Identity-Based Strong Multi-Designated Verifiers Signatures

Sherman S.M. Chow

Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu

Abstract. Designated verifier signatures are privacy-oriented signatures that provide message authenticity only to a specified verifier but nobody else. We consider strong multi-designated verifiers such that knowledge of either one of designated verifiers' private keys is required to verify the signature. We propose the first identity-based construction.

1 Introduction

Designated verifier signatures (DVS), introduced by Chaum and Jakobsson *et al.* [5] independently, convince only a specific verifier about the validity of the signature. Like other privacy-oriented signatures scheme (e.g. undeniable signature, ring signature), the "loss" of the non-repudiation property of traditional signature makes it useful in various commercial cryptographic applications.

Application. We briefly talk about one of its applications. Suppose an organization initiates a call for tenders, asking some companies to propose their own prices for offering certain goods or services. The organization wants authenticity of the tender such that the selected company cannot later repudiate what they agreed to after. They can sign on the tender using traditional scheme, but such signature can be subsequently shown to others (e.g. by the tender-caller) such that other competing parties can prepare a "tailor-made" tender accordingly.

Working Principle. The working mechanism of DVS is that it consists of a proof showing either "the signer has signed on a message" or "the signer has the verifier's secret key" is true. The designated verifier, being confident that his/her private key is kept in secret, get convinced that the signer has signed on a message. No other third party can be convinced by this signature since the designated verifier can always generate such proof with his/her private key.

Strong and Multiple. Yet, this level of *signer ambiguity* (or source-hiding property) is not enough in scenario where one can certain that the verifier has not generated such proof. Consider when the signature is captured before reaching the verifier, the eavesdropper knows who the real signer is as there are only two possibilities. To address this problem, we need a *strong* DVS (termed in [5] and

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 257–259, 2006.

formalized in [7]) such that the verifier needs to use his/her private key to verify the signature. This property is referred as *signer's privacy*, such that given a DVS and two potential signing public keys, it is computationally infeasible to determine under which of the two corresponding signing key is used.

At CRYPTO 03's rump session, Desmedt [3] asked for a multi-designated verifiers signature scheme such that there are more than one designated verifier. Such scheme can help in multi-party activities like distributed contract signing.

Related Work. A generic MDVS construction, from any discrete logarithm based ring signature (e.g. [2]) and any secure multi-party computation protocol, was proposed in [6]. The authors suggested the use of an additional layer of encryption that is indistinguishable under adaptive chosen-ciphertext-attack (CCA2) to remedy the weaker notion of signer privacy. By exploiting the bilinearity of pairings on elliptic curve, strong 2DVS was proposed in the same paper. Generic construction of identity-based (ID-based) scheme was proposed in [8], followed by a recent proposal of strong DVS schemes with short signature length (both PKI-based and ID-based) [4]. These schemes satisfy the strong notion of signer privacy, but only single designated verifier is considered.

Our Contribution. This paper proposes a strong multi-designated verifies signature scheme (SM-DVS). Under traditional public key infrastructure, signer can generate SM-DVS only after *all* of the designated verifiers have obtained the certification. Motivated by the above problem, we consider ID-based keys (for both signer and verifiers), i.e. the public key is derived from a string denoting the identity of the user and there exists a trusted key generation centre (KGC) who generates the corresponding private keys on request.

2 Strong Multi-designated Verifier Signatures (SM-DVS)

Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \cdot)$ be two cyclic groups of prime order q. The bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a map that $\forall P, Q, R \in \mathbb{G}_1$, $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$, and $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$; and $\exists P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1$.

`Setup`: The KGC randomly chooses $s \in_R \mathbb{Z}_q^*$ as the master secret. System parameter is $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub} = sP, Q, H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1, H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*\}$.

`Extract`: The user with identity $ID \in \{0,1\}^*$ submits ID to the KGC. The user's public key Q_{ID} is equal to $H_1(ID) \in \mathbb{G}$, The KGC computes the user's private key S_{ID} by $S_{ID} = sQ_{ID}$, where $s \in \mathbb{Z}_q^*$ is the master secret.

`Sign`: Let $L = \{ID_S, ID_{V_1}, \cdots, ID_{V_n}\}$ be the set of all identities of these $n + 1$ parties. For the signer ID_S to sign on the message m that can be verified by the group of n verifiers $\{ID_{V_i}\}$, he follows the steps below.

