NTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2021.15.88 Volume 15, 2021

Key Protected Deputy Signature Scheme against the Deputy Signing Key Exposure

Jianhong Chen
Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huaian 223003, Jiangsu, China

Kun Yu
Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huaian 223003, Jiangsu, China

Wenhao Wang
Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huaian 223003, Jiangsu, China

Received: January 19, 2021. Revised: July 16, 2021. Accepted: July 28, 2021. Published: July 30, 2021.

***Abstract*—Key exposure is very harmful to a cryptographic system. To decrease the loss from the deputy signing key vulnerability in identity-based proxy signature systems, we propose the method of key protected deputy signature (IBKPDS) using the method of parallel key insulation. The proposed IBKPDS is based on identities and is shown to be secure with the cryptographic proof. In the proof, there is no random oracle. In an IBKPPS crypto-system, a user stores his short-lived deputy signing key by himself and saves two long-lived keys in two heavily guarded boxes respectively. The derived IBKPDS cryptographic system is heavily key-separated. A thief who wants to obtain crucial information can not corrupt the IBKPDS when he get only one long-lived key. In addition, the user can change the short-lived deputy signing keys frequently at low risk.**

.

***Keywords*—Identity, key-separated, long-lived key, deputy signature, low risk.**

I. INTRODUCTION

LOSS of secret keys is dangerous to the security of the public key cryptosystem [1,2]. It is import to rescind users for PKI or Identity-based setting in the settings of the loss of their private keys. When lots of users renew their proprietary keys at short intervals,, communication and computation overhead will make the PKI authority unbearable. Several complementary approaches are to evolve secret keys in case where secrets are in danger [3]. One of the key evolving notions is forward security. In the model of forward security, the opponent is unable to compromise secret keys associated with prior time periods. Another key evolving notions is key insulation mechanism. In the case of key insulation, there are two classes of private keys, i.e. long-lives keys and short-lives keys. A user stores his long-lives keys by himself and saves short-lives keys in a heavily guarded box. The notion of parallel key insulation complements the notion of key insulation. In the setting of parallel key insulation, the user uses different independent helper keys in key evolving operations. In a Parallel key-separated crypto-system, a user stores his long-lives keys by himself and saves two short-lived keys in two physically-secure computationally-limited devices respectively.

In cryptography digital signature [4,5] employs the advanced mathematical technique to check the authenticity of digital messages. In the system of proxy signature [6], there are a foremost signer and a deputy signer. In the event that the foremost signer appoints a deputy signer or an agent to sign papers, the foremost signer should submit a letter of authorization or a warrant to the agent [7]. In a blind signature system [8], the verifier verifies against the original, unblinded message while the signer signs a disguised (blinded) message. Blind signatures are is very useful when the signer and message author are different parties. Deputy sightless signature [9,10] enjoys the advantage of the proxy signature and the merit of sightless signature. In an application system of deputy sightless signature, the deputy signer produces a blind sightless for the foremost signer. The deputy re-signature [11,12] is similar to the deputy signature. In a deputy re-signature system, Jeff is not a fully trusted agent and works as an interpreter between Mary and Tom. To interpret, Jeff changes an old signature into a new signature. The old signature is Mary's signature. The new signature is Tom's signature. Jeff can neither sign in the name of Mary nor sign in the name of Tom because Jeff doesn't know their personal signing keys. In a deputy signature system, Jeff work as a trusted deputy of Mary and can sign arbitrary messages in the name of Mary. Proxy signcryption [13] integrates the functions of signcryption and proxy signature.

Against the deputy key vulnerability in identity-based

deputy signature systems, we propose a construction method of a key protected deputy signature based on identity (IBKPDS) scheme using the method of parallel key insulation. The proposed IBKPPIS method is are shown to be secure with the cryptographic proof.

II. Model of IBKPPIS

A. Our proposed IBKPPIS model

In the system of the IBKPDS, there are some steps as below:

• Setup: The public agency computes the main privy constant and some overt constants. Then the public agency gives the main privy constant and some overt constants to the people involved.

· Ext: The Private Key Generator computes the deputy signer's first short-lived secret key, two long-lived refreshing keys of the deputy signer and the foremost signer's long-lived secret key.

• DUpdateLongLived: The deputy signer computes his short-lived refreshing key for time period *t* using his short-lived device.

• DUpdateUser: The deputy signer computes his short-lived secret key for time period *t* using his short-lived device

• DelegGen: The foremost signer computes the deputy document.

• DelegVerify: The verifier of the proxy document checks whether the deputy document is valid.

• GenPSig: The deputy signer computes the short-lived deputy signing key using his short-lived secret key and the valid deputy document above.

• PSignatureVerify: The deputy signer computes the deputy signature for the designated length of time using his short-term deputy signing key and his deputy document.

• PVerification: The verifier of proxy document verifier checks whether the deputy signature for the designated length of time is valid.

B. the Isolation of the Short-lived Deputy Signing Keys

We use a match between a defier and an opponent to simulate the scenario in which the short-lived deputy signing Keys is isolated against the corruption of the opponent. The match in which the defier competes with opponent is shown as below.

·Setup. The defier computes the main privy constant and some overt constants. The main privy constant and some overt constants are kept by the defier and the opponent respectively.

·Queries. The opponent asks the defier many times for the answers of some questions.

① Questions about Ext. The defier computes the foremost secret key, the earliest deputy signing key and helper keys of the deputy signer. The defier computes the secret key of the foremost signer. The overt constants are stored by the opponent. The opponent keeps the foremost signing key, the earliest deputy signing key and helper keys.

② Questions about the deputy document. The defier computes the deputy document. The opponent keeps the deputy document.

③ Questions about the short-lived deputy signing key. The defier computes the short-lived deputy signing key. The opponent keeps the short-lived deputy signing key.

④ Questions about the deputy signature. The defier computes the deputy signature. The opponent keeps deputy signature

·Counterfeit. The opponent counterfeits the deputy document and the signature. If the statements below are valid, the opponent defeats the defier in the match above.

① The opponent makes a counterfeited typle, (Ψ^*, τ^*, φ^*, p^*) and (Ψ^*, τ^*) is the deputy document of time period τ^* if the statements below are valid: DVerification (p^*,t^*, Ψ^*)=1; the attacked identity of the foremost signer was not involved in the questions about Ext; $\langle p^*,\tau^*,\varphi^*\rangle$ was was not involved in the questions about the deputy document; $\langle p^*,t^*,\Psi^*\rangle$ was not ivolved in the questions about the short-lived deputy signing keys.

② The opponent makes a counterfeited typle (Ψ^*, τ^*,$\xi_p{}^*$,m^*) when the statements below are valid: PVerification ((m^*, τ^*,$\xi_p{}^*$), f^*,p^*)=1 and *f** and *p** are the foremost signer and the deputy signer respectively written in Ψ^*; p^* was not involved in the questions about Ext; $\langle p^*,\tau^*,W^*\rangle$ was not ivolved in the questions about the short-lived deputy signing keys; $\langle \tau^*,\Psi^*,m^*\rangle$ was not ivolved in the questions about the deputy signature.

C. the forceful isolation of the Short-lived Deputy Signing Key

We use a match between a defier and an opponent to simulate the scenario in which the short-lived deputy signing Keys is forcefully isolated against the corruption of the opponent. The match in which the defier competes with opponent is shown as below.

·Setup. The defier computes the main privy constant and some overt constants. The main privy constant and some overt constants are kept by the defier and the opponent respectively.

·Queries. The opponent asks the defier many times for the answers of some questions..

① Questions about Ext. The same as that of the Isolation of the short-lived deputy signing keys.

② Questions about the deputy document. The same as that of the Isolation of the short-lived deputy signing keys.

③ Short-lived deputy signing key queries. the Isolation of the short-lived deputy signing keys.

④ Questions about Deputy signing. the Isolation of the short-lived deputy signing keys.

⑤ Questions about Deputy short-lived keys of the deputy signer. the Isolation of the short-lived deputy signing keys.

·Counterfeit. The opponent counterfeits the deputy document and the signature. If the statements are valid, the opponent defeats the defier in the match above.

① The opponent makes a counterfeited typle, (Ψ^*, τ^*, φ^*, p^*) and (Ψ^*, τ^*) is the deputy document of time period τ^* if the statements below are valid: DVerification (p^*,τ^*,Ψ^*)=1; the attacked identity of the foremost signer was not involved in the questions about Ext; $\langle p^*,\tau^*,\varphi^*\rangle$ was was not involved in the questions about the deputy document; $\langle p^*,\tau^*,\Psi^*\rangle$ was not ivolved in the questions about the short-lived deputy signing keys.

