



R-prime Numbers of Degree k^*

Abdelhakim Chillali

ABSTRACT: In computer science, a one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here, "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way (see Theoretical Definition hereinafter). A twin prime is a prime number that has a prime gap of two, in other words, differs from another prime number by two, for example the twin prime pair (5, 3). The question of whether there exist infinitely many twin primes has been one of the great open questions in number theory for many years. This is the content of the twin prime conjecture, which states: There are infinitely many primes p such that $p + 2$ is also prime. In this work we define a new notion: " r -prime number of degree k " and we give a new RSA trap-door one-way. This notion generalized a twin prime numbers because the twin prime numbers are 2-prime numbers of degree 1.

Key Words: RSA, Prime Number, One-Way function, Cryptography.

Contents

1 Introduction	75
2 The R-prime numbers	76
3 Results and discussion	77
4 New RSA attack	78

1. Introduction

A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here, "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way (see Theoretical Definition, below), [6, 7].

Definition 1.1. *A one-way function f is a function that is easy to compute but computationally hard to reverse.*

1. Easy to calculate $f(x)$ from x
2. Hard to invert, to calculate x from $f(x)$

* USMBA, LSI, FP, Taza, Morocco

2010 *Mathematics Subject Classification*: 11T71, 14G50, 94A60.

Submitted July 15, 2017. Published June 14, 2017

Definition 1.2. A trapdoor one-way function is a one-way function with an additional requirement. Informally, a one-way function might be described as a function for which evaluation in one direction is straightforward, while computation in the reverse direction is far more difficult. Such a function becomes a trapdoor one-way function when one adds the requirement that computation in the reverse direction becomes straightforward when some additional (trapdoor) information is revealed.

Remark 1.3. $f : D \rightarrow R$ is a trapdoor one way function if there is a trapdoor s such that:

1. Without knowledge of s , the function f is a one way function
2. Given s , inverting f is easy.

2. The R-prime numbers

A twin prime is a prime number that has a prime gap of two, in other words, differs from another prime number by two, for example the twin prime pair (41, 43). The question of whether there exist infinitely many twins primes has been one of the great open questions in number theory for many years. This is the content of the twin prime conjecture, which states: There are infinitely many primes p such that $p + 2$ is also prime. In 1849 de polygonal made the more general conjecture that for every natural number k , there are infinitely many prime pairs p and p' such that $p' - p = 2k$. The case $k = 1$ is the twin prime conjecture. Cousin prime numbers are prime numbers that differ by four.

Lemma 2.1. Let p and q are two odd prime numbers, such that $p < q$. Then there exists a number $s \in \mathbb{N}$ such that $q - p = 2s$.

Proof: As a prime p and q are odd, then $q - p$ is an even number. □

Remark 2.2. If $N = pq$ is an RSA number. Then there exists a number $s \in \mathbb{N}$ such that $N = p(p + 2s)$, we have:

$$p = \sqrt{(N + s^2) - s}$$

and

$$q = \sqrt{(N + s^2) + s}$$

Definition 2.3. Let r is a prime number. Two numbers prime p and q , such that $p < q$ are r -prime numbers, if there exists a number $k \in \mathbb{N}$ such that $q - p = 2r^k$. The prime number p is said, in this case, r -prime number of degree k .

Remark 2.4. 1. The twin prime numbers are 2-prime numbers of degree 1.

2. The cousin prime numbers are 2-prime numbers of degree 2.

3. Results and discussion

Let $n \in \mathbb{N}$ and r a prime integer. Let $a_n^{(r)}$ is the number of primes in the set $[[r^n, r^{n+1}]]$, $b_n^{(r)}$ is the number of r -prime numbers of degree k in the set $[[r^n, r^{n+1}]]$ and $c_n^{(r)} = \frac{b_n^{(r)}}{a_n^{(r)}}$.

