Bibak et al. *EPJ Quantum Technology* (2022) 9:8
https://doi.org/10.1140/epjqt/s40507-022-00127-0

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Authentication of variable length messages in quantum key distribution

Khodakhast Bibak[1*], Bruce M. Kapron[2] and Venkatesh Srinivasan[2]

*Correspondence:
bibakk@miamioh.edu
[1]Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio 45056, USA
Full list of author information is available at the end of the article

Abstract

Authentication plays a critical role in the security of quantum key distribution (QKD) protocols. We propose using Polynomial Hash and its variants for authentication of variable length messages in QKD protocols. Since universal hashing is used not only for authentication in QKD but also in other steps in QKD like error correction and privacy amplification, and also in several other areas of quantum cryptography, Polynomial Hash and its variants as the most efficient universal hash function families can be used in these important steps and areas, as well. We introduce and analyze several efficient variants of Polynomial Hash and, using deep results from number theory, prove that each variant gives an ε-almost-Δ-universal family of hash functions. We also give a general method for transforming any such family to an ε-almost-strongly universal family of hash functions. The latter families can then, among other applications, be used in the Wegman–Carter MAC construction which has been shown to provide a universally composable authentication method in QKD protocols. As Polynomial Hash has found many applications, our constructions and results are potentially of interest in various areas.

Keywords: Quantum key distribution; Polynomial Hash; ε-almost-strongly universal; Polynomial congruence

1 Introduction

Key establishment protocols, in which cryptographic keys are securely exchanged between parties over a public channel, usually use methods from public-key cryptography, like Diffie–Hellman key exchange (DH) and elliptic-curve Diffie–Hellman (ECDH); see [1] for a comprehensive treatment of the key establishment protocols in cryptography. However, the security of such schemes relies on the computational hardness of certain mathematical problems (namely, the discrete logarithm problem, the elliptic-curve discrete logarithm problem, and the integer factorization problem) which can be solved on a sufficiently powerful quantum computer running Shor's algorithm. Quantum key distribution (QKD), which relies on the foundations of quantum mechanics, provides a higher level of security than such schemes. QKD is provably secure even against an adversary with unbounded computational power and is also becoming increasingly feasible to implement. QKD has found many surprising applications, its commercialization has been

successful, and QKD networks are now deployed in some metropolitan areas [2]. There are many excellent surveys on QKD (see, e.g., [3–5]).

Studying the security of QKD has become a topic of great importance (see [6, 7] for two excellent surveys). QKD requires a quantum channel and a classical channel. The classical channel needs to be authenticated to avoid man-in-the-middle (MITM) attacks. For the authentication of the communications on the classical channel, the original message authentication codes (MACs) proposed by Wegman and Carter [8], its variants [9], or other efficient constructions [10] are used. All these MACs use universal hash functions in their constructions. In the Wegman–Carter paradigm [8] the message is first hashed with an ε-almost-strongly universal hash function and then encrypted with a one-time pad. The application of the Wegman–Carter paradigm in QKD was originally proposed by Bennett and Brassard [11, 12] in the BB84 protocol (their well-known QKD scheme developed in 1984) and by Bennett et. al. [13], and since then has been studied extensively (see, e.g., [9, 10, 14–18]). The Wegman–Carter MAC construction is described as follows. The legitimate parties share a secret hash function chosen uniformly at random from an ε-almost-strongly universal (ε-ASU) family of hash functions, and a secret encryption key (a sequence of random one-time pads). A message is authenticated by first hashing it with the shared hash function and then encrypting the resulting hash value with the shared encryption key (shared one-time pad). The resulting encrypted hash value, called an *authentication tag*, is transmitted together with the message (as a pair). Upon receiving this pair, the legitimate party recomputes and validates it. Such a MAC algorithm is *information-theoretically* (*unconditionally*) secure, that is, even an adversary who has unbounded computational power cannot forge the MAC with probability greater than the collision probability of the hash function family [8].

Because, in the authentication of the classical channel, the legitimate parties need to share some initial small secret information in advance as described above, QKD is sometimes called a quantum key *growing* (rather than quantum key distribution) protocol. The Wegman–Carter MAC construction has been shown in [18] to be universally composable (UC) [19–21], and therefore it is sufficient for authentication in QKD systems. One way to make QKD protocols more efficient and applicable is to construct efficient ε-ASU hash function families because these families are the main ingredient in the Wegman–Carter construction (and in many other universal hashing based MACs).

In this paper, following [22–24] we propose using *Polynomial Hash* (PH) and its variants for authentication of *variable length messages* in QKD systems. Since universal hashing is used not only for authentication in QKD but also in other steps in QKD like error correction and privacy amplification [7, 13, 25–30], and also in several other areas of quantum cryptography (that we will briefly mention in the last section), Polynomial Hash and its variants as the most efficient universal hash function families can be used in these important steps and areas, as well. Polynomial Hash is a well-known *ε-almost-Δ-universal* (ε-AΔU) family of hash functions which has found various important applications, for example, Galois/Counter Mode (GCM) [31] (which is used in IPsec, SSH, and TLS) and Poly1305 [32] (which is used in Google Chrome's TLS, and later was added to OpenSSH) use this scheme. See also [33–43] for various other applications of Polynomial Hash. We introduce and analyze several efficient variants of Polynomial Hash and, using deep results from number theory, prove that such variants are also ε-AΔU and so can be used in various applications. Furthermore, we propose a general method by which any ε-AΔU hash

function family can be transformed to an ε-ASU family. Therefore, the Polynomial Hash variants constructed in this paper can all be transformed to ε-ASU families which makes them useful for various applications including authentication of variable length messages in QKD.

The rest of this paper is organized as follows. In Sect. 2, we review some results on equations over fields and rings, in particular some rather underappreciated results of Konyagin [44, 45], using which we obtain upper bounds for the number of solutions of polynomial congruences over the ring of integers modulo n, $\mathbb{Z}_n$. In Sect. 3, we formally define universal hashing and its variants and prove a general result for transforming ε-AΔU families to ε-ASU families. In Sect. 4, we construct and analyze several efficient variants of Polynomial Hash and compare our results with available results.

2 Equations over fields and rings

Throughout the paper, n is a positive integer, p is a prime, $\mathbb{Z}_n$ is the ring of integers modulo n defined as $\mathbb{Z}_n = \{0, \dots, n-1\}$, $\mathbb{F}$ is a field, and $\mathbb{F}_q$ is the finite field with q elements, where q is a prime power. Also, $\mathbb{F}_p$ is the prime field. Note that $\mathbb{F}_p = \mathbb{Z}_p = \{0, \dots, p-1\}$.

Finding (the number of) solutions of univariate and multivariate polynomial equations over fields and rings is a fundamental problem in mathematics, computer science, and related areas with many applications in various domains. In this paper, by a polynomial we mean a univariate polynomial. As a classical example, one can mention the Fundamental Theorem of Algebra which gives the exact number of solutions of polynomial equations over the field of complex numbers.

Theorem 2.1 (Fundamental Theorem of Algebra) *Let $f(x)$ be a non-zero polynomial of degree $d \geq 0$ with complex coefficients. Then the equation*

$$f(x) = 0$$

has, counting multiplicities, exactly d complex solutions. Equivalently, the field of complex numbers is algebraically closed.

There are about a hundred proofs(!) of the Fundamental Theorem of Algebra [46]. See [46] for "one of the most elegant and certainly the shortest" proof.

By a *solution* of the polynomial congruence

$$f(x) \equiv 0 \pmod{n}$$

we mean an integer in $\mathbb{Z}_n$ that satisfies the congruence. So, every polynomial congruence modulo n has at most n solutions. Similarly, every multivariate polynomial congruence in k variables modulo n has at most n^k solutions.

