SCIENCE CHINA
Information Sciences

• LETTER •

August 2022, Vol. 65 189103:1–189103:3
https://doi.org/10.1007/s11432-019-2709-7

Hierarchical group signature with verifier-local revocation revisited

Lin HOU[1,2], Dongdai LIN[1,2*] & Renzhang LIU[3]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100195*, China;*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049*, China;*
[3]*Westone Cryptologic Research Center, Westone Information Industry INC., Beijing* 100070*, China*

Received 8 July 2019/Revised 8 October 2019/Accepted 6 November 2019/Published online 24 May 2021

Citation Hou L, Lin D D, Liu R Z. Hierarchical group signature with verifier-local revocation revisited. Sci China Inf Sci, 2022, 65(8): 189103, https://doi.org/10.1007/s11432-019-2709-7

Dear editor,

Group signature (GS) [1] is a milestone in privacy-oriented cryptography, which provides authentication for messages and keeps signers anonymous. Trolin and Wikström [2] properly generalized GS into the notion of hierarchical group signature (HGS) and showed its typical usage in building anonymous credit card systems. Initially, HGS was proposed in a static setting, i.e., no dynamic joining or revocation would be allowed once the group was set up, and this considerably limited its applications. To partially address this issue, Hou et al. [3] formalized the notion of hierarchical GS with verifier-local revocation (VLR-HGS). Furthermore, they showed a generic construction only from verifier-local revocable GS (VLR-GS) [4] holding some strong security, called full-anonymity. However, their work failed to show a more general case of insider-anonymity, which presented a drawback.

In addition, by recognizing the building block of anonymous encryption (AE) [5], we propose an alternative generic construction of VLR-HGS. Our construction enjoys several advantages over [3]. First, it supports more efficient instantiations (from lattices). Please see Table 1 for details. Second, it traces more efficiently for managers excluding the penultimate depth. Third, our construction allows pre-signings. Notations and other preliminaries are put in Appendixes A–E.

VLR-HGS constructions from AE and VLR-GS. Let $\mathcal{AE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be an AE scheme, and let $\mathcal{GS} = (\mathsf{GKg}, \mathsf{GSig}, \mathsf{GVf})$ be a VLR-GS scheme; our construction is demonstrated as follows.

(1) $\mathsf{HKg}(1^n, \mathcal{T})$: First, run $(\mathrm{gpk}, \{\mathrm{grt}[\alpha]\}_{\alpha\in\mathcal{L}(\mathcal{T})}, \{\mathrm{gsk}[\alpha]\}_{\alpha\in\mathcal{L}(\mathcal{T})}) \leftarrow \mathsf{GKg}(1^n, 1^{|\mathcal{L}(\mathcal{T})|})$; then run $(\mathrm{pk}_\beta, \mathrm{sk}_\beta) \leftarrow \mathsf{Kg}(1^n)$ for $\beta \in (\mathcal{T}-\mathcal{L}(\mathcal{T})-\mathcal{T}^{\delta-1})$. The public map hpk is defined as $\mathrm{hpk}(\rho) := (\mathrm{gpk}, \mathrm{pk}_\rho)$, $\mathrm{hpk}(\beta) := \mathrm{pk}_\beta$ for $\beta \in \mathcal{T}^i$, $i = 1, 2, \ldots, \delta-2$, $\mathrm{hpk}(\beta) := \perp$ for $\beta \in (\mathcal{L}(\mathcal{T}) \bigcup \mathcal{T}^{\delta-1})$; the secret map hsk is defined as $\mathrm{hsk}(\beta) := \mathrm{sk}_\beta$ for $\beta \in (\mathcal{T} - \mathcal{L}(\mathcal{T}) - \mathcal{T}^{\delta-1})$, $\mathrm{hsk}(\beta) := \{\mathrm{grt}[\alpha]\}_{\alpha\in\beta}$ for $\beta \in \mathcal{T}^{\delta-1}$, $\mathrm{hsk}(\alpha) := \mathrm{gsk}[\alpha]$ for $\alpha \in \mathcal{L}(\mathcal{T})$; the map hrt is defined as $\mathrm{hrt}(\alpha) := \mathrm{grt}[\alpha]$ for $\alpha \in \mathcal{L}(\mathcal{T})$.

