SCIENCE CHINA
Information Sciences

• **Supplementary File** •

General construction of revocable identity-based fully homomorphic signature

Congge XIE[1], Jian WENG[1*], Wei LU[2] & Lin HOU[1]

[1]*College of Information Science and Technology, Jinan University, Guangzhou,* 510632*, China;*
[2]*School of Data and Computer Science, Sun Yat-sen University, Guangzhou,* 510006*, China*

Appendix A Security proof for the (2,2) vector secret sharing scheme

Our (2,2) vector secret sharing construction is secure under the SIS assumption proved in the following theorem.

Theorem 1. Our special (2,2) vector secret sharing construction is secure if the $\mathsf{SIS}(n, m, q, \beta)$ assumption holds.

Proof. Let $\mathcal{A}$ be some PPT adversary that succeeds in attacking the (2,2) vector secret sharing scheme with non-negligible probability ε. We can construct an algorithm $\mathcal{B}$ that breaks the $\mathsf{SIS}(n, m, q, \beta)$ problem defined by $\mathbf{A}^* \in \mathbb{Z}_q^{n\times m}$. Assume $P^* = \{P_1^*, P_2^*\}$ is the challenge participate set.

In Setup Phase, algorithm $\mathcal{B}$ uses $\mathbf{A}^*$ instead of $\mathbf{A}$, obtains $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(n, q, m)$, picks two random matrices $\mathbf{U}_1^*, \mathbf{U}_2^* \leftarrow (\mathcal{D}_{\mathbb{Z}^m,\eta})^m$ and sets $\mathbf{A}_1 = \mathbf{A}^*\mathbf{U}_1^* - H(P_1^*)\mathbf{B}$, $\mathbf{A}_2 = \mathbf{A}^*\mathbf{U}_2^* - H(P_2^*)$. Then $\mathcal{B}$ sends parameters $pp = (n, q, m, \mathbf{A}^*, \mathbf{B}, \mathbf{A}_1, \mathbf{A}_2)$ to $\mathcal{A}$. From the Corollary 4.4 of [1], the distribution of matrices $\mathbf{A}_1, \mathbf{A}_2$ are statistically close to them in real scheme.

In query phase, algorithm $\mathcal{B}$ answers the sub-secret queries of any shareholders from adversary $\mathcal{A}$, except for answering the queries of P_1^*, P_2^* at the same time. Here we assume adversary $\mathcal{A}$ never queries P_2^*'s sub-secret.

If $P_i \neq P_1^*$, $\mathcal{B}$ samples $\mathbf{E}_{2,1}, \mathbf{E}_{2,2} \leftarrow (\mathcal{D}_{\mathbb{Z}^m,s_1})^m$, $\mathbf{R}_1 \leftarrow \mathcal{D}_{m\times m}$, sets $-\mathbf{U}_{P_i} \leftarrow [\mathbf{A}_0|\mathbf{A}_2 + H(P_2^*)\mathbf{B}] \cdot \begin{pmatrix}\mathbf{E}_{2,1}\\ \mathbf{E}_{2,2}\end{pmatrix}$, stores $\mathbf{U}_{P_i}$ in the shareholder P_i. Then $\mathcal{B}$ samples $\mathbf{E}_i \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{A}_1 + (H(P_i) - H(P_1^*))\mathbf{B}, \mathbf{U}_1^*, \mathbf{T_B}, \mathbf{U}_{P_i}, s_1')$, $\mathbf{E}'_{P_i} \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{A}_1 + (H(P_i) - H(P_1^*))\mathbf{B}, \mathbf{U}_1^*, \mathbf{T_B}, 0, s_1')$ and sets $\mathbf{E}_{P_i} = \mathbf{E}'_{P_i}\mathbf{R}_1$. At last, it returns $(\mathbf{E}_i, \mathbf{E}_{P_i}, \mathbf{R}_1)$ as the query.

