INFORMATICA, 2006, Vol. 17, No. 3, 347–362

Provably Secure Convertible User Designating Confirmer Partially Blind Signatures *

Zhenjie HUANG

Department of Computer Science and Engineering, Zhangzhou Normal University
Fujian, 363000, P. R. China,
State Key Laboratory of Information Security,
Institute of Software of Chinese Academy of Sciences
Beijing 100080, P. R. China,
Department of Computer Science and Engineering, Shanghai Jiao Tong University
Shanghai 200030, P. R. China,
State Key Laboratory of Integrated Service Networks, Xidian University
Xi'an, Shaanxi, 710071, P. R. China
e-mail: zjhuang@stju.edu.cn

Kefei CHEN

Department of Computer Science and Engineering, Shanghai Jiao Tong University
Shanghai 200030, P. R. China
e-mail: kfchen@stju.edu.cn

Yumin WANG

State Key Laboratory of Integrated Service Networks, Xidian University
Xi'an, Shaanxi, 710071, P. R. China
e-mail: ymwang@xidian.edu.cn

Received: January 2005

Abstract. This paper introduces a new concept of convertible user designating confirmer partially blind signature, in which only the designated confirmer (designated by the user) and the user can verify and confirm the validity of given signatures and convert given signatures into publicly verifiable ones. We give a formal definition for it and propose a concrete provably secure scheme with a proof of security and a brief analysis of efficiency. Assuming the intractabilities of the Discrete Logarithm Problem and the ROS-Problem, the proposed scheme is unforgeable under adaptive chosen-message attack.

Key words: cryptography, digital signature, partially blind signature, user designating confirmer signature, convertible.

*This work is supported by the Innovation Foundation for Young Technological Talents of Fujian Province, China, under Grant No.2005J055, the Science and Technology Program of Department of Educatuon of Fujian Province under Grant No. JA04250, and the Natural Science Foundation of Fujian Province of China.

1. Introduction

1.1. *Background and Related Works*

Blind signature, first introduced by Chaum (1982) at Crypto'82, is a variant of digital signatures, which allows the user to get a signature without giving the signer any information about the actual message or the resulting signature. This blindness property plays a central role in applications such as electronic voting and electronic cash schemes where anonymity is of great concern. So, since it was introduced, blind signature has attracted considerable amount of attention.

However, since the signer's view is perfectly shut off from the signing messages and the resulting signatures, there is a particular drawback of blind signatures that the signer can not assure himself that the blind messages accurately contains the information he desires and then the signatures may be used in an unintended way. In a practical sense, it is essential for the signer to include some term of validity in the signing message to prevent abusing. To overcome the weakness of blind signature, Abe and Fujisaki (1996) introduced the concept of *partially blind signature* at Asiacrypt'96, which allows the signer to explicitly include common information in the blind signature under some agreement with the user.

Since Abe and Fujisaki (1996) had introduced partially blind signature in 1996, several partially blind signature schemes have been proposed. Abe and Camenisch (1997) proposed a partially blind signature scheme based on Schnorr signature. Miyazaki, Abe and Sakurai (1997) proposed a partially blind signature scheme based on DSS and a scheme for message recovery signature. Fan and Lei's low-computation scheme is based on quadratic residues problem (Fan and Lei, 1998). In 1999, Juang and Lei (1999) proposed a DL-based partially blind threshold signature scheme, and recently Chien, Jan and Tseng (2003) proposed a RSA-based partially blind threshold signature scheme. The first provably secure partially blind threshold signature scheme was proposed at Crypto2000 by Abe and Okamoto (2000), followed by the Maitland and Boyd's provably secure restrictive partially blind signature scheme (Maitland and Boyd, 2002). In fact, these two schemes' security are proved under non parallel attack only. They are forgeable under the generic parallel attack if the ROS-Problem is solvable, namely security against the generic parallel attack depend on the difficulty of ROS-Problem. Yang and Jan (2004) recently proposed another provably secure restrictive partially blind signature scheme based on the intractability of the ROS-Problem and the hardness of the Discrete Logarithm Problem. At Indocrypt 2003, Zhang, Safavi–Naini and Susilo (2003) proposed a pairing-based partially blind signature scheme. Newly, Chow *et al.* showed that Zhang *et al.*'s scheme is indeed linkable and proposed two new blind signature schemes that achieve unlinkability (Chow *et al.*, 2004). One of their schemes is a partially blind signature scheme in conventional PKI while another one is an ID-based partially blind signature scheme. Zhang *et al.* have revised their scheme to avoid the Chow *et al.*'s attack (Zhang *et al.*, 2004). Recently, Huang *et al.* (2005) proposed a convertible undeniable partially blind signature scheme.

1.2. *Motivation and Main Contribution*

The same as the normal signatures, the partially blind signatures still have the "*self-authenticating*" property that anyone having a copy of any signature can check its validity using the corresponding public information, and the signatures can be transferred in any way by any people. This "self-authenticating" property is necessarily required for many applications of digital signature, but seems to provide too much authentication than necessary in some other applications, where a signed message is personally or commercially sensitive, such as a bill of tax, a bill of health, a writ of summons, a testament etc. Thus it may be preferable to put some restrictions on this property to prevent potential misuse of signatures.

There are several signatures with different restrictions on verification and confirmation available. The *undeniable signature* was introduced by Chaum and Antwerpen (1989) at Crypto'89, in which the signature cannot be verified without the help of the signer. The *directed signature* first proposed by Lim and Lee (1992) at Auscrypto'92, in which only the signer and the recipient can verify the validity of a given signature. The *designated confirmer signature*, introduced by Chaum (1994) at Eurocrypt'94, has a property that the use of signatures is controlled by two people: the signer and the designated confirmer. The *nominative signature*, first proposed by Kim, Park and Won (1996) and improved by Huang and Wang (2004) is the dual signature scheme of the undeniable signature, in which not the signer but only the recipient can control the use of signatures. In addition, in 1999, Araki, Uehara and Imamura proposed the *limited verifier signature* (Araki *et al.*, 1999), and Steinfeld *et al.* proposed the *universal designated-verifier signature* in 2003 (Steinfeld *et al.*, 2003).

We consider the scenarios of signing testament. Suppose that the user Alice wants a lawyer Bob to notarize her testament by signing it. Since the testament is personally sensitive, Alice may desire that: (1) the content of the testament should be blind to Bob; (2) only Alice herself and the beneficiary designated by her, such as her daughter, can verify and confirm to third party the validity of the resulting signature; (3) who is the designated beneficiary should be blind to Bob; (4) when it is necessary, Alice or the designated beneficiary can convert a given signature into a publicly verifiable one. To the best of our knowledge, up to now, there are no signature scheme available satisfying all these four requirements.

