6th International Conference on Applied Informatics
Eger, Hungary, January 27–31, 2004.

Some Applications of a One-Way Function Based on Norm Form Equation

Zoltán Csajbók, József Ködmön

Faculty of Health College, University of Debrecen
csajzo@de-efk.hu
kodmonj@de-efk.hu

Abstract

Recently a new one-way function with collision resistance and avalanche effect has been proposed by A. Bérczes, J. Ködmön, and A. Pethő in [2], whose security is based on the difficulty of solving a norm form equations. As an application to this function, they also have proposed a construction of a one-way hash function. In this paper we will present this hash function in more details, and show how to construct and use it in the practice using Maple programs.

Mathemtics Subject Classification: 94A60, 11Y40, 11Y16

Keywords and phrases: hash function, one-way function, norm form equation

1. One-way hash functions

Hash functions are used in many contexts, and they are also fundamental to cryptography. There is an extensive literature on the hash functions and their applications, e.g. [7], [8], [10], and [3].

Definition 1.1. A hash function is a function h which has, as a minimum, the following two properties

1) compression h maps an input x of arbitrary finite bitlength (called a preimage) to an output of fixed bitlength (called a hash value or simply hash);

2) ease of computation given h and an input x, it is easy to compute $h(x)$.

Cryptographic hash functions, however, must have some additional properties that guarantee their security such as *preimage resistance*, *2nd-preimage resistance*, and *collision resistance*. A *one-way hash function* is a hash function which is

preimage resistant and 2nd-preimage resistant. A *collision resistant hash function* is a hash function which is 2nd-preimage resistant and collision resistant.

A function f has a *strict avalanche effect* when a change in one bit of the input results in a change of half of the output bits.

A one-way function is function f such that for each input x, it is easy to compute $f(x)$, but for essentially all outputs y, it is computationally infeasible to find any input x such that $f(x) = y$.

For the precise mathematical definitions of the above concepts see [2], [6], and [7].

Although widely believed that one-way functions exist, but yet there is no known function which is provably one-way (with no assumptions). These functions should thus properly be qualified as "conjectured" or "candidate" one-way functions. Nevertheless, in the one-way function literature they are widely used the term "one-way function" instead of "conjectured" or "candidate one-way function", as we also will do it in the followings.

2. A new hash function based on norm forms

Let $P(X) \in \mathbb{Z}[X]$ be a fixed monic polynomial of degree $n \geq 3$ having no multiple roots.

Denote by $\alpha_1, \ldots, \alpha_n (\in \mathbb{C})$ the roots of P, let $n \geq m \geq 3$ be a positive integer, and put

$$L^{(i)}(\mathbf{X}) = \sum_{j=1}^{m} \alpha_i^{j-1} X_j \quad \text{for} \quad i = 1, \ldots, n.$$

Define the norm form corresponding to the polynomial P by

$$\mathcal{N}_P(\mathbf{X}) := \prod_{i=1}^{n} L^{(i)}(\mathbf{X}) = \prod_{i=1}^{n} (\alpha_i^0 X_1 + \alpha_i^1 X_2 + \alpha_i^2 X_3 + \cdots + \alpha_i^{m-1} X_m).$$

$\mathcal{N}_P(\mathbf{X})$ is a homogeneous polynomial of degree n in the indeterminantes $X_1, \ldots, X_m$ with integer coefficients [1].

Remark 2.1. In fact, $\mathcal{N}_P(\mathbf{X})$ is a generalization of the concept of *norm form*, and it is a special *decomposable form*.

The

$$\mathcal{N}_P(x_1, \ldots, x_m) = b$$

equation is a *norm form equation*, where $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and $b \in \mathbb{Z}$.

From the cryptographic point of view it is more convenient to work over finite domains.

3. Construction of the one-way function $\mathcal{N}_{P,s}$

Let p and q be primes such that $q > p > q/2$ and $s := pq$. Suppose that $\gcd(m, \varphi(s)) = 1$ (where φ is the Euler's φ-function). For $s \in \mathbb{Z}$ let $\mathbb{Z}_s := \mathbb{Z}/s\mathbb{Z}$.

Define the mapping $\mathcal{N}_{P,s} : \mathbb{Z}_s^m \to \mathbb{Z}_s$ in the following way:

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

Question: Is $\mathcal{N}_{P,s}(\mathbf{X})$ a one-way function?