(2) $\mathsf{HSig}(\mathrm{hpk}, \mathrm{hsk}(\alpha), m)$: Let $\beta_0 := \rho \ni \beta_1 \ni \cdots \ni \beta_\delta := \alpha$ denote the path from the root to the signer, and parse $\mathrm{hpk}(\rho)$ as $(\mathrm{gpk}, \mathrm{pk}_\rho)$; first compute $c_i \leftarrow \mathsf{Enc}(\mathrm{pk}_{\beta_i}, \beta_{i+1})$ for $i = 0, 1, \ldots, \delta-2$, then generate $\sigma' \leftarrow \mathsf{GSig}(\mathrm{gpk}, \mathrm{hsk}(\alpha), m)$; it outputs the signature $\sigma := (c_0, c_1, \ldots, c_{\delta-2}, \sigma')$.

(3) $\mathsf{HVf}(\mathrm{hpk}, \mathrm{RL}, m, \sigma)$: Parse $\mathrm{hpk}(\rho)$ as $(\mathrm{gpk}, \mathrm{pk}_\rho)$, and parse σ as $(c_0, c_1, \ldots, c_{\delta-2}, \sigma')$; output $0/1 \leftarrow \mathsf{GVf}(\mathrm{gpk}, \mathrm{RL}, m, \sigma')$.

We specify the following tracing algorithm for our construction: given a message-signature pair (m, σ) with $\sigma = (c_0, c_1, \ldots, c_{\delta-2}, \sigma')$,

(1) for managers $\beta \in \mathcal{T}^i$, $i = 0, 1, \ldots, \delta-2$, compute $\beta' \leftarrow \mathsf{Dec}(\mathrm{hsk}(\beta), c_i)$, and output β' if $\beta' \in \beta$, otherwise output $\perp$;

(2) for managers $\beta \in \mathcal{T}^{\delta-1}$, parse $\mathrm{hpk}(\rho)$ as $(\mathrm{gpk}, \mathrm{pk}_\rho)$ and parse $\mathrm{hsk}(\beta)$ as $\{\mathrm{grt}[\alpha]\}_{\alpha\in\beta}$; for $\alpha \in \beta$, run $\mathsf{GVf}(\mathrm{gpk}, \{\mathrm{grt}[\alpha]\}, m, \sigma')$ and output the first index for which it says invalid/0, otherwise output $\perp$.

Theorem 1. Our verification algorithm is correct, if the underlying VLR-GS is correct; our tracing algorithm is correct, if both the underlying AE and VLR-GS are correct; our construction holds full/insider anonymity, if the VLR-GS holds full/insider anonymity respectively and the AE is secure; our construction is traceable, if the underlying VLR-GS is traceable.

Proof. See Appendixes F–I.

The size of the signing key in our construction is independent of the tree depth, and thus it is reduced by a factor of δ when compared with [3]. Also, to generate the first $(\delta-1)$ components, we performed comparatively more efficient encryption operations than group signings as used in [3]. Our signing algorithm enjoys the flexibility of trade-off between time and storage because the cipher-text chain can be precomputed without the target message, which helps in further accelerating the signing procedure at the cost of locally storing such chains.

