EHE: nonce misuse-resistant message authentication

Sergey Agievich

Research Institute for Applied Problems of Mathematics and Informatics

Belarusian State University

agievich@{bsu.by,gmail.com}

Abstract

We propose a nonce misuse-resistant message authentication scheme called EHE (Encrypt-Hash-Encrypt). In EHE, a message-dependent polynomial is evaluated at the point which is an encrypted nonce. The resulting polynomial hash value is encrypted again and becomes an authentication tag. We prove the prf-security of the EHE scheme and extend it to two authenticated encryption modes which follow the "encrypt-then-authenticate" paradigm.

1 Introduction

Let $\mathbb{F}$ be a finite field of $N \gg 1$ elements. Polynomial hashing over $\mathbb{F}$ is defined as follows: A message X to be hashed is transformed into a polynomial $f_X(\lambda) \in \mathbb{F}[\lambda]$, this polynomial is evaluated at some point $H \in \mathbb{F}$, the result of evaluation becomes a hash value of X. Further we suppose that the polynomial f_X has positive degree, its constant terms equals 0, different messages are transformed into different polynomials. Usually the message X is divided into blocks which determine the coefficients of f_X. The shorter X, the lower the degree of f_X. Let messages be rather short and $\deg f_X \le d \ll N$.

If H is chosen uniformly at random from $\mathbb{F}$, then the hash values of different messages X and X' coincide with only small probability:

$$\Pr\{f_X(H) = f_{X'}(H)\} = \Pr\{H \text{ is a root of } f_X - f_{X'}\} \le \frac{d}{N}. \tag{1}$$

This simple fact supports security of message authentication schemes based on polynomial hashing. Possibly the most well-known scheme of this type was proposed by M. Wegman and J. Carter in [11] and refined by V. Shoup in [9]. Following [1], we call it WCS, by the first letters of the authors' names.

The WCS scheme was successfully used in GCM, a widely deployed authenticated encryption (AE) mode. GCM was introduced in [5] and standardized in [2]. Recall that an AE mode augments an authentication scheme with encryption one.

Describe WCS with inessential simplifications. The point H becomes a random secret key. The additional key is a random permutation π acting on $\mathbb{F}$. An authentication tag T (a key-dependent hash value) of X is calculated using a unique nonce $S \in \mathbb{F}$ as follows:

$$T = f_X(H) + \pi(S).$$

To instantiate WCS, π is usually chosen as an encryption permutation of some block cipher and H is usually a result of encryption of a fixed element $c \in \mathbb{F}$ using π. This is how WCS is instantiated in GCM.

The uniqueness of nonces is essential. Indeed, if the tags $T = f_X(H) + \pi(S)$ and $T' = f_{X'}(H) + \pi(S')$ are calculated with $X \neq X'$ but $S = S'$, then an adversary can effectively determine H as one of the roots of the polynomial equation $f_X(H) - f_{X'}(H) = T - T'$. After determining H, the adversary finds $\pi(S) = T - f_X(H)$ and then can calculate the tag $T'' = f_{X''}(H) + \pi(S)$ of any X''.

The described situation, the significant loss of security after some event, we call *the security collapse*. Message authentication schemes collapse in different ways. For example, in the schemes of type CBC-MAC (see, for example, [8]) an internal collision, which occurs after processing about $\sqrt{N}$ message blocks, allows to perform a selective forgery, that is, to forge tags of special messages. For comparison, WCS collapses much more seriously: universal forgery after only a single nonce repetition.

In the mentioned standard [2] nonce repetition is considered as misuse of GCM. The standard proposes to solve the misuse problem at the cryptoengineering layer. But it is preferable to solve such problems cryptographically, by designing authentication schemes or AE modes which security does not collapse so much after nonce repetition. Such schemes and modes are called *nonce misuse-resistant*.

The GCM mode follows the "encrypt-then-authenticate" paradigm. In this paradigm the nonce misuse-sensitive scheme WCS cannot provide misuse-resistance of the whole mode. Resistance appears if we turn the paradigm into "authenticate-then-encrypt" keeping WCS. This approach was successfully implemented in the GCM-SIV mode [3]. Unfortunately, due to the paradigm shift, GCM-SIV requires an additional pass over the protected data.

