Information Sciences 179 (2009) 4219–4226

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Analysis of the efficiency of the Chor–Rivest cryptosystem implementation in a safe-parameter range

L. Hernández Encinas [a,*], J. Muñoz Masqué [a], A. Queiruga Dios [b]

[a] Department of Information Processing and Coding, Applied Physics Institute (IFA), Spanish National Research Council (CSIC), C/Serrano 144, 28006 Madrid, Spain
[b] Department of Applied Mathematics, ETSII, University of Salamanca, Avda. Fernández Ballesteros 2, 37700 Béjar, Salamanca, Spain

ARTICLE INFO

Article history:
Received 26 January 2009
Received in revised form 24 July 2009
Accepted 30 August 2009

Keywords:
Chor–Rivest cryptosystem
Knapsack problem
Finite fields
Magma software
Public key cryptography

ABSTRACT

The Chor–Rivest cryptosystem, based on a high-density knapsack problem on a finite field $\mathbb{F}_{q^h}$, was broken by Vaudenay for $q \approx 200, h \approx 24$, and h admitting a factor s verifying a certain condition. A new set of parameters q and h, which prevent this cryptosystem against Vaudenay's attack, is presented and the computational aspects of its implementation in the Magma computational algebra system are analyzed.

1. Introduction

The objective of cryptography is to assure the secrecy and confidentiality of communications and the goal of cryptanalysis is to break the security and privacy of such communications [12,13]. In particular, in public key cryptography (PKC) each user has two keys: the public key, which is publicly known and it is used by the sender to encrypt a message; and the private key, which is kept in secret by the receiver and it is used by him to decrypt encrypted messages. In general, PKC bases its security on the computational intractability of some Number Theory problems, such as factorization problem, discrete logarithm problem and knapsack problem.

In 1985, Chor proposed a cryptosystem based on the knapsack problem (see [2,3]). The last—and the only really efficient—attack to this system has been proposed by Vaudenay [17], but only for the parameters originally proposed.

The Chor–Rivest cryptosystem is based on the arithmetic of finite fields and it needs to compute discrete logarithms in order to determine the keys of the system. The discrete logarithm problem (DLP) can be defined as follows: given a prime integer p, a generator α of the cyclic group $\mathbb{Z}_p^*$, and an element $\beta \in \mathbb{Z}_p^*$, the DLP consists in finding an integer $x, 0 < x \leqslant p-1$, such that $\beta = \alpha^x$. This problem is considered to be difficult because the best known algorithm for solving it is the number field sieve [16] which has a subexponential expected running time:

$$O\left(e^{\left((64/9)^{1/3}+o(1)\right)(\ln p)^{1/3}(\ln\ln p)^{2/3}}\right).$$

The security of the cryptosystem depends on the knapsack problem but not on the discrete logarithm problem. In fact, if the DLP becomes tractable, then the Chor–Rivest cryptosystem is easier to implement, but not easier to break.

* Corresponding author. Tel.: +34 915618806x458; fax: +34 914117651.
E-mail addresses: luis@iec.csic.es (L.H. Encinas), jaime@iec.csic.es (J.M. Masqué), queirugadios@usal.es (A.Q. Dios).

0020-0255/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2009.08.030

As other knapsack cryptosystems, Chor–Rivest cryptosystem is not a very popular public key cryptosystem. Some of its drawbacks are that it needs a large time for generating its keys and a big size of public keys.

Nevertheless, nowadays more knapsack-based cryptosystems are being proposed in order to consider new candidates in PKC (see, for example, [18] and the references therein). One of the main reasons argued by the authors to state that their cryptosystem is secure was that it resists the low-density attacks, due to the fact that its density is 1.2, which is bigger than 0.9408 (see [1,4,14]). Although the system resists low-density attacks, it was recently broken in [19] by means of a heuristic attack, which permits to recover the private key from the public key. This is an added reason to study the security of some of the most important knapsack proposed, as it is the case of Chor–Rivest cryptosystem.

