Safer parameters for the Chor-Rivest cryptosystem

L. Hernández Encinas*, J. Muñoz Masqué
and A. Queiruga Dios

Applied Physics Institute, CSIC
C/ Serrano 144, 28006-Madrid, Spain
{luis, jaime, araceli}@iec.csic.es

Abstract

Vaudenay's cryptanalysis to Chor-Rivest cryptosystem is not applicable if the parameters p and h of the finite field are both prime integers. This case is analyzed below and the parameters for which such cryptosystem is cryptographically interesting are listed. Regrettably the resulting cryptosystems are not very efficient in practice.

Keywords. Chor-Rivest cryptosystem, Cryptanalysis, Finite fields, Prime parameters, Public key cryptography.

1 Introduction

As is well known, the Chor-Rivest cryptosystem (see [3, 4]) is based on the Bose-Chowla theorem and the arithmetic of the Galois field $GF\left(p^h\right)$. The public key of this cryptosystem is defined as $(c_0, \ldots, c_{p-1}, p, h)$, where $c_i = b_i + d$,

*Corresponding author. Tel: (+34) 915618806 (Ext. 458), Fax: (+34) 914117651, Email: luis@iec.csic.es

$d \in [0, p^h - 2]$ play the role of noise, $b_i = a_{\pi(i)}$, with π a permutation of the set $\{0, 1, \ldots, p-1\}$, and $a_i = \log_g (t + \alpha_i)$, where $GF(p^h) = \{\alpha_0, \ldots, \alpha_{p-1}\}$, g is a generator of $GF(p^h)^*$ and $GF(p^h) = GF(p)[t]$, $\deg(t) = h$.

The first efficient attack for the proposed parameters (*i.e.*, $p \cong 200$, $h \cong 24$, in [3, 4]) has been obtained in [14], assuming h has a small factor.

The knapsack cryptosystems of density < 0.94 are known to be insecure after the classical attacks ([2, 5, 6, 8, 9, 11]). The density of Chor-Rivest cryptosystem is usually high; in fact, they are 1.077, 1.139, 1.278, and 1.280 for the parameters originally proposed in [3, 4]. Hence, the aforementioned attacks do not apply to it, but Schnorr and Hörner ([7, 13]) have been partially successful in breaking Chor-Rivest cryptosystem for a certain percent of keys in $GF(103^{12})$ and $GF(151^{16})$. Remark that such parameters are still far from those originally proposed.

In the present work we consider the case of prime parameters p and h, in the range determined by the present computational limitations, which is the remaining case in Vaudenay's attack.

2 The range $10^{44} < n < 10^{60}$

Vaudenay's cryptanalysis ([14]) of the Chor-Rivest cryptosystem ([3, 4]) essentially reduces it to the case in which p as well h are both prime integers.

In this section, we analyze the prime values for p and h such that

(1) $h \leq p$,

(2) $11 \leq h \leq 31$,

(3) $10^{44} < p^h - 1 < 10^{60}$,

(4) The smoothness of $n = p^h - 1$ is equal to or less than 10^{13}, *i.e.*, the greatest prime factor of $p^h - 1$ has 13 decimal digits at most.

Remark We should remark on the fact that the items (1), (3) and (4) imply $h \leq 31$. Actually, from (3) we deduce $h \log p \leq 60$. If $h \geq 41$, then $p \leq 29$,

thus contradicting (1). If $h = 37$, then $p \in \{37, 41, 43\}$, but the smoothness of n for these three cases is much bigger than 10^{13}. In fact, the least one is 10^{24} and it corresponds to the case $p = 43$. The cases $h \in \{2, 3, 5, 7\}$ are not considered in item (2) as they provide too long public keys, violating the requirement of section 3. In fact, the least public key bit length is about $3 \cdot 10^8$ bits.

We denote by D the set of pairs (p, h) satisfying the conditions (1)-(4) above, the list of which is given in Table 1. The following properties are obtained:

(a) $\#D = 175$.

(b) If $D_h = \{p \in \mathbb{Z} \colon (p, h) \in D\}$, then $D = D_{11} \cup D_{13} \cup D_{17}$, where $\#D_{11} = 150$, $\#D_{13} = 24$, and $\#D_{17} = 1$.

