SCIENCE CHINA
Information Sciences

Evolutionary cryptography theory based generating method for a secure Koblitz elliptic curve and its improvement by a hidden Markov models

Chao WANG[1,*], HuanGuo ZHANG[2,3] and LiLi LIU[4]

Citation: SCIENCE CHINA Information Sciences **55**, 911 (2012); doi: 10.1007/s11432-012-4552-4

View online: https://engine.scichina.com/doi/10.1007/s11432-012-4552-4

View Table of Contents: https://engine.scichina.com/publisher/scp/journal/SCIS/55/4

Published by the Science China Press

SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

April 2012 Vol. 55 No. 4: 911–920
doi: 10.1007/s11432-012-4552-4

Evolutionary cryptography theory based generating method for a secure Koblitz elliptic curve and its improvement by a hidden Markov models

WANG Chao[1*], ZHANG HuanGuo[2,3] & LIU LiLi[4]

[1]*Key Lab of Specialty Fiber Optics and Optical Access Network, Ministry of Education, Shanghai University, Shanghai* 200072, *China;*
[2]*Computer School of Wuhan University, Wuhan* 430072, *China;*
[3]*Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan* 430072, *China;*
[4]*Huawei Technologies CO. LTD., Shanghai* 201206, *China*

Received August 25, 2010; accepted June 28, 2011

Abstract Considering potential attacks from cloud-computing and quantum-computing, it is becoming necessary to provide higher security elliptic curves. The hidden Markov models are introduced for designing the trace-vector computation algorithm to accelerate the search for elliptic curve (EC) base-points. We present a new algorithm for secure Koblitz EC generation based on evolutionary cryptography theory. The algorithm is tested by selecting a secure Koblitz EC over the field $F(2^{2000})$, with experiments showing that both the base field and base point of the secure curve generated exceed the parameter range for Koblitz curves recommended by NIST. The base fields generated go beyond 1900 bits, which is higher than the 571 bits recommended by NIST. We also find new secure curves in the range $F(2^{163})$—$F(2^{571})$ recommended by NIST. We perform a detailed security analysis of those secure curves, showing that those we propose satisfy the same security criteria as NIST.

Keywords secure EC selection, evolutionary cryptography theory, ant colony algorithm, Koblitz EC, HMM

Citation Wang C, Zhang H G, Liu L L. Evolutionary cryptography theory based generating method for a secure Koblitz elliptic curve and its improvement by a hidden Markov models. Sci China Inf Sci, 2012, 55: 911–920, doi: 10.1007/s11432-012-4552-4

1 Introduction

Elliptic curve cryptography (ECC) has gradually been included in standards issued by IEEE, ANSI, ISO, NIST and others, and may replace RSA in the future. There are only 30 secure curves recommended by international standards organizations, of which 15 curves were recommended by NIST.

In [1], Zhang get all proposed the concept and design methods for evolutionary cryptography theory by introducing the law of natural biological evolution. This led to several achievements not only in cryptographic design, such as the design of new S-boxes for data encryption standards (DES), bent functions, hash functions and automatic design of cryptographic protocols, but also in cryptanalytic

*Corresponding author (email: wangchao@staff.shu.edu.cn)

areas such as sequence cryptanalysis [1–5]. Evolutionary cryptography theory is different from traditional cryptography methods and has become a principal framework for automatic cryptography design and cryptanalysis.

Based on evolutionary cryptography theory, the current authors proposed a new method for selecting secure Koblitz ECs [6], and tested the method by selecting secure Koblitz ECs over the field $F(2^{800})$ [7], which is beyond the parameter range recommended by NIST for Koblitz curves. This experiment and theoretical analysis also show that evolutionary cryptography theory can successfully design public key cryptosystems.

Although the attacks on ECC don't exceed the First Energy Level proposed by the Certicom Company, which is the NIST definition for cloud-computing [8], it is obvious that a hacker could mount a powerful attack with the high-performance computing ability of cloud-computing. Further, the 128 Qbit commercial quantum computing system offered by D-Wave, a Canadian company that partnered with Google to develop software for recognizing automobiles within images, makes powerful attacks from quantum computing systems possible. Thus it is necessary to find ECC curves with security levels higher than the current NIST recommendations.

