A Note on One Popular Non-Interactive Zero-Knowledge Proof System

Zhengjun Cao[1,2], Xiqi Wang[1], and Lihua Liu[3]
(Corresponding author: Lihua Liu)

Department of Mathematics, Shanghai University, No.99, Shangda Road, Shanghai, China[1]
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications[2]
No.10, Xitucheng Road, Beijing, China
Department of Mathematics, Shanghai Maritime University, No.1550, Haigang Ave, Shanghai, China[3]
(Email: liulh@shmtu.edu.cn)

(Received May 4, 2019; Revised and Accepted Sept. 4, 2019; First Online Sept. 21, 2019)

Abstract

At Eurocrypt'06, Groth *et al.* have proposed one non-interactive zero-knowledge (NIZK) proof system for plaintext being 0 or 1 [its revision published by J. ACM, 59(3), 1-35, 2012]. Based on the system, they presented the first perfect NIZK argument system for any NP language and the first secure NIZK argument with universal composability for any NP language in the presence of a dynamic/adaptive adversary. In this note, we remark that in the scheme the prover is not compelled to invoke any trapdoor key to generate witnesses. The mechanism is dramatically different from the previous works, such as Blum-Feldman-Micali proof system and Blum-Santis-Micali-Persiano proof system. We find if the trapdoor key is available to the prover then he can cheat the verifier to accept a false claim. The characteristic is essentially incompatible with the general primitive of zero-knowledge proof, which does not require any extra trust.

Keywords: Bilinear Groups with Composite Order; Extended Euclid Algorithm; Non-interactive Zero-knowledge Proof; Subgroup Decision Problem

1 Introduction

Non-interactive zero-knowledge (NIZK) proof in the common random string model, introduced by Blum *et al.* [4], plays a key role in many constructions, including digital signatures [11, 25], E-voting [14], Shuffle [2, 27], polynomial evaluation [3], arithmetic circuits [7, 8] and multiple-party computation [1, 9, 20, 26]. In 1988, Blum *et al.* [4] constructed some computational NIZK proof systems for proving a single statement about any NP language. In 1991, they [5] presented the first computational NIZK proof system for multiple theorems. These systems are based on the hardness of deciding quadratic residues modulo a composite number. In 1998, Kilian and Petrank [21] designed an efficient noninteractive zero-knowledge proof system for NP with general assumptions.

In 1999, Feige *et al.* [10] developed a method to construct computational NIZK proof systems based on any trapdoor permutation. Goldreich *et al.* [13] discussed the possibility of converting a statistical zero knowledge (SZK) proof into a NIZK proof. In 2001, Santis *et al.* [23, 24] investigated the robustness and randomness-optimal characterization of some NIZK proof systems. In 2003, Sahai and Vadhan [22] presented an interesting survey on SZK. Groth *et al.* [15, 16, 19] designed some linear algebra with sub-linear zero-knowledge arguments and short pairing-based NIZK arguments. In 2015, Gentry *et al.* [12] discussed the problem of using fully homomorphic hybrid encryption to minimize NIZK proofs.

At Eurocrypt'06, Groth, Ostrovsky and Sahai [17] designed a popular NIZK proof system for plaintext being 0 or 1 using bilinear groups with composite order. The refined version [18] was published by Journal of ACM in 2012. The behind intractability of this work is the subgroup decision problem introduced by Boneh *et al.* [6]. Based on the basic NIZK proof system, they presented one NIZK proof for circuit satisfiability. Furthermore, they constructed the first perfect NIZK argument system for any NP language and the first secure NIZK argument with universal composability for any NP language in the presence of a dynamic/adaptive adversary. They claimed it has resolved a central open problem concerning NIZK protocols.

In this note, we show that in Groth-Ostrovsky-Sahai proof system the prover is not compelled to invoke any trapdoor key to generate witnesses. The mechanism was dramatically different from the previous works, such as Blum-Feldman-Micali proof system [4] and Blum-Santis-Micali-Persiano proof system [5]. They did adopt a different security model although it was not specified explicitly. We also find that if the trapdoor key is available to the prover then he can cheat the verifier to accept a false claim. The characteristic is radically incompatible with the general primitive of zero-knowledge proof. That is, the popular NIZK proof system requires extra trust to set its parameters. This shortcoming renders itself vulnerable to inner attacks.

2 Review of Groth-Ostrovsky-Sahai NIZK Proof System

The system [17] can be described as follows.

