Robust Framework for Certificateless Authenticated Key Agreement Protocol

Smita R. Chunamari
Dept of. Computer Egineering
A.C.Patil College of Egineering Kharghar
Navi Mumbai, India

D. G. Borse
Dept. of Electronic and Telecom. Engg.
A.C.Patil College of Egineering Kharghar
Navi Mumbai, India

ABSTRACT
Authenticated key agreement protocol is exploited to share a secret key for encrypting information being transferred between two or additional parties over a public network. In this implementation can produce multiple public keys for a corresponding private key. In this paper, an alternative key generation technique is proposed for certificate less public key cryptography in order to have one public key for one private key. This will improve the security features of the relevant key generation.

Keywords
Authenticated key agreement; key generation, Certificate less public key cryptography, identity-based public key cryptography, efficiency, security.

1. INTRODUCTION
The challenge today in developing secure systems based on public key cryptography is not choosing appropriately secure algorithms and implementing these, but rather developing an infrastructure to support the authenticity of a user's public key. In the traditional public key infrastructure (PKI), certificates are used to provide an assurance of the relationship between public keys and the identities that hold the corresponding private keys. However, a PKI faces many challenges in practice, such as the scalability of the infrastructure and certificate management. To address the shortcomings of PKI and to simplify key management, Shamir [1] proposed the notion of identity-based public key cryptography (ID-PKC) in which the public keys are derived from the users' identities, such as a username or an e-mail address. Private keys are generated by a trusted third party called a Private Key Generator (PKG), and thus ID-PKC eliminates the need for certificates. Unfortunately, ID-PKC is not without problems. The dependence on a PKG that uses a system-wide master key to generate private keys introduces problems such as key escrow and trust. For instance, the PKG can decrypt any cipher-text from any user to which it has issued a key. Moreover, the PKG can forge any signature and masquarade as any user in the identity-based setting. In Al-Riyami and Paterson proposed the concept of certificateless public key cryptography (CL-PKC) to address the key escrow limitation of ID-PKC. Yet, CL-PKC does not require the use of certificates and can thus be considered a cross between ID-PKC and PKI. A key agreement protocol is wormed to permit two or a lot of parties to ascertain a session key over open networks. Each party will cipher any message such that the parties sharing the key session key will decode the message. Authenticated key agreement should not only be secure against passive adversaries who are eavesdropping communications between parties, however additionally active adversaries who impersonate one party to speak with another party. An authenticated key agreement protocol (AKA) is a fundamental tool in cryptography with which it is possible for two parties to establish a shared session key, using public channels. In certificateless public key cryptography, each user knows three secrets: a) the secret value linked to the public key and generated by its owner; b) The id-based secret (called "partial private key"), generated by the KGC; c) the ephemeral secret, temporary for each session.

The main difficulty today in developing secure systems based on public key cryptography is not the problem of choosing appropriately secure algorithms or implementing those algorithms. Rather, it is the deployment and management of infrastructures to support the authenticity of cryptographic keys: there is a need to provide an assurance to the user about the relationship between a public key and the identity (or authority) of the holder of the corresponding private key. In a traditional Public Key Infrastructure (PKI), this assurance is delivered in the form of certificate, essentially a signature by a Certification Authority (CA) on a public key. The contribution of this paper area of certificate less cryptography is two-fold. It first identifies some weaknesses in generic constructions independently considered. It shows that one of these flaws is also present in the second provably secure CLE scheme of Al-Riyami and Paterson. where it can be very easily fixed.

The paper then explains how to obtain generic constructions which are provably secure in the random oracle model. It does so by first giving a generic random oracle-using conversion to turn any CLE scheme which is only secure against chosen-plaintext attacks into an IND-CCA scheme in the full model of Al-Riyami and Paterson.

2. RELATED WORK
Sattam S. Al-Riyami e.t. al [2] has demonstrated, how hierarchical CL-PKC can be supported. The schemes are all derived from pairings on elliptic curves. The lack of certificates and the desire to prove the schemes secure in the presence of an adversary who has access to the master key requires the careful development of new security models. For reasons of brevity, the focus in this paper is on the security of CL-PKE. Tarjei K. Mandt [3] proposed in this paper a new certificateless authenticated two-party key agreement protocol that only requires each party to compute two pairings. They perform a security analysis and heuristically argue that the protocol obtains the desired security attributes. They also show that our protocol can be used to establish keys between members of distinct domains (under different KGCs). Finally, they compare the protocol's efficiency to current identity-based and certificate less protocols. George Lippold e.t. al [4] has demonstrated in this paper, a more secure than ID-based schemes, in the sense that the KGC can be more actively trying to learn Secrets. To answer Swanson's third

question, whether the edibility of certificate less schemes is worth the increased likeliness of vulnerabilities, we note that the ability of the adversary to replace public keys does not necessarily have to introduce vulnerabilities. CL-AKE schemes therefore combine user edibility with enhanced privacy.

