CONTEMPORARY MATHEMATICS

418

Algebraic Methods in Cryptography

AMS/DMV Joint International Meeting
June 16–19, 2005
Mainz, Germany

International Workshop on Algebraic Methods in Cryptography
November 17–18, 2005
Bochum, Germany

Lothar Gerritzen
Dorian Goldfeld
Martin Kreuzer
Gerhard Rosenberger
Vladimir Shpilrain
Editors

American Mathematical Society

418

Algebraic Methods in Cryptography

AMS/DMV Joint International Meeting
June 16–19, 2005
Mainz, Germany

International Workshop on Algebraic Methods in Cryptography
November 17–18, 2005
Bochum, Germany

Lothar Gerritzen
Dorian Goldfeld
Martin Kreuzer
Gerhard Rosenberger
Vladimir Shpilrain
Editors

American Mathematical Society
Providence, Rhode Island

2000 *Mathematics Subject Classification.* Primary 94A60, 20Fxx, 68P25, 68W20, 68W30, 11T71, 57M05.

Library of Congress Cataloging-in-Publication Data

Special Session on Algebraic Cryptography at the Joint International Meeting of the AMS and the Deutsche Mathematiker-Vereinigung (2005 : Mainz, Germany)

Algebraic methods in cryptography : Special Session on Algebraic Cryptography at the Joint International Meeting of the AMS and the Deutsche Mathematiker-Vereinigung, June 16–19, 2005, Mainz, Germany : International Workshop on Algebraic Methods in Cryptography, November 17–18, 2005, Bochum, Germany / editors, Lothar Gerritzen . . . [et al.].

p. cm. — (Contemporary mathematics, ISSN 0271-4132 ; v. 418)

ISBN-13: 978-0-8218-4037-5 (alk. paper)

ISBN-10: 0-8218-4037-1 (alk. paper)

1. Algebra. 2. Cryptography. I. Gerritzen, Lothar, 1941– II. American Mathematical Society. III. Deutsche Mathematiker-Vereinigung. IV. International Workshop on Algebraic Methods in Cryptography (2005 : Bochum, Germany) V. Title.

QA150.S64 2005

652′.8—dc22 2006043028

Preface

This volume consists of contributions by speakers at the Special Session on Algebraic Cryptography at the Joint International Meeting of the AMS with the Deutsche Mathematiker-Vereinigung held in Mainz, Germany, on June 16–19, 2005, and at the International Workshop on Algebraic Methods in Cryptography held in Bochum, Germany, on November 17–18, 2005.

The readers will find here a variety of contributions, mostly related to public-key cryptography, including design of new cryptographic primitives as well as cryptanalysis of previously suggested schemes. Most papers are original research papers in the area that can be loosely defined as "Non-commutative cryptography"; this means that groups (or other algebraic structures) which are used as platforms are non-commutative.

We are grateful to the American Mathematical Society for assisting us in publication of this volume. In particular, we thank Christine M. Thivierge for her patient work in putting this volume together.

Lothar Gerritzen
Dorian Goldfeld
Martin Kreuzer
Gerhard Rosenberger
Vladimir Shpilrain

Titles in This Series

418 **Lothar Gerritzen, Dorian Goldfeld, Martin Kreuzer, Gerhard Rosenberger, and Vladimir Shpilrain, Editors,** Algebraic methods in cryptography, 2006

417 **Vadim B. Kuznetsov and Siddhartha Sahi, Editors,** Jack, Hall-Littlewood and Macdonald polynomials, 2006

416 **Toshitake Kohno and Masanori Morishita, Editors,** Primes and Knots, 2006

415 **Gregory Berkolaiko, Robert Carlson, Stephen A. Fulling, and Peter Kuchment, Editors,** Quantum Graphs and Their Applications, 2006

414 **Deguang Han, Palle E. T. Jorgensen, and David Royal Larson, Editors,** Operator theory, operator algebras, and applications, 2006

413 **Georgia M. Benkart, Jens C. Jantzen, Zongzhu Lin, Daniel K. Nakano, and Brian J. Parshall, Editors,** Representations of algebraic groups, quantum groups and Lie algebras, 2006

412 **Nikolai Chernov, Yulia Karpeshina, Ian W. Knowles, Roger T. Lewis, and Rudi Weikard, Editors,** Recent advances in differential equations and mathematical physics, 2006

