# On an almost-universal hash function family with applications to authentication and secrecy codes[*]

Khodakhast Bibak [†]    Bruce M. Kapron [†]    Venkatesh Srinivasan [†‡]

László Tóth [§]

December 11, 2015

## 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 $p$ be a prime and $k$ be a positive integer. Define

$$\text{MMH}^* := \{g_{\mathbf{x}} \ : \ \mathbb{Z}_p^k \to \mathbb{Z}_p \mid \mathbf{x} \in \mathbb{Z}_p^k\},$$

where

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

for any $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$, and any $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k$. In this paper, we first give a new proof for the $\triangle$-universality of MMH[*], shown by Halevi and Krawczyk in 1997, via a novel approach, namely, 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 $p$ and let the keys $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ satisfy the conditions $\gcd(x_i, n) = t_i$ $(1 \le i \le k)$, where $t_1, \ldots, t_k$ are given positive divisors of $n$. Applying our aforementioned approach, we prove that the family GRDH is an $\varepsilon$-almost-$\triangle$-universal family of hash functions for some $\varepsilon < 1$ if and only if $n$ is odd and $\gcd(x_i, n) = t_i = 1$ $(1 \le i \le k)$. Furthermore, if these conditions are satisfied then GRDH is $\frac{1}{p-1}$-almost-$\triangle$-universal, where $p$ is the smallest prime divisor of $n$. Finally, as an application of our results, we give a generalization of the authentication code with secrecy studied by Alomair, Clark, and Poovendran.

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

---

# 1    Introduction

Universal hash functions, discovered by Carter and Wegman [8], have many applications in computer science, including cryptography and information security [7, 11, 13, 14, 16, 17, 35, 46, 47], pseudorandomness [15, 33], complexity theory [37, 42], randomized algorithms [20, 31], data structures [34, 41], and parallel computing [21, 25]. 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 [13].

## 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 ([8]) 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 $\frac{1}{|R|} \le \varepsilon < 1$. 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 $\triangle$-universality was introduced in [22, 36, 43]. Suppose that $R$ is an Abelian group. We say that $H$ is a *$\triangle$-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 *$\varepsilon$-almost-$\triangle$-universal* ($\varepsilon$-A$\triangle$U) if this probability is at most $\varepsilon$, $\frac{1}{|R|} \le \varepsilon < 1$. We remark that $\varepsilon$-A$\triangle$U families have applications to message authentication. Informally, it is possible to design a message authentication scheme using $\varepsilon$-A$\triangle$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 $\varepsilon$ ([13]).

Finally, in Section 4 on authentication codes with secrecy, we need the notion of strong universality which was introduced in [47]. 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 *$\varepsilon$-almost-strongly-universal* ($\varepsilon$-ASU) if this probability is at most $\varepsilon$, $\frac{1}{|R|^2} \le \varepsilon < \frac{1}{|R|}$.

We now provide a formal definition of the concepts introduced above as in [13]. 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 $\frac{1}{|R|} \le \varepsilon < 1$. The probabilities below, are taken over the random choice of hash function $h$ from the set $H$.

2

- The family $H$ is a *universal family of hash functions* if for any two distinct $x, y \in D$, we have $\Pr_{h \leftarrow H}[h(x) = h(y)] \leq \frac{1}{|R|}$. 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 ($\varepsilon$-A$\triangle$U) 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 $\Pr_{h \leftarrow H}[h(x) = a, \ h(y) = b] = \frac{1}{|R|^2}$. 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 $\Pr_{h \leftarrow H}[h(x) = a, \ h(y) = b] \leq \frac{\varepsilon}{|R|}$.

## 1.2 MMH$^*$

The hash function family we study, GRDH, is a variant of a well-known family which was named MMH$^*$ by Halevi and Krawczyk [13]. Let $p$ be a prime and $k$ be a positive integer. Each hash function in the family MMH$^*$ takes as input a $k$-tuple, $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k$. It computes the dot product of $\mathbf{m}$ with a fixed $k$-tuple $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$ 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:

$$\text{MMH}^* := \{g_{\mathbf{x}} \ : \ \mathbb{Z}_p^k \to \mathbb{Z}_p \mid \mathbf{x} \in \mathbb{Z}_p^k\}, \tag{1.1}$$

where

$$g_{\mathbf{x}}(\mathbf{m}) := \mathbf{m} \cdot \mathbf{x} \pmod{p} = \sum_{i=1}^{k} m_i x_i \pmod{p}, \tag{1.2}$$

