AN APPLICATION OF INDEX FORMS IN CRYPTOGRAPHY

ATTILA BÉRCZES AND ISTVÁN JÁRÁSI

Abstract. In the present paper we investigate the possibility of using index forms as basic ingredients of cryptographically important functions. We suggest the use of a hash function based on index forms and we prove some important properties of the suggested function.

1. Introduction

In [1] and [2] Bérczes, Ködmön and Pethő investigated the possibility of cryptographical applications of norm forms. They provided a detailed complexity analysis of the computation of values of norm forms, and suggested the use of a hash function based on norm forms. They even proved that in a probabilistic sense their hash function is collision resistant. Further, the company Crypto Ltd. purchased the idea of this hash function from the University of Debrecen and implemented the hash function. They named the product CODEFISH. The aim of the present paper is to investigate the possibility of building a hash function based on index forms.

2. Basic definitions

2.1. **Definition of some cryptographic primitives.** The Handbook of Applied Cryptography [14] defines the one way function in the following way:

Definition 2.1. *A function f from a set X to a set Y is called a one-way function if $f(x)$ is easy to compute for all $x \in X$ but for essentially all*

2000 Mathematics Subject Classification: 94A60, 11Y16.

Keywords and Phrases: index form, hash function.

The research was supported in part by the Hungarian Academy of Sciences, by grants T048791 and K67580 of the Hungarian National Foundation for Scientific Research, by the National Office for Research and Technology and by the grant JP-26/2006.

elements $y \in Im(f)$ it is computationally infeasible to find any $x \in X$ such that $f(x) = y$.

Remark 2.1. *The phrase "for essentially all elements in Y" refers to the fact that there are a few values $y \in Y$ for which it is easy to find an $x \in X$ such that $y = f(x)$. For example, one may compute $y = f(x)$ for a small number of x values and then for these, the inverse is known by table look-up. An alternate way to describe this property of a one-way function is the following: for a random $y \in Im(f)$ it is computationally infeasible to find any $x \in X$ such that $f(x) = y$.*

The above definition is very simple, and shows most clearly the simple ideas behind the concept of one-way function. However, we are looking for cryptographically interesting functions, with some mathematically proved properties, so we shall need rigorous definition of the terms "easy" and "computationally infeasible". Thus 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 [11]. The definition of a *one-way function* and a *collection of one-way functions* below are from the book of Goldwasser and Bellare [10].

Definition 2.2. *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 $k \geq k_c$.*

Definition 2.3. *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

The guarantee is probabilistic. The adversary is not unable to invert the function, but has a low probability of doing so where the probability distribution is taken over the input x to the one-way function where x is of length k, and the possible coin tosses of the adversary. Namely, $x \overset{R}{\in} \{0,1\}^k$ denotes that x is chosen randomly with uniform distribution from all possible binary words with length k, and y is set to $f(x)$. So the meaning of Definition 2.3 is that the probability of the following event is negligible:

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.

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

Definition 2.4. *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 2.2. *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* [14].

Remark 2.3. *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 [5]. Kam and Davida [12] 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 [17] proposed the more stringent notion of avalanche effect:

Definition 2.5. *(Strict avalanche criterion) We say that 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 about the half of the output bits.

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

Definition 2.6. *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 bit-length to an output $f(x)$ of fixed bit-length.*

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 [14] and [16].

2.2. **Index forms.** Let K be an algebraic number field of degree $n \geq 3$ with discriminant D_K and ring of integers $\mathcal{O}_K$. Let $\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_n$ denote the $\mathbb{Q}$-isomorphisms of K in $\mathbb{C}$. For any $\alpha \in K$, put $\alpha^{(i)} = \sigma_i(\alpha)$. Consider the linear forms $l^{(i)}(\mathbf{X}) = X_1 + \alpha^{(i)}X_2 + \cdots + (\alpha^{(i)})^{n-1}X_n$ for $i = 1, \dots, n$, with the convention that $l^{(1)}(\mathbf{X}) = l(\mathbf{X})$. Put $l_{ij}(\mathbf{X}) := l^{(i)}(\mathbf{X}) - l^{(j)}(\mathbf{X})$. Then

