ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2016, Vol. 37, No. 3, pp. 234–239. © Pleiades Publishing, Ltd., 2016.

Towards an Operad-Based Cryptography: Applications of Commutative Operads

A. R. Gaynullina[*] **and S. N. Tronin**[**]

(Submitted by E. K. Lipachev)

N.I. Lobachevskii Institute of Mathematics and Mechanics, Kazan (Volga Region) Federal University, Kremlevskaya ul. 18, Kazan, Tatarstan, 420008 Russia

Received July 6, 2015

Abstract—In this paper we show the use of commutative operads in public-key cryptography. Commutative operads were introduced by S.N. Tronin in 2006. They are a special case of algebraic operads and a natural generalization of commutative algebraic theories. We consider some cryptographic protocols based on commutative operads. For the protocol of the creation a common secret key, we describe and investigate its implementation and cryptographic security in particular cases.

DOI: 10.1134/S1995080216030100

Keywords and phrases: *Operad, commutative operad, algebra over an operad, algebraic cryptography, cryptographic protocol, secret key, cipher, digital signature, authentication, security, tropical semiring.*

1. INTRODUCTION

In the modern mathematical cryptography we see algorithms which use various algebraic platforms. For example, widely used groups [9]. Our goal is to show that the cryptographic algorithms can be constructed by using the platform of commutative operads introduced in [13]. The definitions and the notations necessary for the further can also be found in [13].

2. COMMUTATIVE OPERADS

Definition 1. *A Σ-operad is a family $R = \{R(n)|n = 1, 2, \ldots\}$ of sets such that at each $R(n)$ the permutation group Σ_n, $n = 1, 2, \ldots$ acts on the right and for arbitrary ordered sequences of nonnegative integers $m, n_1, \ldots, n_m$, there are defined some composition operations*

$$R(m) \times R(n_1) \times \cdots \times R(n_m) \longrightarrow R(n_1 + \cdots + n_m),$$
$$(\omega, \omega_1, \ldots, \omega_m) \to \omega\omega_1 \ldots \omega_m.$$

The following properties hold:

(1) *Associativity*

$$\omega(\omega_1\omega_{1,1} \ldots \omega_{1,k_1}) \ldots (\omega_m\omega_{m,1} \ldots \omega_{m,k_m})$$
$$= (\omega\omega_1 \ldots \omega_m)(\omega_{1,1} \ldots \omega_{1,k_1} \ldots \omega_{m,1} \ldots \omega_{m,k_m})$$

(2) *There is a distinguished element $\varepsilon \in R(1)$ (the identity of the operads), such that the identity $\omega(\varepsilon \ldots \varepsilon) = \omega$ and $\varepsilon\omega = \omega$ are valid for all $\omega \in R(m)$.*

[*] E-mail: GaynullinaAlina@gmail.com

[**] E-mail: Serge.Tronin@kpfu.ru

Also, the properties which bind the composition operation and the actions of the group Σ_n must be performed. These properties can be found (*in a slightly different form and in another context*) in [13].

Consider two examples of operads.

Example 1.

Let X be an arbitrary set and let $Map(A, B)$ be the set of all mappings from A into B. Assume $E_X = \{E_X(n)|n \geq 1\}$, $E_X(n) = Map(X^n, X)$ and define the composition as follows.

Given $\omega_i : X^{n_i} \to X$, $1 \leq i \leq m$, and $\omega : X^m \to X$ and then $\omega\omega_1 \ldots \omega_m : X^{n_1+\cdots+n_m} \to X$.

Let $\bar{x} \in X^{n_1+\cdots+n_m}$. Since by definition, $X^{n_1+\cdots+n_m} = X^{n_1} \times \cdots \times X^{n_m}$, then $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_m)$, where $\bar{x}_i \in X^{n_i}$.

