ECvisual: A Visualization Tool for Elliptic Curve Based Ciphers

Jun Tao, Jun Ma
Department of Computer Science
Michigan Technological University
Houghton, MI
{junt,junm}@mtu.edu

Melissa Keranen
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI
msjukuri@mtu.edu

Jean Mayo, Ching-Kuang Shene
Department of Computer Science
Michigan Technological University
Houghton, MI
{jmayo,shene}@mtu.edu

ABSTRACT

This paper describes a visualization tool ECvisual that helps students understand and instructors teach elliptic curve based ciphers. This tool permits the user to visualize elliptic curves over the real field and over a finite field of prime order, perform arithmetic operations, do encryption and decryption, and convert plaintext to a point on an elliptic curve. The demo mode of ECvisual can be used for classroom presentation and self-study. With the practice mode, the user may go through steps in finite field computations, encryption, decryption and plaintext conversion. The user may compute the output for each operation check each answer for correctness. This helps students understand the primitive operations and how they are used in an elliptic curve cipher. The opportunity for self-study provides an instructor greater flexibility in selecting a lecture pace for this detail-filled material. Classroom evaluation was positive and very encouraging.

Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education—*Computer science education, information systems education*

General Terms

Algorithms, Security

Keywords

Cryptography, visualization

1. INTRODUCTION

Modern cryptography research started in the late 1960's, and was quickly developed into a significant field in mathematics and computer science. Landmark textbooks and handbooks appeared [5, 7, 8, 9] and schools began offering courses in cryptography. Due to the increasing interests in network/data security, the CS education community also started to add cryptography into the CS curricula. The demographics of the students taking these courses may cause challenges for educators. While CS students have difficulty dealing with the sophisticated mathematics that the cryptosystems are built upon, Mathematics majors often get lost in the details of the complicated algorithms.

Well-designed pedagogical tools can be used to help alleviate these problems and enhance the learning both inside and outside of the classroom. In recent years, we saw a flood of visualization tools published; however, they are mainly on teaching security (*e.g.*, [11, 12]) with some on cryptography (*e.g.*, [3, 10, 14, 15]). We could not find visualization tools for the elliptic curve based ciphers even though this type of cipher is becoming more important in practice. Thus, we chose to develop ECvisual to fulfill our needs and at the same time contribute to the CS education community. ECvisual is flexible in that it can be used as a demonstration tool in class and also be made available to students to use as a self-study tutorial for them to explore on their own. ECvisual is part of a larger project to provide visualization tools to help address the challenges of teaching cryptography.

ECvisual was used in a junior-level introductory cryptography course. The evaluation showed that it was effective and computer science and mathematics related students rated ECvisual highly although there were small variations among different disciplines. On the other hand, reactions from other students were somewhat different, and further investigation would be needed to determine the cause.

In the following, Section 2 provides the background of our cryptography course, Section 3 presents our visualization tool, Section 4 is a detailed study of our findings from a classroom evaluation, and Section 5 is our conclusion.

2. COURSE INFORMATION

ECvisual was used in a cryptography course, MA3203 Introduction to Cryptography, that was offered out of the Department of Mathematical Sciences at Michigan Technological University. It is a Junior level course that gives a basic introduction to the field of Cryptography. Our course covers classical cryptography, the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), the RSA

SIGCSE '12 Raleigh, North Carolina USA

algorithm, discrete logarithms, hash functions, and elliptic curve cryptography. For each cryptosystem, we study how it was designed, why it works, how one may attack the system, and how it has been used in practice. One of the more recent advances in cryptography was the development of elliptic curve versions for many cryptosystems. The course ends with a study of elliptic curves and how they may be applied in the field of cryptography. The major topic studied is an elliptic curve based ElGamal cryptosystem.

The course is geared towards Mathematics majors, but typically the majority of students are not Math majors, and many of them are Computer Science majors. In this particular semester, the course consisted of 17 Computer Science majors, 9 Mathematics majors, and 12 from other majors.