If $P_i = P_1^*$, $\mathcal{B}$ samples $\mathbf{E}_{1,1}, \mathbf{E}_{1,2} \leftarrow (\mathcal{D}_{\mathbb{Z}^m,s_1})^m$, $\mathbf{R}_1 \leftarrow \mathcal{D}_{m\times m}$, sets $\mathbf{U}_{P_1^*} \leftarrow [\mathbf{A}_0|\mathbf{A}_1 + H(P_1^*)\mathbf{B}] \cdot \mathbf{E}_1$, $\mathbf{E}_{P_1^*} = -\mathbf{U}_1^* \cdot \mathbf{R}_1$, where $\mathbf{E}_1 := \begin{pmatrix}\mathbf{E}_{1,1}\\ \mathbf{E}_{1,2}\end{pmatrix}$. Then it computes $\mathbf{H}_{P_1^*} := \mathbf{E}_{1,1} - \mathbf{E}_{P_1^*}\mathbf{R}_1^{-1}\mathbf{E}_{1,2}$, and stores $\mathbf{H}_{P_1^*}, \mathbf{U}_{P_1^*}$ in the shareholder P_1^*. At last, $\mathcal{B}$ returns $(\mathbf{E}_1, \mathbf{E}_{P_1^*}, \mathbf{R}_1)$ to $\mathcal{A}$ as the query. According the Corollary 4.4 of [1], Theorem 17 and Theorem 19 of [2], the distribution of answered sub-secret is statistically close to the distribution in real scheme.

In the Construction phase, $\mathcal{A}$ provides a valid secret $\mathbf{T}^*$ under challenge participant set P^*. In other words, adversary $\mathcal{A}$ recovers $\mathbf{A}_{P_1^*,P_2^*}$'s short basis $\mathbf{T}^*$, and has $\mathbf{A}_{P_1^*,P_2^*} \cdot \mathbf{T}^* = 0$.

In the following, we will use $\mathcal{A}$'s $\mathbf{T}^*$ to obtain a valid solution of SIS problem. First, let $(\mathbf{t}_{1,1}^T, \mathbf{t}_{1,2}^T, \mathbf{t}_{1,3}^T)^T$ be the first column vector of matrix $\mathbf{T}^*$. Obviously, it has $(\mathbf{A}^*|\mathbf{A}^*\mathbf{U}_1^*|\mathbf{A}^*\mathbf{U}_2^*) \cdot (\mathbf{t}_{1,1}^T, \mathbf{t}_{1,2}^T, \mathbf{t}_{1,3}^T)^T = 0$, that is $\mathbf{A}^* \cdot (\mathbf{t}_{1,1} + \mathbf{U}_1^*\mathbf{t}_{1,2} + \mathbf{U}_2^*\mathbf{t}_{1,3}) = 0$. Since $\|\mathbf{U}_i^*\| \leqslant \eta\sqrt{m}$, $i \in \{1, 2\}$, then it has $\|\mathbf{t}_{1,1} + \mathbf{U}_1^*\mathbf{t}_{1,2} + \mathbf{U}_2^*\mathbf{t}_{1,3}\| \leqslant \sqrt{3m} \cdot (1 + 2\eta\sqrt{m})$. If $\mathbf{t}_{1,1} + \mathbf{U}_1^*\mathbf{t}_{1,2} + \mathbf{U}_2^*\mathbf{t}_{1,3} \neq 0$ and $\sqrt{3m} \cdot (1 + 2\eta\sqrt{m}) \leqslant \beta$, then $\mathbf{t}_{1,1} + \mathbf{U}_1^*\mathbf{t}_{1,2} + \mathbf{U}_2^*\mathbf{t}_{1,3}$ will be a non-zero solution of $\mathsf{SIS}(n, m, q, \beta)$ problem.