② The opponent makes a counterfeited typle (Ψ^*, τ^*,$\xi_p{}^*$,m^*) when the statements below are valid: PVerification ((m^*, τ^*,$\xi_p{}^*$), f^*,p^*)=1 and f^* and p^* are the foremost signer and the deputy signer respectively written in Ψ^*; p^* was not involved in the questions about Ext; $\langle p^*,\tau^*,\Psi^*\rangle$ was not ivolved in the questions about the short-lived deputy signing keys; $\langle \tau^*,\Psi^*,m^*\rangle$ was not involved in the questions about the deputy signature.

III. Our Proposed IBKPDS

We propose a scheme of the identity-based key protected deputy signature (IBKPDS). Our method is to combine the scheme of Feng Cao et al.'s IBPS(proxy signature based on identity) with the scheme of Jian Weng et al.'s IBPKSS (parallel key-separated signature based on identity) which introduced the method of parallel key-isolation into IBS (signature based on identity).

We show IBS (signature based on identity) as below.

(1) Su: $\Omega 1$ is a cyclic group of multiplication. The order of $\Omega 1$ is a prime number. $\Omega 2$ is a cyclic group of multiplication. The order of $\Omega 2$ is a prime number. $\Omega 1\times\Omega 1\rightarrow\Omega 2$ is a bilinear pairing $\hat{p}$ of which the generator is η. We pick a random integer a. $\eta 1$ is η to the power of a. We pick a random integer $\eta 2$ from Ω_1. We pick a random integer $\varpi 1$. $F_{\varpi 1}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. We pick a random integer $\varpi 2$. $F_{\varpi 2}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. $F_{\varpi 1}$ is used to modify the length of the identity to the user's defined length. $F_{\varpi 2}$ is used to modify the length of a message to the user's defined length. We pick a random integer a. η_1 is equal η^a. η_2, $\varpi 1'$ and $\varpi 2'$ are random integers from Ω_1. The vector Φ is equal to (ϕ_t). The length of Φ is $\varpi 1$. The vector Γ is equal to (γ_t). The length of Γ is $\varpi 2$. $\Omega 1$, $\Omega 2$, $\hat{p}$, η, η_1, η_2, $\varpi 1'$, Φ, $\varpi 2'$, Γ, $\varpi 3'$ and Ψ are the overt constants. Then the public agency gives the main privy constant and some overt constants to the people involved.

(2) Ext: The identity ϕ is a string of many bits. The length of ϕ is $\varpi 1$. ϕ_t is the tth bit of ϕ. Φ_ϕ is equal to the set of the subscript ι, in which ϕ_t is equal to 1. The elements of Φ_ϕ are integers which are less than $\varpi 1$ and bigger than 1. The public agency randomly chooses a positive integer β_ϕ and sets the users privy signing key as

$$\lambda_\phi=(\lambda_{\phi 1},\lambda_{\phi 2})=(\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_\phi}\phi_t)^{\beta_\phi},\eta^{\beta_\phi}).$$

(3)SignatureGen: The message γ is a string of many bits. The length of γ is $\varpi 2$. γ_t is the tth bit of γ. Γ_γ is equal to the set of the subscript ι, in which γ_t is equal to 1. The elements of Γ_γ are integers which are less than $\varpi 2$ and bigger than 1. The signer randomly chooses a positive integer β_γ and sets his overt signature as

$$\begin{aligned}S &= (S_1,S_2,S_3)\\ &= (\lambda_{\phi 1}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_t)^{\beta_\gamma},\lambda_{\phi 2},\eta^{\beta_\gamma})\\ &= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_\phi}\phi_t)^{\beta_\phi}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_t)^{\beta_\gamma},\eta^{\beta_\phi},\eta^{\beta_\gamma})\end{aligned}$$

(4) SignatureVerify: The user who wants to check the validity of a signature S parses the signature as (S_1,S_2,S_3) at first. Then he checks the truth of the equation below.

$$\hat{p}(S_1,\eta)=\hat{p}(\eta_1,\eta_2)^2\,\hat{p}((\varpi 1'\prod_{\iota\in\Phi_\phi}\phi_t)^{\beta_\phi},S_2)\,\hat{p}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_t)^{\beta_\gamma},S_3)$$

We show Feng Cao et al.'s IBPS ((proxy signature based on identity) as below.

(1) Su: $\Omega 1$ is a cyclic group of multiplication. The order of $\Omega 1$ is a prime number. $\Omega 2$ is a cyclic group of multiplication. The order of $\Omega 2$ is a prime number. $\Omega 1\times\Omega 1\rightarrow\Omega 2$ is a bilinear pairing $\hat{p}$ of which the generator is η. We pick a random integer a. $\eta 1$ is η to the power of a. We pick a random integer $\eta 2$ from Ω_1. We pick a random integer $\varpi 1$. $F_{\varpi 1}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. We pick a random integer $\varpi 2$. $F_{\varpi 2}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. We pick a random integer $\varpi 3$. $F_{\varpi 3}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 3}$ is a function that is of hash and against collision. $F_{\varpi 1}$ is used to modify the length of the identity to the user's defined length. $F_{\varpi 2}$ is used to modify the length of a message to the user's defined length. $F_{\varpi 3}$ is used to modify the length of a deputy documentto the user's defined length. We pick a random integer a. η_1 is equal η^a. η_2, $\varpi 1'$, $\varpi 2'$ and $\varpi 3'$ are random integers from Ω_1. The vector Φ is equal to (ϕ_t). The length of Φ is $\varpi 1$. The vector Γ is equal to (γ_t). The length of Γ is $\varpi 2$. The vector Ψ is equal to (ψ_t). The length of Γ is $\varpi 3$. $\Omega 1$, $\Omega 2$, $\hat{p}$, η, η_1, η_2, $\varpi 1'$, Φ, $\varpi 2'$, Γ, $\varpi 3'$ and Ψ are the overt constants. Then the public agency gives the main privy constant and some overt constants to the people involved.

(2) Ext: The foremost signer's identity ϕf is a string of many bits. The length of ϕf is $\varpi 1$. ϕ_t is the tth bit of ϕf. $\Phi_{\phi f}$ is equal to the set of the subscript ι, in which ϕf_t is equal to 1. The elements of $\Phi_{\phi f}$ are integers which are less than $\varpi 1$ and bigger than 1. The public agency randomly chooses a positive integer $\beta_{\phi f}$ and sets the foremost signer's privy signing key as

$$\lambda_{\phi f}=(\lambda_{\phi f1},\lambda_{\phi f2})=(\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_t)^{\beta_{\phi f}},\eta^{\beta_{\phi f}}).$$

The deputy signer's identity ϕp is a string of many bits. The length of ϕp is $\varpi 1$. ϕ_t is the tth bit of ϕp. $\Phi_{\phi p}$ is equal to the set of the subscript ι, in which ϕp_t is equal to 1. The elements of $\Phi_{\phi p}$ are integers which are less than $\varpi 1$ and bigger than 1. The public agency randomly chooses a positive integer $\beta_{\phi p}$ and sets the deputy signer's privy signing key as

$$\lambda_{\phi p}=(\lambda_{\phi p1},\lambda_{\phi p2})=(\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_t)^{\beta_{\phi p}},\eta^{\beta_{\phi p}}).$$

(3) DelegGen: The authorization ψ is a string of many bits. The length of ψ is $\varpi 3$. ψ_t is the tth bit of ψ. Ψ_ψ is equal to the set of the subscript t, in which ψ_t is equal to 1. The elements of Ψ_ψ are integers which are less than $\varpi 3$ and bigger than 1. The signer randomly chooses a positive integer β_ψ and sets his overt deputy document as

$$\begin{aligned} S_\psi &= (S_{\psi 1}, S_{\psi 2}, S_{\psi 3}) \\ &= (\lambda_{\phi f 1}(\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta_\psi}, \lambda_{\phi f 2}, \eta^{\beta_\psi}) \\ &= (\eta_2^a (\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi_t)^{\beta_{\phi f}} (\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta_\psi}, \eta^{\beta_{\phi f}}, \eta^{\beta_\psi}) \end{aligned}$$

Then the foremost signer gives the deputy tuple (ψ,S_ψ) to the deputy signer.