Then the composition in this operad is defined as follows:

$$\omega\omega_1 \ldots \omega_m(\bar{x}) = \omega(\omega_1(\bar{x}_1), \ldots, \omega_m(\bar{x}_m)).$$

The permutation group Σ_n acts as follows:

$$\omega\sigma(x_1, \ldots, x_m) = (x_{\sigma(1)}, \ldots, x_{\sigma(m)}),$$

where $\omega \in E_X(m)$, $x_1, \ldots, x_m \in X$, and $\sigma \in \Sigma_m$.

Example 2.

Let G be a semigroup with the identity element 1.

Assume $G = \{G(n)|n \geq 1\}$, where $G(n) = G^n$. An element $G(n)$ is a sequence (string) $\bar{x} = (x_1, \ldots, x_n)$ of elements $x_i \in G$. The action of an element $g \in G$ on the string $\bar{x}$ is defined as follows $g\bar{x} = (gx_1, \ldots, gx_n)$. The composition in this operad is defined as follows:

$$G(m) \times G(n_1) \times \ldots \times G(n_m) \to G(n_1 + \cdots + n_m)$$
$$(\bar{x}, \bar{y}_1, \ldots, \bar{y}_m) \mapsto \bar{x}\bar{y}_1 \ldots \bar{y}_m,$$

where $\bar{x} = (x_1, \ldots, x_m) \in G(m)$, $\quad \bar{y}_i = (y_{i,1}, \ldots, y_{i,n_i}) \in G(n_i)$ for $1 \leq i \leq m$, and $\bar{x}\bar{y}_1 \ldots \bar{y}_m = (x_1\bar{y}_1, \ldots, x_m\bar{y}_m)$.

The permutation group Σ_n acts on a set $G(n)$ as follows:

$$(x_1, \ldots, x_n)\sigma = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Definition 2. *Suppose that R is a Σ-operad. By an algebra over R we mean a set A that is endowed with some mappings of the form:*

$$R(n) \times A^n \longrightarrow A, \qquad (r, \bar{a}) \mapsto r\bar{a},$$

where $r \in R(n), \bar{a} = a_1 \ldots a_n$, $a_i \in A$. Moreover, the following conditions must be satisfied:

(1) $(rr_1 \ldots r_m)\bar{a}_1 \ldots \bar{a}_m = r(r_1\bar{a}_1) \ldots (r_m\bar{a}_m)$.

(2) $\varepsilon a = a$ for all $a \in A$, where $\varepsilon \in R(1)$ *is the identity of R.*

(3) *The identity $(rf)a_1 \ldots a_m = ra_{f(1)} \ldots a_{f(m)}$ holds for all $r \in R(m)$*, $a_1, \ldots, a_m \in A$, $f \in \Sigma_m$.

Definition 3. *Assume that Z is a Σ-operad. We call the operad Z commutative if the identity*

$$\lambda \overbrace{\omega \ldots \omega}^{n} = (\omega \overbrace{\lambda \ldots \lambda}^{m})\sigma_{n,m}$$

is hold for all $\lambda \in Z(n)$ and $\omega \in Z(m)$, *where $\sigma_{n,m} \in \Sigma_{nm}$ and*

$$\sigma_{n,m}(i + (j-1)n) = (j + (i-1)m),$$

for $1 \leq i \leq n, 1 \leq j \leq m$.

We denote by $\sum\limits_{i=1}^{n}{}^{(\lambda)} a_i$ the result of the composition of $\lambda \in Z(n)$ with $a_1, \ldots, a_n \in A$. Let Z be a commutative operad, then for all $\lambda \in Z(n)$ and $\omega \in Z(m)$ the equality

$$\sum_{i=1}^{n}{}^{(\lambda)} \sum_{j=1}^{m}{}^{(\omega)} a_{i,j} = \sum_{j=1}^{m}{}^{(\omega)} \sum_{i=1}^{n}{}^{(\lambda)} a_{i,j}$$

is hold in every Z-algebra.

In these notations, a homomorphism between the algebras over the commutative operads is a map h, such that

$$h\left(\sum_{i=1}^{n}{}^{(\lambda)}a_i\right) = \sum_{i=1}^{n}{}^{(\lambda)}h(a_i)$$

for all $\lambda \in Z(n)$ and $a_1, \ldots, a_n \in A$.