Shengbao Wang e.t. al [5] has proposed in this paper, that the newly proposed protocol is of great efficiency and practical. Moreover, we prove that it provides perfect forward secrecy plus all the other security attributes of authentication and key agreement protocols such as known-key secrecy and no key control.

Yinxia Sun e.t. al [6] has demonstrated in this paper is construction provides optimal bandwidth and quite efficient decryption process compared with the existing CLPKE schemes. It is provably securing against adaptive chosen cipher text attacks in the random oracle model under a slightly stronger assumption.

Benoıt Libert [7] they presented how to easily fix these problems and give a method to achieve generic CLE constructions which are provably CCA-secure in the random oracle model. They finally propose a new efficient pairing- based scheme that performs better than previous proposals without pre- computation. They also prove its security in the random oracle model. They also show that our protocol can be used to establish keys between members of distinct domains (under different KGCs).

Morteza Arifi e.t. al [8] proposed a protocol based on Weil pairing, ID-based authentication and complete ternary tree architecture. The authors show that our protocol satisfies all known security requirements, and therefore it is more secure and efficient than the compared group key exchange protocols that we discuss in this article.

Paulo S. L. M. e.t. al [9] have proposed several new algorithms to implement pairing-based cryptosystems. Our algorithms are all practical and lead to significant improvements, not only for the pairing evaluation process but to other operations as well, such as elliptic curve scalar multiplication and square root extraction.

3. PROBLEM DESCRIPTION

In 2003, Al-Riyami and Paterson proposed the concept of certificateless public key cryptography (CL-PKC) [2]. In a way, CL-PKC combines the best of both worlds by still operating in a certificateless environment like ID-PKC, but using a trust model similar to that of PKI. Thus, CL-PKC does not inherit the escrow property of ID-PKC, making the system ideal for networks where privacy or user anonymity is preferred. Furthermore, the absence of certificates removes the cost incurred by certificate storage, distribution, and verification which makes CL-PKC far more efficient than traditional PKI. CL-PKC still makes use of a trusted authority, but in contrast to ID-PKC, the key generation center (KGC) does not have access to the entities' private keys. Instead, the KGC generates a partial private key that the user then combines with a secret value. Together, these values make up the actual private key, and thus the KGC cannot recover the shared secret established between entities. This change to the scheme also makes it impossible for the KGC to forge any signatures. The public key is generated in a similar way by letting the user combine its secret value with a public parameter selected by the KGC. However, since the secret value is only known to a specific user, public keys can no longer be generated by anyone as in ID-PKC. Thus, the scheme loses the benefit of identity-based key derivation. Consequently, public keys must be provided in some other way, such as through a public directory or by attaching them to messages in a protocol run. Since the introduction of CL-PKC, many new papers have proposed improvements and fixes to the original scheme. However, most of these concern certificateless public key encryption (CL-PKE) and thus few new primitives (such as signature schemes and key agreement protocols) have been proposed. In [2], the original CL-PKE scheme of [2] was improved both in terms of efficiency and security. Later, [10] discovered an adaptive chosen ciphertext vulnerability and proposed a countermeasure to overcome the flaw. In [11], Dent and Kudla argues against a claim that the certificateless schemes cannot be proven secure in the standard model.

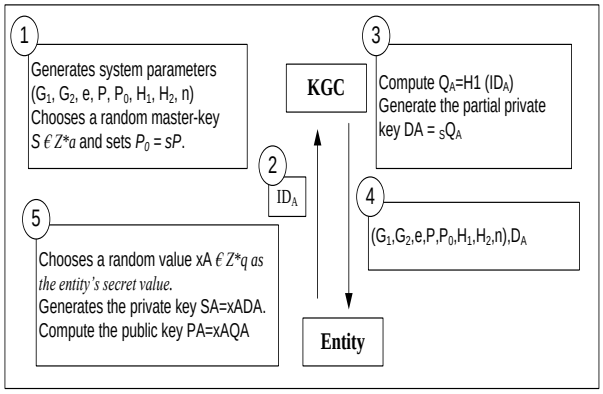
There is always a need to improve the efficiency or security of a key agreement protocol. It is important to understand that protocols are never perfect. Many times, proposed protocols are found to lack certain desirable properties or to be inefficient in some way. Over time, authors will always find new and clever ways to improve the efficiency or the security of protocols. In their seminal paper on CL-PKC, Al-Riyami and Paterson (AP) proposed a certificateless authenticated key agreement protocol. Their protocol essentially requires each party to compute four bilinear pairings. Such pairings can be computationally intensive to compute (for instance, in low-power devices), and should therefore be used moderately in protocols. Moreover, their protocol also requires users to exchange public keys comprising two group elements. Ideally, public keys should only comprise one group element as in identity-based cryptography.

