

Dresden Algorithmics Channel

Modul 71

A Semiprime Factoring Alternating Gradient Synchrotron?

1. The Problem

The security guarantee of the RSA public key cryptosystem [1,2] is determined by the algorithmic complexity and with that the computing difficulty to refactorize the RSA module n , that means to refactorize the product of two sufficiently large nonspecial primes $prime(1)$ and $prime(2)$

$$n = prime(1) \cdot prime(2). \tag{1}$$

The commercial significance of this well-stated problem: **Factorization of a semiprime (1)** [3] and the status of its solution are noticeably documented by the highly-doted factorization award for special semiprimes, the „RSA challenge numbers“ by the American RSA Security Laboratories [4,5,6]. The goal of the RSA Sec. Lab. is hereby, to continuously test the security standard with all imaginable codebreaker ideas, but certainly also to stimulate and encourage the search for new public key cryptography systems.

RSA- d challenge number with d digits	Award for factorization in k \$	State of factorization
100		factored April 1991
110		factored April 1992
120		factored June 1993
129		factored April 1994
130		factored April 1996
140		factored Febr. 1999
150		factored April 2004
155		factored Aug. 1999
160		factored April 2003
174	10	factored Dec. 2003
193	20	open
200		Mai 2005
212	30	open
232	50	open
270	75	nopen
309	100	open
463	150	open
617	200	open

The hereby used algorithms are number theoretically based [1,2,3,4,5,6], the necessary computing resources are extensive, the computing times very long (RSA-200: factorization started in Dec. 2003, finished in May 2005), and the classical mathematical methods and approaches appear to be exhausted. Therefore, the search for alternative factorization algorithms seems to be obvious. In the following a new approach for an engineering based factorization algorithm is presented and put up for discussion.

2. A Fast Algorithm for Decomposition of a Positive Real Number into Two Factors

The output sequence $y(0), y(1), y(2), y(3), \dots$ of the recurrence formula

$$y(t+1) = y(t-1) \frac{1 + 3 \left(\frac{a}{y(t-1) \cdot y(t)} \right)^2}{3 + \left(\frac{a}{y(t-1) \cdot y(t)} \right)^2} \quad (2)$$

shows for positive initial values

$$y(0), y(1) \in \mathbb{R}_+ \quad (3)$$

and constant input

$$x(t) = a \in \mathbb{R}_+ \quad (4)$$

after a short transient process (≈ 20 steps) a periodic steady-state pattern with the period 2

$$\dots, f(1), f(2), f(1), f(2), \dots \quad (5)$$

Hereby is

$$f(1) \cdot f(2) = a. \quad (6)$$

In other words: The recurrence formula (2) in the steady-state performs a decomposition of a constant input a into two factors $f(1)$ and $f(2)$. The actual decomposition is here determined by $y(0)$ and $y(1)$ and in this way controllable („diode \rightarrow transistor“). This also means, that any external „injection“ Δy in only one $y(t)$

$$y(inj, t) = y(t) + \Delta y \in \mathbb{R}_+ \quad (7)$$

leads via a new transient process to another steady-state decomposition of a (see [7]).

The following example 1 demonstrates the performance of this factorization algorithm (eqs. (2) – (6)).

Example 1

$$a = 30; y(0) = 70; y(1) = 65$$

Value table of $y(t)$ and the accompanying difference quotient $dy(t)$:

t	$y(t)$	$dy(t) = \frac{y(t) - y(t+2)}{y(t+2) - y(t+4)}$
0	70.0	3.0135781451882043
1	65.0	3.1232271663789791
2	23.336038281456292547	4.1944765265562106
3	21.689264445289779694	22.7656830020804191
4	7.851468288455681506	6639.8964024243985559
5	7.821962053410289366	$1.4145524615155874 \cdot 10^{11}$
6	4.159810963646690135	$2.5127247785417172 \cdot 10^{33}$
7	7.212830212708991681	$1.5861625645225770 \cdot 10^{100}$
8	4.159254982483571224	
9	7.212830212704685500	
10	4.159254982483571224 = $f(1)$	
11	7.212830212704685500 = $f(2)$	

Column 3 of the value table immediately shows: With increasing t holds

$$dy(t+1) = (dy(t))^3, \quad (8)$$

with increasing accuracy, i.e. the controllable factorization of a positive real number exhibits a cubic convergence!