ECvisual was used extensively in class to complement the lecture. The instructor first introduced the concept of an elliptic curve to the class. ECvisual was used to demonstrate what the graph of a typical elliptic curve looks like. It allowed the instructor to demonstrate both the addition law and the associative law graphically. The instructor then introduced elliptic curves modulo a prime, p. Here, ECvisual was used to demonstrate the addition of points in the field, and it was also used to show the subgroup of any particular point. When the elliptic curve version of the ElGamal cryptosystem was introduced in class, the instructor used ECvisual to demonstrate the algorithm as well as the method used to covert plaintext to a point on the elliptic curve.

In addition to the benefits for demonstration, ECvisual also has practice components built in to allow students to work with elliptic curves on their own. ECvisual was made available to students to download on their own computer. With ECvisual, one is able to practice adding points on the curve, converting plaintext to a point on the curve, encrypting, and decrypting points.

After the students had access to the software for a week, the instructor distributed a survey to the class. Extra credit was offered to anyone who used the software and completed the survey.

3. SOFTWARE DESCRIPTION

ECvisual is designed to help instructors teach and students learn the elliptic curve based ElGamal cryptosystem. It supports Linux, MacOS and Windows. ECvisual has two subsystems, one over the real field and the other over a finite field of order p. Due to screen space limitation, p is restricted to no more than 17. ECvisual has two operation modes: the demo mode and the practice mode. The demo mode may be used by instructors for classroom demonstration and by students to visualize the detail of computations. The practice mode is designed to help students go through the computations step-by-step and perform self-study. Thus, a student may use the practice mode to step through a computation procedure, fill in the answers, and check for correctness.

ECvisual has three pages, the Table page, the Curves page, and the Finite Field page. When ECvisual starts, the Table page is shown, and this is where the elliptic curve formula is set. One can define a particular curve to work with by choosing appropriate parameters on this page (Section 3.2). The continuous elliptic curve is shown on the Curves page (Section 3.1). The Finite Field page illustrates the finite field of an elliptic curve (Section 3.2). This page also includes encryption and decryption (Section 3.3) and plaintext to elliptic curve point conversion algorithms (Section 3.4).

3.1 The Elliptic Curve Group over Reals

This component provides the user with an opportunity to practice and visualize the elliptic curve group over the real number field. The user selects an elliptic curve by supplying the a and b in $y^2 = x^3 + ax + b$. Then, ECvisual draws the curve, allows the user to zoom in and out, selects two points P and Q, computes the intersection point of the line PQ and the curve (*i.e.*, $-$(P+Q)), and shows P+Q.

To visualize the associative law, the user clicks on the Associative Law button, picks three points P, Q and R, and ECvisual displays intermediate computations showing P+Q+R = (P+Q)+R = P+(Q+R) (Figure 1). Thus, the user should be able to easily learn the abstract idea via visualization.

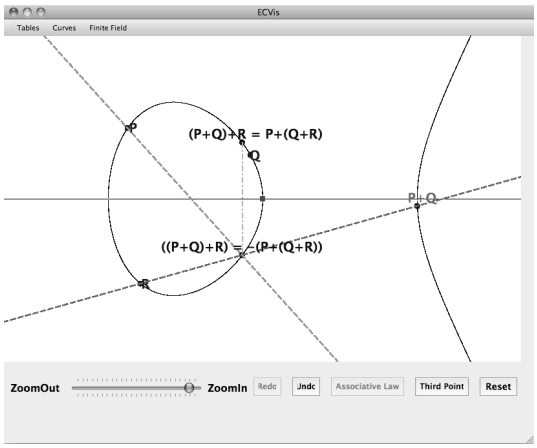

Figure 1: The Elliptic Curve Associative Law

3.2 The Elliptic Curve Group over a Finite Field

The elliptic curve group over finite field $\mathbf{Z}_p$ component helps students visualize and practice elliptic curve computations over a finite field of prime order. The user supplies a prime number $p > 3$ and the parameters a and b in $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$ must hold. Then, the system displays a grid and all points on the curve with the identity element marked as inf at the center of each edge of the grid (Figure 2).