411 **J. Marshall Ash and Roger L. Jones, Editors,** Harmonic analysis: Calderón-Zygmund and beyond, 2006

410 **Abba Gumel, Carlos Castillo-Chavez, Ronald E. Mickens, and Dominic P. Clemence, Editors,** Mathematical studies on human disease dynamics: Emerging paradigms and challenges, 2006

409 **Juan Luis Vázquez, Xavier Cabré, and José Antonio Carrillo, Editors,** Recent trends in partial differential equations, 2006

408 **Habib Ammari and Hyeonbae Kang, Editors,** Inverse problems, multi-scale analysis and effective medium theory, 2006

407 **Alejandro Ádem, Jesús González, and Guillermo Pastor, Editors,** Recent developments in algebraic topology, 2006

406 **José A. de la Peña and Raymundo Bautista, Editors,** Trends in representation theory of algebras and related topics, 2006

405 **Andrew Markoe and Eric Todd Quinto, Editors,** Integral geometry and tomography, 2006

404 **Alexander Borichev, Håkan Hedenmalm, and Kehe Zhu, Editors,** Bergman spaces and related topics in complex analysis, 2006

403 **Tyler J. Jarvis, Takashi Kimura, and Arkady Vaintrob, Editors,** Gromov-Witten theory of spin curves and orbifolds, 2006

402 **Zvi Arad, Mariagrazia Bianchi, Wolfgang Herfort, Patrizia Longobardi, Mercede Maj, and Carlo Scoppola, Editors,** Ischia group theory 2004, 2006

401 **Katrin Becker, Melanie Becker, Aaron Bertram, Paul S. Green, and Benjamin McKay, Editors,** Snowbird lectures on string geometry, 2006

400 **Shiferaw Berhanu, Hua Chen, Jorge Hounie, Xiaojun Huang, Sheng-Li Tan, and Stephen S.-T. Yau, Editors,** Recent progress on some problems in several complex variables and partial differential equations, 2006

399 **Dominique Arlettaz and Kathryn Hess, Editors,** An Alpine anthology of homotopy theory, 2006

398 **Jay Jorgenson and Lynne Walling, Editors,** The ubiquitous heat kernel, 2006

397 **José M. Muñoz Porras, Sorin Popescu, and Rubí E. Rodríguez, Editors,** The geometry of Riemann surfaces and Abelian varieties, 2006

396 **Robert L. Devaney and Linda Keen, Editors,** Complex dynamics: Twenty-five years after the appearance of the Mandelbrot set, 2006

395 **Gary R. Jensen and Steven G. Krantz, Editors,** 150 Years of Mathematics at Washington University in St. Louis, 2006

394 **Rostislav Grigorchuk, Michael Mihalik, Mark Sapir, and Zoran Šunik, Editors,** Topological and asymptotic aspects of group theory, 2006

393 **Alec L. Matheson, Michael I. Stessin, and Richard M. Timoney, Editors,** Recent advances in operator-related function theory, 2006

392 **Stephen Berman, Brian Parshall, Leonard Scott, and Weiqiang Wang, Editors,** Infinite-dimensional aspects of representation theory and applications, 2005

391 **Jürgen Fuchs, Jouko Mickelsson, Grigori Rozenblioum, Alexander Stolin, and Anders Westerberg, Editors,** Noncommutative geometry and representation theory in mathematical physics, 2005

390 **Sudhir Ghorpade, Hema Srinivasan, and Jugal Verma, Editors,** Commutative algebra and algebraic geometry, 2005

389 **James Eells, Etienne Ghys, Mikhail Lyubich, Jacob Palis, and José Seade, Editors,** Geometry and dynamics, 2005

388 **Ravi Vakil, Editor,** Snowbird lectures in algebraic geometry, 2005

387 **Michael Entov, Yehuda Pinchover, and Michah Sageev, Editors,** Geometry, spectral theory, groups, and dynamics, 2005

386 **Yasuyuki Kachi, S. B. Mulay, and Pavlos Tzermias, Editors,** Recent progress in arithmetic and algebraic geometry, 2005

385 **Sergiy Kolyada, Yuri Manin, and Thomas Ward, Editors,** Algebraic and topological dynamics, 2005

384 **B. Diarra, A. Escassut, A. K. Katsaras, and L. Narici, Editors,** Ultrametric functional analysis, 2005

383 **Z.-C. Shi, Z. Chen, T. Tang, and D. Yu, Editors,** Recent advances in adaptive computation, 2005

