Summer 5-25-2013

Authenticated Key Agreement Protocol Based on a Matrix Group and Polynomial Ring over a Finite Field

Yang Jun
JunCollege of Computer Science and Technology, Southwest University for Nationalities

Zhang Jianhua
College of Computer Science and Technology, Southwest University for Nationalities

Chen Jianying
College of Computer Science and Technology, Southwest University for Nationalities

Liu Tiao
College of Computer Science and Technology, Southwest University for Nationalities

Shu Linxin
College of Computer Science and Technology, Southwest University for Nationalities

Authenticated Key Agreement Protocol Based on a Matrix Group and Polynomial Ring over a Finite Field

Jun Yang，*Jianhua Zhang*, *Jianying Chen*，*Tiao Liu*，*Linxin Shu*
College of Computer Science and Technology, Southwest University for Nationalities, Chengdu, Sichuan 610041, China

Abstract: Alongside encryption and signatures, key agreement is one of the fundamental issues in modern cryptography and its security is the main concern in cloud computing and World Wide Web-based applications. In this paper, a novel type of more secure 3-pass key agreement protocol is proposed based on a recently proposed matrix-based key agreement protocol of Romańczuk and Ustimenko. By the hash-and-sign approach and immediate use of new session key, explicit key authentication, forward secrecy and bit security are achieved simultaneously. Cryptanalysis also shows that it is immune to the man-in-the-middle attack while matrix entries from a commutative ring provide an advantageous hiding mechanism.

Keywords: Key agreement protocol, Explicit key authentication, Man-in-the-middle attack, Forward secrecy, Bit security

1. INTRODUCTION

Information and multimedia communications technologies provide cyber-infrastructure and platforms to achieve more efficient business in cloud computing over open computer and communications networks such as the Internet, in particular, via World Wide Web-based tools[1]. Secure services can be realized only if communications are conducted securely and an effective solution is to apply cryptography.

In modern cryptography, cryptographic keys are the basis for secure communication channels and the establishment of secret keys is a major problem and the Achilles' heel for the large-scale deployment of symmetric cryptography[2, 3]. Currently, there are basically two approaches to address the problem: one is the use of a KDC (Key Distribution Centre), such as Kerberos and the other is the use of a key establishment protocol[4]. The latter provides shared secrets between two or more parties, typically for subsequent use as symmetric keys for a variety of information security services including encryption, message authentication, and entity authentication. These protocols may be further subdivided into key exchange (unfortunately, key-exchange protocols also tend to be more involved[4, 5]) and key transport: in the former all participating entities contribute information which is used to derive the shared secret key, while in the latter one entity creates the secret key and securely transfers it to the other(s) .

Up to date, there have been three types of key transport protocols[4],[5]: key transport based on symmetric encryption and hybrid key transport protocols using symmetric encryption in addition to both public-key encryption and signatures. An authenticated key establishment protocol is a key establishment protocol which provides key authentication. It is generally desired that each party in a key establishment protocol be able to determine the true identity of the other(s) which could possibly gain access to the resulting key, implying preclusion of any unauthorized additional parties from deducing the same key. While privacy of keying material is a requirement in key transport protocols, source authentication is also typically needed and the majority of these approaches rely on asymmetric cryptography.

In 2008, Myasnikov, Shpilrain and Ushakov[6]conjectured that groups of matrices over finite commutative rings could be the best platforms for canonical cryptographic protocols because these groups have "the best of both worlds" in the sense that matrix multiplication is non-commutative, but matrix entries coming from a commutative ring provides a good hiding mechanism. In 2010, Romańczuk and Ustimenko[7] proposed a key agreement protocol based on a matrix group and polynomial ring over a finite field. In 2011, Blackburn, Cid and Mullan[8] amounted an attack on it, but it was invalid for the attacker utilized a secret system parameter. In this paper, however, we observe that it is lack of the mechanisms of identification and data origin authentication that causes the RU's protocol to encounter the man-in-the-middle attack. Inspired by the above work, we propose and discuss a hybrid authenticated key agreement transport protocol using the hash-and-sign approach and immediate use of new session key, which turns out to be more secure against several common attacks than the RU's protocol. Section 2 describes the proposed 3-pass protocol. Its security and performance analysis are examined in section 3. Conclusions and future work are presented in section 4.