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

The family MMH$^*$ is widely attributed to Carter and Wegman [8], while it seems that Gilbert, MacWilliams, and Sloane [12] had already discovered it (but in the finite geometry setting). Halevi and Krawczyk [13], using the multiplicative inverse method, proved that MMH$^*$ is a $\triangle$-universal family of hash functions. We also remark that, recently, Leiserson et al. [25] rediscovered MMH$^*$ (called it "DOTMIX compression function family") and using the same method as of Halevi and Krawczyk [13] 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.** ([13, 25]) *The family* MMH$^*$ *is a $\triangle$-universal family of hash functions.*

3

## 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 $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ 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? Clearly, the multiplicative inverse method does not work in this case and new techniques are needed. 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 Theroem 1.3 for the $\triangle$-universality of MMH* via a new approach, namely, 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 $\mathbb{Z}_\ltimes^k \setminus \{\mathbf{0}\}$, 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 $\mathbf{x} = \langle x_1, \ldots, x_k \rangle$ from $\mathbb{Z}_n^{*k}$, or more generally, choosing the keys $\mathbf{x} = \langle x_1, \ldots, x_k \rangle$ 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

4

key ingredient in the proofs is an explicit formula for the number of solutions of restricted linear congruences, recently obtained by Bibak et al. [6], 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 $p^r \mid\mid a$ if $p^r \mid a$ and $p^{r+1} \nmid a$. We also use $\mathbf{0}$ to denote the vector of all zeroes. The multiplicative group of integers modulo $n$ is denoted by $\mathbb{Z}_n^*$.

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

$$a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}. \tag{2.1}$$

By a solution of (2.1), we mean an $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ that satisfies (2.1). The following result, proved by D. N. Lehmer [24], 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 $a_1 x_1 + \cdots + a_k x_k \equiv b$ (mod $n$) 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 [26] where it is used as a key ingredient in studying the subset sum problem for finite Abelian groups ([26]).

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 [6], 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 [5, 9, 10, 27, 29, 32, 38, 39, 44, 45]). Recently, Bibak et al. [6] 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

$$a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}, \quad (x_i, n) = t_i \ (1 \leq i \leq k), \tag{2.2}$$

where $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \geq 1)$ 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 $b = 0$, $a_i = 1$,

$t_i = \frac{n}{m_i}$, $m_i \mid n$ $(1 \le i \le k)$ is related to the *orbicyclic* (multivariate arithmetic) function ([27]), which has very interesting combinatorial and topological applications, in particular, in counting non-isomorphic maps on orientable surfaces. See [6] for a detailed discussion about restricted linear congruences and their applications.

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

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

$$e_p = e_p(a_1, t_1, \dots, a_k, t_k) = \#\{i : 1 \le i \le k, p^{\mathfrak{m}_p} \nmid a_i t_i\}.$$

By definition, $1 \le e_p \le$ the number of $i$ such that $a_i \ne 0$. Note that in many situations instead of $\mathfrak{m}_p(a_1, t_1, \dots, a_k, t_k)$ we write $\mathfrak{m}_p$ and instead of $e_p(a_1, t_1, \dots, a_k, t_k)$ we write $e_p$ for short. However, it is important to note that both $\mathfrak{m}_p$ and $e_p$ always depend on $a_1, t_1, \dots, a_k, t_k, p$.

**Theorem 2.2.** ([6]) *Let $a_i, t_i, b, n \in \mathbb{Z}$, $n \ge 1$, $t_i \mid n$ $(1 \le i \le k)$ and assume that $a_i \ne 0$ for at least one $i$. Consider the linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ $(1 \le i \le k)$. If there is a prime $p \mid n$ such that $\mathfrak{m}_p \le r_p$ and $p^{\mathfrak{m}_p - 1} \nmid b$ or $\mathfrak{m}_p \ge r_p + 1$ and $p^{r_p} \nmid b$, then the linear congruence has no solution. Otherwise, the number of solutions is*

$$\prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right) \prod_{\substack{p \mid n \\ \mathfrak{m}_p \le r_p \\ p^{\mathfrak{m}_p} \mid b}} p^{\mathfrak{m}_p - r_p - 1}\left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \prod_{\substack{p \mid n \\ \mathfrak{m}_p \le r_p \\ p^{\mathfrak{m}_p - 1} \| b}} p^{\mathfrak{m}_p - r_p - 1}\left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right), \qquad (2.3)$$

*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.** ([6]) *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 $\mathfrak{m}_p \le r_p$ and $p^{\mathfrak{m}_p - 1} \nmid b$;*
*(ii) there is a prime $p \mid n$ with $\mathfrak{m}_p \ge r_p + 1$ and $p^{r_p} \nmid b$;*
*(iii) there is a prime $p \mid n$ with $\mathfrak{m}_p \le r_p$, $e_p = 1$ and $p^{\mathfrak{m}_p} \mid b$;*
*(iv) $n$ is even, $\mathfrak{m}_2 \le r_2$, $e_2$ is odd and $2^{\mathfrak{m}_2} \mid b$;*
*(v) $n$ is even, $\mathfrak{m}_2 \le r_2$, $e_2$ is even and $2^{\mathfrak{m}_2 - 1} \| b$.*

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

6

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 [30] proposed a generalization of this problem to arbitrary rings, and studied its average-case complexity. This *generalized knapsack problem*, proposed by Micciancio [30], 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, 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.

