On an almost-universal hash function family with applications to authentication and secrecy codes

Khodakhast Bibak † Bruce M. Kapron † Venkatesh Srinivasan †‡ László Tóth §

April 10, 2016

Abstract

Universal hashing, discovered by Carter and Wegman in 1979, has many important applications in computer science. The following family, called MMH∗ by Halevi and Krawczyk in 1997, is well known: Let q be a prime and k be a positive integer. Define

$$\text{MMH}^* := \{g_x : \mathbb{Z}_q^k \rightarrow \mathbb{Z}_q | x \in \mathbb{Z}_q^k\},$$

where

$$g_x(m) := m \cdot x \pmod{q} = \sum_{i=1}^{k} m_i x_i \pmod{q},$$

for any \(x = (x_1, \ldots, x_k) \in \mathbb{Z}_q^k\), and any \(m = (m_1, \ldots, m_k) \in \mathbb{Z}_q^k\). In this paper, we first give a new proof for the \(\Delta\)-universality of MMH∗, shown by Halevi and Krawczyk in 1997, via connecting the universal hashing problem to the number of solutions of (restricted) linear congruences. We then introduce a new hash function family — a variant of MMH∗ — that we call GRDH, where we use an arbitrary integer \(n > 1\) instead of prime \(q\) and let the keys \(x = (x_1, \ldots, x_k) \in \mathbb{Z}_n^k\) satisfy the conditions \(\gcd(x_i, n) = t_i\) \((1 \leq i \leq k)\), where \(t_1, \ldots, t_k\) are given positive divisors of \(n\). Applying our aforementioned approach, we prove that the family GRDH is an \(\epsilon\)-almost-\(\Delta\)-universal family of hash functions for some \(\epsilon < 1\) if and only if \(n\) is odd and \(\gcd(x_i, n) = t_i = 1\) \((1 \leq i \leq k)\). Furthermore, if these conditions are satisfied then GRDH is \(\frac{1}{p-1}\)-almost-\(\Delta\)-universal, where \(p\) is the smallest prime divisor of \(n\). Finally, as an application of our results, we propose an authentication code with secrecy scheme which generalizes a recent construction.

Keywords: Universal hashing; authentication code with secrecy; restricted linear congruence

2010 Mathematics Subject Classification: 11D79, 11P83, 11L03, 11A25, 94A60, 94A62

*We plan to submit an extended abstract of this paper to ISITA 2016.
†Department of Computer Science, University of Victoria, Victoria, BC, Canada V8W 3P6. Email: \{kbibak,bmkapron,srinivas\}@uvic.ca
‡Centre for Quantum Technologies, National University of Singapore, Singapore 117543.
§Department of Mathematics, University of Pécs, 7624 Pécs, Hungary. Email: ltoth@gamma.ttk.pte.hu
1 Introduction

Universal hash functions, discovered by Carter and Wegman [10], have many applications in computer science, including cryptography and information security [9, 13, 15, 16, 18, 19, 37, 48, 49], pseudorandomness [17, 35], complexity theory [39, 44], randomized algorithms [22, 33], data structures [36, 43], and parallel computing [23, 27]. Since universality of hash functions and its variants are concepts central to this work, we begin by describing them in detail. Our description of these concepts closely follows the definitions given in [15].

1.1 Universal hashing and its variants

Let \( D \) and \( R \) be finite sets. Let \( H \) be a family of functions from domain \( D \) to range \( R \). We say that \( H \) is a universal family of hash functions ([10]) if the probability, over a random choice of a hash function from \( H \), that two distinct keys in \( D \) have the same hash value is at most \( 1/|R| \). That is, universal hashing captures the important property that distinct keys in \( D \) do not collide too often. Furthermore, we say that \( H \) is an \( \varepsilon \)-almost-universal (\( \varepsilon \)-AU) family of hash functions if the probability of collision is at most \( \varepsilon \), for \( 1/|R| \leq \varepsilon < 1 \). In other words, an \( \varepsilon \)-AU family, for sufficiently small \( \varepsilon \), is close to being universal; see Definition 1.1 below. Universal and almost-universal hash functions have many applications in algorithm design. For example, they have been used to provide efficient solutions for the dictionary problem in which the goal is to maintain a dynamic set that is updated using insert and delete operations using small space so that membership queries that ask if a certain element is in \( S \) can be answered quickly.

Motivated by applications to cryptography, a notion of \( \Delta \)-universality was introduced in [24, 38, 45]. Suppose that \( R \) is an Abelian group. We say that \( H \) is a \( \Delta \)-universal family of hash functions if the probability, over a random \( h \in H \), that two distinct keys in \( D \) hash to values that are distance \( b \) apart for any \( b \in R \) is \( 1/|R| \). Note that the case \( b = 0 \) corresponds to universality. Furthermore, we say that \( H \) is an \( \varepsilon \)-almost-\( \Delta \)-universal (\( \varepsilon \)-A\( \Delta \)U) if this probability is at most \( \varepsilon \), \( 1/|R| \leq \varepsilon < 1 \). We remark that \( \varepsilon \)-A\( \Delta \)U families have applications to message authentication. Informally, it is possible to design a message authentication scheme using \( \varepsilon \)-A\( \Delta \)U families such that two parties can exchange signed messages over an unreliable channel and the probability that an adversary can forge a valid signed message to be sent across the channel is at most \( \varepsilon \) ([15]). Also, the well-known leftover hash lemma states that (almost) universal hash functions are good randomness extractors.

Finally, in Section 4 on authentication codes with secrecy, we need the notion of strong universality which was introduced in [49]. We say that \( H \) is a strongly universal family of hash functions if the probability, over a random choice of a hash function from \( H \), that two distinct keys \( x \) and \( y \) in \( D \) are mapped to \( a \) and \( b \) respectively is \( 1/|R|^2 \). We say that \( H \) is an \( \varepsilon \)-almost-strongly-universal (\( \varepsilon \)-ASU) if this probability is at most \( \varepsilon \), \( 1/|R|^2 \leq \varepsilon < 1/|R| \).

We now provide a formal definition of the concepts introduced above as in [15]. For a set \( \mathcal{X} \), we write \( x \leftarrow \mathcal{X} \) to denote that \( x \) is chosen uniformly at random from \( \mathcal{X} \).

**Definition 1.1.** Let \( H \) be a family of functions from a domain \( D \) to a range \( R \). Let \( \varepsilon \) be a constant such that \( 1/|R| \leq \varepsilon < 1 \). The probabilities below, are taken over the random choice of hash function \( h \) from the set \( H \).
• The family $H$ is a universal family of hash functions if for any two distinct $x, y \in D$, we have $\Pr_{h \leftarrow H}[h(x) = h(y)] \leq \frac{1}{|D|}$. Also, $H$ is an $\varepsilon$-almost-universal ($\varepsilon$-AU) family of hash functions if for any two distinct $x, y \in D$, we have $\Pr_{h \leftarrow H}[h(x) = h(y)] \leq \varepsilon$.