Due to these apparent shortcomings, it would be desirable to propose a new certificateless key agreement protocol that offers essentially the same security as AP's protocol, but with improved efficiency.

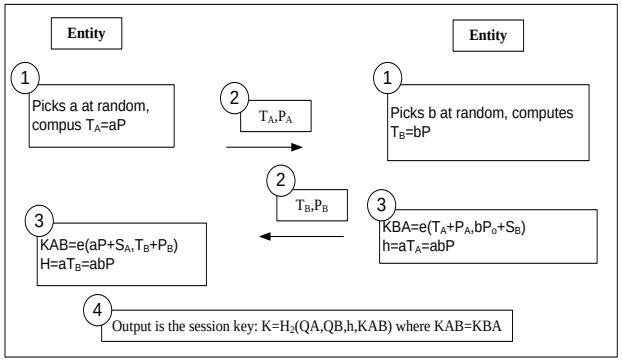
4. PROPOSED PROTOCOL

The advantage and benefits of using a key agreement protocol based on CL-PKC is that there is no PKI and will therefore save communication costs. The solution may therefore be ideal in a wireless environment or in low-power devices where resources are limited. Moreover, a certificateless key agreement protocol does not have the property of key escrow inherent of ID-PKC. Thus, it may be more suited in a distributed environment (in which privacy is a requirement), whereas ID-based protocols seems more suited for smaller networks and closed groups. The proposed protocol is the target to realize higher degree of security by creating one public key for a corresponding private key exploitation the options of ID-PKC.

The relevant projected Algorithms ar given during this section. Figure 1 shows the method flows of the projected key generation and key agreement concerned in CL-PKC. KGC executes Setup algorithmic program to get master-key and system parameters. Then, it runs Partial-Private-Key-Extract algorithmic program to extract the partial personal key for every entity. Each entity chooses a secret worth and computes its public and personal key. Later, two entities run key agreement algorithmic program on-line so as to share a session key.



a) Key Generation



b) Key Agreement

Fig 1. Certificate less Key Generation and Agreement

5. PRELIMINARY

In below there are some following summarize definitions of the security attributes of key agreement protocol.

1) Known-key secrecy: Each run of the protocol should result in an inimitable session key. Key generated in one protocol round is independent and should not be uncovered if other session keys are compromised.

2) Forward secrecy: If the long-term private keys of one or more entities are cooperated, the confidentiality of previously recognized session keys should not be affected.

3) Perfect forward secrecy: If the long-term private keys of all the entities are compromised, the confidentiality of previously established session keys should not be precious.

4) KGC forward secrecy: If the master key of KGC is despoiled, the security of session keys previously recognized should not be compromised by any entity.

5) Key-compromise impersonation: When entity A's long-term private key is compromised, the adversary should not be able to share a session key with A by acting as another entity B.

6) Unknown key-share resilience: Entity A should not share a key with entity C when in fact A thinks that it is sharing the key with entity B.

7) No key control: The session key should be resolute jointly by both entities. None of the entities can control the key alone.

8) Known session-specific temporary information security: The compromise of randomized input used a protocol run should not reveal the agreed session keys.

6. DISCUSSION

In this section, the performance of the proposed protocol is analyzed in terms of security attributes and algorithm intricacy:

Security Attributes

1) Known-key secrecy: A and B choose random a ε Z*q and b ε Z*q respectively in each protocol run; they will have individual session key in each run. Therefore, compromising the secret keys will not affect the next session key to be generated.

2) Forward secrecy: Even if the adversary knows the long-term private keys of *A* and *B*, the adversary still needs to compute *h* from *TA* and *TB* which is a CDH problem. Therefore, cooperation the long-term private keys of all entities will not reveal previously established session keys. As a result, the proposed protocol achieves perfect forward secrecy.

3) KGC forward secrecy: CL-PKC based schemes do not have key escrow problem. If an adversary has the KGC's master private key, *s*, the previously established session keys will not be exposed. Although the adversary may generate the partial private key, both the short-term and long-term private keys of an entity are needed in order to compute the session key.

