SCIENCE CHINA
Information Sciences

• LETTER •

January 2022, Vol. 65 119102:1–119102:3
https://doi.org/10.1007/s11432-019-2704-7

A CCA secure public key encryption scheme based on finite groups of Lie type

Haibo HONG[1*], Jun SHAO[1], Licheng WANG[2], Mande XIE[1], Guiyi WEI[1], Yixian YANG[2], Song HAN[2] & Jianhong LIN[3]

[1]*School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou* 310018*, China;*
[2]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[3]*Zhejiang Ponshine Information Technology Co.,Ltd., Hangzhou* 310000*, China*

Received 28 March 2019/Revised 24 August 2019/Accepted 13 December 2019/Published online 13 May 2021

Citation Hong H B, Shao J, Wang L C, et al. A CCA secure public key encryption scheme based on finite groups of Lie type. Sci China Inf Sci, 2022, 65(1): 119102, https://doi.org/10.1007/s11432-019-2704-7

Dear editor,

Lie groups have important applications in many branches of physics and mathematics, such as mathematical analysis, differential geometry, topology and quantum mechanics [1, 2]. As the important measure of algebraic properties of Lie groups, Lie algebras play an indispensable role while studying Lie groups.

In Lie theory, matrix Lie groups are more prominent and have classical matrix forms with their Lie algebras. Generally speaking, exponential mapping is the usual power series of Lie algebras, and the image set is contained within Lie groups. Besides, exponential mapping has intimate relationship with solving root problem of high degree univariate polynomial equations. However, exponential mapping is not suitable for cryptographic applications directly due to polynomial algorithms for solving high degree univariate polynomial equations [3]. Therefore, we attempt to probe cryptographic applications by combining exponential mapping with new intractable assumptions.

Our contribution. We put forward a series of intractable assumptions based on exponential mapping in finite groups of Lie type, including the non-abelian factorizing assumption and non-abelian inserting assumption. Moreover, in analogy with the construction of FullIdent in [4], we propose a new public key encryption scheme by employing the FO technique [5].

Definitions. For clarity, we first introduce the notations used in this article as shown in Table 1.

Definition 1 (Matrix exponential [2])**.** Let $X \in M_n(\mathbb{C})$ be an $n \times n$ complex matrix. Then the exponential of matrix X is defined as the usual power series $\exp^X = \sum_{m=0}^{\infty} \frac{X^m}{m!}$. In the case when X is a nilpotent matrix, $\exp^X = \sum_{m=0}^{\ell-1} \frac{X^m}{m!}$, where ℓ is the nilpotent index of X.

When $X \in M_n(p)$ is a nilpotent matrix with nilpotent index ℓ, $\exp^X = \sum_{m=0}^{\ell-1} \frac{X^m}{m!}$ is also well defined. Besides, $M_n(p)$ with the multiplication operation constitutes a finite semigroup.

Table 1 Notations

Item	Description
$\mathbb{R}$	Set of real numbers
$\mathbb{C}$	Set of complex numbers
$M_n(\mathbb{C})$	Set of $n \times n$ complex matrices
$GL_n(\mathbb{C})$	Set of all invertible $n \times n$ matrices with complex entries
$\mathbb{F}_p$	The finite field based on a large prime number p
$M_n(p)$	Set of $n \times n$ matrices with entries in $\mathbb{F}_p$
$GL_n(p)$	Set of all invertible $n \times n$ matrices with entries in $\mathbb{F}_p$
exp	Matrix exponential
$\langle X \rangle$	The finite group generated by a matrix X
$C_{\mathbb{G}}(\langle X \rangle)$	The centralizer of $\langle X \rangle$ in $\mathbb{G}$, where $\mathbb{G} = GL_n(p)$

Proposition 1 ([2]). Let X and Y be arbitrary $n \times n$ matrices. Then, we have

1. $\exp^0 = I_n$;
2. $\exp^X$ is invertible and $(\exp^X)^{-1} = \exp^{-X}$;
3. $\exp^{(\alpha+\beta)X} = \exp^{\alpha X} \cdot \exp^{\beta X}$ for all α and β in $\mathbb{C}$;
4. If $XY{=}YX$, then $\exp^{X+Y} = \exp^X \cdot \exp^Y = \exp^Y \cdot \exp^X$.

Item 2 presents that for an arbitrary matrix X, $\exp^X$ is an invertible matrix and belongs to $GL_n(\mathbb{C})$. Item 4 implies the commutativity of $\exp^X$ and $\exp^Y$ depends on X and Y, respectively. Furthermore, for the case in finite groups of Lie type, when $X, Y \in M_n(p)$ are two nilpotent matrices, items 1, 3, 4 also hold. Meanwhile, it is clear that α and β should belong to $\mathbb{F}_p$.