• Suppose $R$ is an Abelian group. The family $H$ is a $\triangle$-universal family of hash functions if for any two distinct $x, y \in D$, and all $b \in R$, we have $\Pr_{h \leftarrow H}[h(x) - h(y) = b] = \frac{1}{|R|}$, where ‘$-\$’ denotes the group subtraction operation. Also, $H$ is an $\varepsilon$-almost-$\triangle$-universal ($\varepsilon$-AU) family of hash functions if for any two distinct $x, y \in D$, and all $b \in R$, we have $\Pr_{h \leftarrow H}[h(x) - h(y) = b] \leq \varepsilon$.

• The family $H$ is a strongly universal family of hash functions if for any two distinct $x, y \in D$, and all $a, b \in R$, we have $\Pr_{h \leftarrow H}[h(x) - h(y) = b] = \frac{1}{|R|^2}$. Also, $H$ is an $\varepsilon$-almost-strongly universal ($\varepsilon$-ASU) family of hash functions if for any two distinct $x, y \in D$, and all $a, b \in R$, we have $\Pr_{h \leftarrow H}[h(x) = a, h(y) = b] \leq \frac{1}{|R|^2}$.

1.2 MMH*

The hash function family we study, GRDH, is a variant of a well-known family which was named MMH* (Multilinear Modular Hashing) by Halevi and Krawczyk [15]. Let $p$ be a prime and $k$ be a positive integer. Each hash function in the family MMH* takes as input a $k$-tuple, $m = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k$. It computes the dot product of $m$ with a fixed $k$-tuple $x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$ and outputs this value modulo $p$.

**Definition 1.2.** Let $p$ be a prime and $k$ be a positive integer. The family MMH* is defined as follows:

$$MMH^* := \{g_x : \mathbb{Z}_p^k \rightarrow \mathbb{Z}_p \mid x \in \mathbb{Z}_p^k\},$$

(1.1)

where

$$g_x(m) := m \cdot x \pmod{p} = \sum_{i=1}^{k} m_i x_i \pmod{p},$$

(1.2)

for any $x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$, and any $m = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k$.

The family MMH* is widely attributed to Carter and Wegman [10], while it seems that Gilbert, MacWilliams, and Sloane [14] had already discovered it (but in the finite geometry setting). Halevi and Krawczyk [15], using the multiplicative inverse method, proved that MMH* is a $\triangle$-universal family of hash functions. We also remark that, recently, Leiserson et al. [27] rediscovered MMH* (called it “DOTMIX compression function family”) and using the same method as of Halevi and Krawczyk [15] proved that DOTMIX is $\triangle$-universal. Then they apply this result in studying the problem of deterministic parallel random-number generation for dynamic multithreading platforms in parallel computing.

**Theorem 1.3.** ([15, 27]) The family MMH* is a $\triangle$-universal family of hash functions.

Very recently, it was proved that MMH* with arbitrary modulus is always almost-universal [6].
1.3 Our contributions

Suppose that, instead of a prime $p$, one uses an arbitrary integer $n > 1$ in the definition of MMH*. Additionally, we ask that the keys $x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ satisfy the conditions $\gcd(x_i, n) = t_i \ (1 \leq i \leq k)$, where $t_1, \ldots, t_k$ are given positive divisors of $n$. We call this new family GRDH and refer the reader to Section 3 for a formal definition.

Many natural questions arise: What can we say about universality (or $\varepsilon$-almost-universality) of GRDH? What can we say about $\triangle$-universality (or $\varepsilon$-almost-$\triangle$-universality) of GRDH? Recently, Alomair, Clark, and Poovendran [1] presented a construction of codes with secrecy based on a universal hash function family that is a special case of GRDH. Is it possible to generalize their construction and analyse its security properties?

- In Section 3, we first give a new proof of Theorem 1.3 for the $\triangle$-universality of MMH* via connecting the universal hashing problem to the number of solutions of (restricted) linear congruences.

- In Theorem 3.3, we prove that if $n, k > 1$ then the family GRDH is an $\varepsilon$-AU family of hash functions for some $\varepsilon < 1$ if and only if $n$ is odd and $\gcd(x_i, n) = t_i = 1 \ (1 \leq i \leq k)$. Furthermore, if these conditions are satisfied then GRDH is $\frac{1}{p-1}$-AU, where $p$ is the smallest prime divisor of $n$. This bound is tight.

- In Remark 3.4, we conclude (from the idea of the proof of Theorem 3.3) that if $k = 1$ then the family GRDH is an $\varepsilon$-AU family of hash functions for some $\varepsilon < 1$ if and only if $\gcd(x_1, n) = t_1 = 1$. Furthermore, if $\gcd(x_1, n) = t_1 = 1$ (that is, if $x_1 \in \mathbb{Z}_n^*$) then the collision probability for any two distinct messages is ‘exactly zero’.

- In Theorem 3.5, we show that if $n > 1$ then the family GRDH is an $\varepsilon$-A$\triangle$U family of hash functions for some $\varepsilon < 1$ if and only if $n$ is odd and $\gcd(x_i, n) = t_i = 1 \ (1 \leq i \leq k)$. Furthermore, if these conditions are satisfied then GRDH is $\frac{1}{p-1}$-A$\triangle$U, where $p$ is the smallest prime divisor of $n$. This bound is tight.

- In Theorem 4.2, we generalize the construction of authentication code with secrecy presented in [1, 3]. Using Theorem 3.5, we show that our construction is a $\frac{1}{(p-1)n^{k-1}}, \frac{1}{p-1}$-authentication code with secrecy for equiprobable source states on $\mathbb{Z}_n^k \setminus \{0\}$, where $n$ is odd, and $p$ is the smallest prime divisor of $n$.

Our results show that if one uses a composite integer $n$ in the definition of MMH* then even by choosing the keys $x = \langle x_1, \ldots, x_k \rangle$ from $\mathbb{Z}_n^k$, or more generally, choosing the keys $x = \langle x_1, \ldots, x_k \rangle$ from $\mathbb{Z}_n^k$ with the general conditions $\gcd(x_i, n) = t_i \ (1 \leq i \leq k)$, where $t_1, \ldots, t_k$ are given positive divisors of $n$, we cannot get any strong collision bound (unless $k = 1$ and $\gcd(x_1, n) = t_1 = 1$; in this case, as we mentioned above, the collision probability for any two distinct messages is ‘exactly zero’). Such impossibility results were not known before.

We believe that connecting the universal hashing problem to the number of solutions of (restricted) linear congruences is a novel idea and could be also of independent interest. A key ingredient in the proofs is an explicit formula for the number of solutions of restricted
linear congruences, recently obtained by Bibak et al. [8], using properties of Ramanujan sums and of the finite Fourier transform of arithmetic functions, that we will review in Section 2. We believe that this is the first paper that introduces applications of Ramanujan sums, finite Fourier transform, and restricted linear congruences in the study of universal hashing. We hope this approach will lead to further work.

