Available online at www.sciencedirect.com

ScienceDirect

Information Processing Letters 107 (2008) 83–86

Information Processing Letters

www.elsevier.com/locate/ipl

Rogue-key attacks on the multi-designated verifiers signature scheme

Kyung-Ah Shim

Department of Mathematics, Ewha Womans University, 11-1 Daehyun-dong, Seodaemun-gu, Seoul 120-750, Republic of Korea

Received 6 July 2007; received in revised form 27 November 2007; accepted 30 November 2007

Available online 7 February 2008

Communicated by D. Pointcheval

Abstract

In 1996, Jakobsson, Sako, and Impagliazzo and, on the other hand, Chaum introduced the notion of designated verifier signatures to solve some of the intrinsic problems of undeniable signatures. The generalization of this concept was formally investigated by Laguillaumie and Vergnaud as multi-designated verifiers signatures. Recently, Laguillaumie and Vergnaud proposed the first multi-designated verifiers signature scheme which protects the anonymity of signers without encryption. In this paper, we show that their scheme is insecure against rogue-key attacks.

Keywords: Cryptography; Digital signature; Multi-designated verifiers signature; Bilinear pairing; Rogue-key attack

1. Introduction

Designated verifier proofs, proposed in 1996 by Jakobsson et al. [7] and Chaum [3], were introduced to solve some of the problems inherent to undeniable signatures. These proofs can be converted into designated verifier signatures via the Fiat and Shamir heuristic [5]. Desmedt [4] extended these signatures to a multi-user setting. This new primitive was formally investigated by Laguillaumie and Vergnaud [9], as multi-designated verifiers signatures, where a generic multi-designated verifiers signature scheme based on discrete-log ring signatures was proposed. Jakobsson et al. [7] also suggested that designated verifier signatures should provide an additional notion of privacy: given such a signature and two potential signing public keys, it should be computationally infeasible for an eavesdropper to determine under which of the two corresponding secret keys the signature was performed. This property has been formalized in [10] and naturally extended to the multi-user setting in [9], where a bi-designated verifiers signature scheme was also proposed which takes advantage of Joux's non-interactive tripartite key exchange [8] to achieve this property. However, the generic scheme from [9] did not catch the notion of privacy of signer's identity without an additional encryption layer. Recently, Laguillaumie and Vergnaud [11] proposed the first multi-designated verifiers signature scheme which protects the anonymity of signers without encryption, which is based on Boneh et al.'s ring signatures [2]. In this paper, we show that their scheme is insecure against rogue-key attacks.

The rest of the paper is organized as follows. In Section 2, we review the Laguillaumie–Vergnaud multi-

E-mail address: kashim@ewha.ac.kr.

0020-0190/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.ipl.2007.11.021

designated verifiers signature scheme. In Section 3, we show that the scheme is insecure against rogue-key attacks. Concluding remarks are given in Section 4.

2. Review of the Laguillaumie–Vergnaud multi-designated verifiers signature scheme

In this section, we review the Laguillaumie–Vergnaud multi-designated verifiers signature (MDVS) scheme from bilinear pairings [11] and the security notion for MDVS schemes [9].

2.1. The Laguillaumie–Vergnaud multi-designated verifiers signature scheme

Let $k \in \mathbb{Z}$ be a security parameter. We denote by A the signer and by B_i a designated verifier. The scheme is illustrated as follows:

The multi-designated verifiers signature scheme: SMDVS

- **Setup:** Let $\mathtt{Gen}$ be a prime-order-BDH-parameter-generator and $(q, P, \mathbb{G}, \mathbb{H}, e)$ be the output of $\mathtt{Gen}(k)$ satisfying the following conditions: a prime number q with $2^{k-1} \leqslant q \leqslant 2^k$, $\mathbb{G}$ and $\mathbb{H}$ are groups of order q, P generates $\mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{H}$ is an admissible bilinear pairing. Let $[\{0,1\}^* \times \mathbb{G}^{n+2} \to \mathbb{G}]$ be a hash function family, and H be its random member.
- **SKeyGen:** It randomly picks an integer $a \in [1, q-1]$ which is the secret key of the signer A. Its public key is $P_A = aP$.
- **VKeyGen:** It randomly picks an integer $b_i \in [1, q-1]$ which is the secret key of the verifier B_i. It's public key is $P_{B_i} = b_i P$.
- **Sign:** Given a message $m \in \{0,1\}^*$, A computes the key $P_B = P_{B_1} + \cdots + P_{B_n}$, chooses a random number $r \in [1, q-1]$ and computes $Y_{B_i} = rP_{B_i}$ for all $i = 1, \ldots, n$ and $Y = rP$. Next, A computes $M = H(m, P_A, P_{B_1}, \ldots, P_{B_n}, Y)$, chooses a random number $r' \in [1, q-1]$ and computes

