A ONE-WAY FUNCTION BASED ON NORM FORM EQUATIONS

A. BÉRCZES, J. KÖDMÖN, AND A. PETHŐ

Abstract. In this paper we present a new one-way function with collision resistance. The security of this function is based on the difficulty of solving a norm form equation. We prove that this function is collision resistant, so it can be used as a one-way hash function. We show that this construction probably provides a family of one-way functions.

1. Introduction

The most basic notion for cryptographic applications is the one-way function. This is a function which is "easy" to compute but "hard" to invert.

The notion of the one-way function is of central importance in cryptography. These functions are important building blocks for most of the protocols and play a fundamental role in verifying passwords and creating digital signatures. Their use is important for constructing a cryptographically secure pseudo-random-sequence generator. There is an extensive literature on one-way functions and their applications. We refer here only to two fundamental books [17] and [22].

After all we have an important remark. Although one-way functions are widely believed to exist, and there are several conjectured candidate one-way functions which are widely used, we currently do not know how to *prove mathematically (without any assumption)* that they actually exist. In the rest of the paper we will say one-way function instead of candidate one-way function, which is a widely accepted convention in the literature.

1991 *Mathematics Subject Classification.* 94A60, 11Y40, 11Y16.

Key words and phrases. one-way function, norm form equation, number field.

The research was supported in part by the Grants F034981, T042985 and T038225 from the Hungarian National Foundation for Scientific Research, by the FKFP grant 3272-13066/201 and by the Netherlands Organization for Scientific Research.

The papers [24], [18], [5] and [14] show how to construct a one-way function. O. Goldreich, L. Levin and N. Nisan [8] make a one-to-one one-way function based on the hardness of inverting RSA and the discrete log problem.

J. Buchmann and S. Paulus [3] use results from algebraic number theory to construct a one-way function. It is based on the hardness of the discrete logarithm problem with respect to the ideal class group of algebraic number fields.

In this paper we present a new one-way function with collision resistance and avalanche effect. The hardness of inverting this function is indicated by the difficulty of solving a *norm form equation*. A norm form equation is a special case of a decomposable form equation. We will construct a function using a norm form; we will prove that this function is "easy" to compute and we will show facts indicating that it is "hard" to invert. There is an extensive literature on decomposable form equations and their applications. For results and further references we refer to the books and survey papers [2], [11], [12], [13], [23], [6] and [21].

2. The definition of one-way functions and their properties

In this paper we will use the modern notion of one-way functions based on complexity theory which involves probabilistic algorithms instead of deterministic ones. This setting was proposed first by Goldwasser and Micali [10]. The definition of a *one-way function* and a *collection of one-way functions* below are from the book of Goldwasser and Bellare [9].

First we define the notion of *negligible functions*:

Definition 1. *The function $\nu : \mathbb{N} \to \mathbb{R}$ is called **negligible**, if for every constant $c \geq 0$ there exists an integer k_c such that $\nu(k) < k^{-c}$ for all $k \geq k_c$.*

Now we present the definition of *one-way functions*:

Definition 2. *The function $f : \{0,1\}^* \to \{0,1\}^*$ is called a **one-way** function if:*

(1) There exists a PPT algorithm[1] *that on input x outputs $f(x)$.*

(2) For every PPT algorithm $\mathcal{A}$ there is a negligible function $\nu_{\mathcal{A}}$ such that for sufficiently large k,

$$\mathbf{P}\left[f(z) = y : \quad x \overset{R}{\in} \{0,1\}^k; \quad y = f(x); \quad z = \mathcal{A}(k,y)\right] \leq \nu_{\mathcal{A}}(k),$$

where the probability is taken over choices of x, and the coin tosses of $\mathcal{A}$.

[1]Probabilistic polynomial time

Let $x \overset{R}{\in} \{0,1\}^k$ denote that x is chosen randomly with uniform distribution from all possible binary words with length k.

The constant k is the security parameter which is identical with the binary length of the input of the cryptosystem and fixed at the time the cryptosystem is setup.

The meaning of Definition 2 is that the probability of the following event is negligable: One chooses x randomly with binary length k and computes $y = f(x)$. The algorithm $\mathcal{A}$ computes from input k and y the output z such that $f(z) = y$.

This definition is less directly relevant to practice, but useful for theoretical purposes. However, in cryptography we must typically envisage not a single one-way function but a collection of them.

