Cryptanalysis of the CFVZ cryptosystem*

Joan-Josep Climent
Departament de Ciència de la Computació
i Intel·ligència Artificial
Universitat d'Alacant
Campus de Sant Vicent del Raspeig
E-03080 Alacant, Spain
jcliment@dccia.ua.es

Elisa Gorla
Department of Mathematics
University of Zürich
Winterthurerstr 190
CH-8057 Zürich, Switzerland
http://www.math.unizh.ch/aa/

Joachim Rosenthal
Department of Mathematics
University of Zürich
Winterthurerstr 190
CH-8057 Zürich, Switzerland
http://www.math.unizh.ch/aa/

February 8, 2006

Abstract

The paper analyzes a new public key cryptosystem whose security is based on a matrix version of the discrete logarithm problem over an elliptic curve.

It is shown that the complexity of solving the underlying problem for the proposed system is dominated by the complexity of solving a fixed number of discrete logarithm problems in the group of an elliptic curve. Using an adapted Pollard rho algorithm it is shown that this problem is essentially as hard as solving one discrete logarithm problem in the group of an elliptic curve.

Keywords: Public Key Cryptography, Diffie-Hellman protocol, Elliptic Curve Cryptography, Generalized Birthday Problem.

*Research supported by Swiss National Science Foundation Grant no. 107887 and by Generalitat Valenciana grant CTESPP-2005-060. The research of this paper was accepted for presentation at the 10th Rhine Workshop on Computer Algebra (RWCA) to be held in Basel, Switzerland March 16, 17.

1 Introduction

Public-key cryptography, based on the intractability of the discrete logarithm problem, was introduced by Diffie and Hellman [5]. The Diffie-Hellman protocol allows two parties Alice and Bob, who are communicating over an insecure channel, to generate a shared secret key which is difficult to compute for an eavesdropper.

The discrete logarithm problem (DLP) over various finite groups has been studied extensively. In the early days the main example has been the multiplicative group over a finite field $\mathbb{F}_q$. Odoni, Varadharajan and Sanders [11] introduced the discrete logarithm problem for matrices over $\mathbb{F}_q$ and a Diffie-Hellman key exchange protocol based on matrices. However, Menezes and Wu [9] reduced the discrete logarithm problem for matrices to some discrete logarithm problems over small extensions of $\mathbb{F}_q$.

In the late eighties Miller [10] and Koblitz [7] independently proposed to study the DLP in the group of $\mathbb{F}_q$-rational points of an elliptic curve. This was the start of an active research in the area of elliptic curve cryptography (ECC), and its use for implementing public-key protocols such as the Diffie-Hellman key agreement. The security of ECC is based on the presumed intractability of the discrete logarithm problem over the curve.

A vast amount of research has been done on the security and efficient implementation of ECC. Finite groups based on elliptic curves are very appealing, as the best algorithms known to tackle the DLP over an elliptic curve has exponential running time, and this despite intensive attempts on this problem. The interested reader may consult the recent book [3].

Recently, Climent, Ferrández, Vicent and Zamora [2] introduced a Diffie-Hellman key exchange protocol which used a combination of matrix algebra ideas and adding points on an elliptic curve. We will describe this new cryptosystem CFVZ in the next section. The main results of this paper will be presented in Section 3. We will show that CFVZ can be reduced to the problem of solving $2rs$ discrete logarithm problems over an elliptic curve in a simultaneous manner. The complexity for doing this is considerably less than solving $2rs$ single discrete logarithm problems over an elliptic curve.

2 The cryptosystem CFVZ of Climent-Ferrández-Vicent-Zamora

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$, and let $E(\mathbb{F}_q)$ denote the group of $\mathbb{F}_q$-rational points of E. Assume that $E(\mathbb{F}_q)$ is a cyclic group of order n. Denote by $\mathrm{Mat}_r(\mathbb{Z})$ the set of all $r \times r$ matrices with integer entries and denote by $\mathrm{Mat}_{r\times s}(E(\mathbb{F}_q))$ the set of all $r \times s$ matrices whose entries are elements of the group $E(\mathbb{F}_q)$. Let r, s be fixed positive integers and consider the set

$$\xi = \left\{ \begin{bmatrix} A & \Pi \\ & B \end{bmatrix} : A \in \mathrm{Mat}_r(\mathbb{Z}), B \in \mathrm{Mat}_s(\mathbb{Z}), \Pi \in \mathrm{Mat}_{r\times s}(E(\mathbb{F}_q)) \right\}.$$

