University of Craiova
Faculty of Sciences
Doctoral school of Sciences

Doctoral thesis

Resume

Author:
Alin Ionuț GOLUMBEANU

Scientific coordinator:
Prof. Univ. Ph.D. Vicenţiu RĂDULESCU

Craiova, 2018

University of Craiova
Faculty of Sciences
Doctoral school of Sciences

Optimizations on differential systems of cryptographic analysis for models which are based on nonsupersingular elliptic curves.

Author:
Alin Ionuț GOLUMBEANU

Scientific coordinator:
Prof. Univ. Ph.D. Vicenţiu RĂDULESCU

Craiova, 2018

Thesis resume

The entire path of development of an differential cryptographic system reveals the beauty of pure mathematics and illustrates its applicability with real results in improving some parameters which have an important role in the final version of an cryptographic analysis system.

In the 1'st chapter we have the first step in the construction necessary for nonlinear asymmetric system, this being the study of the subspaces over which the nonsupersingular elliptic curves will be defined. In this regard, we start from the existing models and highlight the limitations, then we illustrate the particular subspaces which will be used in the developments from the next chapters. Let a a rational number which can be written as $a = q^m \frac{r}{s}$; $r \nmid q^k$, $s \nmid q^k$ and $a \neq 0$. We assign $\mathrm{ord}_{q^k}(a) = m$ and obtain the following rule:

$$\mathrm{ord}_{q^k}(a+b) \geq min\{\mathrm{ord}_{q^k}(a), \mathrm{ord}_{q^k}(b)\},$$

as an equality, excepting the case $\mathrm{ord}_{q^k}(a) = \mathrm{ord}_{q^k}(b)$.

In the same manner for $a \in \mathbb{F}_{q^k}$, we assign $\mathrm{ord}_{q^k}(a) = m$ if $a \in (q^k)^m \mathbb{Z}_{q^k}$ $(q^k)^{m+1}\mathbb{Z}_{q_k}$. This rule also applies for the two definitions of ord_{q^k} sustain $\mathbb{F}_{q^k}$. In both cases we assigned $\mathrm{ord}_{q^k}(0) = \infty$. We keep in mind that ord_{q^k} is an homeomorphism $\mathbb{F}_{q^k}^{\times} \to \mathbb{Z}$.

$E(\mathbb{F}_{q^k})$ has a compact topology and $E^0(\mathbb{F}_{q^k})$ is an open subset. Since $E(\mathbb{F}_{q^k})$ is a subsets union of $E^0(\mathbb{F}_{q^k})$, will result that there is only a finite set which fulfills the requirements.

Let $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ the topology result , $F_{q^k}^3 \backslash \{0,0,0\}$ the topology subset and $\mathbb{P}^2(\mathbb{F}_{q^k})$ the topology coefficient from $F_{q^k}^3 \backslash \{0,0,0\} \to \mathbb{P}^2(\mathbb{F}_{q^k})$. We have that $\mathbb{P}(\mathbb{F}_{q^k})$ is an association of images for subsets type $\mathbb{Z}_{q^k}^{\times} \times \mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k}$, $\mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k}^{\times} \times \mathbb{Z}_{q^k}$, $\mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k}^{\times}$, each one being compact and open then $\mathbb{P}^2(\mathbb{F}_{q^k})$ is compact. The subset $E(\mathbb{F}_{q^k})$ is closed because its the null set of an polynomial.

In relation to this topology on $\mathbb{P}(\mathbb{F}_{q^k})$, two points which are close will have the same reduction module q^k. So $E^0(\mathbb{F}_{q^k})$ is the space intersection $E(\mathbb{F}_{q^k})$ with an open subset from $\mathbb{P}^2(\mathbb{F}_{q^k})$.

It can be easily proven that reduction relation $E^0(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$ is surjective and is defined on the core $E1(\mathbb{F}_{q^k})$.

We assume that $E^n(\mathbb{F}_{q^k})$ is a subgroup from $E(\mathbb{F}_{q^k})$. If $\Omega = (x : y : 1)$ is in $E^1(\mathbb{F}_{q^k})$ then we will have $y \notin \mathbb{Z}_{q^k}$. Let $x = q^{-m}x_0$ and $y = (q^k)^{-m'}y_0$ with x_0 and y_0 from $\mathbb{Z}_{q^k}$.

Then

$$(q^k)^{-2m'}y_0^2 = (q^k)^{-3m}x_0^3 + ap^{-m}x_0 + b$$

From here the subspaces have been developed over which nonsupersingular elliptic curves are defined, which have as the base property the fact that the majority of points with cryptographic interest are proven that they are contained.

In the 2nd chapter, starting from the limitations of the existing systems, for particular cases needed in real implementation, we studied the possibility of extending the studies from the article [154], for the case of two users, we extended the study for the case of an group of users which use low performance devices. But my studies did not consist of reducing the complexity by optimizing the algorithms implementations, but through elaborating a mathematical model by taking into consideration the partitioning of a space over which are defined a set of particular elliptic curves, by this reducing the time needed to compute the parameters. Still maintaining the same Linear Equivalent Complexity of attack, achieved by way the space was partition over which the particular elliptic curves are defined.

The results were published in [60], [61], [62], [31].

In this regard, we developed a model of elliptic curves used in the particular system, described more in depth in the thesis.

Therefore, let E an elliptic curve defined as

$$Y_2 + \gamma_1 XY + \gamma_3 Y = X^3 + \gamma_2 X^2 + \gamma_4 X + \gamma_6$$

and $A_1 = (\omega_1, \eta_1)$, $A_2 = (\omega_2, \eta_2)$ two points on an elliptic curve defined in the described manner.

