M A T H E M A T I C A L E C O N O M I C S

No. 10(17) 2014

INTERNET SECURITY

Andrzej Wilkowski

Abstract. In this paper we present how to use the ZT-UNITAKOD method for dynamic coding. We also talk about a cryptosystem on which to base an elliptic curve. Finally, we discuss the ways to protect the internet user from phishing.

Keywords: dynamic code, elliptic curve, phishing.

JEL Classification: C6.

DOI: 10.15611/me.2014.10.08.

1. Introduction

In this paper we present new methods which would enable increased ICT security. Moreover, we look at the phishing phenomen and we analyse the incidents that breached ICT security in 2012 in Poland.

2. CERT report

The network is becoming more and more influential in business activity as well as in the economy overall during last years. Because of this, it is quite important is to deliver more and more sophisticated methods of security. CERT (Computer Emergency Response Team) has been responsible in Poland for analysing aspects of network security since 1996 (until 2000 it was known under the name of CERTNASK). CERT has beem a member of FIRST (Forum of Incidents Response and Security Teams) since 1997, where it cooperates with similar corporations from the whole world.

According to Wikipedia, the main tasks of CERT team are:

- finding and helping in network security-breach situations,
- alarming users about the appearance of danger which may affect them directly,

Andrzej Wilkowski
Department of Mathematics and Cybernetics, Wrocław University of Economics, Komandorska Street 118/120, 53-345 Wrocław, Poland.
E-mail: andrzej.wilkowski@ue.wroc.pl

- cooperation with other teams in the FIRST project,
- enhancing network security awareness of Internet users,
- monitoring and reporting Polish Internet resources,
- independent tests of products from the Web security branch,
- creating patterns of errors servicing, as well as grading and assembling statistics.

In April 2013, the CERT team presented their analysis of security-breach incidents in 2012. It can be found on www.cert.pl. Below we present the summary of this report:

- in 2012 10,5 million security-breach incidents were automatically noted,
- the number of manually served incidents (the most important) has grown for the first time since 2005 (1082 such cases in 2012, which is almost 80% more than in the previous year),
- Poland is outside the top 10 countries for providing web pages connected with phishing and malware (however, it fares far worse when it comes to problems associated with individual users' computers, like number of bots, scans, etc.),
- the highest number of bots (infected, centrally controlled computers) was connected with Viruta, DNSChanger and ZeuS (about 8000 bots daily),
- the number of phishing incidents is steadily growing, both in a traditional form (like web pages impersonating banks) as well as in malware which can modify web pages visited by users,
- the most frequently attacked service is everlastingly SMB in Windows Microsoft (445/TCP),
- for the first time among the most often attacked services there appeared Remote Desktop in Microsoft Windows (3389/TCP),
- the number of DNS servers of Polish web sites increased significantly (by more than 56%). When they are wrongly configured, they expose all network users,
- in applications which are manually operated, there is a dominance of those from overseas commercial subjects
- the dominance of applications (which are manually operated) from foreign commercial subjects over applications from Polish private users is increasing.

3. Length of key and internet security

Public key cryptography and secure systems of exchanging keys are currently the base of electronic banking security. They enable the remote updating of systems and sending confidential e-mails. The best example of them are RSA and Diffi_Hellman algorithms (up until now, the largest RSA key that was factorized had 768 bits). Basically, longer keys are more robust to attacks. They can be found at www.keylength.com. Some details are given below.

Table 1. Lengths of keys

System	Predicted resistance to attacks (in years)	Length of RSA key (in bites)	Length of key based on elliptic curves (in bites)	Length of hash function (in bites)
Lenstra/Vertheul	to 2013	1513	151	160
Lenstra Updated	to 2013	1191	154	154
Ecrypt II	to 2015	1248	160	160
NIST	to 2030	2048	224	224
ANSSI	to 2020	2048	200	200
BSI	to 2015	1976	224	224
NSA Suite B	No data	Lack of recom-mendation	384	384
Network Working Group RFC 3766	No data	1491	164	164

Source: own work based on www.keylength.com.

However, looking at this table it seems that cryptography based on prime numbers is coming to an end. For example, the American National Security Agency (NSA) did not give any recommendation for cryptosystems RSA and Diffi-Hellman in their package of algorithms Suite B from 2005. The lack of these recommendations is probably also true for NSA Suite A, which was developed to secure the most secret information (and about which little is known officially). This is caused by the existence of effective algorithms to find a discrete logarithm in finite bodies (which enables breaking cryptosystems based on prime numbers).