The set ξ is a semigroup with the formal matrix multiplication

$$\begin{bmatrix} A & \Pi \\ & B \end{bmatrix} \begin{bmatrix} C & \Phi \\ & D \end{bmatrix} = \begin{bmatrix} AC & A\Phi + \Pi D \\ & BD \end{bmatrix},$$

where

$$A\Phi = [a_{ij}][P_{ij}] = [Q_{ij}] \quad \text{with} \quad Q_{ij} = \sum_{k=1}^{r} a_{ik} P_{kj}$$

and similarly for ΠD.

Without loss of generality we will assume that A and B are matrices defined over $\mathbb{Z}/n\mathbb{Z}$. If A and B are invertible matrices over the ring $\mathbb{Z}/n\mathbb{Z}$ then we can consider the subgroup generated by the public element

$$\mathcal{M} = \begin{bmatrix} A & \Pi \\ & B \end{bmatrix}.$$

Let $m \geq 1$ be an integer. A direct computation shows that $\mathcal{M}^m = \begin{bmatrix} A^m & \Pi_m \\ & B^m \end{bmatrix}$ where

$$\Pi_m = \sum_{i=0}^{m} A^{m-1-i} \Pi B^i. \tag{1}$$

One way of setting up a discrete logarithm problem is:

"Given the matrices $\mathcal{M}$ and $\mathcal{M}^m$, find m."

As shown in [2], the order of $\mathcal{M}$ is the least common multiple of the orders of A and B and hence the discrete logarithm problem has the character of a discrete logarithm problem over the matrix ring.

A more interesting problem was introduced in [2], we will call this problem the

CFVZ discrete logarithm problem: given $\Pi, \Phi \in \mathrm{Mat}_{r\times s}(E(\mathbb{F}_q))$, find $m \in \mathbb{Z}$ such that $\Phi = \Pi_m$ (whenever such an m exists).

Remark 2.1. Notice that if the CFVZ discrete logarithm problem has a solution m_0, then it has infinitely many solutions in $\mathbb{Z}$. In fact, each element of the coset $m_0 + l\mathbb{Z}$ is a solution, if we let l be the order of $\mathcal{M}$. Moreover, it may be $\Pi_m = \Pi_{m_0}$ even for values of m for which $\mathcal{M}^m \neq \mathcal{M}^{m_0}$.

Notice in addition that the sequence Π_m is obtained from a recurrence relation, namely

$$\Pi_m = A\Pi_{m-1} + \Pi B^{m-1}.$$

In particular, the sequence of the Π_m has a period. However it is not true in general that $\Pi_i = \Pi_j$ implies $\Pi_{i+1} = \Pi_{j+1}$.

The CFVZ discrete logarithm problem induces a Diffie-Hellman key exchange in the following way:

- Alice chooses a private key k and computes

$$\mathcal{M}^k = \begin{bmatrix} A^k & \Pi_k \\ & B^k \end{bmatrix}.$$

She takes Π_k as her public key.

- Bob chooses a private key l and computes

$$\mathcal{M}^l = \begin{bmatrix} A^l & \Pi_l \\ & B^l \end{bmatrix}.$$

He takes Π_l as his public key.

- Then Alice and Bob consider matrices

$$\mathcal{R} = \begin{bmatrix} A & \Pi_l \\ & B \end{bmatrix} \quad \text{and} \quad \mathcal{S} = \begin{bmatrix} A & \Pi_k \\ & B \end{bmatrix}$$

respectively and compute

$$\mathcal{R}^k = \begin{bmatrix} A^k & (\Pi_l)_k \\ & B^k \end{bmatrix} \quad \text{and} \quad \mathcal{S}^l = \begin{bmatrix} A^l & (\Pi_k)_l \\ & B^l \end{bmatrix}$$

respectively.

The shared secret is then by equation (1)

$$(\Pi_l)_k = \sum_{j=0}^{k} A^{k-1-j} \left(\sum_{i=0}^{l} A^{l-1-i} \Pi B^i \right) B^j = \sum_{i=0}^{l} A^{l-1-j} \left(\sum_{j=0}^{k} A^{k-1-j} \Pi B^j \right) B^i = (\Pi_k)_l,$$

which both Alice and Bob can readily compute.