However, further analysis indicates that it is difficult to select the base point of a secure ECC curve and that it is not useful to produce more secure ECC curves. This paper introduces a hidden Markov models (HMM) to design the trace-vector computation algorithm for accelerating the search for elliptic curves base-points, and a new algorithm for secure Koblitz EC generation based on evolutionary cryptography theory is presented.

2 Development of secure EC selected and recommended by NIST

2.1 Secure ECs recommended by NIST

In 2000, NIST published FIPS 186-2 [9], which recommended 15 secure ECs. Koblitz ECs involve the fields $F(2^{163})$, $F(2^{233})$, $F(2^{283})$, $F(2^{409})$, $F(2^{571})$, for which NIST gives the base-points. The 15 curves recommended by NIST have been frequently used in current engineering applications [10, 11].

2.2 Development of overseas secure EC selecting

At present, secure EC selection methods can be separated into two types: complex multiplication (CM) methods and random curve selecting methods. No superior approach has been proposed in recent years. The SEA algorithm is still the most secure but it is a time-consuming method, and traditional pure mathematics severely restricts the development of ECC.

CM selects ECs based on a given order, and implementation is relatively fast. But the ECs generated by this method have a specific structural feature which is a potential security threat. The random selection method has no such shortcoming, and thus is usually chosen to select secure ECs. The security of an EC depends on its order. Common methods for computing the order include Schoof's algorithm [12], SEA (Schoof-Elkies-Atkin) algorithm [13], Satoh's algorithm [14, 15], Fouquet's algorithm [16], SST algorithm [17], AGM algorithm [18], and MSST algorithms [19]. In addition, for special ECs, such as Koblitz EC, characterized by small prime numbers there is a simpler method for computing the order using Weil's Theorem. The security of these kinds of ECs mainly depends on the size of a safe base field.

3 Evolutionary cryptography and secure Koblitz ECs

We propose a new algorithm for secure EC selection based on evolution cryptography [6,7], and succeed in finding the secure base field of Koblitz curves using ant colony optimization (ACO), showing that evolution cryptography is also applicable in the field of public-key cryptography.

3.1 Koblitz EC

In 1996, Dorigo [20] published a ground-breaking paper applying the ant colony algorithm to a combinatorial optimization problem. His paper pointed out that the ant colony model has the properties of positive feedback, distributed computation and greedy search, where positive feedback explains the rapid optimization, and distributed computation and greedy search can avoid premature convergence. At present, ACO has succeeded at the traveling salesman problem (TSP) and the quadratic assignment problem (QAP).

We design an ant colony model for finding a safe general field by transferring the application to TSP. This model is similar to the max-min ant system (MMAS) [21]. The most striking feature of this model is that it avoids premature convergence by limiting the size of pheromone to an appropriate range.

Step 1. Parameter initialization. Set $\alpha = 1$, $\beta = 5$. They pay more attention to the role of heuristic information in the exploration. Pheromone evaporation factor is $\rho = 0.02$. Experiments show that ρ must be small to avoid rapid convergence of the ant colony algorithm. An ant k at the point i chooses point j as the next access point according to a pseudo-random proportional rule. The rule is described by the following mathematical equation:

$$j = \begin{cases} \arg\max\{\tau_i[\eta_i]^\beta\}, & \text{if} \quad q \leqslant q_0, \\ J, & \text{otherwise}, \end{cases}$$

where q is a random variable distributed homgeneously in the interval [0, 1], and $q_0 (0 \leqslant q_0 \leqslant 1)$ is a parameter. After each iteration of MMAS, only an optimal ant is chosen to carry out global updating:

$$\tau_i \leftarrow (1-\rho)\tau_i + \Delta\tau_i^{\text{best}}.$$

Step 2. At the start of the iteration, five ants are randomly placed at different points. When an ant arrives at a point, it determines whether the order of the point is a large prime number using the objective function. The ant then chooses the next point according to the construction of the model. At each step, all ants need to conduct a local update, but at the end of the iteration, only one optimal ant is chosen to carry out the global update.

