An Authenticated Key Agreement Scheme Based on Cyclic Automorphism Subgroups of Random Orders

Jun YANG[a], Jian-Hua ZHANG[b]

School of Computer Science and Technology, Southwest Univ. for Nationalities, Chengdu, P.R.C.
[a]junyang898@163.com, [b]jianhuazhang@SWUN.edu.cn

Abstract: Group-based cryptography is viewed as a modern cryptographic candidate solution to blocking quantum computer attacks, and key exchange protocols on the Internet are one of the primitives to ensure the security of communication. In 2016 Habeeb et al proposed a "textbook" key exchange protocol based on the semidirect product of two groups, which is insecure for use in real-world applications. In this paper, after discarding the unnecessary disguising notion of semidirect product in the protocol, we establish a simplified yet enhanced authenticated key agreement scheme based on cyclic automorphism subgroups of random orders by making hybrid use of certificates and symmetric-key encryption as challenge-and-responses in the public-key setting. Its passive security is formally analyzed, which is relative to the cryptographic hardness assumption of a computational number-theoretic problem. Cryptanalysis of this scheme shows that it is secure against the intruder-in-the-middle attack even in the worst case of compromising the signatures, and provides explicit key confirmation to both parties.

1 Introduction

Cryptographic techniques are an essential tool to guarantee the security of communication in modern society. Today, the security of nearly all of the cryptographic schemes used in practice is based on number theoretic problems [1,2,3]. However, schemes like these will become insecure as soon as large enough quantum computers arrive. The reason for this is Shor's algorithm [4], which solves number theoretic problems like integer factorization and discrete logarithms in polynomial time on a quantum computer. Therefore, one needs alternatives to those classical public key schemes which are based on mathematical problems not affected by quantum computer attacks. Group-based cryptography is one of the main candidates for this [3,5,6].

In 2016, using semidirect product of two groups, Habeeb et al [7] proposed a key exchange protocol (the HKKS protocol) based on the work of [8, 9]. Unlike all the operating principles of the existing Diffie-Hellman-like protocols, its basic passive security is based on a stronger computational group-theoretic assumption than the current assumptions of hardness of discrete logarithm problems.

However, the HKKS protocol is still a "textbook" key exchange protocol which is actually not suitable for use in real-world applications due to its lack of any oracle interaction among users (public key owners) and an attacker [10]. In this paper, having discarded the unnecessary disguising notion of semidirect product in the HKKS protocol, we will establish a simplified yet enhanced authenticated key agreement scheme (denoted by the HYZ scheme) based on cyclic automorphism subgroups of random orders, which includes mutual identification of Alice and Bob. Our contributions are:

1) The passive security of the HYZ scheme, which is relative to the cryptographic hardness assumption of a computational number-theoretic problem, is analyzed in terms of formal security terminology. Additionally, selection of protocol parameters for passive security is analyzed.

2) To guarantee its active security, we utilize the "encryption-then-signature" mode to protect twofold for the protocol messages. We show that the HYZ scheme is secure against the intruder-in-the-middle attack even in the worst case of compromising the signatures, and obtains the highest level of assurance regarding key agreement, i.e., explicit key confirmation to both parties [11]: A is assured that B has computed the shared symmetric key K, and no one other than B can compute K.

The organization of the paper is as follows. In Section 2, the HYZ scheme is proposed. In Section 3, the shared key formula is proven and its passive and active security properties are discussed. Conclusions are given in Section 4.

2 The Proposed Scheme

In this section, we describe the HYZ scheme utilizing a kind of public-key infrastructure (PKI) [11,12]. Our strategy is to make hybrid use of certificates which are signed by a TA (Trusted Authority) and symmetric-key encryption as challenge-and-responses in the public-key setting. Each user U has a digital signature function sig_{U} with verification algorithm ver_{U}. The TA also has a signature scheme with a public verification algorithm ver_{TA}.The verification algorithms are compiled and made public by the TA , who certifies that ver_{U} is actually the verification algorithm for U and not for any malicious attacker Mallory. Each user U has a certificate

$$\mathrm{Cert}(\mathrm{U}) = \left(\mathrm{ID}(\mathrm{U}),\ ver_{\mathrm{U}},\ sig_{\mathrm{TA}}\left(\mathrm{ID}(\mathrm{U}),\ ver_{\mathrm{U}}\right)\right),$$

where ID(U) is certain identification information for U.