In order to attack the cryptosystem the following Diffie-Hellman problem has to be solved:

Problem 1. Given the matrix $\mathcal{M}$, and the two public keys Π_k and Π_l, find $(\Pi_k)_l = (\Pi_l)_k$.

3 Cryptanalysis of the system

In this section we analyze the security of the CFVZ Diffie-Hellman key exchange as proposed in [2]. We will show that solving the Diffie-Hellman Problem has the same complexity as solving an ECDLP on $E(\mathbb{F}_q)$ and two linear system of equations in $2rs$ and $r+s-1$ or fewer unknowns respectively.

For the applications, the curve E and the field $\mathbb{F}_q$ are always chosen so that the group $E(\mathbb{F}_q)$ has prime order. However, here we will analyze the case when the group $E(\mathbb{F}_q)$ is cyclic of order n, since this introduces no extra difficulty.

3.1 Reduction to a matrix problem

In a first step we show how to reduce the CFVZ discrete logarithm problem to a problem involving matrices defined over $\mathbb{Z}/n\mathbb{Z}$ only. For this assume that $P \in E(\mathbb{F}_q)$ is a generator of the cyclic group $E(\mathbb{F}_q)$.

Let $C = [c_{ij}] \in \mathrm{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z})$ be a matrix such that

$$CP = \Pi \quad \text{where} \quad CP = [c_{ij}P].$$

Define the matrix

$$M = \begin{bmatrix} A & C \\ 0 & B \end{bmatrix},$$

and assume

$$M^k = \begin{bmatrix} A^k & C_k \\ & B^k \end{bmatrix}, \quad \text{where} \quad C_k = \sum_{i=0}^{k} A^{k-1-i} C B^i.$$

The following lemma is readily verified:

Lemma 3.1. *Let k and l be positive integers and let*

$$(C_l)_k = \sum_{j=0}^{k} A^{k-1-j} \left(\sum_{i=0}^{l} A^{l-1-i} C B^i \right) B^j.$$

Then

$$\Pi_k = C_k P \quad \textit{and} \quad (\Pi_l)_k = (C_l)_k P.$$

Based on this lemma, Problem 1 is solved if we solve a number of discrete logarithm problems over the elliptic curve $E(\mathbb{F}_q)$, and the following matrix Diffie-Hellman problem:

Problem 2. Given the matrix M, and the two public keys C_k and C_l, find $(C_k)_l = (C_l)_k$.

In order to solve the CFVZ discrete logarithm problem it is therefore enough to compute

$$\tau := 3rs \tag{2}$$

discrete logarithm problems over the elliptic curve $E(\mathbb{F}_q)$ in order to compute matrices C_k, C_l and C such that

$$\Pi = CP, \quad \Pi_k = C_k P, \quad \text{and} \quad \Pi_l = C_l P.$$

Thereafter one has to tackle the linear algebra Problem 2.

In the remainder of this subsection we show that solving τ discrete logarithm problems over the elliptic curve $E(\mathbb{F}_q)$ with regard to a fixed generator P is considerably less complex than solving τ individual discrete logarithm problems. We now analyze the complexity of solving a fixed number of DLPs in a given cyclic group. We also refer the reader to [8] for a treatment of the same problem.

For this assume that $P_1, \ldots, P_\tau$ are points on the elliptic curve group $E(\mathbb{F}_q)$. We would like to find integers $n_1, \ldots, n_\tau$ such that:

$$P_i = n_i P, \quad \text{for} \quad i = 1, \ldots, \tau.$$

Using an adapted version of the Pollard rho algorithm we compute points of the form:

$$Q_j = \sum_{i=1}^{\tau} c_{ij} P_i + d_j P \quad \text{with} \quad c_{ij}, d_j \in \mathbb{Z}/n\mathbb{Z}.$$

We repeat this computation until there are more than τ equal pairs $Q_i = Q_j$ and $i \neq j$. This is a generalized birthday problem. Let I_{ij} be the random variable having the value 1 if $Q_i = Q_j$ and the value zero otherwise and consider the random variable

$$W := \sum_{i<j} I_{ij}.$$

We are interested that

$$\mathbb{P}(W \geq \tau) > \frac{1}{2} \tag{3}$$

where τ is defined by (2). As explained in [1, p. 104-107] (compare also with the recent survey [4]) the random variable W is well approximated by a Poisson random variable. Based on this fact, the probability of expression (3) can be computed in the following way:

Assume that α points Q_j were computed. Let

$$\lambda := \binom{\alpha}{2} / n. \tag{4}$$

Then the probability in (3) is approximated by the expression:

$$\mathbb{P}(W \geq \tau) = 1 - \sum_{i=0}^{\tau-1} \frac{\lambda^i}{i!} e^{-\lambda}.$$

Already in the early 18'th century de Moivre [6, p. 214] was interested in the maximal value τ such that $\mathbb{P}(W \geq \tau) \geq \frac{1}{2}$. Equivalently we can seek the minimal value α such that with probability more than 1/2 there will be at least τ collisions.

Viewing the Poisson distribution as the limit of a binomial distribution with expected value λ given by (4), one readily gets the approximation

$$\tau \leq \binom{\alpha}{2} / n,$$

or equivalently

$$\sqrt{\alpha(\alpha - 1)} \geq \sqrt{2\tau n}.$$

The expected number of point additions for the τ discrete logarithm problems over $E(\mathbb{F}_q)$ is therefore $\mathcal{O}(\sqrt{rsn})$.

Once we have $t \geq \tau$ collisions we immediately obtain a system of t linear equations:

$$T \begin{bmatrix} P_1 \\ \vdots \\ P_\tau \end{bmatrix} = \begin{bmatrix} v_1 \\ \vdots \\ v_\tau \end{bmatrix} P = vP,$$

where $T \in \mathrm{Mat}_{t\times\tau}(\mathbb{Z}/n\mathbb{Z})$ and the vector $v \in (\mathbb{Z}/n\mathbb{Z})^\tau$. As soon as T has full rank τ, the points P_i can all be computed from P through a simple matrix inversion of T. The cost of inverting T over $\mathbb{Z}/n\mathbb{Z}$ requires $\mathcal{O}(\tau^3)$ modular multiplications.

In order to simultaneously solve the given τ discrete logarithm problems, we can also follow a different approach. Let d be the determinant of the matrix $T \in \mathrm{Mat}_{\tau\times\tau}(\mathbb{Z}/n\mathbb{Z})$

that we obtain after collecting τ relations among the given points. Let $g = \gcd(d, n)$ be the greatest common divisor of d and n, and let $m = n/g$. Then T has full rank over the ring $\mathbb{Z}/m\mathbb{Z}$. Hence a simple matrix inversion gives us $a_1, \ldots, a_\tau \in \mathbb{Z}/m\mathbb{Z}$ such that $n_i = a_i$ modulo m for all $i = 1, \ldots, \tau$. Because of the algorithm of Pohlig and Hellman, for all practical purposes we can assume that n is of the form $n = lp$, where p is prime and l is small. The probability that the determinant d is invertible modulo p is equal to

$$\frac{|GL_\tau(\mathbb{Z}/p\mathbb{Z})|}{|\operatorname{Mat}_{\tau\times\tau}(\mathbb{Z}/p\mathbb{Z})|} = \prod_{i=1}^{\tau} \left(1 - \frac{1}{p^i}\right).$$

Here $|GL_\tau(\mathbb{Z}/p\mathbb{Z})|$ denotes the number of invertible matrices of size $\tau \times \tau$ over $\mathbb{Z}/p\mathbb{Z}$, $|\operatorname{Mat}_{\tau\times\tau}(\mathbb{Z}/p\mathbb{Z})|$ denotes the number of $\tau \times \tau$ matrices over $\mathbb{Z}/p\mathbb{Z}$. Therefore, with high probability we can determine the value of $n_1, \ldots, n_\tau$ modulo p. If l is small, then it is feasible to compute the $\tau\,[l/2]$ points $a_iP, (a_i + p)P, \ldots, (a_i + ([l/2] - 1)p)P$ for $i = 1, \ldots, \tau$, where $[l/2] := \min\{b \in \mathbb{Z} \mid 2b \geq l\}$. Comparing them with P_i and $-P_i$ one can recover the value of n_i modulo n.

If r and s are chosen relatively small in comparison to the size n of the elliptic curve, then the computation of the matrices C_k, C_l and C is dominated by the task to find at least $3rs$ collisions, and this task has an expected complexity of $\mathcal{O}(\sqrt{rsn})$ point additions.