In this manner we can state that:

$$-A_1 = (\gamma_1, -\eta_1 - \gamma_1\omega_1 - \gamma_3)$$

where γ_6 is defined as nonlinear combination obtained from the start parameters used in encryption. From here we obtain

$$\lambda = \frac{\eta_2 - \eta_1}{\omega_2 - \omega_1}$$

și

$$\gamma = \frac{\eta_1\omega_2 - \eta_2\omega_1}{\omega_2 - \omega_1}$$

where ω_1 and ω_2 satisfy the condition $\omega_1 \neq \omega_2$, which allowed to develop the next result:

$$\lambda = \frac{3\omega_1^2 + 2\alpha_2\omega_1 + \alpha_4 - \alpha_1\eta_1}{2\eta_1 + \alpha_1\omega_1 + \alpha_3}$$

și

$$\gamma = \frac{-\omega_1^3 + \alpha_4\omega_1 + 2\alpha_6 - \alpha_3\eta_1}{2\eta_1 + \alpha_1\omega_1 + \alpha_3}$$

An elliptic curve was defined over an subfraction of $\mathbb{F}_q$, in the following manner: $E(\mathbb{F}_{q^k})$. The curve can be easily deducted, it will contain m^2 points of order m, where m will divide q^k-1, because having $E(m)\times E(m)\to\gamma_m$ where γ_m is a group of roots of order m of the unit, in K, will deduct the relation $div(g)=\sum\limits_{D\in E(m)}(B_1'+D)-(D)$ with $B'\in E(\bar{K})$, which fulfills the condition $[m]B'=B$. But, as stated in [11], we can have e_m as being:

$$e_m=\begin{cases} E(m)\times E(m)\to\gamma_m \\ (B_1,B_2)\to\frac{g(X+B_1)}{g(X)}\end{cases}$$

so the subspace determined by the fraction m will fulfill the expressed property, as stated in the formula and g will satisfy $g^2-[t]g+[q]=[0]$.

Starting from the definition of the hierarchical communication access model [29] we will define a generating function of a public key set based on the conjugated information, where the space over which the elliptic curve is defined $\mathbb{F}_{q^n}$ will have a multiplication factor K which will satisfy the relation $|K|\leq\lfloor q/2\rfloor$. From here, corresponding to the level of the communication initiator (let him be A_i) from the user hierarchy, we will define a function like

$$\varphi(level, string)\to public\ Key$$

where string represents the initialization parameters of the generator, as described broadly in the thesis, and level represents the access level to the communication secure communication channel, from which A_i belongs.

In the sense of obtaining the interwoven encryption key, for a pair of participants, let them be (A_i,A_j), they will create a session key if they are on the same level of security from the hierarchy, if the belong to different levels of security there will be a communication initiated by the owner of a higher security level, where these principles are broadly described in [154], [69], [71]. To describe them we will defined:

- $\Pi_{K_{A_i}}$ - the secret key of A_i
- $\Pi_{P_{A_i}}$ - the public kye of A_i
- $\eta^d_{A_i}(\Pi_{K_{A_i}},m)$ - message encryption m with the secret key of A_i
- $\eta^e_{A_i}(\Pi_{P_{A_i}},m)$ - message encryption m with the public key of A_i
- $\mathrm{enc}(s_K,m)$ - symmetric key for message encryption m together with s_K
- $\inf_{A_i}$ - pseudorandom value generated by A_i for every session
- $E(\mathbb{Z}_p)$ - the elliptic curve defined over the field $\mathbb{Z}_p$

- M - message space
- $hf(\cdot)$ - hash function $SHA-1$
- $m_1|m_2$ - concatenation of messages m_1,m_2 when m_1, $m_2 \in M$

An user of the systems let him be A_i (with respect to the conditions expressed in the thesis) will have the following public parameters:

$$(\Pi_{P_{A_i}}, E(\mathbb{Z}_p), P, Q, n)$$

where $P, Q \in E(\mathbb{Z}_p)$ represents two points on the elliptic curve $E(\mathbb{Z}_p)$ and the division p, as stated in the thesis, will have the form q^k with respect to the presented conditions. Also, we will define the functions

- $\eta^d_{A_i}(\Pi_{K_{A_i}}, m)$ and
- $\eta^e_{A_i}(\Pi_{P_{A_i}}, m)$
- $hf(\cdot)$

as public.

For the user A_i, the following parameters are secret:

- $\Pi_{K_{A_i}}$
- $infA_i$

Starting from the presented parameters, we can expose the protocol which establishes the session key between participants A_i and A_j.

- A_i
  1. We generate a random number $\inf_{A_i} \in [1, n-1]$
  2. We compute $A^1_i = \inf_{A_i}(P^{-1} + Q) = (x_1^{A_i}, y_1^{A_i})$. Let $x = x_1^{A_i}\ mod\ n$. If $x = 0$ then we execute step 1
  3. We compute $A^2_i = hf(P_{A_i}|A^1_i)$
  4. We compute $A^3_i = \eta^d_{A_i}(\pi_{K_{A_i}}, A^2_i)$
  5. The first step of communication (from A_i to A_j)
     A_i sends to A_j $(A^1_i|A^2_i)$
- A_j
  1. We compute $A^1_j = hf(P_{A_i}|A^1_i)$
  2. We compute $A^2_j = \eta^e_{A_i}(\pi_{P_{A_i}}, A^2_i)$. If $A^1_j \neq A^2_j$ terminates then the protocol ends with failure

3. We generate a random number $\inf_{A_j} \in [1, n-1]$
4. We compute $A_j^1 = \inf_B(P^{-1} + Q) = (x_1^{A_j}, y_1^{A_j})$. If $x_1^{A_j} = 0$ then returns to step 3 from the steps executed by A_j
5. We compute $A_j^2 = hf(P_{A_j} | A_j^1)$
6. computes $A_j^3 = \eta^d_{A_j}(\pi_{K_{A_j}}, A_j^2)$
7. $K_{A_j} = \inf_{A_j} A_i^1 = (x_2^{A_j}, y_2^{A_j})$
8. $x = x_2^{A_j} \mod n$. If $x = 0$ then returns to step 3 from the steps executed by A_j
9. The second step of communication (from A_j to A_i)
   A_j sends to A_i $(A_j^1 | A_j^3)$

- A_i

  6 We compute
  $s_1^{A_i} = hf(P_{A_j}, A_j^1)$
  $s_2^{A_i} = \eta^e_{A_j}(\pi_{P_{A_i}}, A_j^3)$

  7 If $s_1^{A_i} \neq s_2^{A_i}$ the execution of the protocol ends in failure.

  8 $K_{A_i} = \inf_{A_i} A_j^1$

In order to ensure double authentication of the users involved in the process of secure communication, defined as A_i and A_j, we will define a third step to the described protocol.