Answer A) Calculation of values $\mathcal{N}_{P,s}(\mathbf{x})$ is "easy"

The best method to compute values of $\mathcal{N}_{P,s}(\mathbf{X})$ at point $\mathbf{x} \in \mathbb{Z}^m$ uses *the matrix representation of $\mathcal{N}_{P,s}(\boldsymbol{X})$ with modular arithmetic.*

In [2] A. Bérczes, J. Ködmön and A. Pethő proved that the computing the values of the function $\mathcal{N}_{P,s}(\mathbf{X})$ is "easy":

Theorem 3.1. *The complexity of the computation of $\mathcal{N}_{P,s}(\boldsymbol{x})$, using the best algorithm is $O(n^5 \log^2 s)$, where the constants in O depends only on $P(X)$.*

Answer B) Inverting the function $\mathcal{N}_{P,s}(\mathbf{x})$ is "hard"

Several facts emphasize that in general a norm form equation is "hard" to solve:

- There is not known algorithm which solves all norm form equations.
- We conjecture that the Cerlienco-Mignotte-Piras conjecture concerning linear recurrence sequences implies that the solvability of decomposable form equations is algorithmically not decidable [4].
- A complexity analysis of N.P. Smart [9] shows that the best known algorithm for solution of Thue equations is exponential.

However, there are the wide classes of norm form equations which can be solved using an algorithm of Gaál [5] which combines powerful theorems of Győry with constructive methods.

So far, there is not actually known any algorithm for determining all solutions of general norm form equations, i.e. for inverting the function $\mathcal{N}_{P,s}$. This fact is represented by the following condition:

Definition 3.1. Strong Modular Norm form Assumption(SMNA): For every polynomial Q and every PPT algorithm $\mathcal{A}$, for all sufficiently large s

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

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

Based on the Answer A) and Answer B) we can deduce the following theorem:

Theorem 3.2. *Under SMNA the function $\mathcal{N}_{P,s}$ is a one-way function.*

4. The properties of the one-way function $\mathcal{N}_{P,s}$

4.1. $\mathcal{N}_{P,s}$ is collision resistant

Denote P_{coll} the probability of the collision for the function $\mathcal{N}_{P,s}$:

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

A remarkable result which also has been proved in [2] by A. Bérczes, J. Ködmön and A. Pethő is the following theorem:

Theorem 4.1. *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.

The function $\mathcal{N}_{P,s}(\boldsymbol{x})$ is collision resistant of level 1.

4.2. $\mathcal{N}_{P,s}$ has strict avalanche effect

We tested that *the function $\mathcal{N}_{P,s}$ has* **strict avalanche effect**, *i.e. whenever one input bit of $\mathcal{N}_{P,s}$ is changed, half of output bits must change in average.*

5. How to choose $P(X)$ such that the associated norm form could be easily calculated?

Let $P(X) := X^n - 1$ with $n \geq m \geq 3$. Denote $\zeta_1, \zeta_2, \ldots, \zeta_n (\in \mathbb{C})$ the n different roots of $P(X)$, where $\zeta_1, \zeta_2, \ldots, \zeta_n$ are the n^{th} roots of unity.

If $n > m$ then let $(X_1, X_2, \ldots, X_n) = (X_1, X_2, \ldots, X_m, \underbrace{0, \ldots, 0}_{m-n})$. Then

$$\mathcal{N}_P(\mathbf{X}) \quad = \quad \prod_{i=1}^{n} L^{(i)}(\mathbf{X}) = \prod_{i=1}^{n} (X_1 + \zeta_i X_2 + \cdots + \zeta_i^{n-1} X_n).$$

$\mathcal{N}_P(\mathbf{X})$ is the determinant of the following matrix which has a particular simple form, and called *cyclic matrix* [11]:

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

So, we can define the function $\mathcal{N}_{P,s}$ as follows:

$$\mathcal{N}_{P,s} : \mathbb{Z}_s^n \to \mathbb{Z}_s,\ (x_1, ..., x_n) \mapsto \begin{vmatrix} x_1 & x_2 & \dots & x_n \\ x_n & x_1 & \dots & x_{n-1} \\ \dots & \dots & \dots & \dots \\ x_2 & x_3 & \dots & x_1 \end{vmatrix} \mod s$$

We propose to apply $\mathcal{N}_{P,s}(\mathbf{X})$ as a one-way hash function.

6. The main steps of constructing our hash function

In the practice modular hash functions map messages to 1024 bit words. Hence $s = pq$ should be about of this size.

1. System setup and constant definitions Choose

- n with conditions $n \geq 3$;
- m with $n \geq m \geq 3$;
- the module $s := pq$ of bitlength 1024, p and q secret primes.
  First choose the prime q of size 2^{512} and then the prime p with conditions $q > p > q/2$ and $\gcd(m, (p-1)(q-1)) = 1$.
  Fix the module $s := pq$ and destroy the primes p and q.

2. Blocking Split the message M into subwords $x_1, \dots, x_k$ such that each x_i, $i = 1, \dots, k$ represent an integer in the interval $[1, s-1]$.