Combining the concept of partially blind signature with the concept of designated confirmer signature, we introduce a new concept of *convertible user designating confirmer partially blind signature*, in which only the designated confirmer (designated by the user and blind to the signer) and the user can verify and confirm the validity of a given signature and convert a given signature into a publicly verifiable one, to meet all four requirements above. We present a formal definition for it and propose a concrete provably secure scheme with a proof of security and a brief analysis of efficiency. We prove that the proposed scheme is unforgeable under adaptive chosen-message attack assuming the intractabilities of the Discrete Logarithm Problem and the ROS-Problem. The proposed scheme has an advantage that after a signature was converted, the converted signature is indistinguishable from normal partially blind signatures.

We would like to emphasize some differences between the user designating confirmer signature and the designated confirmer signature: (1) not the signer but the user designates the confirmer in the former while the signer designates the confirmer in the latter; (2) the signer can neither verify nor confirm the validity of given signatures in the former while the signer can do that in the latter; (3) the signer can not know who is the designated confirmer in the former. These three properties with the convertibility make the convertible user designating confirmer signature is very fit for the case of signing testament. Since the lawyer (the signer) can neither use the testament (the signature) nor know who is the beneficiary (the designated confirmer), the interest of the user would be protected farthest. Furthermore, there are two ways for the beneficiary and the user to use the testament, one is proving the validity of the testament using the confirmation proof protocol, another is converting the testament into a publicly verifiable one.

The convertible user designating confirmer partially blind signature is very fit for signing personally or commercially sensitive message and may be useful to the Internet community and Web-based systems community.

1.3. *Organization*

The paper is structured as follows. The preliminaries are given in next section, and in Section 3 we present a formal definition of convertible user designating confirmer partially blind signature. Section 4 proposes a concrete provably secure convertible user designating confirmer partially blind signature scheme with a proof of security and a brief analysis of efficiency. The conclusions are given in Section 5.

2. Preliminaries

2.1. *Cryptographic Setting*

Let p, q be large primes that satisfy $q|(p-1)$, and g be an element in $\mathbb{Z}_p^*$ with order q. Let $\langle g\rangle$ denote the subgroup in $\mathbb{Z}_p^*$ generated by g. Let $\mathcal{H}$: $\{0,1\}^* \rightarrow \mathbb{Z}_q$ and $\mathcal{F}$: $\{0,1\}^* \rightarrow \langle g\rangle$ be public hash functions.

All arithmetic operations are done in $\mathbb{Z}_p^*$ hereafter unless otherwise noted. We will use the notation $a \in_R A$ to mean that a is randomly chosen from A and use the symbol $\|$ to mean concatenation.

Following are three hard problems and their corresponding assumptions.

Discrete Logarithm (DL) Problem: Given $g, u \in \mathbb{Z}_p^*$, find an integer $a \in \mathbb{Z}_q^*$ such that $u = g^a$.

Discrete Logarithm (*DL*) *Assumption*: For every probabilistic polynomial-time algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ to solve DL-Problem is negligible.

Decisional Diffie–Hellman (DDH) Problem: Given $g, h, u, v \in \mathbb{Z}_p^*$, decide whether $\log_g u = \log_h v$.

Decisional Diffie–Hellman (*DDH*) *Assumption*: For every probabilistic polynomial-time algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ to solve DDH-Problem is negligible.

Computational Diffie–Hellman (CDH) Problem: For some $a \in \mathbb{Z}_q^*$, given $g, h, g^a \in \mathbb{Z}_p^*$, compute h^a.

Computational Diffie–Hellman (*CDH*) *Assumption*: For every probabilistic polynomial-time algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ to solve CDH-Problem is negligible.

2.2. *Zero-Knowledge Proof Protocol*

Assume the prover knows the discrete logarithm x of $y = g^x$ and wants to confirm the verifier that $\log_g y = \log_h z$ for given group elements h and z.

ZKP: *Proving the equality of two discrete logarithms* (Chaum and van Antwerpen, 1989)

1. The verifier chooses $a, b \in_R \mathbb{Z}_q^*$, computes $\alpha = h^a g^b$, and sends α to the prover.
2. The prover chooses $t \in_R \mathbb{Z}_q^*$, computes $\beta_1 = \alpha g^t, \beta_2 = \beta_1^x$, then sends (β_1, β_2) to the verifier.
3. The verifier sends (a, b) to the prover.
4. If $\alpha = h^a g^b$, the prover sends t to the verifier.
5. The verifier checks whether $\beta_1 = h^a g^{b+t}, \beta_2 = z^a y^{b+t}$.

It was proved that the protocol above is zero-knowledge and uncheatable (Chaum and van Antwerpen, 1989). The uncheatable means that the prover cannot cheat the verifier with probability exceeding p^{-1} even with infinite computing power.

2.3. *Signature of Knowledge*

A pair (c, s) satisfying $c = \mathcal{H}(g\|h\|y\|z\|\ g^s y^c \| h^s z^c \| m)$ is signature of equality of the discrete logarithm of y with respect to the base g and the discrete logarithm of z with respect to the base h for the message m and is denoted by *SEQDL*(g, h, y, z, m).

A *SEQDL* (g, h, y, z, m) can only be computed if the private key $x = \log_g y = \log_h z$ is known, by choosing $k \in_R \mathbb{Z}_q$, and computing c and s according to $c = \mathcal{H}(g\|h\|y\|z\|g^k\|h^k\|m), s = k - c\,x \pmod q$.

This signature of knowledge can also prove the logarithms of two group elements with respect to two different bases are the same. Signature of knowledge is non-interactive and transferable while the zero-knowledge proof protocol above is interactive and untransferable.

3. Definition of Convertible User Designating Confirmer Partially Blind Signatures

A secure convertible user designating confirmer partially blind signature scheme, which involves three parties: the signer S, the user U and the confirmer C designated by the user, is a ten-tuple (***KG, Sig***$_{S,U}$***, Ver***$_C$***, Conf***$_C$***, Conv***$_C$***, UVer***$_C$***, Ver***$_U$***, Conf***$_U$***, Conv***$_U$***, UVer***$_U$) such that the following held. Assume the signer and the user agree on a piece of common information info.

- ***KG*** is a probabilistic polynomial-time key generation algorithm that takes input security parameter 1^n, outputs a public and private key pair (pk, sk).