(c) The smallest prime integer $p_1^{11} \in D_{11}$ is $p_1^{11} = 10169$, and the greatest one $p_{150}^{11} \in D_{11}$ is $p_{150}^{11} = 233113$. Similarly, we have $p_1^{13} = 2549$, $p_{24}^{13} = 39343$; and $p_1^{17} = 409$.

(d) The number of bits, b_i^j, of the public keys $(c_0, \ldots, c_{p-1}, p, h)$ corresponding to the primes p_1^{11}, p_{150}^{11}, p_1^{13}, p_{24}^{13}, and p_1^{17}, are as follows:

$$\begin{aligned} b_1^{11} &= 1494861, \quad b_1^{13} = 377268, \quad b_1^{17} = 60546 \\ b_{150}^{11} &= 45923283, \quad b_{24}^{13} = 7829277. \end{aligned}$$

In what follows we justify why the items (3) and (4) are needed.

The number of digits for $p^h - 1$ proposed originally by Chor and Rivest ([4]) is 56, 56, 58, and 60, corresponding to the pairs $(197, 24)$, $(211, 24)$, $(3^5, 24)$, and $(2^5, 25)$, respectively. On the other hand, if the number of digits for $p^h - 1$ is small enough (in fact $p = 13$, $h = 12$, see [13]), we know that the algorithm by Schnorr and Hörner breaks the cryptosystem for a significant number (42%-76%) of public keys chosen at random. Moreover, the greatest value for (p, h) to which the aforementioned algorithm applies is (see [7]) $p = 151$, $h = 16$, but only 10% of public keys are broken for these parameters.

Both cases above are not specially interesting as they are covered by Vaudenay's attack, but the method of Schnorr and Hörner can be efficient for prime values of (p, h) within the range of such authors. In any case, the number of digits of n in all the cases considered in [7] and [13] is not greater than 35.

These facts justify the choice of the pairs (p, h) satisfying the conditions (1)-(3) above: Such values of the parameters lie approximately in the original range proposed by Chor-Rivest, but they are far from the parameters affected by Schnorr-Hörner cryptanalysis.

Item (4) is included because of computational feasibility. In fact, the running time for computing a discrete logarithm in $GF(p^h)^*$ is known to be (see [12, 3.65])

$$O\left(\sum_{i=1}^{r} e_i \left(\log_2 n + \sqrt{p_i}\right)\right)$$

group multiplications, where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of the order of the group.

Moreover, a group multiplication in $GF(p^h)^*$ costs $O\left((h-1)^2 \left(\log_2 p\right)^2\right)$ bit operations (cf. [1, 6.2.1] and [10, I,§1]). Hence, if B denotes the smoothness of n, then the previous formula allows us to estimate the running time of a discrete logarithm in $GF(p^h)^*$ as

$$\frac{\left(\log_2 n\right)^3 \left(\log_2 n + \sqrt{B}\right)}{\log_2 B}.$$

In addition, if we assume that the number of bit operations per day in a standard PC is 10^{12}, then in the range of item (3), we obtain $B < 10^{13}$.

3 The key size

The sizes of public keys in the Chor-Rivest cryptosystem are usually much greater than the sizes of those for RSA and ElGamal PKCs. In fact, for the original parameters proposed in [4], denoting by $b(p, h)$ the bit length of the

public keys corresponding to (p, h), we have

$$b(197, 24) = 36064, \quad b(211, 24) = 39259,$$
$$b(243, 24) = 46426, \quad b(256, 25) = 51470.$$

As we have shown in item (d), in the range $10^{44} < n < 10^{60}$ there is a unique pair (p, h) for which the size of its public key is similar to the greatest one of the four cases above; namely, $p = 409$, $h = 17$, for which $b(409, 17) = b_1^{17} = 60546$.

A reasonable bound for the bit length of the public key should be 70000, as this is near to the double of the least bit length of the original values for (p, h).

We have searched for the prime pairs (p, h) such that $10^{44} < n$, $h \leq p$, and the bit length of its corresponding public key is not greater than 70000. Among these pairs, those not included in the range defined by items (1)-(4), are given in Table 2, where d (resp. $B = 10^s$) denotes the number of digits (resp. smoothness) of n. The relevant fact is that none of such pairs has a smoothness $\leq 10^{13}$; *i.e.*, the item (4) does not hold. Actually, the least value for the smoothness of such pairs is 10^{18}, corresponding to $p = 173$, $h = 29$.