- Common reference string. Let $\mathbb{G}, \mathbb{G}_1$ be two cyclic groups of order n, where $n = pq$ and p, q are primes such that it is difficult to factor n. $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ is a bilinear map. We require that $\hat{e}(g, g)$ is a generator of $\mathbb{G}_1$ if g is a generator of $\mathbb{G}$. Pick a generator $h \in \mathbb{G}_q$, where $\mathbb{G}_q \subset \mathbb{G}$ is of order q. The common reference string is $\sigma = (n, \mathbb{G}, \mathbb{G}_1, \hat{e}, g, h)$.

- Statement. The statement is an element $c \in \mathbb{G}$. The claim is that there exists a pair $(m, w) \in \mathbb{Z}^2$ so $m \in \{0, 1\}$ and $c = g^m h^w$.

  Proof. Given (σ, c, m, w), check $m \in \{0, 1\}$ and $c = g^m h^w$. Return failure if check fails. It proceeds as follows. Pick $r \in \mathbb{Z}_n^*$, compute

  $$\begin{aligned} \pi_1 &= h^r \\ \pi_2 &= (g^{2m-1}h^w)^{wr^{-1}} \\ \pi_3 &= g^r. \end{aligned}$$

  Return $\pi = (\pi_1, \pi_2, \pi_3)$. □

- Verification. Given the parameter σ and c, π, check $c \in \mathbb{G}$, $\pi \in \mathbb{G}^3$, and verify that

  $$\begin{aligned} \hat{e}(c, cg^{-1}) &= \hat{e}(\pi_1, \pi_2) \\ \hat{e}(\pi_1, g) &= \hat{e}(h, \pi_3). \end{aligned}$$

Correctness . It is easy to check that

$$\begin{aligned} \hat{e}(c, cg^{-1}) &= \hat{e}(g^m h^w, g^{m-1}h^w) \\ &= \underline{\hat{e}(g, g)^{m(m-1)}}\hat{e}(g, h)^{(2m-1)w}\hat{e}(h, h)^{w^2} \\ \hat{e}(\pi_1, \pi_2) &= \hat{e}(h^r, (g^{2m-1}h^w)^{wr^{-1}}) \\ &= \hat{e}(g, h)^{(2m-1)w}\hat{e}(h, h)^{w^2} \end{aligned}$$

If $m \in \{0, 1\}$, then $\hat{e}(c, cg^{-1}) = \hat{e}(\pi_1, \pi_2)$.

If $m \notin \{0, 1\}$, it seems that Alice has to solve the discrete logarithms among $\hat{e}(g, h), \hat{e}(g, g), \hat{e}(h, h)$, which are reduced to the discrete logarithm of h to g. This possibility can be eradicated in advance by asking Alice and Bob agree to a random seed to a pseudorandom generator for generating g. Based on the observations, Groth *et al.* concluded that the scheme was secure against either the prover's attack or the verifier's attack.

3 Analysis of Groth-Ostrovsky-Sahai NIZK Proof System

For convenience, we will call the prover, Alice, and the verifier, Bob. We now consider the following problems.

3.1 What is the True Statement

Give $c \in \mathbb{G}$, Alice claims that c is of the form $g^m h^w$ for some $(m, w) \in \{0, 1\} \times \mathbb{Z}_n$. This is equivalent to checking whether c or c/g is in the subgroup $\mathbb{G}_q$.

If the trapdoor key q is available, then it suffices to check that

$$c^q = 1, \quad \text{or} \quad (c/g)^q = 1.$$

However, the trapdoor key cannot be directly shown to Bob. Hence, Alice has to produce some witnesses to convince Bob of that c or c/g is indeed in the subgroup $\mathbb{G}_q$.

3.2 How to Understand the Phrase of "Common Reference String"

The notion of "common reference string" used in NIZK model can be traced back to [5]. It had stressed that

> The moral is that one must be careful when using the same set-up, i.e., common reference string, and the same pair (x, y), to prove an "unlimited" number of formulae to be satisfiable.

Apparently, *"common reference string" represents the same set-up known to the prover and the verifier.* But it does not specify whether or not there is any trapdoor key related to the common reference string.

Recalling Blum-Santis-Micali-Persiano proof system [5] and its like, we find they have not any trapdoor key at all. For readers' convenience, we now briefly relate Blum-Santis-Micali-Persiano proof system as follows.

Common reference string. The random string is $\rho = \rho_1\rho_2 \cdots \rho_{n^2}$, each ρ_i has length n.