Next, we will show that $\mathbf{t} := \mathbf{t}_{1,1} + \mathbf{U}_1^*\mathbf{t}_{1,2} + \mathbf{U}_2^*\mathbf{t}_{1,3} \neq 0$. Suppose for an easy case that $\mathbf{t}_{1,2} = 0$ and $\mathbf{t}_{1,3} = 0$; then for a valid short basis we must have $\mathbf{t}_{1,1} \neq 0$ and thus $\mathbf{t} \neq 0$. Suppose on the contrary that $\mathbf{t}_{1,2} \neq 0$ or $\mathbf{t}_{1,3} \neq 0$. In that case, w.l.o.g., let $\mathbf{t}_{1,2} \neq 0$, since $\|\mathbf{t}_{1,2}\| < \sqrt{3m}s_1 \ll q$, then there exists at least one $\mathbf{t}_{1,2}$'s coordinate such that it is non-zero modulo q. We assume $\mathbf{t}_{1,2}$'s last one coordinate is non-zero and set it $\mathbf{y}$. Assume $\mathbf{u}^*$ is the last column of $\mathbf{U}_1^*$ and then we have $\mathbf{t} = \mathbf{y}\mathbf{u}^* + \mathbf{t}'$, where $\mathbf{t}'$ has nothing to do with $\mathbf{u}^*$. We know that only the last column of $\mathbf{U}_1^*$ contains $\mathbf{u}^*$'s information which is available to $\mathcal{A}$. From a simple pigeonhole principle, there are exist many admissible and equally likely vector $\mathbf{u}^*$ that are same with $\mathcal{A}$'s view. $\mathcal{A}$ can not know the value of $\mathbf{y}\mathbf{u}^*$ with probability exceeding once third, then every other $\mathbf{y}\mathbf{u}^*$ would fail to do so. Since we have $\Pr\{\mathbf{t} \neq 0\} > 1 - \exp(-\Omega(m - n\log q)) \to 1$ under $\lambda \to \infty$, then we deduce that $\Pr\{\mathbf{t} \neq 0\} \geqslant 2/3$. Therefore, algorithm $\mathcal{B}$ can solve the $\mathsf{SIS}(n, m, q, \beta)$ problem with the advantage of $(2/3) \cdot \varepsilon$.

* Corresponding author (email: cryptjweng@gmail.com)

Since the SIS problem is as hard as approximating to the worst-case shortest independent vector problem from [3], then the adversary $\mathcal{A}$ can not provide such a valid secret $\mathbf{T}^*$ for challenge participant set P^*. So, the proposed (2,2) vector secret sharing scheme is secure. This concludes the proof.

Appendix B Security proof for the general RIBFHS scheme

Theorem 2. Our general RIBFHS scheme is EUF-sID-CMA secure, if the scheme VSS and the scheme FHS are secure.

Proof. Suppose adversary $\mathcal{A}$ breaks the general construction of RIBFHS. Let $(id^*, t^*, \tau^*, \mu^*)$ be the challenge identity, time, tag and the vector of messages on which the adversary $\mathcal{A}$ will make a forgery. We can construct an algorithm $\mathcal{A}^*$ that succeeds attacking the scheme VSS or construct an algorithm $\mathcal{B}^*$ that forges a valid message/signature pair for scheme FHS. The simulation process is as follows:

Setup$^*(1^\lambda, 1^L, 1^l, N)$**:** $\mathcal{A}^*$ simulates the parameters as in initial phase of VSS, and $\mathcal{B}^*$ perform the algorithm FHS.Setup to obtain other parameters. Send all parameters to $\mathcal{A}$.

PriKeyGen and Key Update Queries: $\mathcal{A}^*$ first picks a node $\nu^* \in \mathsf{BT}$ and allots it to id^*. It is worth noting that there will be two types adversaries:

- Type (a) adversaries are revoked users and can challenge the target identity id^* before or on time t^*.
- Type (b) adversaries can not challenge the target identity id^* at any time.