2 Restricted linear congruences

Throughout the paper, we use \((a_1, \ldots, a_k)\) to denote the greatest common divisor (gcd) of the integers \(a_1, \ldots, a_k\), and write \(\langle a_1, \ldots, a_k \rangle\) for an ordered \(k\)-tuple of integers. Also, for \(a \in \mathbb{Z} \setminus \{0\}\), and a prime \(p\), we use the notation \(p^r \mid | a\) if \(p^r \mid a\) and \(p^{r+1} \nmid a\). We also use \(0\) to denote the vector of all zeroes. The multiplicative group of integers modulo \(n\) is denoted by \(\mathbb{Z}_n^\times\).

Let \(a_1, \ldots, a_k, b, n \in \mathbb{Z}, n \geq 1\). A linear congruence in \(k\) unknowns \(x_1, \ldots, x_k\) is of the form

\[
a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}.
\]

(2.1)

By a solution of (2.1), we mean an \(x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k\) that satisfies (2.1). The following result, proved by D. N. Lehmer [26], gives the number of solutions of the above linear congruence:

**Proposition 2.1.** Let \(a_1, \ldots, a_k, b, n \in \mathbb{Z}, n \geq 1\). The linear congruence \(a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}\) has a solution \(\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k\) if and only if \(\ell \mid | b\), where \(\ell = (a_1, \ldots, a_k, n)\). Furthermore, if this condition is satisfied, then there are \(\ell n^{k-1}\) solutions.

While Proposition 2.1 is quite old and its proof is very simple but it appears that it is rarely known; e.g., Proposition 2.1 is proved in [28] where it is used as a key ingredient in studying the subset sum problem for finite Abelian groups ([28]).

The solutions of the above congruence may be subject to certain conditions, such as \((x_i, n) = t_i\) \((1 \leq i \leq k)\), where \(t_1, \ldots, t_k\) are given positive divisors of \(n\). The number of solutions of these kinds of congruences, which were called **restricted linear congruences** in [8], have been studied, in special cases, in many papers and have found very interesting applications in number theory, combinatorics, and cryptography, among other areas (see [7, 11, 12, 29, 31, 34, 40, 41, 46, 47]). Recently, Bibak et al. [8] dealt with the problem in its ‘most general case’ and using properties of Ramanujan sums and of the finite Fourier transform of arithmetic functions gave an explicit formula for the number of solutions of the restricted linear congruence

\[
a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}, \quad (x_i, n) = t_i\quad (1 \leq i \leq k),
\]

(2.2)

where \(a_1, t_1, \ldots, a_k, t_k, b, n \quad (n \geq 1)\) are arbitrary integers.

The special case of \(k = 2, \ a_i = 1, \ t_i = 1\) \((1 \leq i \leq k)\) of (2.2) is related to a long-standing conjecture due to D. H. Lehmer from 1932. Also, the special case of \(b = 0, \ a_i = 1, \ t_i = \frac{n}{m_i}, \ m_i \mid n\ (1 \leq i \leq k)\) is related to the orbicyclic (multivariate arithmetic) function
which has very interesting combinatorial and topological applications, in particular, in counting non-isomorphic maps on orientable surfaces. See [8] for a detailed discussion about restricted linear congruences and their applications.

If in (2.2) one has \( a_i = 0 \) for every \( 1 \leq i \leq k \), then clearly there are solutions \( (x_1, \ldots, x_k) \) if and only if \( b \equiv 0 \pmod{n} \) and \( t_i \mid n \ (1 \leq i \leq k) \), and in this case there are \( \phi(n/t_1) \cdots \phi(n/t_k) \) solutions.

Consider the restricted linear congruence (2.2) and assume that there is an \( i_0 \) such that \( a_{i_0} \neq 0 \). For every prime divisor \( p \) of \( n \) let \( r_p \) be the exponent of \( p \) in the prime factorization of \( n \) and let \( m_p = m_p(a_1, t_1, \ldots, a_k, t_k) \) denote the smallest \( j \geq 1 \) such that there is some \( i \) with \( p^j \nmid a_{i_0} t_i \). There exists a finite \( m_p \) for every \( p \), since for a sufficiently large \( j \) one has \( p^j \nmid a_{i_0} t_i \). Furthermore, let

\[
e_p = e_p(a_1, t_1, \ldots, a_k, t_k) = \# \{ i : 1 \leq i \leq k, p^{m_p} \nmid a_i t_i \}.
\]

By definition, \( 1 \leq e_p \leq \) the number of \( i \) such that \( a_i \neq 0 \). Note that in many situations instead of \( m_p(a_1, t_1, \ldots, a_k, t_k) \) we write \( m_p \) and instead of \( e_p(a_1, t_1, \ldots, a_k, t_k) \) we write \( e_p \) for short. However, it is important to note that both \( m_p \) and \( e_p \) always depend on \( a_1, t_1, \ldots, a_k, t_k, p \).

**Theorem 2.2.** ([8]) Let \( a_i, t_i, b, n \in \mathbb{Z}, n \geq 1, t_i \mid n \ (1 \leq i \leq k) \) and assume that \( a_i \neq 0 \) for at least one \( i \). Consider the linear congruence \( a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n} \), with \( (x_i, n) = t_i \ (1 \leq i \leq k) \). If there is a prime \( p \mid n \) such that \( m_p \leq r_p \) and \( p^{m_p} \nmid b \) or \( m_p \geq r_p + 1 \) and \( p^{r_p} \nmid b \), then the linear congruence has no solution. Otherwise, the number of solutions is

\[
\prod_{i=1}^{k} \phi \left( \frac{n}{t_i} \right) \prod_{p \mid n \atop m_p \leq r_p} p^{m_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p - 1}}{(p - 1)^{e_p - 1}} \right) \prod_{p \mid n \atop m_p \geq r_p} p^{m_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p}}{(p - 1)^{e_p}} \right), \tag{2.3}
\]

where the last two products are over the prime factors \( p \) of \( n \) with the given additional properties. Note that the last product is empty and equal to 1 if \( b = 0 \).

Formula (2.3) will be the core for the applications to universal hashing that we present in this paper.

**Corollary 2.3.** ([8]) The restricted congruence given in Theorem 2.2 has no solutions if and only if one of the following cases holds:

(i) there is a prime \( p \mid n \) with \( m_p \leq r_p \) and \( p^{m_p - 1} \nmid b \);

(ii) there is a prime \( p \mid n \) with \( m_p \geq r_p + 1 \) and \( p^{r_p} \nmid b \);

(iii) there is a prime \( p \mid n \) with \( m_p \leq r_p, e_p = 1 \) and \( p^{m_p} \mid b \);

(iv) \( n \) is even, \( m_2 \leq r_2, e_2 \) is odd and \( 2^{m_2} \mid b \);

(v) \( n \) is even, \( m_2 \leq r_2, e_2 \) is even and \( 2^{m_2 - 1} \mid b \).

