{\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1} | \boldsymbol{m} = m) \Pr(\boldsymbol{m} = m)}{\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1})} = \Pr(\boldsymbol{m} = m), \quad (12)$$

$$\Pr(\boldsymbol{m} = m | \boldsymbol{\varphi_{k_2}} = \varphi_{k_2}) = \frac{\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2} | \boldsymbol{m} = m) \Pr(\boldsymbol{m} = m)}{\Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2})} = \Pr(\boldsymbol{m} = m). \quad (13)$$

Equations (12) and (13) show that the a posteriori probabilities that the plaintext message is m, given that the observed ciphertexts are φ_{k_1} and φ_{k_2}, are identical to the a priori probability that the plaintext message is m. Hence, both ciphertexts *individually* provide perfect secrecy. However, since they are both an encryption of the same message, there might be information leakage about the plaintext revealed by the combination of φ_{k_1} and φ_{k_2}. One way of measuring how much information is learned by the observation of two quantities is the notion of mutual information. Consider an arbitrary $\varphi_{k_1} \in \mathbb{Z}_p$ and arbitrary $\varphi_{k_2} \in \mathbb{Z}_p^*$. Then, for independent $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ uniformly distributed over $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively, we get:

$$\Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}, \boldsymbol{\varphi_{k_2}} = \varphi_{k_2}) =$$

$$= \sum_m \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}, \boldsymbol{\varphi_{k_2}} = \varphi_{k_2} | \boldsymbol{m} = m) \Pr(\boldsymbol{m} = m) \quad (14)$$

$$= \sum_m \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m, \boldsymbol{k_2} = \varphi_{k_2} \times m^{-1}) \Pr(\boldsymbol{m} = m) \quad (15)$$

$$= \sum_{m} \Pr(\boldsymbol{k_1} = \varphi_{k_1} - m) \Pr(\boldsymbol{k_2} = \varphi_{k_2} \times m^{-1}) \Pr(\boldsymbol{m} = m) \tag{16}$$

$$= \sum_{m} \frac{1}{p} \cdot \frac{1}{p-1} \Pr(\boldsymbol{m} = m) = \Pr(\boldsymbol{\varphi_{k_1}} = \varphi_{k_1}) \Pr(\boldsymbol{\varphi_{k_2}} = \varphi_{k_2}). \tag{17}$$

Equation (16) holds due to the independence of $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$, equation (17) holds due to the uniform distribution of $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ and the uniform distribution of $\boldsymbol{\varphi_{k_1}}$ and $\boldsymbol{\varphi_{k_2}}$, respectively. Consequently, $\boldsymbol{\varphi_{k_1}}$ and $\boldsymbol{\varphi_{k_2}}$ are independent and, thus, their mutual information is *zero* [25]. That is, observing both ciphertexts φ_{k_1} and φ_{k_2} gives no extra information about the plaintext than what the ciphertexts φ_{k_1} and φ_{k_2} give individually.

By definition of one-time pad ciphers, the keys $k = k_1||k_2$ and $k' = k'_1||k'_2$ used for two different encryption operations must be random and independent. Thus, the independence of the two ciphertexts follows directly from the independence of the keys. □

So far, we have shown that φ_{k_2}, using a single modular multiplication, serves as unconditionally secure MAC of the encrypted message, m, without affecting its perfect secrecy. The next section is devoted to comparing the proposed scheme to existing approaches that can achieve the same goals, and to discussing some potential applications where the proposed scheme can be useful.

5 Discussions and Applicability

Consider the classic use of universal hash families for unconditionally secure message authentication. Given a secret key, $(a, b) \in \mathbb{Z}_p^2$, a message, m, is authenticated by the code, $MAC(m) \equiv am + b \pmod{p}$. That is, unconditionally secure integrity is accomplished with two keys, a and b, and two modular operations in $\mathbb{Z}_p$, one addition and one multiplication. With the same two keys and the same two operations, the proposed scheme can achieve the same level of message integrity, *in addition to perfect secrecy*. In other words, our scheme provides additional perfect secrecy with absolutely no extra key material and no extra computational effort.

