Security and Privacy Using One-Round Zero-Knowledge Proofs[*]

Sultan Almuhammadi and Clifford Neuman
University of Southern California
Los Angeles, CA 90089-0781, USA
E-mail: gsultan@gmail.com, bcn@isi.edu

Abstract

A zero-knowledge proof (ZKP) is an interactive proof that allows a prover to prove the knowledge of a secret to a verifier without revealing it. ZKPs are powerful tools to deal with critical applications in security e-commerce. Existing ZKPs are iterative in nature; their protocols require multiple communication rounds. The cost of iteration makes ZKPs unsuitable in practice. We propose a new protocol that meets all the requirements of ZKPs, yet runs in one round. The new approach substantially reduces computation and communications costs. It makes ZKPs more suitable for practical cryptographic systems for both govern-ment and commercial applications.

Index terms – Zero-knowledge proofs, identity theft, computer security, e-commerce, trusted computing, privacy, public-key cryptography.

1. Introduction

A zero-knowledge proof (ZKP) is an interactive proof between two parties: prover and verifier, where the prover proves the possession of a secret without revealing any information about the secret itself. ZKPs were first introduced in 1985 for identity verification systems [9] and became powerful tools for many cryptographic applications [5]. There has been a growing concern about the risk of identity theft in critical situations, like computer security and e-commerce applications. ZKPs are the ideal solution to challenges in identification since they allow customers to prove identities without exchanging sensitive information that may lead to identity theft.

In e-commerce applications, such as identity verification, researchers have proposed different solutions for different challenges. However, most of the traditional verification solutions are based on obtaining more information from the user, like: zip code, secret PIN, etc. If not handled properly, this private information can be a source of future fraud [4]. Even without the risk of possible future fraud, revealing such personal information undermines customers' privacy.

There has always been a trade-off between security and privacy in many identification schemes. The customer gains the trust of the service provider by divulging additional private information. For example, when calling a credit card customer service, the representative might ask for zip code, date of birth, or mother's maiden name to verify the caller. The more the trust needed to be established, the more the customer needs to give out. Therefore, using a verification system that protects privacy and security at the same time becomes essential [5].

Many researchers have shown that ZKP can be alternatively utilized in e-commerce applications, such as smart cards [14], digital cash [2], anonymous communication [6], electronic voting [1], public-key cryptography [10], multimedia security and digital watermarks [3].

Existing ZKPs are iterative in nature; their protocols require multiple communication rounds between parties. Due to the cost of iteration, practitioners see ZKPs as unsuitable in practice and therefore develop other tools to avoid using ZKPs.

The proposed approach creates new protocols that allow the prover to prove knowledge of a secret without revealing it. The new approach, called a one-round zero-knowledge-proof (1-R ZKP), meets all the requirements of ZKPs, yet runs in a single round. The new approach substantially reduces the running-time complexity and communications cost. It eliminates the iteration cost and makes such proofs suitable for practical cryptographic systems for both governmental and commercial applications.

[*] This research was supported in part by King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. Figures and descriptions in this paper were provided by the authors and are used with permission.

2. ZKPs overview

A Zero-knowledge proof is used when someone (the prover) has to prove to someone else (the verifier) his/her knowledge of some secret information while the prover is not willing to reveal the secret. In cryptographic literature they are usually named Peggy (prover) and Victor (verifier). [12]

The usual method for Peggy to prove her knowledge of the secret is to tell Victor the secret. But then, he also gets to know about it and can tell it to anybody he wants. The secret is no longer secret.

Another method is using zero-knowledge proofs. Through these, Peggy can prove to Victor that she does have the secret but it does not give Victor any information about what the secret is. These proofs take the form of an interactive protocol. If Peggy knows the secret, she can answer victor's "questions" correctly, but if she doesn't, then there is a certain probability that she cannot successfully cheat to answer correctly. By repeating the steps for many iterative rounds, the probability that she cheats successfully can be brought down to within a very small fraction. Without iteration, Peggy can pass any particular round with a 50% probability without knowing the secret. By repeating the steps of the protocol, the probability that Peggy cheats becomes negligible.

We present the definition of the zero-knowledge proof formally as a class of problems, which is a subclass of Interactive Proofs (IP). Let us introduce the following definitions from [7] [8].

Definition: (Negligible function)

The function $f\colon N \rightarrow R$ is called negligible if for all $c > 0$ and sufficiently large n, $f(n) < n^{-c}$. f is called nonnegligible if there exists a $c > 0$ such that for all sufficiently large n, $f(n) > n^{-c}$.

