Conditionally Verifiable Signature
(Extended Abstract)

Ian F. Blake[1] and Aldar C-F. Chan[2]

[1] Department of Electrical and Computer Engineering, University of Toronto
Toronto, Ontario M5S 2G5, Canada
[2] INRIA Rhône-Alpes, Inovallée, 38330 Montbonnot Saint Ismier, France

Abstract. We introduce a new digital signature model, called conditionally verifiable signature (CVS), which allows a signer to specify and convince a recipient under what conditions his signature would become valid and verifiable; the resulting signature is not publicly verifiable immediately but can be converted back into an ordinary one (verifiable by anyone) after the recipient has obtained proofs, in the form of signatures/endorsements from a number of third party witnesses, that all the specified conditions have been fulfilled. A fairly wide set of conditions could be specified in CVS. The only job of the witnesses is to certify the fulfillment of a condition and none of them need to be actively involved in the actual signature conversion, thus protecting user privacy. It is guaranteed that the recipient cannot cheat as long as at least one of the specified witnesses does not collude. We formalize the concept of CVS and give a generic CVS construction based on any CPA-secure identity based encryption (IBE) scheme. Theoretically, we show that the existence of IBE with indistinguishability under a chosen plaintext attack (a weaker notion than the standard one) is necessary and sufficient for the construction of a secure CVS.[1]

1 Introduction

Balancing between the accountability and privacy of a signer is an important but largely unanswered issue of digital signatures. A digital signature scheme usually consists of two parties, a signer and a recipient, with the former giving his signature on a message/document to the latter as his commitment or endorsement on the message. To ensure that the signer is held accountable for his commitment, his signature needs to be publicly verifiable. However, public verifiability of a digital signature would put the signer's privacy at risk as a digital signature could be replicated and spread so easily, compared to its handwritten counterpart. More importantly, if the message presents valuable information about the signer, then the signed message itself is a certified piece of that information. Hence, the interests of the signer and the recipient are in conflict.

Of course, ensuring signer privacy and accountability simultaneously seems to be impossible. However, we observe that, in most of the real world scenarios, this conflict could be solved if the signer can ensure non-verifiability of his signature before certain

[1] Due to page limit, some proofs are omitted here but could be found in the full version [7].

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 206–220, 2006.

conditions are fulfilled but still be able to convince the recipient that he will be obligated to exercise his commitment; in other words, he needs to give the recipient some guarantee that his commitment or his signature will become effective or publicly verifiable once all the conditions are fulfilled.

To provide a flexible solution to this problem of controllably passing signatures from one party to another without actively involving a trusted third party (i.e. the third party does not have to see or know the signer's message), we introduce a new signature concept called conditionally verifiable signature (CVS). In the CVS model, a signer is allowed to embed a set of verifiability conditions C into his ordinary signature σ to create a partial signature δ that is solely verifiable by the recipient, who cannot immediately convince others of the validity of δ (as δ is no more convincing than any random number and hence nobody can link it to its alleged signer) but can convert it back to the universally verifiable one σ (i.e. verifiable by everyone) after obtaining from a number of witnesses (appointed by the signer) the proofs that all the specified verifiability conditions have been fulfilled.[2] These proofs are in the form of signatures on condition statements, signed by the witnesses, about how the specified conditions are considered as fulfilled. In order to convince the recipient to accept a given partial signature δ on a message M (whose validity could not be verified), the signer runs a proof/confirmation protocol, which could be interactive or non-interactive, with the recipient to convince the latter that δ is indeed his partial signature on M, from which the corresponding ordinary signature could be recovered using the specified witnesses' signatures on the specified verifiability condition statements in C.

Given that $\mathcal{W}$ is the set of all possible witnesses, an instance set of verifiability conditions C is of the form $\{(c_i, W_i) : c_i \in \{0,1\}^*, W_i \in \mathcal{W}\}$ where each condition statement c_i is a string of arbitrary length describing a condition to be fulfilled. Examples of c_i include "A reservation has been made for Alice on flight CX829, 5 Sept 2006.", "A parcel of XXX has been received for delivery to Bob." and so on. The recipient needs to request each one of the specified witnesses, say W_i, to verify whether the condition stated in c_i is fulfilled and in case it is, to sign on c_i to give him a witness signature σ_i. These witness signatures σ_i's would allow the recipient to recover the publicly verifiable, ordinary signature σ from the partial signature δ. It is not necessary for a recipient to present δ or the message M to the witnesses in order to get these σ_i's. The only trust we place on the witnesses is that they only give out their signatures on a condition statement when the specified conditions are indeed fulfilled. In fact, it is not difficult to imagine that the existence of such witnesses is abundant in any business transaction. In addition, we could achieve a fairly high level of privacy in that the witnesses are unaware of the message or the partial signature when verifying the fulfillment of a given condition, namely, he does not learn the deal between the signer and the recipient.

We could view the partial signature as a blinded version of the ordinary signature, that is, nobody could verify its validity. We formulate this non-verifiability property by the notion of *simulatability* in this paper, that is, anyone could use just public information of the signer to simulate a given partial signature while others cannot judge whether

[2] Throughout the rest of this paper, we will denote the ordinary (universally verifiable) signature and the CVS partial signature by σ and δ respectively, unless otherwise specified.