• $\boldsymbol{Sig}_{S,U}$ is an interactive probabilistic polynomial-time signature issuing protocol between the signer S and the user U, which on common input security parameter 1^n, the signer S's public key pk_S, common information info, the signer S inputs his private key sk_S and the user U inputs message msg, the designated confirmer C's public key pk_C and his private key sk_U privately, respectively. They engage in the signature issuing protocol and stop in polynomial-time. When they stop, the user outputs either "*False*" or a signature $\sigma_{\mathsf{msg},\mathsf{info}}$ for message msg with regard to the common information info. Let $\sum_{\mathsf{msg},\mathsf{info}}$ be the set of signatures $\sigma_{\mathsf{msg},\mathsf{info}}$ for message msg with regard to the common information info.

• $\boldsymbol{Ver}_C$ ($\boldsymbol{Ver}_U$) is a polynomial-time verification algorithm for the designated confirmer C (the user U), in which the designated confirmer (the user) inputs security parameter 1^n, the signer's public key pk_S, the user's (the designated confirmer's) public key $pk_{U(C)}$, the designated confirmer's (the user's) private key $sk_{C(U)}$, message msg, common information info, and a presumed signature σ, outputs either 0 or 1. For all msg and info, for any constant c, and for sufficiently large n, if $\sigma \in \sum_{\mathsf{msg},\mathsf{info}}$,

$$\mathbf{Pr}\big[\boldsymbol{Ver}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_{U(C)}, sk_{C(U)}) = 1\big] > 1 - n^{-c},$$

otherwise,

$$\mathbf{Pr}\big[\boldsymbol{Ver}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_{U(C)}, sk_{C(U)}) = 0\big] > 1 - n^{-c}.$$

• $\boldsymbol{Conf}_C$ ($\boldsymbol{Conf}_U$) is an interactive confirmation proof protocol between the designated confirmer C (the user U) and the third party T, which, on common input security parameter 1^n, message msg, common information info, a presumed signature σ, the signer's public key pk_S and the user's (the designated confirmer's) public key $pk_{U(C)}$. Here the designated confirmer (the user) is the prover with an auxiliary input, his private key $sk_{C(U)}$, and the third party T is the verifier. They engage in the proof protocol and stop in polynomial-time. When they stop, the third party T outputs either 0 or 1. For all msg and info, for any constant c, and for sufficiently large n, if $\sigma \in \sum_{\mathsf{msg},\mathsf{info}}$,

$$\mathbf{Pr}\big[\boldsymbol{Conf}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_{U(C)}, sk_{C(U)}) = 1\big] > 1 - n^{-c},$$

otherwise,

$$\mathbf{Pr}\big[\boldsymbol{CD}_{S(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_U, sk_{S(U)}) = 0\big] > 1 - n^{-c}.$$

• $\boldsymbol{Conv}_C$ ($\boldsymbol{Conv}_U$) is a polynomial-time conversion algorithm for the designated confirmer C (the user U), which, on input security parameter 1^n, message msg, common information info, a valid signature $\sigma_{\mathsf{msg},\mathsf{info}}$, the signer's public key pk_S, the user's (the designated confirmer's) public key $pk_{U(C)}$, the designated confirmer's (the user's) private key $sk_{C(U)}$, outputs a converted signature $\sigma'_{\mathsf{msg},\mathsf{info}}$ which can be universally verified.

• ***UVer***$_C$ (***UVer***$_U$) is a polynomial-time universally verification algorithm, which on input security parameter 1^n, the signer's public key pk_S, message msg, common information info and a converted signature $\sigma'_{\mathsf{msg,info}}$, outputs either 0 or 1. For all msg and info, for any constant c, and for sufficiently large n, if $\sigma'_{\mathsf{msg,info}}$ is a converted signature converted by the designated confirmer C (the user U),

$$\mathbf{Pr}\big[\boldsymbol{UVer}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma'_{\mathsf{msg,info}}, pk_S) = 1\big] > 1 - n^{-c},$$

otherwise,

$$\mathbf{Pr}\big[\boldsymbol{UVer}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma'_{\mathsf{msg,info}}, pk_S) = 0\big] > 1 - n^{-c},$$

• ***Completeness*** If the signer S and the user U follow the signature issuing protocol and the user U outputs $\sigma_{\mathsf{msg,info}}$, then for any constant c and for sufficiently large n,

$$\begin{aligned}
&\mathbf{Pr}\big[\boldsymbol{Ver}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma_{\mathsf{msg,info}}, pk_{U(C)}, sk_{C(U)}) = 1\big] > 1 - n^{-c},\\
&\mathbf{Pr}\big[\boldsymbol{Conf}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma_{\mathsf{msg,info}}, pk_{U(C)}, sk_{C(U)}) = 1\big] > 1 - n^{-c},\\
&\mathbf{Pr}\big[\boldsymbol{UVer}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma'_{\mathsf{msg,info}}, pk_S) = 1\big] > 1 - n^{-c},
\end{aligned}$$

where $\sigma'_{\mathsf{msg,info}}$ is the signature converted from $\sigma_{\mathsf{msg,info}}$.

• ***Unforgeability*** Let $\mathcal{F}$ be a probabilistic polynomial-time forging algorithm which, on input security parameter 1^n, common information info, the public keys $PK = (pk_S, pk_C, pk_U)$, can request and receive signatures of polynomial-many adaptively chosen message and common information pairs $(\mathsf{msg}_i, \mathsf{info}_j)$, and finally outputs $(\mathsf{msg}, \mathsf{info}, \sigma)$ with $(\mathsf{msg}, \mathsf{info}) \notin \{(\mathsf{msg}_i, \mathsf{info}_j)\}$. For all such $\mathcal{F}$, for any constant c, and for sufficiently large n, the probability that $\mathcal{F}$ outputs $(\mathsf{msg}, \mathsf{info}, \sigma)$ for which at least one of $\boldsymbol{Ver}_C$, $\boldsymbol{Conf}_C$, $\boldsymbol{Ver}_U$ and $\boldsymbol{Conf}_U$ outputs 1 is less than n^{-c}, that is,

$$\begin{aligned}
\mathbf{Pr}\Big[&(\mathsf{msg}, \mathsf{info}, \sigma) \leftarrow \mathcal{F}^{\boldsymbol{Sig}}(1^n, \mathsf{msg}, \mathsf{info}, PK)\colon\ (\mathsf{msg}, \mathsf{info}) \notin \{(\mathsf{msg}_i, \mathsf{info}_j)\}\\
&\wedge \big(\boldsymbol{Ver}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_{U(C)}, sk_{C(U)}) = 1\\
&\vee \boldsymbol{Conf}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_{U(C)}, sk_{C(U)}) = 1\big)\Big] < n^{-c}.
\end{aligned}$$