A natural question is whether the Fundamental Theorem of Algebra can be applied to the ring $\mathbb{Z}_n$ (that is, to polynomial congruences modulo n)? The answer is *no*; there is no direct analog of the Fundamental Theorem of Algebra for polynomial congruences. Let us see some examples. The following result, proved by D. N. Lehmer [47], gives an explicit formula for the number of solutions of linear congruences:

Theorem 2.2 (Lehmer's Theorem) *Let $a_1, \ldots, a_k, b \in \mathbb{Z}$. The linear congruence*

$$a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$$

has a solution $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ if and only if $\ell \mid b$, where $\ell = \gcd(a_1, \ldots, a_k, n)$. Furthermore, if this condition is satisfied, then there are ℓn^{k-1} solutions.

Note that the generalization of Lehmer's Theorem to higher degree multivariate polynomial congruences is a challenging problem. In fact, even the quadratic version addressed by Cohen [48] has much more complicated formulas.

By Lehmer's Theorem, the linear congruence $ax \equiv b \pmod{n}$, where a and b are integers, has zero, one, or more solutions (in fact, zero or $\gcd(a, n)$ solutions). As another example, the quadratic congruence $x^2 \equiv 1 \pmod{8}$ has four solutions 1, 3, 5, and 7. These examples show that the Fundamental Theorem of Algebra is not applicable to polynomial congruences. But when the modulus is *prime*, we have the following result due to Lagrange which gives *an upper bound* for the number of solutions (see, e.g., [49]).

Theorem 2.3 (Lagrange's Theorem) *Given a prime p, let*

$$f(x) = a_dx^d + \cdots + a_1x + a_0$$

be a polynomial with integer coefficients such that $a_d \not\equiv 0 \pmod{p}$ (said to be of degree d). Then the polynomial congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most d solutions.

Lagrange's Theorem can be extended from the prime field $\mathbb{Z}_p$ to arbitrary fields (not necessarily finite) as the following (see, e.g., [50]):

Theorem 2.4 *Let $\mathbb{F}$ be a field and $f(x)$ be a non-zero polynomial of degree $d \geq 0$ with coefficients in $\mathbb{F}$. Then the polynomial equation*

$$f(x) = 0$$

has, counting multiplicities, at most d solutions in $\mathbb{F}$. Therefore, it has at most d distinct solutions in $\mathbb{F}$.

It would be useful to compare the above results:

Remark 2.5 The following observations are useful, specially when discussing the Polynomial Hash and its variants:

- Setting $\mathbb{F} = \mathbb{Z}_p$ in Theorem 2.4 we obtain Lagrange's Theorem but not in full generality. In fact, in Theorem 2.4 when $\mathbb{F} = \mathbb{Z}_p$, the coefficients of the polynomial must be in $\mathbb{Z}_p$, but in Lagrange's Theorem the coefficients are arbitrary integers.

- While Theorem 2.4 works on arbitrary fields (including the field of complex numbers), it does not imply the Fundamental Theorem of Algebra. In fact, the Fundamental Theorem of Algebra gives the *exact* number of complex solutions of polynomial equations over the field of complex numbers, but Lagrange's Theorem and Theorem 2.4 just give *upper bounds* for the number of solutions over the prime field and arbitrary fields, respectively.
- The proof of the Fundamental Theorem of Algebra is totally different from the proof of Lagrange's Theorem and Theorem 2.4. In fact, the proof of the Fundamental Theorem of Algebra is usually given as a result in complex analysis and "the shortest" proof [46] still requires two pages, but the proofs of Lagrange's Theorem and Theorem 2.4 are usually given as results in number theory and field theory and can be written in just a few lines (see, e.g., [49, 50]).

Note that Lagrange's Theorem does not hold for composite moduli. For example, the quadratic congruence $x^2 \equiv 1 \pmod 8$ has four solutions 1, 3, 5, and 7. Surprisingly, Vandiver [51] obtained, for 'restricted' solutions, exactly the same upper bound as in Lagrange's Theorem and Theorem 2.4 in the much more general setting of commutative rings with identity (that we call Vandiver's Theorem), but, unfortunately, his result, while is quite interesting, seems to have been forgotten. Let $\mathcal{R}$ be a commutative ring with identity. Two elements $u, v \in \mathcal{R}$ are said to be *absolutely distinct* if $u - v$ is not zero and not a zero divisor.

Theorem 2.6 (Vandiver's Theorem) *Let $\mathcal{R}$ be a commutative ring with identity. Let*

$$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

be a polynomial with coefficients in $\mathcal{R}$ such that $a_d \neq 0$. Then the polynomial equation

$$f(x) = 0$$

has at most d absolutely distinct solutions.

Taking $\mathcal{R} = \mathbb{Z}_n$, Vandiver [51] derived the following version for $\mathbb{Z}_n$. Two integers a and b are said to be *absolutely incongruent* modulo n if $a - b$ is coprime to n.

Theorem 2.7 (Vandiver's Theorem for $\mathbb{Z}_n$) *Given a positive integer n, let*

$$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

be a polynomial with integer coefficients such that $a_d \not\equiv 0 \pmod n$. Then the polynomial congruence

$$f(x) \equiv 0 \pmod n$$

has at most d absolutely incongruent solutions.

Note that setting $n = p$, a prime, in Vandiver's Theorem for $\mathbb{Z}_n$, we re-obtain Lagrange's Theorem since any two distinct elements of $\mathbb{Z}_p$ are absolutely incongruent modulo p.

The rest of this section is devoted to generalizing Lagrange's Theorem to composite moduli (or, equivalently, generalizing Vandiver's Theorem for $\mathbb{Z}_n$ to cover *all* solutions). For generalization to prime power moduli, an upper bound for the number of solutions can be obtained using the following result (see, e.g., [49]).

Theorem 2.8 *Suppose $\alpha > 1$ is an integer and s is a solution of the polynomial congruence*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}.$$

Then we have the following cases:

- *If $f'(s) \not\equiv 0 \pmod{p}$ then s can be lifted in a unique way from $p^{\alpha-1}$ to p^{α}. That is, there is a unique $t \in \mathbb{Z}_{p^\alpha}$ which generates s and which satisfies the polynomial congruence*

$$f(x) \equiv 0 \pmod{p^{\alpha}}.$$

- *If $f'(s) \equiv 0 \pmod{p}$ then*:
  - *If $f(s) \equiv 0 \pmod{p^\alpha}$, s can be lifted from $p^{\alpha-1}$ to p^α in p distinct ways.*
  - *If $f(s) \not\equiv 0 \pmod{p^\alpha}$, s cannot be lifted from $p^{\alpha-1}$ to p^α.*

Given a positive integer n, let

$$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

be a polynomial with integer coefficients such that $a_d \not\equiv 0 \pmod{n}$ (said to be of degree d). Denote by $N_d(a_0, a_1, \ldots, a_d, n)$ the number of solutions of the polynomial congruence

$$f(x) \equiv 0 \pmod{n}.$$

Lemma 2.9 *If $\mathcal{G} := \gcd(a_0, a_1, \ldots, a_d, n) > 1$ then*

$$N_d(a_0, a_1, \ldots, a_d, n) = \mathcal{G} N_d(a_0/\mathcal{G}, a_1/\mathcal{G}, \ldots, a_d/\mathcal{G}, n/\mathcal{G}).$$

Proof The proof easily follows from the basic properties of congruences. □

Therefore, by Lemma 2.9, it suffices to consider the number of solutions of the above polynomial congruence with $\gcd(a_0, a_1, \ldots, a_d, n) = 1$. For simplicity, we denote the number of such solutions by $N(d, n)$.

Using Lagrange's Theorem and Theorem 2.8, we can obtain the following upper bound for $N(d, p^\alpha)$.