(6) DelegVerify: The deputy signer who wants to check the validity of a deputy document S_ψ parses the deputy document as ($S_{\psi 1}$, $S_{\psi 2}$, $S_{\psi 3}$) at first. Then he checks the truth of the equation below.

$$\hat{p}(S_{\psi 1}, \eta) = \hat{p}(\eta_1, \eta_2)^2 \, \hat{p}((\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi_t)^{\beta_{\phi f}}, S_{\psi 2}) \hat{p}((\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta_\psi}, S_{\psi 3})$$

(7) GenPSig: If the deputy signer accepts the deputy document S_ψ, he randomly chooses a positive integer β'_ψ and constructs his deputy signing key as

$$\begin{aligned} & tdsk \\ &= (tdsk_1, tdsk_2, tdsk_3, tdsk_4) \\ &= (S_{\psi 1}\lambda_{\phi p 1}(\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta'_\psi}, S_{\psi 2}, \lambda_{\phi p 2}, S_{\psi 3}\eta^{\beta'_\psi}) \\ &= (\eta_2^a (\varpi 1' \prod_{t\in\Phi_{\phi p}} \phi_t)^{\beta_{\phi p}} (\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta_\psi} \eta_2^a (\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi_t)^{\beta_{\phi f}} \\ &\quad (\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta'_\psi}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi}\eta^{\beta'_\psi}) \\ &= (\eta_2^{2a} (\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi_t)^{\beta_{\phi f}} (\varpi 1' \prod_{t\in\Phi_{\phi p}} \phi_t)^{\beta_{\phi p}} (\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta_\psi + \beta'_\psi}, \\ &\quad \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi + \beta'_\psi}) \end{aligned}$$

(8) PSignatureGen: The message γ is a string of many bits. The length of γ is $\varpi 2$. γ_t is the tth bit of γ. Γ_γ is equal to the set of the subscript t, in which γ_t is equal to 1. The elements of Γ_γ are integers which are less than $\varpi 2$ and bigger than 1. The deputy signer randomly chooses a positive integer β_γ and sets his overt deputy signature as

$$\begin{aligned} S_\gamma &= (S_{\gamma 1}, S_{\gamma 2}, S_{\gamma 3}, S_{\gamma 4}, S_{\gamma 5}) \\ &= (tdsk_1 (\varpi 2' \prod_{t\in\Gamma_\gamma} \gamma_t)^{\beta_\gamma}, tdsk_2, tdsk_3, tdsk_4, \eta^{\beta_\gamma}) \\ &= (\eta_2^{2a} (\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi_t)^{\beta_{\phi f}} (\varpi 1' \prod_{t\in\Phi_{\phi p}} \phi_t)^{\beta_{\phi p}} (\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta_\psi + \beta'_\psi} \\ &\quad (\varpi 2' \prod_{t\in\Gamma_\gamma} \gamma_t)^{\beta_\gamma}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi + \beta'_\psi}, \eta^{\beta_\gamma}) \\ &= (\eta_2^{2a} (\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi_t)^{\beta_{\phi f}} (\varpi 1' \prod_{t\in\Phi_{\phi p}} \phi_t)^{\beta_{\phi p}} (\varpi 3' \prod_{t\in\Psi_\psi} \psi_t)^{\beta''_\psi} \\ &\quad (\varpi 2' \prod_{t\in\Gamma_\gamma} \gamma_t)^{\beta_\gamma}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta''_\psi}, \eta^{\beta_\gamma}), \end{aligned}$$

in which β''_ψ is equal to the sum of β_ψ and β'_ψ.

(9) PSignatureVerify: The user who wants to check the validity of a deputy signature S_γ parses the deputy signature as ($S_{\gamma 1}$, $S_{\gamma 2}$, $S_{\gamma 3}$, $S_{\gamma 4}$, $S_{\gamma 5}$) at first. Then he checks the truth of the equation below.

$$\begin{aligned} & \hat{p}(S_{\gamma 1}, \eta) \\ &= \hat{p}(\eta_1, \eta_2)^2 \, \hat{p}(\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi_t, S_{\psi 2}) \hat{p}(\varpi 1' \prod_{t\in\Phi_{\phi p}} \phi_t, S_{\psi 3}) \hat{p}(\varpi 3' \prod_{t\in\Psi_\psi} \psi_t, S_{\gamma 4}) \\ &\quad \hat{p}(\varpi 2' \prod_{t\in\Gamma_\gamma} \gamma_t, S_{\gamma 5}) \end{aligned}$$

We show the proposed IBKPDS as below.

(1) Su: $\Omega 1$ is a cyclic group of multiplication. The order of $\Omega 1$ is a prime number. $\Omega 2$ is a cyclic group of multiplication. The order of $\Omega 2$ is a prime number. $\Omega 1 \times \Omega 1 \rightarrow \Omega 2$ is a bilinear pairing $\hat{p}$ of which the generator is η. We pick a random integer a. $\eta 1$ is η to the power of a. We pick a random integer $\eta 2$ from Ω_1. We pick a random integer $\varpi 1$. $F_{\varpi 1}: \{0,1\}^* \rightarrow \{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. We pick a random integer $\varpi 2$. $F_{\varpi 2}: \{0,1\}^* \rightarrow \{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. We pick a random integer $\varpi 3$. $F_{\varpi 3}: \{0,1\}^* \rightarrow \{0,1\}^{\varpi 3}$ is a function that is of hash and against collision. $F_{\varpi 1}$ is used to modify the length of the identity to the user's defined length. $F_{\varpi 2}$ is used to modify the length of a message to the user's defined length. $F_{\varpi 3}$ is used to modify the length of a deputy documentto the user's defined length. We pick a random integer a. η_1 is equal η^a. η_2, $\varpi 1'$, $\varpi 2'$ and $\varpi 3'$ are random integers from Ω_1. The vector Φ is equal to (ϕ_t). The length of Φ is $\varpi 1$. The vector Γ is equal to (γ_t). The length of $\Gamma$is $\varpi 2$. The vector Ψ is equal to (ψ_t). The length of $\Gamma$is $\varpi 3$. $\Omega 1$, $\Omega 2$, $\hat{p}$, η, η_1, η_2, $\varpi 1'$, Φ, $\varpi 2'$, Γ, $\varpi 3'$ and Ψ are the overt constants. Then the public agency gives the main privy constant and some overt constants to the people involved.

(2) Ext: The foremost signer's identity ϕf is a string of many bits. The length of ϕf is $\varpi 1$. Φ_t is the tth bit of ϕf. $\Phi_{\phi f}$ is equal to the set of the subscript t, in which ϕf_t is equal to 1. The elements of $\Phi_{\phi f}$ are integers which are less than $\varpi 1$ and bigger than 1. The public agency randomly chooses a positive integer $\beta_{\phi f}$ and sets the foremost signer's privy signing key as

$$\lambda_{\phi f} = (\lambda_{\phi f 1}, \lambda_{\phi f 2}) = (\eta_2^a (\varpi 1' \prod_{t\in\Phi_{\phi f}} \phi f_t)^{\beta_{\phi f}}, \eta^{\beta_{\phi f}}).$$

The deputy signer's identity ϕp is a string of many bits. The length of ϕp is $\varpi 1$. ϕ_t is the tth bit of ϕp. $\Phi_{\phi p}$ is equal to the set of the subscript t, in which ϕp_t is equal to 1. The elements of $\Phi_{\phi p}$ are integers which are less than $\varpi 1$ and bigger than 1. ($-1, \phi p$) is a string of many bits. The length of ($-1, \phi p$) is $\varpi 1$. ϕ_t is the tth bit of ($-1, \phi p$). $\Phi_{-1,\phi p}$ is the output of $F_{\varpi 1}(-1 \| \phi p)$ and equal to the set of the subscript t, in which ϕ_t is equal to 1. The elements of $\Phi_{-1,\phi}$ are integers which are less than $\varpi 1$ and bigger than 1. ($0, \phi p$) is a string of many bits. The length of ($0, \phi p$) is $\varpi 1$. ϕ_t is the tth bit of ($0, \phi p$). $\Phi_{0,\phi p}$ is the output of $F_{\varpi 1}(-1 \| \phi p)$ and equal to the set of the subscript t, in which ϕ_t is equal to 1. The elements of $\Phi_{0,\phi}$ are integers which are less than $\varpi 1$ and bigger than 1. The public agency randomly chooses hp' and hp'' from $\{0,1\}^\kappa$. The function FP is random and pseud. $k_{-1,\phi p}$ is equal to $FP_{hp'}$ ($-1 \| \phi p$). $k_{0,\phi p}$ is equal to $FP_{hp''}$ ($0 \| \phi p$). The public agency randomly chooses a positive integers, $\beta_{\phi p}$, and sets the deputy signer's short-lived privy signing key for time slot 0 as

$$\begin{aligned} & \lambda_{0,\phi p} \\ &= (\lambda_{0,\phi p 1}, \lambda_{0,\phi p 2}, \lambda_{0,\phi p 3}, \lambda_{0,\phi p 4}) \end{aligned}$$

$$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{-1,\phi p}}\phi_\iota)^{k_{-1,\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{0,\phi p}}\phi_\iota)^{k_{0,\phi p}},$$
$$\eta^{k_{-1,\phi p}},\eta^{k_{0,\phi p}},\eta^{\beta_{\phi p}})$$