4. Cryptosystems based on elliptic curves

Here, we present a general concept of an asymmetric cryptosystem based on adding points of elliptic curve [Blake, Seroussi, Smart 2004; Wilkowski 2009]. The theory of elliptic curves has been used on finite bodies to solve various cryptographic problems since 1985. It was used for example to decompose natural numbers into prime numbers, in primality tests and to construct asymmetric cryptosystems. Groups of points of elliptic curves (on finite bodies) are similar to multiplicative finite bodies. However, they have two crucial advantages over them: there are many more of them and it seems that they ensure the same level of security using shorter keys (for more details see Table 1.). It is important in uses which demand very high performance (the RSA algorithms is rather slow).

Definition 1. *Elliptic curve E over the field K is given by*

$$E(K) = \left\{(x, y) \in K^2 : y^2 = x^3 + ax + b \ ; a, b \in K\right\} \cup \{0_E\}, \qquad (1)$$

where 0_E *is called* ***point in infinity****, the polynomial on the right side does not have any multiple roots and the characteristic of field K is different from 2 and 3.*

Let us remember that infinite fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristics equal to 0, while finite fields F_q, which have $q = p^j$ elements or fields $\mathbb{Z} / p\mathbb{Z}$, where p is a prime number, have p characteristic. When the characteristic of field K is equal to 2 or 3, the equation given above slightly differs and we will not consider this situation in this paper.

Table 2. Number of points of elliptic curves

Elliptic curve	Number of points
$y^2 = x^3 + 2x$	2
$y^2 = x^3 + 4x + 2$	3
$y^2 = x^3 + x$	4
$y^2 = x^3 + 3x + 2$	5
$y^2 = x^3 + 1$	6
$y^2 = x^3 + 2x + 1$	7
$y^2 = x^3 + 4x$	8
$y^2 = x^3 + x + 1$	9
$y^2 = x^3 + 3x$	10

Source: own work based on [Yan 2006; Wilkowski 2009].

Example 1 (Yan 2006). Let E be elliptic curve $y^2 = x^3 + 3x$ over the field F_5. In this case, it consists of 10 points:

$$E(F_5) = \{0_E, (0, 0), (1, 2), (1, 3), (2, 2), (2, 3), (3, 1), (3, 4), (4, 1), (4, 4)\}.$$

Here we present some elliptic curves over field F_5 and a number of their points in Table 2.

It can be seen that the numbers are between 2 and 10. In general, the estimation given below is true.

Theorem [Hasse 1933]

$$\left|E(F_p)\right| \leq 1 + p + 2\sqrt{p} \quad .$$

Example 2. Let us consider elliptic curve $E(\mathbb{R})$ (it has an infinite number of points) and crossing straight line:

$$E(\mathbb{R}) = \left\{(x, y) \in \mathbb{R}^2 : y^2 = x^3 - 2x + 4\right\} \cup \{0_E\}, \qquad y = \frac{1}{2}x + \frac{3}{2} \quad .$$

They are presented in Figure 1.

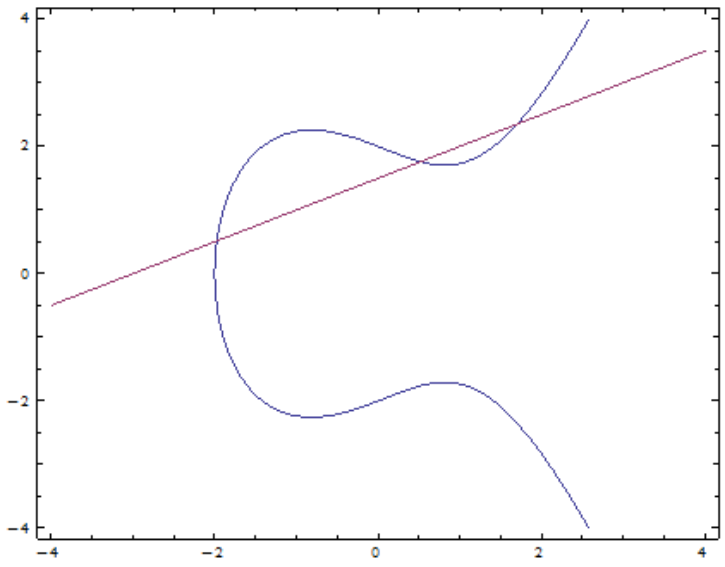

Fig. 1. Elliptic curve $y^2 = x^3 - 2x + 4$ and straight line $y = \frac{1}{2}x + \frac{3}{2}$

Source: own work.