## 3  GRDH

In this section, we introduce a variant of MMH$^*$ that we call GRDH (generalized restricted dot product hash). Then we investigate the $\varepsilon$-almost-universality and $\varepsilon$-almost-$\triangle$-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 $\triangle$-universality of MMH$^*$ using this technique.

*A New Proof for Theorem 1.3.* Let $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k$ and $\mathbf{m}' = \langle m_1', \ldots, m_k' \rangle \in \mathbb{Z}_p^k$ be any two distinct messages. Put $\mathbf{a} = \langle a_1, \ldots, a_k \rangle = \mathbf{m} - \mathbf{m}'$. Since $\mathbf{m} \neq \mathbf{m}'$, so there exists some $i$ $(1 \leq i \leq k)$ such that $a_i \neq 0$. Now, for $b \in \mathbb{Z}_p$ we have

$$g_{\mathbf{x}}(\mathbf{m}) - g_{\mathbf{x}}(\mathbf{m}') = b \iff \sum_{i=1}^k m_i x_i - \sum_{i=1}^k m_i' x_i \equiv b \pmod{p} \iff \sum_{i=1}^k a_i x_i \equiv b \pmod{p}.$$

So, we need to find the number of solutions $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$ of the latter linear congruence. Since

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

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

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

Thus, MMH$^*$ is $\triangle$-universal. □

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:

$$\text{RDH} := \{\Upsilon_{\mathbf{x}} \; : \; \mathbb{Z}_n^k \to \mathbb{Z}_n \; : \; \mathbf{x} \in \mathbb{Z}_n^{*k}\}, \tag{3.1}$$

where

$$\Upsilon_{\mathbf{x}}(\mathbf{m}) := \mathbf{m} \cdot \mathbf{x} \pmod{n} = \sum_{i=1}^{k} m_i x_i \pmod{n}, \tag{3.2}$$

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

It is easy to see that GRDH is not $\varepsilon$-AU, for 'all' positive integers $n$. So, it would be an interesting question to investigate for which values of $n$, GRDH is $\varepsilon$-AU or $\varepsilon$-A$\triangle$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 $i_0$ ($1 \leq i_0 \leq k$) such that $t_{i_0} \neq 1$ then there exists $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ such that for every prime $p \mid n$ we have $\mathfrak{m}_p(a_1, t_1, \ldots, a_k, t_k) > r_p$.*
*(ii) If $t_i = 1$ ($1 \leq i \leq k$) then for every $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ there exists at least one prime $p \mid n$ such that $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$.*

*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 $\mathfrak{m}_p(\frac{n}{t}, t, 0, t_2, \ldots, 0, t_k) > r_p$.
(ii) Let $t_i = 1$ ($1 \leq i \leq k$) and $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ be given. Suppose that for every prime $p \mid n$ we have $\mathfrak{m}_p(a_1, \ldots, a_k) > r_p$. 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 $i$ ($1 \leq i \leq k$) such that $a_i \in \mathbb{Z}_n \setminus \{0\}$. $\qquad \square$

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 $\frac{1}{p-1}$-AU, where $p$ is the smallest prime divisor of $n$. This bound is tight.*

*Proof.* Assume the setting of the family GRDH, and that $\mathbf{t} = \langle t_1, \ldots, t_k \rangle$ 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 $n$. Suppose that $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_n^k$ and $\mathbf{m}' = \langle m_1', \ldots, m_k' \rangle \in \mathbb{Z}_n^k$ are any two distinct messages. Put $\mathbf{a} = \langle a_1, \ldots, a_k \rangle = \mathbf{m} - \mathbf{m}'$. Since $\mathbf{m} \neq \mathbf{m}'$, so there exists some $i$ ($1 \leq i \leq k$) such that $a_i \neq 0$. If in the family GRDH there is a collision between $\mathbf{m}$ and $\mathbf{m}'$, this means

8

that there exists $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ with $(x_i, n) = t_i$, $t_i \mid n$ $(1 \leq i \leq k)$ such that $\Upsilon_{\mathbf{x}}(\mathbf{m}) = \Upsilon_{\mathbf{x}}(\mathbf{m}')$. Clearly,

$$\Upsilon_{\mathbf{x}}(\mathbf{m}) = \Upsilon_{\mathbf{x}}(\mathbf{m}') \Longleftrightarrow \sum_{i=1}^{k} m_i x_i \equiv \sum_{i=1}^{k} m_i' x_i \pmod{n} \Longleftrightarrow \sum_{i=1}^{k} a_i x_i \equiv 0 \pmod{n}.$$