Starting from the steps described in the optimized protocol, described in the thesis, there will be a third step which will ensure session key approval by A_i, by this it will be assured by the double authentication of the participants to the confidential communication channel.

In this regard, A_i will compute

$$hf((inf_{A_i}(P^{-1} + Q))) \mid \mathrm{enc}(K_{A_i}, inf_{A_j}(P^{-1} + Q))$$

and will send the result to A_j.

At this point, when receiving the message, A_j will test the equality:

$$\begin{aligned} & hf((\inf_{A_i}(P^{-1} + Q)) \mid \mathrm{enc}(K_{A_i}, \inf_{A_j}(P^{-1} + Q))) \\ &= hf((\inf_{A_i}(P^{-1} + Q)) \mid \mathrm{enc}(K_{A_j}, \inf_{A_j}(P^{-1} + Q))). \end{aligned}$$

If the test of the equality will return success then the session key is confirmed by the participants. In implementing this system, we defined it as the conformation step. In regard to higher work speed it is used when the participants are of different security levels, because in the case of an inequality at the third step this protocol will be restarted.

From a statistic point of view, the time needed to execute this step alongside with the complexity is of order $\Phi(1/4)$ from the required first two steps.

It was developed a personal version also for the extended algorithm, based on the mathematical model described above.

O version of the expressed protocol can be obtained by defining:

$$h'_{int}(h(k))$$

where $h'_{int} : M \to N$, h' representing the function which will generate a parameter $\eta \in \mathbb{N}$, $h'_{int}(h(k)) = \eta$, $\eta \in \mathbb{N}$, and η will respect the inequality $\eta \leq \sqrt{2} \cdot n$, where n represents the number of security levels. Let L_t, $0 \leq t \leq m$, the security levels. In this case, the key for every participant A^t_j will be created in two steps.

The first step of authentication of users which is fulfilled in the first part of the protocol and the second step - authenticating the key, is made at the additional step (third step).

This version starts form the idea of defining them as being different entities, the first are the participants to the process and the second the session keys used. Therefore it will be used a parametrization of $T.S.$, let it be defined as M^i_t called "master parametrization where t is the security level and i represents the participant index which initiates the communication process.

To highlight the functionality of the model it is necessary to prove the uniqueness of the parameters defined in the grade fraction q^k, over the elliptic curve used, more exactly the existence of the elliptical curve used.

In this sense, we will demonstrate the following theorem describing the parametrization used.

Theorem 1. Let Γ an nonsigular projection of an elliptic curve over fraction q^k, of type 1. In this case there is an elliptic curve, let $E(\mathbb{F}_{q^k})$ over q^k therefore Γ is an homogeneous space for $E(\mathbb{F}_{q^k})$ and $E(\mathbb{F}_{q^k})$ is unique defined by an isomorphism over q^k.

In the thesis there is the full demonstration of the above theorem which illustrates the properties of the used space.

In the 3rd chapter, starting from the idea of cryptographic systems used in session key generation we developed hierarchical models which treat a variety o cases of linear and nonlinear generators depending on the use case of each one. For the linear models, the applicability study can be reduced to the solution analysis of classic mathematical problems to which the Equivalent Linear Complexity is reduced. Regarding the resistance to cryptographic attacks, as a computer science model, they are stable. However, if you study the computational effort with an mathematical analysis model based on solutions of atomic compounds constructed on bijections of the base model, reaching feasible models which are studied in real time.

In this regard, we developed the necessary model for stating and demonstrating the conjecture below, which facilitates the modeling illustration of an optimal system of optimal differential encryption.

Conjecture 1. Berlekamp-Massey for the case of compound dependencies.

For an equations system which describe the behavior a registry set with linear displacement dependencies of length λ, which will have as an output a sequence system

(1) $\alpha_0, \alpha_1, \ldots, \alpha_{N-1}$, for the linear case, where $\alpha_0 \neq 0, N \geq \alpha, \lambda'$-the length of the generated string

(2) $\alpha_0, \alpha_1, \ldots, \alpha_{M-1}$, for the compound case, where $\alpha_0 \neq 0, M > N, \lambda''$-the length of the generated string
will satisfy the relations:

(3) $\lambda' \geq N + 1 - \lambda, \ \lambda'' \geq M + 1 - \lambda$

(4) $\lambda'' > \lambda'$

This is concretized by the following properties on the implementations of those parametrization

- Adding a parameter does not guarantee increasing the output string size / generator period, in other words, the type of comparison "$\circ$" from the Conjecture 1 is given by the type / grade of dependency between the initial parameters and the introduced parameter, let him be noted as: $DL(\lambda', \lambda'')$
- The ideal case, the one of dependence $DL = 0$ is transposed in the fact that the function "$\circ$" from the Conjecture will become the multiplication operation.

Starting from those, we developed an proprietary model of parametrization and construction of equations systems which define a set of shift registries with linear dependencies, named AGNS, which have an grater efficiency factor then the original model used in LFSR. E functional version will be:

$$\frac{C.L.E.}{Complex.Imp.}(AGNS) > \frac{C.L.E.}{Complex.Imp.}(LFSR)$$

where $C.L.E.$ is the equivalent linear complexity and $Complex.Imp.$ represents computation complexity of the implementation, for a generation system of pseudorandom numbers. The results have been illustrated in the published article [31].

In this case we have:

$$b_k \leq b_{k+1} \leq a_{k+1} \leq a_k \text{ și}$$
$$0 \leq a_{k+1} - b_{k+1} \leq (a_k - b_k)/2$$

From those expressed we can construct an proposition (results published in [31]) which illustrate that a iteration of type AGM constructs a sequence of elliptic curves based on a isomorphism of the initial elliptic curve.