Definition 3. *Let I be a set of indices and for $i \in I$ let D_i and R_i be finite sets. A* ***collection of one-way functions*** *is a set*

$$F = \{f_i : D_i \mapsto R_i\}_{i \in I}$$

satisfying the following conditions:

(1) There exists a PPT algorithm $\mathcal{S}_1$ which on input k outputs an $i \in I$ with maximum length k.

(2) There exists a PPT algorithm $\mathcal{S}_2$ which on input $i \in I$ outputs $x \in D_i$.

(3) There exists a PPT algorithm $\mathcal{A}_1$ which on input $i \in I$ and $x \in D_i$ outputs $f_i(x)$, i. e. $\mathcal{A}_1(i, x) = f_i(x)$.

(4) For every PPT algorithm $\mathcal{A}$ there exists a negligible function $\nu_{\mathcal{A}}$, such that for all sufficiently large k

$$\mathbf{P}\left[f_i(z) = y : \quad i \overset{R}{\in} I, \quad x \overset{R}{\in} D_i; \quad y = f_i(x); \quad z = \mathcal{A}(i, y)\right] \leq \nu_{\mathcal{A}}(k).$$

where the probability is taken over choices of i and x, and the coin tosses of algorithm $\mathcal{A}$.

The algorithm $\mathcal{S}_1$ chooses the index and the algorithm $\mathcal{S}_2$ chooses the input x from the domain which corresponds to the index i. The algorithm $\mathcal{A}_1$ calculates the value $f_i(x)$, and the algorithm $\mathcal{A}$ tries to invert the function f_i.

Remark 1. *One can show that the existence of a single one-way function is equivalent to the existence of a collection of one-way functions. For a proof see* [9].

Important properties of one-way functions are the *collision resistance* and the *avalanche effect*. Now we are presenting the definition of these notions.

Definition 4. *A one-way function f is* ***collision resistant*** *if there exists a negligible function ν, such that*

$$\mathbf{P}\left[f(x_1) = f(x_2)\right] \leq \nu(k)$$

holds for any two distinct inputs $x_1 \neq x_2$ and sufficiently large k, where the probability is taken independently over all $x_1, x_2 \in \{0,1\}^k$.

Remark 2. *In this definition (x_1, x_2) is considered as a uniformly distributed vector variable. There is another property of f to find x_2 for fixed input x_1 or to find x_2 for fixed output $f(x_1)$ such that $f(x_1) = f(x_2)$. We call these properties 2nd-preimage resistance and preimage resistance respectively. For their definitions see* [17].

Remark 3. *Obviously the one-to-one functions are collision resistant.*

The notion of **avalanche effect** is discussed first in connection with the S-boxes of DES by Feistel, Notz and Smith [7]. Kam and Davida [15] called this property *completeness* and defined it in the following way: a function is complete if each output bit depends on all input bits. Webster and Tavares [25] proposed the more stringent notion of avalanche effect:

Definition 5. *(Strict avalanche criterion) A function f has* ***strict avalanche effect*** *if whenever one input bit of f is changed, every output bit of f is changing with probability $\frac{1}{2}$.*

More simply, a function has strict avalanche effect if the change of one input bit implies a change on the half of the output bits. We will measure the change of bits via *Hamming-distance*. Its definition is the following:

Definition 6. *(Hamming-distance) Let $x = (\xi_1, ..., \xi_n)$ and $y = (\eta_1, ..., \eta_n)$ be the binary representations of the numbers $x, y \in \mathbb{Z}$, respectively, where $\xi_i, \eta_i \in \{0,1\}$. The* ***Hamming-distance*** *of the numbers x and y is*

$$\varrho(x,y) = \sum_{i=1}^{n} \xi_i \oplus \eta_i,$$

where $\oplus$ denotes the exclusive-or operator.

One-way hash functions play also a fundamental role in modern cryptography.

Definition 7. *The function f is a* ***one-way hash function*** *if f is a one-way, collision resistant function and f maps an input x of arbitrary finite bitlength to an output $f(x)$ of fixed bitlength.*

The widely used one-way hash functions (MD5, RIPE-MD, SHA) are based on block ciphers. For results and further references we refer to the books [17] and [22].