(3) DUpdateLongLived: $(\tau\text{-}2,\phi p)$ is a string of many bits. The length of $(\tau\text{-}2,\phi p)$ is $\varpi 1$. ϕ_ι is the ιth bit of $(\tau\text{-}2,\phi p)$. $\Phi_{\tau\text{-}1,\phi p}$ is the output of $F_{\varpi 1}(\tau\text{-}2\|\phi p)$ and equal to the set of the subscript ι, in which ϕ_ι is equal to 1. The elements of $\Phi_{\tau\text{-}2,\phi}$ are integers which are less than $\varpi 1$ and bigger than 1. $(\tau,\phi p)$ is a string of many bits. The length of $(\tau,\phi p)$ is $\varpi 1$. ϕ_ι is the ιth bit of $(\tau,\phi p)$. $\Phi_{\tau,\phi p}$ is the output of $F_{\varpi 1}(\tau\|\phi p)$ and equal to the set of the subscript ι, in which ϕ_ι is equal to 1. The elements of $\Phi_{\tau,\phi}$ are integers which are less than $\varpi 1$ and bigger than 1. $k_{\tau\text{-}2,\phi p}$ is equal to $FP_{hp'}$ $(\tau\text{-}2\|\phi p)$. $k_{\tau,\phi p}$ is equal to $FP_{hp'}$ $(\tau\|\phi p)$. The deputy signer sets his privy short-lived refreshing key for time slot τ as

$tui_{\tau,\phi p} = (tui_{\tau,\phi p1}, tui_{\tau,\phi p2})$
$= ((\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_\iota)^{k_{\iota,\phi p}} / (\varpi 1'\prod_{\iota\in\Phi_{\tau-2,\phi p}}\phi_\iota)^{k_{\tau-2,\phi p}},\ \eta^{k_{\tau,\phi p}})$

(4) DUpdateUser: Using his privy short-lived refreshing key, $tui_{\tau,\phi p}$, for time slot τ, the deputy signer sets his short-lived privy signing key for time slot τ as

$\lambda_{\tau,\phi p}$
$= (\lambda_{\tau,\phi p1}, \lambda_{\tau,\phi p2}, \lambda_{\tau,\phi p3}, \lambda_{\tau,\phi p4})$
$= (\lambda_{\tau\text{-}1,\phi p1}\ tui_{\tau,\phi p1}, \lambda_{\tau\text{-}1,\phi p3}, tui_{\tau,\phi p2}, \lambda_{\tau\text{-}1,\phi p4})$
$= (\lambda_{\tau\text{-}1,\phi p1}\ tui_{\tau,\phi p1}, \lambda_{\tau\text{-}1,\phi p2}, tui_{\tau,\phi p2}, \lambda_{\tau\text{-}1,\phi p4})$
$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau-2,\phi p}}\phi_\iota)^{k_{\tau-2,\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau-1,\phi p}}\phi_\iota)^{k_{\tau-1,\phi p}}$
$(\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_\iota)^{k_{\iota,\phi p}} / (\varpi 1'\prod_{\iota\in\Phi_{\tau-2,\phi p}}\phi_\iota)^{k_{\tau-2,\phi p}}, \eta^{k_{\tau-1,\phi p}}, \eta^{k_{\tau,\phi p}}, \eta^{\beta_{\phi p}})$.
$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau-1,\phi p}}\phi_\iota)^{k_{\tau-1,\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_\iota)^{k_{\tau,\phi p}},$
$\eta^{k_{\tau-1,\phi p}},\eta^{k_{\tau,\phi p}},\eta^{\beta_{\phi p}})$

(5) DelegGen: The authorization ψ is a string of many bits. The length of ψ is $\varpi 3$. ψ_ι is the ιth bit of ψ. Ψ_ψ is equal to the set of the subscript ι, in which ψ_ι is equal to 1. The elements of Ψ_ψ are integers which are less than $\varpi 3$ and bigger than 1. The signer randomly chooses a positive integer β_ψ and sets his overt deputy document as

S_ψ
$= (S_{\psi 1}, S_{\psi 2}, S_{\psi 3})$
$= (\lambda_{\phi f1}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta_\psi}, \lambda_{\phi f2}, \eta^{\beta_\psi})$
$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta_\psi}, \eta^{\beta_{\phi f}}, \eta^{\beta_\psi})$

Then the foremost signer gives the deputy tuple (ψ,S_ψ) to the deputy signer.

(6) DelegVerify: DelegVerify: The deputy signer who wants to check the validity of a deputy document S_ψ parses the deputy document as $(S_{\psi 1}, S_{\psi 2}, S_{\psi 3})$ at first. Then he checks the truth of the equation below.

$$\hat{p}(S_{\psi 1},\eta) = \hat{p}(\eta_1,\eta_2)^2\ \hat{p}((\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}, S_{\psi 2})\ \hat{p}((\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta_\psi}, S_{\psi 3})$$

(7) GenPSig: If the deputy signer accepts the deputy document S_ψ, he randomly chooses three positive integers β'_ψ, $\beta''_{\tau-1}$, β''_τ, and constructs his short-lived deputy signing key for time slot τ as

$tdsk$
$=(tdsk_{\tau 1}, tdsk_{\tau 2}, tdsk_{\tau 3}, tdsk_{\tau 4}, tdsk_{\tau 5}, tdsk_{\tau 6})$
$= (S_{\psi 1}\lambda_{\tau,\phi p1}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{\beta''_{\tau-1}}(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{\beta''_\tau}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta'_\psi},$
$\lambda_{\tau,\phi p2}\eta^{\beta''_{\tau-1}}, \lambda_{\tau,\phi p3}\eta^{\beta''_\tau}, S_{\psi 2}, \lambda_{\tau,\phi p4}, S_{\psi 3}\eta^{\beta'_\psi})$
$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta'_\psi}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{\beta''_{\tau-1}}\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}$
$(\varpi 1'\prod_{\iota\in\Phi_{\tau-1,\phi p}}\phi_\iota)^{k_{\tau-1,\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_\iota)^{k_{\tau,\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{\beta''_\tau}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta'_\psi},$
$\eta^{k_{\tau-1,\phi p}}\eta^{r''_{\tau-1}}, \eta^{k_{\tau,\phi p}}\eta^{r''_t}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi}\eta^{\beta'_\psi})$
$= (\eta_2^{2a}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{\beta''_{\tau-1}+k_{\tau-1,\phi p}}$
$(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{\beta''_\tau+k_{\tau,\phi p}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta_\psi+\beta'_\psi},$
$\eta^{k_{\tau-1,\phi p}+\beta''_{\tau-1}}, \eta^{k_{\tau,\phi p}+\beta''_\tau}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi+\beta'_\psi})$

(8) PSignatureGen: The message γ is a string of many bits. The length of γ is $\varpi 2$. γ_ι is the ιth bit of γ. Γ_γ is equal to the set of the subscript ι, in which γ_ι is equal to 1. The elements of Γ_γ are integers which are less than $\varpi 2$ and bigger than 1. The deputy signer randomly chooses three positive integers β_γ, $\beta'''_{\tau-1}$, β'''_τ, and sets his overt deputy signature for time slot τ as