Theorem 2.10 *Let $\alpha \geq 1$ be an integer. Then*

$$N(d, p^\alpha) \leq d p^{\alpha-1}.$$

Proof Clearly, if $N(d,p) = 0$ then $N(d,p^\alpha) = 0$, for all integers $\alpha \geq 1$. So, let $N(d,p) > 0$. Then, using Theorem 2.8, corresponding to each solution of the polynomial congruence modulo p there will be 0, 1, or p solutions modulo p^2. So, using Lagrange's Theorem and Theorem 2.8, $N(d,p^2) \leq dp$. Similarly, corresponding to each solution of the polynomial congruence modulo p^2 there will be 0, 1, or p solutions modulo p^3. Therefore, $N(d,p^3) \leq dp^2$. Repeating this process, the result follows. □

Is there a better upper bound for $N(d,p^\alpha)$? Yes(!), and the best upper bound for $N(d,p^\alpha)$ is widely attributed to Stewart [52], and to Schmidt and Stewart [53]. But we have discovered that Konyagin [44, 45] (in Russian and back in 1979) has already obtained a stronger and more general upper bound for $N(d,p^\alpha)$ (that we call Konyagin's Theorem). We remark that all these bounds were obtained using advanced tools in number theory and their proofs are rather long and complicated.

Theorem 2.11 (Konyagin's Theorem) *Let $\alpha \geq 1$ be an integer. Then*

$$N\left(d,p^\alpha\right) \leq \frac{d}{\alpha(p-1)}p^\alpha.$$

Furthermore, if $d \geq 2$ and $p \geq d^{1+1/(d-1)}$, then

$$N\left(d,p^\alpha\right) \leq p^{\alpha(1-1/d)}.$$

So far, we have very good upper bounds for the number of solutions of polynomial congruences modulo prime powers. Now, we generalize these upper bounds to arbitrary moduli. For this we need the following tool (see, e.g., [49]).

Theorem 2.12 *Let $f(x)$ be a polynomial with integer coefficients. Also, let $n_1,\ldots,n_r$ be positive integers, pairwise coprime, and let $n = n_1 \cdots n_r$. Then the polynomial congruence*

$$f(x) \equiv 0 \pmod{n} \tag{1}$$

has a solution if and only if each of the polynomial congruences

$$f(x) \equiv 0 \pmod{n_i} \quad (i = 1,\ldots,r) \tag{2}$$

has a solution. Moreover, if $\nu(n)$ and $\nu(n_i)$ denote the number of solutions of (1) and (2), respectively, then

$$\nu(n) = \nu(n_1)\cdots\nu(n_r).$$

When modulus n is square-free, we obtain the best upper bound for $N(d,n)$ using Lagrange's Theorem and Theorem 2.12 as follows.

Theorem 2.13 *Let n be square-free with r distinct prime factors. Then*

$$N(d,n) \leq d^r.$$

Proof Let n has the prime factorization $n = p_1 \dots p_r$, where p_i's are distinct primes. By Lagrange's Theorem, $N(d, p_i) \leq d$ for all i. Since p_i's are pairwise coprime, using Theorem 2.12 we have

$$N(d,n) = \prod_{i=1}^{r} N(d,p_i) \leq d^r.$$

□

Similarly, when modulus n is an arbitrary positive integer, we obtain the best upper bound for $N(d,n)$ using Konyagin's Theorem and Theorem 2.12 as follows.

Theorem 2.14 *Let $n > 1$ has the prime factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, where p_i's are prime and $\alpha_i \geq 1$ for all i. Then*

$$N(d,n) \leq \frac{nd^r}{\prod_{i=1}^{r} \alpha_i(p_i - 1)}.$$

Furthermore, if $d \geq 2$ and $p_i \geq d^{1+1/(d-1)}$ for all i, then

$$N(d,n) \leq \frac{n}{\prod_{i=1}^{r} p_i^{\alpha_i/d}}.$$

Proof By Konyagin's Theorem, we have

$$N\left(d, p_i^{\alpha_i}\right) \leq \frac{d}{\alpha_i(p_i - 1)} p_i^{\alpha_i},$$

for all i. Since $p_i^{\alpha_i}$'s are pairwise coprime, using Theorem 2.12 we have

$$N(d,n) = \prod_{i=1}^{r} N\left(d, p_i^{\alpha_i}\right) \leq \prod_{i=1}^{r} \frac{d}{\alpha_i(p_i - 1)} p_i^{\alpha_i} = \frac{nd^r}{\prod_{i=1}^{r} \alpha_i(p_i - 1)}.$$

Similarly, if $d \geq 2$ and $p_i \geq d^{1+1/(d-1)}$ for all i, then by Konyagin's Theorem and Theorem 2.12, we have

$$N(d,n) = \prod_{i=1}^{r} N\left(d, p_i^{\alpha_i}\right) \leq \prod_{i=1}^{r} p_i^{\alpha_i(1-1/d)} = \frac{n}{\prod_{i=1}^{r} p_i^{\alpha_i/d}}.$$

□

3 Universal hashing and its variants

Universal hash function families, introduced by Carter and Wegman [54], guarantee a low number of collisions in expectation when a hash function is chosen uniformly at random from the universal hash function family. These hash function families have many important applications in computer science and cryptography (see [55] for a comprehensive list of references). We begin by describing universal hashing and its variants in detail [54, 56–60]. For a set $\mathcal{X}$, we write $x \leftarrow \mathcal{X}$ to denote that x is chosen uniformly at random from $\mathcal{X}$.

Definition 3.1 Let H be a family of functions from a finite domain D to a finite range R, and let ε be a constant such that $\frac{1}{|R|} \leq \varepsilon < 1$.

- The family H is a *universal* family of hash function if the probability, over a random choice of a hash function from H, that two distinct elements of D *collide* (i.e., have the same hash value) is at most $1/|R|$ (that is, distinct elements of D do not collide too often). Formally, H is universal 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 ε-*almost universal* (ε-AU) family of hash functions if for any two distinct $x, y \in D$, we have $\Pr_{h \leftarrow H}[h(x) = h(y)] \leq \varepsilon$. Note that an ε-AU family, for a sufficiently small ε, is *close* to being universal.
- Suppose R is a finite additive Abelian group. The family H is a Δ-*universal* family of hash functions if, given a randomly chosen hash function from H, the difference of the hash values of any two distinct elements of D is uniformly distributed in R. Formally, H is Δ-universal 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 ε-*almost*-Δ-*universal* (ε-AΔU) family of hash functions if for any two distinct $x, y \in D$, and all $b \in R$, we have $\Pr_{h \leftarrow H}[h(x) - h(y) = b] \leq \varepsilon$. When $R = \mathbb{Z}_2^k = \{0,1\}^k$ for some k, the operation '$-$' can be replaced by '$\oplus$' (XOR), and H is also called ε-*almost XOR universal* (ε-AXU) or ε-*otp-secure*.
- The family H is a *strongly universal* (or 2-*wise-independent*) family of hash functions if, given a randomly chosen hash function from H, the hash values of any two distinct elements of D are independent and uniformly distributed in R. Formally, H is strongly universal 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 ε-*almost-strongly universal* (ε-ASU) family of hash functions if for any two distinct $x, y \in D$, and all $a, b \in R$, we have
  - $\Pr_{h \leftarrow H}[h(x) = a] = \frac{1}{|R|}$ (that is, given a randomly chosen h from H, $h(x)$ is uniformly distributed in R), and
  - $\Pr_{h \leftarrow H}[h(x) = a | h(y) = b] \leq \varepsilon$ (that is, given a randomly chosen h from H, $h(x)$ is *hard to guess* even if $h(y)$ is known).

  Equivalently, H is ε-ASU if for any two distinct $x, y \in D$, and all $a, b \in R$, we have
  - $\Pr_{h \leftarrow H}[h(x) = a] = \frac{1}{|R|}$, and
  - $\Pr_{h \leftarrow H}[h(x) = a, h(y) = b] \leq \frac{\varepsilon}{|R|}$.

