Journal of Computer and System Sciences 83 (2017) 73–83

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

A new universal designated verifier transitive signature scheme for big graph data

Chao Lin [a,b], Wei Wu [a,b,*], Xinyi Huang [a,c], Li Xu [a]

[a] *Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian, 350000, China*
[b] *Nanjing University of Information Science and Technology, Nanjing, Jiangsu, 210044, China*
[c] *Fujian Beidou Forest Technology Co. Ltd., China*

ARTICLE INFO

Article history:
Received 10 October 2015
Received in revised form 3 March 2016
Accepted 9 June 2016
Available online 14 July 2016

Keywords:
Universal designated verifier signatures
Transitive Signatures RSA
Privacy
Authenticity

ABSTRACT

We propose a new design of universal designated verifier transitive signatures, to authenticate dynamically growing big graph data. The scheme is built on the classical RSA signature and possesses several desirable properties. It supports edge-signature composition as transitive signatures, i.e., with the signatures of two adjacent edges (i, j) and (j, k), one can obtain a valid signature of the edge (i, k). Additionally, a signature holder can convince only one designated verifier about the existence of an edge. Our design can efficiently achieve a tradeoff between data authenticity (when publishing dynamically growing big graph data) and data privacy (when disseminating big graph data).

1. Introduction

As mentioned in [1], “Among all areas in big data, security is one of the most important issues that takes precedence over the others.” As a case study, we investigate the authenticity of a big graph data system formed by a set of administrative domains, i.e., big data represented by (undirected) graphs. The vertices in the graph represent computers, and two vertices are within the same administrative domain if and only if the edge (i, j) exists. As one can see, if i and j are in a domain $\mathcal{D}$, and j and k are in a domain $\mathcal{D}$, then i and k are in the same domain $\mathcal{D}$. In other words, equivalence relations in such systems are transitive.

There are several methods that can ensure the authenticity of the aforementioned big graph data. By viewing the big data system as a single piece of data, one can protect the data authenticity by digitally signing all vertices and edges in the graph. While it works, signing the data as a whole message does not take the advantage of data structure. By taking into account the “transitive” feature of graph data, one can sign the transitive reduction of the graph, the minimum subset of edges with the same transitive closure as the whole graph. This greatly reduces the signing complexity but would leak the privacy information of a path between two vertices: One must present two signatures of edges (i, j) and (j, k) to prove that the edge (i, k) exists in the whole graph. Transitive signatures [2], the earliest instance of homomorphic signatures, can solve this issue in an efficient way. With transitive signatures, the data owner only needs to sign the edges of transitive reduction, which greatly reduces the signature size. A distinctive feature of transitive signature is that with transitive signatures on edges (i, j) and (j, k), one can obtain a signature of the edge (i, k) without any interaction with the signer. In other words,

[*] Corresponding author.
E-mail address: weiwu81@gmail.com (W. Wu).

http://dx.doi.org/10.1016/j.jcss.2016.06.003
0022-0000/© 2016 Elsevier Inc. All rights reserved.

transitive signatures support public edge composition. This helps to protect the path privacy between edges. Furthermore, newly added vertices and edges only incur a minimum number of operations on the transitive reduction of the graph.

Hou et al. [3] proposed the notion of Universal Designated Verifier Transitive Signatures and the first design. In addition to edge composition, a UDVTS scheme allows a signature holder (say, Alice) of a transitive signature to prove to a designated verifier (say, Bob) that such a signature exists, but Bob is not able to let anyone else believe this fact. Hou et al.'s UDVTS scheme in [3] was constructed in bilinear group and makes the use of bilinear mapping. It is naturally to ask whether we can extend classical signature schemes (e.g., under RSA and other well studied complexity assumptions) into UDVTS. In this paper, we integrate Bellare et al.'s [4] RSATS-2 scheme and Steinfeld et al.'s [5] RSAUDVS scheme to obtain a RSA-based Universal Designated Verifier Transitive Signature (RSAUDVTS) scheme. In our design, we use the existing key generation and signing implementation infrastructure of RSA to construct RSAUDVTS. Differently from the one-way and collision-resistant hash function in [3], the holder of a transitive signature in our scheme computes a zero-knowledge proof of knowledge of the transitive signature to produce a designated verifier signature, where a trapdoor hash function is used. The designated verifier can use his/her private key to produce the universal designated verifier signatures, and as a result he cannot convince anyone else about the validity of the transitive signature. We further prove that our scheme satisfies unforgeability and privacy protection.

