

Contents

1. Preliminaries	9
1.1 Opening remarks	9
1.2 Introduction	13
2. On families of stable subsemigroups and subgroups of affine Cremona Semigroups with exponential growth of periods and Non-commutative Cryptography	21
2.1 On some properties of affine Cremona groups and semigroups	22
2.2 On semigroups defined in terms of Singer graphs and their elements of large period	27
2.3 On linguistic graphs and transformations of affine spaces over commutative rings	30
2.4 On configurations of linguistic graphs, projective geometry and stable semigroups of affine Cremona semigroup.	34
2.5 Semigroups of infinite symbolic strings and linguistic compression maps in the case of single linguistic graph	40
2.6 On semigroups and groups related to Double Schubert graphs and Graphs of the largest Schubert cells	44
2.7 On linguistic graphs of extremal graph theory and expanded plat-forms of Noncommutative Cryptography	48
2.8 On the semigroups with quotients constructed via subconfigurations of $T(n - 1, K)$	56
2.9 Protocols in terms of stable subsemigroups of $CS_n(K)$	66
2.9.1 Twisted Diffie - Hellman protocol.	66
2.9.2 Inverse twisted Diffie-Hellman protocol.	69
2.9.3 Tame families and concept of stability.	70
2.9.4 Key exchange Tahoma protocol.	77

2.9.5	Inverse tahoma word protocol.	79
2.9.6	Inverse tahoma cryptosystem.	81
2.9.7	Modified inverse tahoma protocol	82
2.9.8	Conversion to cryptosystem.	82
2.9.9	On the safe exchange of symbolic transformations.	83
2.9.10	On two versions of the semigroup enveloped symbolic Diffie-Hellman key exchange protocol for stable groups.	85
2.9.11	Inverse semigroup enveloping Diffie Hellman protocol for stable families of transformations.	89
2.9.12	Inverse semigroup enveloping cryptosystems.	90
2.9.13	Example of stable tahoma word protocol.	93
2.9.14	Other protocols.	106
2.9.15	Remarks on complexity.	109

3. On Eulerian semigroups of multivariate transformations and new solutions of Postquantum Cryptography. 111

3.1	On Postquantum Cryptography with maps of minimal density.	111
3.2	On Eulerian semigroup and hard computational problem.	113
3.3	Protocols and cryptosystems in terms of semigroup ${}^nES(K)$	115
3.3.1	Tahoma protocol.	115
3.3.2	Inverse Tahoma protocol.	116
3.3.3	Group enveloped Diffie-Hellman key exchange protocol.	116
3.3.4	The inverse version of group enveloped Diffie-Hellman key exchange protocol.	117
3.3.5	Inverse two wheeled Diffie-Hellman protocol.	117
3.3.6	Two wheeled Diffie-Hellman protocol.	118
3.3.7	Twisted Diffie-Hellman protocol.	118
3.3.8	Inverse twisted Diffie-Hellman protocol.	118
3.4	On some alternatives to public key cryptography with Eulerian maps.	119
3.4.1	Example of bipartite cryptosystem.	119
3.5	On two versions of the semigroup enveloped symbolic Diffie-Hellman key exchange protocol for families of Eulerian transformations.	124
3.5.1	Basic constructions.	127
3.5.2	Homomorphisms of linguistic compression for semigroups of monomial strings.	128
3.5.3	Examples of linguistic graphs over K^* , related semigroups, their homomorphisms and inverse protocol.	129

3.6	Linguistic configurations over multiplicative groups K^* of commutative ring K and their applications.	130
3.6.1	Basic definitions.	130
3.7	Multiplicative projective geometry, its subconfigurations and corresponding subsemigroup of Eulerian semigroup.	132
4.	On generalisations on the case of Lie geometries, corresponding stable multivariate semigroups and Eulerian transformations	139
4.1	Coxeter groups and systems, their geometries and corresponding linguistic configurations.	139
4.1.1	Coxeter linguistic configurations.	139
4.1.2	On universal Cartan linguistic configurations of type X_n	141
4.1.3	Connections with BN -pairs.	143
4.2	Other constructions of semigroup related to linguistic graphs over commutative rings and commutative groups.	144
4.2.1	On the expansions of defined semigroups corresponding to linguistic graphs.	144
4.2.2	Schubert cells in $T(n-1, K)$ and $T(n-1, K^*)$ and expanded semigroups.	146
4.2.3	Description of direct tahoma protocol.	151
4.2.4	Conversion of direct tahoma protocol to a cryptosystem.	153
4.3	On Eulerian groups and semigroups and the usage of stable and toric platforms in tandem.	154
4.3.1	Basic constructions.	154
4.3.2	Generalizations.	155
4.3.3	On general linguistic graphs over commutative groups and generating procedure of mutually inverse transformations of $(K^*)^n$	157
4.4	Implementation of algorithm 2. 1. 2 with subsemigroups $ED(n, K^*)$ and $EA(n, K^*)$ and corresponding cryptosystems.	160
4.4.1	Implementation of protocol 2.3.2.	160
4.4.2	Conversion to a cryptosystem.	160
4.4.3	Asymmetric schemes of multivariate cryptography on safe Eulerian mode.	161
4.5	Groups $GD(n, K)$ and $GA(m, K)$ and corresponding cryptosystems.	162
4.5.1	Implementation of algorithm 2.1.1 with groups $GD(n, K)$ and $GA(m, K)$	162

4.5.2	Conversion to a cryptosystem.	162
4.5.3	Transformation to Eulerian mode.	163
4.5.4	On schemes of quadratic multivariate cryptography on safe Eulerian mode.	163
4.5.5	On the usage of toric and stable platforms in tandem.	163
4.5.6	Conclusion.	165
4.6	Description of the usage of incidence structures $T(n-1, K)$ and $T(n-1, K^*)$ in tandem.	167
4.7	New stream algorithms generating sensitive digests of digital docu- ments.	169
4.7.1	Introduction.	169
4.7.2	On the verification of electronic documents.	170
4.7.3	Requirements to digests.	171
4.7.4	Mathematical background of proposed hash functions.	172
4.7.5	On the option to speed up the algorithm.	173
4.7.6	On the implementation of digest generation algorithms.	174
4.7.7	Conclusion.	175
4.8	Conclusive remarks on the last results and announcements of the future events.	176
4.9	Terminology and notations of algebraic geometry.	179