3. The mappings $\mathcal{N}_P$ and $\mathcal{N}_{P,s}$ are one-way functions

Let $P(X) \in \mathbb{Z}[X]$ be a fixed monic polynomial of degree $n \geq 3$ having no multiple roots. Denote by $\alpha_1, \ldots, \alpha_n$ the roots of P and put

$$L_i(\underline{X}) := \sum_{j=1}^{m} \alpha_i^{j-1} X_j \quad \text{for} \quad i = 1, \ldots, n \text{ and } m \leq n.$$

Define the norm form corresponding to the polynomial P by

$$\mathcal{N}_P(\underline{X}) := \prod_{i=1}^{n} L_i(\underline{X}).$$

In fact, $\mathcal{N}_P(\underline{X})$ is a generalization of the concept of norm form and is a special decomposable form. Further, $\mathcal{N}_P(\underline{X})$ is a homogeneous polynomial of degree n, with integer coefficients.

Construction 1. *Define the mapping $\mathcal{N}_P : \mathbb{Z}^m \to \mathbb{Z}$ in the following way:*

$$\mathcal{N}_P : (x_1, \ldots, x_m) \mapsto \mathcal{N}_P(x_1, \ldots, x_m). \tag{1}$$

Since $\mathcal{N}_P(\underline{X})$ is a homogeneous polynomial with integer coefficients the function value $\mathcal{N}_P(\underline{x})$ will be a rational integer for every $\underline{x} \in \mathbb{Z}^m$.

In the case when P is irreducible a detailed investigation of the complexity of the computation of the value $\mathcal{N}_P(\underline{x})$ using three different methods can be found in [1]. In that paper we proved that the complexity of the determination of $\mathcal{N}_P(\underline{x})$ using matrix representation combined with modular arithmetic is $O(n^7 + n^6 \log \mathbb{X} + n^2 \log^{3/2} \mathbb{X})$, where n denotes the degree of P, $\mathbb{X} = \max\{|x_1|, \ldots, |x_m|, 1\}$ and the constant implied by the O notation depends only on the maximum of the absolute values of the coefficients of P.

This method can be applied in the same manner also in the case of reducible P. Indeed, since α_i^n can be represented as a linear combination of $1, \alpha_i, \ldots, \alpha_i^{n-1}$ we have

$$\alpha_i^k = \sum_{j=0}^{n-1} f_{kj} \alpha_i^j; \quad f_{kj} \in \mathbb{Z},$$

which means that

$$L_i(\underline{X}) \begin{pmatrix} 1 \\ \alpha_i \\ \vdots \\ \alpha_i^{n-1} \end{pmatrix} = (f_{kj}(\underline{X})) \begin{pmatrix} 1 \\ \alpha_i \\ \vdots \\ \alpha_i^{n-1} \end{pmatrix},$$

where $f_{kj}(\underline{X}) \in \mathbb{Z}[\underline{X}]$ are linear polynomials.

From cryptographical point of view it would be more convenient to work over finite domains. For $s \in \mathbb{Z}$ let $\mathbb{Z}_s := \mathbb{Z}/s\mathbb{Z}$.

Construction 2. *Let s be an integer and define the mapping $\mathcal{N}_{P,s} : \mathbb{Z}_s^m \to \mathbb{Z}_s$ in the following way:*

$$\mathcal{N}_{P,s} : (x_1, ..., x_m) \mapsto \mathcal{N}_P(x_1, \ldots, x_m) \bmod s. \tag{2}$$

where $u \bmod s$ denotes the remainder by dividing u by s.

Remark 4. *In Construction 2 the security parameter is the constant s.*

The best way to compute the value $\mathcal{N}_{P,s}(x_1, ..., x_m)$ is the method using matrix representation described in Theorem 2 in [1], however the whole computation can be done mod s. The following theorem shows the complexity of the calculation of the value $\mathcal{N}_{P,s}(x_1, ..., x_m)$.

Theorem 1. *The complexity of the computation of $\mathcal{N}_{P,s}(\underline{x})$, using the algorithm described in Theorem 2 of* [1] *is $O(n^5 \log^2 s)$, where the constant in O depends only on $P(X)$.*

Proof. The proof is nearly identical with the one of Theorem 3 of [1], we just use that our operations are in $\mathbb{Z}_s$ instead of $\mathbb{Z}$. □

The fact that actually there is no known algorithm for determining all solutions of general norm form equations, i.e. inverting $\mathcal{N}_{P,s}$ is described by the following condition:

Definition 8. ***Strong Modular Norm form Assumption(SMNA)**: For every polynomial Q and every PPT algorithm $\mathcal{A}$, and for all sufficiently large positive integers s*

$$P[\mathcal{A}(s, b) = (x_1, ..., x_m) \text{ such that } b = \mathcal{N}_{P,s}(x_1, ..., x_m)] < \frac{1}{Q(k)},$$

where $x_i \in \mathbb{Z}_s$ and the probability is taken over all values x_i and the coin tosses of $\mathcal{A}$.