Remark 1. In Lie theory, $\exp^{tX} = \sum_{m=0}^{\infty} \frac{(tX)^m}{m!}$ is the exponential mapping from a Lie algebra X to its Lie group, where $t \in \mathbb{R}$. For a given X, $\exp^{tX} \in GL_n(\mathbb{C})$ is an injection from Proposition 1 (items 1,2,3). When $X \in M_n(p)$ is a nilpotent matrix, $\exp^{tX} = (\exp^X)^t = \sum_{m=0}^{\ell-1} \frac{(tX)^m}{m!} = \sum_{m=0}^{\ell-1} \frac{t^m X^m}{m!}$ is well defined when $t \in \mathbb{F}_p$. Moreover, $\exp^{tX}$

* Corresponding author (email: honghaibo1985@163.com)

is also an injection, which can be viewed as a finite group generated by X, denoted by $\langle X\rangle$.

Definition 2 (Non-abelian factorizing (NAF) problem)**.** Let $\mathbb{M}=M_n(p)$ be a semigroup, and $\mathbb{G}=GL_n(p)$ be the general linear group. Let $Z,R,T\in\mathbb{M}$ be three given nilpotent matrices such that $C_{\mathbb{G}}(\langle Z\rangle)=\langle Z\rangle$, $C_{\mathbb{G}}(\langle R\rangle)=\langle R\rangle$, $C_{\mathbb{G}}(\langle T\rangle)=\langle T\rangle$ and $\langle Z\rangle\cap\langle R\rangle\cap\langle T\rangle=\{I_n\}$. The non-abelian factorizing (NAF) problem with respect to $\mathbb{G},Z,R,T$, denoted by $\mathtt{NAF}^{\mathbb{G}}_{\exp^Z,\exp^R,\exp^T}$, is to find two elements $x,y\in\mathbb{F}_p$ such that $\exp^Z=\exp^{xR}\cdot\exp^{yT}$.

Note that the map $(x,y)\mapsto\exp^{xR}\cdot\exp^{yT}=\exp^Z$ is an injection with respect to Z, R and T ($C_{\mathbb{G}}(\langle Z\rangle)=\langle Z\rangle$, $C_{\mathbb{G}}(\langle R\rangle)=\langle R\rangle$, $C_{\mathbb{G}}(\langle T\rangle)=\langle T\rangle$ and $\langle Z\rangle\cap\langle R\rangle\cap\langle T\rangle=\{I_n\}$). Therefore, there seems to be no better methods than a naive method to solving (x,y). Next, we discuss the NAF problem.

Theorem 1. The NAF problem is equivalent to solving DLP in $\mathbb{F}_p$, and its complexity is $\Theta(\mathrm{e}^{c(\log p)^{\alpha}(\log\log p)^{1-\alpha}})$ with neglecting the polynomial time for solving the overdetermined linear system, where $\alpha=1/3$, $c=(\frac{32}{9})^{1/3}$.

Proof. Let $A=\exp^{xR}$, $B=\exp^{yT}$ and $C=\exp^Z=\exp^{xR}\cdot\exp^{yT}$, where $C_{\mathbb{G}}(\langle Z\rangle)=\langle Z\rangle$, $C_{\mathbb{G}}(\langle R\rangle)=\langle R\rangle$, $C_{\mathbb{G}}(\langle T\rangle)=\langle T\rangle$, $\langle Z\rangle\cap\langle R\rangle\cap\langle T\rangle=\{I_n\}$, and x, y belong to $\mathbb{F}_p$. In order to recover x and y from $\exp^{xR}\cdot\exp^{yT}$, an efficient way is to extract useful information from the eigenvalues of $\exp^R$ and $\exp^T$. It is well known that any matrix is similar to a Jordan canonical form. For the general case, there is a probability polynomial-time reduction of DLP in $GL_n(p)$ to DLP in $\mathbb{F}_p$ [6]. That means DLP in $GL_n(p)$ is no harder than DLP in $\mathbb{F}_p$. Thus, we attempt to build the reduction between the NAF problem and DLP in $\mathbb{F}_p$. Furthermore, considering the uncertainty of Jordan canonical form of $\exp^R$ and $\exp^T$, we simplify the NAF problem by assuming that $\exp^R$ and $\exp^T$ have different eigenvalues. Then, we utilize eigenvalue decomposition for discussing this case.