  $$Q_A = a^{-1}(M - r'P_B), \qquad Q_B = r'P.$$

  The $(n+2)$-tuple $\sigma = (Q_A, Q_B, Y_{B_1}, \ldots, Y_{B_n})$ is a multi-designated verifiers signature.
- **Verify:** Given a message $m \in \{0,1\}^*$ and a signature $\sigma = (Q_A, Q_B, Y_{B_1}, \ldots, Y_{B_n})$, each B_i ($i = 1, \ldots, n$) retrieves $Y = rP$ by computing $b_i^{-1} Y_{B_i}$. Then B_i verifies, for $j = 1, \ldots, n$ and $j \neq i$, that $e(P_{B_j}, rP) = e(Y_{B_j}, P)$. If they hold, B_i computes $M = H(m, P_A, P_{B_1}, \ldots, P_{B_n}, Y)$ and checks whether

  $$e(M, P) = e(Q_A,\ P_A) \cdot e(Q_B,\ P_B)$$

  holds or not. If it holds, the signature is accepted.

2.2. Unforgeability of multi-designated verifiers signature schemes

Let $B = \{B_1, \ldots, B_n\}$ be a group of n entities (the designated verifiers), k be an integer and $\mathtt{MDVS}$ be a n-designated verifiers signature scheme with security parameter k. For digital signature schemes, the strongest security notion was defined by Goldwasser, Micali and Rivest in [6] as an existential forgery against an adaptively chosen message attack ($\mathtt{EF\text{-}CMA}$). In the MDVS setting, an $\mathtt{EF\text{-}CMA}$-adversary $\mathcal{A}$ is given the n public keys of B_i as well as access to the random oracle $\mathcal{H}$ and to the signing oracle Σ. As $\mathcal{A}$ cannot verify a signature by himself, one may give him access to a verifying oracle to check the validity of signatures, as for single designated verifier signature schemes [14]. On the other hand, the attacker is allowed to corrupt up to $(n-1)$ designated verifiers (and to do so adaptively), i.e., he can access to a corrupting oracle Ξ to obtain the secret information of the corresponding corrupted verifier. Therefore, he is able to verify a signature by himself, and one can omit the verifying oracle. Also, $\mathcal{A}$ is allowed to query the signing oracle on the challenge message m but is supposed to output a signature of the message m not given by Σ.

Security against existential forgery. Let B be n entities, k and t be integers and ε be a real in $[0,1]$, let $\mathtt{MDVS}$ be an n-designated verifiers signature scheme with security parameter k. Let $\mathcal{A}$ be an $\mathtt{EF\text{-}CMA}$-adversary against $\mathtt{MDVS}$. We consider the following random experiment:

```
Experiment: $Exp^{\mathtt{ef\text{-}cma}}_{\mathtt{MDVS},\mathcal{A}}(k)$
$params \leftarrow \mathtt{MDVS}.Setup(k)$
For $i = 1, \ldots, n$ do
  $(pk_{B_i}, sk_{B_i}) \leftarrow_R \mathtt{MDVS}.VKeyGen(params, B_i)$
  $(pk_A, sk_A) \leftarrow_R \mathtt{MDVS}.SKeyGen(params, A)$
  $(m, \sigma) \leftarrow \mathcal{A}^{\mathcal{H},\Sigma,\Xi}(params, pk_{B_1}, \ldots, pk_{B_n}, pk_A)$
  Return $\bigvee_{i=1}^{n} \mathtt{MDVS}.Verify(params, m, \sigma, pk_A, sk_{B_i})$.
```

We define the success of the adversary $\mathcal{A}$, via $\mathbf{Succ}^{\mathtt{ef\text{-}cma}}_{\mathtt{MDVS},\mathcal{A}}(k) = \Pr[\mathbf{Exp}^{\mathtt{ef\text{-}cma}}_{\mathtt{MDVS},\mathcal{A}}(k)] = 1$. $\mathtt{MDVS}$ is said to be (k, t, ε)-$\mathtt{EF\text{-}CMA}$ secure, if no adversary $\mathcal{A}$ running in time t has a success $\mathbf{Succ}^{\mathtt{ef\text{-}cma}}_{\mathtt{MDVS},\mathcal{A}}(k) \geqslant \varepsilon$.