1. Computes $P_V = \sum_{i=1}^{n} \{H_1(ID_{V_i})\}$.
2. Randomly choose l from $\mathbb{Z}_q^*$, computes $Y = lP$ and $k = \hat{e}(lQ, P_{pub})$.
3. For $i \in \{1, 2, \cdots, n\}$, computes $Z_i = lH_1(ID_{V_i}) + lQ$.
4. Randomly chooses $U_2 \in \mathbb{G}_1$ and computes $h_2 = H_2(m||L||U_2||k)$.

5. Chooses $r'_1 \in_R \mathbb{Z}_q^*$, computes $U_1 = r'_1 H_1(ID_S) - U_2 - h_2 P_V$.
6. Computes $h_1 = H_2(m||L||U_1||k)$ and $V = (h_1 + r'_1)S_{ID_S}$.
7. Outputs the signature $\sigma = \{U_1, U_2, V, Y, Z_1, Z_2, \cdots, Z_n\}$.

`Verify`: The verifier ID_{V_i} performs the following steps to verify a SM-DVS.

1. Computes $P_V = \sum_{i=1}^{n} \{H_1(ID_{V_i})\}$ and $k' = \hat{e}(P_{pub}, Z_i)/\hat{e}(Y, S_{ID_{V_i}})$.
2. Computes $h_1 = H_2(m||L||U_1||k')$ and $h_2 = H_2(m||L||U_2||k')$.
3. Return $\top$ if $\hat{e}(P_{pub}, U_1 + h_1 H_1(ID_S) + U_2 + h_2 P_V) = \hat{e}(P, V)$, $\perp$ otherwise.

Efficiency. Only a constant number of pairings are required (sign:1, verify:4).

Security. The security model is basically the same as that in [6], with additional private key extraction query capturing the insider security of ID-based system and a natural extension from 2 verifiers to n verifiers. The scheme's unforgeability and signer ambiguity are directly related to the 1-out-of-n-groups ID-based ring signature in [2]. The signer-privacy can be proven using the idea of the proof of the multi-recipient ID-based encryption scheme against chosen-plaintext-attack (CPA) in [1], and that of the ID-based strong-DVS scheme in [4], yet the signing query of the challenge message can be supported. Thanks to the random oracle model and the bilinear pairing, we do not need decryption oracle from CCA2 security to answer verification queries. CPA security is sufficient since verification can be done by checking whether there exists an input-output tuple in the random oracle simulation satisfy some correct relationship among the signature's components by using pairing.

References

1. Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption. *Public Key Cryptography - PKC 2005*, *LNCS* 3386, pp. 380–397, 2005.
2. Sherman S.M. Chow, S.M. Yiu, and Lucas C.K. Hui. Efficient Identity Based Ring Signature . *Applied Cryptography and Network Security, ACNS 2005*, *LNCS* 3531, pp. 499–512. Also available at Cryptology ePrint Archive, Report 2004/327.
3. Yvo Desmedt. Verifier-designated Signatures. Available at http://www.cs.fsu.edu/∼desmedt/lectures/verifier-designated-signatures.pdf.
4. Xinyi Huang, Willy Susilo, Yi Mu, and Futai Zhang. Short (Identity-Based) Strong Designated Verifier Signature Schemes. *Information Security Practice and Experience, ISPEC 2006*, *LNCS* 3903, pp. 214–225.
5. Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated Verifier Proofs and Their Applications. *EUROCRYPT '96*, *LNCS* 1070, pp. 143–154.
6. Fabien Laguillaumie and Damien Vergnaud. Multi-designated Verifiers Signatures. *Information and Communications Security, ICICS 2004*, *LNCS* 3269, pp. 495–507.
7. Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch. An Efficient Strong Designated Verifier Signature Scheme. *Information Security and Cryptology - ICISC 2003*, *LNCS* 2971, pp. 40–54.
8. Yi Mu Willy Susilo, Fangguo Zhang. Identity-Based Strong Designated Verifier Signature Schemes. In *Australasian Conference on Information Security and Privacy, ACISP 2004*, volume 3108 of *LNCS* 3108, pp. 313–324.