$$D_{K/\mathbb{Q}}(l(\mathbf{X})) := \prod_{1 \leq i < j \leq n} l_{ij}^2(\mathbf{X}) \tag{2.1}$$

is a decomposable form with coefficients in $\mathbb{Z}$. Clearly, we have

$$D_{K/\mathbb{Q}}(l(\mathbf{X})) = (\mathcal{I}_\alpha(\mathbf{X}))^2 D_K, \tag{2.2}$$

where $\mathcal{I}_\alpha(\mathbf{X}) = \mathcal{I}_\alpha(X_2, \dots, X_n)$ is a decomposable form of degree $n(n-1)/2$ with coefficients in $\mathbb{Z}$.

Definition 2.7. *The above form $\mathcal{I}_\alpha(\boldsymbol{X})$ is called the index form of the basis $\{1, \alpha, \dots, \alpha^{n-1}\}$.*

3. Results

Construction 1. *Put $m := n-1$. Let s be an integer and define the mapping $\mathcal{I}_{\alpha,s} : \mathbb{Z}_s^m \to \mathbb{Z}_s$ in the following way:*

$$\mathcal{I}_{\alpha,s} : (x_1, ..., x_m) \mapsto \mathcal{I}_\alpha(x_1, \ldots, x_m) \bmod s. \tag{3.3}$$

where $u \bmod s$ denotes the remainder by dividing u by s. (Note that $\mathcal{I}_\alpha(\boldsymbol{X})$ in fact is a form with integer coefficients in $n-1$ variables.)

Theorem 3.1. *Let α be an algebraic integer of degree $n \geq 5$, and suppose that the Galois group of the extension field $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is S_n. Let p and q be primes such that $q > p > q/2$ and $s := pq$. Suppose that $gcd(\frac{n(n-1)}{2}, \varphi(s)) = 1$. Let $N(\alpha, b, s)$ denote the number of solutions of the congruence $\mathcal{I}_\alpha(x_1, \ldots, x_m) \equiv b \pmod{s}$. Then for large enough values of p and q we have the following:*

- *if $(b, s) = 1$ we have*

$$|N(\alpha, b, s) - s^{m-1}| < c_1(\alpha) s^{m-1-\frac{1}{4}};$$

- *otherwise*

$$N(\alpha, b, s) < c_2(\alpha) s^{m-1}.$$

Theorem 3.2. *Let α be an algebraic integer of degree $n \geq 5$, and suppose that the Galois group of the extension field $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is S_n. Let p and q be primes such that $q > p > q/2$ and $s := pq$. Suppose that $gcd(\frac{n(n-1)}{2}, \varphi(s)) = 1$. Then for large enough values of p and q the probability of collision P_{coll} for the function $\mathcal{I}_{\alpha,s}$ satisfies the inequality*

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

where the constant C depends only on α.

Remark. We mention that in Theorems 4 and 5 of [2] the assumption that the primes p and q are sufficiently large is also necessary. This mistake was observed by A. Pethő. However, using the below Lemma 4.1 and Lemma 4.3 the proof of the results of [2] is also complete. These two Lemmata were established jointly with A. Pethő.

4. Proofs

Lemma 4.1. *Let K be any field. Let $f(\boldsymbol{X}) := f(X_1, \dots, X_m) := \prod_{i=1}^{n}(\beta_{i1}X_1 + \dots + \beta_{im}X_m) \in K[X_1, \dots, X_m]$ be a form with the properties $\beta_{ij} \in K$ for $1 \le i \le n$, $1 \le j \le m$, and $\prod_{i=1}^{n}\prod_{j=1}^{m}\beta_{ij} \neq 0$. Suppose that there exist $1 \le j_1 < j_2 \le n$ such that the polynomial*

$$f_0(X_{j_1}, X_{j_2}) := \prod_{i=1}^{n}(\beta_{ij_1}X_{j_1} + \beta_{ij_2}X_{j_2}) \tag{4.4}$$

has a simple zero. Then the polynomial $f(\boldsymbol{X}) - a$ is irreducible for every $0 \neq a \in K$.