So, we need to find the number of solutions $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ 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 $b = 0$ so none of the two cases stated in the first part of Theorem 2.2 holds. Thus, by formula (2.3), there are exactly

$$\prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right) \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p}} p^{\mathfrak{m}_p - r_p - 1}\left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \tag{3.3}$$

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

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

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

$$P_{\mathbf{a}}(n, \mathbf{t}) = \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p}} p^{\mathfrak{m}_p - r_p - 1}\left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right). \tag{3.4}$$

Now, there are two cases:

*(i)* If for a prime $p \mid n$ we have $\mathfrak{m}_p \leq r_p$ then, by (3.4), the term corresponding to this $p$ in $P_{\mathbf{a}}(n, \mathbf{t})$ equals

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

*(ii)* If for a prime $p \mid n$ we have $\mathfrak{m}_p > r_p$ then, by (3.4), the term corresponding to this $p$ in $P_{\mathbf{a}}(n, \mathbf{t})$ equals 1.

Let there exists an $i_0$ $(1 \leq i_0 \leq k)$ such that $t_{i_0} \neq 1$. Then, by Lemma 3.2(i), there exists $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ such that for every prime $p \mid n$ we have $\mathfrak{m}_p(a_1, t_1, \ldots, a_k, t_k) > r_p$. Now, by (3.4) and case (ii) above, the collision probability for this specific $\mathbf{a}$ 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 $\mathfrak{m}_2(\frac{n}{2}, \frac{n}{2}, 0, \ldots, 0) = r_2$ and $e_2 = 2$, and for every other prime $p \mid n$ we have $\mathfrak{m}_p(\frac{n}{2}, \frac{n}{2}, 0, \ldots, 0) > r_p$. Now, by (3.4) and case (ii) above, the collision probability for this specific $\mathbf{a}$ is *exactly one*.

9

Now, suppose that $n$ is odd and $t_i = 1$ $(1 \leq i \leq k)$. Then, by Lemma 3.2(ii), for every $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ there exists at least one prime $p \mid n$ such that $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$. Now, by (3.4) and cases (i), (ii) above, one can see that

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

is achieved in a specific $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ for which there exists *exactly one* prime $p \mid n$ such that $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$, 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 $\mathbf{m}, \mathbf{m}' \in \mathbb{Z}_n^k$, we have

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

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 $a_3 = \cdots = a_k = 0$. So, we get that $\mathfrak{m}_{p_{\min}}(\frac{n}{p_{\min}}, \frac{n}{p_{\min}}, 0, \ldots, 0) = r_{p_{\min}}$ and $e_{p_{\min}} = 2$, and for every other prime $p \mid n$ we get that $\mathfrak{m}_p(\frac{n}{p_{\min}}, \frac{n}{p_{\min}}, 0, \ldots, 0) > r_p$. Now, by (3.4) and case (ii) above, the collision probability for this specific $\mathbf{a}$ is *exactly* $\frac{1}{p_{\min}-1} \leq \frac{1}{2}$. $\qquad\square$

The following remark gives a necessary and sufficient condition for the $\varepsilon$-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 [6, Th. 3.1]).

**Remark 3.4.** *If $k = 1$ then the family GRDH is an $\varepsilon$-AU family of hash functions for some $\varepsilon < 1$ 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 $\varepsilon$-almost-$\triangle$-universality of GRDH. 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 $\varepsilon$-A$\triangle$U 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 $\frac{1}{p-1}$-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 $\mathbf{t} = \langle t_1, \ldots, t_k \rangle$ 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 $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ and a given $b \in \mathbb{Z}_n$ there is a prime $p \mid n$ such that $\mathfrak{m}_p \leq r_p$ and $p^{\mathfrak{m}_p - 1} \nmid b$, or, such that $\mathfrak{m}_p \geq r_p + 1$ and $p^{r_p} \nmid b$, then, by the first part of Theorem 2.2, the probability that we have $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ is *exactly zero*. Otherwise, given any $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ and any $b \in \mathbb{Z}_n$, the probability that we have $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ is exactly

$$Q_{\mathbf{a},b}(n, \mathbf{t}) = \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p \\ p^{\mathfrak{m}_p} \mid b}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p \\ p^{\mathfrak{m}_p - 1} \| b}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right). \qquad (3.5)$$

10

Now, there are three cases:

*(i)* If for a prime $p \mid n$ we have $\mathfrak{m}_p \leq r_p$ and $p^{\mathfrak{m}_p - 1} \mid\mid b$ then, by (3.5), the term corresponding to this $p$ in $Q_{\mathbf{a},b}(n, \mathbf{t})$ equals

$$p^{\mathfrak{m}_p - r_p - 1} \left( 1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}} \right) \leq p^{r_p - r_p - 1} \left( 1 - \frac{(-1)^1}{(p-1)^1} \right) = \frac{1}{p-1}.$$

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

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

*(iii)* If for a prime $p \mid n$ we have $\mathfrak{m}_p > r_p$ and $p^{r_p} \mid b$ then, by (3.5), the term corresponding to this $p$ in $Q_{\mathbf{a},b}(n, \mathbf{t})$ equals 1.