Proposition 1. [31] Starting from choosing the two parameters a and b, so that $a, b \in 1 + 4\mathbb{Z}_q$ with the property $a/b \in 1 + 8\mathbb{Z}_q$ and an elliptic curve $E_{a,b}$ defined by the equation $y^2 = x(x - a^2)(x - b^2)$, let a' and b', two parameters so that: $a' = (a + b)/2,\ b' = \sqrt{ab}$ and an elliptic curve $E_{a',b'}$, defined by equation $y^2 = x(x - a'^2)(x - b'^2)$. In this case, the elliptic curves $E_{a,b}$ and $E_{a',b'}$ are characterized by the equation:

$$\Phi : E_{a,b} \longrightarrow E_{a',b'} : (x, y) \longmapsto \left(\frac{(x + ab)^2}{4x}, y\frac{(x - ab)(x + ab)}{8x^2} \right)$$

and the greatest part of Φ is $\langle (0, 0) \rangle$. The operation Φ on the differential interval $\frac{dx}{y}$ will have the following form

$$\Phi^* \left(\frac{dx}{y} \right) = 2\frac{dx}{y}.$$

In the 4th chapter we study the optimizations of the mathematical models used in group signing systems, therefore, starting from the concept of group signature presented by Chaum and van Heijst in the year 1991 ([18, 19, 22]), any member of the group can sign a message in behalf of the group so that anyone can verify the validity of the signature but no one can determine which member of the group sent the message ([40], [117], [168], [97], [98]).

From the developments made in the thesis, particular algorithms have resulted which are represented below.

All the models studied in the thesis and the described algorithms have been implemented in two research projects (UEFISCDI PCE and UEFISCDI PCCA) of which I am proud to be a member. Those results have been illustrated by testing and using the Digital Declaration system created, which is unique in Romania and the second system officially implemented at European level.

Algorithm 1 The key generation algorithm for a system derived from Schnorr

1: generating big prime numbers p and two points (P,Q) nonsingular on an nonsupersingular elliptic curve, described in the first chapter of the thesis
2: g is the group generator
3: the private key is selected$x$
4: $y = g^x \pmod p$
5: $\Phi = (p-1)(q-1)$
6: the public key is (p, g, y, P)
7: the private key is (p, g, x, Q)

Algorithm 2 The signing algorithm for a system derived from Schnorr

1: (p, g, x, P) is the private key
2: is selected randomly k so that $0 < k < q$
3: $r = P.x, g^k \pmod p$
4: $e = H(m||r||P.y)$
5: $s = (k - xe) \pmod q$
6: the signature is (e, s)

Algorithm 3 The signature verification algorithm for a system derived from Schnorr

1: (p, g, y, Q) is the public key
2: (e, s) is the signature
3: $r_v = Q.y, g^s y^e$
4: $e_v = H(m||r_v||Q.y)$
5: **if** $(e_v = e)$ **then**
6: $\quad (e, s)$ is valid
7: **end if**

Bibliography

[1] L.M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In LeonardM. Adleman and Ming-Deh Huang, editors, Algorithmic Number Theory, volume 877 of Lecture Notes in Computer Science, pages 28–40. Springer Berlin Heidelberg, 1994.

[2] G.B. Agnew, R.C. Mullin, and S.A. Vastone. An inplementation of ellipic curve cryptosystems over $f_{2^{155}}$. IEEE Journal on Selected areas in Communications, 5(11):804–813, June 1993.

[3] R. Alsaedi, N. Constantinescu, and V. Radulescu. Nonlinearities in elliptic curve authentication. Entropy, 16(9):5144—5158, September 2014.

[4] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime, 1992. Series of emails to the NMBRTHRY mailing list.

[5] J.P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia. Quark: A lightweight hash. Journal of Cryptology, 26(2):313–339, 2013.

[6] R. Avanzi, W.D. Benits, S.D. Galbraith, and J. Mckee. On the distribution of the coefficients of normal forms for frobenius expansions. Designs codes and cryptography, 61(1):71—89, October 2011.

[7] L. Babai. Trading group theory for randomness. ACM Symposium on Theory of Computing, 16:421–429, May 1985.

[8] L. Babai and S. Moran. Arthur - merlin games: A randomized proof system, and a hierarchy of complexity classes. Journal of Computer and System Sciences, 36, 1988.

[9] E.R. Berlekamp. Algebraic coding theory. McGraw-Hill, New York, 1968.

[10] E. Biham. Cryptanalysis of triple modes of operation. Journal of Cryptology, 12(3):161–184, 1999.

[11] I. F. Blake, G. Seroussi, and N. P. Smart. Elliptic Curves in Cryptography. Cambridge University Press, 1999. 4

[12] J. Buchmann and H. Baier. Efficient construction of cryptographically strong elliptic curves. In Bimal Roy and Eiji Okamoto, editors, Progress in Cryptology —INDOCRYPT 2000, volume 1977 of Lecture Notes in Computer Science, pages 191–202. Springer Berlin Heidelberg, 2000.

[13] J. Camenisch. Effcient and generalized group signatures. In In Advances in Cryptology EUROCRYPT '97, volume 1233 of Lecture Notes in Computer Science, pages 465–479. Springer-Verlag, 1997.

[14] J. Camenisch and M. Stadler. Efficient group signatures schemes for large groups. In Advances in Cryptology-Crypto, volume 1294 of Lecture Notes in Computer Science, pages 410–424. Springer-Verlag, 1997.

[15] J. L. Camenisch. Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem. PhD thesis, ETH Zurich, 1998.

[16] D.G. Cantor. Computing in the jacobian of an hyperelliptic curve. Math. Comp., 48(177):95–101, 1987.

[17] R. Carls. A generalized arithmetic geometric mean (GAGM) sequence. PhD thesis, Rijksuniversiteit Groningen, 2004.

[18] D. Chaum and E. van Heyst. Group signatures. Advances in Cryptology EUROCRYPT '91, 547 of Lecture Notes in Computer Science:257–265, 1995. 9

[19] L. Chen and T. P. Pedersen. New group signature schemes. In Advances in Cryptology - EUROCRYPT '94, volume 950 of Lecture Notes in Computer Science, pages 171–181. Springer-Verlag, 1995. 9

[20] M. Ciet. Aspects of Fast and Secure Arithmetics for Elliptic Curve Cryptography. PhD thesis, Universite Catholique de Louvain, 2003.