It is obvious, that each simple line, which is not parallel to axis *Y*, may cut the elliptic curve in three points (we double count the point of contact). For this curve, the point in infinity 0_E should be considered as the point placed infinitely far on axis *Y*, in the direction of more and more steep tangents of this curve, it is the "third point of cut" of every straight vertical, which cuts or is tangent to curve *E*, with this curve. The basic operation on the elliptic curve is adding its points. To define this operation it is advisable to use geometric intuition while analysing Graph 1. The operation of adding points of the elliptic curve can be summarized as follows:

Sum of three points, where straight line cuts elliptic curve equals 0_E

The geometric law of adding points lets us easily see how to add two points of the elliptic curve so we can get the third one. One needs an algebraic formula to do this numerically. Here we present the general formulas, which are true for any characteristic fields different from 2 and 3.
Let

$$P=(x_1,y_1)\ ,\ Q=(x_2,y_2)\ \in$$
$$E(K)=\left\{(x,y)\in K^2 : y^2=x^3+ax+b\ ;a,b\in K\right\}\cup\{0_E\}\ .$$

Then we have

$$P+Q=\begin{cases}0_E, & \text{if} \quad x_1=x_2 \text{ and } y_1=-y_2\\ (x_3,y_3), & \text{in other cases}\end{cases},$$

where $(x_3,y_3)=(d^2-x_1-x_2,\ d(x_1-x_2)-y_1)\in E(K)$,
and

$$d=\begin{cases}\dfrac{3x_1^2+a}{2y_1}, & \text{if} \quad P=Q\\ \dfrac{y_2-y_1}{x_2-x_1}, & \text{in other cases}\end{cases}.$$

Adding points of elliptic curve *E* makes it an abelian group with neutral element 0_E. In 1922, Mordell proved that an abelian group of any elliptic curve's points over field $\mathbb{Q}$ (rational numbers), is the simple sum of a finite subgroup made up of finite order points (torisonal subgroup) and a subgroup that is generated by a finite number of infinite order points. This asset enables us to use elliptic curves in cryptography. The works of [Miller 1986;

Koblitz 1987] were crucial in this field. From this moment, elliptic curves have been strictly analysed for cryptography purposes. There were proposed plenty more secure ways of ciphering and digital signatures, usually used on the Internet. Currently, cryptography that uses elliptic curves has become a benchmark (the Canadian firm Certicom is the world leader in creating cryptographic technology, which uses elliptic curves; it has over 130 licences connected with them). The basic elements from which a cryptosystem based on elliptic curve E, over finite body F_q is built, are calculating the sum given by $P + P + ... + P = kP$, where P is the point of elliptic curve E, and k is the integer. It turns out that this can be made using a repeated doubling operation in $O(\log_2 k(\log_2 q)^3)$ bit operations. This means that the algorithm is fast enough to be used in practice. The security of this cryptosystem is based on the fact that having elliptic curve E, point P, which belongs to it, and point kP of this curve, it is hard to find integer k. This is a **discrete logarithm problem** on the elliptic curve. It is said that if curve E and field F_q are chosen correctly, solving the discrete logarithm problem in $E(F_q)$has a computational complexity that depends exponentially on the size of field F_q. Given that, algorithms which enable this have basically no practical use.

Example 3. Almost every cryptosystem with an open key which is used currently, has its elliptic curve analogue. Here we present the ElGamal analogue [Yan 2006; Wilkowski 2009]:

- Alice and John present publically the choice of elliptic curve E over the field F_q, where $q = p^j$ and p is a large prime number, as well as random point $P \in E$,
- Alice chooses randomly integer r_A (Alice's private key) and marks point $r_A P$ (Alice's open key); John also randomly chooses integer r_B (John's private key) and marks $r_B P$ – John's open key (numbers r_A, r_B are secret while $r_A P$ and $r_B P$ publically known),
- Alice randomly chooses integer k (secret) and sends pair of points $\left(kP, M + k\left(r_B P\right)\right)$ to John,
- John evaluates $M + k\left(r_B P\right) - r_B(kP)$ in order to read message M.

By sending a message to Alice, John uses the same algorithm. Every internet user knows elliptic curve E, point P and the open keys of Alice and John, so one can easily send them secret messages. In order to decode the

message, one has to deal with evaluating the discrete logarithm on curve *E*. As long as the effective method of doing that is not known, the algorithm is safe.