3.2 Experiment results

(1) We obtain a secure EC base field larger than 700 bits (PC takes 3.5 h), which exceeds the 571 bits base field published by the NIST. There are seven base fields whose size is larger than 163, such as the Koblitz curve $E_1 : y^2 + xy = x^3 + x^2 + 1$, for which the order n of the 701 bits base field $k = 2^{701}$ is n=5260135901548373507240989882880128665 5503398028231738594982809030687321542970808221136665362775884512269800074472057387507859154454647132730530677414059685643347943137538780328160843027566494017560570612400380 11.

(2) For comparison, details of our curve and the Koblitz curve recommended by NIST are included in Figures 1 and 2.

3.3 Further analysis

To find the base-point, it is necessary to solve the quadratic equation $z^2 + z + c = 0$. We use the concept of the "trace" to judge quickly whether or not this equation has a root. Assume that α is an element of the domain, so that $\alpha \in \text{GF}(2^m)$. Then the trace of α is defined as $\text{Tr}(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \cdots + \alpha^{2^{m-1}}$. In the binary domain, where $\text{Tr}(c)$ is either 0 or 1, a trace of 0 means that the quadratic equation is solvable while if the trace is 1 the equation is unsolvable.

The most common algorithm for computing the trace is in the following:

INPUT: $a \in \text{GF}(2^m)$

OUTPUT: $T = \text{Tr}(\alpha)$

1 $T \leftarrow \alpha$

2 For I from 1 to $m-1$

  $T \leftarrow T^2 + \alpha$

3 Return T

m	571
a	0
$p(t)$	t571+t10+t5+t2+1
h	4
n	1932268761508629172347675945465 9936721494636648532174993286176 2572575957114478021226813397852 2706711834706712800825351461273 6749740666173119296824216170925 03555733685276673
Gx	0x 69E 202A 15A4 739E 0FEE ECDA 1B17 1AB0 7AC0 8EC3 6369 7701 8FCF 52D2 BF79 7DFD 9E29 19EE A954 1D83 2EE8 E37D DC92 7003 79F5 CBDB F146 8B63 582F ECAB DADA 8AD9 4A21 EF89 4D82 F454
Gy	0x 28C 3E1D 87E3 0527 4B9A C627 9532 E328 BE6A 607C AB08 9FC3 4300 8E22 E46E 9ADD 451D FCBF 8798 E765 A443 40D9 195B 0DBE 98B0 8B95 D737 57AF 5B0E BDD1 CF13 DAD6 DC8A 3D5E A7FF 0A71
Average time	16 min

Figure 1 Our secure curve.

	Curve K-571
a	0
$p(t)$	t571 + t10 + t5 + t2 + 1
n	1932268761508629172347675945465 9936721494636648532174993286176 2572575957114478021226813397 8522706711834706712800825351461 2737647497406661731192968242161 7092503555733685276673
Gx	0x26eb7a859923fbc82189631f8103f e4ac9ca2970012d5d4602480480184 1ca44370958493b205e647da304db4 ceb08cbbd1ba39494776fb988b4717 4dca88c7e2945283a01c8972
Gy	0x349dc807f4fbf374f4aeade3bca953 14dd58cec9f307a54ffc61efc006d8a2 c9d4979c0ac44aea74fbebbb9f772ae dcb620b01a7ba7af1b320430c85919 84f601cd4c143ef1c7a3

Figure 2 Secure curve recommended by NIST.

The trace can also sometimes be calculated by the following method. We introduce an m-dimensional vector Trace_Vector= $\{t_{m-1}, \ldots, t_1, t_0\}$, where $t_i = \mathrm{Tr}(2^i), i = 0, 1, \ldots, m-1$. We have the equation $\mathrm{Tr}(\alpha) = \alpha \& \mathrm{Trace}$.

According to the experimental results, the latter method is better. No matter what value is chosen for 'α', as long as the value of m is invariant, the value of the trace-vector remains unchanged. As long as we know the corresponding trace-vector for m, an arbitrary value for α can be calculated simply using the formula described above, without repeating the former algorithm each time.

Calculating the trace-vector is a very time-consuming process. As m increases, the computational time grows exponentially. Using a configured work station (CPU: AMD Semipro 2800+/RAM: 256 MB), the experimental results show that calculating the trace-vector for m=409 should take about 1 h and calculating the trace-vector for m=571 needs about 13.8 h. Therefore, for larger values of m, a high-precision algorithm is not applicable in practice.