Statement. The odd number $x < n$ is a composite of two different primes p, q. Assume that $|J_x^{+1}| = |J_x^{-1}|$, where

$$J_x^{+1} = \left\{ y \in \mathbb{Z}_x^* \,|\, \text{Jacobi symbol} \left(\frac{y}{x}\right) = 1 \right\},$$
$$J_x^{-1} = \left\{ y \in \mathbb{Z}_x^* \,|\, \text{Jacobi symbol} \left(\frac{y}{x}\right) = -1 \right\}$$

and $\mathbb{Z}_x^* = \{1, 2, \cdots, x - 1\}$. Alice knows p, q and wants to convince Bob of this fact while preventing Bob from knowing p, q.

Proof. Alice picks $y < x$ such that $\left(\frac{y}{x}\right) = 1$ and y is not a quadratic residue of x. She then computes $\left(\frac{\rho_i}{x}\right)$ for $i = 1, 2, \cdots, n^2$. If $\left(\frac{\rho_i}{x}\right) = 1$, compute s_i such that $s_i^2 = \rho_i \bmod x$ or $s_i^2 = y\rho_i \bmod x$. Send these s_i and x, y to Bob.

Verification. Bob checks that x is not a perfect square. Verify that $\left(\frac{y}{x}\right) = 1$ and the number of s_i is greater than $3n$. He then checks that each $\left(\frac{\rho_i}{x}\right) = 1$ and $s_i^2 = \rho_i \bmod x$ or $s_i^2 = y\rho_i \bmod x$.

It is easy to find that in [5] there is not any trapdoor key related to the setup. We refer to Table 1 for the big differences between Blum-Santis-Micali-Persiano proof system and Groth-Ostrovsky-Sahai proof system.

Clearly, Blum-Santis-Micali-Persiano proof system needs only *a very simple common reference string*, and Alice has to make use of her private key (the factors of x) to generate witnesses. To the contrary, Groth-Ostrovsky-Sahai proof system needs *a very complicated common reference string associated with a trapdoor key.*

The model introduced by Blum *et al.* is more suitable to practical applications because *it does not require any extra trust.* But the model considered by Groth *et al.* entails the verifier to trust that the related trapdoor key cannot be accessed to the prover (see the discussion in the following sections). The requirement does contradict the general assumptions for zero-knowledge proof.

3.3 Alice is not Compelled to Invoke Any Trapdoor Key

It is easy to find that Alice does not invoke the trapdoor key (p, q) to generate witnesses. Besides, the system does not specify who is responsible for generating the common reference string. So, it is reasonable to assume that there is a third-party, Cindy, who generates the common reference string. Note that Cindy is not fully trustable and she knows the trapdoor key. Otherwise, the presence of a fully trustable party is indeed incompatible with the primitive of zero-knowledge proof system.

3.4 Alice and Cindy Can Conspire to Cheat Bob

Can Cindy form an alliance with Alice? If so, we now show that Alice and Cindy can conspire to cheat Bob to accept a false claim.

Suppose that Alice picks an integer r and sets

$$\begin{aligned}
\pi_1 &= h^r \\
\pi_3 &= g^r \\
c &= g^{\alpha_1} h^{\alpha_2} \\
\pi_2 &= g^{\beta_1} h^{\beta_2},
\end{aligned}$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2$ are to be determined. Since

$$\begin{aligned}
\hat{e}(c, cg^{-1}) &= \hat{e}(g^{\alpha_1} h^{\alpha_2}, g^{\alpha_1 - 1} h^{\alpha_2}) \\
&= \underline{\hat{e}(g, g)^{\alpha_1(\alpha_1 - 1)}} \hat{e}(g, h)^{\alpha_1\alpha_2 + \alpha_2(\alpha_1 - 1)} \\
&\qquad \cdot \hat{e}(h, h)^{\alpha_2^2}, \\
\hat{e}(\pi_1, \pi_2) &= \hat{e}(h^r, g^{\beta_1} h^{\beta_2}) \\
&= \hat{e}(h, g)^{r\beta_1} \hat{e}(h, h)^{r\beta_2},
\end{aligned}$$

it suffices for Alice to solve the following equations

$$\begin{cases}
\alpha_1(\alpha_1 - 1) = 0 \bmod n \\
2\alpha_1\alpha_2 - \alpha_2 = r\beta_1 \bmod n \\
\alpha_2^2 = r\beta_2 \bmod n
\end{cases} \quad (1)$$

for those exponents. *The authors [17] mistakenly thought that* α_1 *in the equations* (1) *has to take* 0 *or* 1.