The public domain parameters consist of a group $(G,\cdot)$, a given element $g \in G$ with order $r > 1$ and a given element $\phi \in \mathrm{Aut}(\mathrm{G})$ with order s . Denote $\phi^0 = \mathrm{Id}_{\mathrm{Aut}(\mathrm{G})}$. Suppose that Alice and Bob want to establish a symmetric key K to use in an encryption function E_K . $x \in_U S$ means [10] sampling element x is taken uniformly random in set S .

1) Alice chooses a random number $m \in_U \{0, 1, 2, \ldots, s-1\}$. Then she computes and sends the following to Bob:

$$a \leftarrow \prod_{i=0}^{m-1} \phi^i(g)$$

$$\mathrm{A} \rightarrow \mathrm{B}: \left(\mathrm{Cert}(\mathrm{A}),\ a\right)$$

2) Bob chooses a random number $n \in_U \{0, 1, 2, \ldots, s-1\}$. Then he computes and sends the following to Alice:

$$b \leftarrow \prod_{j=0}^{n-1} \phi^j(g)$$

$$K_{\mathrm{B}} \leftarrow \phi^n(a)\cdot b$$

$$C_{\mathrm{B}} \leftarrow E_{K_{\mathrm{B}}}\left(sig_{\mathrm{B}}\left(\mathrm{ID}(\mathrm{A}) \,\|\, b \,\|\, a\right)\right)$$

$$\mathrm{B} \rightarrow \mathrm{A}: \left(\mathrm{Cert}(\mathrm{B}),\ b,\ C_{\mathrm{B}}\right)$$

3) Alice computes:

$$K_{\mathrm{A}} \leftarrow \phi^m(b)\cdot a$$

4) Using K_{A} Alice decrypts C_{B} to obtain $sig_{\mathrm{B}}\left(\mathrm{ID}(\mathrm{A}) \,\|\, b \,\|\, a\right)$.

5) Submitting $\mathrm{Cert}(\mathrm{B})$ to TA, Alice asks TA to verify that ver_{B} is Bob's verification algorithm.

6) Alice uses ver_{B} to verify Bob's signature in Step 4). If the signature is not valid, then she "rejects" and quits. Otherwise, she "accepts", computes and sends the following to Bob:

$$C_{\mathrm{A}} \leftarrow E_{K_{\mathrm{A}}}\left(sig_{\mathrm{A}}\left(\mathrm{ID}(\mathrm{B}) \,\|\, a \,\|\, b\right)\right)$$

$$\mathrm{A} \rightarrow \mathrm{B}: C_{\mathrm{A}}$$

7) Using K_{B} Bob decrypts C_{A} to obtain $sig_{\mathrm{A}}\left(\mathrm{ID}(\mathrm{B}) \,\|\, a \,\|\, b\right)$.

8) Submitting $\mathrm{Cert}(\mathrm{A})$ to TA, Bob asks TA to verify that ver_{A} is Alice's verification algorithm. Finally, Bob uses ver_{A} to verify Alice's signature in Step 7). If the signature is not valid, then he "rejects" and quits. Otherwise, he "accepts".