Example 4. There are also some elliptic-curve-based algorithms recommended by NSA in SuiteB (for details see Table 1). The PDF document from 2010, which can be found on www.nsa.gov (*Mathematical routines for the NIST prime elliptic curves)*, shows some examples on elliptic curve parameters and start point *P*, which are the base of a safe cryptosystem. Coefficients *a*, *b* from (1) in definition 1 are equal to:

$$a = 2^{521} - 4 = 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148,$$

$$b = 1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984.$$

When creating an elliptic-curve-based algorithm, the appropriate choice of start point *P* is very important. In the aforementioned case, it is given by:

$$P = (x_P, y_P),$$

where

$$x_P = 2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846,$$

$$y_P = 3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784.$$

The order of point *P* which (and also the order of group of points of curve given by *a*, *b*) is then equal to *q*, where

$$q = 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449.$$

Finally, quantum cryptography, which uses classical cryptography as well as quantum mechanics, is also worth mentioning. Its main tool is the hypothetical quantum computer [Monroe, Wineland 2008], understood as a physical system, which is designed in such a way that the outcome of its

evolution (in accordance with quantum mechanics laws) will represent the solution of the specified calculation problem. Using such a computer allows to generate ”truly random” random numbers [Mitra 2009] or to factorize natural number N in time $O(\log_2 N)^3$ and memory $O(\log_2 N)$. A proposition of the appropriate algorithm can be found in (Shor 1996). Creating such algorithms would probably be the end of RSA cryptosystems. Two years ago, the Canadian corporation D-Wave presented D-Wave One which is named after the first quantum computer in the world. The results of this machine can be found in [Boixo et al. 2013]. Catherine McGeoch and Cong Wang are scientists who were the first to compare quantum computers with classic (as for solution) problems of optimization. Their article, published under the name Experimental Evaluation of an Adiabiatic Quantum System for Combinatorial Optimization (this can be found on: http://graphics8.nytimes.com/ packages/pdf/ business/quantum-study.pdf), describes experiments in which the quantum computer D-wave Two was used. The results of these experiments show that for those optimization problems which can be run directly on quantum machines, D-wave is more than 4000 times faster than software solutions. When it comes to classic linear algebra problems, using the quantum computer enabled to solve the system of two equations with two unknown factors [Cai et al. 2013]. The authors of the aforementioned work say that the right solutions are usually found nine of ten times but so far it is an immanent attribute of quantum computers.

5. ZT-UNITAKOD method

In this section we talk about the cryptosystem which may improve ICT security. It was created in the early 2000’s in the Wroclaw University of Technology. It is based on the dynamic encryption concept [Juzwiszyn, Wilkowski 2005]. Until then, each cryptosystem had:

- an assignment table,
- a solid, secure key, which requires to be created,

secured, stored and sent,

- the whole was controlled by humans.

These methods are not required in ZT-UNITAKOD [Topolewski 2002]. In this method there is no assignment table (as each sign randomly accepts one of the 256 possible, different every time, forms) or a solid secure key. The human deciding factor is also limited in the system of secured information. It is solely based on permutation generators and mathematical models, which create a disposable, dynamic key. This means that the code

changes with the change of date and time (usually every second). This method is secured by a patent in the USA (no 08/775, 253-SYSTEM AND METHOD ZT-UNITAKOD FOR ENCRYPTING AND DECRYPTING DATA). More information on it can be found here: www.perfect-crypt.pl. The mathematical model of the code is given by:

$$Code = A + B\left(mod\,256\right),$$

where A is a cryptographic table, disposable, dynamic key (it is 256x256 array, which changes with the change of time), and B is the sent public text. The decrypt model is given by:

$$B = S - A\left(mod\,256\right), \quad \text{for} \quad S - A \geq 0,$$

$$B = \left(S - A\right) + 256\left(mod\,256\right), \ \text{for} \quad S - A \leq 0.$$

There are usually two permutation generators to create cryptographic Table *A:*

- multiplicative generator $G_1 = cx_i \left(mod\,256\right)$, where c are the odd numbers from 3 to 255 ,
- mixed generator $G_2 = ax_i + b\left(mod\,256\right)$, where a are the odd numbers from 1 to 255 which meet the following equation $a = 1\left(mod\,4\right)$, b are the odd numbers from 1 to 255.