4 Conclusions

(i) A unique prime pair (p, h) exists in the range (1)-(4) and with a bit length for the public key parameters slightly greater than those proposed originally in [3, 4]; namely, $p = 409$, $h = 17$. Moreover, we have that the number of digits of n is 45, the smoothness is 10^{10}, the bit length of the corresponding public key is $b_1^{17} = 60546$, the density of the cryptosystem for such parameters is bounded from below by 2.77, and the factorization of n is

$$n = 409^{17} - 1 = 2^3 \cdot 3 \cdot 17^2 \cdot 103 \cdot 307 \cdot 443 \cdot 3163 \cdot 43283 \cdot 47363 \cdot 55217 \cdot 21906541 \cdot 329083009.$$

(ii) Although Vaudenay's cryptanalysis to the Chor-Rivest cryptosystem does not include the case of prime parameters (p, h), the results above actu-

ally show that the cryptosystem is useless nowadays due to the present computational limitations, which essentially affect the size of the public key and to the smoothness of n, because of the complexity of the discrete logarithm problem.

Acknowledgement

Supported by Ministerio de Educación y Ciencia of Spain, under grant SEG2004-02418. Authors thanks professors H. Chabanne, R. Durán, A. Menezes, and S. Vaudenay, for their valuable comments and suggestions.

References

[1] E. Bach and J. Shallit, Algorithmic number theory, Vol 1: Efficient algorithms, The MIT Press, Cambridge, MS, 1996.

[2] E. Brickell, Solving low density knapsacks, *Proc. of Crypto'83, Plenum Press* (1984), 25–37.

[3] B. Chor, *Two issues in public key cryptography. RSA bit security and a new knapsack type system*, The MIT Press, Cambridge, MS, 1985.

[4] B. Chor and R.L. Rivest, A knapsack-type public key cryptosystem based on aritmethic in finite fields, *IEEE Trans. Inform. Theory* **34**, 5 (1988), 901–909.

[5] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr, and J. Stern, Improved low-density subset sum algorithms, *Comput. Complexity* **2** (1992), 111–128.

[6] A.M. Frieze, On the Lagarias-Odlyzko algorithm for the subset sum problem, *SIAM J. Comp.* **15**, 2 (1986), 536–539.

[7] H.H. Hörner, Verbesserte Gitterbasenreduktion; getestet am Chor-Rivest Kryptosystem und an allgemeinen Rucksack-Problemen, *Diplomarbeit, Universität Frankfurt* (August, 1994).

[8] F. Jorissen, J. Vandewalle, and R. Govaerts, Extension of Brickell's algorithm for breaking high density knapsacks, *Proc. of Eurocrypt'87, LNCS* **304** (1988), 109–115.

[9] A. Joux and J. Stern, Improving the critical density of the Lagarias-Odlyzko attack against subset sum problems, *Proc. of Fundamentals of Computation Theory'91, LNCS* **529** (1991), 258–264.

[10] N. Koblitz, A course in number theory and cryptography, 2nd. ed., Springer-Verlag, Berlin, 1994.

[11] J.C. Lagarias and A.M. Odlyzko, Solving low-density subset sum problems, *J. ACM* **32**, 1 (1985), 229–246.

[12] A.J. Menezes, P.C. van Oorschot, and S. Vanstone, Handbook of applied cryptography, CRC Press, Boca Raton, FL, 1997.

[13] C.P. Schnorr and H.H. Hörner, Attacking the Chor-Rivest cryptosystem by improved lattice reduction, *Proc. of Eurocrypt'95, LNCS* **921** (1995), 1–12.

[14] S. Vaudenay, Cryptanalysis of the Chor-Rivest cryptosystem, *J. Cryptology* **14** (2001), 87-100.