We consider the following sequences $(a_n^{(r)})_{n \in \mathbb{N}}$, $(b_n^{(r)})_{n \in \mathbb{N}}$ and $(c_n^{(r)})_{n \in \mathbb{N}}$. Where $k = 0$ and $r = 2$, we have the first 21 values of these sequences grouped in the following table:

Table 1: THE FIRST 21 VALUES OF THE SEQUENCES

n	$a_n^{(r)}$	$b_n^{(r)}$	$c_n^{(r)}$
0	1	0	0
1	2	1	0,5
2	2	1	0,5
3	2	0	0
4	5	1	0,2
5	7	2	0,2857142857142860
6	13	5	0,3846153846153850
7	23	4	0,1739130434782610
8	43	8	0,1860465116279070
9	75	14	0,18666666666666670
10	137	28	0,2043795620437960
11	255	41	0,1607843137254900
12	464	72	0,1551724137931030
13	872	122	0,1399082568807340
14	1612	228	0,1414392059553350
15	3030	362	0,1194719471947190
16	5709	656	0,1149062883166930
17	10749	1187	0,1104288771048470
18	20390	2087	0,1023540951446790
19	38635	3776	0,0977352141840300
20	73586	6812	0,0925719566221836

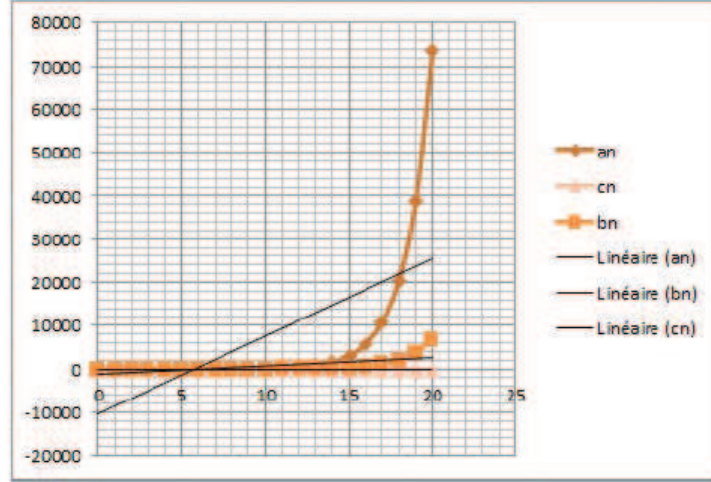


Figure 1: The graphical representation of the sequences

Conjecture:

Let r be a nonzero integer number. There are infinite r -prime of degree k .
The sequence $(c_n^{(r)})_{n \in \mathbb{N}}$ converges to 0.

4. New RSA attack

In this section we assume that $N = p(p + 2r^k)$, is an RSA number, where p is r -prime number of degree k . We have, (see Remark 2.2):

$$p = \sqrt{(N + r^{2k}) - r^k}$$

RSA Algorithm: (see [1], [2])

1. Bob chooses p , secret r -prime number of degree k , and sets that $N = p(p + 2r^k)$
2. Bob chooses e with $\gcd(e, \phi(N)) = 1$
3. Bob computes d so that $de = 1 \pmod{\phi(N)}$
4. Bob makes N and e public but keeps p, r, k and d secret
5. Alice encrypts m as $c = m^e \pmod{N}$
6. Bob decrypts c as $m = c^d \pmod{N}$

Chillali Attack:

1. Chillali knows that $p = \sqrt{(N + r^{2k}) - r^k}$, he takes N
2. Calculate with Maple:


```

> n := length(convert(N, binary));
for k from 1 to n do
  if (isprime(sqrt(N + r^(2 * k)) - r^k) = true) then Return([k, sqrt(N + r^(2 * k)) -
    r^k, sqrt(N + r^(2 * k)) + r^k])
  else end if;
end do;
      
```

Finally, Chillali calculate p and $q = p + 2r^k$, after that factorize N .