$S_{\tau,\gamma}$
$= (S_{\tau,\gamma 1}, S_{\tau,\gamma 2}, S_{\tau,\gamma 3}, S_{\tau,\gamma 4}, S_{\tau,\gamma 5}, S_{\tau,6}, S_{\tau,\gamma 7})$
$= (tdsk_{\tau 1}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{\beta'''_{\tau-1}}(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{\beta'''_\tau}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota)^{\beta_\gamma},$
$tdsk_{\tau 2}\eta^{r'''_{t-1}}, tdsk_{\tau 3}\eta^{r'''_t}, tdsk_{\tau 4}, tdsk_{\tau 5}, tdsk_{\tau 6}, \eta^{\beta_\gamma})$
$= (\eta_2^{2a}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{\beta''_{\tau-1}+k_{\tau-1,\phi p}}$
$(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{\beta''_\tau+k_{\tau,\phi p}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta_\psi+\beta'_\psi}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{\beta'''_{\tau-1}}$
$(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{\beta'''_\tau}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota)^{\beta_\gamma}, \eta^{k_{\tau-1,\phi p}+\beta''_{\tau-1}}\eta^{r'''_{t-1}},$
$\eta^{\beta''_\tau+k_{\tau,\phi p}}\eta^{r'''_t}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi+\beta'_\psi}, \eta^{\beta_\gamma})$
$= (\eta_2^{2a}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{k_{\tau-1,\phi p}+\beta''_{\tau-1}+\beta'''_{\tau-1}}$
$(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{k_{\tau,\phi p}+\beta''_\tau+\beta'''_\tau}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta_\psi+\beta'_\psi}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota)^{\beta_\gamma},$
$\eta^{k_{\tau-1,\phi p}+\beta''_{\tau-1}+\beta'''_{\tau-1}}, \eta^{k_{\tau,\phi p}+\beta''_\tau+\beta'''_\tau}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi+\beta'_\psi}, \eta^{\beta_\gamma})$
$= (\eta_2^{2a}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{k'_{\tau-1,\phi p}}$
$(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{k'_{\tau,\phi p}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta''_\psi}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota)^{\beta_\gamma},$
$\eta^{k'_{\tau-1,\phi p}}, \eta^{k'_{\tau,\phi p}}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta''_\psi}, \eta^{\beta_\gamma}),$
in which $\beta''_\omega = \beta_\psi + \beta'_\psi, k'_{\tau-1,\phi p} = k_{\tau-1,\phi p} + \beta''_{\tau-1} + \beta'''_{\tau-1},$
$k'_{\tau,\phi p} = k_{\tau,\phi p} + \beta''_\tau + \beta'''_\tau$.

(9) PSignatureVerify: The user who wants to check the validity of a deputy signature $S_{\tau,\gamma}$ for the time slot τ parses the deputy signature as $(S_{\tau,\gamma 1}, S_{\tau,\gamma 2}, S_{\tau,\gamma 3}, S_{\tau,\gamma 4}, S_{\tau,\gamma 5}, S_{\tau,\gamma 6}, S_{\tau,\gamma 7})$ at first. Then he checks the truth of the equation below.

$$\hat{p}(S_{\tau,\gamma 1},\eta)$$

$$= \hat{p}(\eta_1,\eta_2)^2\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota, S_{\tau,\gamma 4})\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota, S_{\tau,\gamma 5})$$
$$\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota, S_{\tau,\gamma 2})\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota, S_{\tau,\gamma 3})\,\hat{p}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota, S_{\gamma 6})$$
$$\hat{p}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota, S_{\gamma 7})$$

We show the truth of the computation of the proposed deputy signature above for the time slot τ with two long-lived devices as below.

$$\hat{p}(S_{\tau,\gamma 1},\eta)$$
$$= \hat{p}((\eta_2^{2a}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{k'_{\tau-1,\phi p}}$$
$$(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{k'_{\tau,\phi p}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta''_\psi}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota)^{\beta_\gamma},\eta)$$
$$= \hat{p}(\eta_2^{2a},\eta)\,\hat{p}((\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota)^{\beta_{\phi f}},\eta)\,\hat{p}((\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}},\eta)$$
$$\hat{p}((\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota)^{k'_{\tau-1,\phi p}},\eta)\,\hat{p}((\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota)^{k'_{\tau,\phi p}},\eta)$$
$$\hat{p}((\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota)^{\beta''_\psi},\eta)\,\hat{p}((\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota)^{\beta_\gamma},\eta)$$
$$= \hat{p}(\eta_1,\eta_2)^2\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota,\eta^{\beta_{\phi f}})\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota,\eta^{\beta_{\phi p}})$$
$$\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota,\eta^{k'_{\tau-1,\phi p}})\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota,\eta^{k'_{\tau,\phi p}})$$
$$\hat{p}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota,\eta^{\beta''_\psi})\,\hat{p}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota,\eta^{\beta_\gamma})$$
$$= \hat{p}(\eta_1,\eta_2)^2\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_\iota, S_{\tau,\gamma 4})\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota, S_{\tau,\gamma 5})$$
$$\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_\iota, S_{\tau,\gamma 2})\,\hat{p}(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_\iota, S_{\tau,\gamma 3})\,\hat{p}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_\iota, S_{\gamma 6})$$
$$\hat{p}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_\iota, S_{\gamma 7})$$

For a scenario where the user has only one long-lived device and has only one long-lived key, we modify the above method of IBKPDS and show the deputy signing key separated signature based on identity with only one long-lived device (IBKPDS1)as below.

(1) Su: $\Omega 1$ is a cyclic group of multiplication. The order of $\Omega 1$ is a prime number. $\Omega 2$ is a cyclic group of multiplication. The order of $\Omega 2$ is a prime number. $\Omega 1\times\Omega 1\rightarrow\Omega 2$ is a bilinear pairing $\hat{p}$ of which the generator is η. We pick a random integer a. $\eta 1$ is η to the power of a. We pick a random integer $\eta 2$ from Ω_1. We pick a random integer $\varpi 1$. $F_{\varpi 1}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. We pick a random integer $\varpi 2$. $F_{\varpi 2}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 2}$ is a function that is of hash and against collision. We pick a random integer $\varpi 3$. $F_{\varpi 3}:\{0,1\}^*\rightarrow\{0,1\}^{\varpi 3}$ is a function that is of hash and against collision. $F_{\varpi 1}$ is used to modify the length of the identity to the user's defined length. $F_{\varpi 2}$ is used to modify the length of a message to the user's defined length. $F_{\varpi 3}$ is used to modify the length of a deputy document to the user's defined length. We pick a random integer a. η_1 is equal η^a. η_2, $\varpi 1'$, $\varpi 2'$ and $\varpi 3'$ are random integers from Ω_1. The vector Φ is equal to (ϕ_ι). The length of Φ is $\varpi 1$. The vector Γ is equal to (γ_ι). The length of Γ is $\varpi 2$. The vector Ψ is equal to (ψ_ι). The length of Γ is $\varpi 3$. $\Omega 1$, $\Omega 2$, $\hat{p}$, η, η_1, η_2, $\varpi 1'$, Φ, $\varpi 2'$, Γ, $\varpi 3'$ and Ψ are the overt constants. Then the public agency gives the main privy constant and some overt constants to the people involved.

(2) Ext: The foremost signer's identity ϕf is a string of many bits. The length of ϕf is $\varpi 1$. Φ_ι is the ιth bit of ϕf. $\Phi_{\phi f}$ is equal to the set of the subscript ι, in which ϕf_ι is equal to 1. The elements of $\Phi_{\phi f}$ are integers which are less than $\varpi 1$ and bigger than 1. The public agency randomly chooses a positive integer $\beta_{\phi f}$ and sets the foremost signer's privy signing key as $\lambda_{\phi f}=(\lambda_{\phi f1},\lambda_{\phi f2})=(\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi f_\iota)^{\beta_{\phi f}},\eta^{\beta_{\phi f}})$.