Substituting in eq. (2) the product $y(t-1) \cdot y(t)$ with the sum $y(t-1) + y(t)$, a controllable decomposition of the constant input a into two summands $g(1)$ and $g(2)$ with $g(1) + g(2) = a$ for the steady-state case occurs in the same way like previously described. However, this decomposition converges only linearly.

3. A Combination Idea: Solution of the Semiprime Factorization Problem Utilizing Solutions from the Synchrotron Technology [8,9]

The experimental facts described in part 2 are the basis for an innovative combination idea: Equ. (2) could be used as „accelerator“ and as „focusing magnet“ in a „semiprime factoring alternating gradient synchrotron“ that possesses a higher performance and efficiency than classical factorizing algorithms. However, this immediately implies the necessity to think about elements for an accompanying „defocusing magnet“. The most simple construction idea for this is a recurrence formula with different signs than in eq. (2):

$$y(t+1) = y(t-1) \frac{-1 + 3 \left(\frac{a}{y(t-1) \cdot y(t)} \right)^2}{3 - \left(\frac{a}{y(t-1) \cdot y(t)} \right)^2}; \quad t = 1, 2, 3, \dots \quad (9)$$

Example 2 shows a typical behavioral pattern of the output sequence from eq. (9).

Example 2

$$a = 30; \quad y(0) = 5; \quad y(1) = 7$$

Value table of $y(t)$:

t	$y(t)$	t	$y(t)$
0	5.0	13	-15.2374828327
1	7.0	14	-4.8443495200
2	2.6576576576	15	2.7116016489
3	119.1573564584	16	32.0233615179
4	-0.8646216223	17	-0.6042529769
5	-30.4770655312	18	333.5208036712
6	-1.4656690361	19	0.1894269421
7	-4.2225017154	20	-38.8937295606
8	4.9690311468	21	-0.6798677435
9	-22.6809011887	22	-64.9766841335
10	-1.3358066689	23	-0.1027149858
11	-21.8035898462	24	225.1429060286
12	-1.5037902189		

Although the initial product $y(0) \cdot y(1) = 35$ is close to $a = 30$ (in contradiction to ex. 1 with $y(0) \cdot y(1) = 4550$), the output sequence of eq. (9) diverges as deterministic chaos, and could also be usable for a weighted defocusing.

4. A First Realization Model for a Semiprime Factoring Alternating Gradient Synchrotron

In the following a first simple realization model for a semiprime factoring alternating gradient synchrotron is presented based on the recurrence formulae eq. (2) (acceleration and focusing) and eq. (9) (defocusing).

$$y(0), y(1) \in \mathbb{N} \tag{10}$$

$$y(t+1) = \begin{cases} \text{Floor} \left(y(t-1) \left((1-w) + w \frac{-1 + 3 \left(\frac{a}{y(t-1)y(t)} \right)^2}{3 - \left(\frac{a}{y(t-1)y(t)} \right)^2} \right) \right) & \text{for } t = 1, 3, 5, 7, \dots \\ & \text{defocusing} \\ \text{Ceiling} \left(y(t-1) \frac{1 + 3 \left(\frac{a}{y(t-1)y(t)} \right)^2}{3 + \left(\frac{a}{y(t-1)y(t)} \right)^2} \right) & \text{for } t = 2, 4, 6, 8, \dots \\ & \text{acceleration and} \\ & \text{focusing} \end{cases} \tag{11}$$

$$a = \text{prime}(1) \cdot \text{prime}(2);$$

$$0 < w \ll 1 - \text{defocusing weight}$$

Example 3

$$a = \text{prime}(1) \cdot \text{prime}(2) = 2619143683493;$$

$$\text{prime}(1) = \text{prime}[100000] = 1299709; \text{prime}(2) = \text{prime}[150000] = 2015177;$$

$$y(0) = \text{prime}(1) + 64500 = 1364209 \approx \text{prime}(1) \cdot (1 + 5/100);$$