Because many universal hash functions only work on fixed length messages, it is often necessary to extend the domain of the hash function to work on longer messages. Wegman and Carter [8] introduced a construction which recursively hashes messages to a desired length. Let H be an ε-AU family of hash functions, which maps blocks of length $2l$ to blocks of length l. At each round of tree hash, the message is split into blocks of length $2l$ and each block is hashed with some $h \in H$. The length of the message is halved each round, so the runtime is logarithmic in the size of message, and after n rounds of tree hash, the collision probability is $1 - (1 - \varepsilon)^n$ [61]. However, due to the recursive nature of tree hash, it is not suitable for devices with limited memory. Instead, an iterative method can be constructed by composing hash functions.

Theorem 3.2 ([59]) *For $i = 1, 2$, let $H_i : A_i \to B_i$ be almost-universal families of hash functions where $B_1 = A_2$, and define $H = \{h(m) = h_2(h_1(m)) | h_1 \in H_1, h_2 \in H_2\}$. Then H has the following property*:

- *If H_1 is ε_1-AU and H_2 is ε_2-AU, then H is $(\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2)$-AU.*
- *If H_1 is ε_1-AU and H_2 is ε_2-AΔU, then H is $(\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2)$-A$\Delta$U.*

- *If* H_1 *is* ε_1-AU *and* H_2 *is* ε_2-ASU, *then* H *is* $(\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2)$-ASU.

The last two parts of this result can be used to pair an efficient ε-AU hash family with an ε-AΔU or ε-ASU hash family to create an efficient ε-AΔU or ε-ASU family. We can also use this result to create a Merkle–Damgård like paradigm for universal hash functions. Let $H : A \times B \to B$ be ε-AU and let $b \in B$. Then the family $H^l = \{h_l(m_l, h_{l-1}(\dots h_2(m_2, h_1(m_1, b))\dots)|h_1, \dots, h_l \in H\}$ can hash messages of length l for any positive l, and is $l(2\varepsilon - \varepsilon^2)$-AU. This construction was used by Minematsu and Tsunoo [62], and a more general proof on its collision bound was given by Duval and Leurent [63].

Often the collision probability of a hash function may be larger than desired. For this reason, there are several techniques for reducing the collision probability of a hash function family. If H is an ε-AU family of hash functions, then by hashing a message with two independent keys and concatenating the results, the probability of collision is lowered to ε^2, at the expense of doubling the computational work, the length of the hash value, and the size of the key. The well-known Toeplitz extension, which has been used in several MAC algorithms (c.f. [56, 64]), reduces the key size needed for this technique. Rather than generating independent keys $\mathbf{x} = \langle x_1, x_2, \dots, x_k\rangle$, $\mathbf{x}' = \langle x'_1, x'_2, \dots, x'_k\rangle$, we generate the values $x_1, \dots, x_{k+1}$ and use the keys $\mathbf{x_1} = \langle x_1, x_2, \dots, x_k\rangle$ and $\mathbf{x_2} = \langle x_2, x_3, \dots, x_{k+1}\rangle$. We can easily extend this procedure to concatenate n hash values to get a collision probability of ε^n. While the computation and hash length still increase by a factor of n, the size of the key only increases by n values. Not only does this save key material, it reduces memory accesses, thus potentially improving performance.

Now, we prove a general result for transforming ε-AΔU families to ε-ASU families. Because for authentication in QKD systems we need efficient ε-ASU families, our result implies that constructing such families boils down to constructing efficient ε-AΔU families. Our result is a generalization of the following result by Etzel *et al.* [65] which seems to have remained underappreciated.

Theorem 3.3 *Let the family*

$$H = \{h_k : D \to R | k \in K\}$$

be a Δ*-universal family of hash functions, where* K *is the key space and* R *is a finite additive Abelian group. Then the family*

$$H' = \left\{h'_{k,w} : D \to R | k \in K, w \in R\right\},$$

where

$$h'_{k,w}(x) = h_k(x) + w,$$

and '+' denotes the group addition operation, is strongly universal.

In order to generalize the above result, we also need the following result (see [66]):

Theorem 3.4 *Let* G *be an Abelian group, and let* $\xi_1, \xi_2, \dots, \xi_t$ *be independent random variables which take on values in* G*. If one of* ξ_i *is uniformly distributed in* G*, then the sum* $\xi_1 + \xi_2 + \cdots + \xi_t$ *is also uniformly distributed in* G*.*

More generally, Sherstnev [66] gave necessary and sufficient conditions on the distributions of independent random variables $\xi_1, \xi_2, \ldots, \xi_t$, taking on values in an Abelian group G, under which the sum $\xi_1 + \xi_2 + \cdots + \xi_t$ is uniformly distributed in G.

Now, we are ready to prove our result.

Theorem 3.5 *Let the family*

$$H = \{h_k : D \to R | k \in K\}$$

be an ε-almost-Δ-universal family of hash functions, where K is the key space and R is a finite additive Abelian group. Then the family

$$H' = \left\{h'_{k,w} : D \to R | k \in K, w \in R\right\},$$

where

$$h'_{k,w}(x) = h_k(x) + w,$$

and '+' denotes the group addition operation, is ε-almost-strongly universal.

Proof For any two distinct $x, y \in D$, and all $a, b \in R$, we have

$$\begin{aligned}
&\Pr_{h'_{k,w} \leftarrow H'}\left[h'_{k,w}(x) = a, h'_{k,w}(y) = b\right] \\
&\quad = \Pr_{h'_{k,w} \leftarrow H'}\left[h_k(x) + w = a, h_k(y) + w = b\right] \\
&\quad = \Pr_{h'_{k,w} \leftarrow H'}\left[h_k(x) - h_k(y) = a - b, w = a - h_k(x)\right] \\
&\quad = \Pr_{h'_{k,w} \leftarrow H'}\left[h_k(x) - h_k(y) = a - b\right] \cdot \Pr_{h'_{k,w} \leftarrow H'}\left[a = w + h_k(x)\right].
\end{aligned}$$

Since H is ε-almost-Δ-universal, we have

$$\Pr_{h'_{k,w} \leftarrow H'}\left[h_k(x) - h_k(y) = a - b\right] \leq \varepsilon.$$

Also, by Theorem 3.4 we have

$$\Pr_{h'_{k,w} \leftarrow H'}\left[a = w + h_k(x)\right] = \frac{1}{|R|}.$$

Consequently,

$$\Pr_{h'_{k,w} \leftarrow H'}\left[h'_{k,w}(x) = a, h'_{k,w}(y) = b\right] \leq \frac{\varepsilon}{|R|}.$$

Hence, the result follows. □

4 Polynomial Hash and its variants

An ε-AΔU family of hash functions which has received much attention is *Polynomial Hash* (PH), which is used for hashing variable length messages. The idea is that we put

the message blocks as the coefficients of a polynomial and then evaluate the polynomial at the secret key, where all operations are done in a specific field or ring. In this section, we introduce and analyze several efficient variants of Polynomial Hash and then compare our results with available results. As Polynomial Hash has found many applications, our constructions and results might be of interest in various areas.

4.1 Five variants

Here we introduce five variants of Polynomial Hash (other variants are also possible depending on applications) and analyze their universality using results from Sect. 2.

Polynomial Hash Over Ring of Integers Modulo n (PH-IM): In this family, message blocks m_i are all in $\mathbb{Z}_{p_1}$, where p_1 is the smallest prime divisor of n, the key x is in $\mathbb{Z}_n$, and all operations are performed in $\mathbb{Z}_n$. Formally,

Definition 4.1 (PH-IM) Given an integer $n > 1$ with the smallest prime divisor p_1, we define

$$\text{PH-IM} := \left\{h_x : \mathbb{Z}_{p_1}^{d+1} \to \mathbb{Z}_n | x \in \mathbb{Z}_n\right\},$$

where

$$h_x(\mathbf{m}) := \sum_{i=0}^{d} m_i x^i \pmod n,$$

for every message $\mathbf{m} = \langle m_0, m_1, \ldots, m_d\rangle \in \mathbb{Z}_{p_1}^{d+1}$ and every key $x \in \mathbb{Z}_n$.