We have the following theorem:

Theorem 2. *Under SMNA the function $\mathcal{N}_{P,s}$ is a one-way function.*

Proof. We must show that the function $\mathcal{N}_{P,s}$ satisfies the assumption of Definition 2. Since by Theorem 1 there exists a deterministic algorithm, which computes $\mathcal{N}_{P,s}$, assumption (1) of Definition 2 is satisfied.

The assumption (2) of Definition 2 is an immediate consequence of SMNA. Thus our theorem is proved. □

Using the function $\mathcal{N}_{P,s}$ we can create a collection of one-way functions in the following way.

Construction 3. *Let $\mathcal{P}$ be a subset of all monic and squarefree polynomials of degree $n \geq 4$. Let m, s be integers with $3 \leq m \leq n$ and define*

$$\mathbf{MNFF} := \{\mathcal{N}_{P,s} : \mathbb{Z}_s^m \mapsto \mathbb{Z}_s,\ \mathcal{N}_{P,s} = \mathcal{N}_P \bmod s\}_{P \in \mathcal{P}}.$$

Remark 5. *In Construction 3 the security parameter is the constant s.*

We have the following theorem.

Theorem 3. *If for all $P(\underline{X}) \in \mathcal{P}$ condition SMNA holds for $\mathcal{N}_{P,s}$ then MNFF is a collection of one-way functions.*

Proof. We have to show that **MNFF** satisfies the assumption of Definition 3, provided that each function $\mathcal{N}_{P,s}$ satisfies SMNA.

Obviously the domain and the codomain of each function $\mathcal{N}_{P,s}$ is finite.

The algorithm $\mathcal{S}_1$ chooses randomly a polynomial $P \in \mathbb{Z}[X]$ of degree $n(\geq 4)$ having no multiple roots.

The algorithm $\mathcal{S}_2$ chooses the domain $\mathbb{Z}_s^m$ corresponding to $\underline{x}$.

Let the algorithm $\mathcal{A}_1$ be the deterministic algorithm described in chapter 4 of [1]. This algorithm computes the value $\mathcal{N}_{P,s}(\underline{x}) \in \mathbb{Z}$ from $\underline{x} \in \mathbb{Z}_s^m$. The complexity of this algorithm is polynomial in the input value $\underline{x}$ by Theorem 1.

Since the complexity of algorithms $\mathcal{S}_1, \mathcal{S}_2$ and $\mathcal{A}_1$ are polynomial thus assumptions (1), (2) and (3) of Definition 3 are satisfied.

Assumption (4) is an immediate consequence of SMNA. Thus Theorem 3 is proved. □

Unfortunately we are not able to present pairs P, s for which SMNA holds. In the other direction we prove the following Proposition.

Proposition 1. *Let s be a prime, $P \in \mathbb{Z}[X]$ and $b \in \mathbb{Z}_s$. Then there exists a PPT algorithm which computes $\underline{x} = (x_1, \ldots, x_m) \in \mathbb{Z}_s^m$ with $\mathcal{N}_{P,s}(\underline{x}) = b$.*

Proof. Let $a = \mathcal{N}_{P,s}(1, 0, \ldots, 0)$. Obviously $a \neq 0$. Choose $c \in \mathbb{Z}_s$ such that

$$c^n \mathcal{N}_{P,s}(1, 0, ..., 0) = \mathcal{N}_{P,s}(c, 0, ..., 0) = c^n a = b \pmod{s},$$

that is

$$c^n \equiv \frac{b}{a} \pmod{s}. \tag{3}$$

However, if s is prime, then equation (3) can be solved in probabilistic polynomial time by Berlekamp's factorization algorithm (see [4]). □

Thus in the sequel we suppose that $s = pq$, where p and q are large rational primes. In this case the above method for breaking our one-way function candidate does not work, since the solution of equation (3) is computationally infeasible.