4 Base point rapid generating algorithm based on HMM

The HMM [21] is a probability model that has mainly been used in statistical learning and that has good predictive abilities. According to the theory of HMM, the sequence of states is a Markov chain because the choice of the next state depends only on the current state. However, this state sequence is not observed but is hidden, and only the symbol sequence that these hidden states generate is observed. The most likely state sequence must be inferred from an alignment of the HMM to the observed sequence.

4.1 Design of HMM

Due to the reduced polynomial are known, so it can be used as observations. The trace vector is the state value. We design two random HMM processes as Figure 3.

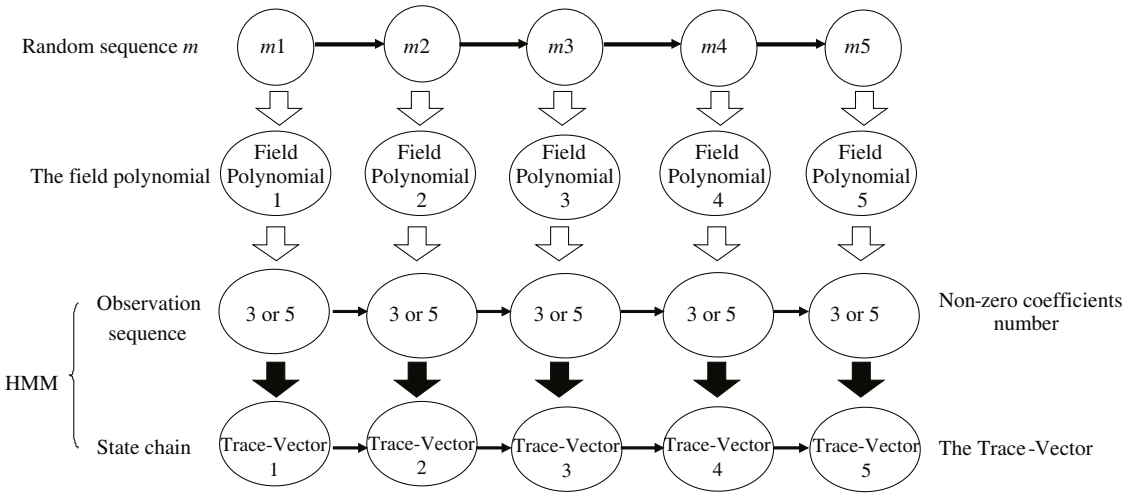

Figure 3 HMM.

4.2 HMM parameters definition

N: The state number of the Markov chain in the model, in this case $N = 3$; q_t is the state at time t. The three state values are:

θ_1 : The trace-vector is equal to 0x1;

θ_2 : The trace-vector is equal to the front part of the field polynomial;

θ_3 : The trace-vector is equal to the front part of the field polynomial with a few bits attached at a high level.

M: Each state corresponds to the number of observations that may occur, with $M = 2$; o_t is a observation at time t. The two possible observations are:

V_1 : The field polynomial has 3 non-zero coefficients;

V_2 : The field polynomial has 5 non-zero coefficients.

π : The initial state vector is the probability of selecting some kind of trace vector in the model at the start of the experiment.

$\pi = (\pi_1, \pi_2, \pi_3)$, where $\pi_i = P(q_1 = \theta_i)$, $1 \leqslant i \leqslant N$.

A : State transition probability matrix $A = (a_{ij})_{3\times 3}$, where $a_{ij} = P(q_{t+1} = \theta_j | q_t = \theta_i), 1 \leqslant i, j \leqslant N$.

This matrix gives the transition probability from trace vector θ_i to trace vector θ_j in the model.

B : Observations probability matrix $B = (b_{jk})_{N\times M}$, where $b_{jk} = P(o_t = V_K | q_t = \theta_j), 1 \leqslant j \leqslant N, 1 \leqslant k \leqslant M$.

This matrix gives the probability of having V_k (3 or 5) field polynomial coefficients in the model when trace vector θ_j occurs.