Corollary 2.3 is the only result in the literature which gives necessary and sufficient conditions for the (non-)existence of solutions of restricted linear congruences in their most general case and might lead to interesting applications/implications. For example, Corollary 2.3 can
be considered as relevant to the generalized knapsack problem. The knapsack problem is of significant interest in cryptography, computational complexity, and several other areas. Micciancio [32] proposed a generalization of this problem to arbitrary rings, and studied its average-case complexity. This generalized knapsack problem, proposed by Micciancio [32], is described as follows: for any ring \(R\) and subset \(S \subset R\), given elements \(a_1, \ldots, a_k \in R\) and a target element \(b \in R\), find \(\langle x_1, \ldots, x_k \rangle \in S^k\) such that \(\sum_{i=1}^{k} a_i \cdot x_i = b\), where all operations are performed in the ring. Interestingly, Corollary 2.3 helps us to deal with this problem in a quite natural case:

**Remark 2.4.** The generalized knapsack problem with \(R = \mathbb{Z}_n\) and \(S = \mathbb{Z}_n^*\) has no solutions if and only if one of the cases of Corollary 2.3 holds.

Theorem 2.2 has also important applications in combinatorics, geometry, string theory, and quantum field theory (QFT) [5], for example, it is related to the famous Harvey’s theorem on the cyclic groups of automorphisms of compact Riemann surfaces [5].

## 3 GRDH

In this section, we introduce a variant of MMH* that we call GRDH (Generalized Restricted Dot Product Hashing). Then we investigate the \(\varepsilon\)-almost-universality and \(\varepsilon\)-almost-\(\Delta\)-universality of GRDH via connecting the problem to the number of solutions of restricted linear congruences. In order to explain this approach we first give a new proof for the \(\Delta\)-universality of MMH* using this technique.

**A New Proof for Theorem 1.3.** Let \(m = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k\) and \(m' = \langle m'_1, \ldots, m'_k \rangle \in \mathbb{Z}_p^k\) be any two distinct messages. Put \(a = \langle a_1, \ldots, a_k \rangle = m - m'\). Since \(m \neq m'\), there exists some \(i\) such that \(a_i \neq 0\). Now, for \(b \in \mathbb{Z}_p\) we have

\[
g_x(m) - g_x(m') = b \iff \sum_{i=1}^{k} a_i x_i \equiv b \pmod{p}.
\]

Since

\[
\gcd_{a=\langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_p^k \setminus \{0\}} (a_1, \ldots, a_k, p) = 1,
\]

given any \(a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_p^k \setminus \{0\}\) and any \(b \in \mathbb{Z}_p\), by Proposition 2.1, there are exactly \(p^{k-1}\) choices for such \(x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k\) that satisfy the above linear congruence. Also, since \(x_i \in \mathbb{Z}_p\) \((1 \leq i \leq k)\), the total number of choices for \(\langle x_1, \ldots, x_k \rangle\) is \(p^k\). Consequently, for any two distinct messages \(m, m' \in \mathbb{Z}_p^k\), and all \(b \in \mathbb{Z}_p\), we have

\[
\Pr_{g_x \leftarrow \text{MMH}^*}[g_x(m) - g_x(m') = b] = \frac{1}{p}.
\]

Thus, MMH* is \(\Delta\)-universal. \(\square\)

Now, we introduce the family GRDH:
Definition 3.1. Let $n$ and $k$ be positive integers ($n > 1$). We define the family RDH as follows:

$$\text{RDH} := \{ \Upsilon_x : \mathbb{Z}_n^k \to \mathbb{Z}_n : x \in \mathbb{Z}_n^* \},$$

(3.1)

where

$$\Upsilon_x(m) := m \cdot x \mod n = \sum_{i=1}^{k} m_i x_i \mod n,$$

(3.2)

for any $x = (x_1, \ldots, x_k) \in \mathbb{Z}_n^k$, and any $m = (m_1, \ldots, m_k) \in \mathbb{Z}_n^k$. Suppose that $t_1, \ldots, t_k$ are given positive divisors of $n$. Now, if in the definition of RDH instead of having $x = (x_1, \ldots, x_k) \in \mathbb{Z}_n^k$, we have, more generally, $x = (x_1, \ldots, x_k) \in \mathbb{Z}_n^k$ with $(x_i, n) = t_i$ ($1 \leq i \leq k$), then we get a generalization of RDH that we call GRDH.

It would be an interesting question to investigate for which values of $n$, GRDH is $\varepsilon$-AU or $\varepsilon$-A$\Delta$U. We now deal with these problems. The explicit formula for the number of solutions of restricted linear congruences (Theorem 2.2) along with our approach for giving a new proof of Theorem 1.3 play key roles here.

First, we prove the following lemma which is needed in proving the main results.

Lemma 3.2. Let $k$ and $n$ be positive integers ($n > 1$). For every prime divisor $p$ of $n$ let $r_p$ be the exponent of $p$ in the prime factorization of $n$. Also, suppose that $t_1, \ldots, t_k$ are given positive divisors of $n$. There are the following two cases:

(i) If there exists some $t_i$ such that $t_i \neq 1$ then there exists $a = (a_1, \ldots, a_k) \in \mathbb{Z}_n^k \setminus \{0\}$ such that for every prime $p \mid n$ we have $m_p(a_1, t_1, \ldots, a_k, t_k) > r_p$.

(ii) If $t_i = 1$ ($1 \leq i \leq k$) then for every $a = (a_1, \ldots, a_k) \in \mathbb{Z}_n^k \setminus \{0\}$ there exists at least one prime $p \mid n$ such that $m_p(a_1, \ldots, a_k) \leq r_p$.

Proof. (i) WLOG, let $t_1 \neq 1$, say, $t_1 = t$ with $t \mid n$ and $t > 1$. Take $a_1 = \frac{n}{t}$ and $a_2 = \cdots = a_k = 0$. Now, for every prime $p \mid n$ we have $p^{r_p} \mid a_i t_i$ ($1 \leq i \leq k$). Therefore, for every prime $p \mid n$ we have $m_p(\frac{n}{t}, t, 0, t_2, \ldots, 0, t_k) > r_p$.

(ii) Let $t_i = 1$ ($1 \leq i \leq k$) and $a = (a_1, \ldots, a_k) \in \mathbb{Z}_n^k \setminus \{0\}$ be given. Suppose that for every prime $p \mid n$ we have $m_p(a_1, \ldots, a_k) > r_p$. This implies that for every prime $p \mid n$ we have $p^{r_p} \mid a_i$ ($1 \leq i \leq k$). Therefore, we get $n \mid a_i$ ($1 \leq i \leq k$) which is not possible because there exists some $i$ such that $a_i \in \mathbb{Z}_n \setminus \{0\}$. \hfill \Box

Now, we are ready to investigate the $\varepsilon$-almost-universality of GRDH.

Theorem 3.3. Let $n$ and $k$ be positive integers ($n, k > 1$). The family GRDH is an $\varepsilon$-AU family of hash functions for some $\varepsilon < 1$ if and only if $n$ is odd and $(x_i, n) = t_i = 1$ ($1 \leq i \leq k$). Furthermore, if these conditions are satisfied then GRDH (which is then reduced to RDH) is $\frac{1}{p_1 \cdot \cdots \cdot p_k}$-AU, where $p_1$ is the smallest prime divisor of $n$. This bound is tight.

