Better Privacy and Security in E-Commerce: Using Elliptic Curve-Based Zero-Knowledge Proofs

Sultan Almuhammadi, Nien T. Sui, and Dennis McLeod
Department of Computer Science, University of Southern California
Los Angeles, CA 90089-0781, USA
E-mail: salmuham@usc.edu, sui@usc.edu, mcleod@usc.edu

Abstract

We propose an approach using elliptic curve-based zero-knowledge proofs in e-commerce applications. We demonstrate that using elliptic curved-based zero-knowledge proofs provide privacy and more security than other existing techniques. The improvement of security is due to the complexity of solving the discrete logarithm problem over elliptic curves.

Index terms – E-commerce, security, privacy, zero-knowledge proofs, elliptic curves.

1. Introduction

E-commerce is not dead, but it is thriving! According to the eSpending report, online shoppers spent $2.95 billion during the second week of December 2003, which is a 48% increase from the same period of 2002. [1] However, the security and privacy challenges are ever increasing. Fraud in credit card payments has increased to around 3% of total transaction volume. [2]

Researchers have proposed different solutions for different challenges of e-commerce. Most of the verification solutions are based on obtaining more information from the user, such as zip code, secret pin, etc. This private information if not handled properly can be a source of future fraud as indicated in [2]. Even without the risk of possible future fraud, revealing such personal information undermines customers' privacy (Why does a customer service operator need to know the customer's mother's maiden name?) Therefore, using a verification system that protects privacy and security at the same time is essential.

This research was supported in part by the Integrated Media Systems Center at USC. The views and conclusions contained in this paper are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the funding agency. Figures and descriptions in this paper were provided by the authors and are used with permission.

In this paper, we are proposing an approach using elliptic curve-based zero-knowledge proofs in e-commerce applications. Our approach provides higher efficiency and better security and privacy. In particular, zero-knowledge proofs (ZKP) can be used whenever there is a need to prove the possession of critical data without a real need to exchange the data itself. Examples of such applications include: credit card verification, digital cash system, digital watermarking, and authentication.

2. Related work

Many e-commerce applications have been implemented not using zero-knowledge proofs techniques for verification purposes. Most of these solutions reveal more information in order to achieve verification. However, researchers have shown that zero-knowledge proofs can be utilized in e-commerce applications, such as Anonymity revocable off-line electronic cash scheme and digital watermark detection [4].

Nguyen et al. presented a batching technique for zero-knowledge proofs to speed up the process of verification in digital cash and fair exchange [5]. However, their ZKP is implemented using modulo n over the multiplicative group Zn. We are proposing implementing ZKP using elliptic curves in e-commerce. This will increase the security level, due to the fact that solving the discrete log problem over elliptic curves takes exponential time, as opposed to sub-exponential time for discrete logarithm over Z_n. [6] [7]

3. Zero-knowledge proofs overview

Zero-knowledge proofs are used when someone (the prover) has to prove to someone else (the verifier) his/her knowledge of secret information without

revealing any information about the secret that the verifier cannot get without executing the protocol.

3.1. Definition of zero-knowledge proofs

From its name, a zero-knowledge proof has two parts:

(1) **Proof**: It should prove convincingly that Peggy knows the secret. At the end of the protocol, Victor should be convinced that Peggy knows the secret. The protocol should not allow Peggy to cheat (within a certain probability in iterative proofs). She must not be able to produce her part of the dialogue without knowing the secret.

(2) **Zero-knowledge:** It should not give Victor any information about the secret. This means that it should be computationally infeasible for Victor to retrieve the secret from the information in the dialogue. [5]

3.2. Classical problems

There are various classical problems that involve zero-knowledge proofs. In this paper, we present two of these problems, namely the discrete logarithm problem [8] and the square root problem [4] these are to be compared to the same problems using elliptic curves, which will be introduced in Section 4.

3.3. Discrete logarithm (DL) problem

Peggy, the prover, wants to prove in zero-knowledge that she knows the discrete logarithm of a given number modulo n. That is, given n, generator g for some field Fn, and b ∈ Fn, to prove in zero-knowledge that Peggy knows x such that

$$g^x = b \ (mod\ n).$$

Solving discrete logarithm problem is known to be computationally infeasible. Therefore, people are interested in proving the knowledge of such a secret without revealing it.

Solution: Peggy generates a random r and computes $h = g^r \bmod n$. She sends h to Victor. Now Victor flips a coin and conveys the outcome to Peggy. If it is heads, Peggy sends r to Victor and he verifies $g^r = h$. If it is tails, she sends $m = x + r$ and Victor verifies $g^m = b.h$. These steps are repeated until Victor is convinced that Peggy must know x with probability of $(1\text{-}2^{-k})$, where k is the number of times these steps are repeated. Figure 1 summarizes this protocol.

