A Note On Groth-Ostrovsky-Sahai Non-Interactive Zero-Knowledge Proof System

Zhengjun Cao[1], Lihua Liu[2,*]

Abstract. In 2006, Groth, Ostrovsky and Sahai designed one non-interactive zero-knowledge (NIZK) proof system [new version, J. ACM, 59(3), 1-35, 2012] for plaintext being zero or one using bilinear groups with composite order. Based on the system, they presented the first perfect NIZK argument system for any NP language and the first universal composability secure NIZK argument for any NP language in the presence of a dynamic/adaptive adversary. This resolves a central open problem concerning NIZK protocols.

In this note, we remark that in their proof system the prover has not to invoke the trapdoor key to generate witnesses. The mechanism was dramatically different from the previous works, such as Blum-Feldman-Micali proof system and Blum-Santis-Micali-Persiano proof system. We would like to stress that the prover can cheat the verifier to accept a false claim if the trapdoor key is available to him.

Keywords: Non-interactive zero-knowledge proof, trapdoor key, bilinear groups with composite order, subgroup decision problem.

1 Introduction

Non-interactive zero-knowledge (NIZK) proof in the common random string model, introduced by Blum et al. [3], plays a key role in many constructions, including digital signatures [9], E-voting [12], Shuffle [1], polynomial evaluation [2], arithmetic circuits [6, 7] and multiple-party computation protocols. In 1988, Blum et al. [3] constructed some computational NIZK proof systems for proving a single statement about any NP language. In 1991, they [4] 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 [18] designed an efficient noninteractive zero-knowledge proof system for NP with general assumptions.

In 1999, Feige et al.[8] developed a method to construct computational NIZK proof systems

[1] Department of Mathematics, Shanghai University, Shanghai, 200444, China.

[3] Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China. * liulh@shmtu.edu.cn

based on any trapdoor permutation. Goldreich et al. [11] discussed the possibility of converting a statistical zero knowledge (SZK) proof into a NIZK proof. In 2001, Santis et al. [20, 21] investigated the robustness and randomness-optimal characterization of some NIZK proof systems. In 2003, Sahai and Vadhan [19] presented an interesting survey on SZK. Groth [14, 15] designed some linear algebra with sub-linear zero-knowledge arguments and short pairing-based NIZK arguments. In 2015, Gentry et al. [10] explored the problem of using fully homomorphic hybrid encryption to minimize NIZK proofs.

At EUROCRYPT'06, Groth, Ostrovsky and Sahai [13] designed a new NIZK proof system for plaintext being zero or one using bilinear groups with composite order. The refined version [16] was published by Journal of ACM in 2012. The behind intractability is the subgroup decision problem introduced by Boneh et al. [5]. 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 universal composability secure NIZK argument for any NP language in the presence of a dynamic/adaptive adversary. This resolves a central open problem concerning NIZK protocols.

In this note, we would like to remark that in Groth-Ostrovsky-Sahai proof system the prover has not to invoke the trapdoor key to generate witnesses. The mechanism was dramatically different from the previous works, such as Blum-Feldman-Micali proof system [3] and Blum-Santis-Micali-Persiano proof system [4]. 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.

2 Review of Groth-Ostrovsky-Sahai NIZK Proof System

Common reference string. $\mathbb{G}, \mathbb{G}_1$ are 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 $\mathsf{failure}$ if check fails. Pick $r \in \mathbb{Z}_n^*$, compute $\pi_1 = h^r$, $\pi_2 = (g^{2m-1} h^w)^{wr^{-1}}$, $\pi_3 = g^r$. Return $\pi = (\pi_1, \pi_2, \pi_3)$.
Verification. Given the parameter σ and c, π, check $c \in \mathbb{G}$ and $\pi \in \mathbb{G}^3$. Check

$$\hat{e}(c, cg^{-1}) = \hat{e}(\pi_1, \pi_2), \qquad \hat{e}(\pi_1, g) = \hat{e}(h, \pi_3)$$

Return 1 if both checks pass, else return 0.

