Publ. Math. Debrecen
94/3-4 (2019), 467–475
DOI: 10.5486/PMD.2019.8433

A generalization of Menon's identity to higher exponent

By YAN LI (Beijing), DAEYEOUL KIM (Jeonju) and RUI QIAO (Beijing)

Abstract. In this note, we shall explicitly compute the following sum

$$\sum_{\substack{1\le a,b_1,\dots,b_k\le n\\ \gcd(a,n)=1}} \gcd(a^\ell-1,b_1,\dots,b_k,n),$$

where $n\ge 1$, $k\ge 0$, $l\ge 1$ are integers. Our results extend Menon's identity and Sury's identity (i.e., $\ell=1$ in the above summation) to higher exponents. Note that in the case $k=0$, some of our results are recovered by the results of [21].

1. Introduction

In 1965, P. K. Menon [6] discovered the following beautiful identity:

$$\sum_{a\in\mathbb{Z}_n^*} \gcd(a-1,n)=\varphi(n)\tau(n), \tag{1}$$

where for a positive integer n, $\mathbb{Z}_n^*$ is the group of units of the ring $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$, $\gcd(\ ,\ )$ represents the greatest common divisor, φ is the Euler totient function and $\tau(n)$ is the number of positive divisors of n.

Mathematics Subject Classification: 11A07, 11A25.
Key words and phrases: Menon's identity, Dirichlet character, Dirichlet convolution, divisor function, Euler's totient function, Chinese remainder theorem.
The first author was supported by the Open Project funded by State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), and the second author was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07041132).
The second author is the corresponding author.

Menon's identity (1) is an interesting number-theoretical identity. Many researchers generalized it in various directions. In 2009, B. Sury [19] found that

$$\sum_{\substack{a\in\mathbb{Z}_n^*\\ b_1,\ldots,b_k\in\mathbb{Z}_n}} \gcd(a-1,b_1,\ldots,b_k,n)=\varphi(n)\sigma_k(n), \tag{2}$$

where $\sigma_k(n)=\sum_{d|n} d^k$, by using the Cauchy–Frobenius–Burnside lemma. It is also interesting to note that Miguel [12]–[13] extended identities (1) and (2) from $\mathbb{Z}$ to any residually finite Dedekind domain.

Recently, Zhao and Cao [25] derived the following elegant Menon-type identity with a Dirichlet character

$$\sum_{a\in\mathbb{Z}_n^*} \gcd(a-1,n)\chi(a)=\varphi(n)\tau\left(\frac{n}{d}\right), \tag{3}$$

where χ is a Dirichlet character modulo n with conductor d. Identity (3) can be viewed giving the explicit Fourier coefficients of the function $f(a)=\gcd(a-1,n)$ on the Abelian group $(\mathbb{Z}/n\mathbb{Z})^*$.

A function $f:\mathbb{Z}\to\mathbb{C}$ is called an even function (mod n) if $f(\gcd(k,n))=f(k)$ holds for any $k\in\mathbb{Z}$. In [22], Tóth further extended (3) from the gcd function to any even function (mod n). In fact, let f be an even function (mod n) and $s\in\mathbb{Z}$. Tóth got the following identity :

$$\sum_{k=1}^{n} f(k-s)\chi(k)=\varphi(n)\chi^*(s)\sum_{\substack{\delta|n/d\\(\delta,s)=1}}\frac{(\mu*f)(\delta d)}{\varphi(\delta d)}, \tag{4}$$

where χ^* is the primitive character (mod d) that induces χ, and $\mu*f$ denotes the Dirichlet convolution of the Möbius function μ and the arithmetic function f (see [22, Theorem 2.4]).

In [10], Li, Hu and Kim further extended identities (2) and (3). They obtained the following identity with a Dirichlet character χ:

$$\sum_{\substack{a\in\mathbb{Z}_n^*\\ b_1,\ldots,b_k\in\mathbb{Z}_n}} \gcd(a-1,b_1,...,b_k,n)\chi(a)=\varphi(n)\sigma_k\left(\frac{n}{d}\right). \tag{5}$$

For other related works on Menon's identity, see [2]–[5], [7]–[9], [11], [14], [16]–[18], [20]–[24], and references therein.