Proof of Lemma 4.1. This is in fact a generalization of Lemma 2 in [2], where the case $K = \mathbb{C}$ is treated. However, the proof is in fact the same for the more general case, too. □

Lemma 4.2. *Let α be an algebraic number of degree $n \ge 5$ over $\mathbb{Q}$. Denote the absolute conjugates of α by $\alpha^{(1)} = \alpha, \alpha^{(2)}, \dots, \alpha^{(n)}$. Suppose that the Galois group of the extension field $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is S_n. Then we have*

$$\alpha^{(1)} + \alpha^{(2)} \notin \left\{\alpha^{(u)} + \alpha^{(v)} \mid 1 \le u < v \le n, (u, v) \neq (1, 2)\right\}.$$

Proof of Lemma 4.2. Let $1 \le u < v \le n$ be two integers with $(u, v) \neq (1, 2)$, and suppose that we have

$$\alpha^{(1)} + \alpha^{(2)} = \alpha^{(u)} + \alpha^{(v)}. \tag{4.5}$$

First suppose that $u = 1$. Then we have $\alpha^{(2)} = \alpha^{(v)}$ and $v \neq 2$ since $(u, v) \neq (1, 2)$. This contradicts the assumption that $\alpha^{(2)}$ and $\alpha^{(v)}$ are two distinct absolute conjugates of α. Clearly, the assumption $u = 2$ leads to a similar contradiction.

Now suppose that $u \neq 1, 2$. Then we also have $v \neq 1, 2$. Now, since the Galois group G of the extension field $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is S_n and $n \ge 5$ there exists an element σ of G such that $\alpha^{(1)}$, $\alpha^{(2)}$ and $\alpha^{(u)}$ are fixed under the action of σ and $\alpha^{(v)}$ is moved to $\alpha^{(w)}$ with $v \neq w$. This leads to $\alpha^{(1)} + \alpha^{(2)} = \alpha^{(u)} + \alpha^{(w)}$, which together with (4.5) shows that $\alpha^{(v)} = \alpha^{(w)}$. Since $v \neq w$ this is again a contradiction. □

Lemma 4.3. *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ a polynomial which has a simple zero over $\mathbb{C}$. Then for any sufficiently large prime $p \in \mathbb{Z}$ the polynomial $\tilde{f}(X,Y) := f(X,Y) \bmod p$ has a simple zero over any fixed algebraic closure of the finite field $\mathbb{F}_p$.*

Proof of Lemma 4.3. If p is large enough, then the procedure for computing the $\gcd(f,f')$ is exactly the same over $\mathbb{F}_p$ as over $\mathbb{Z}$. Thus Lemma 4.3 follows. □

Proof of theorem 3.1. We consider the equation $\mathcal{I}_\alpha(X_1,...,X_m) \equiv b \pmod{s}$ and put $f := \mathcal{I}_\alpha(X_1,...,X_m) - b$.

First suppose that $\gcd(b,s) = 1$. It is easily seen that by Lemmata 4.1, 4.2 and 4.3 the polynomial f is absolutely irreducible over $\mathbb{F}_p$, if $p \in \mathbb{Z}$ is a sufficiently large prime.

Thus by a theorem of S. Lang and A. Weil [13], 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

$$\left|N(f,p) - p^{m-1}\right| < C(f)p^{m-1-\frac{1}{2}}, \tag{4.6}$$

where the constant $C(f)$ depends only on the coefficients of the absolutely irreducible polynomial f. Further, in our case the constant $C(f)$ does not depend on the value of b. Indeed, since $\gcd(b,s) = 1$ and $\gcd(n(n-1)/2, \varphi(s)) = 1$ for every $0 \neq b \in \mathbb{Z}_s$ there exists a $0 \neq a \in \mathbb{Z}_s$ such that $a^{n(n-1)/2} \equiv b \pmod{s}$, and thus we have

$$\begin{aligned}\mathcal{I}_\alpha(X_1,...,X_m) - b \equiv{}& \mathcal{I}_\alpha(X_1,...,X_m) - a^{n(n-1)/2} \\ \equiv{}& a^{n(n-1)/2}\left(\mathcal{I}_\alpha\left(\frac{X_1}{a},...,\frac{X_m}{a}\right) - 1\right) \pmod{s}.\end{aligned}$$

Thus the number of solutions of $f \equiv 0 \pmod{s}$ is the same as the number of solutions of $\mathcal{I}_\alpha(Y_1,...,Y_m) \equiv 1 \pmod{s}$ (as shown by the simple transformation $(X_1,...,X_m) = a(Y_1,...,Y_m)$), and the number of solutions of this latter congruence clearly does not depend on b.