Organization. The remainder of our paper is organized as follows. Section 2 reviews the related works. We present some preliminaries required by this paper in Section 3. Formal definitions and security models of UDVTS are given in Section 4. In Section 5, we describe our RSAUDVTS scheme and its security/performance analysis. We conclude this paper in Section 6.

2. Related work

This section is devoted to the review on related work.

2.1. Transitive signatures

Transitive signatures for undirected graph. In 2002, Micali and Rivest [2] introduced the notion of transitive signatures, a useful tool to build an authenticated and dynamically growing graph. As an example, an undirected graph can represent a set of administrative domains. The vertices represent computers and an edge (i, j) means that i and j are in the same administrative domain. It is obvious that if i and j are in the same administrative domain, and if j and k are in the same administrative domain, then i and k belong to the same administrative domain. Thus, transitive undirected graphs represent equivalence relations. When the signature object is a transitive graph, transitive signatures provide the advantage of reducing the amount of edge signatures and computational complexity. There are two schemes proposed in [2]. The first scheme is transitively unforgeable against adaptive chosen message attacks under the discrete logarithm assumption. Here, "*transitively unforgeable*" means even if an adversary can adaptively request the legitimate transitive signatures of graph G, he cannot forge the signature of any new vertex or other edge outside the transitive closure of G in polynomial-time. The second scheme is built from RSA assumption and merely transitively unforgeable under non-adaptive chosen message attacks.

Shortly after the introduction of transitive signatures in [2], Bellare and Neven [4] enlarged the set of assumptions that transitive signatures can be based on and improved the existing schemes. Several new schemes are proposed, based on the factoring problem, the one-more discrete logarithm problem, and the gap Diffie–Hellman groups in [4]. Additionally, they answered the open question raised in [2] and proved that the RSA-based scheme in [2] is transitively unforgeable under adaptive chosen-message attacks assuming the one-more RSA-inversion problem is hard. Another contribution of [2] is hash-based modifications of their proposed schemes to eliminate the need of node certificates. But these schemes are provably secure only in the random oracle model.

Shahandashti et al. [6] presented a transitive signature scheme from bilinear pairing. The security requirement of the underlying standard signature schemes is relaxed from secure under chosen message attacks to known message attacks. The scheme they proposed is proven transitively unforgeable under adaptive chosen message attacks, assuming the hardness of the computational co-Diffie–Hellman problem in bilinear group pairs.

Ma et al. [7] introduced a new method to transform stateful transitive signature schemes, i.e., the signing algorithm must maintain the state information for each queried node of graph, to the stateless ones without loss of security. Their approach is different from the stateless schemes proposed by Bellare and Neven in [4]. According to the proposed method, they presented stateless transitive signature schemes based on the hardness of Factoring and RSA problems. In the random oracle model, the modified schemes are secure against adaptive chosen-message attacks. Gong et al. [8] constructed a transitive signature scheme from Linear Feedback Sequence Register (LFSR), whose security can be reduced to the discrete logarithm assumption in the standard model. They compared the performance amongst LFSR-TS and other schemes. The result shows that LFSR-TS is more effective in "Edge Signing" and "Edge Composition".

As mentioned in [9], it is standard practice in cryptography to seek new and alternative realizations of primitives of potential interest. In order to accomplish these objectives, Wang et al. [10] presented the first construction of transitive signatures in braid groups. In the random oracle model, their design is transitively unforgeable against adaptively chosen message attacks under the assumption of one-more matching conjugate problem defined in [11]. Compared to the traditional