The cryptographic table has 256 rows and 256 columns, so A has 65536 bites. Because of that the number of possible permutations is given by:

$$(256!)^{256}.$$

This is the potential power of cryptosystems based on the ZT--UNITAKOD method (better than the currently used RSA-type methods).

It seems, that the commonly used asymmetric algorithms (e.g. based on elliptic curves) should be used to send software of cryptosystems based on the ZT-UNITAKOD method. When there is a low number of potential users (e.g. chairmen of banks, diplomats), dynamic coding is the best solution for sending important information between them and cypher databases. The methods based on dynamic coding, as well as cryptosystems based on one-way functions, will very likely become more and more popular in the near future.

6. Phishing

In this section ways of securing internet users from phishing will be discussed [Cranor 2009; Wilkowski 2009]. It is one of the most popular internet crimes. According to Wikipedia, phishing is *"the attempt to acquire sensitive information such as user names, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies."* In the USA alone, the loss caused by phishing in 2007 had a value of 3,2 billion dollars [Cranor 2009]. Let us now provide some advice that may be helpful while surfing the Web:

- one should first verify the authenticity of the e-mail with a request to visit and log in some services,
- one should not open hyperlinks directly from e-mail,
- if you have any doubts about the page address, use web browser (a fake address will not appear at the beginning of the result list),
- remember to update your software as often as possible,
- you should not send your passwords or personal data under any circumstances,
- most services use HTTPS protocol, so if the visited page does not use this protocol, you should not enter there any passwords, etc.,
- using OpenDNS is advisable (OpenDNS is a free server system and communication protocol which enables converting addresses known by people into those understandable for the Web),
- do not use newly created web sites,
- do not use sites with a known logo when it does not belong to its owner,
- URL that has @, -, IP address, or more than 5 dots are suspicious.

More information can be found in [Cranor 2009] or under this address: http://apwg.org/advice. The technics used for preventing phishing are shown in [Khan 2013].

References

Blake I., Seroussi G., Smart N. (2004). *Krzywe eliptyczne w kryptografii,* Wydawnictwa Naukowo-Techniczne. Warszawa.

Boixo S., Isakov S., Wang Z., Wecker D., Lidar D., Martinis J., Troyer M. (2013). *Quantum annealing with more than one hundred qubits*. arXiv:1304.4595v1 [quant-ph] 16 April 2013.

Cai X.-D., Weedbrook C., Su Z.-E., Chen M.-C., Mile Gu, Zhu M.-J., Li Li, Nai-Le Liu, Lu C.-Y., Pan J.-W. (2013). *Experimental quantum computing to solve systems of linear equations,* Physical. Review Letters 110.

Cranor L. (2009). *Czy phishing da się zwalczyć ?* „Świat Nauki". No 1 (209).

Joux A. (2013). *Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields.* Cryptology ePrint Archive: Report 2012/720.

Juzwiszyn J., Wilkowski A. (2005). *Kryptografia dynamiczna.* Prace Naukowe Akademii Ekonomicznej. No 1096. Wrocław.

Khan A (2013). *Preventing Phishing Attacks using One Time Password and User Machine Identification.* International Journal of Computer Applications. Vol. 68. No. 3.

Koblitz N. (1987). *Elliptic Curve Cryptosystems.* Mathematics of Computation. No 48.

Koblitz N. (2000). *Algebraiczne aspekty kryptografii.* Wydawnictwa Naukowo-Techniczne. Warszawa.

Miller V. (1986). *Uses of Elliptic Curves in Cryptography.* Advances in Cryptology. CRYPTO '85. Proceedings. Lecture Notes in Computer Science. No 218. Springer-Verlag.

Mitra A. (2009). *Uncontrollable random number generation is possible*. arXiv:0904.3677 Fri. 24 Apr 2009.

Monroe Ch., Wineland D. (2008). *Jonowe maszyny cyfrowe.* Świat Nauki. No 9 (205).

Shor W. (1996). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. arXiv:quant-ph/9508027v2 25 Jan 1996.

Silverman J. (1994). *Advanced Topics In the Arithmetic of Elliptic Curves.* Springer-Verlag.

Topolewski Z. (2002). *Komputerowe zabezpieczenie poufności informacji w zarządzaniu.* Wydawnictwo Continuo. Wrocław.

Wilkowski A. (2009). *Elliptic curves and their uses in Internet security*. Mathematical Economics. No 5(12). The Publishing House of the Wrocław University of Economics. Wrocław.

Yan S. (2006). *Teoria liczb w informatyce.* Wydawnictwo Naukowe PWN. Warszawa.