[21] C. Clavier and M. Joye. Universal exponentiation algorithm a first step towards provable spa-resistance. In CetinK. Koc, David Naccache, and Christof Paar, editors, Cryptographic Hardware and Embedded Systems — CHES 2001, volume 2162 of Lecture Notes in Computer Science, pages 300–308. Springer Berlin Heidelberg, 2001.

[22] H. Cohen. A course in computational algebraic number theory, volume 138 of Graduate texts in mathematics. Springer, 1993. 9

[23] H. Cohen and G. Frey. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathematics And Its Applications Series Editor Kenneth H.Rosen, Chapman & Hall/CRC, 2006.

[24] H. Cohen and H. W. Lenstra jr. Primality testing and jacobi sums. Mathematics of Computation, 42:297–330, 1984.

[25] H. Cohen, A. Miyaji, and T. Ono. Efficient elliptic curve exponentiation using mixed coordinates. In Kazuo Ohta and Dingyi Pei, editors, Advances in Cryptology — ASIACRYPT'98, volume 1514 of Lecture Notes in Computer Science, pages 51–65. Springer Berlin Heidelberg, 1998.

[26] N. Constantinescu. The agreement of the common key. Annals of the University of Craiova - Mathematics and Computer Science Series, 30(2):59–65, 2003.

[27] N. Constantinescu. Authentication ranks with identities based on elliptic curves. Annals of the University of Craiova, Mathematics and Computer Science Series, XXXIV(1):94–99, 2007.

[28] N. Constantinescu. Criptografie. Editura Academiei Române, Bucureşti, 2009.

[29] N. Constantinescu. Authentication hierarchy based on blind signature. Journal of Knowledge Communication and Computing Technologies, 1(1):77–84, 2010. 4

[30] N. Constantinescu. Security system vulnerabilities. Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science, 13(2):175–179, 2012.

[31] N. Constantinescu, O.A. Ţicleanu, and A. Golumbeanu. Nonlinearities on cryptographic shift registers. Annals of the University of Craiova, Mathematics and Computer Science Series, 43(1):27–32, 2016. 3, 9

[32] N. Constantinescu and G. Stephanides. Secure key-exchange. Recent Advances in Communications and Computer Science, 7:162–166, 2003.

[33] N. Constantinescu and G. Stephanides. Identification of parts in identity-based encryption. Technical report, Wessex Institute of Technology, UK, developed with University of Bergen, Norway, 2004. Research Notes in Data Security.

[34] N. Constantinescu, G. Stephanides, M. Cosulschi, and M. Gabroveanu. Rsa-padding signatures with attack studies. In WEBIST 2006,

Proceedings of the Second International Conference on Web Information Systems and Technologies: Internet Technology / Web Interface and Applications, Setúbal, Portugal, April 11-13, 2006, pages 97–100, 2006.

[35] J.S. Coron, D. Lefranc, and G. Poupard. A new baby-step giant-step algorithm and some applications to cryptanalysis. In JosyulaR. Rao and Berk Sunar, editors, Cryptographic Hardware and Embedded Systems - CHES 2005, volume 3659 of Lecture Notes in Computer Science, pages 47–60. Springer Berlin Heidelberg, 2005.

[36] J.M. Couveignes. Quelques calculs en théorie des nombres. PhD thesis, Universite de Bordeaux, 1994.

[37] J.M. Couveignes. Computing l-isogenies with the p-torsion. In ANTS-II: Algorithmic Number Theory, Lecture, volume 1122, pages 59–65. Springer-Verlag, 1996.

[38] J. Cowie, B. Dodson, R. M. E.-Huizing, A. K. Lenstra, P. L. Montgomery, and J. Zayer. A world wide number field sieve factoring record: On to 512 bits. In Advances in Cryptology-ASIACRYPT '96, volume 1 of Lecture Notes in Computer Science, pages 382–394. Springer-Verlag, 1996.

[39] R.E. Crandall. Method and apparatus for public key exchange in a cryptographic system, October 1992. US Patent 5,159,632.

[40] O.A. Ţicleanu, N. Constantinescu, and D. Ebânca. Intelligent data retrieval with hierarchically structured information. In Intelligent Interactive Multimedia Systems and Services - Proceedings of the 6th International Conference on Intelligent Interactive Multimedia Systems and Services, IIMSS 2013, Sesimbra, Portugal, 26-28 June 2013, ISI indexed, pages 345–351, 2013. 9

[41] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkorper. Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, 14(1):197–272, 1941.

[42] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22:644–654, November 1976.

[43] I.M. Duursma, P. Gaudry, and F. Morain. Speeding up the discrete log computation on curves with automorphisms. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, Advances in Cryptology - ASIACRYPT'99, volume 1716 of Lecture Notes in Computer Science, pages 103–121. Springer Berlin Heidelberg, 1999.

[44] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In Computational Perspectives on Number Theory (Chicago, IL, 1995) AMS/IP Stud. Adv. Math., Amer. Math. Soc., Providence, RI, 7(2):21–76, 1998.

[45] A. Enge. Computing discrete logarithms in high-genus hyperelliptic jacobians in provably subexponential time. Mathematics of Computation, 71(238):729–742, November 2001.

[46] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. Acta Arithmetica, 102:83–103, 2002.

[47] A. Enge and A. Stein. Smooth ideals in hyperelliptic function fields. Mathematics of Computation, 71(239):1219–1230, October 2001.

[48] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. Journal of Cryptology, 1:77–94, 1987.

[49] R. Flassenberg and S. Paulus. Sieving in function fields. Experimental Mathematics, 8(4):339–349, 1999.

[50] M. Fouquet, P. Gaudry, and R. Harley. On satoh's algorithm and its implementation. Journal Ramanujan Mathematical Society, 15(2):281–318, 2000.

[51] S.D. Galbraith, XB. Lin, and M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. Journal of cryptology, 24(3):446—469, July 2011.

[52] R. Gallant, R. Lambert, and S. Vanstone. Improving the parallelized pollard lambda search on binary anomalous curves. Mathematics of Computation, 69:1699–1705, 1998.