The value of a commutative operad is showed by the following theorem proved in [14].

Theorem 1. *The center of a multicategory is a commutative operad. The center of a commutative operad R coincides with R.*

Next, consider several examples of commutative operads.

Example 3.

Consider an operad Z for which $Z(0) = \emptyset$, $Z(1)$ is a singleton, and if $n \geq 2$, then $Z(n) = \emptyset$. We may assume that Z is a $FSet$-operad. The definition of a commutative operad for Z is fulfilled trivially. The category of algebras over this operad is actually the category of all sets.

Example 4.

Generalizing Example 3 to some extent consider an operad with a unique nonempty component $Z(1)$, which is a commutative monoid. This operad is also commutative, and the category of algebras over it is rationally equivalent to the category of left $Z(1)$-sets, i.e. the sets on which the left action of the monoid $Z(1)$ is defined.

Example 5.

Let G be a commutative monoid with the operation written multiplicatively. Consider an operad from Example 2. Easy verification shows that the so-constructed operad is commutative. If G is a commutative associative ring with unity then the variety of algebras over the operad is rationally equivalent to the category of left G-modules. In some cases, it will be convenient to denote the above operad like the monoid itself, i.e. by G.

Example 6.

Clearly, a suboperad of a commutative operad is also commutative. In many cases, some important examples are given by operads defined over a smaller verbal category than that over which the ambient commutative operad is defined. However, there are interesting cases when no restriction of the verbal category appears. For example, the operad of simplices Δ, studied in [12], is a suboperad in the $FSet$-operad $\mathbb{R}$, where $\mathbb{R}$ is the field of reals, and the corresponding operad is constructed as in Example 5. We proved in [12] that Δ admits a $FSet$-operad structure.

3. CRYPTOGRAPHIC PROTOCOLS

Let Z be a commutative operad, let A be an algebra over Z. Assume that these data are public (not secret).

Protocol 1. The creation of a common secret key

Alice's secret is a $\omega \in Z(n)$. Bob's secret is a $\lambda \in Z(m)$. Public elements are $a_{i,j} \in A$, $1 \leq i \leq n$, $1 \leq j \leq m$.

(1) Alice computes $\alpha_j = \sum\limits_{i=1}^{n}{}^{(\omega)}a_{i,j}$, $1 \leq j \leq m$.

(2) Bob computes $\beta_i = \sum\limits_{j=1}^{m}{}^{(\lambda)}\, a_{i,j}$, $1 \leq i \leq n$.

(3) Alice sends the elements α_j to Bob.

(4) Bob sends the elements β_i to Alice.

(5) Finally, Alice computes $\sum\limits_{i=1}^{n}{}^{(\omega)}\beta_i$, and Bob computes $\sum\limits_{j=1}^{m}{}^{(\lambda)}\alpha_j$.

By definition of a commutative operad, $\sum\limits_{i=1}^{n}{}^{(\omega)}\sum\limits_{j=1}^{m}{}^{(\lambda)}a_{i,j} = \sum\limits_{j=1}^{m}{}^{(\lambda)}\sum\limits_{i=1}^{n}{}^{(\omega)}a_{i,j}$. Thus, Alice and Bob receive a common secret key.

The security of the protocol is based on the complexity of the task of finding $\xi \in Z(k)$ using known $b_1, \dots, b_k \in A$ and $\sum\limits_{i=1}^{k}{}^{(\xi)}b_i \in A$.

Protocol 2. The key exchange

The public data are a commutative operad Z, a number n, and an element $\omega \in Z(n)$.

(1) Alice picks a random element $\alpha \in Z(m)$ and sends to Bob the element $\alpha\overbrace{\omega \dots \omega}^{m} = \alpha\omega^m$.

(2) Bob picks a random element $\beta \in Z(k)$ and sends to Alice the element $\beta\omega^k$.