3. Padding Extend the function $\mathcal{N}_{P,s}(\mathbf{X})$ in the following way:

$$h(x_1, \dots, x_n) := \mathcal{N}_{P,s}(x_1, \dots, x_n)$$

and we define recursively:

- Case 1: there is exists $t \geq 0 \in \mathbb{Z}$ that $k = n + t(n-1)$. Then

$$h(x_1, \dots, x_{n+l(n-1)}) :=$$

$$\mathcal{N}_{P,s}(h(x_1, \dots, x_{n+(l-1)(n-1)}), x_{n+(l-1)(n-1)+1}, \dots, x_{n+l(n-1)}),$$

where $l = 1, \dots, t$.

- Case 2: if k is not of the form $n + t(n-1)$ with some suitable $t \geq 0 \in \mathbb{Z}$ then we can extend M with words representing 0 until k has the required form.

4. Calculation Calculate the hash value $h(x_1, \dots, x_k) \in \mathbb{Z}$.

6.1. Calculating the hash value $\mathcal{N}_{P,s}(\mathbf{x})$

Let $n = 4 > m = 3 \geq 3$, $k = 3$, and $P(X) = X^4 - 1$ be a polynomial due to our proposal, i.e

$$\mathcal{N}_P(\mathbf{X}) = \prod_{i=1}^{4} L^{(i)}(\mathbf{X}) = \begin{vmatrix} X_1 & X_2 & X_3 & 0 \\ 0 & X_1 & X_2 & X_3 \\ X_3 & 0 & X_1 & X_2 \\ X_2 & X_3 & 0 & X_1 \end{vmatrix}.$$

Let

$q :=$ 2681561585988519419914804999641169225495873164118478675544712288744352806014709395360374859633380685538006371637297210170750776562389313989286729801216835 1

$p :=$ 1340780792994259709957402499820584612747936582059239337772356144372176403007354697680187429816690342769003185818648605085375388281194656994643364900608424 1

and

$s :=$ 3595386269724631815458610381578049467235953957884613145468601623154653516110019262654169546448150720422402277597427867153175795376288332449856948612789542688612963310758286792898286336274034264741596118887966094167645324367344287855404102626415314139657338456734983287167278273703419966195766613676526180056591

Bitlength of s : 1024 bit (number of decimally digits: 309).

$\gcd(3, (p-1)(q-1)) = 1$

$M :=$ $ICAI2004EgerHungaryJanuaryfrom27to31$ $6thInternationalConferenceonAppliedInformatics$ $TheUniversityofDebrecenandtheEszterhazyKaroly$ $CollegeCallforpapersandparticipationTheConferen$ $ceisorientedtowardstrictlyprofessionalexchangeofi$ $deasinthefieldofAppliedInformaticsThescopeofthe$ $Conferenceistoprovideaforumforthediscussionof$ $academicresearchesWearesurethattheplaceofthe$ $conferencehasbeenchosen$

$x_1 :=$ 1252514080749714366361233983481480454991105402878877781214281614141865599143604710194149825929159408659772404089680835693945547064355637135322607081184665292105143179642455126546203197734671645691539775986511962455208901167182287007227289343135507924943070786609196871

$x_2 :=$ 3822505752215754591460071324617952329911537222227265819850839610241464844399021378133261054824643971

435202576109641025874441265748374118557208448790539 52
269507215619587179407295065432606928391930199548505 82
027566535281191395806250849207250335775097799353047 23
70960720114

$x_3 :=$ 320014719163857297145434099318964989909359455 2
636324034558865479797318984267442710854781830200355 5
192774048197631105674029291482285863718701347266466 5
132126781582629563195477878472308279540753946640914 3
115510007324676573063865668535888226741943838450543 1
645936672051

The corresponding bitlengths: 3056 (128+128+126 byte) of M; 887 (128 byte) ofx_1; 896 (128 byte) of x_2; 882 (126 byte) of x_3.

These bitlengths will be shorter by concatenation: 128 byte $\leq$ 1024 bit.

The hash value of M:

$$h(M) = \mathcal{N}_{P,s}(x_1, x_2, x_3) = \begin{vmatrix} x_1 & x_2 & x_3 & 0 \\ 0 & x_1 & x_2 & x_3 \\ x_3 & 0 & x_1 & x_2 \\ x_2 & x_3 & 0 & x_1 \end{vmatrix} \bmod s =$$

$=$ 780757540922665452223440
742208813577518752206899057830801154054168486170 7
351570355085475480223768346292662068977052601660 3
988955773623619905976778449412687731277384783217 2
845579291399206582112711063447132379831934098378 9
396824023336631569781961245574592187006693924230 6
750692501312294368509118232924590925851

Bitlength of $h(M)$: 1023 bit. Number of decimally digits of $h(M)$: 308.