By (4.6) we have

$$|N(\alpha,b,p) - p^{m-1}| < C_1 p^{m-1-\frac{1}{2}} \tag{4.7}$$

and

$$|N(\alpha,b,q)-q^{m-1}|<C_1q^{m-1-\frac{1}{2}}. \tag{4.8}$$

By the Chinese remainder theorem (see [4]) the number of solutions of the equation $f\equiv 0 \pmod{s}$ is $N(\alpha,b,s)=N(\alpha,b,p)N(\alpha,b,q)$. Thus, using $q/2<p<q$, we have

$$\begin{aligned}N(\alpha,b,s)<&(pq)^{m-1}+(pq)^{m-1}\left(\frac{C_1}{p^{1/2}}+\frac{C_1}{q^{1/2}}\right)+(pq)^{m-1}\frac{C_1^2}{(pq)^{1/2}}\\ <&(pq)^{m-1}+(pq)^{m-1}\frac{C_2}{(pq)^{1/4}}<s^{m-1}+C_2s^{m-1-1/4}.\end{aligned}$$

The inequality

$$N(\alpha,b,s)>s^{m-1}-C_3s^{m-1-1/4}$$

follows similarly.

Now suppose that $\gcd(b,s)\neq 1$. If $\gcd(b,p)\neq 1$ then $\mathcal{I}_\alpha(X_1,\dots,X_m)\equiv 0 \pmod{p}$, and since $\mathcal{I}_\alpha$ factorises into linear factors, all solutions of this congruence are contained in the union of at most $n(n-1)/2$ linear subspaces of $\mathbb{Z}_p^m$ of dimension $m-1$. Thus $N(\alpha,b,p)<\frac{n(n-1)}{2}p^{m-1}$. If $\gcd(b,p)=1$ then by (4.7) we have $N(\alpha,b,p)<C_4p^{m-1}$. Similar reasoning is true for $N(\alpha,b,q)$. Thus we have

$$N(\alpha,b,s)<c_2(\alpha)s^{m-1} \tag{4.9}$$

for any b. This concludes the proof of Theorem 3.1

□

Proof of Theorem 3.2. Since we have $P_{coll}:=\frac{N(\alpha,b,s)}{s^m}$ Theorem 3.2 is a simple consequence of Theorem 3.1. □

5. Complexity of computing the value of an index form

Let K be again an algebraic number field of degree $n\geq 3$ with discriminant D_K and α a primitive integral element of K. Consider the index form $\mathcal{I}_\alpha(\mathbf{X})$ defined in (2.1). Since

$$D_{K/\mathbb{Q}}(l(\mathbf{X}))=(\mathcal{I}_\alpha(\mathbf{X}))^2D_K,$$

in order to calculate the value of $\mathcal{I}_\alpha(\mathbf{X})$ at a point $\mathbf{x} = (x_2, \ldots, x_n)$, we only have to compute the discriminant of the element

$$\beta := x_2\alpha + x_3\alpha^2 + \cdots + x_n\alpha^{n-1},$$

divide it by D_K and take square root of the result. Clearly, D_K can be computed as a pre-computation. Thus the complexity of computing the value $\mathcal{I}_\alpha(\mathbf{x})$ will be essentially the same as computing the discriminant of the corresponding element $\beta = l(\mathbf{x})$.

Let T be the ordinary hight of the minimal polynomial of α and $A := \max_{2\le i\le n}\{|x_i|\}$.

Clearly, $D_{K/\mathbb{Q}}(\beta) = D(C_\beta(X))$, where $C_\beta(X)$ is the characteristic polynomial of β. Further, let M_β be the matrix representation of β, i.e. the matrix of the linear map which is defined by the multiplication by β in the $\mathbb{Q}$-vector space $\mathbb{Q}(\alpha)$. Then $C_\beta(X)$ is the characteristic polynomial of the matrix M_β.