382 **Mark Agranovsky, Lavi Karp, and David Shoikhet, Editors,** Complex analysis and dynamical systems II, 2005

381 **David Evans, Jeffrey J. Holt, Chris Jones, Karen Klintworth, Brian Parshall, Olivier Pfister, and Harold N. Ward, Editors,** Coding theory and quantum computing, 2005

380 **Andreas Blass and Yi Zhang, Editors,** Logic and its applications, 2005

379 **Dominic P. Clemence and Guoqing Tang, Editors,** Mathematical studies in nonlinear wave propagation, 2005

378 **Alexandre V. Borovik, Editor,** Groups, languages, algorithms, 2005

377 **G. L. Litvinov and V. P. Maslov, Editors,** Idempotent mathematics and mathematical physics, 2005

376 **José A. de la Peña, Ernesto Vallejo, and Natig Atakishiyev, Editors,** Algebraic structures and their representations, 2005

375 **Joseph Lipman, Suresh Nayak, and Pramathanath Sastry,** Variance and duality for cousin complexes on formal schemes, 2005

374 **Alexander Barvinok, Matthias Beck, Christian Haase, Bruce Reznick, and Volkmar Welker, Editors,** Integer points in polyhedra—geometry, number theory, algebra, optimization, 2005

373 **O. Costin, M. D. Kruskal, and A. Macintyre, Editors,** Analyzable functions and applications, 2005

372 **José Burillo, Sean Cleary, Murray Elder, Jennifer Taback, and Enric Ventura, Editors,** Geometric methods in group theory, 2005

For a complete list of titles in this series, visit the AMS Bookstore at **www.ams.org/bookstore/**.

Contents

Contemporary Mathematics
Volume 418, 2006

KEY AGREEMENT, THE ALGEBRAIC ERASER^{TM}, AND LIGHTWEIGHT CRYPTOGRAPHY

Iris Anshel, Michael Anshel, Dorian Goldfeld, Stephane Lemieux

§1. Introduction:

Our purpose is to present a new key agreement protocol for public-key cryptography suitable for implementation on low-cost platforms which constrain the use of computational resources. In the process we introduce the concept of an Algebraic Eraser^{TM}, AE, and make a case that AE is a suitable primitive for use within lightweight cryptography. Our underlying motivation is the need to secure networks which deploy Radio Frequency Identification (RFID) tags used for identification, authentication, tracing and point-of-sale applications. The reader should consult [GJP] and [OSK] for further discussion.

The idea behind AE is to deny the cryptanalyst certain algebraic information inherent in many contemporary algebraic key agreement protocols employing group-theoretic transformations such as discrete exponention certain finite abelian groups or conjugation on certain infinite groups including braid groups (see [KM]). AE employs certain groups, homomorphisms, and actions of groups on monoids which to date force the cryptanalyst to primarily employ exhaustive search to determine the key. After careful formulation of the basic structure of AE we specify a general key agreement protocol based on the AE and go on to give some explicit examples including possible attacks and choice of secure parameters.

§2. The Algebraic Eraser^{TM} and its Associated Protocol:

The concept of the Algebraic Eraser emerges naturally when considering the following structures in tandem. Let M, N denote monoids and let S denote a group which acts on M on the left, and does not act on N. Given elements $s \in S$ and $m \in M$, we denote the result of s acting on m by ${}^{s}m$. The semidirect product of M and S, $M \rtimes S$ is defined to be the monoid whose underlying set is $M \times S$ and whose internal binary operation is given by

$$(m_1, s_1) \circ (m_2, s_2) \;=\; (m_1 {}^{s_1}m_2,\; s_1 s_2).$$

The authors would like to thank SecureRF for its support of this research. The authors would also like to thank Alan Silvester for doing a lot of the C++ coding.

The direct product of N and S is denoted by $N \times S$.