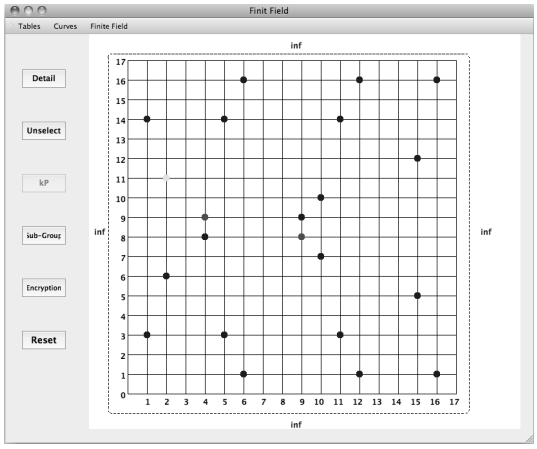

Figure 2: An Elliptic Curve Over a Finite Field: $y^2 = x^3 + 3x + 5$ (mod 17)

The user may click on the Table button to show the addi-

tive, multiplicative, and additive and multiplicative inverse tables (Figure 3).

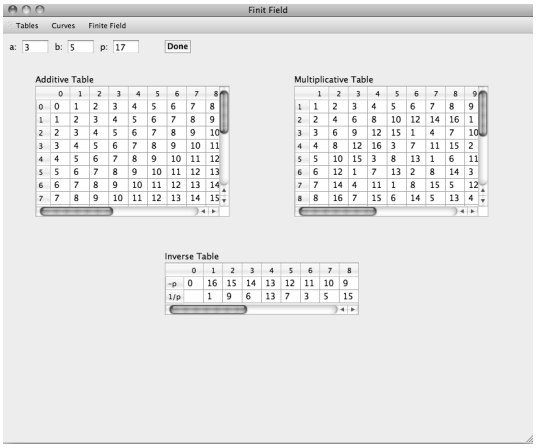

Figure 3: Addition, Multiplication, and Inverse Tables Over a Finite Field: $y^2 = x^3 + 3x + 5$ (mod 17)

The Detail button (Figure 2) on the left panel brings up the **Detail Computation** window with which the user can practice computations on an elliptic curve. For example, the user may click on two points, which are shown in red and whose values are shown in the **Detail Computation** window as P and Q in the order of selection (Figure 4). Initially, all fields other than P and Q are blank. The user may choose Run, Step or Practice. The Run button asks the system to compute P + Q and displays all intermediate results such as $y_2 - y_1$, $x_2 - x_1$, the multiplicative inverse of $x_2 - x_1$ (*i.e.*, $(x_2 - x_1)^{-1}$), the slope λ of the line PQ, the x-coordinate of the intersection point of line PQ and the elliptic curve, and the corresponding y-coordinate. The point P + Q is shown in yellow.

The user may select Step to step through the computation. In this case, the user fills in the result one-by-one with the help of the computation tables (Figure 3), and the system verifies the input and displays **Correct!** if the answer is a correct one. The user may also select Practice and fill in *all* answers. The system then verifies all input and displays **Correct!** if all of them are correct. Incorrect answers are highlighted and **Wrong!** is displayed.

With this environment, the user may try to find a subgroup of prime order by repeatedly computing P, 2P = P+P, etc until $(n-1)$P is the identity. This can be performed by clicking on the kP button on the left panel. ECvisual is also