First we would like to estimate the time of computation of the matrix M_β. Using the Newton formulae (see Ch. 4.2.2 [4]) we can determine the canonical representation of the values α^{n+i} for $i = 1, \ldots, n-1$. This will take $O(n^2)$ operations (see the proof of Theorem 3 [1]). The entries of the matrix M_β will be bounded by $B = AT^n$. So for the computation of the characteristic polynomial of M_β (using Algorithm 2.2.7 [4]) we need n^4 multiplications. Since the coefficients of $C_\beta(X)$ are bounded by $2^n \cdot n^n \cdot B^n$ (see Proposition 2.2.10 [4]) we can use modular arithmetic with the modulus $M = 2^n \cdot n^n \cdot B^n$ and we get the time estimate $O(n^4 \log^2 M)$ for the calculation of $C_\beta(X)$. This means in fact that we are done in $O\left(n^4(n\log 2 + n\log n + n\log(AT^n))^2\right) = O(n^8 + n^7 \log A + n^6 \log^2 A)$ operations.

Now we only have to calculate the discriminant of $C_\beta(X)$ using the subresultant algorithm, which has complexity $O(n^4 \log^2(nN))$ (see p. 119 [4]), where N is the bound on the coefficients of $C_\beta(X)$ and $C'_\beta(X)$, i.e. $N \le nM$. Thus the complexity will be $O(n^4 \log^2(n^2 M)) = O(n^4 \log^2(2^n n^{n+2} A^n T^{n^2})) = O(n^4(n^2 + n\log A)^2) = O(n^8 + n^7 \log A + n^6 \log^2 A)$. This means that the overall complexity of computing the value $I(\alpha)$ is also $O(n^8 + n^7 \log A + n^6 \log^2 A)$.

6. An application

In the previous sections we have investigated important properties of the function $\mathcal{I}_{\alpha,s}$. Since pseudo-random functions can also be constructed using the one-way function $\mathcal{I}_{\alpha,s}$ in this section we will suggest the use of a hash function based on such index forms.

The first question to be analyzed is how to choose α in order to guarantee the security of our hash function. The methods developed for the solution of "arbitrary" index form equations at the recent moment make it possible to solve index form equations where α has degree at most 6. For results concerning the general cubic case see [9], for the quartic case [8] and for the quintic case [7]. A long computation of about one month on a computer with six parallel processors of 1GH under linux made possible for Bilu, Gaál and Győry to solve an index form equation over a sextic field with Galois group S_6 (see [3]). Further, there are algorithms for solving index form equations also when α has degree ≥ 6 in the case when the field $K := \mathbb{Q}(\alpha)$ has proper subfields, or when the Galois group of K is cyclic. For a broad survey of these kind of results and also for the description of the algorithms which make possible to solve index form equations see the book of Gaál [6] and the references given there.

The above facts show that we shall choose our α such that $K := \mathbb{Q}(\alpha)$ is a totally real primitive extension of $\mathbb{Q}$ of degree at least 7. Further, we have to ensure that $\gcd(\frac{n(n-1)}{2}, \varphi(s)) = 1$, so we have to avoid the degrees $8, 9$.

An α fulfilling all our requirements is for instance any root of the polynomial

$$x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1. \tag{6.10}$$

(see [15]).

Now, concerning the choice of $s = pq$, with p, q primes we have to be aware of the following. First of all s has to be about the size of 1024 bits, and it has to resist any attempt to factorization, otherwise we cannot guarantee the collision resistance of our hash function. Thus, choose the prime q of size about 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 $\gcd(\frac{n(n-1)}{2}, \varphi(s)) = 1$, i.e. $\gcd(21, \varphi(s)) = 1$.

Now we define our hash function in the following way. Let s be chosen in the above way and let α be a root of the polynomial (6.10). Define $\mathcal{I}_{\alpha,s}(x_1,\dots,x_6)$ by (3.3). Since the largest prime divisor of the non-zero discriminant the corresponding polynomial $I_\alpha(x_1,x_2,0,\dots,0)$ is less then 2^{70}, thus by the choice of p and q, the statements of Theorem 3.1 and 3.2 are true for $\mathcal{I}_{\alpha,s}$.