3.2 Solution of the matrix problem

We are giving the matrix M in block-form, with $A \in \operatorname{Mat}_{r\times r}(\mathbb{Z}/n\mathbb{Z})$, $C \in \operatorname{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z})$, and $B \in \operatorname{Mat}_{s\times s}(\mathbb{Z}/n\mathbb{Z})$. We are working under the assumption that both A and B are invertible. In fact, as we will see in the sequel we do not need this assumption in the analysis of the complexity of Problem 2.

We can regard the operation of associating C_i to C as a map

$$\begin{array}{rcl} -_i : \operatorname{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \operatorname{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z}) \\ C & \mapsto & C_i \end{array}.$$

The next lemma shows that the map distributes with respect to the sum.

Lemma 3.2. *For any $U, V \in \operatorname{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z})$ we have the identity*

$$(U + V)_i = U_i + V_i \quad \textit{for} \quad i \in \mathbb{N}.$$

Proof. Let

$$M_X = \begin{bmatrix} A & X \\ 0 & B \end{bmatrix}$$

for $X = U, V, U + V$. Then X_i is defined by

$$(M_X)^i = \begin{bmatrix} A^i & X_i \\ 0 & B^i \end{bmatrix},$$

hence $X_i = AX_{i-1} + XB^{i-1}$. We prove the thesis by induction on i. If $i = 1$, then

$$(U + V)_1 = U + V = U_1 + V_1$$

and the thesis is readily verified. Assume that $(U+V)_{i-1} = U_{i-1} + V_{i-1}$ and prove the analogous identity for i. We have

$$\begin{aligned}
(U+V)_i &= A(U+V)_{i-1} + (U+V)B^{i-1} \\
&= AU_{i-1} + AV_{i-1} + UB^{i-1} + VB^{i-1} \\
&= U_i + V_i.
\end{aligned}$$

□

In the next lemma we prove that applying the map $-_i$ commutes with multiplying copies of A on the left, and copies of B on the right. In fact, the same is true if we multiply on the left by a matrix that commutes with A and on the right by a matrix that commutes with B.

Lemma 3.3. *For any $U \in \mathrm{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z})$ and for any $j \in \mathbb{N}$, the following identities hold*

$$(A^jU)_i = A^jU_i, \qquad (UB^j)_i = U_iB^j.$$

Proof. Let

$$N = \begin{bmatrix} A & A^jU \\ 0 & B \end{bmatrix},$$

then $(A^jU)_i$ is defined by

$$N^i = \begin{bmatrix} A^i & (A^jU)_i \\ 0 & B^i \end{bmatrix}.$$

We prove the thesis by induction on i. If $i = 1$ then $(A^jU)_1 = A^jU = A^jU_1$, so the thesis is true. Assume that $(A^jU)_{i-1} = A^jU_{i-1}$ and prove the analogous identity for i. By direct computation, using the induction hypothesis, we obtain

$$\begin{aligned}
(A^jU)_i &= A(A^jU)_{i-1} + (A^jU)B^{i-1} \\
&= A(A^jU_{i-1}) + A^j(UB^{i-1}) \\
&= A^j(AU_{i-1} + UB^{i-1}) \\
&= A^jU_i.
\end{aligned}$$

We can obtain the second identity by a similar argument. □

In the next proposition we show how Problem 2 can be reduced to solving a linear system over $\mathbb{Z}/n\mathbb{Z}$.

Proposition 3.4. *Consider the linear system*

$$C_k = a_1C_1 + \cdots + a_{r+s-1}C_{r+s-1} \tag{5}$$

where $C_1, \ldots, C_{r+s-1}, C_k \in \mathrm{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z})$ are known, and $a_1, \ldots, a_{r+s-1} \in \mathbb{Z}/n\mathbb{Z}$ are the unknowns. The system has (at least) a solution. Any solution of (5) determines a homogeneous linear form $f_k(x_1, \ldots, x_{r+s-1}) = a_1x_1 + \cdots + a_{r+s-1}x_{r+s-1} \in (\mathbb{Z}/n\mathbb{Z})[x_1, \ldots, x_{r+s-1}]$ such that for all $l \in \mathbb{N}$ one has