Example: N:=231050157050211693511442883590272793692823342220378050683
 69184013602091563871138235678867947944083169451792431476929041560652772
 47629000001688200665366006126547704450909752445235424454270043561406355
 45753140946219708965818306866514888719957661965405851024491978519747462
 89311761704392108467278159097880556535254176253894918316061865675653026
 09395548314272614438073332602941867076943075860873447304529609874560137
 57843061591115121595618678481036468578754127802736900994003492889297848
 26707805575901209801574136266012471647659311504304475511529833656967203
 88212474437558047923651526803288274197476734709278639566434182849560033
 07926267513048197531152196902817891598320803667831557662808965419770497
 13144212497330207468670215447192208209295099046735385799602958377024507
 40924668594109950540607709194449721253948881610539655118578099642226407
 27085239318417494857207610120397660280877656392004458132548781300062350
 08190819146798730521855771107862733447064168353600013738065442207368666
 97893870000303656801853743691684751394401424575504470497533620522381258
 81574145943355596488198911362938663877398327892615465227175516620242370
 18504184541387632511891585502575927699549113199077552297940101855689274
 11774220699743869415856293813933733201943967049676734793814210906360031
 15661231900502344995308154989802245768768522811186751561992977314442317
 83537123268919152597466963910301009572626572234154572284489734855246302
 57308086133483541660308753416229307708587311346451027770820896525763754
 65396458525284055734496065656351861782535579454684465322799054384243373
 77689035595525871196359634779023066660545089421338683918411759063105692
 97684515397794748485029085348783413039486936987679550121423453363688354
 36369229270292900712866175334123643837735493751019128184486369991141635
 60739851665791738790155932665526776228632148601429208366710548876116592
 83266441854431456841810247559463812590173075713011443968356032997885082
 28541419118146048063764600760093135129042914840583176328719412281152369
 89721210162843531576964089925867361332192877107048896703135024419322206
 20410630352980446326230908415581876479192688172638225756038559468327391
 04015013152015747568982806330549254309556441490703198427725521443659631
 64177741517576482245257348649796699104895786560188192257402380454372534
 83841576510168302088081314513638707766296789901030339211938239440116889
 81577132999451898260552681471669107912266884782939665820674197034855129
 21684376520043791321730578268474930861222410500438244177732415865420961

42545008362692644603319019822350057408247949948178033155734213742694604
 64683129585171581552542234865987608871199079412384256552908397685702979
 22041596224541874514397435783611066323734003448300258673551201248275950
 20710360022446683113131806169483371526741281720911526354654806876601646
 88248156915664213123858997965815068095425233075877617726803742635717625
 07159628529747347251413158307289338011987404435024741362131016095680669
 07615343746051283727645706670045385354373738064205590434595173445877051
 34528581605348270829397366336756125838019035939179671758414901218987995
 87071931336041936682752284045334186639120873647553637002540518051734196
 93326749559050205367382988606045857619643573299938466447955392471483265
 95284667753546009598754789720143821641755006445897246304310495086049810
 31772852762360022422195649470208324644395676231701237807779388978343161
 44456252295923758436591945974586378826106762195428797200286806944150816
 40915223256053884861125327221746007682648938345006209114894195028685586
 40368599632233170253974032281689273785347114135137924970075797157453139
 01491144418647705957576874486830114146340571230690197310970369185189618
 31741642143412124020201290224363093409901847631917823468792306821721320
 87221782111843278544783174227538657131087505793176001.

p:=1044388814131525066917527107166243825799642490473837803842334832
 83953907971557456848826811934997558340890106714439262837987573438185793
 60726323608785136527794595697654370999834036159013438371831442807001185
 59462263763188393977127456723346843445866174968079087058037040712840487
 40118609114467977783598029006686938976881787785946905630190260940599579
 45343282346930302669644305902501597239986771421554169383555988529148631
 82379144344967340878118726394964751001890413490084170616750936683338505
 51032972088269550769983616369411933015213796825837188091833656751221318
 49284636812555022599830041234478486259567449219461702380650591324561082
 57318353800876086221028342701976982023131690176780066751954850799216364
 19370285375124784014907159135459982790513399611551794271106831134090584
 27288427979155484978295432353451706522326906139490598769300212296339568
 77828789484406160074129456749198230505716423771548163213806310459029161
 36926708342856440730447899971901781465763473223850267253059899795996090
 79946920177462481771844986745565925017832907047311943316555080756822184
 65717463732968849128195203174570024409266169108741483850784119298045229
 81857338977648103126085903001302413467189726673216491511131602920781738
 033436090243804708340403154192097.