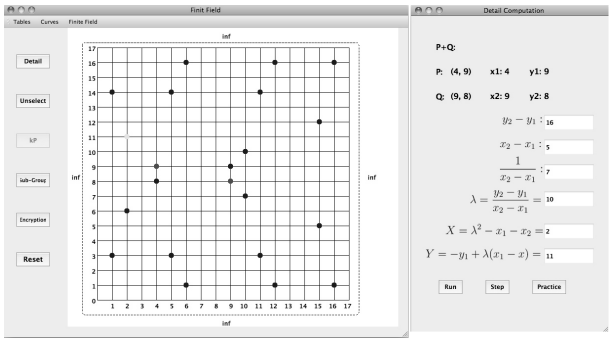

Figure 4: Compute $(2, 11) = (4, 9) + (9, 8)$

able to find and display *all* subgroups of prime order by clicking on the Sub-Group button. Each subsequent click on the Sub-Group button will cycle through the prime order subgroups one-by-one. Thus, the user may step through these subgroups to choose an appropriate one for encryption. The preferable subgroup is the one with maximum prime order. Figure 5 shows a subgroup of order 23 with the edges showing the generation order of this subgroup.

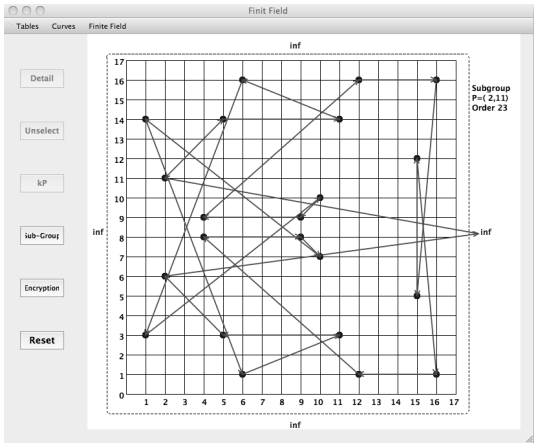

Figure 5: A Subgroup of Order 23 Starting with $(2, 11)$: $y^2 = x^3 + 3x + 5$ (mod 17)

3.3 Encryption and Decryption

Once a maximum prime order subgroup is found, the p in $\mathbf{Z}_p$, the equation of the chosen elliptic curve, and the point P and its order n are the public domain parameters. After this, the user may practice encryption and decryption easily by clicking on the Encryption button. This brings up the **Encryption & Decryption** window. For example, the user may select a private key d randomly in the interval $[0, n-1]$ and compute the public key Q= dP. The sender represents the text by a point M on the elliptic curve, selects randomly a number k in $[1, n-1]$, computes $C_1 = k$P and C_2 =M+kQ, and sends (C_1, C_2) to the recipient. The recipient uses her private key d to compute $dC_1 = d(k\mathsf{P}) = k(d\mathsf{P}) = k\mathsf{Q}$, and, hence, recovers M= $C_2 - k$Q. In this way, elliptic curve encryption and decryption can be practiced easily with the visualization/practice system.

Figure 6 shows an encryption practice session. The system selects point P and a subgroup of maximum prime order, and allows the user to select a private key and fill in intermediate results. Again, the system will tell the user whether his/her computation is correct or wrong.

3.4 Plaintext to Elliptic Curve Point

Converting a plaintext to a point on an elliptic curve is not very trivial and requires larger p to be "practical." Hence, this component is independent of the remaining components because large p is impractical for visualization. ECvisual uses the Koblitz method [6]. Figure 7 shows a demonstration session of the Koblitz technique.

4. EVALUATION

The ECvisual survey consists of two components, a set of nine questions and 13 write-in comments. The nine questions are listed in Table 1. Choices available are 5:strongly

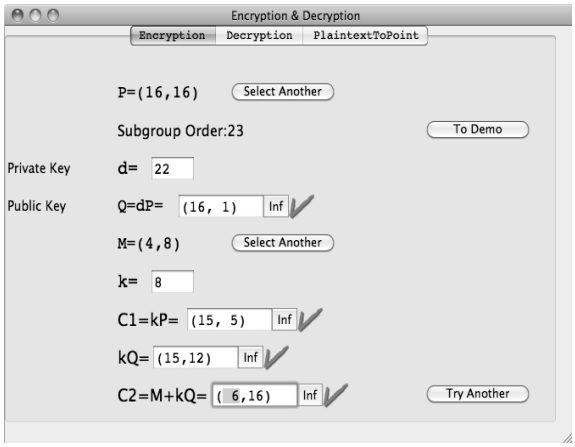

Figure 6: Encryption Practice: $y^2 = x^3 + 3x + 5$ (mod 17)