Proof. Assume the setting of the family GRDH, and that $t = (t_1, \ldots, t_k)$ is given. Let $n > 1$ and for every prime divisor $p$ of $n$ let $r_p$ be the exponent of $p$ in the prime factorization of $n$. Suppose that $m = (m_1, \ldots, m_k) \in \mathbb{Z}_n^k$ and $m' = (m_1', \ldots, m_k') \in \mathbb{Z}_n^k$ are any two distinct
messages. Put $a = \langle a_1, \ldots, a_k \rangle = m - m'$. Since $m \neq m'$, there exists some $i$ such that $a_i \neq 0$. If in the family GRDH there is a collision between $m$ and $m'$, this means that there exists $x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ with $(x_i, n) = t_i, t_i \mid n \ (1 \leq i \leq k)$ such that $\Upsilon_x(m) = \Upsilon_x(m')$. Clearly,

$$\Upsilon_x(m) = \Upsilon_x(m') \iff \sum_{i=1}^{k} a_i x_i \equiv 0 \pmod{n}.$$ 

So, we need to find the number of solutions $x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ of the restricted linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv 0 \pmod{n}$, with $(x_i, n) = t_i, t_i \mid n \ (1 \leq i \leq k)$. Here, since $b = 0$, none of the two cases stated in the first part of Theorem 2.2 holds. Thus, by formula (2.3), there are exactly

$$\prod_{i=1}^{k} \varphi \left( \frac{n}{t_i} \right) \prod_{p \mid n, m_p \leq r_p} p^{m_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p - 1}}{(p - 1)^{e_p - 1}} \right)$$

(3.3)

choices for such $x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ that satisfy the aforementioned restricted linear congruence, where the last product is over the prime factors $p$ of $n$ with $m_p \leq r_p$, $r_p$ is the exponent of $p$ in the prime factorization of $n$, $m_p$ is the smallest $j \geq 1$ such that there is some $i$ with $p^j \nmid a_i t_i$, and

$$e_p = \# \{i : 1 \leq i \leq k, p^{m_p} \nmid a_i t_i \}.$$ 

Also, since $(x_i, n) = t_i \ (1 \leq i \leq k)$, the total number of choices for $\langle x_1, \ldots, x_k \rangle$ is $\prod_{i=1}^{k} \varphi \left( \frac{n}{t_i} \right)$. Therefore, given any $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$, the collision probability is exactly

$$P_a(n, t) = \prod_{p \mid n, m_p \leq r_p} p^{m_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p - 1}}{(p - 1)^{e_p - 1}} \right).$$

(3.4)

Now, there are two cases:

(i) If for a prime $p \mid n$ we have $m_p \leq r_p$ then, by (3.4), the term corresponding to this $p$ in $P_a(n, t)$ equals

$$p^{m_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p - 1}}{(p - 1)^{e_p - 1}} \right) \leq p^{r_p - r_p - 1} \left( 1 - \frac{(-1)^{2 - 1}}{(p - 1)^{2 - 1}} \right) = \frac{1}{p - 1}.$$

(ii) If for a prime $p \mid n$ we have $m_p > r_p$ then, by (3.4), the term corresponding to this $p$ in $P_a(n, t)$ equals 1.

Let there exists some $i_0$ such that $t_{i_0} \neq 1$. Then, by Lemma 3.2(i), there exists $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$ such that for every prime $p \mid n$ we have $m_p(a_1, t_1, \ldots, a_k, t_k) > r_p$. Now, by (3.4) and case (ii) above, the collision probability for this specific $a$ is exactly one. Now, assume that $t_i = 1 \ (1 \leq i \leq k)$. Then, if $n$ is even, by taking $a_1 = a_2 = \frac{n}{2}$ and $a_3 = \cdots = a_k = 0$, one can see that $m_2(a_1, \frac{n}{2}, 0, \ldots, 0) = r_2$ and $e_2 = 2$, and for every other prime $p \mid n$ we have $m_p(\frac{n}{2}, \frac{n}{2}, 0, \ldots, 0) > r_p$. Now, by (3.4) and case (ii) above, the collision probability for this specific $a$ is exactly one.
Now, suppose that $n$ is odd and $t_i = 1$ ($1 \leq i \leq k$). Then, by Lemma 3.2(ii), for every $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$ there exists at least one prime $p \mid n$ such that $m_p(a_1, \ldots, a_k) \leq r_p$.

Now, by (3.4) and cases (i), (ii) above, one can see that

$$\max_{a=m-m'\in\mathbb{Z}_n^k \setminus \{0\}} P_a(n, t)$$

is achieved in a specific $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$ for which there exists exactly one prime $p \mid n$ such that $m_p(a_1, \ldots, a_k) \leq r_p$, and furthermore, $p$ has to be the smallest prime divisor of $n$ that we denote by $p_{\min}$.

Consequently, if $n$ is odd and $(x_i, n) = t_i = 1$ ($1 \leq i \leq k$) then for any two distinct messages $m, m' \in \mathbb{Z}_n^k$, we have

$$\Pr_{x \leftarrow \text{GRDH}}[\Upsilon_x(m) = \Upsilon_x(m')] \leq \max_{a=m-m'\in\mathbb{Z}_n^k \setminus \{0\}} P_a(n, t) \leq \frac{1}{p_{\min} - 1} \leq \frac{1}{2}.$$

Therefore, if $n$ is odd and $(x_i, n) = t_i = 1$ ($1 \leq i \leq k$) then GRDH (which is then reduced to RDH) is $\frac{1}{p_{\min} - 1}$-AU. We also note that this bound is tight: take $a_1 = a_2 = \frac{n}{p_{\min}}$ and $a_3 = \ldots = a_k = 0$. So, we get that $m_{p_{\min}}(\frac{n}{p_{\min}}, \frac{n}{p_{\min}}, 0, \ldots, 0) = r_{p_{\min}}$ and $e_{p_{\min}} = 2$, and for every other prime $p \mid n$ we get that $m_p(\frac{n}{p_{\min}}, \frac{n}{p_{\min}}, 0, \ldots, 0) > r_p$. Now, by (3.4) and case (ii) above, the collision probability for any two distinct messages is ‘exactly zero’.

The following remark gives a necessary and sufficient condition for the $\epsilon$-almost-universality of the family GRDH in the case of $k = 1$. We omit the proof as it is simply obtained from the above argument (this special case can be also proved directly, or, from [8, Th. 3.1]).

**Remark 3.4.** If $k = 1$ then the family GRDH is an $\epsilon$-AU family of hash functions for some $\epsilon < 1$ if and only if $(x_1, n) = t_1 = 1$. Furthermore, if $(x_1, n) = t_1 = 1$ then the collision probability for any two distinct messages is ‘exactly zero’.

Now, we investigate the $\epsilon$-almost-\(\triangle\)-universality of GRDH. Note the change from $k > 1$ in Theorem 3.3 to $k \geq 1$ in Theorem 3.5. The proof idea is similar to that of Theorem 3.3; so, in the proof we only write the parts which need more arguments.

**Theorem 3.5.** Let $n$ and $k$ be positive integers ($n > 1$). The family GRDH is an $\epsilon$-A\(\triangle\)U family of hash functions for some $\epsilon < 1$ if and only if $n$ is odd and $(x_i, n) = t_i = 1$ ($1 \leq i \leq k$). Furthermore, if these conditions are satisfied then GRDH (which is then reduced to RDH) is $\frac{1}{p-1}$-A\(\triangle\)U, where $p$ is the smallest prime divisor of $n$. This bound is tight.