Theorem 4.2 *Let $n > 1$ has the prime factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, where p_i's are prime and $\alpha_i \geq 1$ for all i. Then we have the following cases*:

- *The family* PH-IM *is* $\frac{d^r}{\prod_{i=1}^{r} \alpha_i(p_i-1)}$*-almost-*$\Delta$*-universal.*
- *If n is square-free, then the family* PH-IM *is* $\frac{d^r}{n}$*-almost-*Δ*-universal.*
- *If $d \geq 2$ and $p_i \geq d^{1+1/(d-1)}$ for all i, then the family* PH-IM *is* $\frac{1}{\prod_{i=1}^{r} p_i^{\alpha_i/d}}$*-almost-*$\Delta$*-universal.*

Proof We only prove the last part; the proofs for other parts are similar. Let $\mathbf{m} = \langle m_0, m_1, \ldots, m_d\rangle \in \mathbb{Z}_{p_1}^{d+1}$ and $\mathbf{m}' = \langle m_0', m_1', \ldots, m_d'\rangle \in \mathbb{Z}_{p_1}^{d+1}$ be any two distinct messages. Put $\mathbf{a} = \langle a_0, a_1, \ldots, a_d\rangle = \mathbf{m} - \mathbf{m}'$. For every $b \in \mathbb{Z}_n$ we have

$$h_x(\mathbf{m}) - h_x(\mathbf{m}') = b \quad \Longleftrightarrow \quad \sum_{i=0}^{d} a_i x^i \equiv b \pmod n.$$

Since $\mathbf{m} \neq \mathbf{m}'$, there exists some i_0 such that $a_{i_0} \neq 0$. Now, we need to find the maximum number of solutions of the above polynomial congruence over all choices of $\mathbf{a} = \langle a_0, a_1, \ldots, a_d\rangle \in \mathbb{Z}_{p_1}^{d+1} \setminus \{\mathbf{0}\}$ and $b \in \mathbb{Z}_n$. Note that since a_i's are in $\mathbb{Z}_{p_1}$ and at least one of them is not zero, we have $\gcd(a_0, a_1, \ldots, a_d, n) = 1$. Now, by Theorem 2.14, if $d \geq 2$ and $p_i \geq d^{1+1/(d-1)}$ for all i, then the polynomial congruence

$$\sum_{i=0}^{d} a_i x^i \equiv b \pmod n,$$

has at most

$$\frac{n}{\prod_{i=1}^{r} p_i^{\alpha_i/d}}$$

solutions. Consequently, for part (iii) we have

$$\Pr_{h_x \leftarrow \text{PH-IM}}\left[h_x(\mathbf{m}) - h_x(\mathbf{m}') = b\right] \leq \frac{n}{n\prod_{i=1}^{r} p_i^{\alpha_i/d}} = \frac{1}{\prod_{i=1}^{r} p_i^{\alpha_i/d}}. \qquad \square$$

Polynomial Hash With Probability At Least 1/2 *Zero Collision (PH-ZC)*: Let p be an odd prime and k be a positive even integer not divisible by p. Denote the set of even elements of $\mathbb{Z}_p$ by E and the set of odd elements of $\mathbb{Z}_p$ by O. In this family, message blocks m_i are all in E or are all in O, the key x is in $\mathbb{Z}_{kp}$, and all operations are performed in $\mathbb{Z}_{kp}$. We define the family over E; the definition and the result over O are similar. Formally,

Definition 4.3 (PH-ZC) Given an odd prime p and a positive even integer k not divisible by p, we define

$$\text{PH-ZC} := \left\{h_x : E^{d+1} \to \mathbb{Z}_{kp} | x \in \mathbb{Z}_{kp}\right\},$$

where

$$h_x(\mathbf{m}) := \sum_{i=0}^{d} m_i x^i \pmod{kp},$$

for every message $\mathbf{m} = \langle m_0, m_1, \ldots, m_d\rangle \in E^{d+1}$ and every key $x \in \mathbb{Z}_{kp}$.

Theorem 4.4 *The family* PH-ZC *is* $\frac{d}{p}$*-almost-*Δ*-universal. Furthermore, with probability at least* 1/2 *the collision probability is exactly zero.*

Proof Let $\mathbf{m} = \langle m_0, m_1, \ldots, m_d\rangle \in E^{d+1}$ and $\mathbf{m}' = \langle m_0', m_1', \ldots, m_d'\rangle \in E^{d+1}$ be any two distinct messages. Put $\mathbf{a} = \langle a_0, a_1, \ldots, a_d\rangle = \mathbf{m} - \mathbf{m}'$. For every $b \in \mathbb{Z}_{kp}$ we have

$$h_x(\mathbf{m}) - h_x(\mathbf{m}') = b \quad \Longleftrightarrow \quad \sum_{i=0}^{d} a_i x^i \equiv b \pmod{kp}.$$

Since $\mathbf{m} \neq \mathbf{m}'$, there exists some i_0 such that $a_{i_0} \neq 0$. Now, we need to find the maximum number of solutions of the above polynomial congruence over all choices of $\mathbf{a} = \langle a_0, a_1, \ldots, a_d\rangle \in E^{d+1} \setminus \{\mathbf{0}\}$ and $b \in \mathbb{Z}_{kp}$. Since m_i's are all even, a_i's are also all even. For every $b \in \mathbb{Z}_{kp}$, if b is odd then the polynomial congruence

$$\sum_{i=0}^{d} a_i x^i \equiv b \pmod{k},$$

has no solution, but if b is even then it has at most k solutions. On the other hand, by Lagrange's Theorem, for every $b \in \mathbb{Z}_{kp}$ the polynomial congruence

$$\sum_{i=0}^{d} a_i x^i \equiv b \pmod{p},$$

has at most d solutions. Now, using Theorem 2.12 the polynomial congruence

$$\sum_{i=0}^{d} a_i x^i \equiv b \pmod{kp},$$

has no solution if b is odd, and has at most kd solutions if b is even.

Consequently, we have

$$\Pr_{h_x \leftarrow \text{PH-ZC}}\left[h_x(\mathbf{m}) - h_x(\mathbf{m}') = b\right] \leq \frac{kd}{kp} = \frac{d}{p}.$$

Note that although $\frac{d}{p}$ is an upper bound for the collision probability, but when b is odd and possibly in other cases (so with probability at least 1/2) the collision probability is exactly zero. Hence, the result follows. □

Polynomial Hash Over Prime Fields (PH-PF): In this family, each message block m_i and the key x are in $\mathbb{Z}_p$, and all operations are performed in $\mathbb{Z}_p$. Formally,

Definition 4.5 (PH-PF) Given a prime p,

$$\text{PH-PF} := \left\{h_x : \mathbb{Z}_p^{d+1} \to \mathbb{Z}_p | x \in \mathbb{Z}_p\right\},$$

where

$$h_x(\mathbf{m}) := \sum_{i=0}^{d} m_i x^i \pmod{p},$$

for every message $\mathbf{m} = \langle m_0, m_1, \ldots, m_d \rangle \in \mathbb{Z}_p^{d+1}$ and every key $x \in \mathbb{Z}_p$.

Theorem 4.6 *The family* PH-PF *is* $\frac{d}{p}$*-almost-*Δ*-universal.*

Proof Same as above, just use Lagrange's Theorem or Theorem 2.4. □

Remark 4.7 It is important to note that we do not have to restrict the message blocks to be in $\mathbb{Z}_p$ or $\mathbb{Z}_n$. In fact, the message blocks can be *arbitrary* non-negative integers as long as no two messages have all their corresponding blocks congruent modulo p or modulo n. See Theorem 4.9 for an example of such constructions in the case of $\mathbb{Z}_p$ but the same technique is also applicable to $\mathbb{Z}_n$.