$$y(1) = \text{prime}(2) - 1999573 = 15604 \approx \text{prime}(2) \cdot (1 - 99/100);$$

$$w = 9 \cdot 10^{-6}$$

Value table of $y(t)$:

t	$y(t)$	t	$y(t)$
0	1364209	5924	1299721
1	15604	5925	2015159
2	1364159	5926	1299720
3	46804	5927	2015160
4	1364109	5928	1299719
5	140190	5929	2015162
6	1364059	5930	1299718
7	414686	5931	2015164
8	1364004	5932	1299717
9	1108329	5933	2015165
10	1302650	5934	1299716
11	1915567	5935	2015167
12	1302652	5936	1299715
13	2010568	5937	2015168
14	1302652	5938	1299714
15	2010625	5939	2015170
16	1302651	5940	1299713
17	2010626	5941	2015171
18	1302650	5942	1299712
19	2010628	5943	2015173
20	1302649	5944	1299711
21	2010629	5945	2015174
22	1302648	5946	1299710
23	2010631	5947	2015176
24	1302647	5948	1299709
25	2010632	5949	2015177
26	1302646	5950	1299709 = <i>prime</i> (1)
27	2010634	5951	2015177 = <i>prime</i> (2)
28	1302645	5952	1299709
29	2010636	5953	2015177
30	1302644	5954	1299709
31	2010637	5955	2015177

The above value table demonstrates for the model eq. (10) and eq. (11): **Semiprime factoring is possible in principle** providing suitable chosen parameters $y(0)$, $y(1)$ and w .

One can distinguish three characteristic working ranges in the output sequence of this model:

1. Transient response range, in ex. 3 from $t = 0$ to $t = 15$:
strong changes of $y(t)$ toward two values that in the following
2. Creep range, here from $t = 16$ to $t = 5947$:
 - 2-periodically,
 - opposite monotone, and
 - almost linear
change only minimally, here $\text{abs}(y(t) - y(t + 2)) \in \{1, 2\}$.
3. **Prime capture range**, here beginning with $t = 5948$:

$(\forall t) y(t) = y(t + 2) \in \{\text{prime}(1), \text{prime}(2)\}$, i.e., **the model provides here for a constant input** $a = \text{prime}(1) \cdot \text{prime}(2)$ **the output sequence** $\dots, \text{prime}(1), \text{prime}(2), \text{prime}(1), \text{prime}(2), \dots$.

Example 4

$a = \text{prime}(1) \cdot \text{prime}(2) = 11606868967288127684640649$;
 $\text{prime}(1) = \text{prime}[10 \cdot 10^{10}] = 2760727302517$;
 $\text{prime}(2) = \text{prime}[15 \cdot 10^{10}] = 4204279414597$;
 $y(0) = \text{prime}(1) + 6666 = 27607273309183$;
 $y(1) = \text{prime}(2) - 11111111111 = 4193168303486$;
 $w = 10^{-6}$

Value table of $y(t)$:

t	$y(t)$	t	$y(t)$
0	2760727309183	72077	2760727302525
1	4193168303486	72078	4204279414585
2	2760727338561	72079	2760727302524
3	4204279340228	72080	4204279414587
4	2760727338561	72081	2760727302523
5	4204279359707	72082	4204279414588
6	2760727338560	72083	2760727302522
7	4204279359708	72084	4204279414590
8	2760727338559	72085	2760727302521
9	4204279359710	72086	4204279414591
10	2760727338558	72087	2760727302520
11	4204279359711	72088	4204279414593
12	2760727338557	72089	2760727302519
13	4204279359713	72090	4204279414594
14	2760727338556	72091	2760727302518
15	4204279359714	72092	4204279414596
16	2760727338555	72093	2760727302517
17	4204279359716	72994	4204279414597
18	2760727338554	72095	2760727302517 = $\text{prime}(1)$
19	4204279359717	72096	4204279414597 = $\text{prime}(2)$

Larger primes result in the same behavioral pattern as in ex. 3, too.