[53] S. Gao, J. von Zur Gathen, D. Panario, and V. Shoup. Algorithms for exponentiation in finite fields. Journal of Symbolic Computation, 29(6):879–889, 2000.

[54] S.R. Ghorpade, S. Ul Hasan, and M. Kumari. Primitive polynomials, singer cycles and word-oriented linear feedback shift registers. Designs, Codes and Cryptography, 58(2):123–134, 2011.

[55] O. Goldreich, S. Micali, and Avi Wigderson. Proofs that yield nothing but their validity. Journal of the ACM, 38:690–728, July 1991.

[56] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. Proc. 27th Annual Symposium on Foundations of Computer Science, pages 291–304, 1985.

[57] J.Dj. Golić and R. Menicocci. Edit probability correlation attacks on stop/ go clocked keystream generators. Journal of Cryptology, 16(1):41–68, 2003.

[58] J.Dj. Golic and R. Menicocci. Correlation analysis of the alternating step generator. Designs, Codes and Cryptography, 31(1):51–74, 2004.

[59] J.Dj. Golić, M. Salmasizadeh, and E. Dawson. Fast correlation attacks on the summation generator. Journal of Cryptology, 13(2):245–265, 2000.

[60] A.I. Golumbeanu. Digital declaration implementation study. Journal of Knowledge Communication and Computing Technologies, 3(2):1–11, 2011. 3

[61] A.I. Golumbeanu. Application of differential cryptography to a gn authentication hierarchy scheme. Electronic Journal of Differential Equations,, 2017(20):1–8, 2017. 3

[62] A.I. Golumbeanu and O.A. Ţicleanu. Elliptic curves differentiation with application to group signature scheme. Electronic Journal of Differential Equations, 2017(237):1–21, 2017. 3

[63] J. Guajardo and C. Paar. Itoh-tsujii inversion in standard basis and its application in cryptography and codes. desing. Codes and Cryptography, 2(25):207–216, February 2002.

[64] R. Harley. Asymptotically optimal p-adic point-counting, December 2002. Email to normal font NMBRTHRY mailing list.

[65] R. Harley. Method for solving frobenius equations for elliptic-curve cryptography, 2004. US Patent App. 10/733,320.

[66] R. Harley and J.F. Mestre. Method for generating secure elliptic curves using an arithmetic-geometric mean iteration, April 2003. US Patent App. 10/172,776.

[67] T. Herlestam. On the complexity of functions of linear shift register sequences. In IEEE ISIT, Les Arcs, France. IEEE, 1982.

[68] I. Iancu, N. Constantinescu, and M. Colhon. Fingerprints identification using a fuzzy logic system. International Journal of Computers, Communications and Control, 5(4):525–531, 2010.

[69] O.A. Ţicleanu. Mathematical models in cryptography. Journal of Knowledge Communication and Computing Technologies, 4(1):1–9, 2013. 4

[70] O.A. Ţicleanu. Nonlinear analysis on elliptic curves subspaces with cryptographic applications. Annals of the University of Craiova, Mathematics and Computer Science Series, 41(2):292–299, 2014.

[71] O.A. Ţicleanu. Differential operators over particular elliptic curves spaces with cryptographic applications. Electronic Journal of Differential Equations, 2015(303):1–9, 2015. 4

[72] O.A. Ţicleanu. Endomorphisms on elliptic curves for optimal subspaces and applications to differential equations and nonlinear cryptography. Electronic Journal of Differential Equations, 2015(214):1–9, 2015.

[73] O.A. Ţicleanu and N. Constantinescu. Studying models issues on e-commerce cashing. In In International Conference on Applied Mathematics and Computational Methods in Engineering II (AMCME '14), IOS Press, pages 116–128. IOS Press, 2014.

[74] M. Jacobson and A. van der Poorten. Computational aspects of nucomp. In Claus Fieker and DavidR. Kohel, editors, Algorithmic Number Theory, volume 2369 of Lecture Notes in Computer Science, pages 120–133. Springer Berlin Heidelberg, 2002.

[75] T. Johansson. A shift register construction of unconditionally secure authentication codes. Designs, Codes and Cryptography, 4(1):69–81, 1994.

[76] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. Soviet Physics Doklady, 7(7):595–596, 1963.

[77] K. S. Kedlaya. Counting points on hyperelliptic curves using monsky-washnitzer cohomology. J. Ramunujan Mathematical Society, pages 323–338, 2001.

[78] J. Kilian and E. Petrank. Identity escrow. In Advances in Cryptology - CRYPTO '98, volume 1642 of Lecture Notes in Computer Science, pages 169–185, Berlin, 1998.

[79] H.Y. Kim, J.Y. Park, J.H. Cheon, J.H. Park, J.H. Kim., and S.G. Hahn. Fast elliptic curve point counting using gaussian normal basis. In Claus Fieker and DavidR. Kohel, editors, Algorithmic Number Theory, volume 3076 of Lecture Notes in Computer Science, pages 292–307. Springer Berlin Heidelberg, 2004.

[80] A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. J. Cryptology, 10(2):111–147, 1997.

[81] D. E. Knuth. The Art of Computer Programming. ddison-Wesley, 1981.

[82] N. Koblitz. p-Adic Numbers, p-Adic Analysis, and Zeta-Functions. Springer-Verlag, GTM 58, 1984.

[83] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48(177):203–209, January 1987.

[84] N. Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In AlfredJ. Menezes and ScottA. Vanstone, editors, Advances in Cryptology-CRYPT0' 90, volume 537 of Lecture Notes in Computer Science, pages 156–167. Springer Berlin Heidelberg, 1991.

[85] N. Koblitz. A Course in Number theory and Cryptography. New York. Springer, 1994.

[86] D.R. Kohel. The $agm - x_0(n)$ heegner point lifting algorithm and elliptic curve point counting. In Chi-Sung Laih, editor, Advances in Cryptology - ASIACRYPT 2003, volume 2894 of Lecture Notes in Computer Science, pages 124–136. Springer Berlin Heidelberg, 2003.

[87] A. G. Konheim. Computer Security and Cryptography. Wiley, 2007.

[88] T. Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. Applicable Algebra in Engineering, Communication and Computing, 15(5):295–328, February 2005.