4. The properties of the function $\mathcal{N}_P$ and $\mathcal{N}_{P,s}$

In this section we investigate the probability of the collision for the function $\mathcal{N}_{P,s}$, i. e. we are interested in the probability

$$P_{coll} = P[\mathcal{N}_{P,s}(\underline{x}) = \mathcal{N}_{P,s}(\underline{y}) : \underline{x}, \underline{y} \in {\mathbb{Z}_s}^m].$$

Our main result is the following theorem.

Theorem 4. *Let $P(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree at least 3 having no multiple roots. Let p and q be primes such that $q > p > q/2$ and $s := pq$. Suppose that $gcd(m, \varphi(s)) = 1$. Let $N(P, b, s)$ denote the number of solutions of the congruence $N_P(x_1, \dots, x_m) \equiv b \pmod{s}$.*

- *If $(b, s) = 1$ we have*
$$|N(P, b, s) - s^{m-1}| < c_1(P) s^{m-1-\frac{1}{4}};$$
- *otherwise*
$$N(P, b, s) < c_2(P) s^{m-1}.$$

Theorem 5. *Let $P(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree at least 3 having no multiple roots. Let p and q be primes such that $q > p > q/2$ and $s := pq$. Suppose that $gcd(m, \varphi(s)) = 1$. Then the probability of collision P_{coll} for the function $\mathcal{N}_{P,s}$ satisfies the inequality*

$$P_{coll} < \frac{C}{s},$$

where the constant C depends only on the polynomial P.

To prove Theorem 4 we need two lemmas.

Lemma 1. *Let $P(X) \in \mathbb{C}[X]$ be a polynomial, which has at least one simple zero. Then the polynomial $Z^n - P(X) \in \mathbb{C}[X, Z]$ is absolutely irreducible for every $n \geq 2$.*

Proof of Lemma 1. This is a consequence of a theorem of Capelli (see e.g. [20] p.662). □

Lemma 2. *Let $f(\underline{X}) := f(X_1, \dots, X_m) := \prod_{i=1}^{n} (\alpha_{i1} X_1 + \dots + \alpha_{im} X_m) \in \mathbb{C}[X_1, \dots, X_m]$ be a form with the properties $\alpha_{ij} \in \mathbb{C}$ for $1 \leq i \leq n$, $1 \leq j \leq m$, and $\prod_{i=1}^{n} \prod_{j=1}^{m} \alpha_{ij} \neq 0$. Suppose that there exist $1 \leq j_1 < j_2 \leq n$ such that*

$$\frac{\alpha_{ij_1}}{\alpha_{ij_2}} \notin \left\{ \frac{\alpha_{kj_1}}{\alpha_{kj_2}} : 1 \leq k \leq n, k \neq i \right\}. \tag{4}$$

Then the polynomial $f(\underline{X}) - a$ is irreducible for every $0 \neq a \in \mathbb{C}$.

Proof of Lemma 2. Suppose indirectly that $f(\underline{X}) - a$ is reducible. Put $f_0(X_{j_1}, X_{j_2}) = \prod_{i=1}^{n}(\alpha_{ij_1}X_{j_1} + \alpha_{ij_2}X_{j_2}) \in \mathbb{C}[X_{j_1}, X_{j_2}]$.

It is easily seen that from the reducibility of $f(\underline{X}) - a$ follows the reducibility of $f_0(X_{j_1}, X_{j_2}) - a$. Indeed, if there exists a non-trivial factorization $f(\underline{X}) - a = g(\underline{X})h(\underline{X})$ of $f(\underline{X}) - a$ then using that the total degree of $f(\underline{X}) - a$ is n and $0 < \deg_{X_i}(f(\underline{X}) - a) < n$ for every $i = 1, \ldots, m$ it follows that $0 < \deg_{X_i} g(\underline{X}) < n$ and $0 < \deg_{X_i} h(\underline{X}) < n$ for every $i = 1, \ldots, m$. Thus every non-trivial factorization of $f(\underline{X}) - a$ induces a non-trivial factorization of $f_0(X_{j_1}, X_{j_2}) - a$. Further,

$$\begin{aligned} f_0(X_{j_1}, X_{j_2}) - a =& a_0X_{j_1}^n + a_1X_{j_1}^{n-1}X_{j_2} + \cdots + a_nX_{j_2}^n - a = \\ &= X_{j_2}^n\left(a_0\left(\frac{X_{j_1}}{X_{j_2}}\right)^n + a_1\left(\frac{X_{j_1}}{X_{j_2}}\right)^{n-1} + \cdots + a_n\right) - a. \end{aligned}$$