In this note, as an application of (5), we will explicitly compute

$$\sum_{\substack{a\in\mathbb{Z}_n^*\\ b_1,\dots,b_k\in\mathbb{Z}_n}} \gcd(a^\ell-1,b_1,\dots,b_k,n) \tag{6}$$

by techniques of characters, where ℓ is any positive integer. Our main result is Theorem 2.5, which relates (6) to a certain kind of Dirichlet convolution. For $\ell=1$, Theorem 2.5 easily reduces to Sury's identity (2).

Note that in the case $k=0$, Corollary 2.6 is recovered by [21, Corollary 15]). Also, if $k=0$ and n is odd, then Theorem 2.5 is recovered by [21, Corollary 16]). Richards [14] remarked that for any polynomial g with integer coefficients,

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} \gcd(g(k),n)=\varphi(n)\sum_{d\mid n}\eta_g(d),$$

where $\eta_g(d)$ stands for the number of solutions $x \pmod d$ of the congruence $g(x)\equiv 0 \pmod d$ such that $\gcd(x,d)=1$ (see [21]).

2. Main results

Let

$$\mathbb{Z}_n^* \xrightarrow{L} \mathbb{Z}_n^* : L(a)=a^\ell, \quad \forall\ a\in\mathbb{Z}_n^*,$$

be the ℓ-th power map. Denote its image by $\operatorname{im} L$ and its kernel by $\ker L$. Clearly, we have

$$\sum_{\substack{a\in\mathbb{Z}_n^*\\ b_1,\dots,b_k\in\mathbb{Z}_n}} \gcd(a^\ell-1,b_1,\dots,b_k,n)=|\ker L|\sum_{\substack{a\in\operatorname{im} L\\ b_1,\dots,b_k\in\mathbb{Z}_n}} \gcd(a-1,b_1,\dots,b_k,n), \tag{7}$$

where $|\ |$ represents the cardinality.

To proceed on, we need the following lemma, which transforms the summation on the subgroup $\operatorname{im} L$ to the summation on the whole group $\mathbb{Z}_n^*$ with characters. From now on, for a finite Abelian group G, we denote the group of characters of G by $\widehat{G}$.

Lemma 2.1. For $a\in\mathbb{Z}_n^*$,

$$\sum_{\substack{\chi\in\widehat{\mathbb{Z}_n^*}\\ \chi^\ell=1}} \chi(a)=\begin{cases}|\ker L|, & \text{if } a\in\operatorname{im} L,\\ 0, & \text{otherwise.}\end{cases}$$

PROOF. By definition of $\widehat{\mathbb{Z}_n^*}[\ell]$, we derive

$$\widehat{\mathbb{Z}_n^*}[\ell] = \{\chi \in \widehat{\mathbb{Z}_n^*} | \chi^\ell = 1\} = \{\chi \in \widehat{\mathbb{Z}_n^*} | \chi(\operatorname{im} L) = 1\}. \tag{8}$$

Therefore, if $a \in \operatorname{im} L$, then

$$\sum_{\chi^\ell=1} \chi(a) = \sum_{\chi^\ell=1} 1 = |\ker L|.$$

The last equality is due to $\widehat{\mathbb{Z}_n^*} \backsimeq \mathbb{Z}_n^*$ as Abelian groups (see [1, Proposition 2.1.16]). Otherwise, for $a \notin \operatorname{im} L$, there is a character ψ of $\mathbb{Z}_n^*/\operatorname{im} L$ such that $\psi(\overline{a}) \neq 1$, where $\overline{a}$ is the image of a in $\mathbb{Z}_n^*/\operatorname{im} L$ (see [1, Corollary 2.1.18]). Denote the lifting of ψ in $\widehat{\mathbb{Z}_n^*}$, i.e., the composition of ψ and the natural homomorphism $\mathbb{Z}_n^* \to \mathbb{Z}_n^*/\operatorname{im} L$, still by ψ. Hence, $\psi(a) \neq 1$ and $\psi(\operatorname{im} L) = 1$, which implies that $\psi \in \widehat{\mathbb{Z}_n^*}[\ell]$ by (8). Since $\widehat{\mathbb{Z}_n^*}[\ell]$ is a group and ψ belongs to it, we have

$$\sum_{\chi^\ell=1} \chi(a) = \sum_{\chi^\ell=1} \psi\chi(a) = \psi(a) \sum_{\chi^\ell=1} \chi(a).$$