Polynomial Hash Over Prime Fields With Arbitrary Message Blocks (PH-PA): Let A be a subset of $\mathbb{Z}_{\geq 0}^{d+1}$ such that no two elements of A have all their corresponding coordinates congruent modulo p. In this family, each message $\mathbf{m}$ is in A, the key x is in $\mathbb{Z}_p$, and all operations are performed in $\mathbb{Z}_p$. Formally,

Definition 4.8 (PH-PA) Given a prime p,

$$\text{PH-PA} := \{h_x : A \to \mathbb{Z}_p | x \in \mathbb{Z}_p\},$$

where

$$h_x(\mathbf{m}) := \sum_{i=0}^{d} m_i x^i \pmod{p},$$

for every message $\mathbf{m} = \langle m_0, m_1, \ldots, m_d \rangle \in A$ and every key $x \in \mathbb{Z}_p$.

Theorem 4.9 *The family* PH-PA *is* $\frac{d}{p}$*-almost-*Δ*-universal.*

Proof Same as above, just use Lagrange's Theorem. Note that when we find the difference of the two polynomials, at least one of the coefficients is non-zero modulo p (by the definition of the set A) so the assumption of Lagrange's Theorem is satisfied. Also, note that Theorem 2.4 is not applicable here because message blocks are not necessarily in $\mathbb{Z}_p$. □

Polynomial Hash Over Finite Fields (PH-FF): In this family, each message block m_i and the key x are in $\mathbb{F}_q$, and all operations are performed in $\mathbb{F}_q$. Formally,

Definition 4.10 (PH-FF) Given the finite field $\mathbb{F}_q$ with q elements, where q is a prime power,

$$\text{PH-FF} := \left\{ h_x : \mathbb{F}_q^{d+1} \to \mathbb{F}_q | x \in \mathbb{F}_q \right\},$$

where

$$h_x(\mathbf{m}) := \sum_{i=0}^{d} m_i x^i,$$

for every message $\mathbf{m} = \langle m_0, m_1, \ldots, m_d \rangle \in \mathbb{F}_q^{d+1}$ and every key $x \in \mathbb{F}_q$.

Theorem 4.11 *The family* PH-FF *is* $\frac{d}{q}$*-almost-*Δ*-universal.*

Proof Same as above, just use Theorem 2.4. □

Corollary 4.12 *Using Theorem 3.5, any* ε*-*AΔ*U family, in particular the families studied in this paper, can be transformed to* ε*-*ASU *families which makes them useful for various applications including authentication of variable length messages in QKD. This can be done by adding a uniform value* $w \leftarrow R$ *to the hash functions, where* R *is the range of the corresponding hash functions.*

4.2 Comparison and remarks

The above techniques and results on the Polynomial Hash and its variants and comparing them with what were known before, reveals some remarks:

- Polynomial Hash is widely attributed to Wegman and Carter [8], Dietzfelbinger et. al. [67], den Boer [68], Bierbrauer et. al. [69], and Taylor [70]. But we have discovered that it has been already introduced by Mehlhorn and Vishkin [71] back in 1984 (of course, Wegman and Carter [8] already studied the degree one case).

- So far, only the families PH-PF and PH-FF have been introduced in the literature but, unfortunately, there is a growing number of papers that explicitly or implicitly have used the Fundamental Theorem of Algebra to prove the ε-almost-Δ-universality of these families. As discussed in detail in Remark 2.5, the Fundamental Theorem of Algebra works only over the field of complex numbers not over the prime field or finite fields, so is not applicable to the families PH-PF and PH-FF. Instead, those papers should have used Lagrange's Theorem or Theorem 2.4 as we did.
- Polynomial Hash has been already used to provide a very efficient universal hash function family, for authentication in QKD [22–24] but it has not been explained why that is the case. In fact, the efficiency of Polynomial Hash comes from at least the following observations:
  - The evaluation of a polynomial $f(x)$ of degree d,

    $$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

    needs only d multiplications and d additions since, by Horner's rule, $f(x)$ can be written as

    $$f(x) = a_0 + x\big(a_1 + x\big(a_2 + x\big(a_3 + \cdots + x(a_{d-1} + xa_d)\cdots\big)\big)\big).$$

    Therefore, hashing a message of length $d+1$ using Polynomial Hash needs only d multiplications and d additions, while hashing the same message using most other universal hash function families needs more computations, for example, hashing it using MMH* [56, 72, 73] (which is one of the most well-known universal hash function families) needs $d+1$ multiplications and $d+1$ additions.
  - Unlike most other universal hash function families (e.g., MMH* and its variants) which hash fixed length messages (that is, once the key is chosen we can only hash message of the same length as the key) Polynomial Hash can be used for hashing variable length messages because each message block becomes the coefficient of the polynomial, and so is independent of the key.
- Even though the collision bounds of the hash families introduced in this paper are quite strong, even if for some application we pick a family with a slightly weaker collision bound thanks to the *everlasting security* of QKD [5, 6, 74] if authentication remains unbroken during the execution of the QKD protocol, then the resulting key is information-theoretically secure; breaking authentication after the protocol has output the key will not change the security of the generated key.
- As universal hashing is used not only for authentication in QKD but also in other steps in QKD like error correction and privacy amplification [7, 13, 25–30], our constructions and results might lead to improvements in QKD protocols, among other areas.
- Universal hash functions have been recently used in studying quantum secure direct communication (QSDC) [75] (see also, [76–80]), quantum secret sharing (QSS) (either directly [81, 82] or via a security proof based on QKD [83]), quantum conference key agreement (QCKA) [84–86], and quantum authentication [87–89]. Therefore, our efficient and secure constructions and results might lead to improvements in these directions as well.

- Our study of Polynomial Hash over $\mathbb{Z}_n$ and its variants also demonstrate various benefits which do not hold in the case of the two well-known variants of Polynomial Hash. In particular,
  - We do not have to restrict the message blocks to be in $\mathbb{Z}_p$ or $\mathbb{Z}_n$. In fact, the message blocks can be *arbitrary* non-negative integers (unlike the two well-known versions). See Remark 4.7 and Theorem 4.9 for the details.
  - In some of these variants with probability at least $1/2$ the collision probability is exactly zero (see Theorem 4.4).
  - We do not need large prime numbers or finite field arithmetic anymore (that is, all arithmetic is done in $\mathbb{Z}_n$).
  - It is also possible to introduce, generalize, and analyze other variants of Polynomial Hash (for specific applications) using results from Sect. 2.
  - Although in QKD the legitimate parties need to share some initial small secret information in advance for the authentication of the classical channel, each round of QKD provides substantially larger fresh key materials, part of which can be used for authentication in the next round of QKD. Furthermore, keys generated in each round of QKD are completely independent of all prior keys and messages [5, 6, 74]. Therefore, even if any of our schemes uses more key materials at the expense of other benefits, the protocol compensates it in the next round.
  - We connected Polynomial Hash and QKD with deep results in number theory. This may motivate more work in these areas.

Acknowledgements
The authors would like to thank the editor and the referees for carefully reading the paper, and for their useful comments which helped improve the paper.

Funding
BK was supported in part by NSERC RGPIN-2021-02481, and VS was supported in part by NSERC Discovery Grant RGPIN-2017-04039.

Availability of data and materials
No data is needed for this work.

Declarations

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
All authors read and approved the final manuscript.

Author details
[1]Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio 45056, USA. [2]Department of Computer Science, University of Victoria, Victoria, BC V8W 3P6, Canada.

Publisher's Note

Received: 29 July 2021 Accepted: 6 February 2022 Published online: 16 February 2022

References

1. Boyd C, Mathuria A, Stebila D. Protocols for authentication and key establishment. 2nd ed. Berlin: Springer; 2020.
2. Sasaki M. Quantum key distribution and its applications. IEEE Secur Priv. 2018;16(5):42–8.
3. Bruss D, Erdélyi G, Meyer T, Riege T, Rothe J. Quantum cryptography: a survey. ACM Comput Surv. 2007;39(2):6.
4. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74:145–95.

