cryptographic functions, the monitoring of multiple message-image pairs can show the value of the hashing key. Since the hashing key is used frequently in computationally secure MACs, the revealing of the hashing key will lead to breaking the safety of the MAC. While, processing the compressed image with a cryptographic primitive is required for the safety of this class of MACs. This implies that unconditionally secure MACs based on universal hashing are more capable than computationally secure ones. On the other hand, unconditionally secure universal hashing-based MACs are considered unrealistic in the latest applications, due to the strain of accessing one-time keys.

In our day to day life, there is an increasing demand for the deployment of networks consisting of a collection of small apparatus. The main concept of such apparatus is to transfer short messages, in many empirical applications. For example, a sensor network which can be deployed to observe certain events and report some assembled data. In some sensor network applications, reported data consist of short confidential measurements such as a sensor network deployed in a battlefield. The confidentiality and integrity of reported events are of critical importance, in such applications.

II. METHODS AND MATERIAL

A. Proposed System

Let *N*-1 be an upper bound on the length, in bits, of communicated messages. That is, messages to be authenticated should not be exceed than (*N*-1)-bit long. Select p to an *N*-bit long prime integer. Choose an integer k_s uniformly at random from the multiplicative group $\mathbb{Z}_p^*$; k_s is the secret key of the scheme. The prime integer, p, and the secret key, k_s are given out to the trusted parties and will be used for message protection. Note that the value of k_s is the secret key.

Let Ɛ be any IND-CPA secure encryption algorithm and m be a short message that is to be exchanged to the planned recipient in a confidential manner. As an alternative of using a regular MAC algorithm, consider the following steps. Choose message m and a random nonce $r \in \mathbb{Z}_p$ as an input. Assume that integers representing discrete messages are also distinct, which can be done by suitable encoding messages.

Now, r is added to the message and the output will be m || r, where "||" represents the concatenation operation, goes to the encoding algorithm as an input. Then, the authentication tag of message m can be evaluated as follow:

$$\mathcal{T} \equiv mk_s + r \pmod{p}$$

B. Encrypting with Pseudorandom Permutations

The main concept of this method is that the input-output relation of the encryption operation can be realized as a pseudorandom permutation.

i. The Advanced Method

Let $\mathcal{F} : \{0,1\}^N \longrightarrow \{0,1\}^N$ be the function symbolizing the block cipher. We presume that $\mathcal{F}$ acts as a strong pseudorandom permutation, a representative supposition modern block ciphers are believed to satisfy. Presume further that communicated messages are *N*-bit long.

ii. Message Encryption

Let m be a short message that is to be transferred to the planned recipients in a secured way. A random nonce $r \in \mathbb{Z}_{2N}$ is selected for every message to be transferred.

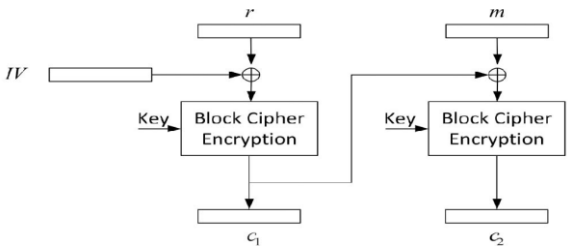

Fig. 1. The cipher block chaining mode of encryption used for message encryption. The random number, r, is treated as the first block of the plaintext.

Then, the concatenation of r and m goes to the encoding algorithm, say $\mathcal{E}$, as an input. Let, consider $\mathcal{E}$ to be a strong pseudorandom permutation and N can be adequately long (e.g., 128 or larger), building a block cipher that maps 2*N*-bit strings to 2*N*-bit strings can be overpriced.

Fig. 1, represents the CBC mode of operation. The nonce *r* is standard as the initial plaintext block and is XORed with the initialization vector (IV) to provide IND-CPA protection. The initial ciphertext block,

$$C1= \mathcal{F}k\varepsilon(IV \oplus cr)$$

to produce the second cipher block, it is then XORed with the second plaintext block, m in our construction

$$C2= \mathcal{F}k\varepsilon(c_1+m)$$

Here $k\varepsilon$ is the key corresponding to the block cipher.

$$C= \varepsilon(r,m)=IV||c_1||c_2$$

As the cipher text it is then transmitted to the intended receiver.

iii. Message Authentication

The authentication becomes simpler than the one in the previous section along the encryption described above.