To get the same level of message secrecy and integrity, without using the proposed scheme, one will need to encrypt the message with a one-time key, then implement the encrypt-then-authenticate approach with an unconditionally secure MAC to authenticate the ciphertext. Therefore, one will need three keys, one for encryption and two for authentication, in addition to computing one modular multiplication and two modular addition. Therefore, the proposed scheme can achieve the same security goals with less key material and fewer computations. Since key length requirement is the most important issue in one-time pad systems, a 33.3% reduction of key length requirement, for the same security results using less computational effort, is a considerable improvement. A further substantial key reduction is described in Section 6.

The new idea introduced here is to combine encryption and authentication using one-time key to achieve both perfect secrecy and unconditional message integrity in

one round. By taking advantage of the fact that the message to be authenticated is secret, properties of the integer field $\mathbb{Z}_p$ are used to authenticate the message with a single key using one multiplication operation. To the best of our knowledge, the idea of authenticating secret messages using a single modular multiplication, as proposed here, has never appeared in the literature of cryptography.

Moreover, recall that, by Theorem 1, any modification of only one of φ_{k_1} or φ_{k_2} will be detected with probability one. If the sender has the ability to transmit the encryption, φ_{k_1}, and the MAC, φ_{k_2}, over two different channels, at which the adversary controls only one of them, message integrity is guaranteed with probability *one*. This includes applications where the adversary is equipped with only one antenna, and applications where frequency hopping techniques are used for transmission at which the adversary does not detect both channels. With the increase spreading of frequency hopping techniques in the context of providing security for a variety of applications in wireless communications (see, e.g., [26]), the proposed idea might be useful for providing a strong notion of message integrity in some applications.

5.1 Potential Applications

Even though OTP systems are considered impractical in many situations due to their key requirement, they are used in exchanging highly confidential diplomatic or military information. In fact, the hotline between Moscow and Washington D.C., established in 1963 after the Cuban missile crisis, used teleprinters protected by a commercial OTP system. Each country prepared the keying tapes used to encode its messages and delivered them via their embassy in the other country [27]. Given the simplicity and high level of integrity of the proposed scheme, we believe it is a suitable method to provide integrity to OTP ciphers in cases where both unconditional secrecy and integrity are desired.

In a totally different direction, consider a scenario where a businessman is in a trip and needs to send an urgent confidential message to his broker (e.g.,“buy 1,000,000 shares”). In addition to authenticity, the confidentiality of this message might be of extreme importance to the businessman. Given the simple computations of the proposed scheme (single addition and multiplication), the task can be accomplished, with unconditional secrecy and integrity, using a basic calculator (or even by hand). If the businessman is equipped with a mobile device that can store few megabytes of data (for the secret key), he can implement the proposed technique to transmit multiple authenticated encrypted messages before exhausting his key, without the need to carry sophisticated devices.

In another application, consider a battery powered, computationally constrained sensor node that is setup to send updated measurements to its anchor node every hour. Assuming each measurement is 20-byte long, and the node is preloaded with only one megabyte long secret key. The node can use the proposed scheme to send unconditionally secure measurements in a perfectly secret manner, for about three years before it exhausts its preloaded secret key. On the other hand, if the existing method of encrypting with OTP followed by authenticating using universal hash families, as described earlier, the lifetime of the system will be reduced to bout two years. Furthermore, the

reduction in key usage detailed in the next section can almost double the lifetime of the system.

6 Reducing Key Size

In this section, we discuss a modification of the proposed scheme that can substantially reduce the length of the authentication key, k_2, in the proposed scheme.

Let the message to be encrypted be $m \in \mathbb{Z}_{2^n} \backslash p\mathbb{Z}$ (as opposed to $m \in \mathbb{Z}_p \backslash \{0\}$ as in the original scheme), for an arbitrary message length, n. Further, let n (the length of the message in bits) be greater than ℓ (the length of p in bits). Then, for $k_1 \in \mathbb{Z}_{2^n}$ and $k_2 \in \mathbb{Z}_p^*$, define two functions $\varphi_{k_1}(m) : \mathbb{Z}_{2^n} \backslash p\mathbb{Z} \rightarrow \mathbb{Z}_{2^n}$ and $\varphi_{k_2}(m) : \mathbb{Z}_{2^n} \backslash p\mathbb{Z} \rightarrow \mathbb{Z}_p^*$ as follows:

$$\varphi_{k_1}(m) \equiv k_1 + m \pmod{2^n}, \tag{18}$$

$$\varphi_{k_2}(m) \equiv k_2 \times m \pmod{p}. \tag{19}$$

As before, the ciphertext is the concatenation of $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$. The obvious problem here is that all messages that are different by multiples of p will be mapped to the same $\varphi_{k_2}(m)$ and, unlike the original scheme where $m \in \mathbb{Z}_p^*$, that does not imply that the messages are the same. That is, since $m \in \mathbb{Z}_{2^n} \backslash p\mathbb{Z}$, $m \pm p\mathbb{Z} \not\equiv m \pmod{2^n}$, while $\varphi_{k_2}(m \pm p\mathbb{Z}) \equiv \varphi_{k_2}(m) \pmod{p}$. Therefore, any modification of the message by multiples of p will go undetected, leading to the acceptance of modified messages. Next, we describe our solution to this problem.

6.1 Unknown Modulus

Recall that, by equation (7), an adversary modifying $\varphi_{k_1}(m)$ alone is undetected if and only if

$$\delta \times k_2 \equiv 0 \pmod{p}, \tag{20}$$

for some $\delta \in \mathbb{Z}_{2^n} \backslash \{0\}$ of the adversary's choice. Furthermore, by equation (9), an adversary modifying both $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$ is undetected if and only if

$$\delta^{-1} \times \epsilon \equiv k_2 \pmod{p}, \tag{21}$$

for some non-zero δ and ϵ of the adversary's choice.

Therefore, if the prime modulus, p, is unknown to the adversary, then the probability of successful forgery by modifying $\varphi_{k_1}(m)$ alone is equivalent to guessing the prime p. This is because only if $\delta \in p\mathbb{Z}$ it will satisfy equation (20). Now, even if the adversary is assumed to know the length of the prime integer, say ℓ-bits, the prime number theorem shows that the number of primes less than 2^ℓ can be approximated by [28]:

$$\pi(2^\ell) \approx 2^\ell / \ell \ln(2), \tag{22}$$

where $\pi(x)$ is the prime-counting function. That is, the probability of randomly guessing the used prime integer is an exponentially decreasing function in ℓ. (The adversary can also increase her chances by multiplying multiple ℓ-bit primes, but devices will

overflow rather quickly. For example, using MATLAB 2007, multiplying 10 primes of length 100-bits caused an overflow.)

On the other hand, solving equation (21) is still equivalent to guessing the value of k_2. Hence, the probability of successful forgery by modifying both $\varphi_{k_1}(m)$ and $\varphi_{k_2}(m)$ is still $1/(p-1)$, as in the original scheme. Therefore, the probability of successful forgery, in the modified scheme, is a negligible function in the security parameter and, thus, the modified scheme is also resilient to active attacks.

However, it is uncommon in cryptographic literature to assume that the used modulus, p, will remain secret. To overcome this problem, we propose below a method to secretly exchange a new prime modulus (to be used for authentication) for each operation.

6.2 Exchanging the Modulus Secretly

Assume that the prime modulus, p, has not been agreed-upon and is unknown to the intended receiver. Given the length of φ_{k_1}, say n bits, the receiver uses n bits of secret key material to construct k_1. By subtracting the constructed k_1 from the received φ_{k_1} modulo 2^n (or alternatively XORing k_1 with φ_{k_1} if the XOR operation is used for encryption), the receiver can correctly decrypt the transmitted message. Assuming that p is embedded somewhere in the encrypted message, the receiver can extract it and use it for authentication. Since the message is sent in a perfectly secret manner, the adversary can do no better than randomly guessing the value of p.

With this described approach, the authentication key, k_2, can be much shorter than the length of the message. For example, a 128-bit key can be used to authenticate an arbitrarily long message with high level of integrity. Therefore, this approach can substantially reduce the amount of required key material.

7 Conclusions

In this work, the problem of authenticated encryption is addressed. An OTP cipher that carries its own MAC in a way that preserves perfect secrecy is proposed. When short messages need to be encrypted and authenticated, the proposed scheme can be implemented using devices with extremely limited computational power. In fact, the operation is simple to the point it can be performed by hand or using a basic calculator. Moreover, unlike previous authenticated encryption proposals, the proposed scheme is designed to achieve unconditional secrecy and unconditional integrity.

The proposed cipher is shown to be secure in a novel way based on unique properties of the integer field $\mathbb{Z}_p$ and the fact that the message to be authenticated is encrypted. The utilization of these properties allowed the design of a perfectly secret authenticated encryption scheme that is computed by performing a single modular addition and a single modular multiplication. Since key lengths is a particularly important issue in one-time key systems, we propose an extension to the main scheme that can substantially reduce the required key length, without affecting the security of the scheme.