Therefore, the HMM can be written as $\lambda = (N, M, A, B, \pi)$, and can be abbreviated as $\lambda = (A, B, \pi)$.

4.3 Calculation process for predicting trace-vector though HMM

(1) HMM initialization.

According to the above data we know: 8 sets of data are in state θ_1, 4 sets of data are in state θ_2, 13 sets of data are in state θ_3. The whole state sequence is a random process, so we can get the approximate state transition matrix and initial state probabilities:

$$A = \left\{ \begin{array}{ccc} 0.32 & 0.16 & 0.52 \\ 0.32 & 0.16 & 0.52 \\ 0.32 & 0.16 & 0.52 \end{array} \right\}, \quad \pi = \{ \begin{array}{ccc} 0.32 & 0.16 & 0.52 \end{array} \}.$$

In addition, for θ_1 there are 6 data points with 3 non-zero polynomial coefficients and have 2 with 5 non-zero coefficients; for θ_2, all 4 data points have 3 non-zero coefficients, and for θ_3 all data points have 5 non-zero coefficients. This gives the following observations probability matrix:

$$B = \begin{Bmatrix} 0.75 & 0.25 \\ 1 & 0 \\ 0 & 1 \end{Bmatrix}.$$

(2) HMM parameter training.

The observation sequence is a random process chain in which 25 data points, {13, 17, 19, . . . , 409, 571}, are randomly divided into five groups each containing 5 elements. The following figure shows a random grouping and the corresponding observation sequence:

$$\begin{aligned}
&(83,\ 109,\ 359,\ 277,\ 41) \Rightarrow (V_2 \quad V_2 \quad V_1 \quad V_2 \quad V_1),\\
&(113,\ 103,\ 13,\ 331,\ 409) \Rightarrow (V_2 \quad V_1 \quad V_2 \quad V_2 \quad V_1),\\
&(347,\ 101,\ 233,\ 19,\ 97) \Rightarrow (V_1 \quad V_2 \quad V_2 \quad V_2 \quad V_2),\\
&(23,\ 131,\ 107,\ 571,\ 311) \Rightarrow (V_2 \quad V_2 \quad V_1 \quad V_2 \quad V_1),\\
&(349,\ 329,\ 283,\ 163,\ 17) \Rightarrow (V_1 \quad V_1 \quad V_2 \quad V_2 \quad V_1).
\end{aligned}$$

The HMM is trained using (83, 109, 359, 277, 163). The first training results are

$$A = \begin{Bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0.28 & 0.38 & 0.33 \end{Bmatrix}, \quad B = \begin{Bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{Bmatrix}.$$

Similarly, the observed sequences for the other four groups are trained to give the final HMM parameters:

$$A = \begin{Bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0.25 & 0.25 & 0.5 \end{Bmatrix}, \quad B = \begin{Bmatrix} 0.9 & 0.1 \\ 1 & 0 \\ 0 & 1 \end{Bmatrix}.$$

After the training process has been completed, the model can predict the trace vector for larger values of m.

(3) Predicted trace vector using HMM.

The sequence (701,1153,1249,1597,1913) corresponds to the observation values $(V_2, V_1, V_1, V_2, V_1)$. The observation values are substituted into the HMM to find the state sequence with the largest probability using the Viterbi algorithm. The state sequence found is $(\theta_3, \theta_1, \theta_1, \theta_3, \theta_2)$.

- For θ_1, we can directly predict that the trace-vector is 0x1, as in the cases m=1153 and 1249.
- For θ_2, we can predict that the trace-vector is equal to the front part of the field polynomial.

The field polynomial for m=1913 is 0x2000400000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001.

The predict trace-vector is 0x8001.

The case for θ_3 is more complicated. For simplicity, because we were unable to predict them, the high levels of the trace-vector are considered to be zero.

The field polynomial for $m = 701$ is 0x2000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000010015.

The predicted trace-vector is 0x20000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001.

The field polynomial for $m = 1597$ is 0x2000400d.

The predicted trace-vector is 0x8001.

Analysis The trace-vector generated by the above model is only an approximation of the actual result, and there may be some difference between them. The most direct reason for these errors is an incorrect decision when solving the quadratic equation $z^2 + z + c = 0$. In other words, some points which are not in the cyclic group are considered to be in it, making the $kP = O$ test invalid and wasting a lot of computational resources. To make analysis easier, the Hamming distance could be used to indicate this type of error. Experimental results show that the Hamming distance should be no more than 3.