The value of our hash function on a binary string $x=(x_1,\dots,x_6)$ of bit-length $6\cdot 1024$ (x_i being of bit-length 1024) is defined by

$$h(x) := (\mathcal{I}_{\alpha,s}(x_1,\dots,x_6) \bmod pq) \bmod 1024.$$

If the bit-length of our binary string is not $6\cdot 1024$ bit, then we complete x to a binary string of length $6\cdot k\cdot 1024$, where k is the least integer such that $6\cdot k\cdot 1024$ is larger then the length of x. This is done by copying so many bits from the beginning of the string to the end of it that are needed to get a binary string of bit-length $6\cdot k\cdot 1024$. Then for each block of length $6\cdot 1024$ we apply the function h, and then we consider the output as a new input string. We continue this iteration until the output has bit-length 1024.

This function will keep collision free in all the steps of the iteration. Further, we have experimentally investigated the avalanche effect of the above hash function. We generated 100 random sequences of bits and changed 10 times consecutively one randomly chosen bit of each one. Then we counted the number of changes of the bits of the output. The results can be summarized as follows. The average of the number of the changed bits was 511.556. The least number of changed bits was 468, while the largest number of changed bits was 554. We have tested t he normality of the distribution of the above sample. We used a Kolmogorov-Smirnov test, and we find that the null hypothesis stating that the distribution of the sample can be accepted at the significance level of 6,6

The above facts mean that the hash function suggested by us based on index forms, which is proven to be collision resistant, is also promising from the point of view of the avalanche effect. These properties guarantee its security.

Acknowledgements. The research was supported in part by the National Office for Research and Technology. The authors are grateful to the referee for his useful and helpful remarks.

The authors are grateful for Professor Attila Pethő for his useful remarks.

References

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

[2] A. Bérczes, J. Ködmön and A. Pethő, A one-way function based on norm form equations, *Period. Math. Hungar.*, **49** (2004), 1–13.

[3] Y. Bilu, I. Gaál and K. Győry, Index form equations in sextic fields: a hard computation, *Acta Arith.*, **115** (2004), 85–96.

[4] H. Cohen, *A course in computational algebraic number theory*, vol. 138 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin, 1993.

[5] H. Feistel, W. A. Notz and J. L. Smith, Some cryptographic techniques for machine-to-machine data communications, in: *Proceedings of the IEEE*, 1975, vol. 63, pp. 1545–1554.

[6] I. Gaál, *Diophantine equations and power integral bases*, Birkhäuser Boston Inc., Boston, MA, 2002, new computational methods.

[7] I. Gaál and K. Győry, Index form equations in quintic fields, *Acta Arith.*, **89** (1999), 379–396.

[8] I. Gaál, A. Pethő and M. Pohst, Simultaneous representation of integers by a pair of ternary quadratic forms—with an application to index form equations in quartic number fields, *J. Number Theory*, **57** (1996), 90–104.

[9] I. Gaál and N. Schulte, Computing all power integral bases of cubic fields, *Math. Comp.*, **53** (1989), 689–696.

[10] S. Goldwasser and M. Bellare, Lecture Notes on Cryptography, MIT Press, 2001.

[11] S. Goldwasser and S. Micali, Probabilistic encryption, *J. Comput. System Sci.*, **28** (1984), 270–299.

[12] J. B. Kam and G. I. Davida, Structured design of substitution-permutation encryption networks, *IEEE Trans. Comput.*, **28** (1979), 747–753.

[13] S. Lang and A. Weil, Number of points of varieties in finite fields, *Amer. J. Math.*, **76** (1954), 819–827.

[14] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1997.

[15] M. Pohst, Invarianten des total reellen Körpers seibten Grades mit Minimaldiskriminante, *Acta Arith.*, **30** (1976), 199–207.

[16] B. Schneier, *Applied cryptography. Protocols, algorithms and source code in C. 2nd ed.*, John Wiley & Sons, 1996.

[17] A. Webster and S. Tavares, On the design of S-boxes, in: *Advances in Cryptology-CRYPTO'85 (LNCS 218)*, 1986, pp. 523–534.

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

I. Járási
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: ijarasi@math.klte.hu