[89] A. K. Lenstra and H. W. Lenstra Jr. The development of the number field sieve. In LNCS, volume 1554 of Lecture Notes in Mathematics. Springer-Verlag, 1993.

[90] R. Lercier. Computing isogenies in $\mathbb{F}_{2^n}$. In Henri Cohen, editor, Algorithmic Number Theory, volume 1122 of Lecture Notes in Computer Science, pages 197–212. Springer Berlin Heidelberg, 1996.

[91] R. Lercier. Algorithmique des courbes elliptiques dans les corps finis. PhD thesis, Ecole Polytechnique, 1997.

[92] R. Lercier and D. Lubicz. Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time. In Advances in Cryptology—EUROCRYPT '2003, Lecture Notes in Computer Science, volume 2656, pages 360–373. Springer-Verlag, 2003.

[93] R. Lercier and F. Morain. Counting points in elliptic curves over f_{p^n} using couveignes algorithm. Technical report, Ecole polytechnique - LIX, September 1995. Research Report LIX/RR/95/09.

[94] C. Lim and P. Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In Jr. Kaliski, BurtonS., editor, Advances in Cryptology — CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pages 249–263. Springer Berlin Heidelberg, 1997.

[95] D. Lorenzini. An Invitation to Arithmetic Geometry (Graduate Studies in Mathematics, Vol.9). American Mathematical Society, 1996.

[96] J. Lubin, J.P. Serre, and J. Tate. Elliptic curves and formal groups. Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Woods Hole, 1964. American Mathematical Society.

[97] A. Lysyanskaya. Signature Schemes and Applications to Cryptographic Protocol Design. PhD thesis, MIT, 2002. 9

[98] A. Lysyanskaya and Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. Proc. of Second International Conference on Financial Cryptography, 1998. 9

[99] Zhen Ma, Wen-Feng Qi, and Tian Tian. On affine sub-families of the NFSR in grain. Des. Codes Cryptography, 75(2):199–212, 2015.

[100] J.L. Massey. Shift-register synthesis and bch decoding. IEEE Trans. Inf. Theory, IT-15(1):122–127, 1969.

[101] G. McGuire and E.S. Yilmaz. Further results on the number of rational points of hyperelliptic supersingular curves in characteristic 2. Designs codes and cryptography, 77(2-3):653—662, 2015.

[102] W. Meier and O. Staffelbach. Fast correlation attacks on certain stream ciphers. Journal of Cryptology, 1(3):159–176, 1989.

[103] W. Meier and O. Staffelbach. Correlation properties of combiners with memory in stream ciphers. Journal of Cryptology, 5(1):67–86, 1992.

[104] A. Menezes, S. Vanstone, and T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing, STOC '91, pages 80–89. ACM, 1991.

[105] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[106] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography, 5th Ed. CRC Press, 2001.

[107] A.J. Menezes, Y.-H. Wu, and R. Zuccherato. An elementary introduction to hyperelliptic curves. In N.Koblitz, editor, Algebraic Aspects of Cryptography, pages 155–178. Springer-Verlag, 1996.

[108] W. Messing. The crystals associated to Barsotti-Tate groups: with applications to abelian schemes. Springer-Verlag, 1972. Lecture Notes in Mathematics (Book 264).

[109] J.F. Mestre. Lettre adressée á gaudry et harley, December 2000. Available at http://webusers.imj-prg.fr/ jean-francois.mestre/.

[110] V. S. Miller. Use of elliptic curves in cryptography. In HughC. Williams, editor, Advances in Cryptology — CRYPTO '85 Proceedings, volume 218 of Lecture Notes in Computer Science, pages 417–426. Springer Berlin, 1986.

[111] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit condition of elliptic curve trace for fr-reduction. IEICE Trans. Fundamentals, E84 A(5), 2001.

[112] R.T. Moenck. Fast computation of gcds. In Proceedings of the Fifth Annual ACM Symposium on Theory of Computing, STOC '73, pages 142–151. ACM, 1973.

[113] P.L. Montgomery. Modular multiplication without trial division. Mathematics of Computation, 170(44):519–521, 1985.

[114] V. Muller. Fast multiplication on elliptic curves over small fields of characteristic two. Journal of Cryptology, 11(4):219–234, 1998.

[115] V. Muller, A. Stein, and C. Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. Mathematics of Computation, 68(226):807–822, April 1999.

[116] K. Nagao. Improving group law algorithms for jacobians of hyperelliptic curves. In Wieb Bosma, editor, Algorithmic Number Theory, volume 1838 of Lecture Notes in Computer Science, pages 439–447. Springer Berlin Heidelberg, 2000.

[117] U.S. Dept of Commerce/NIST. Digital signature standard (dss), Jan 2000. 9

[118] R. Oppliger. Contemporary Cryptography. Artech House, 2005.

[119] IEEE P1363. Standard specifications for public-key cryptography, September 1998. Draft version 7.

[120] Certicom White Paper. The elliptic curve cryptosystem for smart card, May 1998.

[121] S. Paulus and A. Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In JoeP. Buhler, editor, Algorithmic Number Theory, volume 1423 of Lecture Notes in Computer Science, pages 576–591. Springer Berlin Heidelberg, 1998.

[122] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In ColinD. Walter, ÇetinK. Koç, and Christof Paar, editors, Cryptographic Hardware and Embedded Systems - CHES 2003, volume 2779 of Lecture Notes in Computer Science, pages 351–365. Springer Berlin Heidelberg, 2003.

[123] H. Petersen. How to convert any digital signature scheme into a group signature scheme. Security Protocols Workshop, 1997.

[124] N.R. Pillai and S.S. Bedi. Algebraic attacks on a class of stream ciphers with unknown output function. Designs, Codes and Cryptography, 69(3):317–330, 2013.

[125] S.C. Pohlig and M.E. Hellman. An improved algorithm for computing logarithms over gf(p) and its cryptographic significance. Information Theory, IEEE Transactions on, 24(1):106–110, January 1978.

[126] J. M. Pollard. A monte carlo method for factorization. BIT, 1975.