The *algebraic eraser* $\mathbf{E}$ is the binary operation specified within the 6-tuple,

$$(M \rtimes S, N, \Pi, \mathbf{E}, A, B),$$

termed the $\mathbf{E}$–*structure*, where $M \rtimes S$ and N are as above, Π is (an easily computable) monoid homomorphism

$$\Pi : M \to N,$$

$\mathbf{E}$ is the function

$$\mathbf{E} : (N \times S) \times (M \rtimes S) \to N \times S$$

given by

$$\mathbf{E}\big((n, s), (m_1, s_1)\big) = \big(n\ \Pi({}^{s}m_1), {}^{s}s_1\big),$$

and A, B are submonoids of $M \rtimes S$ such that for all $(a, s_a) \in A, (b, s_b) \in B$

$$\mathbf{E}\big((\Pi(a), s_a), (b, s_b)\big) = \mathbf{E}\big((\Pi(b), s_b), (a, s_a)\big). \tag{1}$$

The submonoids A and B, which satisfy (1) above, are termed $\mathbf{E}$–*Commuting*. For simplicity we will use the notation $\star$ as follows:

$$\mathbf{E}\big((n, s), (m_1, s_1)\big) \ = \ (n, s) \star (m_1, s_1).$$

The operation $\star$ satisfies the property that given $(n, s) \in N \times S$ and $(m_1, s_1), (m_2, s_2) \in M \rtimes S$ then

$$\Big((n, s) \star (m_1, s_1)\Big) \star (m_2, s_2) \ = \ (n, s) \star \Big((m_1, s_1) \circ (m_2, s_2)\Big). \tag{2}$$

The identity (2) is easily verified and allows one to compute $\star$ iteratively provided an element $(m, s) \in M \rtimes S$ is expressed as a product of generators.

The term *algebraic eraser* is a fitting description of the function $\mathbf{E}$ in that given an elements of $N \times S$,

$$(n, s), \qquad \mathbf{E}\big((n, s), (m_1, s_1)\big)$$

the element (m_1, s_1) cannot generally be recovered since the action of the element s on m_1 is not visible once the function Π has been applied to ${}^{s}m_1$ i.e., the action of s on m_1 has been effectively erased.

With the algebraic eraser $\mathbf{E}$ and its associated $\mathbf{E}$–*structure* specified we are in a position to introduce an associated key agreement protocol, $\mathbf{E}$–KAP. Referring to the protocol users as Alice and Bob, each user is assigned a submonoid of N, N_A and N_B respectively so that N_A and N_B commute. Furthermore Alice and Bob are assigned the $\mathbf{E}$–commuting submonoids A and B, respectively, which are determined by the fixed $\mathbf{E}$–structure. With these assignments in place Alice and Bob choose their respective private keys which take the form

$$A_{\text{Private}} \ = \ \text{Alice's Private Key} \ = \ \Big(n_a, \langle (a_1, s_{a_1}), (a_2, s_{a_2}), \ldots, (a_k, s_{a_k})\rangle\Big)$$

and

$$B_{\text{Private}} \ = \ \text{Bob's Private Key} \ = \ \Big(n_b, \langle (b_1, s_{b_1}), (b_1, s_{b_2}), \ldots, (b_\ell, s_{b_\ell})\rangle\Big)$$

where $n_a \in N_A$, $n_b \in N_B$,

$$(a_1, s_{a_1}), (a_2, s_{a_2}), \ldots, (a_k, s_{a_k}) \in A,$$

and

$$(b_1, s_{b_1}), (b_2, s_{b_2}), \ldots, (b_\ell, s_{b_\ell}) \in B.$$

Having made these choices, Alice and Bob can then announce their respective public keys:

$$A_{\text{Public}} = \text{Alice's Public Key} = (\cdots((n_a, \text{id})\star(a_1, s_{a_1}))\star(a_2, s_{a_2}))\star\cdots)\star(a_k, s_{a_k}) \in N\times S,$$

$$B_{\text{Public}} = \text{Bob's Public Key} = (\cdots((n_b, \text{id})\star(b_1, s_{b_1}))\star(b_2, s_{b_2}))\star\cdots)\star(b_\ell, s_{b_\ell}) \in N\times S,$$

where id denoted the identity element in S. With this done Alice and Bob are now each in a position to compute the shared secret:

(3)

$$(\cdots((n_a, \text{id}) \cdot B_{\text{Public}}\star(a_1, s_{a_1})) \star (a_2, s_{a_2})) \star \cdots) \star (a_k, s_{a_k}) = (\cdots((n_b, \text{id}) \cdot A_{\text{Public}} \star (b_1, s_{b_1})) \star (b_2, s_{b_2})) \star \cdots) \star (b_\ell, s_{b_\ell}),$$

where $\cdot$ denoted multiplication in $N \times S$. The identity (3) holds because the submonoids A, B where chosen to **E**–commute, and the submonoids N_A, N_B themselves commute.