(3) Alice computes $\alpha(\beta\omega^k)^m = (\alpha\beta^m)\omega^{mk}$.

(4) Bob computes

$$\beta(\alpha\omega^m)^k = (\beta\alpha^k)\omega^{mk} = ((\alpha\beta^m)\sigma_{m,k})(\omega^{mk}) = (\alpha\beta^m)(\omega^{mk})\sigma'.$$

The security of the protocol is based on the complexity of the task of finding α using known $\alpha\omega^m$ and ω.

Protocol 3. The encryption

A bit string m of length ℓ is encrypted. The public data are an element $g \in Z(n)$ and a hash function h that maps the elements of the operad Z to bit strings of length ℓ. The secret key is $x \in Z(m)$. The public key is $y = xg \dots g \in Z(mn)$.

The encryption begins with a random selection of the session key $k \in Z(d)$.

The first part of the ciphertext is the element $c_1 = kg \dots g \in Z(dn)$. The second part of the ciphertext is the bit string $c_2 = m \oplus h(ky \dots y)$.

The decryption: $m = c_2 \oplus h((xc_1 \dots c_1)\sigma)$, where $\sigma = \sigma_{d,m}{}^{*}\alpha$, $\alpha = \overbrace{(n, \dots, n)}^{dm}$ (see [14]). The security of this protocol is based on the complexity of the task of finding an element x of the operad according to the known g and $xg \dots g$.

Protocol 4. The authentication

Alice's secret is an element $x \in Z(n)$.

(1) Bob picks an element $g \in Z(m)$ and sends it to Alice.

(2) Alice computes $y = xg^n$ and sends it to Bob.

(3) Bob picks an element $k \in Z(\ell)$ and sends it to Alice.

(4) Finally, Alice computes $z = xk^n g^{n\ell}$, where $z \in R(n\ell m)$ and sends it to Bob.

Verification. Bob knows g, k, y and can compute:

$$k\underbrace{y \dots y}_{\ell} = k\underbrace{(xg^n) \dots (xg^n)}_{\ell} = (k\underbrace{x \dots x}_{\ell})g^{n\ell}$$
$$= ((xk \dots k)\sigma_{\ell,n})g^{n\ell} = ((xk \dots k)g^{n\ell})\sigma'.$$

Then Bob compares this element with the received z.

The security of the protocol is based on the complexity of the task of finding element of operad $x \in Z(n)$ using known $g \in Z(m)$ and $y = xg^n$.

4. IMPLEMENTATION AND CRYPTOGRAPHIC SECURITY

In this section, we describe and investigate the cryptographic security and the implementation of Protocol 1.

Let K be an associative commutative ring or semiring, Z be a commutative operad from Examples 2 and 5, where $G = K$, $Z(n) = K^n$.

Let k be a fixed positive integer. Consider an arbitrary suboperad R of operad Z, and determine the structure of R-algebra on $A = K^m$. We define mappings:

$$R(n) \times A^n \longrightarrow A$$

$$\xi a_1 \dots a_n = \sum_{i=1}^{n}{}^{(\xi)} a_i = x_1^k a_1 + \dots + x_n^k a_n,$$

where $\xi = (x_1, \dots, x_n) \in R(n)$, $a_i = (a_{1,i}, \dots, a_{m,i})$, $1 \le i \le n$.

Lemma 1. *A is an R-algebra.*

Proof. By definition. □

Lemma 2. *Let $b = (b_1, \dots, b_m) \in A$. The equality $\xi a_1 \dots a_n = b$ is equivalent to the system of equations in the ring or semiring K:*

$$\begin{cases} a_{1,1}x_1^k + \dots + a_{1,n}x_n^k = b_1 \\ \dots \quad \dots \quad \dots \quad \dots \\ a_{m,1}x_1^k + \dots + a_{m,n}x_n^k = b_m \end{cases} \tag{1}$$

Proof. By definition. □

Theorem 2. *The cryptographic security of Protocol 1 depends on the complexity of solving a large system of equations of the type (1) over the ring or semiring K. Moreover, it should be considered only solutions $(x_1, \dots, x_n) \in R(n)$.*

Proof. The proof follows from Lemmas 1 and 2. □

Next, consider some examples of rings and semirings.