p	h	p	h	p	h	p	h	p	h
409	17	2549	13	2593	13	2659	13	2707	13
3323	13	3547	13	4999	13	5059	13	5413	13
5807	13	6247	13	8443	13	9467	13	10169	11
10333	11	10487	13	11083	11	11783	13	11789	11
11927	11	12109	13	12413	11	12119	13	12163	13
12919	11	13033	11	13099	11	13499	11	13687	11
13721	11	13907	11	14081	11	14347	11	14407	13
14537	11	14731	11	14753	11	15277	11	15361	11
15809	11	17183	11	17299	11	17359	11	17389	11
17509	11	18121	11	18353	11	18401	11	18691	13
19433	11	20287	11	21031	11	21061	11	21377	11
22543	11	22963	11	23333	11	23629	11	23633	11
25457	11	25693	11	25763	11	26489	13	28001	11
28027	11	28219	11	28477	11	28537	11	29879	11
30367	11	30649	11	32533	13	33247	11	33829	11
33967	11	35809	11	36013	11	36563	11	37529	11
38431	11	38833	13	39343	13	39953	11	40151	11
40787	11	41057	11	41957	11	42737	11	44389	11
44543	11	45413	11	46447	11	47917	11	48907	11
51239	11	53551	11	55439	11	56897	11	58907	11
62497	11	64033	11	64403	11	65099	11	66821	11
68113	11	68749	11	70199	11	70249	11	70607	11
72379	11	74027	11	74597	11	75181	11	76831	11
77291	11	79133	11	79973	11	83089	11	83423	11
88969	11	89231	11	90971	11	92381	11	92647	11
92723	11	92849	11	95369	11	95393	11	95581	11
97729	11	98869	11	99787	11	100189	11	101411	11
102217	11	104381	11	104953	11	108761	11	111773	11
119233	11	121501	11	124489	11	124699	11	131479	11
135403	11	144481	11	149173	11	152407	11	153911	11
157897	11	159073	11	163901	11	167269	11	167971	11
172849	11	181757	11	183089	11	184211	11	185987	11
192149	11	205391	11	207293	11	209563	11	211039	11
211949	11	213359	11	215801	11	219823	11	221203	11
221411	11	221567	11	229819	11	231131	11	233113	11

Table 1. Values of the pairs (p, h) verifying the conditions (1)-(4)

p	h	d	s	p	h	d	s	p	h	d	s	p	h	d	s
109	29	60	38	113	29	60	50	127	29	62	41	131	29	62	41
137	29	62	51	139	29	63	33	149	29	64	29	151	29	64	62
157	29	64	20	163	29	65	39	167	29	65	43	173	29	65	18
179	29	66	51	181	29	66	30	191	29	67	34	193	29	67	38
197	29	67	55	199	29	67	20	211	29	68	55	223	29	69	35
227	29	69	51	229	29	69	67	233	29	69	45	239	29	69	94
241	29	70	40	251	29	70	53	257	29	70	32	263	29	71	46
269	29	71	30	271	29	71	25	277	29	71	33	281	29	72	63
283	29	72	69	293	29	72	29	83	31	60	22	89	31	61	53
97	31	62	47	101	31	63	25	103	31	63	38	107	31	63	28
109	31	64	40	113	31	64	44	127	31	66	64	131	31	66	64
137	31	67	32	139	31	67	56	149	31	68	26	151	31	68	60
157	31	69	49	163	31	69	45	167	31	69	40	173	31	70	53
179	31	70	37	181	31	70	41	191	31	71	45	193	31	71	34
199	31	72	49	197	31	72	69	211	31	73	49	223	31	73	56
227	31	74	30	229	31	74	33	233	31	74	45	239	31	74	23
241	31	74	72	251	31	75	63	257	31	75	29	263	31	76	42
269	31	76	30	271	31	76	34	277	31	76	71	41	37	60	49
43	37	61	24	47	37	62	50	53	37	64	43	59	37	66	30
61	37	67	65	67	37	68	46	71	37	69	38	73	37	69	43
79	37	71	41	83	37	72	36	89	37	73	25	97	37	74	72
101	37	75	42	103	37	75	39	107	37	76	71	109	37	76	52
113	37	76	74	127	37	78	60	131	37	79	34	137	37	80	42
139	37	80	61	149	37	81	70	151	37	81	67	157	37	82	36
163	37	82	35	167	37	83	77	173	37	83	40	179	37	84	61
181	37	84	65	191	37	85	57	193	37	85	28	197	37	85	45
199	37	86	68	211	37	86	47	223	37	87	25	227	37	88	56
229	37	88	26	233	37	88	55	239	37	89	60				

Table 2. Values of the prime pairs (p, h) verifying $10^{44} < p^h - 1$, $h \leq p$, and $b(p, h) < 70000$