§3. Algebraic Constructions

The **E**–structure $(M \rtimes S, N, \Pi, \mathbf{E}, A, B)$ and its associate key agreement protocol lend themselves naturally to various natural algebraic/categorical constructions. Furthermore when we focus on the case of M being a group and S being a (sub)group of automorphisms of the group, a generalized commutator emerges from the **E**–commuting condition.

The direct product of two **E**–structures, $\mathbf{E}_1$ and $\mathbf{E}_2$ yield a third **E**–structure:

$$(M_1 \rtimes S_1, N_1, \Pi_1, \mathbf{E}_1, A_1, B_1) \times (M_2 \rtimes S_2, N_2, \Pi_2, \mathbf{E}_2, A_2, B_2) = \Big((M_1 \times M_2) \rtimes (S_1 \times S_2), N_1 \times N_2, \Pi_1 \times \Pi_2, \mathbf{E}_1 \times \mathbf{E}_2, A_1 \times A_2, B_1 \times B_2\Big).$$

Given a submonoid $H \leq M$ which is S invariant, there is a natural sub–**E**–structure of $(M \rtimes S, N, \Pi, \mathbf{E}, A, B)$ to consider:

$$(H \rtimes S, N, \Pi \downarrow_H, \mathbf{E} \downarrow_{(N\times S)\times(H\rtimes S)}, A \cap H, B \cap H).$$

Finally the concept of a image of an **E**–structure can be approached by starting with a homomorphism $\Psi : N \to N_0$ and considering the **E**–structure

$$(M \rtimes S, N_0, \Psi \circ \Pi, \mathbf{E}_0, A, B),$$

where $\Psi \circ \Pi$, denotes the composite of Ψ and Π.

In the case M is actually a group and the homomorphism Π is surjective, then another possible image can be defined. In this case we know that $N \cong M/K$ where $K \trianglelefteq M$. If $L \trianglelefteq M$ is a subgroup which is invariant under S then S acts on the group M/L and we can form $M/L \rtimes S$. This allows us to define an image of

$$(M \rtimes S, M/K, (M \to M/K), \mathbf{E}, A, B),$$

to be

$$\Big((M/L \rtimes S), M/LK, (M/L \to M/LK), \mathbf{E}_L, (AL/L) \rtimes S, (BL/L) \rtimes S\Big)$$

where unspecified homomorphisms are simply the natural homomorphisms.

When we again restrict ourselves to the case of a group, G and we assume the group S is actually a group of automorphisms of G, $S \leq \mathrm{Aut}(G)$ then the hypothesis of **E**–commuting takes the following form. Elements in the subgroups A, B can be written as

$$(a, \alpha), \quad (b, \beta)$$

where $a, b \in G$ and $\alpha, \beta \in \mathrm{Aut}(G)$. The function Π can be assumed to take the form $G \to G/K$, and the identity (1) becomes

$$\big(a\ \alpha(b)\big)K, \alpha \circ \beta) \ = \ \big((b\ \beta(a)\big)K, \beta \circ \alpha).$$

The identity emerging from the first component leads naturally to the following generalization of the classical commutator. Given elements $x, y \in G$, and $(a, \alpha), (b, \beta) \in \mathrm{Aut}(G)$ define

$$C(\alpha, \beta, x, y) \ = \ x\ y\beta(x^{-1})\alpha(y^{-1}).$$

Clearly when $\alpha, \beta = \mathrm{id}$ we are reduced to the classical definition. Some analogues of the various classical commutator identities generalize as follows (and are left to the reader to verify). Let

$$\Omega(\alpha, \beta, x, y) \ = \ \alpha(x)\ y\ \beta(x)^{-1},$$

then we have

Proposition 1. *With the notation as above, the following identities hold:*

- $C(\alpha, \beta, x, y)^{-1} \ = \ C(\beta^{-1}, \alpha^{-1}, \alpha(y), \beta(x))$
- $C(\alpha, \beta, xy, z) \ = \ \Omega\big(\mathrm{id}, \beta, x, C(\alpha, \beta, y, z)\big)\ C(\mathrm{id}, \mathrm{id}, \beta(x), \alpha(z))$
- $C(\alpha, \beta, x, yz) \ = \ C(\mathrm{id}, \mathrm{id}, x, y)\ \Omega\big(\mathrm{id}, \alpha, y, C(\alpha, \beta, x, z)\big)$
- (identity of Hall–Witt type, see [MKS])