2. THE PROPOSED PROTOCOL

In this section, inspired by the idea of Romańczuk and Ustimenko and introducing a symmetric encryption algorithm and digital signatures with a secure one-way hash function, we propose a three-pass variation of the famous Station-to-Station protocol (STS) which allows the establishment of a shared secret key between two parties with mutual entity authentication and mutual explicit key authentication. The protocol also facilitates anonymity – the identities of A and B may be protected from eavesdroppers.

The Proposed Protocol

SUMMARY: parties A and B exchange 3 messages.

RESULT: key agreement, mutual entity authentication, explicit key authentication.

1. One-time setup (definitions and publication of system parameters)

Let $\mathrm{GL}_n(\mathrm{F}_q)$ denote the group of invertible $n \times n$ matrices over a finite field F_q of order q, and let $\mathrm{F}_q[x, y]$ denote the polynomial ring over F_q in two variables x and y. Let $C, D \in \mathrm{GL}_n(\mathrm{F}_q)$ be two commuting matrices and let $d \in \mathrm{F}_q^n$. The matrices C, D and the vector d are made public.

Each user U has a signature scheme, where its signature algorithm is denoted as Sig_U and verification algorithm Ver_U, and has a public-key certificate $\mathrm{Cert}(U) = (\mathrm{ID}(U), \mathrm{Ver}_U, \mathrm{Sig}_{\mathrm{CA}}(\mathrm{ID}(U), \mathrm{Ver}_U))$, where $\mathrm{Sig}_{\mathrm{CA}}$ is the signature algorithm of a Certification Authority (CA). Let E be a symmetric encryption algorithm. $S_A(m)$ denotes A's signature on a string m using A's private key, defined as $S_A(m) = \mathrm{Sig}_A(H(m))$, where H is a secure one-way hash function and any n-dimensional vector is coded as the bitwise concatenation of its components prior to being hashed.

2. Protocol messages and actions

1) Alice randomly picks a polynomial $f_A(x, y) \in \mathrm{F}_q[x, y]$, computes:

$$\omega_A \leftarrow f_A(C, D)\, d,$$

and then sends $\mathrm{Cert}(U)$ P ω_A to Bob.

2) Bob randomly picks a polynomial $f_B(x,y) \in \mathrm{F}_q[x, y]$, computes:

$$\omega_B \leftarrow f_B(C,D)d,$$

$$K \leftarrow f_B(C,D)\omega_A,$$

$$\sigma_B \leftarrow E_K\left(S_B(\mathrm{ID}(A) \ \mathrm{P}\ \omega_B \ \mathrm{P}\ \omega_A) \right),$$

and then sends $\mathrm{Cert}(B) \ \mathrm{P}\ \omega_B \ \mathrm{P}\ \sigma_B$ to Alice.

3) Alice uses Ver_B to verify σ_B .If the signature σ_B is invalid, then she "rejects and exits"; otherwise she "accepts", and performs the following steps:

3.1) Compute $K \leftarrow f_A(C,D)\omega_B$

3.2) Hash-sign-and-encrypt:

$$\sigma_A \leftarrow E_K\left(S_A(\mathrm{ID}(B) \ \mathrm{P}\ \omega_A \ \mathrm{P}\ \omega_B) \right)$$

3.3) $A \rightarrow B$: σ_A

4) Bob uses Ver_A to verify σ_A .If the signature σ_A is invalid, then she "rejects and exits"; otherwise she "accepts".