• ***Verification Untransferability*** Let $\mathcal{A}$ be a probabilistic polynomial-time attacking algorithm which, on input security parameter 1^n, the public keys $PK = (pk_S, pk_C, pk_U)$, message msg, common information info and a presumed signature σ, can request the execution of $\boldsymbol{Ver}_C$, $\boldsymbol{Conf}_C$, $\boldsymbol{Ver}_U$ and $\boldsymbol{Conf}_U$ for polynomial-many adaptively chosen strings except σ, and finally outputs either 0 or 1. For all such $\mathcal{A}$, for any constant c, and for sufficiently large n,

$$\begin{aligned}
\Big|\mathbf{Pr}\big[&\mathcal{A}^{\boldsymbol{Ver}_{C(U)}, \boldsymbol{Conf}_{C(U)}}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, PK)\\
&= \boldsymbol{Ver}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_{U(C)}, sk_{C(U)})\big] - 1/2\Big| < n^{-c}.
\end{aligned}$$

• ***Confirmation Untransferability*** Let $\boldsymbol{Conf}_{\mathcal{A}}$ be a probabilistic polynomial-time (interactive) proof protocol which, on input security parameter 1^n, the public keys $PK = (pk_S, pk_C, pk_U)$, message msg, common information info and a presumed signature σ, can request the execution of $\boldsymbol{Conf}_C$, $\boldsymbol{Conf}_U$, $\boldsymbol{Conv}_C$ and $\boldsymbol{Conv}_U$ for polynomial-many adaptively chosen strings, where $\boldsymbol{Conf}_{\mathcal{A}}$ can request execution of $\boldsymbol{Conf}_C$ and $\boldsymbol{Conf}_U$ on the given (msg, info, σ) but cannot request execution of $\boldsymbol{Conv}_C$ and $\boldsymbol{Conv}_U$ on (msg, info, σ). The attacker and the third party engage in protocol $\boldsymbol{Conf}_{\mathcal{A}}$ and stop in polynomial-time. When they stop, the third party T outputs either 0 or 1. For all such $\boldsymbol{Conf}_{\mathcal{A}}$, for any constant c, and for sufficiently large n,

$$\Big|\mathbf{Pr}\big[\boldsymbol{Conf}_{\mathcal{A}}^{\boldsymbol{Ver}_{C(U)},\boldsymbol{Conf}_{C(U)}}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, PK) = \boldsymbol{Ver}_{C(U)}(1^n, \mathsf{msg}, \mathsf{info}, \sigma, pk_S, pk_{U(C)}, sk_{S(U)})\big] - 1/2\Big| < n^{-c}.$$

• ***Partially Blindness*** Let S' be a probabilistic polynomial-time algorithm, U_0 and U_1 be two honest users. U_0 and U_1 engage in the signature issuing protocol with S' for messages msg_b and msg_{1-b} with regard to the common information info, and output $\sigma_{\mathsf{msg}b,\,\mathsf{info}}$ and $\sigma_{\mathsf{msg1\text{-}}b,\,\mathsf{info}}$, respectively, where $b \in_R \{0,1\}$. Sends (msg_0, msg_1, $\sigma_{\mathsf{msg}b,\,\mathsf{info}}$, $\sigma_{\mathsf{msg1\text{-}}b,\,\mathsf{info}}$) to S' and then S' outputs $b' \in \{0,1\}$. For all such S', U_0 and U_1, for any constant c, and for sufficiently large n, $|\mathbf{Pr}[b = b'] - 1/2| < n^{-c}$.

4. Concrete Provably Secure Scheme

In this section, we propose a concrete provably secure convertible user designating confirmer partially blind signature scheme. The idea behind the proposed scheme to achieve the designated confirmer property is embedding $y_C^{x_U} = y_U^{x_C}$ into signatures so that the signatures cannot be verified without the user's private key x_U nor the designated confirmer's private key x_C and prevent other people from verifying signature. The confirmation protocol base on a zero-knowledge proof protocol.

4.1. *Proposed Scheme*

Assume the signer S, the user U and the designated confirmer C's public and private key pairs are $(y_S, x_S), (y_U, x_U)$ and (y_C, x_C), respectively, where $y_* = g^{x_*}$. Let msg be the message to be signed. The signer and the user first agree on common information info in a predetermined way.

• *Signing*

1. The signer chooses $u, s, d \in_R \mathbb{Z}_q^*$, computes

$$z = \mathcal{F}(\mathsf{info}),$$
$$a = g^u,$$
$$b = g^s z^d,$$

then sends (a, b) to the user.

2. The user chooses $t_1, t_2, t_3, t_4 \in_R \mathbb{Z}_q^*$, computes

$$
\begin{aligned}
z &= \mathcal{F}(\mathsf{info}),\\
\alpha &= a g^{t_1} y_S^{t_2},\\
\beta &= b\, g^{t_3} z^{t_4},\\
\varepsilon &= \mathcal{H}(\alpha \| \beta \| z \| \mathsf{msg}),\\
e &= \varepsilon - t_2 - t_4 \pmod q,
\end{aligned}
$$

then sends e to the signer.

3. The signer computes

$$
\begin{aligned}
c &= e - d \pmod q,\\
r &= u - c\, x_S \pmod q,
\end{aligned}
$$

then sends (r, c, s, d) to the user.

4. The user checks whether

$$
\begin{aligned}
g^r y_S^c &= a,\\
g^s z^d &= b.
\end{aligned}
$$

If two equations above are held, he computes

$$
\begin{aligned}
t &= \mathcal{H}(y_C^{x_U} \| \varepsilon \| \mathsf{info} \| \mathsf{msg})\\
\rho &= (r + t_1) t^{-1} \pmod q,\\
\omega &= (c + t_2) \pmod q,\\
\sigma &= (s + t_3) t^{-1} \pmod q,\\
\delta &= (d + t_4) \pmod q,
\end{aligned}
$$

and publishes the signature $\sigma_{\mathsf{msg},\mathsf{info}} = (\rho, \omega, \sigma, \delta)$ for message msg with regard to common information info. Otherwise, outputs "*False*".

- *Verification*

The *User's Verification* and the *Designated Confirmer's Verification* are the same. The user or the designated confirmer computes

$$
t = \mathcal{H}\big(y_C^{x_U} \| \omega + \delta \| \mathsf{info} \| \mathsf{msg}\big) = \mathcal{H}\big(y_U^{x_C} \| \omega + \delta \| \mathsf{info} \| \mathsf{msg}\big)
$$

and then checks whether

$$
\omega + \delta = \mathcal{H}\big(g^{\rho t} y_S^{\omega} \| g^{\sigma t} z^{\delta} \| \mathcal{F}(\mathsf{info}) \| \mathsf{msg}\big),
$$

where and hereafter $z = \mathcal{F}(\mathsf{info})$.