$$\begin{aligned} y^{-1}C\big(\mathrm{id}, \alpha, &C(\alpha, \alpha, y, \alpha(x^{-1})), \alpha(z^{-1})\big)y \\ &\cdot z^{-1}C\big(\mathrm{id}, \alpha, C(\alpha, \alpha, z, \alpha(y^{-1})), \alpha^2(x^{-1})\big)z \\ &\cdot \alpha(x^{-1})C\big(\mathrm{id}, \alpha, C(\alpha, \alpha^2, \alpha(x), z^{-1}), \alpha(y^{-1})\big)\alpha(x) \end{aligned}$$

Before delving into the examples of our protocol we present a brief aside regarding a group theoretic authentication method. Recall the protocol introduced in [AAG1]: users Alice and Bob each choose private elements a, b in assigned subgroups A, B of a group G and in the end agree on the commutator $[a, b]$ known only to the users. In the course of the protocol Alice actually obtains the conjugate $b^{-1}ab$ and hence is in a position to compute the element

$$b^{-1}ab \cdot a \cdot [a, b] \ = \ b^{-1}a^2b \ = \ (b^{-1}ab)^2.$$

Assuming that extraction of roots, in particular square roots, is known to be a difficult problem, Alice can forward the element $b^{-1}a^2b$ to Bob who can then conjugate by the inverse of his private key b^{-1} to obtain the element a^2. Thus Alice has

effectively transmitted the square of her private key a^2 to Bob over an open channel. With this done, any choice of a hash function $\mathcal{H}$ (i.e., a one–way collision–free function) generates an authentication protocol in the spirit of [D]:

(i) Alice chooses an element $r \in G$ and sends Bob the the element $c = \mathcal{H}(ra^2r^{-1})$,

(ii) Bob chooses a random bit d and sends d to Alice,

(iii) If $d = 0$ Alice sends the element r and Bob verifies that $c = \mathcal{H}(ra^2r^{-1})$,

(iv) If $d = 1$ Alice sends the conjugate $s = ra^2r^{-1}$ and Bob verifies that $c = \mathcal{H}(s^2)$.

§4. Examples of Key Agreement based on the Algebraic Eraser^{TM}:

Fix an integer $n \geq 7$ and a prime $p > n$. As an example of an algebraic eraser $\mathbf{E}$ whose associated key agreement protocol merits attention we begin by considering a subgroup

$$M \leq \mathrm{GL}(n, \mathbb{F}_p(t)),$$

where $t = (t_1, \ldots, t_n)$. Also, let $S = S_n$ be the symmetric group on n symbols. The group S acts on $\mathrm{GL}(n, \mathbb{F}_p(t))$ by permuting the variables $\{t_1, \ldots, t_n\}$, and we shall assume that the action of S maps M to itself. Furthermore we assume that the semidirect product $M \rtimes S$ is finitely generated by some set of elements,

$$\big\{(x_1(t), s_1), \ldots, (x_\lambda(t), s_\lambda)\big\}. \tag{4}$$

In this example, the monoid N is chosen to be

$$N = \mathrm{GL}(n, \mathbb{F}_p).$$

In order to define the homomorphism Π, we fix n elements in $\mathbb{F}_p$,

$$\tau_1, \tau_2, \ldots, \tau_n \in \mathbb{F}_p,$$

and then evaluate

$$\Pi : M \to N$$

by setting

$$t_1 = \tau_1, \quad t_2 = \tau_2, \quad \ldots, \quad t_n = \tau_n.$$

A crucial assumption needs to be made at this point.

Assumption τ: *Let $\tau = (\tau_1, \tau_2, \ldots, \tau_n)$. We assume that $x_i(\tau)$, $x_i(\tau)^{-1}$ are well defined for all $i = 1, 2, \ldots, n$.*