[127] J. M. Pollard. Monte carlo methods for index computation (mod p). Mathematics of Computation, 32:918–924, July 1978.

[128] C. Pomerance. The quadratic sieve factoring algorithm. In Advances in Cryptology, volume 209 of Lecture Notes in Computer Science, pages 169–182. Springer-Verlag, 1985.

[129] M. O. Rabin. Probabilistic algorithm for testing primality. Journal of Number Theory, 12:128–138, 1980.

[130] Certicom Research. Sec 2: Recommended elliptic curve domain parameters, September 2000. Version 1.0.

[131] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21(2):120–126, February 1978.

[132] S. Ronjom. Improving algebraic attacks on stream ciphers based on linear feedback shift register over $\mathbb{F}_{2^k}$. Designs, Codes and Cryptography, 82(1-2):27–41, 2017.

[133] H.G. Ruck. On the discrete logarithm in the divisor class group of curves. Mathematics of Computation, 68(226):805–806, April 1999.

[134] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. Journal of the Ramanujan Mathematical Society, 15(4):247–270, January 2000.

[135] T. Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In Claus Fieker and DavidR. Kohel, editors, Algorithmic Number Theory, volume 2369 of Lecture Notes in Computer Science, pages 43–66. Springer Berlin Heidelberg, 2002.

[136] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Fields and Their Applications, 9(1):89–101, 2003.

[137] C. P. Schnorr. Eficient signature generation by smart cards. Journal of Cryptology, 4(3):161–174, January 1991.

[138] C.P Schnorr. Efficient identification and signatures for smart cards. In Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '89, pages 239–252. Springer-Verlag, 1990.

[139] A. Schonhage and V. Strassen. Schnelle multiplikation grosser zahlen. Computing (Arch. Elektron. Rechnen), 7(3-4):281–292, 1971.

[140] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp., 44:483–494, 1985.

[141] J.P. Serre. Local Fields. Springer-Verlag, GTM 67, 1979.

[142] A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology, volume 196 of Lecture Notes in Computer Science, pages 47–53. Springer-Verlag, 1984.

[143] D. Shanks. On gauss and composition i and ii. In R. Mollin, editor, Number Theory and its Applications, volume 265, pages 163–204. Kluwer Academic Publishers, 1989.

[144] J.H. Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag, GTM 106, 1986.

[145] E. Simion and N. Constantinescu. Complexity computations in code cracking problems. In Concurrent Engineering in Electronic Packaging 2001. 24th International Spring Seminar, IEEE Communication, pages 225–232. IEEE, 2001.

[146] B. Skjernaa. Satoh's algorithm in characteristic 2. Mathematics of Computation, 72(241):477–487, March 2002.

[147] N. Smart. How secure are elliptic curves over composite extension fields? In EUROCRYPT 2001, volume 2045 of Lecture Notes in Computer Science, pages 30–39. Springer-Verlag, 2001.

[148] N.P. Smart. The discrete logarithm problem on elliptic curves of trace one. Journal of Cryptology, 12(3):193–196, 1999.

[149] N.P. Smart. Elliptic curves over small fields of odd characteristic. Journal of Cryptography, 12(2):141–151, 1999.

[150] S.C. So, T. Kim, and S. Hong. Accelerating elliptic curve scalar multiplication over gf(2(m)) on graphic hardwares. Journal of parallel and distributed computing, 75:152—167, January 2015.

[151] J.A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. In Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings, pages 357–371, 1997.

[152] J.A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. Springer-Verlag, 1997.

[153] A. Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. Journal of the Ramanujan Mathematical Society, 16(2):1–86, January 2001.

[154] G. Stephanides and N. Constantinescu. The gn-authenticated key agreement. Applied Mathematics and Computation, 170(1):531–544, 2005. 3, 4

[155] H. Stichtenoth. Algebraic Function Fields and Codes. Springer-Verlag, 1993.

[156] D.R. Stinson. Cryptography Theory and Practice - Second Edition. CRC Press, 2002.

[157] H. Tanaka. A realization scheme for identity-based cryptosystem. In Advances in Cryptology, volume 293 of Lecture Notes in Computer Science, pages 341–349. Springer-Verlag, 1987.

[158] E. Teske. Speeding up pollard's rho method for computing discrete logarithms. In JoeP. Buhler, editor, Algorithmic Number Theory, volume 1423 of Lecture Notes in Computer Science, pages 541–554. Springer Berlin Heidelberg, 1998.

[159] T. Tian and Wen-Feng Qi. On the largest affine sub-families of a family of NFSR sequences. Des. Codes Cryptography, 71(1):163–181, 2014.

[160] J.T. van Lint. Introduction to Coding Theory. Springer-Verlag New York, Inc., 1982.

[161] P.C. van Oorschot and M.J.Wiener. Parallel collision search with cryptanalytic applications. Journal of Cryptology, Springer-Verlag, 12(1):1–28, 1999.

[162] S. Vaudenay. The security of dsa and ecdsa - bypassing the standard elliptic curve certification scheme. In Public Key Cryptography'03, pages 309–323. Springer-Verlag, 2003.

[163] J. Velu. Isogenies entre courbes elliptiques. C.R. Acad. Sc. Paris, Seerie A, 273:238–241, 1971.

[164] F. Vercauteren. Computing Zeta Functions of Curves over Finite Fields. PhD thesis, Katholieke Universiteit Leuven, 2003.

[165] F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of satoh's algorithm. In Birgit Pfitzmann, editor, Advances in Cryptology — EUROCRYPT 2001, volume 2045 of Lecture Notes in Computer Science, pages 1–13. Springer Berlin Heidelberg, 2001.

[166] J. von zur Gathen and J. Gerhard. Modern Computer Algebra. Cambridge University Press, 1999.

[167] A. Weil. Numbers of solutions of equations in finite fields. Bulletin of the American Mathematical Society, 55(5):497–508, 1949.

[168] D. Yong and G. Feng. High speed modular divider based on gcd algorithm over gf(2m). Journal on Communications, 29(10):199–204, October 2008. 9

[169] M. Zhang. Maximum correlation analysis of nonlinear combining functions in stream ciphers. Journal of Cryptology, 13(3):301–314, 2000.