Let $M1 := HCAI2004EgerHungary...$ (one bit changed)

Relative Hamming-distance: $\frac{\varrho(h(M),h(M1))}{l(M)} = 0.4926686217$

6.2. Passphrase-checking

$n := 4$, $m := 3$, $s := pq$ (s stored and primes p, q destroyed), bitlength of s is 1024; fix cyclic matrix with entries $X_1, X_2, X_3, 0$.

Login Name	**Hash Value**	**Salt**
Alice	$h(PPH_1)$	ST_1
Bob	$h(PPH_2)$	ST_2
...	...	...

$ST_i := RS_{i,1} + RS_{i,2}$, where $RS_{i,j}$ random string with length 64 byte.

$PPH_i := PPH_{i,1} + PPH_{i,2}$ is passphrase of users (minimum 2 x 10 byte)

$h(PPH_i) := \mathcal{N}_{P,s}(PPH_{i,1} + RS_{i,1}, PPH_{i,2} + RS_{i,2}, ST_i)$

Here length of x_1, x_2 are at least 74 byte and x_3 is 128 byte.

The system accepts of Alice's passphrase if $h(PPH_A) = h(PPH_1)$, where PPH_A is Alice's present passphrase and $h(PPH_1)$ is Alice's stored hash value.

6.3. Passphrase-checking (concrete calculation)

Passphrase (without space):

$PPH := Thisone - wayfunctionseemssecurebeca$
$useithasstrictavalancheeffect$ (length 32 byte)

Salt (random string with length 128 byte)

```
ST:=M\\k\\C[oFsY]mUFdDtCi[irDLZpPmkBRudgOVO
QFtcc‘‘ulaOaqZIo^T^muqvRLYHsOwYdm_nSUSuAgRH
\\[kumHhSpvRF^PgEtwQWEsoSrntUuaxPVvSV_NwuC]
t_iDefH
```

$h(PPH) =$ 87784731131987101605117356608421805
37831916616696065189686983044576617751152217274
75991156745758734372389268385949029056430476502
15839471521330280039184034790013361517341642781
43156400044775696914781200053245205163438708060
36711010951995519659955155583830038366487222497
09294824469772766138668988456262094619

Let $PPH1 := Uhisone - wayfunction...$ (one bit changed)

Relative Hamming-distance: $\frac{\varrho(h(PPH),h(PPH1))}{l(PPH)} = 0.4946236559$

This construction seems secure because the one-way hash function $\mathcal{N}_{P,s}(\underline{X})$ has **strict avalanche effect** i.e. if whenever one input bit is changed, every output bit must change with probability 1/2.

References

[1] A. Bérczes, J. Ködmön, *Methods for the Calculation of Values of a Norm Form*, Publicationes Mathematicae Debrecen **63**/**4** (2003), 751-768.

[2] A. Bérczes, J. Ködmön, A. Pethő, *A one-way function based on norm form equations*, to appear in Periodica Math. Hungar.

[3] J. A. Buchmann, *Introduction to Cryptography*, Springer-Verlag, 2000.

[4] L. Cerlienco, M. Mignotte, F. Piras, *Suites r écurrentes linéaires. Propriétés algébriques et arithmétiques. (Linear recurrence sequences. Algebaric and arithmetic properties* , L'Euseign. Math. 33 (1987), 425-436.

[5] I. Gaál, *Computing power integral bases in algebraic number fields, In: Number theory: Diophantine, computational and algebraic aspects (ed. by K. Győry, A. Pethő and V.T. Sós)*, 243-254, Walter de Gruyter, Berlin 1998.

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

[7] A. J. Menezes, P. C. van Oorschot, S. Vanstone, *Hadbook of Applied Cryptography*, CRC Press, 1997.

[8] B. Schneier, *Applied Cryptography, Second Edition. Prorocols, Algorithms, and Source Code in C*, John Wiley & Sons, 1996.

[9] N. P. Smart, *How Difficult is it to Solve a Thue Equation?* In ANTS-2, LNCS **1122**, 363-373, 1996.

[10] D. R. Stinson, *Cryptography. Theory and Practice*, CRC Press, 1995.

[11] T. Szele, *Bevezetés az algebrába.* Tankönyvkiadó, Budapest, 1972.

Postal addresses

Zoltán Csajbók
Faculty of Health College
University of Debrecen
H-4400 Nyíregyháza, Sóstói u. 2-4.,
Hungary

József Ködmön
Faculty of Health College
University of Debrecen
H-4400 Nyíregyháza, Sóstói 2-4.,
Hungary