5. Stebila D, Mosca M, Lütkenhaus N. The case for quantum key distribution. In: Sergienko AV, Pascazio S, Villoresi P, editors. Quantum communication and quantum networking, first international conference, QuantumComm 2009, revised selected papers. Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering. vol. 36. Naples, Italy. October 26–30, 2009. Berlin: Springer; 2009. p. 283–96.
6. Alléaume R, Branciard C, Bouda J, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier P, Länger T, Lütkenhaus N, Monyk C, Painchault P, Peev M, Poppe A, Pornin T, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H, Zeilinger A. Using quantum key distribution for cryptographic purposes: a survey. Theor Comput Sci. 2014;560:62–81.
7. Tomamichel M, Leverrier A. A largely self-contained and complete security proof for quantum key distribution. Quantum. 2017;1:14.
8. Wegman MN, Carter JL. New hash functions and their use in authentication and set equality. J Comput Syst Sci. 1981;22:265–79.
9. Bibak K, Ritchie R, Zolfaghari B. Everlasting security of quantum key distribution with 1K-DWCDM and quadratic hash. Quantum Inf Comput. 2021;21(3&4):181–202.
10. Bibak K, Ritchie R. Quantum key distribution with PRF(Hash, Nonce) achieves everlasting security. Quantum Inf Process. 2021;20:228.
11. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems and signal processing. 1984. p. 175–9.
12. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.
13. Bennett CH, Bessette F, Brassard G, Salvail L, Smolin JA. Experimental quantum cryptography. J Cryptol. 1992;5(1):3–28.
14. Cederlof J, Larsson J. Security aspects of the authentication used in quantum cryptography. IEEE Trans Inf Theory. 2008;54(4):1735–41.
15. Fung C-HF, Ma X, Chau HF. Practical issues in quantum-key-distribution postprocessing. Phys Rev A. 2010;81:012318.
16. Li Q, Zhao Q, Le D, Niu X. Study on the security of the authentication scheme with key recycling in QKD. Quantum Inf Process. 2016;15(9):3815–31.
17. Peev M, Nölle M, Maurhardt O, Lorünser T, Suda M, Poppe A, Ursin R, Fedrizzi A, Zeilinger A. A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography. Int J Quantum Inf. 2005;03(01):225–31.
18. Portmann C. Key recycling in authentication. IEEE Trans Inf Theory. 2014;60(7):4383–96.
19. Canetti R. Universally composable security: a new paradigm for cryptographic protocols. In: 42nd annual symposium on foundations of computer science, FOCS 2001. 14–17 October 2001. Las Vegas, Nevada, USA. 2001. p. 136–45.
20. Canetti R, Dodis Y, Pass R, Walfish S. Universally composable security with global setup. In: Vadhan SP, editor. Proceedings, theory of cryptography, 4th theory of cryptography conference, TCC 2007. Lecture notes in computer science. vol. 4392. Amsterdam, The Netherlands, February 21–24, 2007. 2007. p. 61–85.
21. Maurer U, Renner R. Abstract cryptography. In: Chazelle B, editor. Innovations in computer science – ICS 2011. Proceedings. Tsinghua University, Beijing, China: January 7–9, 2011; 2011. p. 1–21.
22. Kiktenko EO, Malyshev AO, Gavreev MA, Bozhedarov AA, Pozhar NO, Anufriev MN, Fedorov AK. Lightweight authentication for quantum key distribution. IEEE Transactions on Information Theory. 2020.
23. Pacher C, Abidin A, Lorünser T, Peev M, Ursin R, Zeilinger A, Larsson J. Attacks on quantum key distribution protocols that employ non-its authentication. Quantum Inf Process. 2016;15(1):327–62.
24. Walenta N, Burg A, Caselunghe D, Constantin J, Gisin N, Guinnard O, Houlmann R, Junod P, Korzh B, Kulesza N, Legré M, Lim CW, Lunghi T, Monat L, Portmann C, Soucarros M, Thew RT, Trinkler P, Trolliet G, Vannel F, Zbinden H. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New J Phys. 2014;16(1):013047.
25. Renner R, König R. Universally composable privacy amplification against quantum adversaries. In: Kilian J, editor. Theory of cryptography. Lecture notes in computer science. vol. 3378. Second Theory of Cryptography Conference, TCC 2005, Proceedings. Cambridge, MA, USA. February 10–12, 2005. Berlin: Springer; 2005. p. 407–25.
26. König R, Maurer UM, Renner R. On the power of quantum memory. IEEE Trans Inf Theory. 2005;51(7):2391–401.
27. König R, Renner R. Sampling of min-entropy relative to quantum knowledge. IEEE Trans Inf Theory. 2011;57(7):4760–87.
28. Tomamichel M, Schaffner C, Smith AD, Renner R. Leftover hashing against quantum side information. IEEE Trans Inf Theory. 2011;57(8):5524–35.
29. Tsurumaru T. Leftover hashing from quantum error correction: unifying the two approaches to the security proof of quantum key distribution. IEEE Trans Inf Theory. 2020;66(6):3465–84.
30. Schwonnek R, Goh KT, Primaatmaja IW, Tan EY-Z, Wolf R, Scarani V, Lim CC-W. Device-independent quantum key distribution with random key basis. Nat Commun. 2021;12:2880.
31. McGrew DA, Viega J. The security and performance of the Galois Counter mode (GCM) of operation. In: Canteaut A, Viswanathan K, editors. Progress in cryptology – INDOCRYPT 2004. Lecture notes in computer science. 2005. p. 343–55.
32. Bernstein D. The Poly1305-AES message-authentication code. In: Fast software encryption – FSE'05. Lecture notes in computer science. vol. 3557. 2005. p. 32–49.
33. Ben-Sasson E, Fehr S, Ostrovsky R. Near-linear unconditionally-secure multiparty computation with a dishonest minority. In: Safavi-Naini R, Canetti R, editors. Proceedings. Lecture notes in computer science. vol. 7417. Advances in Cryptology – CRYPTO 2012–32nd Annual Cryptology Conference. Santa Barbara, CA, USA. August 19–23, 2012. Berlin: Springer; 2012. p. 663–80.
34. Chakraborty D, Nandi M. An improved security bound for HCTR. In: Nyberg K, editor. Fast software encryption, 15th international workshop, FSE 2008, lausanne. Lecture notes in computer science. vol. 5086. Revised Selected Papers. February 10–13, 2008. Berlin: Springer; 2008. p. 289–302.
35. Ghazi B, Haramaty E, Kamath P, Sudan M. Compression in a distributed setting. In: Papadimitriou CH, editor. 8th innovations in theoretical computer science conference, ITCS 2017. LIPIcs. vol. 67. Berkeley, CA, USA. January 9–11, 2017. 2017. p. 19:1–19:22.