Put $P(Y) := a_0Y^n + a_1Y^{n-1} + \cdots + a_n \in \mathbb{C}[Y]$ and $Z := a^{1/n}X_{j_2}^{-1}$. Then $f_0(X_{j_1}, X_{j_2}) - a$ is reducible over $\mathbb{C}$, thus the polynomial $P(Y) - Z^n \in \mathbb{C}[Y, Z]$ is also reducible over $\mathbb{C}$. However, from (4) it follows that $P(Y)$ has a simple zero, and thus by Lemma 1 $P(Y) - Z^n$ is irreducible, which is a contradiction. □

Proof of Theorem 4. First suppose that $\gcd(b, s) = 1$. Consider the equation $\mathcal{N}_P(X_1, ..., X_m) \equiv b \pmod{s}$ and put $f := \mathcal{N}_P(X_1, ..., X_m) - b$. By Lemma 2 the polynomial f is absolutely irreducible. Indeed, we can choose $i = 1$, $j_1 = 2$ and $j_2 = 1$ and since now the condition required in Lemma 2 is $\alpha_1 \notin \{\alpha_2, \ldots, \alpha_n\}$, and since P has no multiple roots this condition is fulfilled.

Now we can use a theorem of S. Lang and A. Weil [16]. By this theorem, if the prime modulus p is sufficiently large the number of solutions $N(f, p)$ of the equation $f \equiv 0 \pmod{p}$ satisfies the inequality

$$\left|N(f, p) - p^{m-1}\right| < C(f)p^{m-1-\frac{1}{2}}, \tag{5}$$

where the constant $C(f)$ depends only on the coefficients of the absolutely irreducible polynomial f. Further, we note that the constant $C(f)$ in our case does not depend on the value of b. Indeed, since $\gcd(m, \varphi(s)) = 1$ for every $0 \neq b \in \mathbb{Z}_s$ there exists a $0 \neq a \in \mathbb{Z}_s$ such that $a^m \equiv b \pmod{s}$, and thus we have

$$\mathcal{N}_P(X_1, ..., X_m) - b \equiv \mathcal{N}_P(X_1, ..., X_m) - a^m \equiv a^m\left(\mathcal{N}_P\left(\frac{X_1}{a}, ..., \frac{X_m}{a}\right) - 1\right) \pmod{s}.$$

Thus the solutions of $f \equiv 0 \pmod{s}$ can be derived from the solutions of $\mathcal{N}_P(Y_1, ..., Y_m) \equiv 1 \pmod{s}$ using the simple transformation $(X_1, ..., X_m) =$

$a(Y_1, ..., Y_m)$, and the number of solutions of $\mathcal{N}_P(Y_1, ..., Y_m) \equiv 1 \pmod{s}$ clearly does not depend on b.

By (5) we have

$$|N(P, b, p) - p^{m-1}| < C_1 p^{m-1-\frac{1}{2}} \tag{6}$$

and

$$|N(P, b, q) - q^{m-1}| < C_1 q^{m-1-\frac{1}{2}}. \tag{7}$$

By the Chinese remainder theorem (see [4]) the number of solutions of the equation $f \equiv 0 \pmod{s}$ is $N(P, b, s) = N(P, b, p)N(P, b, q)$. Thus we have

$$\begin{aligned} N(P, B, s) &< (pq)^{m-1} + (pq)^{m-1}\left(\frac{C_1}{p^{1/2}} + \frac{C_1}{q^{1/2}}\right) + (pq)^{m-1}\frac{C_1^2}{(pq)^{1/2}} \\ &< (pq)^{m-1} + (pq)^{m-1}\frac{C_2}{pq^{3/2}} < s^{m-1} + \frac{C_3}{s^{m-1-1/4}}. \end{aligned}$$

The inequality

$$N(P, b, s) > s^{m-1} - \frac{C_4}{s^{m-1-1/4}}$$

follows similarly.