As $\psi(a) \neq 1$, we get

$$\sum_{\chi^\ell=1} \chi(a) = 0, \quad \text{for all } a \notin \operatorname{im} L. \qquad \square$$

Substituting Lemma 2.1 into (7) and changing the order of summation, we obtain

$$\begin{aligned}
&\sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\ldots,b_k\in\mathbb{Z}_n}} \gcd(a^\ell - 1, b_1, \ldots, b_k, n) \\
&= |\ker L| \sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\cdots,b_k\in\mathbb{Z}_n}} \left(\frac{1}{|\ker L|} \sum_{\chi^\ell=1} \chi(a) \right) \gcd(a - 1, b_1, \ldots, b_k, n) \\
&= \sum_{\chi^\ell=1} \sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\ldots,b_k\in\mathbb{Z}_n}} \chi(a)\gcd(a - 1, b_1, \ldots, b_k, n).
\end{aligned}$$

Substituting (5) into the above equation, finally we prove the following theorem:

Theorem 2.2. *For $\ell \in \mathbb{N} \cup \{0\}$,*

$$\sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\ldots,b_k\in\mathbb{Z}_n}} \gcd(a^\ell - 1, b_1, \ldots, b_k, n) = \varphi(n) \sum_{\substack{a\in\widehat{\mathbb{Z}_n^*} \\ \chi^\ell=1}} \sigma_k\left(\frac{n}{d_\chi}\right), \tag{9}$$

where d_χ is the conductor of χ.

For $d|n$, let

$$N_n^{(\ell)}(d) := |\{\chi \in \widehat{\mathbb{Z}_n^*} | \chi^\ell = 1, \text{the conductor of } \chi \text{ is } d\}|. \tag{10}$$

In the following, we will calculate $N_n^{(\ell)}(d)$ explicitly.

To do this, we first show $N_n^{(\ell)}(d)$ does not depend on n.

For $m|n$, since the natural homomorphism $\mathbb{Z}_n^* \to \mathbb{Z}_m^*$ sending $a \bmod n$ to $a \bmod m$ is surjective, the induced homomorphism $\widehat{\mathbb{Z}_m^*} \to \widehat{\mathbb{Z}_n^*}$ is injective. Denote the image of $\widehat{\mathbb{Z}_m^*}$ in $\widehat{\mathbb{Z}_n^*}$ by T_m. If $m'|m''|n$, then the following diagram of natural homomorphisms is commutative.

$$\begin{array}{ccc} \mathbb{Z}_n^* & \to & \mathbb{Z}_{m'}^* \\ \downarrow & \nearrow & \\ \mathbb{Z}_{m''}^* & & \end{array}$$

This implies that

$$T_{m'} \subset T_{m''} \subset \widehat{\mathbb{Z}_n^*}, \quad \text{if } m'|m''|n. \tag{11}$$

Let $n = \prod_{i=1}^{s} p_i^{v_i}$ be the prime factorization of n. The Chinese remainder theorem implies that $\mathbb{Z}_n^*$ is isomorphic to the direct product of $\mathbb{Z}_{p_i^{v_i}}^*$ naturally, i.e.,

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{v_1}}^* \times \mathbb{Z}_{p_2^{v_2}}^* \times \cdots \times \mathbb{Z}_{p_s^{v_s}}^*.$$

Therefore, $\widehat{\mathbb{Z}_n^*}$ is the direct product of $T_{p_i^{v_i}}$, i.e.,

$$\widehat{\mathbb{Z}_n^*} = T_{p_1^{v_1}} \times T_{p_2^{v_2}} \times \cdots \times T_{p_s^{v_s}}. \tag{12}$$