3. SECURITY AND PERFORMANCE ANALYSIS

A key establishment protocol should ideally result in the sharing of secret keys that have the same attributes as keys that were established by people who know each other and meet in a secure location to select a key by repeatedly tossing a fair coin. In particular, subsequent use of the secret keys in a cryptographic protocol should not in any way reduce the security of that protocol. This notion of security has proved very difficult to formalize. Instead, for a two-party key agreement protocol, the main security goals of a key establishment protocol are implicit/explicit key authentication [2]-[5]:

1) *Implicit key authentication.* A key establishment protocol is said to provide implicit key authentication (of *B* to *A*) if entity *A* is assured that no other entity aside from a specifically identified second entity *B* can possibly learn the value of a particular session key. The property does not imply that *A* is assured of *B* actually possessing the key.

2) *Explicit key authentication*. A key establishment protocol is said to provide key confirmation (of *B* to *A*) if entity *A* is assured that the second entity *B* can compute or has actually computed the session key. If both implicit key authentication and key confirmation (of *B* to *A*) are provided, then the key establishment protocol is said to provide explicit key authentication (of *B* to *A*). Explicit key authentication of both entities normally requires three passes (messages exchanged).

In step 3.1), Alice and Bob have the proof of their shared key *K* as follows:
Since

$$\begin{cases} K_B \leftarrow f_B(C,D)\omega_A = f_B(C,D)f_A(C,D)d \\ K_A \leftarrow f_A(C,D)\omega_B = f_A(C,D)f_B(C,D)d \end{cases} \quad (1)$$

and $CD = DC$, one has that

$$f_A(C,D)f_B(C,D) = f_B(C,D)f_A(C,D).$$

Therefore, $K_A = K_B$, which means that Alice is assured that Bob can compute or has actually computed the session key K. Likewise, after step 4) is successfully executed, Bob is assured that Alice can compute or has actually computed the session key K. Furthermore, no entity apart from Alice and Bob can compute K, due to the following two properties: $f_A(C,D)$ and $f_B(C,D)$ are two secret system parameters any passive attacker cannot eavesdrop. And any active attacker cannot solve the system (1) of matrix equations, given $K\ (= K_A = K_B)$, ω_A, ω_B, and d [6]. In other words, the proposed protocol provides explicit key authentication.

When examining the security of protocols, it is assumed that the underlying cryptographic mechanisms used, such as encryption algorithms and digital signatures schemes, are secure. Thus, there are other possible ways to attack our protocol as follows.

The man-in-the-middle attack: As shown above, any attacker cannot acquire the session key K, and hence he cannot decrypt σ_B and σ_A in steps 2) and 3.2). Although he can intercept ω_A and ω_B in steps 1) and 2), and could substitute them for $\omega_A^{'}$ and $\omega_B^{'}$, respectively, he has to continue to substitute the original signatures for $S_B(\mathrm{ID}(A)\ \mathrm{P}\ \omega_B\ \mathrm{P}\ \omega_A^{'})$ and $S_A(\mathrm{ID}(B)\ \mathrm{P}\ \omega_A\ \mathrm{P}\ \omega_B^{'})$. Fortunately, since he does not know the signature algorithms Sig_B and Sig_A, he cannot compute B's or A's signature with respect to the string $\mathrm{ID}(A)\ \mathrm{P}\ \omega_B\ \mathrm{P}\ \omega_A^{'}$ or $\mathrm{ID}(B)\ \mathrm{P}\ \omega_A\ \mathrm{P}\ \omega_B^{'}$. This means that our protocol is immune to the man-in-the-middle attack.

Other merits of our protocol include:

Two parties sharing no a priori keying material can end up with a shared secret key.

The publicly transported factors ω_A and ω_B, which are the main contribution to the key agreement and not allowed to be impersonated, are encrypted by a symmetric encryption algorithm together with a secure one-way hash function H to guarantee the integrity and authenticity[9].Therefore, the proposed protocol can be classified as a secret key exchange[10], and thus be assured forward secrecy and bit security providing that the session key K in the above should actually be set to $H(K)$.

All the inverses of underlying matrix group $\mathrm{GL}_n(\mathrm{F}_q)$ can be obtained by pre-computation before the protocol actions are taken. During the whole process of the protocol execution, all the matrix multiplication, exponentiation, and evaluation of polynomials cab be efficiently conducted[11]-[13], which facilitates on-line key establishment.