If there exists some $i_0$ $(1 \leq i_0 \leq k)$ such that $t_{i_0} \neq 1$ then the argument is exactly the same as before (just take $b = 0$). Now, assume that $t_i = 1$ $(1 \leq i \leq k)$. 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 $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ for these specific $\mathbf{a}$ and $b$ is *exactly one*.

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

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

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

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

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

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 $\frac{1}{p_{\min}-1}$-A$\triangle$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 $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ for these specific $\mathbf{a}$ and $b$ is *exactly* $\frac{1}{p_{\min}-1}$. $\qquad\square$

We remark that Theorem 3.5 in the special case of $k = 1$, gives the main result of the paper by Alomair, Clark, and Poovendran [1, Th. 5.11] which was obtained via a very long argument.

**Remark 3.6.** *Using Corollary 2.3 and the idea of the proof of Theorem 3.3 (or 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.*

11

# 4 Applications to authentication with secrecy

As an application of the results of the preceding section, we give a generalization of the authentication code with secrecy presented in [1, 3]. (We remark that Alomair et al. have applied their scheme in several papers; see, e.g., [2] for an application of this approach in the authentication problem in RFID systems.) We adopt the notation of [28] 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 $C = (\mathcal{S}, \mathcal{M}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, specified by the following sets: $\mathcal{S}$ of *source states* (or *plaintexts*), $\mathcal{M}$ of *messages* (or *ciphertexts*), $\mathcal{K}$ of *keys*, $\mathcal{E}$ of *authenticated encryption (AE) functions* and $\mathcal{D}$ of *verified decryption functions*. The sets $\mathcal{E}$ and $\mathcal{D}$ are indexed by $\mathcal{K}$. For $k \in \mathcal{K}$, $\mathcal{E}_k : \mathcal{S} \to \mathcal{M}$ is the associated authenticated encryption function and by $D_k : \mathcal{M} \to \mathcal{S} \cup \{\bot\}$ is the associated verified decryption function. The encryption and decryption functions have the property that for every $m \in \mathcal{S}$, $\mathcal{D}_k(\mathcal{E}_k(m)) = m$. Moreover, for any $c \in \mathcal{M}$, if $c \neq \mathcal{E}_k(m)$ for some $m \in \mathcal{S}$, $\mathcal{D}_k(c) = \bot$.

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 [18] (see also [19]), 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 $C = (\mathcal{S}, \mathcal{M}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ provides $\varepsilon$-*secrecy* on $\mathcal{S}' \subseteq \mathcal{S}$ if every $m \in \mathcal{S}'$ and $c \in \mathcal{M}$,

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

Thus, $\frac{1}{|\mathcal{S}|}$-secrecy on $\mathcal{S}$ corresponds to the standard notion of Shannon secrecy [40] (for a uniform message distribution.)

With respect to authentication, we restrict attention to *substitution attacks*, also known as *spoofing attacks of order* 1. A $C$-*forger* is a mapping $\mathcal{F} : \mathcal{M} \to \mathcal{M}$. 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 $\mathcal{F}$,

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

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 $\mathbf{m} = \langle m_1, \ldots, m_k \rangle$, keys are pairs $\langle \mathbf{x}, \mathbf{y} \rangle$ of $k$-tuples $\mathbf{x} = \langle x_1, \ldots, x_k \rangle$, $\mathbf{y} = \langle y_1, \ldots, y_k \rangle$, and ciphertexts are pairs $\langle \mathbf{c}, t \rangle$.