5 Experimental results

The hardware device is PC, which its CPU is AMD Sempron 2800+ and its RAM is 256 MB, while the software platform is Microsoft Visual C++ 2005.

(1) We search for secure base fields for both kinds of Koblitz ECs over $\left[2^{163}, 2^{2000}\right]$, and find a secure EC base field exceeding 1900 bits (5 h), which is larger than the largest recommended by NIST.

- For Koblitz ECs with $a = 0$, $b = 1$, there are more than 9 secure base fields, including 2^{1913}.
- For Koblitz ECs with $a = 1$, $b = 1$, there are more than 10 secure base fields, including 2^{701}.

(2) From part (1), we obtain enough secure base fields. Then we combine the HMM above to accelerate the search for base-points, and find all base-points for the different secure base fields above. We report the base field parameters and base-point parameters for secure Koblitz ECs over $\mathrm{F}(2^{1913})$ (Table 1).

6 Security analysis

According to our information, the U.S. NIST Digital Signature Standard FIPS 186-2 and FIPS 186-3 do not explicitly state the security guidelines used to recommend secure EC parameters. In FIPS 186-3, it is mentioned that the method used to generate curve parameters is the same as in ANSI X9.62, so the guidelines NIST use are at least the same as in AISI X9.62. The following are the guidelines mentioned in ANSI X9.62, and we also list the corresponding guidelines used in our experiment.

- The order $\#E(\mathrm{GF}(q))$ is divisible by a large prime $n > 2^{160}$.

If $\#E(\mathrm{GF}(q))$ for the selected ECC curves has a prime factor larger than 2^{160}, the square root attack method (baby step/giant step, Pollard-ρ) is invalid for the curve, and the Pohlig-Hellman attack also can be avoided.

We select a safe base field in the range 2^{163} to 2^{2000}. As the order of the EC is the same to the

Table 1 The parameters, base points and computation time for the evolutionary computing experiments to find a secure base field with $m = 1913$

m	1913
a	0
$P(t)$	t1913 + t462 + 1
h	4
n	1854905179312287918075583275310253320130712317083693686382831178331741529037031911623159910318771582347127907195077732409786694854454271860823301532849986915566161378680316362858339353430424909079230651033188901993700410316057018783071792693641756073577136786578341583341708144895627481715293910951050208044662130734050634412444538075852058928127051474378809227569635054287482828860058338975911755934640281128910856977249191069538500634179279407842899958058954181228580057928571643944817300556265360473255013692615332126062867124167282393858362186809054179818256521745459113 43
Gx	0x171AE2E4006571ED0FC82A2EF714ABA236FE448D044B2BC749AF4B8C04EE882F8DFDEE4001F34E9BCD4A1F38E1822D10A822F8BA360D5FE27FC6B4877E544512885C00705D3199A48E0C9F3F558E90F09171A4A157AFEE940EE7BE528D36CC7C6E69266BEAF137096197C411FBFF86142A2AF4A4E1172BCD167DD09FE3F3B0759CB8B9C3B3BEE8EE03ADC792D9F05FCAA75DF356843B6B2962317FC94AF5E1ACFDDD215234BD7D6FA5E4B87A740BA0791639B286BE0B8735438B13D732ACFA8E41818A1C824D8170323937B93BDE6705C021C38B5ABF2BDACD6668BFAE0937526A550F3A99E380C724428CE0F825AFA
Gy	0x9C3C42689601F773755657361F05D7B4EDAC6F75DBEBB9CC5228E82D31CB1F673405745CB34F169BDF04A1FD2F7A2CA71D7957FFDCC3F6CF07CDCD7D04E7CAB98AE66A76FFAA764EF676107A26040FF0389ECD699BBD4044E553DF38BAA7A0C28C8C711C6F2FBCB72DE91CD9145AB4249C57A8EBA3309DA372519558719E5C0814E649D59A0DAC36A73A7928C85B60C8854C99AF793A8B3D808A2EC6C34141110568E0D4AEDB1F11B82197297FA4D96FCAD54D69783DC9599D9ED88DE0FCAAFB45A2BE9E9284E1F20D0E354292934EDDE6EEA1585E82EF70C198E8A92ED7F5DA7672DA9CECF835645A23CBCA25585B
Time	3.3 h