3 Proof of the Shared Key and Security Analysis

3.1 Proof of the Shared Key

Theorem 1 : Alice and Bob share the same symmetric key K , i.e.,

$$K_{\mathrm{A}} = K_{\mathrm{B}} = K = \prod_{i=0}^{m+n-1} \phi^i(g).$$

Proof: Since $\phi \in \mathrm{Aut}(\mathrm{G})$, by the definition in [13], one has

$$\phi^m(b) = \phi^m\left(\prod_{j=0}^{n-1} \phi^j(g)\right) = \prod_{j=0}^{n-1} \phi^m\left(\phi^j(g)\right)$$

$$= \prod_{j=0}^{n-1} \phi^{m+j}(g) = \prod_{j=m}^{m+n-1} \phi^j(g).$$

Hence, $K_{\mathrm{A}} = \phi^m(b)\cdot a$

$$= \prod_{j=m}^{m+n-1} \phi^j(g)\cdot\prod_{i=0}^{m-1} \phi^i(g) = \prod_{i=0}^{m+n-1} \phi^i(g).$$

Similarly, $K_{\mathrm{B}} = \phi^n(a)\cdot b$

$$= \prod_{i=n}^{n+m-1} \phi^i(g)\cdot\prod_{j=0}^{n-1} \phi^j(g) = \prod_{i=0}^{m+n-1} \phi^i(g)$$

Therefore, $K_{\mathrm{A}} = K_{\mathrm{B}} = K$. This completes the proof.

3.2 The Passive Security Properties of the HYZ Scheme

Taking $\phi = \mathrm{Id}_{\mathrm{Aut}(\mathrm{G})}$, we see that the standard Diffie-Hellman protocol is a special case of the HYZ scheme, and so it provides a heuristic evidence of the basic security of the HYZ scheme.

From the random numbers $m,\ n \in \{0, 1, 2, \ldots, s\text{-}1\}$ chosen by Alice and Bob, and their shared key

$K = \prod_{i=0}^{m+n-1} \phi^i(g)$, one of the necessary conditions for passive security of the HYZ scheme is that the order s should be chosen large enough to thwart exhaustive key search.

The two cyclic automorphism subgroups of $\mathrm{Aut}(\mathrm{G})$ of random orders involved in the HYZ scheme are $\langle\phi\rangle_m = \{\phi^0, \phi^1, \phi^2, ..., \phi^{m-1}\}$ and $\langle\phi\rangle_n = \{\phi^0, \phi^1, \phi^2, ..., \phi^{n-1}\}$, both of which act on g .The period of ϕ with respect to g is defined to the smallest positive integer t such that $\phi^t(g) = e_G$ (the identity element of group G). Another necessary condition for passive security of the HYZ scheme is that the period t should be chosen large enough; otherwise, whenever $i \geq t$, we have $\phi^i(g) = \phi^{i-t}(\phi^t(g)) = \phi^{i-t}(e_G) = e_G$, which shows that large private exponents m and n would be wasted in the final result $K = \prod_{i=0}^{m+n-1} \phi^i(g)$, and thus the key space size

$$\left\{K = \prod_{i=0}^{m+n-1} \phi^i(g) : m, n \in_U \{0, 1, 2, ..., s-1\}\right\}$$

would be limited (we call this phenomenon "falsely big data").

The basic security of the HYZ scheme is based on the cryptographic hardness assumption of the following computational number-theoretic problem: Given ϕ, g and $a \left(= \prod_{i=0}^{m-1} \phi^i(g)\right)$, it is computationally infeasible to compute m . More specifically, consider the following experiment for a pair of group-generation algorithms $(\mathcal{G}_1, \mathcal{G}_2)$, algorithm $\mathcal{A}$, and the security parameter n (1^n denotes the string comprised of n ones) :

The cyclic automorphism subgroup factoring experiment $\mathrm{CASF}_{\mathcal{A},\mathcal{G}}(n)$:

1. Run $\mathcal{G}_1(1^n)$ to obtain (G, g), where g is an element with order $r > 1$ in group G .
2. Run $\mathcal{G}_2(1^n)$ to obtain $(\mathrm{Aut}(\mathrm{G}), \phi)$, where ϕ is an element with order s in the automorphism group $\mathrm{Aut}(\mathrm{G})$.
3. Choose a uniform $a \in G$.
4. $\mathcal{A}$ is given ϕ , g and a , and outputs $x \in \{0, 1, 2, ..., s-1\}$.
5. The output of the experiment is defined to be 1 if $a = \prod_{i=0}^{x-1} \phi^i(g)$, and 0 otherwise.