Now for $m', m''|n$, let

$$m' = \prod_{i=1}^{s} p_i^{v_i'} \quad \text{and} \quad m'' = \prod_{i=1}^{s} p_i^{v_i''},$$

where $0 \leqslant v_i', v_i'' \leqslant v_i$. The same reasoning shows that

$$T_{m'} = T_{p_1^{v_1'}} \times T_{p_2^{v_2'}} \times \cdots \times T_{p_s^{v_s'}}, \qquad T_{m''} = T_{p_1^{v_1''}} \times T_{p_2^{v_2''}} \times \cdots \times T_{p_s^{v_s''}}, \tag{13}$$

where $T_{p_i^{v_i'}}, T_{p_i^{v_i''}}$ are subgroups of $T_{p_i^{v_i}}$ for $1 \leqslant i \leqslant s$. As (12) is a direct product, we get

$$T_{m'} \bigcap T_{m''} = \prod_{i=1}^{s} T_{p_i^{v_i'}} \bigcap T_{p_i^{v_i''}} = \prod_{i=1}^{s} T_{p_i^{\min\{v_i', v_i''\}}} \tag{14}$$

by (13). Therefore,

$$T_{m'} \bigcap T_{m''} = T_{\gcd(m',m'')}, \quad \text{for } m', m''|n. \tag{15}$$

For $\chi \in \widehat{\mathbb{Z}_n^*}$, the conductor of χ is the smallest (for divisibility) positive integer $d|n$ such that $\chi \in T_d$. Since $\widehat{\mathbb{Z}_d^*} \to \widehat{\mathbb{Z}_n^*}$ is an injective homomorphism, the following two sets

$$\{\chi \in \widehat{\mathbb{Z}_n^*} | \chi^\ell = 1, \text{the conductor of } \chi \text{ is } d\}$$

and

$$\{\chi \in \widehat{\mathbb{Z}_d^*} | \chi^\ell = 1, \text{the conductor of } \chi \text{ is } d\}$$

are in one-to-one correspondence. Hence, by (10),

$$N_n^{(\ell)}(d) = N_d^{(\ell)}(d) \tag{16}$$

does not depend on n. We denote $N_d^{(\ell)}(d)$, i.e., the number of primitive characters modulo d with orders dividing ℓ, by $N^{(\ell)}(d)$ in short.

Lemma 2.3. *For $\ell \in \mathbb{N}$, let*

$$C^{(\ell)}(n) := |\{\chi \in \widehat{\mathbb{Z}_n^*} | \chi^\ell = 1\}|. \tag{17}$$

Then $C^{(\ell)}(n)$ is a multiplicative arithmetic function such that

$$C^{(\ell)}(p^v) = \gcd(\ell, \varphi(p^v)), \tag{18}$$

and

$$C^{(\ell)}(2^v) = \begin{cases} \gcd(\ell, \varphi(2^v)), & v = 1, 2, \\ \gcd(\ell, 2)\gcd(\ell, \varphi(2^{v-1})), & v \geqslant 3, \end{cases} \tag{19}$$

where p is an odd prime and v is a positive integer.

Proof. From [1, Proposition 2.1.16], we know $\widehat{\mathbb{Z}_n^*}$ is non-canonically isomorphic to $\mathbb{Z}_n^*$. Therefore,

$$C^{(\ell)}(n) = |\{a \in \mathbb{Z}_n^* | a^\ell = 1\}. \tag{20}$$

Equation (20) and the Chinese remainder theorem imply that $C^{(\ell)}(n)$ is multiplicative with respect to n. Since $\mathbb{Z}_{p^v}^*$ is a cyclic group of order $\varphi(p^v)$ for p being an odd prime, $\mathbb{Z}_{2^v}^*$ is cyclic for $v = 1, 2$ and $\mathbb{Z}_{2^v}^*$ is isomorphic to $\mathbb{Z}/2^{v-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $v \geqslant 3$ (see [1, Proposition 2.1.24] or [15, p. 44]), we get the desired result. □

Lemma 2.4. *The number of primitive characters modulo d with orders dividing ℓ is equal to*

$$N^{(\ell)}(d) = (\mu * C^{(\ell)})(d). \tag{21}$$

Proof. Combining (10) and (17), we get

$$\sum_{d|n} N_n^{(\ell)}(d) = C^{(\ell)}(n). \tag{22}$$

By (16),

$$N_n^{(\ell)}(d) = N^{(\ell)}(d) \tag{23}$$

does not depend on n. Substituting (23) into (22) and using the Möbius inversion formula, we get (21). □