The deputy signer's identity ϕp is a string of many bits. The length of ϕp is $\varpi 1$. ϕ_ι is the ιth bit of ϕp. $\Phi_{\phi p}$ is equal to the set of the subscript ι, in which ϕp_ι is equal to 1. The elements of $\Phi_{\phi p}$ are integers which are less than $\varpi 1$ and bigger than 1. $(0,\phi p)$ is a string of many bits. The length of $(0,\phi p)$ is $\varpi 1$. ϕ_ι is the ιth bit of $(0,\phi p)$. $\Phi_{0,\phi p}$ is the output of $F_{\varpi 1}(\text{-}1||\phi p)$ and equal to the set of the subscript ι, in which ϕ_ι is equal to 1. The elements of $\Phi_{0,\phi}$ are integers which are less than $\varpi 1$ and bigger than 1. The public agency randomly chooses hp' from $\{0,1\}^\kappa$. The function FP is random and pseud. $k_{0,\phi p}$ is equal to $FP_{hp'}(0||\phi p)$. The public agency randomly chooses a positive integers, $\beta_{\phi p}$, and sets the deputy signer's short-lived privy signing key for time slot 0 as

$$\lambda_{0,\phi p}$$
$$= (\lambda_{0,\phi p1},\lambda_{0,\phi p2},\lambda_{0,\phi p3})$$
$$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{0,\phi p}}\phi_\iota)^{k_{0,\phi p}},\eta^{k_{0,\phi p}},\eta^{\beta_{\phi p}}),$$

(3) DUpdateLongLived: $(\tau',\phi p)$ is a string of many bits. The length of $(\tau',\phi p)$ is $\varpi 1$. ϕ_ι is the ιth bit of $(\tau',\phi p)$. $\Phi_{\tau',\phi p}$ is the output of $F_{\varpi 1}(\tau||\phi p)$ and equal to the set of the subscript ι, in which ϕ_ι is equal to 1. The elements of $\Phi_{\tau',\phi p}$ are integers which are less than $\varpi 1$ and bigger than 1. $k_{\tau',\phi p}$ is equal to $FP_{hp'}(\tau||\phi p)$. $(\tau,\phi p)$ is a string of many bits. The length of $(\tau,\phi p)$ is $\varpi 1$. ϕ_ι is the ιth bit of $(\tau,\phi p)$. $\Phi_{\tau,\phi p}$ is the output of $F_{\varpi 1}(\tau||\phi p)$ and equal to the set of the subscript ι, in which ϕ_ι is equal to 1. The elements of $\Phi_{\tau,\phi}$ are integers which are less than $\varpi 1$ and bigger than 1. $k_{\tau,\phi p}$ is equal to $FP_{hp'}(\tau||\phi p)$. The deputy signer sets his privy short-lived refreshing key for time slot τ as

$$tui_{\tau,\phi p}=(tui_{\tau,\phi p1},tui_{\tau,\phi p2})$$
$$=((\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_\iota)^{k_{t,\phi p}}/(\varpi 1'\prod_{\iota\in\Phi_{\tau',\phi p}}\phi_\iota)^{k_{\tau',\phi p}},\eta^{k_{\tau,\phi p}})$$

(4) DUpdateUser: Using his privy short-lived refreshing key, $tui_{\tau,\phi p}$, for time slot τ, the deputy signer sets his short-lived privy signing key for time slot τ as

$$\lambda_{\tau,\phi p}$$
$$= (\lambda_{\tau,\phi p1},\lambda_{\tau,\phi p2},\lambda_{\tau,\phi p3})$$
$$= (\lambda_{t',\phi p1}\,tui_{\tau,\phi p1},tui_{\tau,\phi p2},\lambda_{t',\phi 3})$$
$$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau',\phi p}}\phi_\iota)^{k_{\tau',\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_\iota)^{k_{t,\phi p}}/(\varpi 1'\prod_{\iota\in\Phi_{\tau',\phi p}}\phi_\iota)^{k_{\tau',\phi p}},$$
$$\eta^{k_{\tau,\phi p}},\eta^{\beta_{\phi p}})$$
$$= (\eta_2^a(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_\iota)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_\iota)^{k_{\tau,\phi p}},\eta^{k_{\tau,\phi p}},\eta^{\beta_{\phi p}})$$

(5) DelegGen: The authorization ψ is a string of many bits. The length of ψ is $\varpi 3$. ψ_ι is the ιth bit of ψ. Ψ_ψ is equal to the

set of the subscript ι, in which ψ_ι is equal to 1. The elements of Ψ_ψ are integers which are less than $\varpi 3$ and bigger than 1. The signer randomly chooses a positive integer β_ψ and sets his overt deputy document as

$$\begin{aligned} & S_\psi \\ &= (S_{\psi 1}, S_{\psi 2}, S_{\psi 3}) \\ &= (\lambda_{\phi f 1}(\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta_\psi}, \lambda_{\phi f 2}, \eta^{\beta_\psi}) \\ &= (\eta_2^a (\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}} (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta_\psi}, \eta^{\beta_{\phi f}}, \eta^{\beta_\psi}) \end{aligned}$$

Then the foremost signer gives the deputy tuple (ψ,S_ψ) to the deputy signer.

(6) DelegVerify: DelegVerify: The deputy signer who wants to check the validity of a deputy document S_ψ parses the deputy document as ($S_{\psi 1}$, $S_{\psi 2}$, $S_{\psi 3}$) at first. Then he checks the truth of the equation below.

$$\hat{p}(S_{\psi 1}, \eta) = \hat{p}(\eta_1, \eta_2)^2 \, \hat{p}((\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}}, S_{\psi 2}) \hat{p}((\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta_\psi}, S_{\psi 3})$$

(7) GenPSig: If the deputy signer accepts the deputy document S_ψ, he randomly chooses two positive integers β'_ψ, β''_τ, and constructs his short-lived deputy signing key for time slot τ as

$$\begin{aligned} & tdsk \\ &= (tdsk_{\tau 1}, tdsk_{\tau 2}, tdsk_{\tau 3}, tdsk_{\tau 4}, tdsk_{\tau 5}) \\ &= (S_{\psi 1} \lambda_{\tau,\phi p 1} (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{\beta''_\tau} (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta'_\psi}, \\ & \quad \lambda_{\tau,\phi p 2} \eta^{\beta''_\tau}, S_{\psi 2}, \lambda_{\tau,\phi p 3}, S_{\psi 3} \eta^{\beta'_\psi}) \\ &= (\eta_2^a (\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}} (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta'_\psi} \eta_2^a (\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota)^{\beta_{\phi p}} \\ & \quad (\varpi 1' \prod_{\iota \in \Phi_{\tau,\phi p}} \phi_\iota)^{k_{\tau,\phi p}} (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{\beta''_\tau} (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta'_\psi}, \\ & \quad \eta^{k_{\tau,\phi p}} \eta^{r''_\tau}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi} \eta^{\beta'_\psi}) \\ &= (\eta_2^{2a} (\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}} (\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota)^{\beta_{\phi p}} (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{\beta''_\tau + k_{\tau,\phi p}} \\ & \quad (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta_\psi + \beta'_\psi}, \eta^{k_{\tau,\phi p} + \beta''_\tau}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi + \beta'_\psi}) \end{aligned}$$

(8) PSignatureGen: PSignatureGen: The message γ is a string of many bits. The length of γ is $\varpi 2$. γ_ι is the ιth bit of γ. Γ_γ is equal to the set of the subscript ι, in which γ_ι is equal to 1. The elements of Γ_γ are integers which are less than $\varpi 2$ and bigger than 1. The deputy signer randomly chooses two positive integers β_γ, β'''_τ, and sets his overt deputy signature for time slot τ as

$$\begin{aligned} & S_{\tau,\gamma} \\ &= (S_{\tau,\gamma 1}, S_{\tau,\gamma 2}, S_{\tau,\gamma 3}, S_{\tau,\gamma 4}, S_{\tau,\gamma 5}, S_{\tau,6}) \\ &= (tdsk_{\tau 1} (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{\beta'''_\tau} (\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota)^{\beta_\gamma}, \\ & \quad tdsk_{\tau 2} \eta^{r'''_\tau}, tdsk_{\tau 3}, tdsk_{\tau 4}, tdsk_{\tau 5}, \eta^{\beta_\gamma}) \\ &= (\eta_2^{2a} (\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}} (\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota)^{\beta_{\phi p}} (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{\beta''_\tau + k_{\tau,\phi p}} (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta_\psi + \beta'_\psi} \\ & \quad (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{\beta'''_\tau} (\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota)^{\beta_\gamma}, \eta^{\beta''_\tau + k_{\tau,\phi p}} \eta^{r'''_\tau}, \\ & \quad \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta_\psi + \beta'_\psi}, \eta^{\beta_\gamma}) \\ &= (\eta_2^{2a} (\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}} (\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota)^{\beta_{\phi p}} \\ & \quad (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{k'_{\tau,\phi p}} (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta''_\psi} (\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota)^{\beta_\gamma}, \\ & \quad \eta^{k'_{\tau,\phi p}}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta''_\psi}, \eta^{\beta_\gamma}), \end{aligned}$$

in which $\beta''_\omega = \beta_\psi + \beta'_\psi$, , $k'_{\tau,\phi p} = k_{\tau,\phi p} + \beta''_\tau + \beta'''_\tau$.