• *Confirmation*

The *User's Confirmation* and the *Designated Confirmer's Confirmation* are the same. The user or the designated confirmer (the prover) computes $A = g^{\rho t}, B = g^{\sigma t}$, then sends A, B and proves $\log_{g^\rho} A = \log_{g^\sigma} B$ to the third party (the verifier) using ***ZKP***. Then the third party checks whether

$$\omega + \delta = \mathcal{H}\big(Ay_S^{\omega} \| Bz^{\delta} \| \mathcal{F}(\mathsf{info}) \| \mathsf{msg}\big).$$

• *Selective Conversion*

The *User's Conversion* and the *Designated Confirmer's Conversion* are the same. When the user or the designated confirmer wants to convert a signature $\sigma_{\mathsf{msg},\mathsf{info}} = (\rho, \omega, \sigma, \delta)$ into a publicly verifiable one, he computes

$$\begin{aligned} t &= \mathcal{H}\big(y_C^{x_U} \| \omega + \delta \| \mathsf{info} \| \mathsf{msg}\big) = \mathcal{H}\big(y_U^{x_C} \| \omega + \delta \| \mathsf{info} \| \mathsf{msg}\big), \\ \rho' &= \rho t \pmod q, \\ \sigma' &= \sigma t \pmod q, \end{aligned}$$

and publishes the converted signature $\sigma'_{\mathsf{msg},\mathsf{info}} = (\rho', \omega, \sigma', \delta)$.

Remark. The converted signature is indistinguishable from normal partially blind signatures.

• *Universally Verification*

Anyone can verify the converted signature $\sigma'_{\mathsf{msg},\mathsf{info}} = (\rho', \omega, \sigma', \delta)$ by checking

$$\omega + \delta = \mathcal{H}\big(g^{\rho'} y_S^{\omega} \| g^{\sigma'} z^{\delta} \| \mathcal{F}(\mathsf{info}) \| \mathsf{msg}\big).$$

4.2. *Security*

• ***Completeness.*** The completeness can easily be verified by straightforward calculating.

• ***Unforgeability.*** Assuming the intractability of the Discrete Logarithm Problem and idea randomness of hash functions $\mathcal{H}$ and $\mathcal{F}$, the proposed scheme is unforgeable under adaptive chosen-message attack. The proof of the unforgeability of the proposed scheme follows the proof of the Lemma 2 in (Abe and Okamoto, 2000) given by Abe and Okamoto (see Appendix).

The proof of the Lemma 2 in (Abe and Okamoto, 2000) did not take the generic parallel attack into account. In fact, the scheme in (Abe and Okamoto, 2000) is forgeable under the generic parallel attack if the ROS-Problem is solvable, so the security against the generic parallel attack to this scheme depends on the difficulty of ROS-Problem. Our scheme's security is the same as that of the scheme in (Abe and Okamoto, 2000). Finding a provably secure DL-based partially blind signature scheme, in which its security does not depend on the difficulty of ROS-Problem, remains an open problem.

• ***Verification Untransferability.*** In the proposed scheme, to verify a given signature $\sigma_{\mathsf{msg},\mathsf{info}} = (\rho, \omega, \sigma, \delta)$, one needs to compute $t = \mathcal{H}(y_C^{x_U} \| \omega + \delta \| \mathsf{info} \| \mathsf{msg}) = \mathcal{H}(y_U^{x_C} \| \omega + \delta \| \mathsf{info} \| \mathsf{msg})$, which is equivalent to compute $y_C^{x_U} = y_U^{x_C}$. Assuming the intractability of the CDH-Problem, any adversary can not compute $y_C^{x_U} = y_U^{x_C}$. So the verification untransferability is held under the Computational Diffie–Hellman Assumption.

• ***Confirmation Untransferability.*** Since ***ZKP*** used in the confirmation protocol is zero-knowledge (Chaum and van Antwerpen, 1989), the proposed scheme is confirmation untransferability under the Decisional Diffie–Hellman Assumption.

• ***Correctness of Confirmation.*** By confirmation protocol, the prover proves that he knows t such that $\omega + \delta = \mathcal{H}(g^{\rho t} y_S^{\omega} \| g^{\sigma t} z^{\delta} \| \mathcal{F}(\mathsf{info}) \| \mathsf{msg})$, namely, the prover proves that he can extract a valid signature for message msg with regard to common information info. Since the scheme is unforgeable, it guarantees that the signer indeed issued the signature and the prover holds it.

• ***Partially Blindness.*** For $i = 0, 1$, let $(a_i, b_i, e_i, r_i, c_i, s_i, d_i)$ be data appearing in the view of the signer S during the execution of the signature issuing protocol with the user for message msg_i with regard to common information info, and let $(\rho_i, \omega_i, \sigma_i, \delta_i)$ be the corresponding signatures. It is sufficient to show that there exists a tuple of factors (t_1, t_2, t_3, t_4) that maps $(a_i, b_i, e_i, r_i, c_i, s_i, d_i)$ to $(\rho_j, \omega_j, \sigma_j, \delta_j)$ for each $i, j \in \{0, 1\}$. To this end, we define $t_1 = \rho_j t_j - r_i$, $t_2 = \omega_j - c_i$, $t_3 = \sigma_j t_j - s_i$, $t_4 = \delta_j - d_i$, where $t_j = \mathcal{H}(y_C^{x_U} \| \omega_j + \delta_j \| \mathsf{info} \| \mathsf{msg}_j)$, and have that

$$a_i g^{t_1} y_S^{t_2} = g^{r_i} y_S^{c_i} g^{\rho_j t_j - r_i} y_S^{\omega_j t_j - c_i} = g^{\rho_j t_j} y_S^{\omega_j} = \alpha_j,$$
$$b_i g^{t_3} z^{t_4} = g^{s_i} z^{d_i} g^{\sigma_j t_j - s_i} z^{\delta_j - d_i} = g^{\sigma_j t_j} z^{\delta_j} = \beta_j.$$

Thus, $(a_i, b_i, e_i, r_i, c_i, s_i, d_i)$ and $(\rho_j, \omega_j, \sigma_j, \delta_j)$ have exactly the same relation defined by the signature issuing protocol. Such (t_1, t_2, t_3, t_4) always exist regardless of the values of $(a_i, b_i, e_i, r_i, c_i, s_i, d_i)$ and $(\rho_j, \omega_j, \sigma_j, \delta_j)$. Therefore, even for an infinitely powerful S', the probability $\mathbf{Pr}\ [b = b'] = 1/2$, and the proposed scheme is partially blind.