Theorem 2.5. *For $\ell \in \mathbb{N} \cup \{0\}$,*

$$\sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\dots,b_k\in\mathbb{Z}_n}} \gcd(a^\ell - 1, b_1, \dots, b_k, n) = \varphi(n)(\mathrm{id}_k * C^{(\ell)})(n),$$

where $C^{(\ell)}(n)$ is the number of ℓ-torsion elements of $\mathbb{Z}_n^*$, which is a multiplicative arithmetic function explicitly determined by (18) *and* (19), *and $\mathrm{id}_k(n) = n^k$.*

Proof. By Theorem 2.2 and equation (10), we have

$$\sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\dots,b_k\in\mathbb{Z}_n}} \gcd(a^\ell - 1, b_1, \dots, b_k, n) = \varphi(n) \sum_{\substack{\chi\in\widehat{\mathbb{Z}_n^*} \\ \chi^\ell = 1}} \sigma_k\left(\frac{n}{d_\chi}\right) = \varphi(n) \sum_{d|n} \sigma_k\left(\frac{n}{d}\right) N_n^{(\ell)}(d).$$

Substituting Lemma 2.4 and equation (23) into the above equation, we get

$$\sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\dots,b_k\in\mathbb{Z}_n}} \gcd(a^\ell - 1, b_1, \dots, b_k, n) = \varphi(n)(\sigma_k * N^{(\ell)})(n) = \varphi(n)(\sigma_k * \mu * C^{(\ell)})(n).$$

Since $\sigma_k * \mu = \mathrm{id}_k$, we get the desired identity. □

Corollary 2.6. *Let $w(n)$ be the number of distinct prime divisors of n. Then*

$$\sum_{\substack{a\in\mathbb{Z}_n^* \\ b_1,\dots,b_k\in\mathbb{Z}_n}} \gcd(a^2 - 1, b_1, \dots, b_k, n) = \varphi(n)(\mathrm{id}_k * C^{(2)})(n),$$

where $\mathrm{id}_k(n) = n^k$ *and*

$$C^{(2)}(n) = \begin{cases} 2^{w(n)-1}, & 2||n, \\ 2^{w(n)}, & 2 \nmid n \text{ or } 2^2||n, \\ 2^{w(n)+1}, & 2^3|n. \end{cases}$$

Here, $p^i||n$ *means* $p^i|n$ *and* $p^{i+1} \nmid n$.

PROOF. Let $\ell = 2$ in Theorem 2.5, equations (18) and (19). □

Remark. Note that $C^{(2)}(n)$ is closely related to $2^{w(n)}$, i.e., the number of square-free divisors of n.

Remark. When $\ell=1$, Theorem 2.5 reduces to Sury's identity(2), as $C^{(\ell)}(n)=1$ for all positive integers n. In the case $k = 0$, Corollary 2.6 is recovered by [21, Corollary 15]). Also, if $k = 0$ and n is odd, then Theorem 2.5 is recovered by [21, Corollary 16]).

ACKNOWLEDGEMENTS. We are grateful to the anonymous referee, who carefully read the paper in a short time and gave valuable suggestions, which made the paper more elegant and readable.

References

[1] H. COHEN, Number Theory. Vol. I. Tools and Diophantine Equations, Graduate Texts in Mathematics, Vol. **239**, *Springer-Verlag*, *New York*, 2007.

[2] P. HAUKKANEN, Menon's identity with respect to a generalized divisibility relation, *Aequationes Math.* **70** (2005), 240–246.

[3] P. HAUKKANEN, J. WANG, High degree analogs of Menon's identity, *Indian J. Math.* **39** (1997), 37–42.

[4] P. HAUKKANEN and J. WANG, A generalization of Menon's identity with respect to a set of polynomials, *Portugal. Math.* **53** (1996), 331–337.

[5] P. H. VAN DER KAMP, On the Fourier transform of the greatest common divisor, *Integers* **13** (2013), Paper No. A24, 16 pp.