**Proof.** Assume the setting of the family GRDH, and that $t = \langle t_1, \ldots, t_k \rangle$ is given. Let $n > 1$ and for every prime divisor $p$ of $n$ let $r_p$ be the exponent of $p$ in the prime factorization of $n$. If for a given $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$ and a given $b \in \mathbb{Z}_n$ there is a prime $p \mid n$ such that $m_p \leq r_p$ and $p^{m_p - 1} \mid b$, or, such that $m_p \geq r_p + 1$ and $p^{r_p + 1} \mid b$, then, by the first part of Theorem 2.2, the probability that we have $\Upsilon_x(m) - \Upsilon_x(m') = b$ is exactly zero. Otherwise, given any $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$ and any $b \in \mathbb{Z}_n$, the probability that we have $\Upsilon_x(m) - \Upsilon_x(m') = b$ is exactly

$$Q_{a,b}(n, t) = \prod_{\substack{p \mid n \atop m_p \leq r_p \atop p^{m_p} \mid b}} p^{m_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p - 1}}{(p - 1)^{e_p - 1}} \right) \prod_{\substack{p \mid n \atop m_p \leq r_p \atop p^{m_p - 1} \parallel b}} p^{m_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p}}{(p - 1)^{e_p}} \right). \quad (3.5)$$

10
Now, there are three cases:

(i) If for a prime $p | n$ we have $m_p \leq r_p$ and $p^{m_p - 1} \parallel b$ then, by (3.5), the term corresponding to this $p$ in $Q_{a,b}(n,t)$ equals

$$p^{m_p - r_p - 1} \left(1 - \frac{(-1)^{r_p}}{(p-1)^{r_p}}\right) \leq p^{r_p - r_p - 1} \left(1 - \frac{(-1)^1}{(p-1)^1}\right) = 1 - \left(\frac{1}{p-1}\right)^r.$$ 

(ii) If for a prime $p | n$ we have $m_p \leq r_p$ and $p^{m_p} | b$ then, by (3.5), the term corresponding to this $p$ in $Q_{a,b}(n,t)$ equals

$$p^{m_p - r_p - 1} \left(1 - \frac{(-1)^{r_p}}{(p-1)^{r_p}}\right) \leq p^{r_p - r_p - 1} \left(1 - \frac{(-1)^{2-1}}{(p-1)^2-1}\right) = 1 - \left(\frac{1}{p-1}\right)^r.$$ 

(iii) If for a prime $p | n$ we have $m_p > r_p$ and $p^{r_p} | b$ then, by (3.5), the term corresponding to this $p$ in $Q_{a,b}(n,t)$ equals $1$.

If there exists some $t_0$ such that $t_i \neq 1$ then the argument is exactly the same as before (just take $b = 0$). Now, assume that $t_i = 1$ for $1 \leq i \leq k$. Then, if $n$ is even, take $a_1 = b = \frac{n}{2}$ and $a_2 = \cdots = a_k = 0$. Now, one can see that, by (3.5) and case (iii) above, the probability that we have $\Upsilon_x(m) - \Upsilon_x(m') = b$ for these specific $a$ and $b$ is exactly one.

Now, suppose that $n$ is odd and $t_i = 1$ for $1 \leq i \leq k$. Then, by (3.5), Lemma 3.2(ii), and cases (i), (ii), (iii) above, one can see that

$$\max_{a=m-m'\in\mathbb{Z}_n^k\setminus\{0\}} Q_{a,b}(n,t)$$

is achieved in a specific $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$ and a specific $b \in \mathbb{Z}_n$ for which there exists exactly one prime $p | n$ such that $m_p(a_1, \ldots, a_k) \leq r_p$ and $p^{m_p - 1} \parallel b$, or, $m_p(a_1, \ldots, a_k) \leq r_p$ and $p^{m_p} | b$, and also $p^{r_p} | b$ for every other prime $p | n$; furthermore, $p$ has to be the smallest prime divisor of $n$ that we denote by $p_{\min}$.

Consequently, if $n$ is odd and $(x_i,n) = t_i = 1$ for $1 \leq i \leq k$ then for any two distinct messages $m, m' \in \mathbb{Z}_n^k$ and all $b \in \mathbb{Z}_n$, we have

$$\Pr_{x \leftarrow \text{GRDH}}[\Upsilon_x(m) - \Upsilon_x(m') = b] \leq \max_{a=m-m'\in\mathbb{Z}_n^k\setminus\{0\}} Q_{a,b}(n,t) \leq \frac{1}{p_{\min} - 1} \leq \frac{1}{2}.$$ 

Therefore, if $n$ is odd and $(x_i,n) = t_i = 1$ for $1 \leq i \leq k$ then GRDH (which is then reduced to RDH) is $\frac{1}{p_{\min} - 1} \cdot A \Delta U$. We also note that this bound is tight: take $a_1 = b = \frac{n}{p_{\min}}$ and $a_2 = \cdots = a_k = 0$. Now, by (3.5) and case (iii) above, one can see that the probability that we have $\Upsilon_x(m) - \Upsilon_x(m') = b$ for these specific $a$ and $b$ is exactly $\frac{1}{p_{\min} - 1}$. $\square$

**Remark 3.6.** While the proofs of Theorem 3.3 and Theorem 3.5 are quite simple and in fact are just a straightforward application of Theorem 2.2, but there may be other simpler proofs (say, without relying on the counting arguments as we do) for these results. However, given the general statements of Theorem 3.3 and Theorem 3.5, possible simpler proofs for these results which cover the ‘whole’ statements may not be necessarily that shorter. Besides, we believe that our proof techniques have their own merit and these connections and techniques may motivate more work in universal hashing and related areas.
Remark 3.7. If in Theorem 3.5 we let $k = 1$, then we get the main result of the paper by Alomair et al. [1, Th. 5.11] which was obtained via a very long argument.

Remark 3.8. Using Theorem 2.2 and the idea of the proof of Theorem 3.5 one can see that there are cases in which the collision probability in the family GRDH is ‘exactly zero’ (Corollary 2.3 completely characterizes all these cases). This can be considered as an advantage of the family GRDH and is not the case in the family MMH*, as the collision probability in MMH* is always exactly $\frac{1}{p}$ which never vanishes.

4 Applications to authentication with secrecy

As an application of the results of the preceding section, we propose an authentication code with secrecy scheme which generalizes a recent construction [1, 3]. We remark that Alomair et al. have applied their scheme in several other papers; see, e.g., [2] for an application of this approach in the authentication problem in RFID systems. So, our results may have implications in those applications, as well. We adopt the notation of [30] in specifying the syntax of these codes. In particular, we consider key-indexed families of coding rules.