In this paper we propose another approach: strengthening the basic message authentication scheme. In Section 2 we introduce a nonce misuse-resistant scheme called EHE. We justify its security and then, in Section 3, discuss details of its instantiation based on a block cipher. In Section 4 we extend EHE to AE modes which preserve the "encrypt-then-authenticate" paradigm. We denote these modes as AE[EHE]. Note that the first mode was standardized in [10] under the name `belt-datawrap`. We accompanied it with a rather cumbersome proof of security. In this paper the proof is drastically simplified.

2 The EHE scheme

In the proposed EHE scheme, a key is a pair of permutations π_1 and π_2 acting on $\mathbb{F}$. A message X to be authenticated is represented by a polynomial f_X which satisfies the previous restrictions. A tag T is calculated using a nonce $S \in \mathbb{F}$ as a value of the following function:

$$\varphi[\pi_1, \pi_2](X, S) = \pi_2(f_X(\pi_1(S))).$$

In this function we start with the permutation π_1, continue with polynomial hashing and finish with the permutation π_2. The permutations mean block encryption, so we deal with the Encrypt-Hash-Encrypt cascade or EHE in short.

In contrast to WCS, the polynomials f_X are evaluated not in a fixed point $H = \pi(c)$ but generally in different points $H = \pi_1(S)$. It is well known (see for example [4, Theorem 6.13]) that the polynomial $g(\lambda, \lambda') = f_X(\lambda) - f_{X'}(\lambda') \in \mathbb{F}[\lambda, \lambda']$ has at most $\deg g \cdot N = \max(\deg f_X, \deg f_{X'})N$ roots in $\mathbb{F}^2$. Therefore, for independent random H, H', each uniformly

distributed over $\mathbb{F}$, and for arbitrary messages X, X' it holds that:

$$\Pr\{f_X(H) = f_{X'}(H')\} \le \frac{\max(\deg f_X, \deg f_{X'})N}{N^2} \le \frac{d}{N}.$$

This bound forms the basis of our security proofs of EHE.

More precisely, we use the slightly stronger bound:

$$\Pr\{f_X(H) = f_{X'}(H') \mid H \ne H'\} \le \frac{d}{N}. \tag{2}$$

It followed from the fact that the polynomial $g(\lambda, \lambda')$ has at most $d(N-1)$ roots (H, H') such that $H \ne H'$. Indeed, the substitution $\lambda' = \lambda + \mu$ transforms g into a polynomial $g'(\lambda, \mu)$. A number of the suitable roots of g is the number of roots of g' with a nonzero last coordinate. This coordinate can be chosen in $N-1$ ways. Each choice $\mu = c$ yields the univariate polynomial $g'(\lambda, c)$ which has at most d roots.

Let us justify the prf-security of EHE, that is, the indistinguishability of $\varphi[\pi_1, \pi_2]$ from a truly random (ideal) message authentication function. The indistinguishability means that $\varphi[\pi_1, \pi_2]$ is pseudorandom (it "looks" like random) or prf in short. Let an adversary (a probabilistic algorithm) have access to a message authentication oracle G which on a query (X, S) gives a response T. The oracle implements either the function $\varphi[\pi_1, \pi_2]$ (a real implementation) or a truly random function ρ (an ideal implementation). In the real implementation, the permutations π_1, π_2 are chosen independently uniformly at random from the set of all permutations on $\mathbb{F}$. In the ideal implementation, the oracle, given a new query, chooses a response T uniformly at random from $\mathbb{F}$ independently of previous responses. The adversary can make arbitrary queries, can collect and analyze the corresponding responses. Its task is to determine which function G implements. The adversary returns 1 if it is $\varphi[\pi_1, \pi_2]$, or 0 if it is ρ. Let A^G be the output of A.

The quality of A's distinguishing capabilities is characterized by the advantage

$$\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) = |\Pr\{A^{\varphi[\pi_1,\pi_2]} = 1\} - \Pr\{A^{\rho} = 1\}|.$$

The probabilities here are over the random tape of A and over the random choice of π_1, π_2 and ρ. If $\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A)$ is small then the adversary is hard to distinguish $\varphi[\pi_1, \pi_2]$ from ρ.

