Perfect Concurrent Signature Schemes

Willy Susilo\textsuperscript{1}, Yi Mu\textsuperscript{1}, and Fangguo Zhang\textsuperscript{2}

\textsuperscript{1} School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia
\{wsusilo,ymu\}@uow.edu.au

\textsuperscript{2} Department of Electronics and Communication Engineering
Sun Yat-Sen University
Guangzhou 510275, P.R. China
isdzhfg@zsu.edu.cn

Abstract. The notion of concurrent signatures was recently introduced by Chen, Kudla and Paterson in their seminal paper in [5]. In concurrent signature schemes, two entities can produce two signatures that are not binding, until an extra piece of information (namely the keystone) is released by one of the parties. Upon release of the keystone, both signatures become binding to their true signers concurrently. In this paper, we extend this notion by introducing a new and stronger notion called \textit{perfect} concurrent signatures. We require that although both signers are known to be trustworthy, the two signatures are still ambiguous to any third party (c.f. [5]). We provide two secure schemes to realize the new notion based on Schnorr’s signature schemes and bilinear pairing. These two constructions are essentially the same. However, as we shall show in this paper, the scheme based on bilinear pairing is more efficient than the one that is based on Schnorr’s signature scheme.

1 Introduction

Consider a situation where Alice would like to purchase a laptop from Bob. Alice signs a payment instruction to pay Bob the price of the laptop, and Bob agrees by signing a statement that he authorizes her to pick the laptop up from the shop. We need to achieve a situation where both Alice’s and Bob’s signatures are binding at the same time. In this particular scenario, the signature will be binding when Alice picks up her laptop from the shop. Alice’s payment instruction will be binding, and Bob’s signature (or the receipt) will also be binding to allow Alice to pick up her laptop. This is a typical application where concurrent signatures are applicable, as introduced in their seminal paper in [5]. The signature from both parties will be simultaneously binding after the so-called “keystone” is released by one of the party involved.

In [5], Chen, Kudla and Paterson presented a concrete concurrent signature scheme based on a variant of Schnorr based ring signature scheme [1]. In their scheme, any third party cannot be convinced that a signature has indeed been
signed by one particular signer, since any signer can always generate this signature by himself/herself. However, we note that in a situation where Alice and Bob are known to be honest players, any third party can be sure that both signers have signed the messages even before the keystone is released. We will highlight this idea in Section 3. In this paper, we firstly extend this notion to perfect concurrent signature schemes, which will allow full ambiguity of the concurrent signatures, even both signers are known to be trustworthy.

Our Contribution
In this paper, we firstly introduce a stronger notion of concurrent signature schemes namely perfect concurrent signature schemes. We argue that this notion is extremely important, especially in the case where both signers are known to be trustworthy. We provide two concrete schemes to satisfy this model, and show their security proofs. Our first scheme is based on a variant of Schnorr ring signature scheme, and our second scheme is based on bilinear pairing. These two schemes are essentially the same. However, our second scheme is more efficient that the first one.

The rest of this paper is organized as follows. In the next section, we will review some of the previous and related works in this area. In section 3, we recall the notion of concurrent signatures introduced in [5], and analyze the concrete signature scheme proposed in the same paper. As we shall show in this section, if both parties are honest, then any third party can be sure who has issued the published signatures. We strengthen this notion by introducing perfect concurrent signatures in section 4. We provide a concrete perfect concurrent signature scheme based on Schnorr’s signature scheme in section 5 and based on bilinear pairing in section 6. Section 7 concludes this paper.

2 Related Work
Fair exchange in digital signatures has been considered as a fundamental problem in cryptography. Fairness in exchanging signatures is normally achieved with the help of a trusted third party (TTP) (which is often offline). There were some attempts where a fair exchange of signatures can be achieved with a “semi-trusted” TTP who can be called upon to handle disputes between signers [2]. This type of fair exchanges is also referred to as optimistic fair exchange. The well-known open problem in fair exchange is the requirement of a dispute resolving TTP whose role cannot be replaced by a normal certification authority.

In [8], the notion of ring signatures was formalized and an efficient scheme based on RSA was proposed. A ring signature scheme allows a signer who knows at least one secret information (or trapdoor information) to produce a sequence of \( n \) random permutation and form them into a ring. This signature can be used to convince any third party that one of the people in the group (who knows the trapdoor information) has authenticated the message on behalf of the group. The authentication provides signer ambiguity, in the sense that no one can identify who has actually signed the message. In [1], a method to construct