Definition: (Interactive proof)

An interactive proof $<P,V>$ for language L is a two-party protocol in which a computationally unrestricted prover, P, interacts with a probabilistic polynomial-time verifier, V, by exchanging messages. Both parties share a common input x. At the end, V either accepts or rejects and both completeness and soundness properties hold.

Definition: (Completeness property)

For any $c > 0$ and sufficiently long $x \in L$, Probability (V accepts x) > $1 - |x|^{-c}$.

In other words, an interactive proof (protocol) is complete if, given an honest prover and an honest verifier, the protocol succeeds with overwhelming probability.

Definition: (Soundness property)

For any $c > 0$ and sufficiently long $x \notin L$, Probability (V accepts x) < $|x|^{-c}$, (i.e. negligible), even if the prover deviates from the prescribed protocol.

In other words, if the prover does not know the secret, her chance to pass the proof successfully is negligible.

Definition: (Zero-knowledge proof)

An interactive proof $<P,V>$ is called zero-knowledge if for every probabilistic polynomial-time V^*, there exists a probabilistic expected polynomial-time simulator (algorithm) M_{v^*} that on inputs $x \in L$ produces probability distributions $M_{v^*}(x)$ polynomially indistinguishable from the distributions $<P,V^*> (x)$.

"Polynomially indistinguishable" means that there exists no probabilistic polynomial time algorithm which can decide with better than negligible error probability, when given a polynomial number of samples, from which of the distributions they are drawn.

3. Classical problems

It is important to distinguish between three different, but related, issues regarding zero-knowledge proofs: (1) the *application* that uses the zero-knowledge proof, (2) the *problem* for which the zero-knowledge proof is built, and (3) the *cryptographic scheme* (technique) used to build the proof.

The problems for which zero-knowledge proofs are built vary according to the application they are used for. In each problem, the prover wants to prove the knowledge of some secret without revealing any information about the secret itself. Typically the secret is just a solution (or a witness) of the problem. The following examples are some of the classical problems used for ZKPs: the discrete logarithm, the square root problem, graph isomorphism, the equality of two discrete-logs, and one of two discrete-logs. In general, these problems belong to a class of problems known as NP problems. There is no known efficient (polynomial time) algorithm to solve any of these problems. However, the solution can be verified in polynomial time. In this section, we discuss the existing iterative ZKP of a problem that is widely used for e-commerce applications. Then, in Section 4, we show how the same problem can have more efficient one-round ZKP.

Discrete-logarithm (DL) problem

Peggy, the prover, wants to prove in zero-knowledge that she knows the discrete logarithm of a given number. That is, given a large prime p, a generator g for the multiplicative group Z_p, and $b \in Z_p$, Peggy wants to prove in zero-knowledge that she knows x such that

$$g^x = b \pmod{p}$$

Solving a DL problem is known to be computationally infeasible. Therefore, people are interested in proving the knowledge of such a secret without revealing it. This is the basic problem for ZKP and many applications have been built using the ZKP of this problem [2] [3] [9] [6] [1] [14].

Solution: This solution can be found in [3]. Initially, Peggy and Victor both know the generator g and b. Peggy generates a random r and computes $h = g^r$ mod p. She sends h to Victor. Then, 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 $g^m = b{\cdot}h$. 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 2 summarizes this iterative protocol of ZKP of the DL problem.

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

Figure 1: ZKP of DL problem

The ZKP of the DL problems play a major role in many applications, such as multi-media security [3], identity verification [9], smart cards [14], digital cash [2], anonymous communication [6], and electronic election [1].

4. New Approach: One-Round Zero-Knowledge Proofs

The goal of our new approach is to eliminate the iterations in the existing ZKPs. Although they are useful for many applications, iterative ZKPs have high computation and communication costs. We propose a new approach to create protocols that satisfiy the requirements of the existing ZKPs, but run in one round. This reduces the cost of ZKP substantially.

4.1. One-round ZKP of DL problem

Here is a one-round protocol for Peggy to prove in zero-knowledge that she knows x such that

$$g^x = b \pmod{p}$$

Solution: This is a challenge-and-response kind of protocol. Victor generates a random y and computes $c = g^y \pmod{p}$. He sends c as a challenge to Peggy. Peggy responds by computing $r = c^x \pmod{p}$ and sending r to Victor. Victor can verify the validity of Peggy's response by verifying that $r = b^y \pmod{p}$. The chart below summarizes these steps.

		Peggy (P)	Victor (V)
0		g, b, p, x	g, b, p
1	V generates a random y		y
2	V sends $c = g^y \pmod{p}$	c	$c = g^y$
3	P sends $r = c^x \pmod{p}$	$r = c^x$	r
4	V verifies that $r = b^y \pmod{p}$		

Figure 2: 1-R ZKP of DL problem

This is a one-round proof based on the framework. All parameters are set up at Step 0. There are no more auxiliary messages needed for this protocol.