Theorem 1. Let EHE be built over a field of N elements. Let an adversary A make at most q queries (X, S) and messages X in these queries be such that $\deg f_X \le d$. Then

$$\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) \le \frac{q(q-1)d}{2N}.$$

Proof. Let $(X_1, S_1), \ldots, (X_q, S_q)$ be different queries and $T_1, \ldots, T_q$ be different elements of $\mathbb{F}$ (potential responses). It is sufficient to prove that

$$p = \Pr\{\varphi[\pi_1, \pi_2](X_i, S_i) = T_i \colon i = 1, \ldots, q\} \ge \frac{1}{N^q}(1 - \varepsilon),\ \varepsilon = \frac{q(q-1)(d-1)}{2N}.$$

Indeed, then using the H-coefficients technique [7] or, more precisely, Theorem 1 from [6], we obtain

$$\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) \le \frac{q(q-1)}{2N} + \varepsilon = \frac{q(q-1)d}{2N}.$$

Let $H_i = \pi_1(S_i)$ and $Y_i = f_{X_i}(H_i)$, $i = 1, \ldots, q$. Introduce the event $\mathcal{D}_1$ that all Y_i are distinct and the event $\mathcal{D}_2$ that $\pi_2(Y_i) = T_i$ for each i. Let us estimate the probabilities $\Pr\{\mathcal{D}_1\}$ and $\Pr\{\mathcal{D}_2 \mid \mathcal{D}_1\}$. They are correspondingly determined by the random choice of π_1 and π_2.

The estimates (1), (2) imply

$$\Pr\{Y_i = Y_j\} = \Pr\{f_{X_i}(\pi_1(S_i)) = f_{X_j}(\pi_1(S_j))\} = \Pr\{f_{X_i}(H_i) = f_{X_j}(H_j)\} \le \frac{d}{N}$$

regardless of whether S_i and S_j coincide or not. Indeed, if $S_i = S_j$ then $H_i = H_j$ is uniformly distrubuted over $\mathbb{F}$ and (1) works. If $S_i \ne S_j$ then (H_i, H_j) is uniformly distributed over $\mathbb{F}^2 \setminus \{(a,a)\colon a \in \mathbb{F}\}$ and (2) works. In whole,

$$\Pr\{\mathcal{D}_1\} \ge 1 - \sum_{1 \le i < j \le q} \Pr\{Y_i = Y_j\} \ge 1 - \frac{q(q-1)d}{2N}.$$

Denote by $N^{[q]}$ the qth factorial power of N:

$$N^{[q]} = N(N-1)\dots(N-q+1) = N^q \prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right) \le N^q \left(1 - \frac{q(q-1)}{2N}\right).$$

We have

$$\Pr\{\mathcal{D}_2 \mid \mathcal{D}_1\} = \frac{1}{N^{[q]}} \ge \frac{1}{N^q}\left(1 + \frac{q(q-1)}{2N}\right)$$

and

$$p \ge \Pr\{\mathcal{D}_2 \mid \mathcal{D}_1\} \Pr\{\mathcal{D}_1\} \ge \frac{1}{N^q}\left(1 + \frac{q(q-1)}{2N}\right)\left(1 - \frac{q(q-1)d}{2N}\right) \ge \frac{1}{N^q}(1-\varepsilon)$$

which was to be proved. □

The theorem implies that the EHE authentication remains prf-secure as long as the number of messages processed by a single key is well below $\sqrt{N/d}$. The prf-security is the strongest property of the message authentication schemes. In particular, it implies the security against forgery attacks. In these attacks an adversary interacts with $G = \varphi[\pi_1, \pi_2]$ making arbitrary queries and getting corresponding responses. The adversary's aim is to predict a response to a query that has not been made yet.

Both permutations π_1 and π_2 in EHE are necessary. Confirm this fact in the context of the forgery attacks. If π_1 is omitted, then an adversary can effectively find different messages X and X' with the same hash values $f_X(S)$ and $f_{X'}(S)$. Then using a tag $T = \pi_2(f_X(S))$ of X the adversary determines the tag $T' = T$ of X' without a query. If π_2 is omitted, then an adversary finds $H = \pi_1(S)$ from $T = f_X(H)$ and determines the tag $T' = f_{X'}(H)$ of arbitrary X', again without a query.

The theorem means that EHE preserves security even if nonces repeat. In principle, EHE can be used with a fixed nonce $S = c$. But in this case the security is collapsed in the following sense. As soon as an adversary finds a collision of tags T and T' of different messages X and X', it obtains the polynomial equiation $f_X(H) = f_{X'}(H)$ in $H = \pi_1(c)$. After determining H, the adversary constructs a new message X'' such that $f_{X''}(H) = f_X(H)$ and determines its tag $T'' = T$ without a query. Note that the collision $T = T'$ is expected to occur and EHE is expected to collapse after about $\sqrt{N}$ queries to the authentication oracle. This fact does not contradict to the bound of the theorem.