Now suppose that $\gcd(b, s) \neq 1$. If $\gcd(b, p) \neq 1$ then $\mathcal{N}_P(X_1, \ldots, X_m) \equiv 0 \pmod{p}$, and since $\mathcal{N}_P$ factorises into linear factors, all solutions of this congruence are contained in the union of at most n linear subspaces of $\mathbb{Z}_p^m$ of dimension $m - 1$. Thus $N(P, b, p) < np^{m-1}$. If $\gcd(b, s) = 1$ then by (6) we have $N(P, b, p) < C_5 p^{m-1}$. Similar reasoning is true for $N(P, b, q)$. Thus we have

$$N(P, b, s) < c_2(P)s^{m-1} \tag{8}$$

for any b. This concludes the proof of Theorem 4. □

Proof of theorem 5. By (8) we have

$$P_{coll} := \frac{N(P, b, s)}{s^m} < \frac{C}{s}.$$

□

Corollary 1. *If the module s is sufficiently large then the function $\mathcal{N}_{P,s}$ is collision resistant.*

To test the avalanche effect of the function $\mathcal{N}_{P,s}$ we used an implementation of these functions in the computer algebraic system MAPLE. Denote by $\underline{x}$ a binary input value and by $\underline{x}'$ another binary input value, which differs in a single bit from x.

These implementations calculated the following relative Hamming-distances

$$RH_{P,s} := \frac{\rho(\mathcal{N}_{P,s}(\underline{x}), \mathcal{N}_{P,s}(\underline{x}'))}{l(s)}.$$

where $l(.)$ denotes the binary length function and $\rho(.,.)$ is the Hamming-distance described in Definition 6.

The tests were run 1000 times with randomly generated inputs with size 2^{160}. The positions of the changed input bits in $\underline{x}'$ were also randomly generated.

Conjecture 1. *The function $\mathcal{N}_{P,s}$ satisfies the strict avalanche criterion described in Definition 5.*

5. Some applications

In the former sections we described some basic properties of norm form functions associated to polynomials with integer coefficients. Here we consider the same problem from a more practical point of view.

The functions $\mathcal{N}_{P,s}$ is adaptable all the wonted cryptographically application namely checking data integrity, entity authentication, digital signatures and generation of pseudo random sequences. These functions can play an important role on building of cryptographic protocols.

Pseudorandom functions can be constructed also based on the one-way function $\mathcal{N}_{P,s}$.

The first question is how to choose $P(X)$ such that the associated norm form could be easily calculated. Let $P(X) := X^n - 1$. Denote ζ one of the primitive n-th roots of unity and let

$$L(\underline{X}) := X_1 + \zeta X_2 + \cdots + \zeta^{n-1} X^n.$$

As

$$\zeta^j L(X) = X_{n-j+1} + \zeta X_{n-j+2} + \cdots + \zeta^{j-1} X_n + \zeta^j X_1 + \cdots + \zeta^{n-1} X_{n-j}$$

holds for all $1 \leq j \leq n$ we obtain that $\mathcal{N}_P(\underline{X})$ is the determinant of the circular matrix

$$\begin{pmatrix} X_1 & X_2 & \dots & X_n \\ X_n & X_1 & \dots & X_{n-1} \\ \dots & \dots & \dots & \dots \\ X_2 & X_3 & \dots & X_1 \end{pmatrix},$$

which has particular simple form. $P(X)$ has only simple roots, hence the assumption of Theorem 4 is satisfied. Thus $\mathcal{N}_P(\underline{X})$ is collision resistant.

We propose to apply $N_{P,s}(\underline{X})$ as a hash function. In the practice hash functions map messages to 160 bit words. Hence $s = pq$ should be about of this size. Unfortunately, in our case this setting is not secure, because 160 bit integers can be easily factorized and by Proposition 1 one can find

arguments, which cause collision. Enlarging however the set of possible hash values to at least 2^{1024}, our function becomes collision resistant. Hence $s = pq$ should be about this size.

Choose the prime q of size 2^{512} and then the prime p such that $q > p > q/2$. This is certainly possible by Tschebishev's theorem. Moreover we have to be aware of the condition $\gcd(m, (p-1)(q-1)) = 1$. After choosing p and q appropriately put $s = pq$.

Having a message M consider it as a binary word and split it into subwords $x_1, \dots, x_k$ such that each x_i, $i = 1, \dots, k$ represents an integer in the interval $[1, s-1]$. Assume that $k \geq m$, otherwise extend the sequence by words representing 0. There are several possibilities to extend the function $N_{P,s}(\underline{X})$ to the more general situation. We prefer the following:

$$h(x_1, \dots, x_m) := N_{P,s}(x_1, \dots, x_m)$$

and we define recursively

$$h(x_1, \dots, x_{m+t(m-1)}) := N_{P,s}(h(x_1, \dots, x_{m+(t-1)(m-1)}), x_{m+(t-1)(m-1)+1}, \dots, x_{m+t(m-1)}).$$

If k is not of the form $m + t(m-1)$ with some suitable $t \in \mathbb{Z}$ then we can extend M with words representing 0 until k has the required form.