magnitude of base field, if is also in the range 2^{163} to 2^{2000}. In addition, the cofactor is limited to at most 4, which can be seen from the formula:

$$\text{base} - \text{point order} = \text{EC order} \div \text{Cofactor}.$$

So the base-point order must be in the range 2^{161} to 2^{1998}, and its magnitude must be at least 2^{160}.

• The MOV condition holds.

To resist the MOV attack, the requirement that $q^i \neq 1 \bmod n$ (where $i = 1, 2, \ldots, \log_2(q/8)$, and n is the order of the base-point) must be met. Namely, super-singular ECs should not be selected.

Experimental results show that the MOV attack is effective only for a small proportion of ECs. We take this into account for the remainder of this paper. As MOV detection is only related to the base field and the base-point order, we should carry out detection after calculating the order rather than after calculating the base-point. Base-point orders are processed as shown in Figure 4.

We send these base field p=2^m(m=163, 223, 239, 277, 283, 311, 331, 347, 349, 359, 409, 571, 701, 1153, 1249, 1597, 1621, 1913), selected previously, and the corresponding base-point order n to the detection model. The results show that the above base fields are not vulnerable to the MOV attack, and therefore the EC parameters for the above base fields are secure.

• The anomalous condition holds.

Theoretically, to resist the SSSA attack, the base-point order should not be equal to the base field order. Actually, the base field of a Koblitz EC has characteristic 2, so when the base-point order is equal to the base field order, it is certainly not a prime number. Hence, it is unnecessary to consider this attack when selecting a safe Koblitz EC.

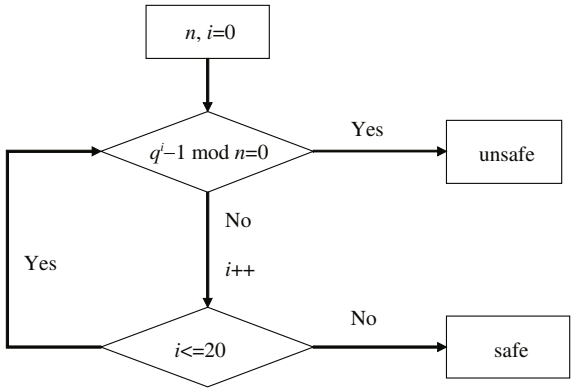

Figure 4 MOV detection model.

• Furthermore, to guard against possible future attacks on special classes of non-super-singular curves, it is prudent to select an EC at random.

In this paper, we are concerned with Koblitz ECs, for which the random problem does not exist. In addition, we take into account that the Weil descent attack (GHS attack) is the same as the MOV attack that is effective for a small proportion of ECs. Menezes and others studies have shown that, if we set the parameter m from the base field 2^m to be a prime number, the GHS attack becomes difficult to achieve. Hence, we only take into account prime numbers between 160 and 2000. From the final results, we can clearly see that the parameters $m = 163, 233, \ldots, 1913$ found to be prime numbers.

• The problem of cofactors.

Furthermore, FIPS 186-3 clearly pointed out that ANSI X9.62 (1998) did not take into account the size of cofactors while generating curve parameters. FIPS 186-3 states the maximum value which each cofactor can achieve for different base fields. Meanwhile, it also points out that smaller cofactors are better. The cofactors for the Koblitz ECs we studied are usually equal to 2 or 4, so they are small enough.

To summarize, the algorithm in this paper has the same safety criteria as the NIST recommended curves. Therefore, the curves presented in this paper cover the 5 secure Koblitz ECs released by NIST. Over this base field, we also found other secure EC with adequate security. This research extends the scope of secure base fields by an order of magnitude.

7 Conclusions and outlook

Based on ideas from evolutionary cryptography and HHMs, this paper proposes a new algorithm for selecting secure Koblitz ECs. We have completed a preliminary base field and base point generating experiment for Koblitz ECs, which generated secure Koblitz ECs over $\left[2^{163}, 2^{2000}\right]$, and obtained the same 5 Koblitz ECs recommended by NIST. Furthermore, we have found new secure Koblitz ECs larger than 2^{571}.