To determine H the adversary first finds roots of the polynomial $f_X(\lambda) - f_{X'}(\lambda)$ (let us ignore the time required) and then checks each of them to localize the right one. To check a root it is necessary to make a special query, for example, (X'', S). Let M be the number

of different roots. If M is large, then the number of check queries is large too. But if M is small, then the collision probability $\frac{M}{N}$ is small too. Therefore, regardless of M, check-time to collision-probability ratio for the pair (X, X') is of order N.

The situation changes drastically if nonces do not repeat. In this case the collision $T = T'$ means that (H, H') is a root of the bivariate polynomial $g(\lambda, \lambda') = f_X(\lambda) - f_X(\lambda')$. Let g have M different roots. There are at least $\frac{M}{2d}$ different coordinates of these roots and time to check is of lower order $\frac{M}{d}$. The collision occurs with the probability $\frac{M}{N(N-1)}$ and check-time to collision-probability ratio of the pair (X, X') is of lower order $\frac{N^2}{d}$, that is, it dramatically increases comparing to the previous situation.

3 Instantiation

Instead of two secret permutations it is convenient to use only one, say π, and derive π_1 and π_2 from it. We are interested in two variants (*instantiation templates*) of such deriving: $(\pi_1, \pi_2) = (\pi, \pi)$ and $(\pi_1, \pi_2) = (\pi^2, \pi)$. The first template is clearly natural, the second one will be used in the following section while extending EHE to AE[EHE]. Let, as usual, π be chosen uniformly at random from the set of all permutations on $\mathbb{F}$.

Theorem 2. Let EHE be built over a field of N elements with $(\pi_1, \pi_2) = (\pi, \pi)$. Let an adversary A make at most q queries (X, S) and messages X in these queries be such that $\deg f_X \le d$. Then

$$\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) \le \frac{q(3q-1)d}{2N}.$$

Proof. Modify the previous proof. Let the event $\mathcal{D}_1$ suppress not only the collisions $Y_i = Y_j$ but also the collisions $Y_i = S_j$ and $T_i = H_j$. Additional restrictions mean that every pair (Y_i, T_i) is *fresh*, that is, π_2 can map Y_i to T_i despite the facts that $H_j = \pi_1(S_j)$ and $\pi_1 = \pi_2$.

There are q^2 additional collisions of each type, their probabilities:

$$\Pr\{Y_i = S_j\} = \Pr\{f_X(\pi_1(S_i)) = S_j\} = \Pr\{\pi_1(S_i) \text{ is a root of } f_X - S_j\} \le \frac{d}{N},$$
$$\Pr\{T_i = H_j\} = \Pr\{\pi_1(S_j) = T_i\} = \frac{1}{N}.$$

In whole,

$$\Pr\{\mathcal{D}_1\} \ge 1 - \frac{q(q-1)d}{2N} - \frac{q^2 d}{N} - \frac{q^2}{N} = 1 - \frac{q(3q-1)d + 2q^2}{2N}.$$

The event $\mathcal{D}_1$ fixes no more than q different pairs (a preimage S_i, an image H_i) of $\pi_1 = \pi$. So there are at least $(N-q)^{[q]}$ ways to determine images of $\pi_2 = \pi$ for the q additional preimages $Y_1, \ldots, Y_q$ and only one of these ways is suitable, that is, $T_1, \ldots, T_q$. Repeating the estimation technique of the previous proof, we obtain

$$\Pr\{\mathcal{D}_2 \mid \mathcal{D}_1\} \ge \frac{1}{(N-q)^{[q]}} \ge \frac{1}{N^q}\left(1 + \frac{q(3q-1)}{2N}\right).$$

Combining the bounds on $\Pr\{\mathcal{D}_1\}$ and $\Pr\{\mathcal{D}_2 \mid \mathcal{D}_1\}$ completes the proof. □

The permutation π can be interpreted as an ideal implementation of a block encryption oracle E. It is an internal oracle of EHE to which A does not have a direct access. A real implementation of E is a permutation F_K uniformly at random chosen from a family F of

permutations acting on $\mathbb{F}$. This family is called a block cipher. The index K above is a random key of this cipher. Let EHE[F] be the EHE scheme with the described instantiation of E.