Note that we will sometimes write pairs using the notation $\cdot || \cdot$ rather than the usual $\langle \cdot, \cdot \rangle$, e.g., we write a key pair as $\mathbf{x} || \mathbf{y}$. Also, we may abuse terminology, and for a ciphertext $\mathbf{c} || t$,

call $\mathbf{c}$ the ciphertext and $t$ the *tag*. The authenticated encryption function $\mathcal{E}$ is defined as follows:

$$\mathcal{E}_{\mathbf{x}||\mathbf{y}}(\mathbf{m}) = \Psi_{\mathbf{x}}(\mathbf{m})||\Upsilon_{\mathbf{y}}(\mathbf{m}),$$

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

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

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

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

Then

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

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 $\Pi_{\mathrm{RDH}}^{n,k}$ is a $\frac{1}{(p-1)n^{k-1}}, \frac{1}{p-1}$-authentication code with secrecy for equiprobable source states on $\mathbb{Z}_{\ltimes}{}^k \setminus \{\mathbf{0}\}$.*

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 $\Pi_{\mathrm{RDH}}^{n,k}$ is $\frac{1}{(p-1)n^{k-1}}$-secret on $\mathbb{Z}_n^k \setminus \{\mathbf{0}\}$.*

*Proof.* We first note that for any $\mathbf{m}$, $\mathbf{c}$, and $t$,

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

This follows from the independence of $\Psi_{\mathbf{x}}(\mathbf{m'})$ and $\Upsilon_{\mathbf{y}}(\mathbf{m'})$, conditioned on $\mathbf{m'} = \mathbf{m}$, along with the fact that $\Psi$ provides Shannon secrecy. But

$$\Pr_{\mathbf{m'}\leftarrow\mathbb{Z}_n^k,\mathbf{y}\leftarrow(\mathbb{Z}_n^*)^k}[\mathbf{m'} = \mathbf{m}|\Upsilon_{\mathbf{y}}(\mathbf{m'}) = t] = \Pr_{\mathbf{m'}\leftarrow\mathbb{Z}_n^k,\mathbf{y}\leftarrow(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}}(\mathbf{m'}) = t|\mathbf{m'} = \mathbf{m}]/n^{k-1}$$

$$\leq \frac{1}{(p-1)n^{k-1}},$$

where the equality follows by Bayes' rule and the fact that for $\mathbf{m'} \leftarrow (\mathbb{Z}_n)^k$ and $\mathbf{y} \leftarrow (\mathbb{Z}_n^*)^k$, $\Upsilon_{\mathbf{y}}(\mathbf{m'})$ is uniformly distributed in $\mathbb{Z}_n$, and the inequality follows, assuming $\mathbf{m} \neq \mathbf{0}$, by Theorem 3.5. $\square$

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

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

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

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

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

Note that

$$\begin{aligned}
\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t|\mathbf{y}'=\mathbf{y}] &= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t\wedge\mathbf{y}'=\mathbf{y}]/\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\
&= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}}(\mathbf{m})=t\wedge\mathbf{y}'=\mathbf{y}]/\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\
&= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k}[\Upsilon_{\mathbf{y}}(\mathbf{m})=t]\cdot\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]/\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\
&= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k}[\Upsilon_{\mathbf{y}}(\mathbf{m})=t]=\frac{1}{|\mathbb{Z}_n|},
\end{aligned}$$

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

$$\begin{aligned}
&\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}|\Upsilon_{\mathbf{y}'}(\mathbf{m})=t]\\
&\qquad= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t|\mathbf{y}'=\mathbf{y}]\cdot\frac{\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]}{\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t]}.\quad(4.1)
\end{aligned}$$

But

$$\begin{aligned}
\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t] &= \sum_{\mathbf{y}\in(\mathbb{Z}_n^*)^k}\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t|\mathbf{y}'=\mathbf{y}]\cdot\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\
&= \frac{1}{|\mathbb{Z}_n|}.
\end{aligned}$$

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

**Remark 4.5.** This key hiding property does not hold in general. The given proof depends on the fact that $\mathbf{m}$ 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 $\Pi_{\mathrm{RDH}}^{n,k}$ 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 $\mathbf{m}\in\mathbb{Z}_n^k$ such that if $\mathcal{E}_{\mathbf{x}||\mathbf{y}}(\mathbf{m})=\mathbf{c}||t$, for random $\mathbf{x}$ and $\mathbf{y}$, then $\mathcal{F}(\mathbf{c}||t)=\mathbf{c}'||t'$ such that $\mathbf{c}'||t'\neq\mathbf{c}||t$ and $\Upsilon_{\mathbf{y}}(\Phi_{\mathbf{x}}^{-1})(\mathbf{c}')=t'$. Let $b=t-t'$ and $\mathbf{m}'=(\Phi_{\mathbf{x}}^{-1})(\mathbf{c}')$. Note that it must be the case that $\mathbf{m}'\neq\mathbf{m}$. By the preceding lemma, $\mathbf{y}$ and $\mathbf{m}'$ are statistically independent. So,