In fact, armed with the trapdoor key p, q, Alice can obtain k, ℓ using extended Euclid algorithm such that

$$kq - \ell p = 1.$$

She sets $\underline{\alpha_1 = kq}$. Clearly,

$$\alpha_1(\alpha_1 - 1) = kq(kq - 1) = kq\ell p \equiv 0 \bmod n.$$

She then picks $\underline{\beta_1 < n}$ and computes

$$\begin{aligned}
\alpha_2 &= r\beta_1(2kq - 1)^{-1} \bmod n \\
\beta_2 &= \alpha_2^2 r^{-1} \bmod n.
\end{aligned}$$

It is easy to check that the above values c, π_1, π_2, π_3 pass the original verification.

Obviously, $\alpha_1 = kq \neq 0, 1$. Besides,

$$(g^{\alpha_1})^q = (g^{kq})^q = (g^{\ell p + 1})^q = g^q \neq 1, \text{ i.e., } g^{\alpha_1} \notin \mathbb{G}_q.$$

Thus, there does not exist an integer α' such that

$$g^{\alpha_1} = h^{\alpha'}.$$

That means $c = g^{\alpha_1} h^{\alpha_2}$ *cannot be eventually expressed as* h^{w_1} *or* gh^{w_2}. Therefore, the adversary can cheat Bob to accept the false claim $c = g^{\alpha_1} h^{\alpha_2}$, where $\alpha_1 \neq 0$ or 1.

4 Conclusion

We remark that the Groth-Ostrovsky-Sahai proof system adopts an artificial security model due to the existence of trapdoor key related to the common reference string. Under the strong assumption that the adversary cannot access to the trapdoor key, the proof system seems secure. But the assumption is ultimately incompatible with the general primitive of zero-knowledge proof *which does not require any extra trust*, and makes the system itself unsuitable to more broader applications.

We would like to stress that the first thing for designing a cryptographic scheme is to consider what is trusted or untrusted. Otherwise, an assumption for extra trust suffices to ruin the whole system.

Acknowledgements

We thank the National Natural Science Foundation of China (#61411146001), and Open Foundation of State key Laboratory of Networking and Switching Technology (#SKLNST-2016-2-03, Beijing University of Posts and Telecommunications). We gratefully acknowledge the reviewers for their valuable suggestions.

Table 1: Two kinds of common reference strings

	Blum-Santis-Micali-Persiano	Groth-Ostrovsky-Sahai
Common reference string [trapdoor key]	A random string $\rho = \rho_1\rho_2\cdots\rho_{n^2}$, where each ρ_i is of length n. NO	$(n, \mathbb{G}, \mathbb{G}_1, \hat{e}, g, h)$ where $n = pq$. (p, q)
Statement	Knowing the factors of the integer x.	c is of the structure $g^m h^w$ with $(m, w) \in \{0, 1\} \times \mathbb{Z}$.
Proof	$x; y, \{s_i\}$	$c; \pi_1, \pi_2, \pi_3$
Verification	$\binom{\rho_i}{x} = 1$, and $s_i^2 = \rho_i \bmod x$ or $s_i^2 = y\rho_i \bmod x$	$\hat{e}(c, cg^{-1}) = \hat{e}(\pi_1, \pi_2)$, and $\hat{e}(\pi_1, g) = \hat{e}(h, \pi_3)$

References

[1] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, "Design of an anonymous lightweight communication protocol for smart grid and its implementation on 8-bit avr and 32-bit arm," *International Journal of Network Security*, vol. 21, no. 4, pp. 607–617, 2019.

[2] S. Bayer and J. Groth, "Efficient zero-knowledge argument for correctness of a shuffle," in *Proceedings of 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'12)*, pp. 263–280, 2012.

[3] S. Bayer and J. Groth, "Zero-knowledge argument for polynomial evaluation with application to blacklists," in *Proceedings of 32st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'13)*, pp. 646–663, 2013.

[4] M. Blum, P. Feldman, and S. Micali, "Noninteractive zero-knowledge and its applications," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC'88)*, pp. 103–112, 1988.

[5] M. Blum and *et al.*, "Noninteractive zero-knowledge," *SIAM Journal on Computing*, vol. 20, no. 6, pp. 1084–1118, 1991.

[6] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in *Proceedings of 2nd Theory of Cryptography Conference (TCC'05)*, pp. 325–341, Feb. 2005.