There are, of course, many possible choices for the commuting submonoids N_A, N_B, which need to be chosen. One elementary choice for N_A and N_B is to first fix a matrix $m_0 \in GL(n, \mathbb{F}_p)$ of order $p^n - 1$. Then let $N_A = N_B$ be the submonoid of all matrices of the form

$$\ell_1 m_0^{k_1} + \ell_2 m_0^{k_2} + \cdots + \ell_r m_0^{k_r}, \tag{5}$$

where $\ell_1, \ell_2, \ldots, \ell_r \in \mathbb{F}_p$ and $r, k_1, k_2, \ldots, k_r \in \mathbb{Z}^+$. Each users private n_a and n_b are then elements of the above form (5). As to the subgroups $A, B \leq M \rtimes S$,

which must **E**–commute for the protocol to succeed, one possibility is to proceed as follows. Fix an element $z \in M \rtimes S$ and choose two subsets of generators of $M \rtimes S$,

$$\Big\{\big(x_{a_1}(t), s_{a_1}\big), \ldots, \big(x_{a_\mu}(t), s_{a_\mu}\big)\Big\}, \qquad \Big\{\big(x_{b_1}(t), s_{b_1}\big), \ldots, \big(x_{b_\nu}(t), s_{b_\nu}\big)\Big\},$$

so that

$$x_{a_i}(t) \cdot x_{b_j}(t) = x_{b_j}(t) \cdot x_{a_i}(t), \qquad i = 1, \ldots, \mu, \quad j = 1, \ldots, \nu, \tag{6}$$

$$s_{a_i} t_{b_j} = t_{b_j} s_{a_i}, \qquad i = 1, \ldots, \mu, \quad j = 1, \ldots, \nu, \tag{7}$$

and

$$^{s_{a_i}} x_{b_j}(t) = x_{b_j}(t), \quad ^{s_{b_j}} x_{a_i}(t) = x_{a_i}(t), \quad i = 1, \ldots, \mu, \quad j = 1, \ldots, \nu. \tag{8}$$

Alice and Bob are then assigned the subgroups

$$\begin{aligned} &z \cdot \Big\langle \big(x_{a_1}(t), s_{a_1}\big), \ldots, \big(x_{a_\mu}(t), s_{a_\mu}\big) \Big\rangle \cdot z^{-1}, \\ &z \cdot \Big\langle \big(x_{b_1}(t), s_{b_1}\big), \ldots, \big(x_{b_\nu}(t), s_{b_\nu}\big) \Big\rangle \cdot z^{-1}, \end{aligned} \tag{9}$$

respectively, which will automatically **E**–commute with each other.

Hidden Elements Assumption: *We assume that the element $z \in M \rtimes S$ and the elements $x_{a_1}(t), \ldots, x_{a_\mu}(t)$, $x_{b_1}(t), \ldots, x_{b_\nu}(t) \in M$ are secretly chosen and that it is difficult to determine these elements given that the conjugates (9) are publically announced.*

We are now in a position to summarize the above example of the Algebraic Eraser^{TM} key agreement protocol.

General Public Information: A subgroup M of the matrix group

$$N = GL\big(n, \mathbb{F}_p(t_1, \ldots, t_n)\big).$$

The symmetric group $S = S_n$ acting on the n variables $t_1, \ldots, t_n$ by permuting them. The subgroup M is chosen to be invariant under the action of S allowing for the formation of the semidirect product $M \rtimes S$.

Covert Information: A finite set of generators,

$$\Big\{\big(x_{a_1}(t), s_{a_1}\big), \ldots, \big(x_{a_\mu}(t), s_{a_\mu}\big)\Big\} \bigcup \Big\{\big(x_{b_1}(t), s_{b_1}\big), \ldots, \big(x_{b_\nu}(t), s_{b_\nu}\big)\Big\} \subseteqq \Big\{\big(x_1(t), s_1\big), \ldots, \big(x_\lambda(t), s_\lambda\big)\Big\},$$

of $M \rtimes S$ satisfying (6), (7), (8), and the hidden elements assumption. An element $z \in M \rtimes S$ satisfying the hidden elements assumption.

Public Information: *An integer $n \geq 7$. A prime number $p > n$. The* **E***–commuting subgroups*

$$A = z \cdot \Big\langle \big(x_{a_1}(t), s_{a_1}\big), \ldots, \big(x_{a_\mu}(t), s_{a_\mu}\big) \Big\rangle \cdot z^{-1},$$

$$B = z \cdot \Big\langle \big(x_{b_1}(t), s_{b_1}\big), \ldots, \big(x_{b_\nu}(t), s_{b_\nu}\big) \Big\rangle \cdot z^{-1},$$

where z is the hidden conjugating element and the $x_i(t)$ are the hidden subgroup generators. The homomorphism $\Pi : M \to N$ satisfying Assumption τ. The operation $\star$ satisfying (2). A fixed matrix $m_0 \in N$.