In particular, if there exist invertible matrices S_R and S_T satisfying that

$$S_R^{-1}\cdot\exp^R\cdot S_R=\Lambda_R=\begin{pmatrix}\sigma_1&&&\\&\sigma_2&&\\&&\ddots&\\&&&\sigma_n\end{pmatrix}$$

and

$$S_T^{-1}\cdot\exp^T\cdot S_T=\Lambda_T=\begin{pmatrix}\delta_1&&&\\&\delta_2&&\\&&\ddots&\\&&&\delta_n\end{pmatrix},$$

then,

$$\begin{aligned}C&=\exp^{xR}\cdot\exp^{yT}\\&=S_R\Lambda_R^xS_R^{-1}S_T\Lambda_T^yS_T^{-1}\\&\Rightarrow\Lambda_R^{-x}S_R^{-1}CS_T=S_R^{-1}S_T\Lambda_T^y.\end{aligned}$$

Therefore, recovering the diagonal matrices Λ_R^{-x} and Λ_T^y amounts to solving an overdetermined linear system of n^2 equations and n unknown pairs $(\sigma_i^{-x},\delta_i^y)$ for $1\leqslant i\leqslant n$, the complexity of which is no more than $\Theta(n^3)$ from the best current asymptotic result [7]. Furthermore, there is a unique pair (x,y) ensuring that all n pairs $(\sigma_i^{-x},\delta_i^y)$ satisfy all n^2 equations. Hence, neglecting the complexity of solving overdetermined linear system, recovering the pair (x,y) is equivalent to solving DLP in $\mathbb{F}_p$. Consequently, according to the classical index calculation algorithm (ICA) for high characteristic p [8], the complexity of NAF problem is $\Theta(\mathrm{e}^{c(\log p)^{\alpha}(\log\log p)^{1-\alpha}})$, where $\alpha=1/3$, $c=(\frac{32}{9})^{1/3}$.

Definition 3 (Non-Abelian inserting (NAI) problem)**.** Let $\mathbb{M}=M_n(p)$ be a semigroup, and $\mathbb{G}=GL_n(p)$ be the general linear group. Let $X,Y,R,T\in\mathbb{M}$ be four given nilpotent matrices such that $C_{\mathbb{G}}(\langle X\rangle)=\langle X\rangle$, $C_{\mathbb{G}}(\langle Y\rangle)=\langle Y\rangle$, $C_{\mathbb{G}}(\langle R\rangle)=\langle R\rangle$, $C_{\mathbb{G}}(\langle T\rangle)=\langle T\rangle$ and $\langle X\rangle\cap\langle Y\rangle\cap\langle R\rangle\cap\langle T\rangle=\{I_n\}$. The non-Abelian inserting (NAI) problem with respect to $\mathbb{G},X,Y,R,T$, denoted by $\mathtt{NAI}^{\mathbb{G}}_{\exp^X,\exp^Y,\exp^R,\exp^T}$, is to recover $\exp^{(a+c)R}\cdot\exp^{(b+d)T}$ from the given pair $(\exp^{aR}\cdot\exp^{bT},\ \exp^{cR}\cdot\exp^{dT})\in\mathbb{G}^2$, where a,b,c,d are selected from $\mathbb{F}_p$ such that $\exp^X=\exp^{aR}\cdot\exp^{bT}$ and $\exp^Y=\exp^{cR}\cdot\exp^{dT}$.

It is easy to see that a solution to NAF problem would imply a solution to NAI problem. Specifically, the adversary can use the solution of the NAF problem to get a,b,c,d with input $\exp^{aR}\cdot\exp^{bT}$ and $\exp^{cR}\cdot\exp^{dT}$, respectively. After that, the adversary can obtain the NAI solution $\exp^{(a+c)R}\cdot\exp^{(b+d)T}$. Actually, due to the non-commutability, the NAI problem looks very difficult. As far as we know, there is no better solution for the NAI problem other than solving NAF problem.

Full Scheme. The presented scheme based on the NAI problem is comprised of three algorithms: key pair generation algorithm `KeyGen`, encryption algorithm `Enc`, and decryption algorithm `Dec`. The details are presented as follows.

`KeyGen`(κ): It takes the security parameters κ_1, κ_2 as input, it outputs a public key $\mathrm{pk}=(\mathbb{M},\mathbb{G},Z,R,T,\Sigma,H_1,H_2,H_3)$, and the corresponding private key $\mathrm{sk}=(\exp^{r\cdot R},\exp^{t\cdot T})$. The key pair satisfies the following conditions.