$$\Upsilon_{\mathbf{y}}(\mathbf{m})-\Upsilon_{\mathbf{y}}(\mathbf{m}')=b,$$

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

## 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, 23] 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 $\mathrm{M} = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{M}, \mathcal{V})$ where $\mathcal{S}$ is the set of *source states*, $\mathcal{T}$ is the set of *tags*, $\mathcal{K}$ is the set of *keys*, $\mathcal{M} : \mathcal{K} \times \mathcal{S} \to \mathcal{T}$, and $\mathcal{V} : \mathcal{K} \times \mathcal{T} \to \{0, 1\}$. It must be the case that for all $k \in \mathcal{K}$ and $m \in \mathcal{S}$, $\mathcal{V}_k(m || \mathcal{M}_k(m)) = 1$. A *forger* is a mapping $\mathcal{F} = \langle \mathcal{F}_1, \mathcal{F}_2 \rangle$ where $\mathcal{F}_1 : \mathcal{S} \times \mathcal{T} \to \mathcal{S}$ and $\mathcal{F}_2 : \mathcal{S} \times \mathcal{T} \to \mathcal{T}$. We say $\mathrm{M}$ is *$\varepsilon$-secure against substitution attacks* if for every forger $\mathcal{F}$ and distribution $\mathbf{S}$ on $\mathcal{S}$,

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

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

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

$$\Pr_{\substack{k \leftarrow \mathcal{K}, m \leftarrow \mathbf{S} \mathcal{S} \\ t \leftarrow \mathcal{M}_k(m)}} [\mathcal{F}_1(m, t) \neq m \wedge \mathcal{V}_k(\mathcal{F}(m || t)) = 1]$$

$$= \Pr_{\substack{k \leftarrow \mathcal{K} \\ t \leftarrow \mathcal{M}_k(m')}} [\mathcal{F}_1(m', t) \neq m' \wedge \mathcal{V}_k(\mathcal{F}(m' || t) = 1]$$

$$= \Pr_{\substack{k \leftarrow \mathcal{K} \\ t \leftarrow \mathcal{M}_k(m')}} [\mathcal{F}_1(m', t) \neq m' \wedge \mathcal{V}_k(\mathcal{F}(m' || t) = 1 | t = t'] \cdot \Pr_{\substack{k \leftarrow \mathcal{K} \\ t \leftarrow \mathcal{M}_k(m')}} [t = t']$$

$$= \Pr_{k \leftarrow \mathcal{K}} [\mathcal{F}_1(m', t') \neq m' \wedge \mathcal{V}_k(\mathcal{F}(m' || t') = 1 \wedge \mathcal{M}_k(m') = t']$$

$$= \Pr_{k \leftarrow \mathcal{K}} [m'' \neq m' \wedge \mathcal{M}_k(m'') = t'' \wedge \mathcal{M}_k(m') = t'] > \varepsilon.$$

$\square$

# Acknowledgements

# 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. Cryptol.* **4** (2010), 121–148.

[2] B. Alomair, L. Lazos, and R. Poovendran, Securing low-cost RFID systems: An unconditionally secure approach, *J. Comput. Secur.* **19** (2011), 229–257.

[3] B. Alomair and R. Poovendran, Information theoretically secure encryption with almost free authentication, *J.UCS* **15** (2009), 2937–2956.

[4] M. Bellare and C. Namprempre, Authenticated encryption: relations among notions and analysis of the generic composition paradigm, *Advances in Cryptology — ASIACRYPT 2000*, LNCS **1976**, 2000, 531–545.

[5] K. Bibak, B. M. Kapron, and V. Srinivasan, On a restricted linear congruence, *Int. J. Number Theory*, to appear.

[6] K. Bibak, B. M. Kapron, V. Srinivasan, R. Tauraso, and L. Tóth, Restricted linear congruences, *J. Math. Cryptol.*, revised; arXiv: 1503.01806.

[7] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, UMAC: Fast and secure message authentication, *Advances in Cryptology — CRYPTO 1999*, LNCS **1666**, 1999, 216–233.

[8] J. L. Carter and M. N. Wegman, Universal classes of hash functions, *J. Comput. System Sci* **18** (1979), 143–154.

[9] E. Cohen, A class of arithmetical functions, *Proc. Natl. Acad. Sci. USA* **41** (1955), 939–944.

[10] J. D. Dixon, A finite analogue of the Goldbach problem, *Canad. Math. Bull.* **3** (1960), 121–126.

[11] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, *SIAM J. Comput.* **38** (2008), 97–139.

[12] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, *Bell Syst. Tech. J.* **53** (1974), 405–424.

[13] S. Halevi and H. Krawczyk, MMH: Software message authentication in the Gbit/second rates, *Fast Software Encryption — FSE 1997*, LNCS **1267**, 1997, 172–189.

[14] H. Handschuh and B. Preneel, Key-recovery attacks on universal hash function based MAC algorithms, *Advances in Cryptology — CRYPTO 2008*, LNCS **5157**, 2008, 144–161.