(9) PSignatureVerify: The user who wants to check the validity of a deputy signature $S_{\tau,\gamma}$ for the time slot τ parses the deputy signature as ($S_{\tau,\gamma 1}$, $S_{\tau,\gamma 2}$, $S_{\tau,\gamma 3}$, $S_{\tau,\gamma 4}$, $S_{\tau,\gamma 5}$, $S_{\tau,6}$) at first. Then he checks the truth of the equation below.

$$\begin{aligned} & \hat{p}(S_{\tau,\gamma 1}, \eta) \\ &= \hat{p}(\eta_1, \eta_2)^2 \, \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota, S_{\tau,\gamma 3}) \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota, S_{\tau,\gamma 4}) \\ & \quad \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota, S_{\tau,\gamma 2}) \hat{p}(\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota, S_{\gamma 5}) \hat{p}(\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota, S_{\gamma 6}) \end{aligned}$$

We show the truth of the computation of the proposed deputy signature above for the time slot τ with only one long-lived device as below.

$$\begin{aligned} & \hat{p}(S_{\tau,\gamma 1}, \eta) \\ &= \hat{p}(\eta_2^{2a} (\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}} (\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota)^{\beta_{\phi p}} \\ & \quad (\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{k'_{\tau,\phi p}} (\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta''_\psi} (\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota)^{\beta_\gamma}, (\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota)^{\beta_\gamma}, \eta) \\ &= \hat{p}(\eta_2^{2a}, \eta) \hat{p}((\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota)^{\beta_{\phi f}}, \eta) \hat{p}((\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota)^{\beta_{\phi p}}, \eta) \\ & \quad \hat{p}((\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota)^{k'_{\tau,\phi p}}, \eta) \hat{p}((\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota)^{\beta''_\psi}, \eta) \hat{p}((\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota)^{\beta_\gamma}, \eta) \\ &= \hat{p}(\eta_1, \eta_2)^2 \, \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota, \eta^{\beta_{\phi f}}) \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota, \eta^{\beta_{\phi p}}) \\ & \quad \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota, \eta^{k'_{\tau,\phi p}}) \hat{p}(\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota, \eta^{\beta''_\psi}) \hat{p}(\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota, \eta^{\beta_\gamma}) \\ &= \hat{p}(\eta_1, \eta_2)^2 \, \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\phi f}} \phi_\iota, S_{\tau,\gamma 3}) \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\phi p}} \phi_\iota, S_{\tau,\gamma 4}) \\ & \quad \hat{p}(\varpi 1' \prod_{\iota \in \Phi_{\iota,\phi p}} \phi_\iota, S_{\tau,\gamma 2}) \hat{p}(\varpi 3' \prod_{\iota \in \Psi_\psi} \psi_\iota, S_{\gamma 5}) \hat{p}(\varpi 2' \prod_{\iota \in \Gamma_\gamma} \gamma_\iota, S_{\gamma 6}) \end{aligned}$$

IV. SECURITIY

The proposed IBKPDS is secure from the proof of the following two theorems.

Theorem 1. The deputy signing key is isolated so that The proposed IBKPDS is against key exposure.

Proof: We use a match between a defier and an opponent to simulate the scenario in which the short-lived deputy signing Keys is isolated against the corruption of the opponent. The match in which the defier competes with opponent is shown as below. The opponent can ask the difier some questions and know η to the power of a and η to the power of b. Although ,the opponent does not know a and b, he wants to know η to the power of ab using the answers of the difier. The defier tosses a coin and decides which game he will plays with the opponent.

If the defier gets the front of the coin, he will play game I with the opponent. If the defier gets the back of the coin, he will play game II with the opponent.

Game I:

In Game I, the defier assumes that the opponent the opponent can get only one long-lived key and can not two long-lived keys.

The opponent and the defier interact with each other as follows.

(1) Initiation. ku, kv and km are randomly chosen from Z by the defier. k_u, $k_v$and k_m are positive integers. lu *is* set to be $3(q_e+2q_d+2q_{sld}+2q_{ps})$ and lv is set to be $3(q_e+2q_d+2q_{sld}+2q_{ps})$, $2(q_d+q_{pg})$ and $2q_{ps}$ respectively. x', s' and z' are randomly chosen from Z_{lu}, Z_{lv} and Z_{lm} respectively by the defier. X, S and Z are set to be (x_i) of length n_u, (s_j) of length n_v and (z_k) of length n_m when x_i s_j and z_k are randomly chosen from Z_{lu}, Z_{lv} and Z_{lm} respectively by the defier. Y, T and W are set to be (y_i) of length n_u, (τ_j) of length n_v and (w_k) of length n_m when y_i, τ_j and w_k are randomly chosen from Z_p.

$R(\phi)$ is set to be $x' + \sum_{i\in\Phi_\phi} x_i - lu\cdot ku$.

$J(\phi)$ is set to be $y' + \sum_{i\in\Phi_\phi} y_i$.

$E(\psi)$ is set to be $s' + \sum_{j\in\Psi_\psi} s_j - lv\cdot kv$.

$I(\psi)$ is set to be $\tau' + \sum_{j\in\Psi_\psi} \tau_j$.

$K(\gamma)$ is set to be $z' + \sum_{k\in\Gamma_\gamma} z_k - lm\cdot km$.

$L(\gamma)$ is set to be $w' + \sum_{k\in\Gamma_\gamma} w_k$.

The overt constants are:

$\eta_1=\eta^a$, $\eta_2=\eta^b$

$u'=\mu_2^{-l_u k_u + x'}\eta^{y'}$, $u_i=\eta_2^{x_i}\eta^{y_i}$ $1\le i\le n_u$

$v'=\eta_2^{-l_v k_v + s'}\eta^{\tau'}$, $v_j=\eta_2^{s_j}\eta^{\tau_j}$ $1\le j\le n_v$

$m'=\eta_2^{-l_m k_m + z'}\eta^{w'}$, $m_k=\eta_2^{z_k}\eta^{w_k}$ $1\le k\le n_m$

Then, $\eta_2^{R(\mathbf{u})}\eta^{J(\mathbf{u})} = u'\prod_{i\in\mathbf{U}}\prod u_k$, $\eta_2^{E(w)}\eta^{I(w)} = v'\prod_{j\in\mathbf{V}_w}\prod v_j$,

$\eta_2^{K(\mathbf{m})}\eta^{L(\mathbf{m})} = m'\prod_{k\in M_m}\prod m_k$.

l_r is a list. l_r is empty at first. $R\_Query(u)$ is an algorithm. $R\_Query(u)$ return $\hat{r}$ when $\langle u, \hat{r}\rangle$ is in l_r. $R\_Query(u)$ picks $\hat{r}$ randomly from $\{0,1\}^*$ to add $\langle u, \hat{r}\rangle$ to l_r and return $\hat{r}$ when $\langle u, \hat{r}\rangle$ is not in l_r. l_hk is a list. l_hk is empty at first. $HK\_Query(u)$ is an algorithm. $HK\_Query(u)$ return hku, when $\langle u,hku\rangle$ is in l_r. $HK\_Query(u)$ picks hku randomly from $\{0,1\}^*$ to add $\langle u,hku\rangle$ to l_hk and return $\hat{r}$ when $\langle u,hku\rangle$ is not in l_hk.

(2) Questions. The opponent can ask the defier any of the following questions.

①The question of extraction. When the input is $\langle u\rangle$, the defier will say "error" to exit if $R(u)$ is 0. When the input is $\langle u\rangle$, the defier will output $\langle u,hku\rangle$ using $HK\_Query(u)$ and output $\langle u, \hat{r}\rangle$ using $R\_Query(u)$ at first when $R(u)$ is not 0.