Moreover, the recommendations for the most popular public key cryptosystems (RSA, ElGamal, etc.) suggest to increase the size of their parameters, due, basically, to the results in quantum computation and in the improvements of the computational time for some number theory problems (see [9,10]). In this way, the recommended bitlength of the keys are around 2048–4096 (for example, nowadays there are millions of ID cards in Europe with keys of these sizes).

For these reasons, it is relevant and of interest to study safe alternative cryptosystems, and the Chor–Rivest cryptosystem may be one of them.

In spite of several attacks against Chor–Rivest cryptosystem have been proposed (see [2,3]):

- low-density attacks,
- nothing known (by E. Brickell),
- known g and r,
- known t and r,
- known t (by O. Goldreich),
- known π and r (by A. Odlizko).

None of them is efficient without knowing a part of the private key.

In [17] the Chor–Rivest cryptosystem was broken for the original proposed parameters, i.e., when the cryptosystem is defined over a finite field $\mathbb{F}_{q^h}$ with $q \approx 200$ and $h \approx 24$. This attack is based on a weakness derived from the fact that the cryptosystem is insecure if the parameter h has a factor s verifying the following condition:

$$s \geqslant \sqrt{h+\frac{1}{4}}+\frac{1}{2}. \tag{1}$$

In order to avoid Vaudenay's attack, in [7] a new pair of parameters has been determined for using safely this cryptosystem. In fact, these parameters were computed in a suitable range guaranteeing its security and its computational feasibility; such parameters are $q = 409$ and $h = 17$. Only a new pair of values was obtained! This is clearly not useful for cryptographic applications.

Here, we present a new set of parameters q and h, which prevent Chor–Rivest cryptosystem against Vaudenay's attack. Moreover, the main computational aspects of its implementation in the Magma computational algebra system are analyzed. These results show that there are many (in fact, infinite) values of new parameters for which Vaudenay's attack are unfeasible, which is relevant from a cryptographic point of view. In addition, this new implementation is more efficient than that proposed in [6].

2. Preliminaries

A brief description (see [2,3,7] for the details), of the Chor–Rivest cryptosystem is as follows:

1. Choose a prime number q and an integer $h \leqslant q$ so that the DLP can be efficiently solved in the finite field $\mathbb{F}_{q^h}$. This fact is important to generate the keys because this generation needs to compute discrete logarithms in the group $\mathbb{F}_{q^h}^*$. The reason is that the DLP can be solve in a efficient way by using the Pohlig–Hellman algorithm if the order of the multiplicative group considered, $n = q^h - 1$, factorizes as a product of small prime factors [12,15].
2. Select a random algebraic element of degree h over $\mathbb{F}_{q^h}$, t, and a random irreducible monic polynomial, $f(t)$, of degree h, such that $\mathbb{F}_{q^h} \approx \mathbb{F}_q[t]/(f(t))$.
3. Choose a random generator, g, of the group $\mathbb{F}_{q^h}^*$. Such generator can be chosen at random in $\mathbb{F}_{q^h}^*$ until it verifies $g^{(q^h-1)/l} \neq 1$ for all prime divisors, l, of $q^h - 1$.
4. Compute the discrete logarithms $\log_g(t+\alpha_i) = a_i, \forall \alpha_i \in \mathbb{F}_q$.
5. Generate a random permutation of q elements, $\pi : \{0,1,\ldots,q-1\} \to \{0,1,\ldots,q-1\}$ and compute $b_i = a_{\pi(i)}$.
6. Add a random noise, $0 \leqslant r \leqslant q^h - 2$, to obtain the elements of the knapsack: $c_i \equiv (b_i + r) \pmod{q^h - 1},\ 0 \leqslant i \leqslant q-1$, which are the public key.
7. The private key is formed by the values (t, g, π, r).

The messages to be encrypted, M, are binary vectors of length q and weight h [5], i.e.,