Definition: We say that the CASF problem is hard relative to polynomial-time algorithms $(\mathcal{G}_1, \mathcal{G}_2)$ if for all probabilistic polynomial-time algorithms $\mathcal{A}$ there exists a negligible function negl such that

$$\Pr[\mathrm{CASF}_{\mathcal{A},\mathcal{G}}(n) = 1] \leq \mathrm{negl}(n).$$

The CASF assumption is that there exists a pair of $(\mathcal{G}_1, \mathcal{G}_2)$ for which the CASF problem is hard.

If the adversary is passive, then the session in the HYZ scheme will terminate with both parties "accepting" (provided they behave honestly). That is, A and B successfully identify themselves to each other, and they both compute the key K . The adversary cannot compute any information about the key K , assuming the intractability of the CASF problem.

3.3 The Active Security Properties of the HYZ Scheme

We first shall show how the HYZ scheme is secure against the intruder-in-the-middle attack even in the worst case that the ciphertexts C_A and C_B are decrypted by the intruder, or the signatures of the legitimate communication parties are obliviously leaked to an outsider, as shown in Figure 1.

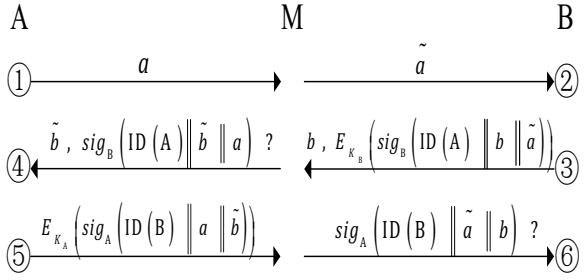

Figure 1. Thwarted intruder-in-the-middle attack on the HYZ scheme

Suppose that Mallory intercepts a in pass ① and replaces it with $\tilde{a}$ in pass ② . M then receives $(\mathrm{Cert}(\mathrm{B}), b, E_{K_B}(sig_B(\mathrm{ID}(\mathrm{A}) \| b \| a)))$ from Bob in pass ③. He would like to replace $(b, \tilde{a})$ with $(\tilde{b}, a)$. However, this means that he must also replace the signature by $sig_B(\mathrm{ID}(\mathrm{A}) \| \tilde{b} \| a)$ in pass ④ . Unfortunately for M, he cannot compute B's signature on the string $\mathrm{ID}(\mathrm{A}) \| \tilde{b} \| a$ because he doesn't know B's signing algorithm sig_B . Similarly, M is unable to replace $sig_A(\mathrm{ID}(\mathrm{B}) \| a \| \tilde{b})$ in pass ⑤ by $sig_A(\mathrm{ID}(\mathrm{B}) \| \tilde{a} \| b)$ in pass ⑥ because he does not know A's signing algorithm sig_A .

This situation is illustrated in Figure 1, in which the question marks indicate signatures that the adversary is unable to compute. It is the use of signatures that

provides for mutual identification of A and B. This in turn thwarts the intruder-in-the-middle attack.

Next, we shall show that the HYZ scheme provides explicit key confirmation [11].

The HYZ scheme is established involving mutual identification in the public-key setting. So, if an adversary is active, he will be detected by the honest participants in the session.

Using the properties discussed above, let us see what we can infer about the HYZ scheme if A or B "accepts." Suppose that A "accepts."Let us analyze why A should believe that B has computed K .The reason for this belief is that in step 4), A uses her symmetric key K_{A} to decrypt C_{B} which has been encrypted by B using K_{B} in step 2), which is identical to K_{A} by Theorem 1, and has obtained B's signature $sig_{\mathrm{B}}\left(\mathrm{ID}\left(\mathrm{A}\right)\left\| b \right\| a\right\|\right)$.Now, assuming that B executed the scheme according to its specifications, and the signature is valid in step 6), A can infer that B has computed the value of $K_{\mathrm{B}} = \phi^{n}\left(a\right)\cdot b$.