[15] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, A pseudorandom generator from any one-way function, *SIAM J. Comput.* **28** (1999), 1364–1396.

[16] M. Hayashi, General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel, *IEEE Trans. Inf. Theory* **52** (2006), 1562–1575.

[17] M. Hayashi, Exponential decreasing rate of leaked information in universal random privacy amplification, *IEEE Trans. Inf. Theory* **57** (2011), 3989–4001.

[18] M. Huber, Authentication and secrecy codes for equiprobable source probability distributions, *IEEE International Symposium on Information Theory — ISIT 2009*, 1105–1109.

[19] M. Huber, Combinatorial designs for authentication and secrecy codes, *Foundations and Trends in Communications and Information Theory*, 5(6), 581–675, (2010).

[20] R. Impagliazzo and D. Zuckerman, How to recycle random bits, *Proceedings of the 30th Annual Symposium on Foundations of Computer Science — FOCS 1989*, 248–253.

[21] H. J. Karloff, S. Suri, and S. Vassilvitskii, A model of computation for MapReduce, *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms — SODA 2010*, 938–948.

[22] H. Krawczyk, LFSR-based hashing and authentication, *14th Annual International Cryptology Conference — CRYPTO 1994*, 129–139.

[23] H. Krawczyk, The order of encryption and authentication for protecting communications (or: how secure is SSL?), *Advances in Cryptology — CRYPTO 2001*, 310–331.

[24] D. N. Lehmer, Certain theorems in the theory of quadratic residues, *Amer. Math. Monthly* **20** (1913), 151–157.

[25] C. E. Leiserson, T. B. Schardl, and J. Sukha, Deterministic parallel random-number generation for dynamic-multithreading platforms, *Proceedings of the 17th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming — PPoPP 2012*, 193–204.

[26] J. Li and D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Theory Ser. A* **119** (2012), 170–182.

[27] V. A. Liskovets, A multivariate arithmetic function of combinatorial and topological significance, *Integers* **10** (2010), 155–177.

[28] L. McAven, R. Safavi-Naini, and M. Yung, Symmetric authentication codes with secrecy and unconditionally secure authenticated encryption, *Progress in Cryptology — INDOCRYPT 2004*, 148–161.

[29] A. Mednykh and R. Nedela, Enumeration of unrooted maps of a given genus, *J. Combin. Theory Ser. B* **96** (2006), 706–729.

[30] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions, *Comput. Complexity* **16** (2007), 365–411.

[31] R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, (1995).

[32] C. A. Nicol and H. S. Vandiver, A von Sterneck arithmetical function and restricted partitions with respect to a modulus, *Proc. Natl. Acad. Sci. USA* **40** (1954), 825–835.

[33] N. Nisan, Pseudorandom generators for space-bounded computations, *Proceedings of the 22nd Annual ACM symposium on Theory of Computing — STOC 1990*, 204–212.

[34] A. Pagh and R. Pagh, Uniform hashing in constant time and optimal space, *SIAM J. Comput.* **38** (2008), 85–96.

[35] R. Renner and S. Wolf, Simple and tight bounds for information reconciliation and privacy amplification, *Advances in Cryptology — ASIACRYPT 2005*, 199–216.

[36] P. Rogaway, Bucket hashing and its application to fast message authentication, *15th Annual International Cryptology Conference — CRYPTO 1995*, 29–42.

[37] S. Rudich and A. Wigderson, *Computational Complexity Theory*, IAS/Park City Mathematics Series, American Mathematical Society, (2004).

[38] J. W. Sander, On the addition of units and nonunits mod $m$, *J. Number Theory* **129** (2009), 2260–2266.

[39] J. W. Sander and T. Sander, Adding generators in cyclic groups, *J. Number Theory* **133** (2013), 705–718.

[40] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, **28** (1949), 656–715.

[41] A. Siegel, On universal classes of extremely random constant-time hash functions, *SIAM J. Comput.* **33** (2004), 505–543.

[42] M. Sipser, A complexity theoretic approach to randomness, *Proceedings of the 15th Annual ACM symposium on Theory of Computing — STOC 1983*, 330–335.

[43] D. R. Stinson, On the connection between universal hashing, combinatorial designs and error-correcting codes, *Electronic colloquium on computational complexity (ECCC)*, 2(52), 1995.

[44] C.-F. Sun and Q.-H. Yang, On the sumset of atoms in cyclic groups, *Int. J. Number Theory* **10** (2014), 1355–1363.

[45] L. Tóth, Some remarks on a paper of V. A. Liskovets, *Integers* **12** (2012), 97–111.

[46] H. Tyagi and A. Vardy, Universal hashing for information-theoretic security, *Proceedings of the IEEE* **103** (2015), 1781–1795.

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