36. Goldreich O. Modern cryptography, probabilistic proofs and pseudorandomness. Algorithms and combinatorics. vol. 17. Berlin: Springer; 1998.
37. Goldreich O. A taste of randomized computations. 2001.
38. Ho T, Leong B, Koetter R, Médard M, Effros M, Karger DR. Byzantine modification detection in multicast networks with random network coding. IEEE Trans Inf Theory. 2008;54(6):2798–803.
39. Krovetz T, Rogaway P. Fast universal hashing with small keys and no preprocessing: the polyr construction. In: Won D, editor. Proceedings, information security and cryptology – ICISC 2000, third international conference. Lecture notes in computer science. vol. 2015. Seoul, Korea. December 8–9, 2000. Berlin: Springer; 2000. p. 73–89.
40. Krovetz TD. Software-optimized universal hashing and message authentication. Ph.D thesis. Davis: University of California; 2000.
41. Lemire D. The universality of iterated hashing over variable-length strings. Discrete Appl Math. 2012;160(4–5):604–17.
42. Lemire D, Kaser O. Faster 64-bit universal hashing using carry-less multiplications. J Cryptogr Eng. 2016;6(3):171–85.
43. Thorup M. High speed hashing for integers and strings. 2020. 1504.06804.
44. Konyagin S. The number of solutions of congruences of the *n*th degree with one unknown. Mat Sb (NS). 1979;109(151)(2):171–87. (In Russian).
45. Konyagin S. Letter to the editors: "The number of solutions of congruences of the *n*th degree with one unknown. Mat Sb (NS). 1979;109(151)(2):171–87. (In Russian), Mat Sb (NS). 1979;**110(152)**(1):158.
46. Aigner M, Ziegler G. Proofs from the book. 6th ed. Berlin: Springer; 2018.
47. Lehmer DN. Certain theorems in the theory of quadratic residues. Am Math Mon. 1913;20:151–7.
48. Cohen E. Rings of arithmetic functions. II: the number of solutions of quadratic congruences. Duke Math J. 1954;21:9–28.
49. Apostol TM. Introduction to analytic number theory. New York: Springer; 1976.
50. Lidl R, Niederreiter H. Finite fields. 2nd ed. Cambridge: Cambridge University Press; 1997.
51. Vandiver HS. On the foundation of a constructive theory of discrete commutative algebra (second paper). Proc Natl Acad Sci. 1935;21(3):162–5.
52. Stewart CL. On the number of solutions of polynomial congruences and Thue equations. J Am Math Soc. 1991;4(4):793–835.
53. Schmidt WM, Stewart CL. Congruences, trees, and *p*-adic integers. Trans Am Math Soc. 1997;349(2):605–39.
54. Carter JL, Wegman MN. Universal classes of hash functions. J Comput Syst Sci. 1979;18:143–54.
55. Bibak K. Restricted congruences in computing. Boca Raton: CRC Press; 2020.
56. Halevi S, Krawczyk H. MMH: software message authentication in the Gbit/second rates. In: Biham E, editor. Fast software encryption – FSE'97. Lecture notes in computer science. vol. 1267. 1997. p. 172–89.
57. Krawczyk H. LFSR-based hashing and authentication. In: Desmedt YG, editor. Advances in cryptology – CRYPTO '94. Lecture notes in computer science. 1994. p. 129–39.
58. Rogaway P. Bucket hashing and its application to fast message authentication. In: Coppersmith D, editor. Advances in cryptology – CRYPTO' 95. Lecture notes in computer science. vol. 12. 1995. p. 29–42.
59. Stinson DR. Universal hashing and authentication codes. Des Codes Cryptogr. 1994;4:369–80.
60. Stinson DR. On the connections between universal hashing, combinatorial designs and error-correcting codes. Congr Numer. 1996;114:7–27.
61. Boesgaard M, Christensen T, Zenner E. Badger – a fast and provably secure MAC. In: Ioannidis J, Keromytis A, Yung M, editors. Applied cryptography and network security. 2005. p. 176–91.
62. Minematsu K, Tsunoo Y. Provably secure MACs from differentially-uniform permutations and AES-based implementations. In: Robshaw M, editor. Fast software encryption – FSE'06. Lecture notes in computer science. 2006. p. 226–41.
63. Duval S, Leurent G. Lightweight MACs from universal hash functions. In: Smart card research and advanced applications. Lecture notes in computer science. vol. 11833. 2020. p. 195–215.
64. Black J, Halevi S, Krawczyk H, Krovetz T, Rogaway P. UMAC: fast and secure message authentication. In: Advances in cryptology – CRYPTO'99. Lecture notes in computer science. vol. 1666. 1999. p. 216–33.
65. Etzel M, Patel S, Ramzan Z. Square hash: fast message authentication via optimized universal hash functions. In: Wiener M, editor. Advances in cryptology – CRYPTO' 99. Lecture notes in computer science. vol. 1666. 1999. p. 234–51.
66. Sherstnev VI. A random variable uniformly distributed on a finite Abelian group as a sum of independent summands. Ross Akad Nauk Teor Veroâtn Ee Primenen. 1998;43(2):397–403.
67. Dietzfelbinger M, Gil J, Matias Y, Pippenger N. Polynomial hash functions are reliable. In: Kuich W, editor. International colloquium on automata, languages and programming – ICALP'92. 1992. p. 235–46.
68. Boer BD. A simple and key-economical unconditional authentication scheme. J Comput Secur. 1993;2:65–72.
69. Bierbrauer J, Johansson T, Kabatianskii G, Smeets B. On families of hash functions via geometric codes and concatenation. In: Advances in cryptology – CRYPTO'93. Lecture notes in computer science. vol. 5665. 1993. p. 331–42.
70. Taylor R. An integrity check value algorithm for stream ciphers. In: Stinson DR, editor. Advances in cryptology – CRYPTO' 93. Lecture notes in computer science. vol. 773. 1994. p. 40–8.
71. Mehlhorn K, Vishkin U. Randomized and deterministic simulations of PRAMs by parallel machines with restricted granularity of parallel memories. Acta Inform. 1984;21:339–74.
72. Bibak K, Kapron BM, Srinivasan V. MMH* with arbitrary modulus is always almost-universal. Inf Process Lett. 2016;116:481–3.
73. Gilbert EN, Macwilliams FJ, Sloane NJA. Codes which detect deception. Bell Syst Tech J. 1974;53:405–24.
74. Unruh D. Everlasting multi-party computation. In: Canetti R, Garay JA, editors. Advances in cryptology – CRYPTO 2013. 2013. p. 380–97.
75. Qi R, Sun Z, Lin Z, Niu P, Hao W, Song L, Huang Q, Gao J, Yin L, Long G-L. Implementation and security analysis of practical quantum secure direct communication. Light Sci Appl. 2019;8:22.
76. Deng F-G, Long GL, Liu X-S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A. 2003;68:042317.
77. Qi Z, Li Y, Huang Y, Feng J, Zheng Y, Chen X. A 15-user quantum secure direct communication network. Light Sci Appl. 2021;10:183.

78. Sheng Y-B, Zhou L, Long G-L. One-step quantum secure direct communication. Sci Bull. 2022;67(4):367–74.
79. Zhang W, Ding D-S, Sheng Y-B, Zhou L, Shi B-S, Guo G-C. Quantum secure direct communication with quantum memory. Phys Rev Lett. 2017;118:220501.
80. Zhou L, Sheng Y-B, Long G-L. Device-independent quantum secure direct communication against collective attacks. Sci Bull. 2020;65(1):12–20.
81. Walk N, Eisert J. Sharing classical secrets with continuous-variable entanglement: composable security and network coding advantage. PRX Quantum. 2021;2:040339.
82. Kogias I, Xiang Y, He Q, Adesso G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. Phys Rev A. 2017;95:012315.
83. Williams BP, Lukens JM, Peters NA, Qi B, Grice WP. Quantum secret sharing with polarization-entangled photon pairs. Phys Rev A. 2019;99:062311.
84. Grasselli F, Kampermann H, Bruß D. Conference key agreement with single-photon interference. New J Phys. 2019;21:123002.
85. Murta G, Grasselli F, Kampermann H, Bruß D. Quantum conference key agreement: a review. Adv Quantum Technol. 2020;3:2000025.
86. Proietti M, Ho J, Grasselli F, Barrow P, Malik M, Fedrizzi A. Experimental quantum conference key agreement. Sci Adv. 2021;7:eabe0395.
87. Garg S, Yuen H, Zhandry M. New security notions and feasibility results for authentication of quantum data. In: Katz J, Shacham H, editors. Advances in cryptology – CRYPTO 2017–37th annual international cryptology conference, proceedings, part II. Lecture notes in computer science. vol. 10402. Santa Barbara, CA, USA. August 20–24, 2017. Berlin: Springer; 2017. p. 342–71.
88. Portmann C. Quantum authentication with key recycling. In: Coron J, Nielsen J, editors. Advances in cryptology – EUROCRYPT 2017 – 36th annual international conference on the theory and applications of cryptographic techniques, proceedings, part III. Lecture notes in computer science. vol. 10212. Paris, France. April 30–May 4, 2017. 2017. p. 339–68.
89. Unruh D. Revocable quantum timed-release encryption. J ACM. 2015;62(6):49:1–49:76.