* Corresponding author (email: ddlin@iie.ac.cn)

Table 1 Efficiency comparison between [3] and this letter

		Ref. [3]	Scheme 1	Scheme 2
		Full-anonymity	Full-anonymity	Insider-anonymity
Signature size	$\sigma_{i=0,1,\ldots,\delta-2}$	$\widetilde{O}(n^2)\cdot\lvert\mathcal{T}^i\rvert$	$\widetilde{O}(n)$	$\widetilde{O}(n)$
	$\sigma_{\delta-1}$	$\widetilde{O}(n^2)\cdot\lvert\mathcal{L}(\mathcal{T})\rvert$	$\widetilde{O}(n^2)\cdot\lvert\mathcal{L}(\mathcal{T})\rvert$	$\widetilde{O}(n)\cdot\log\lvert\mathcal{L}(\mathcal{T})\rvert$
Public key size	$\mathrm{hpk}(\rho)$	$\widetilde{O}(n^2)\cdot\lvert\mathcal{T}\rvert$	$\widetilde{O}(n^2)\cdot\lvert\mathcal{L}(\mathcal{T})\rvert$	$\widetilde{O}(n^2)\cdot\log\lvert\mathcal{L}(\mathcal{T})\rvert$
	$\mathrm{hpk}(\beta),\beta\in\mathcal{T}^{i=1,2,\ldots,\delta-2}$	–	$\widetilde{O}(n^2)$	$\widetilde{O}(n^2)$
Token size	$\mathrm{hrt}(\beta),\beta\in(\mathcal{T}-\mathcal{L}(\mathcal{T})-\rho)$	$\widetilde{O}(n^2)$	–	–
	$\mathrm{hrt}(\alpha),\alpha\in\mathcal{L}(\mathcal{T})$	$\widetilde{O}(n^2)$	$\widetilde{O}(n^2)$	$\widetilde{O}(n)$
Secret key size	$\mathrm{hsk}(\beta),\beta\in\mathcal{T}^{i=0,1,\ldots,\delta-2}$	$\widetilde{O}(n^2)\cdot\lvert\mathrm{child}(\beta)\rvert$	$\widetilde{O}(n)$	$\widetilde{O}(n)$
	$\mathrm{hsk}(\beta),\beta\in\mathcal{T}^{\delta-1}$	$\widetilde{O}(n^2)\cdot\lvert\mathrm{child}(\beta)\rvert$	$\widetilde{O}(n^2)\cdot\lvert\mathrm{child}(\beta)\rvert$	$\widetilde{O}(n)\cdot\lvert\mathrm{child}(\beta)\rvert$
	$\mathrm{hsk}(\alpha),\alpha\in\mathcal{L}(\mathcal{T})$	$\widetilde{O}(n^2)\cdot\delta$	$\widetilde{O}(n^2)$	$\widetilde{O}(n)\cdot\log\lvert\mathcal{L}(\mathcal{T})\rvert$

In [3], the manager's tracing cost is linear to the number of its direct children. Comparatively, for managers at not the penultimate depth, the tracing algorithm of our construction involves only a decryption operation with constant costs. Such efficiency improvement will show its power especially for a large set of managers. It is worth mentioning that for VLR-GS, it remains open how to design an efficient revocation mechanism (with sub-linear cost to the size of the revocation list). Obviously, progresses in solving this problem will contribute naturally to the tracing efficiency of managers at the penultimate depth.

Also, a signer's secret key in [3] includes the signing keys of its ancestors as well. As a result, by querying the secret keys of challenge identities' siblings, the adversary can obtain the revocation tokens which should be forbidden to avoid triviality, and thus breaks the anonymity. However, our construction additionally enables an insider-to-insider transformation, and this result contributes to more efficient instantiations as shown below.

Lattice-based instantiations. With rapid developments of quantum computing, lattice-based cryptography [6], a most promising post-quantum element, has become a top-notch research area. Hou et al. [3] have given a VLR-HGS scheme from lattices; however, as the size of both public key and signature is $N\cdot\widetilde{O}(n^2)$ in the underlying GKV scheme [7] (a variant), with N being the group size, their construction seems less satisfactory in terms of efficiency. By contrast, in the LLNW scheme [8], the sizes of public key and signature are $\widetilde{O}(n^2)\cdot\log N$ and $\widetilde{O}(n)\cdot\log N$, respectively. Its security is based on $\mathsf{SIVP}_{\gamma(n)}$, with $\gamma(n)=\widetilde{O}(n^{2.5})$ for insider-anonymity and $\gamma(n)=\widetilde{O}(n^{1.5})$ for traceability. Unfortunately, the LLNW scheme cannot be used to instantiate the construction [3] owing to the strong anonymity requirement. On the other hand, Gentry et al. [9] proposed a lattice-based AE scheme, which is secure assuming hardness of $\mathsf{SIVP}_{\widetilde{O}(n^{1.5})}$.