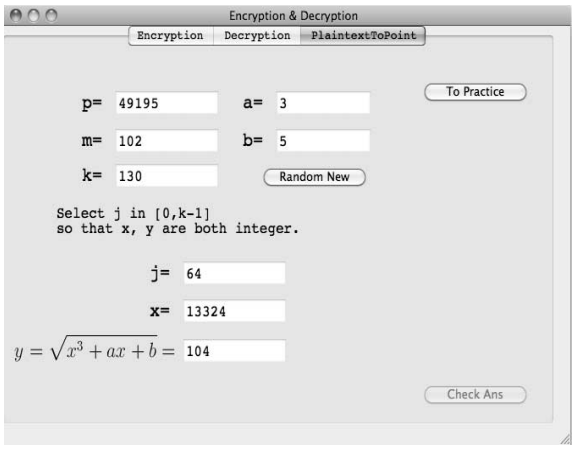

Figure 7: Plaintext to Elliptic Curve Point

agree, 4:agree, 3:neutral, 2:disagree, and 1:strongly disagree. Because we intend to study the impact of ECvisual on multiple disciplines, students were asked to fill in their disciplines. We collected 31 survey forms of which two were invalid. The distribution of majors is as follows: 3 in computer network and system administration (CNSA), 5 in computer and electrical engineering (CpE), 13 in computer science (CS), 5 in mathematics (Math), 1 in materials engineering, 1 in biological science, and 1 undeclared. The last three are grouped into the Other category.

4.1 General Discussion

Table 2 shows the mean and standard deviation of each question. In general, reactions to ECvisual are positive. The highest score of 4.2 with a small standard deviation of 0.5 was given to Q1, indicating that students agreed highly that ECvisual helped them understand what an elliptic curve is. Q4, Q5 and Q9 received the same score of 3.9, suggesting that ECvisual enhanced self-study and the course, and helped students understand the arithmetic on an elliptic curve. The remaining five questions were rated approximately the same (*i.e.*, 3.6 and 3.7) with slightly larger standard deviation. Thus, student reactions are mixed although the general trend is still in the positive side.

Correlations among student responses are high. The highest correlation is between Q2 and Q6 (0.87), which means students learned elliptic curve representations with the demo mode and practice mode. The lowest correlations 0.61 are between Q1 and Q8, and between Q1 and Q9. Overall, students answered questions in a rather similar pattern.

Table 3 shows the effect sizes (*i.e.*, Cohen's d [1, 4]) among questions. We noted that the mean of Q1 (4.2) is very different from those of Q2, Q3, Q6 and Q8 (3.6) with effect sizes no less than 0.8. Additionally, effect sizes among Q2, Q3, Q6 and Q8 are very small. Therefore, student responses to Q2, Q3, Q6 and Q8 are nearly identical, and significantly different from responses to Q1. The effect sizes between Q1 and Q4 (0.44) and Q1 and Q5 (0.36) are moderate, indicating responses to Q1 and Q4, and those to Q1 and Q5 are moderately different. Moreover, the effect size between Q4 and Q5 is zero, suggesting students answered these two questions nearly identically. Consequently, students liked ECvisual for elliptic curve arithmetic and for self-study. It is interesting to point out that, except for Q1, effect sizes of Q8 and other questions are very small (0) to moderate (0.52). This indicates that except for Q1, students ratings of Q8 and other questions are not very different. The effect sizes between Q9 and Q1 and between Q9 and Q8 are moderate (0.5); but, effect sizes between Q9 and other questions are very small (0.05) to moderate (0.4). Hence, except for Q1 and Q8, students rated other questions similar to Q9.