Obviously, Type (a) adversaries are the insider adversaries and Type (b) are the outsider adversaries. For Type (a) adversaries, $\mathcal{A}^*$ first picks a node $\nu^* \in \mathsf{BT}$ and may be allot it to id^*. We know that these adversaries are revoked users which can issue id^*'s private key query before or on time t^*. For PriKeyGen queries, when the adversary issues the target identity id^*, $\mathcal{A}^*$ samples $\mathbf{E}_{1,1}, \mathbf{E}_{1,2} \leftarrow (\mathcal{D}_{\mathbb{Z}^m, s_1})^m$, $\mathbf{R}_1 \leftarrow \mathcal{D}_{m\times m}$ as the answer which corresponds to the case $i = i^*$ of VSS's sub-secret query; Otherwise, $\mathcal{A}^*$ uses the VSS's $i \neq i^*$ sub-secret queries to answer. For Key Update queries, when the adversary does not ask the update key at $t = t^*$, $\mathcal{A}^*$ also can use the VSS's $i \neq i^*$ sub-secret queries to answer; when the adversary issues the $t = t^*$ update key query, $\mathcal{A}^*$ samples $\mathbf{E'}_{1,1}, \mathbf{E'}_{1,2} \leftarrow (\mathcal{D}_{\mathbb{Z}^m, s_1})^m$, $\mathbf{R}_2 \leftarrow \mathcal{D}_{m\times m}$ as the answer which corresponds to the case $i = i^*$ of VSS's sub-secret query. For Type (b) adversaries, $\mathcal{A}^*$ also first picks a node $\nu^* \in \mathsf{BT}$ and may be assign it id^*. We know that these adversaries can never issue id^*'s private key query. Then for the PriKeyGen queries, $\mathcal{A}^*$ can use the VSS's $i \neq i^*$ sub-secret queries to answer. For Key Update queries, when the adversary challenge the update key at $t \neq t^*$, $\mathcal{A}^*$ also can use the VSS's $i \neq i^*$ sub-secret queries to answer; when the adversary issues the $t = t^*$ update key query, $\mathcal{A}^*$ samples $\mathbf{E'}_{1,1}, \mathbf{E'}_{1,2} \leftarrow (\mathcal{D}_{\mathbb{Z}^m, s_1})^m$, $\mathbf{R}_2 \leftarrow \mathcal{D}_{m\times m}$ as the answer which corresponds to the case $i = i^*$ of VSS's sub-secret query.

Signature Queries: $\mathcal{A}$ issues a series of signature queries. $\mathcal{B}$ simulates signatures of messages μ for $\mathcal{A}$'s signature queries as follows. $\mathcal{B}^*$ answers these

- If the queried messages μ are under target identity id^* in target time t^*. $\mathcal{B}$ answers these queries same to the answers of FHS's signature queries.
- If the queried messages μ are under identity $id \neq id^*$ or in time $t \neq t^*$, $\mathcal{B}$ answers as follows:

1. if $id \neq id^*$, sample vector using SampleRight's extension algorithm SampleRightExt from [**?**]:

$$\sigma \leftarrow \mathsf{SampleRightExt}(\mathbf{A}_0, (H(id) - H(id^*))\mathbf{B}, \mathbf{A}_{t,\mu}, \mathbf{T}_\mathbf{B}, 0, s'_2)$$

2. if $t \neq t^*$, sample vector

$$\sigma \leftarrow \mathsf{SampleRightExt}(\mathbf{A}_0, (H(t) - H(t^*))\mathbf{B}, \mathbf{A}_{id,\mu}, \mathbf{T}_\mathbf{B}, 0, s'_2)$$

3. Output σ.

Forgery: Adversary $\mathcal{A}$ outputs the signing key SK_{id^*,t^*} or a forgery (μ^*, σ^*, C^*).

If $\mathcal{A}$ outputs the signing key SK_{id^*,t^*}, then $\mathcal{A}^*$ outputs SK_{id^*,t^*}. It means that $\mathcal{A}^*$ breaks the scheme VSS. If $\mathcal{A}$ outputs a forgery (μ^*, σ^*, C^*), then $\mathcal{B}^*$ outputs this result. It means that $\mathcal{B}^*$ breaks the scheme FHS. Since the schemes VSS and FHS are secure, then our general construction is secure.