$$\mathcal{T} \equiv m + r \pmod{2^N}$$

III. RESULTS AND DISCUSSION

A. Performance Discussion

Assuming devices are equipped already with a secure block cipher to encrypt messages, the authentication technique of this section requires only one modular addition. While addition is performed in O(n) time, the fastest integer multiplication algorithms typically require O(n log n log log n) time. The authentication technique of this section is at least O(logn log logn) faster. By absorbing large constants Complexity analysis can be inaccurate. This is indeed the case in comparing the basic scheme of previous Section to the scheme of this section. For n =32, the simple addition of this scheme runs in about 0.02 cycles/byte5 as opposed to the 1.5 cycles/ byte of the previous scheme. Due to the modular reduction it is better than O(logn log logn). While reduction modulo a prime integer is a nontrivial operation, reduction modulo 2n can be performed by simply stopping at the nth bit. We focus on two of the prominent single-pass authenticated encryption schemes, the IAPM and the OCB. Both IAPM and OCB require pre-processing plaintext blocks before block cipher encryption, to give performance comparisons with authenticated encryption primitives. For example, IAPM requires XORing plaintext blocks with pairwise differentially uniform sequences named si. Each si is generated by performing modular multiplication over the finite field $\mathbb{Z}_p$, similar to the multiplication of our first scheme of third Section. In the OCB mode of operation, each message block, M[i] is XORed with a string the authors denoted as Z[i]. Take the reminder after dividing the multiplication result by a fixed irreducible polynomial and the computation of each Z[i] requires the generation of a Gray code γ_i, multiply two polynomials over GF2^n. Without any pre-processing, the proposed scheme, plaintext blocks go to the block cipher. The scheme proposed here is the first scheme that does not require multiplication operations either before block cipher encryption, such as single-pass authenticated encryption primitives, or after block cipher encryption, such as generically composed authenticated encryption systems. As the first block cipher call both IAPM and OCB also require the encryption of a nonce, which is similar to the first block cipher call in our scheme. After the whitened plaintext blocks are encrypted, an additional block cipher call is needed to encrypt the resulting check-sum and is computed. Both IAPM and OCB require two additional block cipher calls, as opposed to a single additional block cipher call in the proposed scheme to block cipher calls required for encrypting the plaintext itself. Therefore, an extra block cipher call will contribute significantly to the total power consumption of the scheme in which plaintext messages occupy only a single block.

Before we give formal security analysis of the proposed technique, we give a formal security model that will be used for the analysis.

B. Security Model

Remind that, to model the protection of a message authentication scheme in the standard setup, a probabilistic polynomial time adversary, A, is given oracle access to the 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. 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 against to plaintext-tag pair in the standard model. This implies that the adversary must come up with a valid ciphertext-tag pair for victories counterfeit.

Let ε *be* the underlying encryption algorithm. The signing oracle internally calls the encryption algorithm and outputs a ciphertext-tag pair. That is, given an encryption algorithm ε, on input a key k and a message m, the signing algorithm, where c is the ciphertext representing to m and τ is its authentication tag. The validating oracle must also be changed to properly model the system. That is, given the decryption algorithm $\mathcal{D}$, on input a key k, a ciphertext c, and an authentication tag τ, the verifying oracle $\mathcal{VD}$ outputs a bit, with 1 standing for accept and 0 for reject. For a basic verify condition, namely that authentic tags are accepted with probability one.

As in the standard model, an adversary is a probabilistic polynomial time algorithm, $\mathcal{A}$. Formally, $\mathcal{A}$'s attack on the scheme is described by the following experiment:

1. A random string is selected as the shared secret, *k*.
2. Suppose A makes a signing query m. The oracle calculates (c, τ), the ciphertext-tag pair, and returns it to $\mathcal{A}$.
3. Suppose $\mathcal{A}$ makes a validate query (c, τ). The oracle evaluates the decision $d = \mathcal{VD}(k, c, \tau)$ and returns it to $\mathcal{A}$.

The output of running the experiment in the presence of an adversary is used to describe protection. We say that $\mathcal{A}$, is successful if it makes a validate query (c, τ) which is accepted, for a (c, τ) that has not been outputted by the signing oracle.

IV. CONCLUSION

In this work, we projected a new method for authenticating short encrypted messages. This method is based on the fact, the message to be authenticated must also be encrypted is used to distribute a random nonce to the planned recipient via the ciphertext. This authorized the design of an authentication code that benefits from the simplicity of unconditionally secure authentication without the need to manage one-time keys. It has been confirmed in this paper that authentication tags can be evaluated with a single addition and modular multiplication, in specific. If the messages are quite short, addition and modular multiplication can be executed earlier than existing computationally secure MACs in the literature of cryptography. A second method that utilizes the reality that block ciphers can be modelled as strong pseudorandom permutations is proposed to authenticate messages using a single modular addition, when devices are equipped with block ciphers to encrypt messages. The proposed schemes are shown to be orders of magnitude faster, and use orders of magnitude less energy than traditional MAC algorithms. Therefore, they are more suitable to be used in computationally constrained mobile and pervasive devices.

V. REFERENCES

[1] B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes: Security of Authentication Based on a Universal Hash-Function Family," J. Math. Cryptology, vol. 4, no. 2, 2010.

[2] B. Preneel and P.V. Oorschot, "MDx-MAC and Building Fast MACs from Hash Functions," Proc. 15th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '95), vol. 963, pp. 1-14, 1995.

[3] J. Katz and Y. Lindell, Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

[4] M. Furer, "Faster Integer Multiplication," Proc. ACM Symp. Theory of Computing (STOC '07), p. 66, 2007.

[5] P. Rogaway, M. Bellare, and J. Black, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption," ACM Trans. Information and System Security, vol. 6, no. 3, pp. 365-403, 2003.