• ***Unlinkability.*** Since the signature $(\rho, \omega, \sigma, \delta)$ is partially blind, the only way for the signer to link a signature to its owner is extracting some information about the owner from t. But, under the CDH-Assumption, given any public key pair $(y_1 = g^{x_1}, y_2 = g^{x_2})$, the signer can not decide whether $t = \mathcal{H}(y_1^{x_2} \| \omega + \delta \| \mathsf{info} \| \mathsf{msg})$ or not. Thus the signer can not link a signature to its owner.

4.3. *Efficiency*

In computation, compared with the Abe and Okamoto's scheme (Abe and Okamoto, 2000), to achieve the designated confirmer property our scheme only has one additional Hash function computation in both signing procedure and verification procedure. The verification of converted signature is the same as that of Abe and Okamoto's scheme.

In communication, the proposed scheme is the same as Abe and Okamoto's scheme.

5. Conclusions

A feasible solution to prevent potential misuse of signatures is to control their verification and confirmation. In this paper, we introduce a new concept of convertible user designating confirmer partially blind signature along with a formal definition for it and a concrete provably secure scheme that implements it. The convertible user designating confirmer partially blind signature is fit for signing personally or commercially sensitive message such as a testament and may be useful to the Internet community and Web-based systems community.

The security against the generic parallel attack to all DL-based partially blind signature schemes available depends on the difficulty of ROS-Problem. Finding a provably secure DL-based partially blind signature scheme, in which its security does not depend on the difficulty of ROS-Problem, remains an open problem.

Finally, we would like to point out that the proposed scheme can easily be transformed into a fully blind one by fixing common information to a single string. Furthermore, let $t = 1$, the proposed scheme becomes a normal partially blind signature scheme.

Appendix: Proof of the Unforgeability of the Proposed Scheme

The proof of the unforgeability of the proposed scheme follows the proof of the Lemma 2 in (Abe and Okamoto, 2000) given by Abe and Okamoto.

We first treat the common-part forgery where an adversary forges a signature with regard to common information info that never requested to signing oracle. Next we treat one-more forgery. For this case, we first prove the security with restricted signing oracle that issues signatures only for a fixed info, and then eliminate the restriction by showing the reduction from the unrestricted signing oracle model to the restricted one.

For each info, let l_{info} be the number of queries with the common information info asked from attacker to signing oracle. (For info that has never asked to signing oracle, define $l_{\mathsf{info}} = 0$.) Let $q_{\mathcal{F}}$, $q_{\mathcal{H}}$ and q_S be the maximum number of queries asked from attacker to $\mathcal{F}$, $\mathcal{H}$, and signing oracle, respectively.

First, we consider common-part forgery. Assume that $\mathcal{U}^*$ is a common-part adversary with probability $\mu > n^{-c}$. By using $\mathcal{U}^*$, we construct a machine $\mathcal{M}$ that forges a non-blind version of signature and then use $\mathcal{M}$ to solve the discrete logarithm problem by exploiting the collision property. Let (y, g) be the problem that we want to solve $\log_g y$, we construct $\mathcal{M}$ as following:

- Select $I \in_R \{1, \cdots, q_{\mathcal{F}} + q_S\}$ and $J \in_R \{1, \cdots, q_{\mathcal{H}} + q_S\}$.
- Run $\mathcal{U}^*$ with $pk_S := (y, g, p, q)$ simulating $\mathcal{H}$, $\mathcal{F}$ and signing oracle as follows.
  - For i-th query to $\mathcal{F}$, return z such that
    - $z := \mathcal{F}(\mathsf{info}_I)$ if $i = I$, or
    - $z := g^{w_i}$ where $w_i \in_R \mathbb{Z}_q^*$, otherwise.
  - For j-th query to $\mathcal{H}$,
    - ask $\mathcal{H}$ if $j = J$, or

  - ∗ randomly select the answer from $\mathbb{Z}_q$, otherwise.
- For requests to signing oracle with a common information info_k. If $\mathcal{F}(\mathsf{info}_k)$ is not defined yet, define it as mentioned above. Then,
  - ∗ if $\mathsf{info}_k \neq \mathsf{info}_I$, simulate a signer by using witness w_k as follows:
    1. $\mathcal{M}$ computes and sends commitments $a = g^r y^c, b = g^v$ to $\mathcal{U}^*$, where $r, c, v \in_R \mathbb{Z}_q^*$.
    2. $\mathcal{U}^*$ computes and sends his challenge e to $\mathcal{M}$. Here $\mathcal{M}$ queries oracle service $\mathcal{F}$ and $\mathcal{H}$ as mentioned above.
    3. $\mathcal{M}$ sends answer (r, c, s, d) to $\mathcal{U}^*$, where $d = e - c$, $s = v - d\, w_k$.
    4. $\mathcal{U}^*$ completes signing procedure and outputs signature.
  - ∗ if $\mathsf{info}_k = \mathsf{info}_I$, we expect that $\mathcal{U}^*$ aborts the session before it receives (r, c, s, d) and just to simulate the state of abortion. If $\mathcal{U}^*$ tries to complete the session, the simulation fails. In this case, $\mathcal{M}$ sends random $a, b, r, c, s$and d to $\mathcal{U}^*$.
- If $\mathcal{U}^*$ eventually outputs signature $(\rho, \omega, \sigma, \delta)$ with regard to info_I and msg_J, output them.

The simulation of signing oracle above shows an important fact that the proposed scheme is *witness indistinguishable*, which is necessary for our proof.

Note that the queries to $\mathcal{F}$ and $\mathcal{H}$ may include the ones inquired during the simulation of signing oracle. So, $\mathcal{F}$ and $\mathcal{H}$ are defined at $q_{\mathcal{F}} + q_S$ and $q_{\mathcal{H}} + q_S$ points during the simulation, respectively. The simulation of signing for $\mathsf{info}_k \neq \mathsf{info}_I$ can be perfectly done with w_k due to witness indistinguishability. The probability that $\mathcal{U}^*$ is successful without asking $\mathcal{F}, \mathcal{H}$ in a proper way is negligible because of the unpredictability of those hash functions. Thus, the success probability of $\mathcal{M}$ is only negligibly worse than $\mu/(q_{\mathcal{F}} + q_S)(q_{\mathcal{H}} + q_S)$ which is not negligible in n. By μ', we denote the success probability of $\mathcal{M}$.