In summary, we found students felt that ECvisual helped them understand elliptic curves and their arithmetic, and also helped self-study.

4.2 Discipline Specific Discussion

Because the class has students from more than five disciplines, it is very helpful to understand the differences among these groups. Table 4 shows summary statistics by disciplines. On average, CS students rated ECvisual the highest

Table 1: Survey Questions

Number	Question
Q1	ECvisual's demo mode helped me understand what an elliptic curve is
Q2	ECvisual's demo mode helped me understand how to represent plaintext as a point on an elliptic curve
Q3	ECvisual's demo mode helped me understand how to encrypt and decrypt using elliptic curve version of the ElGamal cryptosystem
Q4	ECvisual's demo mode was helpful for my self-study
Q5	ECvisual's practice mode helped me understand how to add points on an elliptic curve
Q6	ECvisual's practice mode helped me understand how to represent plaintext as a point on an elliptic curve
Q7	I understand the elliptic curve version of the ElGamal cryptosystem more after I was able to use ECvisual
Q8	By using ECvisual I was able to identify the parts of the elliptic curve version of the ElGamal cryptosystem that I do not understand
Q9	ECvisual enhanced the course.

Table 2: Mean and Standard Deviation

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Mean	4.2	3.6	3.6	3.9	3.9	3.6	3.7	3.6	3.9
S.Dev	0.5	0.9	0.7	0.7	0.8	0.9	0.8	0.7	0.7

Table 3: Effect Sizes Among Questions

	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Q1	0.80	0.89	0.44	0.36	0.87	0.70	1.02	0.51
Q2		0.02	-0.30	-0.40	0.08	-0.10	0.09	-0.30
Q3			-0.40	-0.40	0.07	-0.20	0.08	-0.40
Q4				-0.00	0.44	0.24	0.50	0.05
Q5					0.46	0.27	0.52	0.09
Q6						-0.20	0.00	-0.40
Q7							0.24	-0.20
Q8								-0.50

(3.85) with the smallest standard deviation (0.21). Slightly lower is from CpE students (3.82) with a slightly larger standard deviation (0.34), meaning CpE student responses were not as concentrated as those of CS students. Both CNSA and Math students rated ECvisual similarly; but, CNSA has a smaller standard deviation. Students in Other rated ECvisual lower with the largest standard deviation.

Table 4: Discipline-Specific Summary Statistics

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
CNSA	4.0	3.3	3.7	3.7	3.7	3.7	4.0	3.7	4.0
CpE	4.2	3.8	3.6	4.2	4.0	3.4	3.6	3.4	4.2
CS	4.2	3.6	3.8	4.0	3.9	3.6	4.0	3.7	3.8
Math	4.2	3.4	3.4	3.8	4.2	4.0	3.4	3.6	4.0
Other	4.0	4.0	3.3	3.3	3.7	2.7	3.0	3.0	3.0

	CNSA	CpE	CS	Math	Other
Mean	3.74	3.82	3.85	3.78	3.33
S.Dev	0.22	0.34	0.21	0.34	0.47

Table 5 has the correlation coefficient and effect size of each discipline pair. The correlation between CS and CNSA (0.69) is the highest, followed by the correlation between CS and CpE (0.67). This suggests that ratings by CS, CpE and CNSA students are reasonably similar; however, the correlation between CNSA and CpE is smaller (0.31). On the other hand, correlation between CpE and Math and correlation between CpE and Other are slightly larger than 0.5. The correlation between Other and CNSA is -0.27, indicating students in these two disciplines rated ECvisual oppositely.

Table 5: Discipline-Specific Correlation/Effect Size

Numbers are presented as correlation (effect size)

	CpE	CS	Math	Other
CNSA	0.31 (-0.30)	0.69 (-0.55)	0.36 (-0.14)	-0.27 (1.17)
CpE		0.67 (-0.11)	0.53 (0.14)	0.52 (1.26)
CS			0.43 (0.28)	0.36 (1.51)
Math				0.10 (1.15)

The effect sizes of Other and other disciplines are rather large, suggesting students in Other rated ECvisual very differently from mathematics and computer related disciplines. The correlation (0.69) and effect size (-0.55) between CSNA and CS are moderate, indicating individual question ratings may still have a moderate difference. Other effect sizes are small, and rating differences are insignificant.

