Computers and Electrical Engineering 38 (2012) 563–572

Contents lists available at SciVerse ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A provably secure authenticated key agreement protocol for wireless communications ☆

Hua Guo [a,*], Chang Xu [a], Yi Mu [b], Zhoujun Li [c]

[a] School of Computer Science and Engineering, Beihang University, Beijing, People's Republic of China
[b] School of Computer Science Software Engineering, University of Wollongong, NSW, Australia
[c] State Key Laboratory of Software Development Environment, Beihang University, Beijing, People's Republic of China

ARTICLE INFO

Article history:
Available online 21 November 2011

ABSTRACT

Designing elliptic curve password-based authenticated key agreement (ECPAKA) protocols for wireless mobile communications is a challenging task due to the limitation of bandwidth and storage of the mobile devices. Some well-published ECPAKA protocols have been proved to be insecure. We notice that until now none of the existing ECPAKA protocols for wireless mobile communication is provided any formal security analysis. In this paper, we propose a novel protocol and conduct a formal security analysis on our protocol. Compared with other ECPAKA protocol, our protocol meets all basic security properties and is the first ECPAKA protocol with formal security proof for wireless communication. We also explore the suitability of the novel protocol for 3GPP2 specifications and improve the A-Key (Authentication Key) distribution for current mobile cellular systems.

1. Introduction

Confidentiality and authentication are two fundamental security goals for the wireless mobile networks. Authenticated key agreement (AKA) protocols can be used to achieve these security goals. Many AKA protocols have been proposed (e.g., [1–7]). Unfortunately, most of these existing AKA protocols are not suitable for the wireless mobile communications due to the constraints on power consumption, bandwidth and storage in mobile devices.

In 1985, Koblitz and Miller [8,9] independently proposed the public-key cryptosystem-elliptic curve cryptography (ECC). One of the most important features of ECC is the great strength-per-key-bit and the small parameters. For example, the 160 bits key-length of ECC has almost the same levelity as the 1024 bits key-length of RSA [10,11]. Therefore, cryptographic schemes based on ECC are suitable for environments where processing power, storage space, bandwidth, or power consumption is constrained, hence have gained more and more attention in the deployment of smart cards in mobile applications.

The first authentication and key agreement protocol for wireless communication based on ECC was introduced by Miller et al. in 1998 [9]. Although it provides identity authentication, key validation and user anonymity, it is PKI-based (Public-Key Infrastructure) and thus needs the user devices (with limited power) to process the certificates. In 2005, Sui et al. [12] proposed an Elliptic Curve password-based authenticated key agreement (ECPAKA) protocol based on the password-based authenticated key agreement algorithm (PAKA) proposed by Seo and Sweeney [13]. Their scheme is applicable to securing wireless mobile communications due to its low computation overhead. However, Sui et al.'s protocol cannot resist the off-line password guessing attack [14]. To remedy the security flaw, Lu et al. proposed an enhanced authenticated key agreement protocol for wireless mobile communications. Unfortunately, Pu pointed out that Lu et al.'s scheme still cannot resist

☆ Reviews processed and proposed for publication to Editor-in-Chief by Associate Editor Dr. Glaucio H.S. Carvalho.
* Corresponding author.
E-mail address: hguo.xyz@163.com (H. Guo).

0045-7906/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2011.10.015

against the off-line password guessing attack [15]. Later, Lo et al. [16] proposed an password-based authenticated key agreement protocol using elliptic curve cryptography (ECC), included their protocol in 3GPP2 specifications and claimed their scheme could withstand various attacks. Recently, He pointed out that Lo et al.'s protocol cannot resist the off-line password guessing attack, and proposed an efficient countermeasure to overcome the weakness [17]. However, none of the above protocols provide a formal security analysis.

In this paper, we present a novel authenticated key agreement protocol for wireless communications. To give a sound proof of our new scheme, we introduce a new assumption which is called *w*-Elliptic Curve Decisional Diffie-Hellman (*w*-ECDDH) assumption. We firstly show that the hardness of the new assumption is weaker than that of the known Elliptic Curve Decisional Diffie-Hellman (ECDDH) assumption. Under this new assumption of *w*-ECDDH, we prove the security of our scheme in the random oracle model. We also analyze other security requirements. Compared with other ECPAKA protocol, our protocol meets all basic security properties and is the first ECPAKA protocol with formal security proof for wireless communication. As a practical application, we include our protocol in 3GPP2 specifications to improve A-Key distribution for current mobile cellular systems.

The rest of this paper is arranged as follows. In Section 2, we introduce some notations, the basic security properties and the security model. In Section 3, we present a novel authenticated key agreement protocol and give a formal security analysis, and show that our protocol meets all security requirements. In Section 4, we compare our new ECPAKA protocol with other ECPAKA protocols from security properties and formal security proof. In Section 5, we consider including our protocol in 3GPP2 specifications. We conclude this paper in Section 6.

2. Notation and basic knowledge

In this section we introduce some notations and the relevant knowledge on security assumption and security models.

2.1. Notation

We provide the following notations that will be used in our paper.

- Alice (A), Bob (B): two communication users.
- $\mathbb{E}$: an elliptic curve defined over a finite field $\mathbb{F}_q$ with large group order.
- n: a secure large prime.
- $\mathbb{G}$: an additional cyclic group of the order n.
- P,Q: two points in $\mathbb{G}$ with large order n.
- $\mathcal{D}$: a uniformly distributed dictionary of size $|\mathcal{D}|$.
- S: a low-entropy password shared between Alice and Bob, which is randomly chosen from $\mathcal{D}$.
- t: the value t is derived from the password S in a predetermined way, which is uniformly distributed in $\mathbb{Z}_n^*$.
- a $\in_R S$: choose a randomly from set S.
- H_1: a secure one-way hash function.
- H_2:$\{0,1\}^* \to \{0,1\}^n$, a key derivation function ($n \geqslant 128$).

2.2. Security assumptions

Now we introduce some security assumptions.

Definition 1. (ECDLP) Given a point $Q = xP$, where $0 \leqslant x \leqslant n-1$, it is hard to determine such an x.

Definition 2. (ECCDH) Given random (P,aP,bP), for $0 \leqslant a,b \leqslant n-1$, it is hard to compute abP.

Definition 3. (ECDDH) For $a, b \in_R \mathbb{Z}_q^*$ and $R \in_R \mathbb{G}$, differentiating (P, aP, bP, abP) and (P, aP, bP, R) is hard.

We introduce a variant of ECDDH assumption, *w*-ECDDH assumption, which is weaker than ECDDH:

Definition 4. (*w*-ECDDH) For $a \in_R \mathbb{Z}_q^*$ and $R \in_R \mathbb{G}$, differentiating (P,a^2P,a^3P) and (P,a^2P,R) is hard.

We call this variant of ECDDH assumption as *w*-ECDDH assumption, since ECDDH assumption implies *w*-ECDDH assumption.

Theorem 1. *If there exists a polynomial time algorithm to solve w-ECDDH problem with non-negligible probability, then there exists a polynomial time algorithm for ECDDH problem with non-negligible probability.*

Proof. If there is a polynomial time algorithm $\mathcal{A}$ to solve the *w*-ECDDH problem, we construct a polynomial time algorithm $\mathcal{B}$ to solve the ECDDH problem.