Appendix C Comparisons

Appendix C.1 Efficiency comparisons

It is known that our proposed RIBFHS scheme is a general construction, which utilizes (2,2) vector secret sharing as a black box to transform any FHS scheme into a RIBFHS scheme. In other words, if a concrete and secure FHS scheme is input into (2,2) vector secret sharing black box, it will output a concrete and secure RIBFHS scheme. Since we proposed a RIBFHS general construction, we cannot analyze its efficiency accurately. While there is no RIBFHS scheme at present, we are the first to propose a RIBFHS scheme and cannot provide efficiency comparisons with the existing schemes directly. In terms of revocation mechanism, we can compare the PKG's workload between existing lattice-based RIBS schemes (Xiang's RIBS [4]and Hung's RIBS [5]) and our RIBFHS scheme. In Xiang's RIBS scheme, since the PKG needs to interact with users to generate the update key secretly, then the number of update keys is linear with the non-revoked users' number $N_{\max} - r$, where $N_{\max}$ is the maximum number of users in the system, r is the number of revoked users. In Hung's RIBS scheme, their update key algorithm has nothing to do with revocation list and produces all users' update key in the system.

In other words, the number of update keys is the maximum number of users $N_{\max}$. Our RIBFHS scheme adopts complete tree revocation technology from [6], which causes that the number of update keys has $r\log(N_{\max}/r)$ function associated with revoked users' number r and maximum number of users $N_{\max}$. In practical use, few users will be revoked in each time period. For example, suppose that there is only one user is revoked in some time period, then the update keys' numbers in our RIBFHS, Xiang's RIBS and Hung's RIBS are $\log(N_{\max})$, $N_{\max}-1$ and $N_{\max}$, respectively. Thus the update keys' number in our scheme is logarithmic with the maximum number of users $N_{\max}$. But the update keys' number in both Xiang's RIBS and Hung's RIBS are linear with the maximum number of users $N_{\max}$.

Appendix C.2 Functionality comparisons

According to functionality, we also present some comparisons with Xiang's RIBS and Hung's RIBS in Table C1 to highlight our RIBFHS's strengths. Firstly, our RIBFHS can be easily achieved through (2,2) vector secret sharing as a black box and FHS. But both Xiang's RIBS and Hung's RIBS are concrete schemes and cannot easily achieved through any black boxes. Secondly, both our RIBFHS and Xiang's RIBS are secure in the standard model. But Hung's RIBS is secure under the random oracle model, which has not yet met the requirement of reality. Thirdly, both our RIBFHS and Hung's RIBS broadcast the update keys regularly through public channels. But Xiang's scheme uses secure channels to send periodic update keys. Finally, Our RIBFHS can perform homomorphic operations over signatures, which can be suitable to be applied in the untrusted cloud computing environment. Furthermore, such computed signatures can be made context hiding to ensure that they do not reveal anything about the underlying data beyond the outcome of the computation. However, none of Xiang's RIBS and Hung's RIBS have this practical property.

Table C1 The comparison table between the existing RIBS schemes and our RIBFHS scheme

	Xiang's RIBS [4]	Hung's RIBS [5]	Our RIBFHS
Update keys' number	$N_{\max}-r$	$N_{\max}$	$r\log(N_{\max}/r)$
Black box	No	No	Yes
Security model	Standard model	Random oracle model	Standard model
Update key' transport channel	Secure channel	Public channel	Public channel
Homomoriphic property	No	No	Yes
Context hiding	No	No	Yes

References

1 Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, 2008. 197–206

2 Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, 2010. 553-572

3 Micciancio D, Regev O. Worst-case to average-case reductions based on gaussian measures. SIAM Journal on Computing, 2007, 37(1): 267–302

4 Xiang X Y. Adaptive secure revocable identity-based signature scheme over lattices. Computer Engineering, 2015, 10: 025

5 Hung Y H, Tseng Y M, Huang S S. Revocable id-based signature with short size over lattices. Security and Communication Networks, 2017, 7571201: 1-9

6 Naor M, Nissim K. Certificate revocation and certificate update. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 561-570