# General Conversion for Obtaining Strongly Existentially Unforgeable Signatures

Isamu Teranishi[1,2], Takuro Oyama[2], and Wakaha Ogata[2]

[1] NEC Corporation
1753, Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, 211-8666, Japan
[2] Tokyo Institute of Technology
2-12-1 Ookayama, Meguro-ku Tokyo, 152-8550, Japan
teranisi@ah.jp.nec.com, taku-zy@crypt.ss.titech.ac.jp,
wakaha@mot.titech.ac.jp

**Abstract.** We say that a signature scheme is strongly existentially unforgeable if no adversary, given message/signature pairs adaptively, can generate a new signature on either a signature on a new message or a new signature on a previously signed message. Strongly existentially unforgeable signature schemes are used to construct many applications, such as an IND-CCA2 secure public-key encryption scheme and a group signature scheme.

We propose two general and efficient conversions, both of which transform a secure signature scheme to a strongly existentially unforgeable signature scheme. There is a tradeoff between the two conversions. The first conversion requires the random oracle, but the signature scheme transformed by the first conversion has shorter signature length than the scheme transformed by the second conversion. The second conversion does not require the random oracle. Therefore, if the original signature scheme is of the standard model, the strongly existentially unforgeable property of the converted signature scheme is proved also in the standard model.

Both conversions ensure tight security reduction to the underlying security assumptions. Moreover, the transformed schemes by the first or second conversion satisfy the on-line/off-line property. That is, signers can precompute almost all operations on the signing before they are given a message.

**Keywords:** signature scheme, strong unforgeability, standard model.

## 1 Introduction

Strong existential unforgeability (SEU) is a stronger variant of the usual security notion, existential unforgeability, of a signature scheme. Ordinary existential unforgeability prohibits an adversary from forging a valid signature on a message which a signer has not signed. However, it does not prohibit an adversary from forging a new valid signature on a message which a signer has already signed. That is, the adversary, by giving a message/signature pair $(M, \sigma)$, may be able to forge a new valid signature $\sigma' \neq \sigma$ on $M$. SEU is a security notion which ensures

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 191–205, 2006.

not only existential unforgeability but also that no adversary can execute the type of forgery mentioned above.

SEU is useful in constructing many applications, such as IND-CCA2 secure public-key encryption schemes [DDN00, CHK04] and a group signature scheme [BBS04]. We review how SEU signatures are used in such applications. In the encryption schemes [DDN00, CHK04], an SEU signature $\sigma$ is used as one part of a ciphertext. It is a signature on the other part $C$ of the ciphertext. The SEU property ensures the IND-CCA2 security of these schemes. Indeed, if the signature scheme is not SEU, an adversary may be able to obtain a new ciphertext $(C, \sigma')$ by modifying the signature of another ciphertext $(C, \sigma)$. This means that the encryption is malleable [DDN00], and hence is not IND-CCA2 secure.

In group signature schemes [BBS04], an authority issues a signature $\sigma$ on a user's secret key $x$ in advance. The signature will be used as an ID of the user. Hence, if the user succeeds in forging a signature, he also succeeds in forging his ID. Therefore, no signature should be able to be forged, especially, a new signature $\sigma' \neq \sigma$ on the user's secret key $x$. Therefore, we require not only the usual existential unforgeability but SEU property.

### 1.1 Our Contributions

We propose two general and efficient conversions, both of which transform a secure signature scheme to a SEU signature scheme. There is tradeoff between the two conversions. The first conversion requires the random oracle [BR93], but the signature scheme transformed by the first conversion has shorter signature length than the scheme transformed by the second conversion.

The second conversion does not require the random oracle. Therefore, if the original signature scheme is of the standard model, the SEU property of the converted signature scheme is proved also in the standard model. The scheme transformed by the first conversion has SEU property, if the original scheme is existentially unforgeable, and the discrete logarithm problem is hard to solve. The scheme transformed by the second conversion has SEU property, if the above two assumptions hold and the collision resistance of a hash function holds.

Both conversions ensure the tight security reduction to the underlying security assumptions. That is, if there exists an adversary who succeeds in breaking the SEU property of the converted scheme with probability $\varepsilon'$ within $t'$ steps, there exists an adversary who can break at least one of assumptions mentioned above with probability $\varepsilon \simeq \varepsilon'$ within $t \simeq t'$ steps.

Moreover, the schemes transformed by the first or second conversion satisfy the on-line/off-line property. That is, signers can precompute almost all operations on the signing before they are given a message. Therefore, the signer can generate signatures quite efficiently.

### 1.2 Previous Work

In PKC 2006, Boneh, Shen, and Waters [BSW06] proposed a SEU signature scheme by modifying the Waters signature scheme [W05]. They also showed that their modification is applicable to not only the Waters scheme but also any