4. CONCLUSIONS AND FUTURE WORK

The proposed 3-pass protocol is a novel type of hybrid authenticated key transport protocol satisfying several desirable security properties and efficient in computation and communication. Its basic security is based on the widespread difficulty problem of the discrete logarithm and secure against the passive attack and some active attacks: By the hash-and-sign approach and immediate use of new session key, explicit key authentication, forward secrecy and bit security are achieved simultaneously and the man-in-the-middle attack is naturally prevented. Furthermore, it requires no keys private or public to be exchanged beforehand, which is its inherent

advantage.

While it is unconditionally secure and does not depend on any computational intractability assumptions, the quantum key establishment protocol is currently not practical for actual applications[14]. Future work includes designing efficient and authenticated key transport protocols provably secure in the random oracle model for network security systems, conducting simulation and doing in-depth performance analysis of the proposed novel protocol.

ACKNOWLEDGEMENT

This research was supported by the Natural Science Foundation of the State Ethnic Affairs Commission of China (10XN08), "National College Students Innovation and Entrepreneurship Training Programme" Project of SWUN (201210656014), Technological Application Basic Project of Sichuan Province (2012JY0096), and Humanities and Social Science Project of Ministry of Education of China (12YJAZH004).

REFERENCES

[1] Jangra1 A, Bala R. (2012). A Survey on Various Possible Vulnerabilities and Attacks in Cloud Computing Environment[J]. International Journal of Computing and Business Research, 3(1): 1-13

[2] Menezes A J, Oorschot P Van, Vanstone S. (1997). Handbook of Applied Cryptography[M]. Boca Raton: CRC Press, 489-492, 519-520

[3] Cohen H, Frey G. (2006). Handbook of Elliptic and Hyperelliptic Curve Cryptography[M]. Boca Raton: Chapman & Hall/CRC, 573-576

[4] Katz J, Lindell Y. (2012). Introduction to Modern Cryptography: Principles and Protocols[M]. Beijing: National Defense Industry Press, 212-216 (in Chinese)

[5] Zhang Hua, Wen Qiaoyan, Jin Zhengping. (2012). Provably Secure Algorithms and Protocols[M]. Beijing: Science Press, 280-295 (in Chinese)

[6] Myasnikov A, Shpilrain V, Ushakov A. (2008). Group-based Cryptography (in: Advanced Courses in Mathematics CRM Barcelona) [M]. Birkhauser: Verlag AG, 65-67

[7] Romanczuk U, Ustimenko V. (2010). On the $PSL_2(q)$, Ramanujan graphs and key exchange protocols. http://aca 2010.info/index.php/aca2010/aca2010/paper/viewFile/80/3

[8] Blackburn S R, Cid C, Mullan C. (2011). Cryptanalysis of three matrix-based key establishment protocols[J]. Journal of Mathematical Cryptology, 5 (2): 159-168

[9] Anderson R J, translated by Qi Ning, Han Zhiwen, Liu Guoping. (2012). Security Engineering: A Guide to Building Dependabale Distributed Systems (2nd Ed.) [M]. Beijing: Tsinghua University Press, 98 (in Chinese)

[10] Goldwasser S, Bellare M. (2008). Lecture Notes on Cryptography: 217-218. http://www.math. uni-bonn.de/~ saxena/courses/WS2010-ref1.pdf

[11] Shoup V. (2008). A Computational Introduction to Number Theory and Algebra [M]. Cambridge: Cambridge University Press, 64-69, 77-82

[12] Cormen T H, Leiserson C E, Rivest R L, et al. (2008). Introduction to Algorithms (2nd Ed.) [M]. Massachusetts: The MIT Press, 735-751

[13] Knuth D E. (2010). The Art of Computer Programming,Vol 2: Seminumerical Algorithms (3rd Ed.) [M]. Beijing: Posts & Telecom Press, 499-501

[14] Barrett J, Colbeck R, Kent A. (2013). Memory Attacks on Device-Independent Quantum Cryptography[J]. Physical Review Letters, American Physical Society, 110 (1): 67-71