The defier randomly chooses hp' and hp'' from $\{0,1\}^\kappa$. The function FP is random and pseud. $k_{-1,\phi p}$ is equal to $FP_{hp'}(-1\|\phi p)$. $k_{0,\phi p}$ is equal to $FP_{hp''}(0\|\phi p)$. The defier randomly chooses a positive integers, $\beta_{\phi p}$, and sets the deputy signer's short-lived privy signing key for time slot 0 as

$$\begin{aligned}&\lambda_{0,\phi p}\\ &= (\lambda_{0,\phi p1}, \lambda_{0,\phi p2}, \lambda_{0,\phi p3}, \lambda_{0,\phi p4})\\ &= (\eta_1^{-\frac{J(u)}{R(u)}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_t)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{-1,\phi p}}\phi_t)^{k_{-1,\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{0,\phi p}}\phi_t)^{k_{0,\phi p}},\\ &\quad \eta^{k_{-1,\phi p}}, \eta^{k_{0,\phi p}}, \eta_1^{-\frac{1}{R(u)}}\eta^{\beta_{\phi p}})\end{aligned}$$

②The question of the short-lived deputy signing key. When the input is $\langle u\rangle$, the defier will say "error" to exit if $R(u)$ is 0. When $R(u)$ is not 0, the defier sets the short-lived deputy privy signing key for time slot τ as

$$\begin{aligned}&\lambda_{\tau,\phi p}\\ &= (\lambda_{\tau,\phi p1}, \lambda_{\tau,\phi p2}, \lambda_{\tau,\phi p3}, \lambda_{\tau,\phi p4})\\ &= (\eta_1^{-\frac{J(u)}{R(u)}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_t)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau-1,\phi p}}\phi_t)^{k_{\tau-1,\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{\tau,\phi p}}\phi_t)^{k_{\tau,\phi p}},\\ &\quad \eta^{k_{\tau-1,\phi p}}, \eta^{k_{\tau,\phi p}}, \eta_1^{-\frac{1}{R(u)}}\eta^{\beta_{\phi p}})\end{aligned}$$

③The question of the deputy document. When the input is $\langle u\rangle$, the defier will say "error" to exit if $R(u)$ is 0. When $R(u)$ is not 0, the defier sets the deputy document to be

$$(\eta_1^{-\frac{J(u)}{R(u)}}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_t)^{\beta_{\phi f}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_t)^{\beta_\psi}, \eta^{\beta_{\phi f}}, \eta^{\beta_\psi})$$

④The question of the deputy signature. When the input is $\langle u\rangle$, the defier will say "error" to exit if $R(u)$ is 0. When $R(u)$ is not 0, the defier sets the proxy signature for time slot τ as

$$\begin{aligned}&(\eta_1^{-\frac{J(u)}{R(u)}}(\varpi 1'\prod_{\iota\in\Phi_{\phi f}}\phi_t)^{\beta_{\phi f}}(\varpi 1'\prod_{\iota\in\Phi_{\phi p}}\phi_t)^{\beta_{\phi p}}(\varpi 1'\prod_{\iota\in\Phi_{t-1,\phi p}}\phi_t)^{k'_{\tau-1,\phi p}}\\ &(\varpi 1'\prod_{\iota\in\Phi_{t,\phi p}}\phi_t)^{k'_{\tau,\phi p}}(\varpi 3'\prod_{\iota\in\Psi_\psi}\psi_t)^{\beta''_\psi}(\varpi 2'\prod_{\iota\in\Gamma_\gamma}\gamma_t)^{\beta_\gamma},\\ &\eta^{k'_{\tau-1,\phi p}}, \eta^{k'_{\tau,\phi p}}, \eta^{\beta_{\phi f}}, \eta^{\beta_{\phi p}}, \eta^{\beta''_\psi}, \eta^{\beta_\gamma}).\end{aligned}$$

(3) Forgery. The simulation will succeed in computing g^{ab} when the defier does not say "error" and answers the above questions.

Game II:

The simulation is similar to that of Game I. In Game II, however, the opponent can obtain only one of the two long-lived keys.

The running time and advantage can be computed using the method of IBS (identity based signature).

.

Theorem 2. The deputy signing key is forcefully isolated so that The proposed IBKPDS is forcefully against key exposure.

Proof: The poof is the same with that of **Theorem 1** except that in the opponent can obtain two long-lived keys.

V. Assesment

We give the computational complexity of the algorithms of the proposed IBKPDS system as follows. There is not any pairing computation in the algorithms of DUpdateLongLived, DUpdateUser, DelegGen, GenPSig and PSignatureGen. DelegVerify and PSignatureVerify need 4 and 8 pairing computations respectively.

We assess the proposed IBKPDS in Table 1. τ_p is equal to be computation time of pairings. τ_e is equal to the exponential computation time. $|\tau|$ is equal to the number of bits used for a time slot. $|\Omega 1|$ is equal to the number of bits used for an element in $\Omega 1$.

Our IBKPDS signatures consist of 7 group elements and $1|\tau|$.

To defend against key exposure, we refresh the deputy signing keys at regular intervals in the IBKPDS system. So the signature size is relatively large and the verification needs more pairing computations. In the aspect of signature size and computational cost, our IBKPDS scheme is not competitive with traditional deputy signature schemes because we trade the decreased efficiency for the increased security.

Scheme	PERFORMANCE		
	Proxy signature length	***Proxy signature issuing***	***Verification of proxy signature***
Proposed IBKPDS Scheme	$1\|\tau\|+7\|\Omega 1\|$	$6\tau_e$	$8\tau_p$

Table 1. the performance of our IBKPDS scheme

VI. Conclusion

It is required by classical deputy signature systems that deputy signing keys be securely retained. In reality, however, there appears to be a certain inevitability for the keys to be exposed due to theft, virus, network vulnerability etc. The deputy signature system will not be secure at all if deputy signing keys are exposed.

To defend against the above threat of key exposure, we give the key protected deputy signature (IBKPDS) using the method of parallel key insulation. The given IBKPDS is shown to be secure with the cryptographic proof. We evolve the deputy signing keys with two physically-secure computationally-limited devices. An attacker who obtained the short-lived deputy signing keys of some time slots can not compromise the safety of the IBKPDS system of any other time slots.

Acknowledgment

At last, we are particularly grateful to the experts who review this paper for their priceless remarks.

References

[1] N. Ghadbane,"On public key cryptosystem based on the problem of solving a non linear system of polynomial equations", *WSEAS Transactions on Computer Research*, vol.8, pp. 106-110, 2020.

[2] A. Chillali,"Finite Ring Of Characteristic 2 And Cryptography", *Int. J. of Applied Mathematics, Computational Science and Systems Engineering*, vol.2, pp. 1-4, 2020.

[3] S. Dutta, and K. Saini,"Securing Data: A Study on Different Transform Domain Techniques", *WSEAS Transactions on Computer Research*, vol.16, pp. 110-120, 2021.

[4] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang,"Digital Signature Scheme for Information Non-repudiation in Blockchain: a State of the Art Review", *EURASIP Journal on Wireless Communications and Networking*, no.56, pp. 1-15, 2020.

[5] G. Verma, B. Singh, N. Kumar, M. Obaidat, B. He, and H. Singh,"An efficient and provable certificate-based proxy signature scheme for IIoT environment", *Information Sciences*, vol. 518, pp. 142-156, 2020.

[6] F. Wu, W. Yao, X. Zhang, W. Wang, and Z. Zheng, "Identity-based proxy signature over NTRU lattice", *International journal of communication systems*, vol. 32, no.3, pp. e3867.1-e3867.11, 2018.

[7] R. Gao, and J. Zeng,"Forward secure certificateless proxy multi-signature scheme", *International Journal of Electronic Security and Digital Forensics*, vol. 13, no.1, pp. 1-27, 2021

[8] S. Singh, and S. Padhye,"Identity based blind signature scheme over NTRU lattices", *Information Processing Letters*, vol. 155, pp.105898.1 -105898.3, 2020.

[9] S. James, G. Thumbur, and P.V. Reddy,"An Efficient Pairing-Free Identity Based Proxy Blind Signature Scheme with Message Recovery", *International Journal of Information Security and Privacy*, vol. 15, no.1, pp. 117-137, 2021.

[10] K. Tiliwalidi, J. Zhang, and S. Xie,"A Multi-bank E-Payment Protocol Based on Quantum Proxy Blind Signature", *International Journal of Theoretical Physics*, vol. 58, no.10, pp. 3510-3520, 2020.

[11] J. Zhang," Improvement of ID-based Proxy Re-signature Scheme with Pairing-free", *Wireless Networks*, vol. 25, no.7, pp. 4319-4329, 2019.

[12] F. Luo, S. Al-Kuwaria, W. Susilo, and D. Duong," Attribute-based Proxy Re-signature from Standard Lattices and its Applications", *Computer Standards & Interfaces*, vol. 75, pp. 1-9, 2020.

[13] H. Zhu, Y. Wang, C. Wang, and X. Cheng,"An efficient identity-based proxy signcryption using lattice", *Future Generation Computer Systems*, vol. 117, pp. 321-327, 2021..