An authentication code with secrecy (or code for short) is a tuple $C = (S, M, K, E, D)$, specified by the following sets: $S$ of source states (or plaintexts), $M$ of messages (or ciphertexts), $K$ of keys, $E$ of authenticated encryption (AE) functions and $D$ of verified decryption functions. The sets $E$ and $D$ are indexed by $K$. For $k \in K$, $E_k : S \rightarrow M$ is the associated authenticated encryption function and by $D_k : M \rightarrow S \cup \{\bot\}$ is the associated verified decryption function. The encryption and decryption functions have the property that for every $m \in S$, $D_k(E_k(m)) = m$. Moreover, for any $c \in M$, if $c \neq E_k(m)$ for some $m \in S$, $D_k(c) = \bot$.

Before presenting our construction, we first note that although it is not explicitly stated in [1, 3], the construction given there is correct only for the case of a uniform distribution on source states. This will be the case for our construction, as well. We note that this assumption, while unrealistically strong from a security perspective, is commonly used in the study of authentication codes with secrecy. Following the terminology of [20] (see also [21]), we will call such codes authentication and secrecy codes for equiprobable source probability distributions. Henceforth we will work under the assumption of equiprobable source states.

We now give the security definitions required for authentication and secrecy. We begin with a definition of secrecy.

**Definition 4.1.** We say that $C = (S, M, K, E, D)$ provides $\varepsilon$-secrecy on $S' \subseteq S$ if every $m \in S'$ and $c \in M$,

$$\Pr_{m' \leftarrow S, k \leftarrow K} [m' = m | E_k(m') = c] \leq \varepsilon.$$  

Thus, $\frac{1}{|S|}$-secrecy on $S$ corresponds to the standard notion of Shannon secrecy [42] (for a uniform message distribution.)

With respect to authentication, we restrict attention to substitution attacks, also known as spoofing attacks of order 1. A C-forgery is a mapping $F : M \rightarrow M$. Note that there are
no computational restrictions on $\mathcal{F}$. We say that $C$ is $\delta$-secure against substitution attacks if for every $C$-forger $\mathcal{F}$,

$$\Pr_{m \leftarrow S, k \leftarrow \mathcal{K}, c \leftarrow \mathcal{E}_k(m)}[\mathcal{F}(c) \neq c \land \mathcal{D}_k(\mathcal{F}(c)) \neq \mathcal{\bot}] \leq \delta.$$ 

Finally, we say that $C$ is an $\varepsilon, \delta$-authentication code with secrecy for equiprobable source states on $\mathcal{S}'$ if it is $\varepsilon$-secret on $\mathcal{S}'$ and $\delta$-secure against substitution attacks.

For any $n, k \in \mathbb{N}$, we define $C_{\text{RDH}}^{n,k}$ as follows: $\mathcal{S} = \mathbb{Z}_n^k$, $\mathcal{K} = \mathbb{Z}_n^k \times (\mathbb{Z}_n^*)^k$, $\mathcal{M} = \mathbb{Z}_n^k \times \mathbb{Z}_n$. Thus, source states are $k$-tuples $m = \langle m_1, \ldots, m_k \rangle$, keys are pairs $\langle x, y \rangle$ of $k$-tuples $x = \langle x_1, \ldots, x_k \rangle$, $y = \langle y_1, \ldots, y_k \rangle$, and ciphertexts are pairs $\langle c, t \rangle$.

Note that we will sometimes write pairs using the notation $\cdot || \cdot$, e.g., we write a key pair as $\langle x, y \rangle$. Also, we may abuse terminology, and for a ciphertext $c || t$, call $c$ the ciphertext and $t$ the tag. The authenticated encryption function $\mathcal{E}$ is defined as follows:

$$\mathcal{E}_{x||y}(m) = \Psi_x(m)||\Upsilon_y(m),$$

where $\Upsilon$ is the RDH hash function, and

$$\Psi_x(m) = m + x \pmod{n} = \langle m_1 + x_1 \pmod{n}, \ldots, m_k + x_k \pmod{n} \rangle.$$

To define $\mathcal{D}$, we first define $\Psi^{-1}$:

$$\Psi^{-1}_x(c) = c - x \pmod{n} = \langle c_1 - x_1 \pmod{n}, \ldots, c_k - x_k \pmod{n} \rangle.$$

Then

$$\mathcal{D}_{x||y}(c||t) = \begin{cases} \Psi^{-1}_x(c) & \text{if } \Upsilon_y(\Psi^{-1}_x(c)) = t; \\ \bot & \text{otherwise.} \end{cases}$$

Now, we are ready to state and prove our main result in this section:

**Theorem 4.2.** Let $n, k \in \mathbb{N}$, where $n$ is odd, and $p$ the smallest prime divisor of $n$. Then $C_{\text{RDH}}^{n,k}$ is a $\frac{1}{(p-1)n^{k-1}}, \frac{1}{p-1}$-authentication code with secrecy for equiprobable source states on $\mathbb{Z}_n^k \setminus \{0\}$.

We will establish this theorem by the following sequence of lemmas.

**Lemma 4.3.** Let $n, k \in \mathbb{N}$, where $n$ is odd, and $p$ the smallest prime divisor of $n$. Then $C_{\text{RDH}}^{n,k}$ is $\frac{1}{(p-1)n^{k-1}}$-secret on $\mathbb{Z}_n^k \setminus \{0\}$.

**Proof.** We first note that for any $m, c$, and $t$,

$$\Pr_{m', x \leftarrow \mathbb{Z}_n^k, y \leftarrow (\mathbb{Z}_n^*)^k}[m' = m|\mathcal{E}_{x||y}(m') = c||t] = \Pr_{m' \leftarrow \mathbb{Z}_n^k, y \leftarrow (\mathbb{Z}_n^*)^k}[m = m|\Upsilon_y(m') = t].$$

This follows from the independence of $\Psi_x(m')$ and $\Upsilon_y(m')$, conditioned on $m' = m$, along with the fact that $\Psi$ provides Shannon secrecy. But

$$\Pr_{m' \leftarrow \mathbb{Z}_n^k, y \leftarrow (\mathbb{Z}_n^*)^k}[\Upsilon_y(m') = t|m' = m]/n^{k-1} \leq \frac{1}{(p-1)n^{k-1}},$$
where the equality follows by Bayes’ rule and the fact that for \( m' \sim (\mathbb{Z}_n)^k \) and \( y \sim (\mathbb{Z}_n^*)^k \), \( \Upsilon_y(m') \) is uniformly distributed in \( \mathbb{Z}_n \), and the inequality follows, assuming \( m \neq 0 \), by Theorem 3.5.

We now establish a key hiding property which will be needed to prove resistance to substitution attacks.