We present two instantiations of our construction. First, our Scheme 1 is instantiated with the GKV scheme (the same variant used in [3]) and the GPV scheme [9]. As a main result, our Scheme 2 is an insider-anonymous instantiation using the GPV scheme and the LLNW scheme. Since the tree size is polynomially bounded in n, $\Theta(\log n)$ bits are sufficient to specify each node in $\mathcal{T}$ by proper encoding. Thus, both our schemes use the k-bit version of the GPV scheme with $k=\Theta(\log n)$, where the sizes of public key, secret key and ciphertext are $\widetilde{O}(n^2)$, $\widetilde{O}(n)$ and $\widetilde{O}(n)$ respectively.

A detailed comparison between schemes in [3] and ours is given in Table 1. The comparison for public key size seems less straightforward by Table 1, and here we give further explanations. In [3], both the signing and the verification algorithm need $\mathrm{hpk}(\rho)$ of size $\widetilde{O}(n^2)\cdot|\mathcal{T}|$. In both our schemes, for signing purposes, it needs only the (non-empty) public keys associated with nodes from the signer to the root, with sizes of $\widetilde{O}(n^2)\cdot O(|\mathcal{L}(\mathcal{T})|)$ and $\widetilde{O}(n^2)\cdot O(\log|\mathcal{T}|)$ for Schemes 1 and 2, respectively; on the other hand, for verifications, it takes $\mathrm{hpk}(\rho)$ (more specifically gpk) of sizes $\widetilde{O}(n^2)\cdot|\mathcal{L}(\mathcal{T})|$ and $\widetilde{O}(n^2)\cdot\log|\mathcal{L}(\mathcal{T})|$ for Schemes 1 and 2 respectively. Overall, the public key size in Scheme 1 is comparable to that of [3], and Scheme 2 enjoys smaller public key than [3].

Summary. We propose a more efficient designing paradigm for VLR-HGS. For VLR-GS, backward unlinkability is quite useful in specific scenarios, and clearly, it is straightforward to extend our construction to capture this property. For future work, it is admirable to propose lattice-based VLR-HGS schemes with smaller sizes, and on the other hand, enhancing VLR-HGS to a fully dynamic case seems also attractive.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61872359, 61936008).

Supporting information Appendixes A–I. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Chaum D, van Heyst E. Group signatures. In: Proceedings of Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, 1991. 257–265
2 Trolin M, Wikström D. Hierarchical group signatures. In: Proceedings of the 32nd International Colloquium on Automata, Languages and Programming, Lisbon, 2005. 446–458
3 Hou L, Liu R, Qiu T, et al. Hierarchical group signatures with verifier-local revocation. In: Proceedings of the 20th International Conference on Information and Communications Security, Lille, 2018. 271–286
4 Boneh D, Shacham H. Group signatures with verifier-local revocation. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, 2004. 168–177
5 Bellare M, Boldyreva A, Desai A, et al. Key-privacy in public-key encryption. In: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, 2001. 566–582
6 Ajtai M. Generating hard instances of lattice problems (extended abstract). In: Proceedings of the 28th Annual ACM

Symposium on the Theory of Computing, Philadelphia, 1996. 99–108
7 Gordon S D, Katz J, Vaikuntanathan V. A group signature scheme from lattice assumptions. In: Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2010. 395–412
8 Langlois A, Ling S, Nguyen K, et al. Lattice-based group signature scheme with verifier-local revocation. In: Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, 2014. 345–361
9 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, 2018. 197–206