It is easy to check its correctness because

$$\hat{e}(c, cg^{-1}) = \hat{e}(g^m h^w, g^{m-1}h^w) = \utilde{\hat{e}(g,g)^{m(m-1)}}\hat{e}(g,h)^{(2m-1)w}\hat{e}(h,h)^{w^2}$$

$$\hat{e}(\pi_1, \pi_2) = \hat{e}(h^r, (g^{2m-1}h^w)^{wr^{-1}}) = \hat{e}(g,h)^{(2m-1)w}\hat{e}(h,h)^{w^2}$$

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

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 "common reference string"

The notion of "common reference string" used in NIZK can be traced back to Ref.[4]. 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 that whether or not there is any trapdoor key related to the common reference string.

Recalling the Blum-Santis-Micali-Persiano proof system [4] and its like, we find they have not any trapdoor key at all. For completeness, we now briefly describe Blum-Santis-Micali-Persiano proof system [4] 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

$$J_x^{+1} = \left\{ y \in \mathbb{Z}_x^* \,|\, \text{Jacobi symbol } \begin{pmatrix} y \\ x \end{pmatrix} = 1 \right\}, \; J_x^{-1} = \left\{ y \in \mathbb{Z}_x^* \,|\, \begin{pmatrix} y \\ x \end{pmatrix} = -1 \right\}$$

and $\mathbb{Z}_x^* = \{1, 2, \cdots, x-1\}$. Alice knows p, q and want to convince Bob of this fact while preventing Bob from knowing p, q.
Proof. Alice picks $y < x$ such that $\binom{y}{x} = 1$ and y is not a quadratic residue of x. She then computes $\binom{\rho_i}{x}$ for $i = 1, 2, \cdots, n^2$. If $\binom{\rho_i}{x} = 1$, 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 $\binom{y}{x} = 1$ and the number of s_i is greater than $3n$. He then checks that each $\binom{\rho_i}{x} = 1$ and $s_i^2 = \rho_i$ or $s_i^2 = y\rho_i \bmod x$.

It is easy to find that in Ref.[4] there is not any trapdoor key related to the set-up. We refer to the following table for the differences between Blum-Santis-Micali-Persiano proof system and Groth-Ostrovsky-Sahai proof system.

	Blum-Santis-Micali-Persiano	Groth-Ostrovsky-Sahai
Common reference string	A random string $\rho = \rho_1\rho_2 \cdots \rho_{n^2}$, where each ρ_i is of length n.	$(n, \mathbb{G}, \mathbb{G}_1, \hat{e}, g, h)$ where $n = pq$.
[trapdoor key]	NO	(p, q).
Statement	Knowing the factorization 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	$\left(\frac{\rho_i}{x}\right) = 1$, and $s_i^2 = \rho_i$ or $s_i^2 = y\rho_i \bmod x$	$\hat{e}(c, cg^{-1}) = \hat{e}(\pi_1, \pi_2)$, and $\hat{e}(\pi_1, g) = \hat{e}(h, \pi_3)$

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 to generate witnesses. To the contrary, Groth-Ostrovsky-Sahai proof system needs a very complicated common reference string accompanied with a trapdoor key. They did adopt different security models.

3.2 What is the true claim

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 check 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 $c^q = 1$ or $(c/g)^q = 1$. However, the trapdoor key q cannot be directly shown to Bob. Therefore, Alice has to produce some witnesses to convince Bob of that c or c/g is indeed in the subgroup $\mathbb{G}_q$.

3.3 Does Alice invoke the 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 that 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. Of course, Cindy is not fully trustable and she knows the trapdoor key.

3.4 Can Alice and Cindy 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.

Alice picks $\underline{\text{an integer } r}$ and sets $\underline{\pi_1 = h^r, \pi_3 = g^r,\ c = g^{\alpha_1}h^{\alpha_2}, \pi_2 = g^{\beta_1}h^{\beta_2}}$, where $\alpha_1, \alpha_2, \beta_1, \beta_2$

are to be determined. Since

$$\hat{e}(c, cg^{-1}) = \hat{e}(g^{\alpha_1}h^{\alpha_2}, g^{\alpha_1 - 1}h^{\alpha_2}) = \utilde{\hat{e}(g,g)^{\alpha_1(\alpha_1-1)}}\hat{e}(g,h)^{\alpha_1\alpha_2+\alpha_2(\alpha_1-1)}\hat{e}(h,h)^{\alpha_2^2}$$

$$\hat{e}(\pi_1, \pi_2) = \hat{e}(h^r, g^{\beta_1}h^{\beta_2}) = \hat{e}(h,g)^{r\beta_1}\hat{e}(h,h)^{r\beta_2}$$

it suffices for Alice to solve

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

for those exponents.