The advantage of A against EHE[F] is defined and estimated in the following way:

$$\begin{aligned}\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}[F]}(A) = |\Pr\{A^{\varphi[F_K,F_K]}=1\} - \Pr\{A^{\rho}=1\}| \le \\ \le \mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) + |\Pr\{A^{\varphi[F_K,F_K]}=1\} - \Pr\{A^{\varphi[\pi,\pi]}=1\}|.\end{aligned}$$

The last summand characterizes the quality of distinguishing of E, that is, differentiating between its real implementation F_K and its ideal implementation π. The advantage of an adversary B which distinguish E is defined similar to the advantage of A:

$$\mathbf{Adv}^{\mathtt{prp}}_{F}(B) = \left|\Pr\{B^{F_K}=1\} - \Pr\{B^{\pi}=1\}\right|.$$

Let $\mathbf{Adv}^{\mathtt{prp}}_{F}(t,q)$ be the maximum of $\mathbf{Adv}^{\mathtt{prp}}_{F}(B)$ over all B which run in time at most t and make at most q queries to E.

The adversary B can use A to distinguish E. To do this, B simulates the oracle $G = \varphi[E,E]$ which responses $E(f_X(E(S)))$ to (X,S) the adversary determines making two queries to E and one polynomial hashing. The adversary B grants A access to the simulated oracle, waits for the output from A and returns this output as its own. The simulation of G needs $q^* = 2q$ queries to E and time $t^* = O(qd)$.

If A runs in time t, then

$$|\Pr\{A^{\varphi[F_K,F_K]}=1\} - \Pr\{A^{\varphi[\pi,\pi]}=1\}| = \mathbf{Adv}^{\mathtt{prp}}_{F}(B) \le \mathbf{Adv}^{\mathtt{prp}}_{F}(q^*, t+t^*)$$

and, in whole,

$$\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}[F]}(A) \le \mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) + \mathbf{Adv}^{\mathtt{prp}}_{F}(q^*, t+t^*).$$

The arguments above are standard in provable security. The last estimate can be used to continue all our further theorems. In such a continuation one should only refine q^* (the total number of A's indirect queries to the internal oracle E) and t^* (time to simulate G over E).

4 The AE[EHE] modes

The permutation π can be used not only to instantiate EHE, but also to manage encryption, that is, to extend EHE to AE[EHE]. In this section we provide two modes of authenticated encryption based on EHE. In both modes plaintexts and ciphertexts are considered as words in the alphabet $\mathbb{F}$.

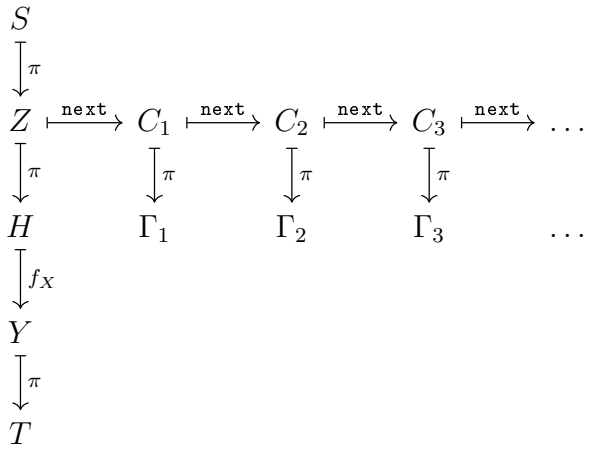
A plaintext is encrypted in the counter mode using a full-cycle permutation $\mathtt{next}$ acting on $\mathbb{F}$. A nonce S is used to calculate $H = \pi(S)$ and then the sequence $C_1 = \mathtt{next}(H)$, $C_2 = \mathtt{next}(C_1) = \mathtt{next}^2(H), \ldots$ of counters. The encrypted counters $\Gamma_k = \pi(C_k)$ are added to the plaintext symbols during encryption or subtracted from the ciphertext symbols during decryption. An adversary can get $\pi(C_k)$ (it can subtract a known plaintext from an intersected ciphertext) but not C_k.

The obtained ciphertext and arbitrary additional data form a message X which is authenticated using EHE. Since $\deg f_X \le d$, the length of the plaintext cannot exceed d and at most d symbols Γ_k are sufficient for encryption.