Example 7.

Let K be a tropical semiring. Recall [11] that the tropical semiring is the semiring which has support $\mathbb{R} \cup \{+\infty\}$ and operations $a \oplus b = \min\{a, b\}$ and $a \otimes b = a + b$.

The tropical semiring are already used in cryptography (see [8]). There are several works, where it was introduced and investigated algorithms for solving systems of linear equations over such K (see [2, 3, 7]). A.P. Davydow in [2] recently proved that the Grigoriev's algorithm is a non-polynomial time algorithm, where

$$t = \Omega(n^{\frac{m}{6}} \log(\mathrm{poly}(n^{\frac{m}{6}}))).$$

Thus, the case of the tropical semiring looks promising.

Example 8.

Let $K = \mathbb{Z}$ and $A = \mathbb{Z}^m$. Then (1) is a system of the Diophantine equations. The complexity of the solutions for the case $k = 1$ (linear Diophantine equations) was studied in [4, 5, 10]. According to the following lemma, the Euclidean algorithm gives the polynomial solvability of one linear diophantine equation.

Lemma 3. *A linear diophantine equation with rational coefficients can be solved in polynomial time* [10].

It was shown by M.A. Frumkin in [4] and J. von zur Gathen and M. Sieveking in [5] that also systems of linear diophantine equations can be solved in polynomial time.

Example 9.

Let K be a finite field and $k = 1$. Yu.V. Nesterenko considered (see [6]) only the case of the square sparse matrixes. G.V. Bard considered in [1] the case of $GF(2)$. There is an polynomial-time algorithm in both cases. However, these cases does not cover all interesting for us systems of linear equations over finite fields.

Obviously, these three examples do not exhaust the plurality of rings and semirings that should be explored. Our research will be continued in subsequent publications.

Some results of this paper were announced in [15].

ACKNOWLEDGMENTS

This work was partially funded by the subsidy allocated to Kazan Federal University for the state assignment in the sphere of scientific activities (the registration number is 114 090 970 010).

REFERENCES

1. G. V. Bard, *Algebraic Cryptanalysis* (Springer, New York, 2009).
2. A. P. Davydov, J. of Math. Sc. **192** (3), 295 (2013).
3. A. P. Davydow, arXiv:1309.5206 [cs.CC] (2013).
4. M. A. Frumkin, Studies in Discrete Optimization, 97 (1976) [In Russian].
5. J. von zur Gathen and M. Sieveking, Lecture Notes in Comp. Sc. **43**, 49 (1976).
6. E. A. Grechnikov, S. V. Mikhailov, Yu. V. Nesterenko, and I. A. Popovyan, *Hard Computational Problems in Number Theory* (Moscow University Press, Moscow, 2012) [In Russian].
7. D. Grigoriev, Computational Complexity **22** (1), 71 (2013).
8. D. Grigoriev and V. Shpilrain, Comm. in Alg. **42** (6), 2624 (2014).
9. A. Myasnikov, V. Shpilrain, and A. Ushakov, *Group-based Cryptography* (Birkhauser Verlag, Basel, Berlin, New York, 2008).
10. A. Schrijver, *Theory of Linear and Integer Programming* (Wiley, Chichester, 1998).
11. D. Speyer and B. Sturmfels, Math. Magazine **82** (3), 163 (2009).
12. S. N. Tronin, Russian Math. **46** (3), 38 (2002).
13. S. N. Tronin, Sib. Math. J. **47** (3), 555 (2006).
14. S. N. Tronin, Russian Math. **55** (11), 49 (2011).
15. S. N. Tronin and A. R. Gaynullina, *Proc. Internat. Conf. "Algebra and Mathematical Logic: Theory and Applications"* (Kazan University Press, Kazan, 2014), p. 146–147.