[7] J. Bootle and *et al.*, "Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting," in *Proceedings of 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'16)*, pp. 327–357, 2016.

[8] J. Bootle and *et al.*, "Efficient zero-knowledge proof systems," in *Proceedings of Foundations of Security Analysis and Design (FOSAD'16)*, pp. 1–31, June 2016.

[9] R. Challa and V. Gunta, "Additively lwe based homomorphic encryption for compact devices with enhanced security," *International Journal of Network Security*, vol. 21, no. 3, pp. 378–383, 2019.

[10] U. Feige, D. Lapidot, and A. Shamir, "Multiple non-interactive zero knowledge proofs under general assumptions," *SIAM Journal on Computing*, vol. 29, no. 1, pp. 1–28, 1999.

[11] J. Garay, P. MacKenzie, and K. Yang, "Strengthening zero-knowledge protocols using signatures," *Journal of Cryptology*, vol. 19, no. 2, pp. 169–209, 2006.

[12] C. Gentry and *et al.*, "Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proofs," *Journal of Cryptology*, vol. 28, no. 4, pp. 820–843, 2015.

[13] O. Goldreich, A. Sahai, and S. Vadhan, "Can statistical zero knowledge be made non-interactive? or on the relationship of szk and niszk," in *Proceedings of 19th Annual International Cryptology Conference (CRYPTO'99)*, pp. 467–484, Aug. 1999.

[14] J. Groth, "Non-interactive zero-knowledge arguments for voting," in *Proceedings of 3rd International Conference on Applied Cryptography and Network Security (ACNS'05)*, pp. 467–482, June 2005.

[15] J. Groth, "Linear algebra with sub-linear zero-knowledge arguments," in *Proceedings of 29th Annual International Cryptology Conference (CRYPTO'09)*, pp. 192–208, Aug. 2009.

[16] J. Groth, "Short pairing-based non-interactive zero-knowledge arguments," in *Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'10)*, pp. 321–340, Dec. 2010.

[17] J. Groth, R. Ostrovsky, and A. Sahai, "Perfect non-interactive zero knowledge for np," in *Proceedings of 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'06)*, pp. 339–358, May 2006.

[18] J. Groth, R. Ostrovsky, and A. Sahai, "New techniques for noninteractive zero-knowledge," *Journal of ACM*, vol. 59, no. 3, pp. 1–35, 2012.

[19] J. Groth and A. Sahai, "Efficient noninteractive proof systems for bilinear groups," *SIAM Journal on Computing*, vol. 41, no. 5, pp. 1193–1232, 2012.

[20] M. S. Hwang, C. C. Lee, and S. T. Hsu, "An elgamal-like secure channel free public key encryption with keyword search scheme," *International Journal of Foundations of Computer Science*, vol. 30, no. 2, pp. 255–273, 2019.

[21] J. Kilian and E. Petrank, "An efficient noninteractive zero-knowledge proof system for np with general assumptions," *Journal of Cryptology*, vol. 11, no. 1, pp. 1–27, 1998.

[22] A. Sahai and S. Vadhan, "A complete problem for statistical zero knowledge," *Journal of ACM*, vol. 50, no. 2, pp. 196–249, 2003.

[23] A. Santis, G. Crescenzo, and G. Persiano, "Randomness-optimal characterization of two np proof systems," in *Proceedings of 6th International Workshop on Randomization and Approximation Techniques (RANDOM'02)*, pp. 179–193, Sep. 2002.

[24] A. Santis and *et al.*, "Robust non-interactive zero knowledge," in *Proceedings of 21st Annual International Cryptology Conference (CRYPTO'01)*, pp. 566–598, Aug. 2001.

[25] C. Y. Tsai, P. F. Ho, and M. S. Hwang, "A secure group signature scheme," *International Journal of Network Security*, vol. 20, no. 2, pp. 201–205, 2018.

[26] C. Y. Tsai and *et al.*, "A publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms," *International Journal of Network Security*, vol. 19, no. 3, pp. 443–448, 2017.

[27] Y. L. Wang, J. J. Shen, and M. S. Hwang, "A novel dual image-based high payload reversible hiding technique using lsb matching," *International Journal of Network Security*, vol. 20, no. 4, pp. 801–804, 2018.

Zhengjun Cao is an associate professor with the Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Xiqi Wang is currently pursuing his M.S. degree from Department of Mathematics, Shanghai University. His research interests include information security and cryptography.

Lihua Liu is an associate professor with the Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.