		Peggy (P)	Victor (V)
0		g, b, n, x	g, b, n
1	Peggy generates random r	r	
2	P sends $h = g^r \bmod n$ to V	h	h
3	V flips a coin c = H or T	c	c
4	If c = H, P sends r to V		Check $g^r = h$
5	If c = T, P sends m = x + r		Check $g^m = b.h$
6	Steps 1-5 are repeated until Victor is convinced that Peggy must know x (with probability $1\text{-}2^{-k}$, for k iterations).		

Figure 1: ZKP Discrete log problem

3.4. Square-root problem

Peggy wants to prove in zero-knowledge that she knows the square root of a given number modulo a large composite number n. i.e. to prove in zero-knowledge that she knows x such that

$$x^2 = b \ (mod\ n),\ \text{for known } b, n.$$

Solution: Peggy generates a random r and computes $s = r^2 \ mod\ n$. She sends s to Victor. Victor flips a coin and accordingly asks Peggy for either r or $m = r.x$. Victor verifies the value he receives. By repeating these steps enough number of times, Victor can be convinced. Figure 2 summarizes the steps of this protocol.

		Peggy (P)	Victor (V)
0		b, n, x	b, n
1	Peggy generates random r	r	
2	P sends $s = r^2 \bmod n$ to V	s	s
3	V flips a coin c = H or T	c	c
4	If c = H, P sends r to V		check $r^2 = s$
5	If c = T, P sends m = r.x		check $m^2 = s.b$
6	Steps 1-5 are repeated until Victor is convinced that Peggy must know x (with prob $1\text{-}2^{-k}$, for k iterations).		

Figure 2: ZKP Square-root problem

4. Zero-knowledge proofs using elliptic curves

In this section, we show two examples of using elliptic curve in zero-knowledge proof. One example is on discrete logarithm over elliptic curve (DLEC) problem, and the other is on square root problem over elliptic curve (SREC). We choose these two examples to show why elliptic curve is good for one but not the other, as we explain in the next section.

An elliptic curve over some field K (of characteristic ≠ 2, 3) is the set of all points $(x, y) \in K \times K$ that satisfy the equation: $y2 = x3 + ax + b$, where $a, b \in K$. If characteristic of K is 2 or 3, then the elliptic curve equation will have some other types [8].

4.1. Discrete logarithm over elliptic curve problem

Given an elliptic curve E over a field F_n, $G \in E/F_n$ (where G is a generator, or its order contains a large prime), and $B = m.G \in E/F_n$, Peggy wants to prove in zero-knowledge that she knows m such that $m.G = B$.

Solution: Since Peggy claims that she knows m such that $m.G = B$, where B is public, she generates a random $r \in F_n$ and computes $A = r.G$. She sends A to Victor. Now Victor flips a coin and conveys the outcome to Peggy. If it is heads, Peggy sends r to Victor and he verifies that $r.G = A$. If it is tails, she sends $x = r + m$ and Victor verifies $x.G = A+B$. Repeating these steps increases exponentially the confidence of Victor that Peggy knows the secret m. See Figure 3.

		Peggy (P)	Victor (V)
0		G, B, m	G, B
1	Peggy generates random r	r	
2	P sends A = r.G to V	A	A
3	V flips a coin c = H or T	c	c
4	If c = H, P sends r to V		Check r.G = A
5	If c = T, P sends x = r + m		Check x.G= A+B
6	Steps 1-5 are repeated until Victor is convinced that Peggy must know m (with probability $1-2^{-k}$, for k iterations).		

Figure 3: ZKP DLEC

4.2. Square-root over elliptic curve problem

The elliptic curve version of the zero-knowledge proof for the square-root problems can be described as follows: Given E/F_n (for composite n) and $B \in E/F_n$, Peggy wants to prove in zero-knowledge that she knows $A \in E/F_n$ such that $2A = B$, i.e. $A + A = B$. Since n is composite, solving this problem is known to be infeasible.

Solution: Peggy wants to prove that she knows A such that $2A = A+A = B$. First, Peggy generates a random $R \in E/F_n$ and computes $S = 2R$. She sends S to Victor. Victor flips a coin and accordingly asks Peggy for either R or $M = R+A$. See Figure 4.

		Peggy (P)	Victor (V)
0		A, B	B
1	Peggy generates random R ∈ E/F_n	R	
2	P sends S = 2R to V	S	S
3	V flips a coin c = H or T	c	c
4	If c = H, P sends r to V		Check 2R = S
5	If c = T, P sends M = R+A		Check 2M = S+B
6	Steps 1-5 are repeated until Victor is convinced that Peggy must know x (with probability $1-2^{-k}$, for k iterations).		