This function will keep collision free in all the steps of the iteration and has avalanche effect (see Theorem 4. and Conjecture 1.). These properties guarantee its security.

References

[1] A. Bérczes, J. Ködmön, *Methods for the calculation of values of a norm form*, Publ. Math. Debrecen. 63 (2003), 751-768

[2] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1967, 2nd ed.

[3] J. Buchmann, S. Paulus, *A one-way function based on ideal arithmetic in number fields*, Lect. Notes Comput. Sci. 1294 (1997), 385-394.

[4] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

[5] L.R. Chao, Y.C. Lin, *Associative one-way function and its significances to cryptographics*, In. J. Inf. Manage. Sci. 5 (1994), 53-59.

[6] J.H. Evertse, K. Győry, *Decomposable form equations, In: New advances in transcendence theory (ed. by A. Baker)*, 175-202, Cambridge Univ Press, Cambridge 1988.

[7] H. Feistel, W. A. Notz, J. L. Smith, *Some cryptographic techniques for machine-to-machine data communications*, Proceedings of the IEEE, 63 (1975), 1545-1554.

[8] O. Goldreich, L. Levin, N. Nisan, *On constructing 1-1 one-way functions*, Electronic colloquium on computational complexity, TR-95-029, 6/25/95, 1995.

[9] S.Goldwasser, M.Bellare, *Lecture Notes on Cryptography*, MIT Press, Cambridge, Massachusetts 2001.

[10] S. Goldwasser, S. Micali, *Probabilistic encryption*, J. CSS, 28 (1984), 270-299.

[11] K. Győry, *Résultats effectifs sur la représentation des entires par des formes décomposables (Queen's Papers in Pure and Appl. Math. 56)*, Queen's Univ., Kingston 1980.
[12] K. Győry, *On norm form, discriminant form and index form equations, In: Topics in classical number theory(ed. by G. Halász; Colloq. Math. Soc. János Bolyai 34)*, 617-676, North-Holland, Amsterdam 1984.
[13] K. Győry, *On the distribution of solutions of decomposable form equations. Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, 237–265, de Gruyter, Berlin, 1999.
[14] L.A. Hemaspaandra, J. Rothe, *Creating strong, total, commutative, associative one-way functions from any one-way function in comlexity theory*, J. Comput. Syst. Sci. 58 (1999), 648-659.
[15] J. Kam, G. Davida, *Structured design of substitution-permutation encryption networks*, IEEE Transactions on Computers, 28 (1979), 747-753.
[16] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Am. J. Math. 76 (1954), 819-827.
[17] A.J.Menezes, P.C.van Oorschot, S.Vanstone, *Hadbook of Applied Cryptography*, CRC Press, 1997.
[18] R.C. Merkle, *A fast software one-way hash function*, J. Cryptology 3 (1990), 43-58.
[19] A.Pethő, *Algebraische Algorithmen*, Vieweg Verlag, 1999.
[20] L. Rédei, *Algebra I*, Akademische Verlagsgeselschaft Geest & Portig K.-G., Leipzig, 1959.
[21] W. M. Schmidt, *Diophantine approximations and diophantine equations (Lecture Notes in Math. 1467)*, Springer, Berlin 1991.
[22] B.Schneier, *Applied Cryptography*, John Wiley & Sons,1996.
[23] T.N. Shorey, R. Tijdeman, *Exponential diophantine equations*, Cambridge Univ. Press, Cambridge 1986.
[24] Q. Sun, *A kind of trap-door one-way function over algebraic integers*, J. Sichuan Univ., Nat. Sci. Ed. No. 2 (1986), 22-27.
[25] A.F. Webster, S.E. Tavares, *On the design of S-boxes*, Advances in Cryptology-CRYPTO'85 (LNCS 218), 523-534, 1986.

A. Bérczes
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: berczesa@math.klte.hu

J. Ködmön
Faculty of Health College
University of Debrecen
H-4400 Nyíregyháza, Sóstói 2., Hungary
E-mail address: kodmonj@de-efk.hu

A. Pethő
Institute of Informatics
University of Debrecen
H-4010 Debrecen, P.O. Box 12
E-mail address: pethoe@inf.unideb.hu