The analysis from the point of view of B is similar.

Summarizing the discussion above, we have established the following theorem.

Theorem 2: The HYZ scheme is an authenticated key agreement scheme that provides explicit key confirmation to both parties, assuming that the CASF problem is intractable.

4 Conclusion

Based on the HKKS protocol and cyclic automorphism subgroups of random orders, we proposed the HYZ scheme and proved its shared key formula. Two necessary conditions for its passive security are analyzed: the order s of automorphism $\phi\in\mathrm{Aut}\left(\mathrm{G}\right)$ and the period of ϕ with respect to g should be chosen large enough to thwart exhaustive key search and avoid the phenomenonof "falsely big data", respectively. Furthermore, we conducted the $\mathrm{CASF}_{A,g}\left(n\right)$ experiment, defined the CASF problem and depicted the CASF assumption in terms of formal security terminology. To guarantee its active security, we utilized twofold protections for the protocol messages. It was showed that the HYZ scheme is secure against the intruder-in-the-middle attack even in the worst case of compromising the signatures, and is an authenticated key agreement scheme that provides explicit key confirmation to both parties, assuming that the CASF problem is intractable.

Compared with the HKKS protocol, the security of the HYZ scheme has been improved in a number of aspects. Future work includes cryptanalysis of the HYZ scheme resistance to the “linear algebra attack” mounted by Romank'ov [14].

Acknowledgement

The Research of both authors was supported by the Fundamental Research Funds for the Central Universities–Southwest University for Nationalities (2014NYB04) and Sichuan Provincial Project of Science and Technology(2012JY0096).

References

1. J. Hoffstein, J. Pipher, and J. H. Silverman, An Introduction to Mathematical Cryptography, New York: Springer Science + Business Media, LLC, 2008, pp. 59–62.
2. J. Katz and Y. Lindell, Introduction to Modern Cryptography, 2nd ed., Boca Raton: CRC Press, 2015, pp. 285–286, p. 320.
3. A. Petzoidt, J. Ding, and L.Wang, "Eliminating decryption failures from the simple matrix encryption scheme". http://eprint.iacr.org/2016/010.
4. P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". SIAM Journal on Computing, 1997, 26 (5) : pp. 1484–1509.
5. A. G. Myasnikov, V. Shilprain, and A. Ushakov, Group-based cryptography, Basel-Boston-Berlin: Birkhauser Verlag, 2008, pp. 77–78.
6. E. Alkim, L. Ducas, T. Poppelmann, et al, "Post-quantum key exchange - a new hope". http://eprint. iacr.org/2015/1092.
7. M. Habeeb, D. Kahrobaei, C. Koupparis, et al, "Using semidirect product of (semi)groups in public key cryptography", A. Beckmann et al (Eds): CiE 2016, LNCS, Springer International Publishing Switzerland, 2016: pp. 132–141.
8. M. Habeeb, D. Kahrobaei, and V. Shilprain, "Public key exchange using semidirect product of (semi)groups", M. Jacobson et al (Eds). Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2013: pp.475–486.
9. D. Kahrobaei, C. Koupparis, and V. Shilprain, "Public group-based cryptography using matrices over group rings", Groups, Complexity, Cryptology , 5 (2013) : pp. 97–115.
10. W. Mao, Modern Cryptography: Theory and Practice, Upper Saddle River: Prentice Hall PTR, 2004, pp. 358–362.
11. D. R. Stinson, Cryptography: Theory and Practice, 3rd ed., Boca Raton: Chapman & Hall/CRC, 2006, pp. 367–368, pp. 429–436 .
12. W. Trappe and L. C. Washington, Introduction to Cryptography with Coding Theory, 2nd ed. , Upper Saddle River: Pearson Prentice Hall, 2006, pp. 256–259.
13. S. Lang, Algebra, Revised 3rd ed., New York: Springer-Verlag New York, Inc., 2002, p. 10, p. 54.
14. V. Romank'ov, "Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups", Computer Science, 2015 (August): pp. 1–7.