We cannot justify the security of AE[EHE] in the general case if the template $(\pi_1,\pi_2) = (\pi,\pi)$ is used. It is due to possible similarities between f_X and $\mathtt{next}^k$. For example,

if f_X and $\mathtt{next}^k$ act identically, then an adversary can predict $T = \pi(f_X(\pi(S)))$ using $\Gamma_k = \pi(\mathtt{next}^k(\pi(S))) = T$. We should either impose restrictions on $\mathtt{next}$ or change the template.

Start with the second option. The simplest suitable template is $(\pi_1, \pi_2) = (\pi^2, \pi)$. It separates a preimage $\pi^2(S)$ of f_X from a preimage $\pi(S)$ of $\mathtt{next}^k$ and makes similarities between f_X and $\mathtt{next}^k$ ineffective. The whole AE[EHE] mode with the new template can be depicted as follows:



Theorem 3. Let EHE be built over a field of N elements with $(\pi_1, \pi_2) = (\pi^2, \pi)$. Let an adversary A make at most q queries (X, S) and messages X in these queries be such that $\deg f_X \le d$. Let the adversary in addition to each response T receive at most d first elements of the sequence

$$\Gamma_1 = \pi(\mathtt{next}(\pi(S))),\ \Gamma_2 = \pi(\mathtt{next}^2(\pi(S))), \dots$$

and let r be the total number of such elements. Then

$$\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) \le \frac{q(5q + 2r - 1)d}{2N}.$$

Proof. Again modify the previous proof. Let $Z_i = \pi(S_i)$, $H_i = \pi(Z_i)$, $C_{i,k} = \mathtt{next}^k(Z_i)$, $\Gamma_{i,k} = \pi(C_{i,k})$. In the event $\mathcal{D}_1$ suppress the following collisions:

collisions	quantity	probability (upper bound)
$Y_i = Y_j$	$q(q-1)/2$	d/N
$Y_i = S_j$	q^2	d/N
$Y_i = Z_j$	q^2	d/N
$Y_i = C_{j,k}$	qr	d/N
$T_i = Z_j$	q^2	$1/N$
$T_i = H_j$	q^2	$1/N$
$T_i = \Gamma_{j,k}$	qr	$1/N$

These restrictions guarantee the freshness of the pairs (Y_i, T_i). Processing the last two columns of the table, we obtain

$$\Pr\{\mathcal{D}_1\} \ge 1 - \frac{q(5q + 2r - 1)d + 4q^2 + 2qr}{2N}.$$

The event $\mathcal{D}_1$ fixes at most $2q+r$ different images of π. Hence there are at least $(N-2q-r)^{[q]}$ ways to determine q additional images which correspond to the preimages $Y_1,\dots,Y_q$ and only one of these ways is suitable. In result,

$$\Pr\{\mathcal{D}_2 \mid \mathcal{D}_1\} \ge \frac{1}{(N-2q-r)^{[q]}} \ge \frac{1}{N^q}\left(1+\frac{q(5q+2r-1)}{2N}\right).$$

Repeating the estimation technique of the previous proof, we get the result required. □

The instantiation template $(\pi_1,\pi_2)=(\pi,\pi)$ is preferable than $(\pi_1,\pi_2)=(\pi^2,\pi)$ because it requires 1 less encryption. As we said before, to securely use the template $(\pi_1,\pi_2)=(\pi,\pi)$, it is necessary to impose restrictions on `next`. These restrictions should impede the collisions of the form $f_X(H)=\mathtt{next}^k(H')$ or even the form $f_X(H)=\mathtt{next}^k(H')$, $H\ne H'$.

In this connection, call the permutation `next` (d,δ)-*uniform*, if for any suitable f_X with $\deg f_X \le d$ and each $k=1,\dots,d$ it holds that

$$\Pr\{f_X(H)=\mathtt{next}^k(H)\},\ \Pr\{f_X(H)=\mathtt{next}^k(H') \mid H\ne H'\} \le \frac{d\delta}{N}.$$

Here H and H' are independent random, each uniformly distributed over $\mathbb{F}$.