q:=22123000461052396300949980998377306929368108700408171024880396070
 30594706308528699609927451156519227304929012295618862153402576648997071
 29727684600752063778727863167653029811001452412580528071420983756084893
 09180536668659968880129659834397222332464847994781289335628495373320168
 91201579033534315162059194255916786734094941260689076533414272188890713
 46753073863774447155764711093604167689543607055127510364613253246652709
 03661807447176302368144397196068371897929698555147237167618426748896515
 67689771506035588261566493053025353700061442029161099191377524177377375
 88597059735745331080362036268448863892078508213332597025459352395852905

58897982189013856141332586397318862056785406871855243778222925651640684
39732525640977522105746855231559022257735603402548515260996858865283235
15799686197670674244538668451013585735375988136548297852376643115167931
82163298335295781998512260795540369613780153368159514687066673081292948
71610587868926258587583385361968736705364374940026133933249697506677901
12286794114822609118897738868141237037222648305993868907421342346683945
62473767819419473796425543017381922924553750645900196756798937649003238
70026457579854503805963580090994214240686076075971778066104438302498457
89301394276469257947629476793497353948872169881256122429089718632857895
71495287044890095052754662553918351683021424748885230800808209430465635
54614838883198398132177767880678349380363182698199951297101602422600327
10523246723039230740436972381727917009663634628258617197597838460302747
60950197371652789941493667272208798099709711683282703068674053630482745
05788933711073472293374004525879941041154716905027086495391676016247956
82639777089424737984614508551823363909402064502765793650549161811922585
23641404436043178335564416730158751517204691803432150700582479110210777
21712932677561049832191340400275422142880411127801571486543090928761606
54232476147505657791572474193512801881860104899755113636776703462548771
09384583948254741273683797714310057805255843625983694177938754016515996
91032130823728277712284810578453031198824020933630934041210741528244128
53030503979042384424971530705028930080812673212757886126346255496537896
72796188210958480093248698786319428866341906653025501378989412897343406
87649784135376844000894058400790333992612021797470307112698708685506611
29658851380796456363638530444343908309312716419672209105620673794099191
99293785089303505326452733190090173013633539009751968237268389562128930
61697455914643854922135886874844006792372454381035535704185613034293926
3100587260271134433.

Execution time:= 11.107

Table 2: COMPLEXITY OF CALCULUS

The number r	Size of N	Executed Time
2	12393	11.107
3	10241	13.245
31	10469	58.345
41	13422	121.556
101	33403	1367.942

Conclusion:

In this work we could factor a number of 33403 size, in a time of 1367,942 second. So if you know a trap for RSA, its security is broken, for the one must seek another useful encryption, which will be safer.

Acknowledgments

The author gratefully acknowledges that his research is supported by Sidi Mohamed Ben Abdellah University, Polydisciplinary Faculty of Taza (FPT), and the Laboratory of Engineering Sciences (LSI) at FP, Taza, Morocco. We thank the referee by your suggestions.

References

1. Rivest, R.; Shamir, A.; Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21 (2): 120–126, (1978).
2. Boneh Dan, *Twenty Years of attacks on the RSA Cryptosystem*, Notices of the American Mathematical Society 46 (2): 203–213,(1999).
3. A. Chillali, *Cryptography over elliptic curve of the ring*, World Academy of Science, Engineering and Technology, (2011).

Abdelhakim Chillali,
Sidi Mohamed Ben Abdellah University,
FP, LSI, Taza, Morocco.
E-mail address: `abdelhakim.chillali@usmba.ac.ma`