Now we use $\mathcal{M}$ to solve $\log_g y$. The trick is to simulate $\mathcal{F}$ by responding to the query from $\mathcal{M}$ with yg^γ where $\gamma \in_R \mathbb{Z}_q^*$. Note that $\mathcal{M}$ asks each of $\mathcal{F}$ and $\mathcal{H}$ only once. Furthermore, the query to $\mathcal{F}$ happens before the query to $\mathcal{H}$ with overwhelming probability when $\mathcal{M}$ is successful because $\mathcal{F}(\mathsf{info})$ is contained in the inputs of $\mathcal{H}$. Using the standard oracle replay technique (Feige *et al.*, 1988) on $\mathcal{H}$. That is, run $\mathcal{M}$ with a random tape and a random choice of $\mathcal{H}$. $\mathcal{M}$ then outputs a valid signature, say $(\rho, \omega, \sigma, \delta)$, with probability at least $1 - \mathrm{e}^{-1}$ (here, e is base of natural logarithms) after $1/\mu'$ trials. Then rewind $\mathcal{M}$ with the same random tape and run it with a different choice of $\mathcal{H}$. By repeating this rewind-trial $2/\mu'$ times, we get another valid signature, say $(\rho', \omega', \sigma', \delta')$, with probability at least $(1 - \mathrm{e}^{-1})/2$. In other words, with constant probability and polynomial running time, we have two valid signatures $(\rho, \omega, \sigma, \delta)$ and $(\rho', \omega', \sigma', \delta')$ with regard to the same α and β. Thus, $\rho t + \omega x = \rho' t + \omega' x$, $\sigma + \delta(x + \gamma) = \sigma' + \delta'(x + \gamma)$, and $\omega + \delta \neq \omega' + \delta'$ are held. Since at least $\omega \neq \omega'$ or $\delta \neq \delta'$ happens, we can get x as $x = (\rho - \rho')/(\omega - \omega')$ or $x = (\sigma - \sigma')/(\delta - \delta') - \gamma$.

Next, we consider the case where the forgery is attempted against info such that $l_{\mathsf{info}} \neq 0$. As the first step, we consider the case where the common information is a fixed one.

Assume $\mathcal{U}_F^*$ is a single-info adversary with non-negligible probability. We construct an algorithm $\mathcal{M}$ that utilizes $\mathcal{U}_F^*$ as black-box and breaks the intractability assumption of the discrete logarithm, namely, on input (g, z_0), computes w_0 such that $z_0 = g^{w_0}$.

$\mathcal{M}$ firstly selects $b \in_R \{0, 1\}$ and assigns (y, z) as $(y, z) = (g^x, z_0 g^\gamma)$ if $b = 0$, or $(y, z) = (z_0 g^\gamma, g^w)$ if $b = 1$ by choosing γ, x (or w) $\in_R \mathbb{Z}_q^*$. F is defined so that it returns appropriate value of z according to the choice. Hereafter, without loss of generality, we assume that b = 0 is chosen. $\mathcal{M}$ can then simulate the signing oracle, since the signing protocol is witness indistinguishable and having $x = \log_g y$ is sufficient to complete the protocol. Let $\hat{S}$ denote the signer simulated by $\mathcal{M}$.

If $\mathcal{U}_F^*$ is successful with probability at least η, we can find a random tape string for $\mathcal{U}_F^*$ and $\hat{S}$ with probability at least $1/2$ such that $\mathcal{U}_F^*$ with succeeds with probability at least $\eta/2$.

By employing $\mathcal{U}_F^*$ as a black-box, we can construct $\overline{\mathcal{U}}^*$ which has exactly the same interface with $\hat{S}$ as $\mathcal{U}_F^*$ has, and plays the role of an impersonator in the interactive identification protocol with verifier $\overline{\mathcal{H}}$ (Suppose that $\overline{\mathcal{H}}$ has the knowledge of x_l's and can verify the signatures). When $\mathcal{U}_F^*$ asks at most $q_{\mathcal{H}}$ queries to random oracle $\mathcal{H}$, $\overline{\mathcal{U}}^*$ is successful in completing the identification protocol with verifier $\overline{\mathcal{H}}$ with probability at least $\eta/2q_{\mathcal{H}}^{l_{\mathsf{info}}+1}$, since, with probability greater than $1/2q_{\mathcal{H}}^{l_{\mathsf{info}}+1}$, $\overline{\mathcal{U}}^*$ can guess a correct selection of $l_{\mathsf{info}}+1$ queries that $\overline{\mathcal{U}}^*$ eventually uses in the forgery. Similar to the case of common-part forgery, using the standard oracle replay technique, $\mathcal{M}$ can obtain $w_0 = (\sigma_i - \sigma_i')/(\delta_i - \delta_i') - \gamma$ such that $z_0 = g^{w_0}$ with probability $\eta^2/240(l_{\mathsf{info}} + 1)(l_{\mathsf{info}} + 2)^2 q_{\mathcal{H}}^{2(l_{\mathsf{info}}+1)}$ (Abe and Okamoto, 2000), where i is an random index of the successful challenge tuple.

Now we consider the case where the common information is not all the same. Given successful forger $\mathcal{U}_B^*$, we construct successful forger $\mathcal{U}_F^*$ of the fixed-info version as following.

- Select J randomly from $\{1, \cdots, q_{\mathcal{F}} + q_S\}$.
- Run $\mathcal{U}_B^*$ simulating $\mathcal{H}$, $\mathcal{F}$ and signing oracle as follows.
  - For j-th query to $\mathcal{F}$, return $z := \mathcal{F}(\mathsf{info}_J)$ if $j = J$, or $z := g^{w_j}$ where $w_j \in_R \mathbb{Z}_q^*$, otherwise. (If z has been already defined at query point info_j, return that value.)
  - For all queries to $\mathcal{H}$, ask $\mathcal{H}$.
  - For requests to signing oracle
    - If $\mathcal{U}_B^*$ initiates the signature issuing protocol with regard to info_J, $\mathcal{U}_F^*$ behaves transparently so that $\mathcal{U}_B^*$ can talk with signer.
    - If $\mathcal{U}_B^*$ initiates the signature issuing protocol with regard to info_j where $j \neq J$, $\mathcal{U}_F^*$ simulates a signer by using w_j as above.
- Output what $\mathcal{U}_B^*$ outputs.

$\mathcal{U}_F^*$ is successful if $\mathcal{U}_B^*$ is successful and correct J is chosen so that the final output of $\mathcal{U}_B^*$ is a signature with regard to info_J. Therefore, the success probability of $\mathcal{U}_F^*$ is $\mu/(q_{\mathcal{F}} + q_S)$ where μ is the success probability of $\mathcal{U}_B^*$.

References

Abe, M., and E. Fujisaki (1996). How to date blind signatures. In *Advances in Cryptology – ASIACRYPT'96*, *Lecture Notes in Computer Science*, vol. 1163. Springer-Verlag, Berlin. pp. 244–251.