Armed with the trapdoor key p, q, Alice can obtain k, ℓ using Extended Euclid Algorithm such that

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

She then sets $\underline{\alpha_1 = kq}$. She picks $\underline{\beta_1 < n}$ and computes $\underline{\alpha_2 = r\beta_1(2kq-1)^{-1}, \beta_2 = \alpha_2^2 r^{-1} \bmod n}$.

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

Clearly, $\alpha_1 = kq \neq 0, 1$. Besides, $(g^{\alpha_1})^q = (g^{kq})^q = (g^{\ell p+1})^q = g^q \neq 1$, namely $g^{\alpha_1} \notin \mathbb{G}_q$. 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}. Thus, the adversary can cheat Bob to accept a false claim.

4 Conclusion

We remark that the Groth-Ostrovsky-Sahai proof system adopts a special 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 somewhat incompatible with the general primitive of zero-knowledge proof, and makes the system itself unsuitable to more broader applications.

References

[1] S. Bayer, J. Groth: Efficient zero-knowledge argument for correctness of a shuffle, In proceedings of EUROCRYPT'12, pp. 263-280, 2012.

[2] S. Bayer, J. Groth: Zero-knowledge argument for polynomial evaluation with application to blacklists, In proceedings of EUROCRYPT'13, pp. 646-663, 2013.

[3] M. Blum, P. Feldman, and S. Micali: Non-interactive zero-knowledge and its applications, In proceedings of STOC'88, pp. 103-112, 1988.

[4] M. Blum, et al.: Noninter-active zero-knowledge, SIAM Jornal of Computation, 20(6), pp. 1084-1118, 1991.

[5] D. Boneh, E. Goh, and K. Nissim: Evaluating 2-dnf formulas on ciphertexts, In proceedings of TCC'05, pp. 325-341, 2005.

[6] J. Bootle, et al.: Efficient zero-knowledge arguments for arithmetic circuits in the discrete Log setting, In proceedings of EUROCRYPT'16, pp. 327-357, 2016.

[7] J. Bootle, et al.: Efficient zero-knowledge proof systems, In proceedings of FOSAD'16, pp. 1-31, 2016.

[8] Uriel Feige, Dror Lapidot, and A. Shamir. Multiple non-interactive zero knowledge proofs under general assumptions, SIAM J. Comput., 29 (1), pp. 1-28, 1999.

[9] J. Garay, Philip DMacKenzie, and K. Yang: Strengthening zero-knowledge protocols using signatures, In proceedings of EUROCRYPT'03, pp. 177-194, 2003.

[10] C. Gentry, et al.: Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proofs, J. Cryptology, 28(4), pp. 820-843, 2015.

[11] 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 CRYPTO'99, pp. 467-484, 1999.

[12] J. Groth: Non-interactive zero-knowledge arguments for voting, In proceedings of ACNS'05, pp. 467-482, 2005.

[13] J. Groth, R. Ostrovsky, and A. Sahai: Perfect non-interactive zero knowledge for NP, In proceedings of EUROCRYPT'06, pp. 339-358, 2006.

[14] J. Groth: Linear algebra with sub-linear zero-knowledge arguments, In proceedings of CRYPTO'09, pp. 192-208, 2009.

[15] J. Groth: Short pairing-based non-interactive zero-knowledge arguments, In proceedings of ASIACRYPT'10, pp. 321-340, 2010.

[16] J. Groth, R. Ostrovsky, and A. Sahai: New techniques for noninteractive zero-knowledge, J. ACM, 59(3), pp. 1-35, 2012.

[17] J. Groth, A. Sahai: Efficient noninteractive proof systems for bilinear groups, SIAM J. Comput. 41(5), pp. 1193-1232, 2012.

[18] J. Kilian and E. Petrank: An efficient noninteractive zero-knowledge proof system for np with general assumptions, J. of Cryptology, 11(1), pp. 1-27, 1998.

[19] A. Sahai and S. Vadhan: A complete problem for statistical zero knowledge, J. ACM, 50(2):196-249, 2003.

[20] A. Santis, et al.: Robust non-interactive zero knowledge, In proceedings of CRYPTO'01, pp. 566-598, 2001.

[21] A. Santis, G. Crescenzo, and G. Persiano: Randomness-optimal characterization of two np proof systems, In proceedings of RANDOM'02, pp. 179-193, 2002.