[6] P. KESAVA MENON, On the sum $\sum(a-1,n)[(a,n)=1]$, *J. Indian Math. Soc. (N.S.)* **29** (1965), 155–163.

[7] Y. LI and D. KIM, A Menon-type identity with many tuples of group of units in residually finite Dedekind domains, *J. Number Theory* **175** (2017), 42–50.

[8] Y. LI and D. KIM, Menon-type identities derived from actions of subgroups of general linear groups, *J. Number Theory* **179** (2017), 97–112.

[9] Y. LI and D. KIM, Menon-type identities with additive characters, *J. Number Theory* **192** (2018), 373–385.

[10] Y. LI, X. HU and D. KIM, A generalization of Menons identity with Dirichlet characters, *Int. J. Number Theory* **14** (2018), 2631–2639.

[11] Y. Li, X. Hu and D. Kim, A Menon-type Identity with multiplicative and additive characters, *Taiwanese J. Math.* (2019) (*to appear*), https://projecteuclid.org/euclid.twjm/1531382426.

[12] C. Miguel, Menon's identity in residually finite Dedekind domains, *J. Number Theory* **137** (2014), 179–185.

[13] C. Miguel, A Menon-type identity in residually finite Dedekind domains, *J. Number Theory* **164** (2016), 43–51.

[14] I. M. Richards, A remark on the number of cyclic subgroups of a finite group, *Amer. Math. Monthly* **91** (1984), 571–572.

[15] M. Rosen and K. Ireland, A Classical Introduction to Modern Number Theory, Second Edition, Graduate Texts in Mathematics, Vol. **84**, *Springer-Verlag*, *New York*, 1990.

[16] W. Schramm, The Fourier transform of functions of the greatest common divisor, *Integers* **8** (2008), A50, 7 pp.

[17] V. Sita Ramaiah, Arithmetical sums in regular convolutions, *J. Reine Angew. Math.* **303/304** (1978), 265–283.

[18] R. Sivaramakrishnan, A number-theoretic identity, *Publ. Math. Debrecen* **21** (1974), 67–69.

[19] B. Sury, Some number-theoretic identities from group actions, *Rend. Circ. Mat. Palermo (2)* **58** (2009), 99–108.

[20] M. Tărnăuceanu, A generalization of Menon's identity, *J. Number Theory* **132** (2012), 2568–2573.

[21] L. Tóth, Menon's identity and arithmetical sums representing functions of several variables, *Rend. Semin. Mat. Univ. Politec. Torino* **69** (2011), 97–110.

[22] L. Tóth, Menon-type identities concerning Dirichlet characters, *Int. J. Number Theory* **14** (2018), 1047–1054.

[23] L. Tóth, Weighted gcd-sum functions, *J. Integer Seq.* **14** (2011), Article 11.7.7, 10 pp.

[24] L. Tóth and P. Haukkanen, The discrete Fourier transform of r-even functions, *Acta Univ. Sapientiae Math.* **3** (2011), 5–25.

[25] X.-P. Zhao and Z-F. Cao, Another generalization of Menon's identity, *Int. J. Number Theory* **13** (2017), 2373–2379.

DAEYEOUL KIM
DEPARTMENT OF MATHEMATICS AND
INSTITUTE OF PURE AND APPLIED
MATHEMATICS
CHONBUK NATIONAL UNIVERSITY
567 BAEKJE-DAERO, DEOKJIN-GU
JEONJU-SI, JEOLLABUK-DO 54896
SOUTH KOREA

E-mail: kdaeyeoul@jbnu.ac.kr

RUI QIAO
DEPARTMENT OF APPLIED MATHEMATICS
CHINA AGRICULTURAL UNIVERSITY
BEIJING 100083
CHINA

E-mail: 470258057@163.com

YAN LI
DEPARTMENT OF APPLIED MATHEMATICS
CHINA AGRICULTURAL UNIVERSITY
BEIJING 100083
CHINA

AND

STATE KEY LABORATORY OF
INFORMATION SECURITY
INSTITUTE OF INFORMATION
ENGINEERING
CHINESE ACADEMY OF SCIENCES
BEIJING 100093
CHINA

E-mail: liyan_00@cau.edu.cn

(Received August 30, 2018; revised January 24, 2019)