**Lemma 4.4.** For \( n, k \in \mathbb{N}, y \in (\mathbb{Z}_n^*)^k, c \in \mathbb{Z}_n^k \) and \( t \in \mathbb{Z}_n \),

\[
\Pr_{\mathbf{x}, m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [y' = y | \xi_{\mathbf{x}}| y'(m) = c | t] = \frac{1}{|\mathbb{Z}_n^*|^k}.
\]

**Proof.** First note that since \( \mathbf{x} \) and \( m \) are chosen independently of \( y' \), it is the case that \( \Psi_{\mathbf{x}}(m) \) and \( y' \) are independent. So we just need to show that

\[
\Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [y' = y | \Upsilon_y(m) = t] = \frac{1}{|\mathbb{Z}_n^*|^k}.
\]

Note that

\[
\Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [\Upsilon_y(m) = t | y' = y] = \frac{\Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [\Upsilon_y(m) = t \wedge y' = y]}{\Pr_{y' \in (\mathbb{Z}_n^*)^k} [y' = y]} = \frac{\Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [\Upsilon_y(m) = t \wedge y' = y]}{\Pr_{y' \in (\mathbb{Z}_n^*)^k} [y' = y]} = \Pr_{m \in \mathbb{Z}_n^k} [\Upsilon_y(m) = t] \cdot \frac{\Pr_{y' \in (\mathbb{Z}_n^*)^k} [y' = y]}{\Pr_{y' \in (\mathbb{Z}_n^*)^k} [y' = y]} = \Pr_{m \in \mathbb{Z}_n^k} [\Upsilon_y(m) = t] = \frac{1}{|\mathbb{Z}_n|},
\]

where the last equality follows because the product of a uniformly random element of \( \mathbb{Z}_n \) and a fixed element of \( \mathbb{Z}_n^* \) is uniformly distributed in \( \mathbb{Z}_n \), and the sum of a fixed number of uniformly random elements of \( \mathbb{Z}_n \) is uniformly distributed in \( \mathbb{Z}_n \). We now have

\[
\Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [y' = y | \Upsilon_y(m) = t] = \Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [\Upsilon_y(m) = t | y' = y] \cdot \frac{\Pr_{y' \in (\mathbb{Z}_n^*)^k} [y' = y]}{\Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [\Upsilon_y(m) = t]}
\]

But

\[
\Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [\Upsilon_y(m) = t] = \sum_{y \in (\mathbb{Z}_n^*)^k} \Pr_{m \in \mathbb{Z}_n^k, y' \in (\mathbb{Z}_n^*)^k} [\Upsilon_y(m) = t | y' = y] \cdot \Pr_{y' \in (\mathbb{Z}_n^*)^k} [y' = y] = \frac{1}{|\mathbb{Z}_n|}.
\]

Combining this with (4.1) completes the proof. \( \square \)

**Remark 4.5.** This key hiding property does not hold in general. The given proof depends on the fact that \( m \) is uniformly distributed in \( \mathbb{Z}_n^k \).
Lemma 4.6. Let $n, k \in \mathbb{N}$, where $n$ is odd, and $p$ the smallest prime divisor of $n$. Then $C_{RDH}^{n,k}$ is $\frac{1}{p-1}$-secure against substitution attacks.

Proof. By way of contradiction suppose that $\mathcal{F}$ produces a substitution with probability greater than $\frac{1}{p-1}$. By averaging, there must be some $m \in \mathbb{Z}_n^k$ such that if $E_x || y(m) = c || t$, for random $x$ and $y$, then $\mathcal{F}(c||t) = c'||t'$ such that $c'||t' \neq c||t$ and $\Upsilon_y(\Phi^{-1}_x(c')) = t'$. Let $b = t - t'$ and $m' = (\Phi^{-1}_x(c'))$. Note that it must be the case that $m' \neq m$. By the preceding lemma, $y$ and $m'$ are statistically independent. So,

$$\Upsilon_y(m) - \Upsilon_y(m') = b,$$

for randomly chosen $y \in (\mathbb{Z}_n^*)^k$, violating that RDH is $\frac{1}{p-1}$-A∆U by Theorem 3.5. □

4.1 Discussion

The proposed scheme, which is a generalization of the scheme proposed in [1, 3], is defined using the encrypt-and-authenticate paradigm (see [4, 25] and the references therein, for a detailed discussion about these generic constructions and their security analysis). Since this approach requires the decryption of a purported ciphertext before its authentication, it is susceptible to attacks if the implementation of the decryption function leaks information when given invalid ciphertexts. Surprisingly, the preferred encrypt-then-authenticate approach will not work in our setting because it is not key-hiding.

We now show that the assumption that messages are generated uniformly at random is necessary for our result, by showing that any authentication scheme achieving $\varepsilon$-security against substitution attacks for arbitrary source distributions is in fact an $\varepsilon$-ASU hash family.

We begin with some definitions.

Definition 4.7. A authentication code is specified by a tuple $M = (S, T, K, \mathcal{M}, \mathcal{V})$ where $S$ is the set of source states, $T$ is the set of tags, $K$ is the set of keys, $\mathcal{M} : K \times S \rightarrow T$, and $\mathcal{V} : K \times T \rightarrow \{0, 1\}$. It must be the case that for all $k \in K$ and $m \in S$, $\mathcal{V}_k(m||\mathcal{M}_k(m)) = 1$. A forger is a mapping $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ where $\mathcal{F}_1 : S \times T \rightarrow S$ and $\mathcal{F}_2 : S \times T \rightarrow T$. We say $M$ is $\varepsilon$-secure against substitution attacks if for every forger $\mathcal{F}$ and distribution $S$ on $S$,

$$\Pr_{k \leftarrow K, m \leftarrow S, t \leftarrow \mathcal{M}_k(m)}[\mathcal{F}_1(m, t) \neq m \land \mathcal{V}_k(\mathcal{F}(m||t)) = 1] \leq \varepsilon.$$

Theorem 4.8. Suppose $M = (S, T, K, \mathcal{M}, \mathcal{V})$ is $\varepsilon$-secure against substitution attacks. Then $\{\mathcal{M}_k \mid k \in K\}$ is an $\varepsilon$-ASU hash function family.

Proof. Suppose $\{\mathcal{M}_k \mid k \in K\}$ is not an $\varepsilon$-ASU hash family. So there are $m' \neq m'' \in S$ and $t', t'' \in T$ such that $\Pr_{k \leftarrow K}[\mathcal{M}_k(m'') = t'' \land \mathcal{M}_k(m') = t'] > \varepsilon$. Take $\mathcal{F}$ such that
\( F(m'|t') = m''|t''\), and let \( S \) be the distribution on \( S \) which puts all weight on \( m' \). Then

\[
\begin{align*}
\Pr_{k \leftarrow K, m \leftarrow g^S} [F_1(m, t) \neq m \land V_k(F(m||t)) = 1] \\
&= \Pr_{k \leftarrow K, t \leftarrow M_k(m')} [F_1(m', t) \neq m' \land V_k(F(m'||t) = 1] \\
&= \Pr_{k \leftarrow K, t \leftarrow M_k(m')} [F_1(m', t) \neq m' \land V_k(F(m'||t) = 1] \cdot \Pr_{k \leftarrow K, t \leftarrow M_k(m')} [t = t'] \\
&= \Pr_{k \leftarrow K, t \leftarrow M_k(m')} [m'' \neq m' \land M_k(m'') = t' \land M_k(m') = t'] \\
&> \varepsilon.
\end{align*}
\]

\[\square\]

Acknowledgements

The authors would like to thank Martin Dietzfelbinger, Igor Shparlinski, and Roberto Tauraso for helpful comments on earlier versions of this paper. During the preparation of this work the first author was supported by a Fellowship from the University of Victoria (UVic Fellowship).

References