$$(C_l)_k = f_k(C_l, (C_l)_2, \ldots, (C_l)_{r+s-1}).$$

Proof. Let $\chi_M(x) = \det(xI - M)$ be the characteristic polynomial of M. Since $\chi_M(M) = 0$, then there exist $\alpha_0, \dots, \alpha_{r+s-1} \in \mathbb{F}_p$ such that

$$M^k = \sum_{i=0}^{r+s-1} \alpha_i M^i.$$

Hence by definition

$$C_k = \sum_{i=0}^{r+s-1} \alpha_i C_i = \sum_{i=1}^{r+s-1} \alpha_i C_i,$$

since $C_0 = 0$. Then $(\alpha_1, \dots, \alpha_{r+s-1})$ is a solution of the linear system (5), in particular the system always has at least a solution.

Now let $(a_1, \dots, a_{r+s-1})$ be a solution of (5). We claim that for all $l \in \mathbb{N}$ one has

$$(C_l)_k = \sum_{i=1}^{r+s-1} a_i (C_l)_i.$$

The thesis is trivially verified for $l = 0$ since $C_0 = 0$. If $l = 1$ then $(C_1)_i = C_i$ for all i, and

$$C_k = \sum_{i=1}^{r+s-1} a_i C_i$$

since $(a_1, \dots, a_{r+s-1})$ is a solution of (5) by assumption. We proceed by induction on $l \geq 1$.

Assume that the thesis holds for $l-1$ and prove it for l. By induction hypothesis we have that

$$(C_{l-1})_k = \sum_{i=1}^{r+s-1} a_i (C_{l-1})_i.$$

Since $C_l = AC_{l-1} + C_1 B^{l-1}$, then by Lemmas 3.2 and 3.3 we have the following chain of equalities

$$\begin{aligned}
\sum_{i=1}^{r+s-1} a_i (C_l)_i &= \sum_{i=1}^{r+s-1} a_i \left(AC_{l-1} + C_1 B^{l-1}\right)_i \\
&= \sum_{i=1}^{r+s-1} a_i (AC_{l-1})_i + \sum_{i=1}^{r+s-1} a_i (C_1 B^{l-1})_i \\
&= \sum_{i=1}^{r+s-1} a_i A (C_{l-1})_i + \sum_{i=1}^{r+s-1} a_i (C_1)_i B^{l-1} \\
&= A \left[\sum_{i=1}^{r+s-1} a_i (C_{l-1})_i\right] + \left[\sum_{i=1}^{r+s-1} a_i (C_1)_i\right] B^{l-1} \\
&= A(C_{l-1})_k + C_k B^{l-1} \\
&= A(C_k)_{l-1} + C_k B^{l-1}
\end{aligned}$$

where the last equality follows from the fact that for each i, j one has $(C_i)_j = (C_j)_i$. Moreover, by definition one has that

$$A(C_k)_{l-1} + C_k B^{l-1} = (C_k)_l = (C_l)_k.$$

This completes the proof. □

Remarks 3.5.

- In the proof of Proposition 3.4 we do not need to make any assumption on the matrices A, B. In fact, we only require the existence of a polynomial $\chi_M(x)$ of degree smaller than or equal to $r+s-1$, with the property that $\chi_M(M) = 0$. Such a polynomial $\chi_M(x)$ always exists, since every square matrix over a finite filed has a minimal and characteristic polynomial. In particular, we do not need to assume that A and B are invertible.

- The system (5) may or may not have a unique solution. If the system does not have a unique solution, one of its solutions does not necessarily give us enough information to recover A^k or B^k, hence k (solving a DLP in a matrix group).

- The rank of the system (5), hence the dimension of the family of solutions of the system itself, is not relevant towards the goal of solving Problem 2. In fact, it follows from Proposition 3.4 that any solution of (5) enables us to compute $(C_l)_k$ from the knowledge of C_k and C_l. In practice, in order to simplify the computations it may be useful to choose a sparse solution for the linear system (5) whenever this is possible.

- A necessary condition for uniqueness of the solution of the system (5) is that M be non-derogatory (i.e. $\chi_M(x)$ is equal to the minimal polynomial of M).

The next corollary is a straightforward consequence of Proposition 3.4.