Given these findings, we may conclude that students in computer related disciplines (*i.e.*, CSNA, CS and CpE) rated ECvisual similarly, Math students have their own somewhat different view about the effectiveness of ECvisual, and students in Other have a significantly different feeling. But, we should keep in mind that sample size of the Other category is small and further investigation would be needed. This raises questions to be addressed in the future: (1) are there discipline differences in the use of visualization tools? (2) what are the causes of these differences? and (3) how can we address these differences?

4.3 Student Comments

The set of 13 write-in questions is designed to allow students to make suggestions which can be used for future development. We focus on the following issues: (1) whether elliptic curves modulo p for $p \leq 17$ is good enough, (2) whether the representation of the identity element (infinity) is intuitive, (3) whether the representation of subgroups of prime order is useful, (4) whether the elliptic curve version of the ElGamal cipher needs improvement, (5) the evaluation of the demo and practice modes, (6) frequency of using ECvisual for self-study, and (7) software installation problems.

Student comments showed that the $p \leq 17$ restriction is sufficient for understanding the concepts. Only a few mentioned p should be much larger to be "realistic". However, this is impractical because screen asset is not enough for large p visualization. One way to somewhat overcome this restriction would be adding a zooming capability and allowing the user to mouse over to see the details such as coordinates of a point.

There were no very negative comments on the design of ECvisual. Typical comments were "It is easy to use", "Perfect, except for the $p \leq 17$ thing", "Good design, easy to follow and very helpful in learning the system" and "Simple and to the point." Some issues were raised. Major ones were (1) should support $p > 17$ as mentioned earlier, (2) should use symbols and notations exactly the same as in the textbook, (3) finite field computation tables should always be visible and available rather than putting them under a tab, and (4) providing comments and descriptions for each step would be more user friendly and more convenient.

Students were very positive about the identity element and subgroups visualization. Some indicated "the identity element helped me understand exactly how infinity was represented" while one student believed the identity element should only be above the top edge. Comments for the subgroups of prime order were nearly all positive. Students said "It was very clear and useful", "I like that it lights up all the dots, a very useful setup", and "I like being able to cycle through subgroups and orders". Again, some students wished to have step-by-step comments and descriptions so that they can follow the flow easier.

The practice mode was also very welcome with comments like "The practice mode is also good. If an answer is wrong there will be a big warning sign to inform you", "The practice mode helped check that you are doing the work correctly, so that is useful", "The practice mode works well and allows for some user interaction", and "Good to check answers. It is useful to be able to switch between practice and demo".

Because the students only had a week to play with ECvisual before taking this survey, the frequency of using this tool is not very high. Most of them used the tool a few times, and a few of them played with the tool "quite often". In general, they used ECvisual when they were solving

problems, checking for some details, forgot the inner working of the algorithm, and used it for practice and further understanding. Since the encryption and decryption algorithms are simple once the concepts of finite fields and elliptic curves are understood, we are not surprised by the fact that a few students only used it once or twice, or did not use it at all. As a result, some students said this component is useful or somewhat useful. Students did not report any installation issues, although three of them complained about system crashes.

In summary, with the statistics and student comments presented above, we believe ECvisual has fulfilled its purpose, helping students learn and the instructor teach the ElGamal cryptosystem based on elliptic curves over finite fields. With the comments and suggestions, we should be able to improve ECvisual significantly in the near future.

5. CONCLUSION

The above presented a visualization tool ECvisual for teaching and learning elliptic curve groups over the real field and over a finite field of prime order, and the ElGamal cryptosystem based on elliptic curves. With ECvisual instructors are able to present all the details and inner working of these algorithms. It also helps students see the "flow" of each algorithm, learn the concepts about elliptic curves, and practice the computation steps using the practice mode.

