Time Capsule Signature: Efficient and Provably Secure Constructions*

Bessie C. Hu[1], Duncan S. Wong[1], Qiong Huang[2], Guomin Yang[1], and Xiaotie Deng[1]

[1] Department of Computer Science
City University of Hong Kong
Hong Kong, China
{bessiehu,duncan,csyanggm,deng}@cs.cityu.edu.hk
[2] csqhuang@cityu.edu.hk

Abstract. Time Capsule Signature, first formalized by Dodis and Yum in Financial Cryptography 2005, is a digital signature scheme which allows a signature to bear a (future) time t so that the signature will only be valid at time t or later, when a trusted third party called time server releases time-dependent information for checking the validity of a time capsule signature. Also, the actual signer of a time capsule signature has the privilege to make the signature valid *before* time t.

In this paper, we provide a new security model of time capsule signature such that time server is not required to be fully trusted. Moreover, we provide two efficient constructions in random oracle model and standard model. Our improved security model and proven secure constructions have the potential to build some new E-Commerce applications.

Keywords: Time Capsule Signature.

1 Introduction

Modern business is in nature the business for future. A contract signed now is a commitment for some future cooperation; a ticket bought now presents an entry permit at a specific time in the future; an option obtained now, in the derivative markets, ensures the privilege of buying/selling a stock at some time in the future. The success of these practices requires the integrity of credential releasers, and the involvement of an authority who can judge the rules for legal players. To realize these activities in E-Commerce platforms, a new primitive, which has a great promise to be a very useful tool, is called Time Capsule Signature [13].

A time capsule signature involves a signer (known as credential releaser), a verifier (known as credential receiver) and a time server (known as authority). The signer can issue a *future* signature indicated by some time information,

* The second author was supported by a grant from City University of Hong Kong (Project No. 7002001).

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 126–142, 2007.

say t, and enjoys the following properties: 1) The credential receiver can verify immediately that a signature will become valid at time t. 2) The signature will automatically become valid at time t, even without the cooperation of signer. 3) The legal signer has the privilege to make the signature valid before time t.

Property 1 and 2 are easy to comprehend in the current practice. However, in a naive solution of signing a statement that 'the message m will become valid from time t', the verifier is required to be aware of the current time [13]. When time is generalized to arbitrary events, this becomes even more problematic. Moreover, signer has lost control of the validation time t once the statement is produced. For the variety of E-Commerce, we do need to provide signers the power to validate their future signature before the committed time t. For example, in the case of debt repayment, a borrower can sign a check to indicate the repayment day (e.g. due day), he may also have the desire to repay his debt earlier, so to improve his credit history. Of course he can sign another check indicating the actual repayment time, but the original check should be handled carefully to avoid 'double spending'. Time capsule signature supports this desirable feature with a process of making a signature valid at any time by the actual signer known as *prehatch*, as opposed to *hatch* the signature at time t when some additional information is published by the time server. We refer readers to [13] for more discussions on the applications of time capsule signature. Property 3 may also be captured in a signed statement that 'the signature of message m will become valid from time t, or when the signer release some secret information'. Again, such a statement has problems when time is generalized to arbitrary events.

The notion of time capsule signature was first formalized by Dodis and Yum [13] in 2005. Besides the above three properties, they also require that prehatched signature should be indistinguishable from hatched signature. For practical use of time capsule signature as discussed above, the indistinguishability between prehatched signature and hatched signature is actually undesirable. Since the purpose of prehatching is to make a signature valid before time t, the verifier can simply compare the time t with the current time to identify if a signature is prehatched or normally hatched. Furthermore, in some scenarios, we actually need to distinguish a prehatched signature from a hatched signature. In the above debt repayment case, a prehatched signature has to be identified for credit history checking. On the other hand, under the property of indistinguishability, the time server has to be fully trusted, otherwise, there is no way to tell if a signature which becomes valid before time t is generated by the actual signer or a cheating time server.

Therefore, in this paper, we remove the requirement of indistinguishability for time capsule signature while retaining all other properties. This allows us to modify the security model for capturing attacks launched by a cheating time server. Our generic construction is based on a new primitive called identity-based trapdoor relation (IDTR). We propose two efficient implementations for the IDTR primitive, one is proven secure in the random oracle model, the other in the standard model.