Corollary 3.6. *With the notation of Section 1 and of Proposition 3.4 one has*

$$(\Pi_l)_k = f_k(\Pi_l, (\Pi_l)_2, \ldots, (\Pi_l)_{r+s-1}).$$

4 Complexity Analysis

In this paper we analyzed the complexity of solving the Diffie-Hellman Problem, as arising from the Diffie-Hellman key-exchange proposed in [2]. The approach that we suggest in order to solve the problem is the following:

1. Use a modified version of the algorithm rho of Pollard and find matrices $C, C_k, C_l \in \mathrm{Mat}_{r\times s}(\mathbb{Z}/n\mathbb{Z})$ such that $CP = \Pi$, $C_k P = \Pi_k$, and $C_l P = \Pi_l$.

2. Compute $C_1, \ldots, C_{r+s-1}$, then find one solution $(a_1, \ldots, a_{r+s-1})$ of the linear system

$$C_k = a_1 C_1 + \ldots + a_{r+s-1} C_{r+s-1}. \tag{6}$$

3. Compute $(C_l)_k = a_1(C_l)_1 + \cdots + a_{r+s-1}(C_l)_{r+s-1}$.

4. Compute the secret key $(\Pi_l)_k = (C_l)_k P$.

We showed that the complexity of the first step amounts to solving $\tau = 3rs$ simultaneous DLP's in $E(\mathbb{F}_q)$ and the expected complexity is $\mathcal{O}(\sqrt{rsn})$.

The complexity of the second step amounts to the inversion of a $(r+s-1) \times (r+s-1)$ matrix over $\mathbb{Z}/n\mathbb{Z}$. When $n \gg r, s$ this complexity is polynomial in $\log n$. Similarly the third step is an easy linear algebra task. Finally the fourth step involves a number of costly point additions on the elliptic curve.

When $n \gg r, s$ the complexity of the first step dominates the complexities of the other steps. In this case the complexity of solving Problem 1 is at most $\mathcal{O}(\sqrt{rsn})$.

Instead of computing $3rs$ DPL's it is also possible to only find the matrices C and C_k by solving $2rs$ DPL's. Like in step 2 one finds $(a_1, \ldots, a_{r+s-1})$ satisfying (6).

Using the recurrence relation one then finds $(\Pi_l)_1, \ldots, (\Pi_l)_{r+s-1}$. From this the secret key $(\Pi_l)_k$ is readily computed as:

$$(\Pi_l)_k = a_1(\Pi_l)_1 + \cdots + a_{r+s-1}(\Pi_l)_{r+s-1}.$$

The advantage of this variant of the algorithm is that only $2rs$ DLP's have to be computed. The disadvantage is that many more point additions are required in order to compute $(\Pi_l)_k$. This variant is however faster in situations when r, s are small in comparison to n.

Acknowledgments

The first author would like to thank the University of Zürich for a pleasant stay in Zürich which provided the basis of this research. All authors would like to thank A. Barbour for pointing out Reference [6] and a referee at RWCA for helpful comments.

References

[1] A. D. Barbour, L. Holst, and S. Janson. *Poisson Approximation*, volume 2 of *Oxford Studies in Probability*. The Clarendon Press Oxford University Press, New York, 1992. Oxford Science Publications.

[2] J. J. Climent, F. Ferrández, J. F. Vicent, and A. Zamora. A nonlinear elliptic curve cryptosystem based on matrices. Applied Mathematics and Computation, In Press, Available online 27 June 2005.

[3] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[4] A. DasGupta. The matching, birthday and the strong birthday problem: a contemporary review. *J. Statist. Plann. Inference*, 130(1-2):377–389, 2005.

[5] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22(6):644–654, 1976.

[6] A. Hald. *A History of Probability and Statistics and their Applications before 1750*. Wiley Series in Probability and Mathematical Statistics: Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, 1990. A Wiley-Interscience Publication.

[7] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[8] F. Kuhn and R. Struik. Random walks revisited: extensions of Pollard's rho algorithm for computing multiple discrete logarithms. In *Selected areas in cryptography*, volume 2259 of *Lecture Notes in Comput. Sci.*, pages 212–229. Springer, Berlin, 2001.

[9] A. J. Menezes and Y.-H. Wu. The discrete logarithm problem in $\mathrm{Gl}(n, q)$. *Ars Combin.*, 47:23–32, 1997.

[10] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, Berlin, 1986.

[11] R. W. K. Odoni, V. Varadharajan, and P. W. Sanders. Public key distribution in matrix rings. *IEE Electr. Letters*, 20:386–387, 1984.