Example. Consider an affine permutation $\mathtt{aff}\colon H\mapsto \alpha H+\beta$, $\alpha,\beta\in\mathbb{F}\setminus\{0\}$. If α is the multiplicative unit of $\mathbb{F}$, then `aff` is $(d,1)$-uniform, the best we can get, but it is a full-cycle only if $\mathbb{F}$ is prime. For arbitrary $\mathbb{F}$ the permutation `aff` turns into an almost-full-cycle if α is primitive. Indeed, in this case `aff` decomposes into a cycle of length $N-1$ and a fixed point $\beta/(1-\alpha)$. The probability to fall into the sole fixed point during encryption is negligible and `aff` can be used in the counter mode without meaningful loss of security. □

Theorem 4. Let EHE be built over a field of N elements with $(\pi_1,\pi_2)=(\pi,\pi)$. Let an adversary A make at most q queries (X,S) and messages X in these queries be such that $\deg f_X \le d$. Let the adversary in addition to each response T receive at most d first elements of the sequence

$$\Gamma_1=\pi(\mathtt{next}(\pi(S))),\ \Gamma_2=\pi(\mathtt{next}^2(\pi(S))),\dots$$

and let r be the total number of such elements. Let `next` be (d,δ)-uniform. Then

$$\mathbf{Adv}^{\mathtt{prf}}_{\mathrm{EHE}}(A) \le \frac{q(3q+2r\delta-1)d}{2N}.$$

Proof. Modify the proof of Theorem 2. Let $C_{i,k}=\mathtt{next}^k(H_i)$, $\Gamma_{i,k}=\pi(C_{i,k})$. In the event $\mathcal{D}_1$ suppress the following collisions:

collisions	quantity	probability (upper bound)
$Y_i=Y_j$	$q(q-1)/2$	d/N
$Y_i=S_j$	q^2	d/N
$Y_i=C_{j,k}$	qr	$d\delta/N$
$T_i=H_j$	q^2	$1/N$
$T_i=\Gamma_{j,k}$	qr	$1/N$

The result required follows from the estimates:

$$\Pr\{\mathcal{D}_1\} \ge 1-\frac{q(3q+2r\delta-1)d+2q^2+2qr}{2N},$$
$$\Pr\{\mathcal{D}_2 \mid \mathcal{D}_1\} \ge \frac{1}{(N-q-r)^{[q]}} \ge \frac{1}{N^q}\left(1+\frac{q(3q+2r-1)}{2N}\right).$$

□

To fully justify the security of the proposed AE[EHE] modes we need to show that it is hard to distinguish from random not only the tags T but also the symbols Γ_k (provided that the nonces S do not repeat). Technically, it can be quite easily done by rebuilding the proofs of Theorems 3 and 4. We leave such rebuilding outside the scope of this paper.

References

[1] D. Bernstein, Stronger security bounds for Wegman-Carter-Shoup authenticators, in: *Advances in Cryptology — EUROCRYPT'2005*, Lecture Notes in Comp. Sci. 3494, Springer, Berlin (2005), 164–180.

[2] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: Galois-Counter Mode (GCM) for Confidentiality and Authentication*, NIST Special Publication 800-38D (2007), `http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf`.

[3] S. Gueron and Y. Lindell, GCM-SIV: full monce misuse-resistant authenticated encryption at under one cycle per byte, in: *CCS'15 – Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (2015), 109–119.

[4] R. Lidl, H. Niederraiter, *Finite Fields*, Cambridge University Press, 1997.

[5] D. A. McGrew and J. Viega, The security and performance of the Galois / Counter Mode (GCM) of operation, in: *Advances in Cryptology — INDOCRYPT'2004*, Lecture Notes in Comp. Sci. 3348, Springer, Berlin (2004), 343–355.

[6] M. Nandi, Improved security analysis for OMAC as a pseudorandom function, *J. Math. Cryptol.* **3** (2009), 133–148.

[7] J. Patarin, *Etude des Gènèrateurs de Permutations Basès sur le Sch'ema du D.E.S.*, Ph.D. thesis, University of Paris, 1991.

[8] P. Rogaway, *Evaluation of Some Blockcipher Modes of Operation*, Cryptography Research and Evaluation Committees (CRYPTREC) (2011), `http://www.cryptrec.go.jp/estimation/techrep_id2012_2.pdf`.

[9] V. Shoup, On fast and provably secure message authentication based on universal hashing, in: *Advances in Cryptology — CRYPTO'2006*, Lecture Notes in Comp. Sci. 1109, Springer, Berlin (1996), 313–328.

[10] *STB 34.101.31-2011. Information Technology and Security. Data Encryption and Integrity Algorithms*, Standard of Belarus (2011), `http://apmi.bsu.by/assets/files/std/belt-spec27.pdf`, in Russian.

[11] M. Wegman and J. Carter, New hash functions and their use in authentication and set equality, *J. Comp. and System Sci.* **22** (1981), 265–279.