Example 5

$a = \text{RSA-160} = 2152741102718889701896015201312825429257773588845675980170497676$
 $7781331452188591356730110597734910596024979071115852143020793146$
 $65202840140619946994927570407753$;
 $\text{prime}(1) = 45427892858481394071686190649738831656137145778469793250959984709250$
 004157335359 ;
 $\text{prime}(2) = 47388090603832016196633832303788951973268922921040957944741354648812$
 028493909367 [14] ;
 $y(0) = \text{prime}(1) + 33000$;
 $y(1) = \text{prime}(2) - 111111111111$;
 $w = 10^{-12}$

The prime capture range is reached with $t = 66003$ in this example.

Further experiments with the presented model show:

- Reaching the prime capture range strongly depends on the parameters $y(0)$, $y(1)$ and w at a given input a .
- Depending on the computing accuracy, phantom capture ranges with $\dots, f(1), f(2), f(1), f(2), \dots$ but $f(1) \cdot f(2) \neq a$ can occur.
- When missing the prime capture range, the creep range eventually leads into the terminal capture range with the output sequence $\dots, a, 1, a, 1, \dots$.
- Improvements and extensions of the above presented primary model are possible and necessary. This particularly refers to the broadening and symmetrization of the initialization interval $(y(0), y(1)) = (\sqrt{a} + \Delta, \sqrt{a} - \Delta)$, such that the prime capture range is reached via a shortest possible creep range. We consider the following realization possibilities:
 - Output dependent control of w in the transient response range and in the creep range
 - Data dependent injection into $y(t)$ following eq. (7)
 - Incorporation of an output controlled weighting factor also in the acceleration and focusing part of eq. (11)
 - Incorporation of oscillating elements in eq. (11) (resonance und carrying over effects, see [10,11,12])
 - Utilization of further problem solutions from the synchrotron technology (stability, focusing, oscillations, tandem operation) [8,9,13]
 - Coupled operation of product and sum decomposition.

5. Conclusion

Inverting the argument, it is obvious to investigate the above discussed recurrence formulae (including derivatives and extensions) for suitability as trapdoor oneway functions for public key cryptosystems.

The author thanks Dr. Dagmar Schönfeld for technical support and for many helpful discussions during the preparation of this module.

References

- [1] Crandall,R.E.; Pomerance,C.: *Prime Numbers. A Computational Perspective*. New York, Berlin,...,Tokyo 2001
- [2] <http://mathworld.wolfram.com/RSAEncryption.html>
- [3] <http://mathworld.wolfram.com/Semiprime.html>
- [4] <http://www.crypto-world.com>
- [5] <http://www.rsasecurity.com>
- [6] <http://mathworld.wolfram.com/news/2005-05-10/rsa-200>
- [7] Stoschek,E.P.: *Abenteuer Algorithmus*. Teil 2, Kap. 4, Dresden 1997
- [8] Wilson,E.J.N.; Wilson,E.: *An Introduction to Particle Accelerators*. Oxford, New York 2001
- [9] Chao,A.W.; Tigner,M.: *Handbook of Accelerator Physics and Engineering*. Singapore 2002
- [10] <http://www.wissenschaft.de/wissen/news/257654.html>

- [11] Strogatz,S.H.; Abrams,D.M.; McRobie,A.; Eckhardt,B.; Ott,E.: *Crowd synchrony on the Millenium Bridge*. Nature 438, 43-44 (3 Nov. 2005)
- [12] Ito,T. ; Ito,K. : *Nonlinear dynamics of homeothermic temperature control in skunk cabbage, *Symplocarpus foetidus**. Phys. Rev. E 72, 051909 (2005)
- [13] Plettner,T. et al. : *Visible-Laser Acceleration of Relativistic Electrons in a Semi-Infinite Vacuum*. Phys. Rev. Lett. 95, 134801 (2005)
- [14] <http://www.rsasecurity.com/rsalabs/node.asp?id=2097>

Are you looking for suggestions and ideas on algorithms, mathematical, and computer-aided graphic design (textile, ceramics, book illustration, calligraphy, logo, advertising etc.)?

Visit <http://www.DresdenAlgorithmicsChannel.de> !

e.p.stoschek	17.11.2005
stoschek@tcs.inf.tu-dresden.de	