This paper reports a successful application of the evolutionary cryptography approach to public-key cryptosystem. Theoretical analyses and experimental results show that evolutionary cryptography is effective for public-key cryptosystems and symmetrical cryptosystems.

The algorithm, which has the same safety standards as the secure ECs recommended by NIST, can resist current attacks. The evolutionary cryptography approach has greater flexibility for designing objective functions and is suitable for further security developments.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grand Nos. 60970006, 60970115, 91018008), Key Laboratory Open Fund of Sky Information Security and Trusted Computing (Grand No. AISTC20-

09_04), and Shanghai Key Subject and Committee of Science and Technology of Key Laboratory (Grand Nos. S30108, 08DZ2231100).

References

1 Zhang H G, Feng X T, Tan Z P. Evolutionary cryptography and the evolutionary design for DES. J Commun, 2002, 5: 57–64
2 Meng Q S, Zhang H G, Wang Z Y, et al. Designing bent functions using evolving method. Acta Electron Sin, 2004, 11: 1901–1903
3 Wang Z Y, Li B, Zhang H G. Research on security of Hash functions. Comput Engin Appl, 2005, 12: 18–19
4 Wang Z Y, Li L, Zhang H G. Automatic design approach of security protocols. Comput Engin Appl, 2005, 12: 16–17
5 Chen L J, Zhao Y, Zhang H G. Cryptanalysis for stream cipher based on evolutionary computation. Comput Appl, 2008, 8: 1912–1915
6 Zhang H G, Wang C, Shi X Y, et al. Fast Generating Algorithm for ECC Secure Cure Based on Evolutionary Computation. China Patent, 200910200504. 2010-5-26
7 Wang C, Zhang H G, Liu L L. The experiment of Koblitz elliptic curves generating based on evolutionary cryptography theory and verifying the parameters recommended by NIST. China Commun, 2011, 8: 41–49
8 Dustin O. Securing elasticity in the cloud. Commun ACM, 2010, 53: 46–51
9 NIST. Digital Signature Standard. Federal Information Processing Standards Publication, 2000
10 Brown M, Hankerson D, Lopez J, et al. Software implementation of the NIST elliptic curves over prime fields. In: Topics in Cryptology – CT-RSA 2001, Proceedings Lecture Notes in Computer Science, 2001. 250–265
11 Guneysu T, Paar C. Ultra High Performance ECC over NIST Primes on Commercial FPGAs. In: Lecture Notes in Computer Science. Berlin/Heidelberg: Springer, 2008. 62–78
12 Schoof R. Elliptic curves over finite fields and the computation of square roots mod P. Math Comput, 1985, 44: 483–494
13 Elkies N D. Elliptic and modular curves over finite fields and related computational issues. Comput Perspect Number Theory, 1998, 7: 21–76
14 Satoh T. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J Raman Math Soc, 2000, 15: 483
15 Satoh T. On p-adic point counting algorithms for elliptic curves over finite fields. In: Algorithmic number theory, 5th international symposium, ANTS-V, Sydney, 2002. LNCS 2369. 43–66
16 Fouquet M, Gaudry P, Harley R. An extension of Satoh's algorithm and its implementation. Raman Math Soc, 2000, 15: 281
17 Satoh T, Skjernaa B, Taguchi Y. Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Field Their Appl, 2003, 9: 98–101
18 Satoh T. On p-adic point counting algorithms for elliptic curves over finite fields. In: Algorithmic number theory, 5th international symposium, ANTS-V, Sydney, 2002. LNCS 2369. 43–66
19 Gaudry P. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. In: Asiacrypt 2002. LNCS 2501. 311
20 Dorigo M, Maniezzo V, Colorni A. Introduction to natural algorithms. Rivista Inform, 1994, 24: 179–197
21 Colorni A, Dorigo M, Maniezzo V. An investigation of some properties of an ant algorithm. In: Proceedings of the Parallel Problem Solving from Nature Conference (PPSN 92). Elsevier Publishing, 1992. 509–520