Our evaluation results showed that ECvisual was effective in classroom presentation and for student self-study. Students in this class were in five disciplines with computer science majors being the largest. We also investigated the impact of ECvisual on each group. Our findings indicated that the computer science related group reacted to ECvisual in the most positive way. The non-CS and non-Math majors reacted to ECvisual slightly differently, but the sample size of this group is very small. It is interesting to point out that the same trend was observed in our earlier DESvisual study [15]. Whether this is a disciplinary difference is not clear at this point and further investigation is required. However, the positive impact of ECvisual on computer science students learning is undeniable.

ECvisual is a part of larger development project of cryptography visualization tools. In the near future, ECvisual will be extended in a number of ways. The most needed extensions are (1) the support of larger finite field (*i.e.*, larger p) and better ways of navigation and visualization, (2) a better visualization for the finite field grid, perhaps automatically adjusting the maximum value of p by a detection of screen size and permitting zooming, (3) a better operation scheme that allows the user to mouse over the finite field grid to show the coordinates of each point, (4) a better design so that the finite field tables are always visible and available, (5) a better hint, comment, and error reporting feature so that the user can retrieve the needed hints and comments easily for self-study, and (6) a library to support elliptic curve cryptosystems based programming assignments. Moreover, we plan to design a class library with which student programs may turn on or off the visualization feature without extra instrumentation so that the visual aid may also be used as a debugging tool. In other words, ECvisual becomes the front-end of a larger system that supports programming and visualization. This technique was used in ThreadMentor successfully [2, 13].

Prototypes of DESvisual and ECvisual and classroom evaluation forms are available at the following URL:

`http://www.cs.mtu.edu/~shene/NSF-4`.

6. REFERENCES

[1] M. Borenstein, L. V. Hedges, J. P. T. Higgins, and H. R. Rothstein. *Introduction to Meta-Analysis*. Wiley, 2009.

[2] S. Carr, J. Mayo, and C.-K. Shene. ThreadMentor: A pedagogical tool for multithreaded programming. *ACM Journal on Educational Recourses in Computing*, 3(1), March 2003.

[3] G. Cattaneo, D. D. Santis, and U. F. Petrillo. Visualization of cryptographic protocols with grace. *Journal of Visual Languages & Computing*, 19:258–290, 2008.

[4] J. Cohen. *Statistical Power Analysis for the Behavioral Sciences*. Lawrence Earlbaum Associates, Hillsdale, NJ, second edition, 1988.

[5] D. E. R. Denning. *Cryptography and Data Security*. Addison-Wesley, 1982.

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

[7] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[8] A. Salomaa. *Public-Key Cryptography*. Springer-Verlag, 1992.

[9] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, second edition, 1995.

[10] D. Schweitzer and L. Baird. The design and use of interactive visualization applets for teaching ciphers. In *Proceedings of the 7th IEEE Workshop on Information Assurance*. IEEE, June 2006.

[11] D. Schweitzer and L. Baird. Grasp: A visualization tool for teaching security protocols. In *Proceedings of the 11th Colloquium for Information Systems Security Education*, 2006.

[12] D. Schweitzer and W. Brown. Using visualization to teach security. *Journal of Computing Sciences in College*, 24(5):143–150, May 2009.

[13] C.-K. Shene. Multithreaded Programming with ThreadMentor: A Tutorial, 2001. `http://www.cs.mtu.edu/~shene/NSF-3/e-Book/index.html`.

[14] X. Simms and H. Chi. Enhancing cryptography education via visualization tools. In *ACM Southeast Regional Conference*, pages 344–345. ACM, March 2011.

[15] J. Tao, J. Ma, M. Keranen, J. Mayo, and C.-K. Shene. DESvisual: A visualization tool for the des cipher. *Journal of Computing Sciences in College*, 27(1):74–80, 2011.