Proof of correctness: If Peggy knows the secret x, she just computes and sends $r = c^x$. Since Victor knows y, he can verify that $r = c^x = g^{xy} = (g^x)^y = b^y \pmod{p}$. However, if Peggy does not know x, she cannot compute r. According to Diffie-Hellman assumption [11], it is computationally infeasible to find g^{xy} knowing only g^x and g^y. Moreover, this one-round protocol does not reveal any information about the secret x since solving for x at Step 3 is infeasible.

4.2. Discussion

Both iterative and one-round ZKPs are useful tools to deal with security and privacy issues in e-commerce applications. We discuss here the advantage of the one-round ZKP and compare its performance to the existing iterative ZKP.

The approach of the one-round ZKP is superior to the iterative approach in the following measures: (1) better execution-time complexity – saves local computations; (2) less communication cost – exchanges much less information in terms of bits; and (3) less latency – exchange fewer messages over the internet or the network. The following table summarizes the results.

	1-R ZKP	Iterative ZKP
execution-time	t^2 *log t log log t*	t^3 *log t log log t*
communication	$2t$	$2t^2$
latency	$2d$	$2td + d$

Figure 3: Cost table

5. Conclusion

Zero-knowledge proofs can be used whenever there is critical data to exchange while only proving the possession of such data is needed. ZKPs are the natural tools to meet the challenges in many applications that deal with both security and privacy. The existing ZKPs are iterative, which implies high computation and communication costs. Therefore, researchers may not see ZKPs suitable in practice and try to develop other tools to avoid using ZKPs.

The proposed one-round ZKP overcomes the iteration problem. It allows the prover to prove the knowledge of a secret without revealing it and meet all the requirements of ZKPs, yet runs in one round. This reduces the computation and communication cost substantially and makes the new ZKPs more practical.

In this paper, we have presented a one-round ZKP for the discrete-logarithm problem. The same approach can be used for other problems. We have shown that the new one-round ZKP is superior to the existing ones in terms of execution-time, communication cost and latency.

References

[1] O. Baudron, P. Fouque, D. Pointcheval, G. Poupard and J. Stern, “Practical Multi-Candidate Election System,” Proceedings of the 20th annual ACM symp. on Principles of distributed computing, 2001, pp. 274-283.

[2] Franklin, M. and Yung, M. “Secure and efficient off-line digital money,” Proceedings of the 20th International Colloquium on Automata, Languages and Programming (ICALP ’93), Lecture Notes in Computer Science 700, Springer-Verlag, Lund, Sweden, July 1993, pp. 265-276.

[3] Scott Craver, “Zero-knowledge Watermark Detection," Proceedings of the Third International Workshop on Information Hiding, Lecture Notes in Computer Science 1768, Springer, 2000, pp. 101-116.

[4] David Guerin, “Fraud in Electronic Payment,” Trintech Group, Nov. 2003.

[5] Sultan Almuhammadi, Nien T. Sui, Dennis McLeod, "Better Privacy and Security in E-Commerce: Using Elliptic Curve-Based Zero-Knowledge Proofs," Proceeding of the IEEE Conference on E-Commerce Technology, CEC'04, San Diego, July 2004, pp. 299-302.

[6] Luis Ahn, Andrew Bortz and Nicholas Hopper, “k-Anonymous Message Transmission,” Proceedings of the 10th ACM conference on Computer and communication security, 2003, pp. 122-130.

[7] T. Okamoto, “Provably secure and practical identification schemes and corresponding signature schemes,” Proceedings of CRYTPO'92, Lecture Notes in Computer Science 740, Springer-Verlag, 1993, pp. 31-53.

[8] K. Nguyen, V. Varadharajan and Y. Mu, “Batching proofs of knowledge and its applications,” The 10th International Workshop on Databases and Expert Systems Applications, IEEE Press, 1999, pp. 844 – 849.

[9] U. Feige, A. Fiat and A. Shamir, “Zero-knowledge proofs of Identity,” Proceedings of the 19th annual ACM conference on Theory of computing, New York, 1987, pp. 210-217.

[10] J. Camenisch, M. Michels, “Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes,” Basic Research in Computer Science, 1998.

[11] W. Diffie and M. Hellman, “New dictions in cryptography,” IEEE Transactions on Information Theory, vol. 22, 1976, pp. 644-654.

[12] Goldwasser, Micali and Rackoff, “Knowledge Complexity of Interactive Proof Systems,” Proceedings of the 17th ACM Symp. on Theory of Computing, Providence, 1985, pp. 291-304.