References

1. Shannon, C.: Communication Theory and Secrecy Systems. Bell Telephone Laboratories (1949)
2. Gilbert, E., MacWilliams, F., Sloane, N.: Codes which detect deception. Bell System Technical Journal 53 (1974) 405–424
3. Wegman, M., Carter, J.: New classes and applications of hash functions. Foundations of Computer Science, 1979., 20th Annual Symposium on (1979) 175–182
4. Black, J., Halevi, S., Krawczyk, H., Krovetz, T., Rogaway, P.: UMAC: Fast and Secure Message Authentication. Advances in Cryptology-Crypto'99: 19th Annual International Cryptology Conference, Santa Barbara, California, USA August 15-19, 1999 Proceedings (1999)
5. US National Bureau of Standards: DES Modes of Operation. Federal Information Processing Standard (FIPS) Publication 81 Available as http://www.itl.nist.gov/fipspubs/fip81.htm (December 1980)
6. Bellare, M., Guerin, R., Rogaway, P.: XOR MACs: New methods for message authentication using finite pseudorandom functions. Advances in Cryptology–CRYPTO95 (LNCS 963) (1995) 15–28
7. Bellare, M., Canetti, R., Krawczyk, H.: Keying hash functions for message authentication. Advances in Cryptology–CRYPTO 96 (1996) 1–15
8. Rogaway, P., Black, J.: PMAC: Proposal to NIST for a parallelizable message authentication code (2001)
9. Ylonen, T., Lonvick, C.: The Secure Shell (SSH) Transport Layer Protocol. Technical report, (RFC 4253, January 2006)
10. Freier, A., Karlton, P., Kocher, P.: The SSL Protocol Version 3.0 (1996)
11. Kent, S.: RFC4303: IP encapsulating security payload (ESP),. Internet EFC. STD. FYI/BCP archives. December (2005)
12. Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology–ASIACRYPT (2000) 531–545
13. KRAWCZYK, H.: The order of encryption and authentication for protecting communications(or: How secure is SSL?). Advances in Cryptology–CRYPTO 2001 (2001) 310–331
14. Meyer, C., Matyas, S.: Cryptography: A New Dimension in Computer Data Security. John Wiley & Sons (1982)
15. Kohl, J., Neuman, C.: The Kerberos Network Authentication Service (V5). Technical report, RFC 1510, September 1993 (1993)
16. Gligor, V., Donescu, P.: Integrity-Aware PCBC Encryption Schemes. Security Protocols: 7th International Workshop, Cambridge, Uk, April 19-21, 1999: Proceedings (2000)
17. Jutla, C.: Encryption modes with almost free message integrity. Advances in Cryptology–EUROCRYPT 2045 (2001) 529–544
18. Gligor, V., Donescu, P.: Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes. Fast Software Encryption: 8th International Workshop, FSE 2001, Yokohama, Japan, April 2-4, 2001: Revised Papers (2002)
19. Rogaway, P., Bellare, M., Black, J.: OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption. ACM Trans. Inf. Syst. Secur. 6 (2003) 365–403
20. Ferguson, N., Whiting, D., Schneier, B., Kelsey, J., Lucks, S., Kohno, T.: Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive, Fast Software Encryption 2003, LNCS 2887 (2003)

21. Kohno, T., Viega, J., Whiting, D.: CWC: A high-performance conventional authenticated encryption mode. Fast Software Encryption (2004) 408–426
22. Bellare, M., Rogaway, P., Wagner, D.: The EAX mode of operation. Fast Software Encryption (2004) 389–407
23. Stinson, D.: Cryptography: Theory and Practice. CRC Press (2006)
24. Goldreich, O.: Foundations of Cryptography. Cambridge University Press (2001)
25. Cover, T., Thomas, J.: Elements of Information Theory. Wiley-Interscience New York (2006)
26. Strasser, M., Popper, C., Capkun, S., Cagalj, M.: Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping. In: IEEE Symposium on Security and Privacy, 2008. SP 2008. (2008) 64–78
27. Kahn, D.: The codebreakers. Weidenfeld and Nicolson (1974)
28. Cormen, T., Leiserson, C., Rivest, R.: Introduction to Algorithms. McGraw-Hill (1999)