4) Key-compromise impersonation: Assume that an Adversary knows the private key of *A*, *SA*, and impersonates *B* to share the session key with *A*. The adversary will have the knowledge on *SA*, *aP*, and *b*, however, he would not be able to compute $e(P,QB)^{asxB}$ as S_B is unknown. Another option is to compute *asxBP* which is a CDH problem.

5) Unknown key-share resilience: As *QA* and *QB* are used for computing the session key, each entity knows who he shares the key with.

6) No key control: Minimum two entities collaborate together to produce a session key using their random short-term private keys. However, key control can be imperfect when *A* sends its (*PA*, *TA*) to *B*, but *B* does not send its (*PB*, *TB*) to *A*. This particular security attribute can be supported externally using individual error checking or troubleshooting methods in the protocols.

7) Known session-specific temporary information security: Even the adversary compromises the short-term private keys of a session; he will not be able to calculate the session key as the long-term private keys are unidentified to him.

8) Passive attack: Assume that the adversary observes the messages (P_A, T_A, T_B, P_B) transferred between the entities and he knows the master key of KGC, *s*. The adversary will not be able to compute the session key as he needs to calculate *abP* from *aP* and *bP*. This is a CDH problem.

7. CONCLUSION

In the final conclusion in this paper is secure and efficient certificate less authenticated key generation and agreement protocol are presented that produces distinct public key for a corresponding personal key. Within the original scheme, a dishonest KGC might restore AN entity's public key by one

that it knows the key price without worrying of being recognized. However, in our planned theme, the existence of two public key for AN identity will solely result from the existence of two partial personal keys binding that entity to two totally different public keys; solely KGC might have created these two partial personal keys. Thus, the new binding technique makes the KGC's substitute of a public key noticeable.

The security analysis shows that the key agreement protocol achieves most of the illustrious fascinating security attributes like known-key secrecy, key-compromise impersonation, unknown key-share, illustrious session-specific temporary info security, forward secrecy and no key control. What is more, it conveys higher potency in distinction to the present protocols. Additionally, the key generation and agreement protocols cut back the quantity of trust on KGC. Currently, among the longer term work that we tend to attempt to pursue includes investigation the potency of the projected protocol in distributed environments, e.g. peer-to-peer and grid computing platforms.

8. REFERENCES

[1] A. Shamir. Identity-based cryptosystems and signature schemes, In G. R. Blakley and D. Chaum, editors, Advances in Cryptology - CRYPTO'84, volume 196 of Lecture Notes in Computer Science, pages 47-53. Springer-Verlag, 1985.

[2] S.S. Al-Riyami and K. Paterson. Certificateless Public Key Cryptography. In C. S. Laih, editor, Advances in Cryptology - Asiacrypt 2003, volume 2894 of Lecture Notes in Computer Science, pages 452-473. Springer-Verlag, 2003.

[3] T. K. Mandt and C. H. Tan, "Certificateless authenticated two-party key agreement protocols," in Proc. ASIAN'06, Berlin, Heidelberg: Springer-Verlag, 2007, p. 37–44.

[4] G. Lippold, C. Boyd, and J. Gonzalez Nieto, "Strongly secure certificateless key agreement," in Proc. Pairing '09, Berlin, Heidelberg, Germany: Springer-Verlag, 2009, p. 206–230.

[5] S. Wang, Z. Cao, and H. Bao, "Efficient certificateless authentication and key agreement (cl-ak) for grid computing," International Journal of Network Security, vol. 7, no. 3, pp. 342–347, 2006.

[6] Y. Sun and F. Zhang, "Secure certificateless public key encryption without redundancy," Cryptology ePrint Archive, Report 2008/487, 2008, http://eprint.iacr.org/.

[7] B. Libert and J. jacques Quisquater, "On constructing certificateless cryptosystems from identity based encryption," in PKC 2006. Springer- Verlag, 2006, p. 474–490.

[8] Morteza Arifi, An ID-Based Key Agreement Protocol Based on ECC Among Users of Separate Networks, International Journal of Computer Science and Security, 2012.

[9] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," Advances in Cryptology -- Crypto'2002, Lecture Notes on Computer Science 2442, Springer-Verlag (2002), pp. 354--368.

[10] Z. Zhang and D. Feng. On the Security of a Certificateless Public-Key Encryption. Cryptology ePrint Archive, Report 2005/426.

[11] A.W. Dent and C. Kudla. On Proofs of Security for Certificateless Cryptosystems. Cryptology ePrint Archive, Report 2005/426.