- $\mathbb{M}=M_n(p)$ is a finite semigroup with respect to multiplication operation.
- $\mathbb{G}=GL_n(p)$ is a finite non-abelian group of Lie type with rank n.
- p is a large prime number with $p=\Theta(2^{\kappa_1})$, and $|\mathbb{G}|\approx|\mathbb{M}|=\Theta(p^{n^2})=\Theta(2^{n^2\kappa_1})$.
- $Z,R,T\in\mathbb{M}$ are three given non-commutative nilpotent matrices ($C_{\mathbb{G}}(\langle Z\rangle)=\langle Z\rangle$, $C_{\mathbb{G}}(\langle R\rangle)=\langle R\rangle$, $C_{\mathbb{G}}(\langle T\rangle)=\langle T\rangle$ and $\langle Z\rangle\cap\langle R\rangle\cap\langle T\rangle=\{I_n\}$), where r and t are selected from $\mathbb{F}_p$ such that $\Sigma=\exp^Z=\exp^{r\cdot R}\cdot\exp^{t\cdot T}$.
- H_1,H_2,H_3 are three cryptographically secure hash functions: $H_1:\{0,1\}^{\kappa_2+\ell}\to\mathbb{F}_p\times\mathbb{F}_p$, $H_2:\mathbb{G}\to\{0,1\}^{\kappa_2}$, and $H_3:\{0,1\}^{\kappa_2}\to\{0,1\}^{\ell}$, where ℓ is the bit length of the message.

At last, r,t should be securely destroyed.

`Enc`(pk,m): It takes a public key $\mathrm{pk}=(\mathbb{M},\mathbb{G},Z,R,T,\Sigma,H_1,H_2,H_3)$ and a message $m\in\{0,1\}^{\ell}$ as input, and it outputs the corresponding ciphertext $C=(C_1,C_2,C_3)$ by performing the following steps.

- Choose a random number σ from $\{0,1\}^{\kappa_2}$.
- Compute $(s_r,s_t)=H_1(\sigma||m)$.
- Compute $C_1=H_2(\exp^{s_r\cdot R}\cdot\Sigma\cdot\exp^{s_t\cdot T})\oplus\sigma$.
- Compute $C_2=\exp^{s_r\cdot R}\cdot\exp^{s_t\cdot T}$.
- Compute $C_3=H_3(\sigma)\oplus m$.

$\mathtt{Dec}(\mathrm{sk}, C)$: It takes a private key $\mathrm{sk} = (\exp^{r\cdot R}, \exp^{t\cdot T})$ and a ciphertext $C = (C_1, C_2, C_3)$ as input, and it outputs the corresponding message using the following steps.

- Compute $\sigma' = C_1 \oplus H_2(\exp^{r\cdot R} \cdot C_2 \cdot \exp^{t\cdot T})$.
- Compute $m' = C_3 \oplus H_3(\sigma')$.
- Compute $(s'_r, s'_t) = H_1(\sigma' || m')$.
- Check whether both $C_1 = H_2(\exp^{s'_r\cdot R} \cdot \Sigma \cdot \exp^{s'_t\cdot T}) \oplus \sigma'$ and $C_2 = \exp^{s'_r\cdot R} \cdot \exp^{s'_t\cdot T}$ hold. If they hold, set $m = m'$; otherwise, set $m = \perp$.
- Output m.

Remark 2. The interested reader can refer to the supplementary file (Appendixes A and B) for the formal security analysis and the performance of our proposal.

Acknowledgements This work was partially supported by the National Natural Science Foundation of China (NSFC) (Grant Nos. 61602408, 61972050, 61972352, U1709217), Zhejiang Provincial Natural Science Foundation (Grant Nos. LY19F020005, LY18F020009, LZ18F020003), and Key Research and Development Program of Hangzhou (Grant No. 20182011A46).

Supporting information Appendixes A and B. 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 Gilmore R. Lie groups, Lie algebras, and Some of Their Applications. Massachusetts: Courier Corporation, 2012
2 Hall B. Lie Groups, Lie Algebras, and Representations: an Elementary Introduction. Berlin: Springer, 2015
3 Courtois N, Klimov A, Patarin J, et al. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Proceeding of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2000. 392–407
4 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. In: Proceeding of Annual International Cryptology Conference. Berlin: Springer, 2001. 213–229
5 Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes. In: Proceeding of Annual International Cryptology Conference. Berlin: Springer, 1999. 537–554
6 Menezes A J, Wu Y H. The discrete logarithm problem in $GL(n, q)$. Ars Combinatoria, 1997, 47: 23–32
7 Joux A. Algorithmic Cryptanalysis. Boca Raton: Chapman and Hall/CRC, 2009
8 Joux A, Odlyzko A, Pierrot C. The past, evolving present, and future of the discrete logarithm. In: Open Problems in Mathematics and Computational Science. Berlin: Springer, 2014. 5–36