Abe, M., and J. Camenisch (1997). Partially blind signature schemes. In: *Proceedings of Symposium on Cryptography and Information Security*, SCIS97-33D.

Abe, M., and T. Okamoto (2000). Provably secure partially blind signatures. In *Advances in Cryptology – CRYPTO2000*, *Lecture Notes in Computer Science*, vol. 1880. Springer-Verlag, Berlin. pp. 271–286.

Araki, S., S. Uehara and K. Imamura (1999). The limited verifier signature and its application. *IEICE Trans. Fundamentals*, E82-A(1), 63–68.

Chaum, D. (1982). Blind signatures for untraceable payments. In *Advances in Cryptology – Proceedings of Crypto'82*. Prenum Publishing Corporation, New York. pp. 199–204.

Chaum, D., and H. van Antwerpen (1989). Undeniable signatures. In *Advances in Cryptology – CRYPTO'89*, *Lecture Notes in Computer Science*, vol. 435. Springer-Verlag, Berlin. pp. 212–216.

Chaum, D. (1994). Designated confirmer signatures. In *Advances in Cryptology – EUROCYPT'94*, *Lecture Notes in Computer Science*, vol. 950. Springer-Verlag, Berlin. pp. 86–91.

Chien, H., J. Jan and Y. Tseng (2003). Partially blind threshold signature based on RSA. *Informatica*, **14**(2), 155–166.

Chow, S., L. Hui, S. Yiu and K. Chow (2004). Two Improved partially blind signature schemes from bilinear pairings. Cryptology ePrint Archive 2004/108. Available at `http://eprint.iacr.org`.

Fan, C., and C. Lei (1998). Low-computation partially blind signatures for electronic cash. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E81-A(5), 818–824.

Feige, U., A. Fiat and A. Shamir (1988). Zero-knowledge proofs of identity. *Journal of Cryptology*, **1**, 77–94.

Huang, Z., and Y. Wang (2004). Convertible nominative signatures. In *Information Security and Privacy*: *9th Australasian Conference, ACISP 2004*, *Lecture Notes in Computer Science*, vol. 3108. Springer-Verlag, Berlin. pp. 348–357.

Huang, Z., Z. Chen and Y. Wang (2005). Convertible undeniable partially blind signatures. In *Proceedings of 19th International Conference on Advanced Information Networking and Applications* (*AINA 2005*), vol. 1. IEEE Computer Society Press. pp. 609–614.

Juang, W., and C. Lei (1999). Partially blind threshold signatures based on discrete logarithm. *Computer Communications*, **22**, 73–86.

Kim, S., S. Park and D. Won (1996). Zero-knowledge nominative signatures. In *Proc. of PragoCrypt'96, International Conference on the Theory and Applications of Cryptology*, Prague. pp. 380–392.

Lim, C., and P. Lee (1992). Modified Maurer–Yacobi's scheme and its applications. In *Advances in Cryptology – AUSCRYPT'92*, *Lecture Notes in Computer Science*, vol. 718. Springer-Verlag, Berlin. pp. 308–323.

Maitland, G., and C. Boyd (2002). A provably secure restrictive partially blind signature scheme. In *Public Key Cryptography*, *PKC 2002*, *Lecture Notes in Computer Science*, vol. 2274. Springer-Verlag, Berlin. pp. 99–114.

Miyazaki, S., M. Abe and K. Sakurai (1997). Partially blind signature schemes for the DSS and for a discrete log based message recovery signature. In *Proceedings of Korea–Japan Joint Workshop on Information Security and Cryptology*. pp. 217–226.

Pointcheval, D., and J. Stern (2000). Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, **13**(3), 361–396.

Steinfeld, R., L. Bull, H. Wang *et al.* (2003). Universal designated-verifier signatures. In *Advances in Cryptology-ASIACRYPT 2003*, *Lecture Notes in Computer Science*, vol. 2894. Springer-Verlag, Berlin. pp. 523–542.

Yang, F., and J. Jan (2004). A provably secure scheme for restrictive partially blind signatures. Cryptology ePrint Archive 2004/037. Available at `http://eprint.iacr.org`.

Zhang, F., R. Safavi–Naini and W. Susilo (2003). Efficient verifiably encrypted signature and partially blind signature from bilinear pairings. In *Proceedings of Indocrypt 2003, Lecture Notes in Computer Science*, vol. 2904. Springer-Verlag, Berlin. pp. 191–204.

Zhang, F., R. Safavi–Naini and W. Susilo (2004). Efficient verifiably encrypted signature and partially blind signature from bilinear pairings, revised version. Available at `http://www.uow.edu.au/~fangguo`.

Z. Huang obtained the PhD degree in cryptography from School of Communication Engineering at Xidian University in 2005. Now he is a professor and the director of Department of Computer Science and Engineering at Zhangzhou Normal University. His current research interests focus on the areas of cryptography, electronic commerce security, and network security etc.

K. Chen obtained the BS and the MS degrees in applied mathematics from Xidian University in 1982 and 1985, respectively, and the PhD degree from Justus–Liebig University, Germany, in 1994. Now he is a professor and a doctoral supervisor of Department of Computer Science and Engineering, a vice dean of School of Information Security Engineering, the director of Cryptography and Information Security Lab at Shanghai Jiao Tong University. His current research interests focus on the areas of cryptography and information security, especially in public key cryptography, authentication, digital signature, block cipher, digital watermarking, networks security, electronic commerce, and coding theory etc.

Y. Wang is a professor and a doctoral supervisor at Xidian University, a senior member of IEEE, a fellow of the Chinese Institute of Communication, a fellow of the Chinese Institute of Electronics, and a member of the Board of Governors of the Chinese Institute of Cryptography. His research interests focus on the areas of the general theory of communication, information theory, coding, cryptography, and network security.

Įrodomai saugūs dalinai akli parašai su vartotojo paskirtu patvirtintoju

Zhenjie HUANG, Kefei CHEN, Yumin WANG

Šis straipsnis pristato naują dalinai aklo parašo su vartotojo paskirtu patvirtintoju sąvoką, kurioje tik vartotojo paskirtas patvirtintojas ir pats vartotojas gali patikrinti ir patvirtinti parašo galiojimą ir paversti parašą viešai patikrinamu. Tokia sąvoka yra formaliai apibrėžta ir konkreti įrodomai saugi schema yra pasiūlyta bei pateiktas jos saugumo įrodymas ir trumpa efektyvumo analizė. Pasiūlyta schema yra nesuklastojama adaptyviai parinktų pranešimų atakos.