Figure 4: ZKP SREC

5. Application to e-commerce

In this section, we will perform a high-level assessment of the proposed approach of using elliptic curve-based zero-knowledge proofs in e-commerce. This will be in light of the following aspects: technological, economic, social, and regulatory aspects [9]. The proposed approach covers the following key requirements: (1) *Authentication:* It provides user authentication via proving the possession of an authentication secret. (2) *Privacy:* The private information is not revealed; only the possession of such information is checked. (3) *Security:* Zero-knowledge proofs on DLEC provide higher level of security than on discrete logarithm over Z_n, or current RSA. Refer to Section 6. (4) *Ease of Use:* The authentication process is performed transparent to the users.

6. Advantages of elliptic curve-based ZKP

Having DLEC as building blocks makes the zero-knowledge proof scheme more secure than the classical scheme using multiplicative groups (e.g. Z_n) [6]. It has been proven in [10] that the classical DL problem in F_q^* can be solved in sub-exponential time, *L(1/3)*. The time complexity to solve the classical DL problem reduced to

$$Exp(O((\log q)^{1/3} (\log \log q)^{2/3})).$$

However, the best-known algorithm to solve the DLEC problem in E/F_q is by using giant-step baby-step approach, but it takes exponential time [7]. The time complexity of the algorithm is $O(N^{1/2})$, where N is the group order. For an elliptic curve over the field F_q, the time complexity is *Exp(O(log q))*.

The observation we make here is that if the Elliptic curve scheme is not based entirely on DLEC, weaker parts in the scheme can be attacked in sub-exponential time, and hence using elliptic curve gives no more security than the classical ones. For example, the protocol of the zero-knowledge proof of the square-root problem (SREC) presented in Section 4 has no advantage over the protocol presented in Section 3.4 even though it is elliptic curve-based. The reason is that Victor can solve for *R* at step 2 of the protocol (of Section 4) by factoring n in sub-exponential time. Then he can cheat at step 3 by setting the coin to tail to force Peggy to send him $M = R+A$. Once Victor gets *M*, he can learn the secret *A* (in sub-exponential time) as $A = M-R$.

7. Conclusion

In this paper, we proposed an approach using elliptic curve-based zero-knowledge proofs in e-commerce applications. Zero-knowledge proofs techniques are powerful tools in such critical applications for providing both security and privacy at the same time. We demonstrated that using elliptic curved-based zero-knowledge proof give more security in the case of discrete logarithm problem, but not in the case of square-root problem. The improvement of security is due to the higher complexity of solving the discrete logarithm problem over elliptic curves than over the multiplicative group Z_n. This advantage is applicable to all applications, in which the zero-knowledge proof is based on the discrete logarithm over elliptic curve, including: anonymity revocable off-line digital cash, and its batching scheme.

Acknowledgements

The authors would like to thank the Integrated Media Systems Center at USC for its partial support, and Clifford Neuman of USC-ISI for his review and valuable comment for this paper.

8. References

[1] Rosencrance, Linda, "Report: Online holiday sales up 46% over last year," ComputerWorld, Dec 24, 2003.

[2] Guerin, David, "Fraud in Electronic Payment," Trintech Group, Nov 2003.

[3] Jan Camenisch, Ueli Maurer, and Markus Stadler, "Digital Payment Systems with Passive Anonymity-Revoking Trustees", proceedings of Computer Security - ESORICS '96, volume 1146 of Lecture Notes in Computer Science, pages 31-43.

[4] Craver, Scott "Zero Knowledge Watermark Detection", Proceedings of the Third International Workshop on Information Hiding, Springer Lecture Notes in Computer Science, vol. 1768, 2000, pages 101-116.

[5] Khanh Quoc Nguyen; Varadharajan, V.; Yi Mu; **"**Batching proofs of knowledge and its applications" 1999. Proceedings Tenth International Workshop on Database and Expert Systems Applications, 1-3 Sept.1999, pages 844-849

[6] Koblitz, Neal, "Elliptic curve implementation of zero-knowledge blobs", Journal of Cryptology, Vol. 4, 1991, pages 207-213.

[7] Balasubramaniam, R, Koblitz, N., "The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes - Okamoto - Vanstone Algorithm", Journal of Cryptology, 11(2) 1998 pages 141-145

[8] Koblitz, Neal "A Course in Number Theory and Cryptography", Springer, 1994.

[9] Zon-Yau Lee; Hsiao-Cheng Yu; Pei-Jen Ku, An analysis and comparison of different types of electronic payment systems, Management of Engineering and Technology, 2001. PICMET '01, Volume 2: Supplement, 2001, pages 38 -45

[10] Koblitz, Neal, Algebraic Aspects of Cryptography, Springer, 1997, pages 131-136.