Alice's Private Key: *A matrix of the form $n_a = \ell_1 m_0^{\alpha_1} + \ell_2 m_0^{\alpha_2} + \cdots + \ell_r m_0^{\alpha_r}$, where $\ell_1, \ldots, \ell_r \in \mathbb{F}_p$ and $r, \alpha_1, \ldots, \alpha_r \in \mathbb{Z}^+$ are secret.*
A subset of generators $\left\{ \left(x_{a_{i_1}}(t), s_{a_{i_1}}\right), \ldots, \left(x_{a_{i_\mu}}(t), s_{a_{i_\mu}}\right) \right\}$ of A.

Alice's Public Key:

$$A_{\text{Public}} = \left(\left(\cdots \left((n_a, id) \star z \right) \star \left(x_{a_{i_1}}(t), s_{a_{i_1}}\right) \star \cdots \right) \star \left(x_{a_{i_\mu}}(t), s_{a_{i_\mu}}\right) \right) \star z^{-1}$$

Bob's Private Key: *A matrix of the form $n_b = \ell'_1 m_0^{\beta_1} + \ell'_2 m_0^{\beta_2} + \cdots + \ell'_{r'} m_0^{\beta_{r'}}$, where $\ell'_1, \ldots, \ell'_{r'} \in \mathbb{F}_p$ and $r', \beta_1, \ldots, \beta_{r'} \in \mathbb{Z}^+$ are secret.*
A subset of generators $\left\{ \left(x_{b_{j_1}}(t), s_{b_{j_1}}\right), \ldots, \left(x_{b_{j_\nu}}(t), s_{b_{j_\nu}}\right) \right\}$ of B.

Bob's Public Key:

$$B_{\text{Public}} = \left(\left(\cdots \left((n_b, id) \star z \right) \star \left(x_{b_{j_1}}(t), s_{b_{j_1}}\right) \star \cdots \right) \star \left(x_{b_{j_\nu}}(t), s_{b_{j_\nu}}\right) \right) \star z^{-1}$$

Shared Secret:

$$\begin{aligned} &\left(\cdots \left((n_a, id) \cdot B_{\text{Public}} \star z \right) \star \left(x_{a_{i_1}}(t), s_{a_{i_1}}\right) \right) \star \cdots \right) \star \left(x_{a_{i_\mu}}(t), s_{a_{i_\mu}}\right) \Big) \star z^{-1} \\ &\quad = \left(\cdots \left((n_b, id) \cdot A_{\text{Public}} \star z \right) \star \left(x_{b_{j_1}}(t), s_{b_{j_1}}\right) \right) \star \cdots \right) \star \left(x_{b_{j_\nu}}(t), s_{b_{j_\nu}}\right) \Big) \star z^{-1}. \end{aligned}$$

In order to analyze the cryptographic applicability of the above algorithm, we shall make the following simplifying assumptions and definition.

- $i_\mu = j_\nu = g$ = *the number of generators in Alice and Bob's private keys.*
- $\lambda \leq n^2$ *where λ is equal to the number of generators of $M \rtimes S$.*

It is now possible to compute the size (in bits) of the public and private keys that occur in the Algebraic Eraser^{TM} Key Agreement Protocol. First of all, Alice and Bob's public keys will simply be a pair consisting of an $n \times n$ matrix with coefficients in the finite field $\mathbb{F}_p$ and an element of the permutation group S_n. Each entry in this matrix will have at most $\log_2(p)$ bits. It follows that the matrix component of the public key will have bit size equal to $n^2 \log_2(p)$. The permuation can be specified by a list of n numbers where each number is between 1 and n. Thus the bit size of the permutation is at most $n \log_2(n) \leq n \log_2(p)$. Consequently, the size of the public key is at most $(n^2 + n) \log_2(p)$. The private key also has two saperate components. First, the high power of the fixed matrix m_0 can be represented with at most $n^2 \log_2(p)$ bits. Secondly, each generator can be specified with at most $\log_2(\lambda) \leq 2 \log_2(n)$ bits. It follows that the size of the private key is at most $n^2 \log_2(p) + 2 \log_2(n) g$. We record these observations in the following proposition.

Proposition 2. *In the Algebraic Eraser^{TM} protocol specified above, the bit-size of the private key is at most*

$$n^2 \log_2(p) + 2\log_2(n)g, \tag{10}$$

while the bit-size of the public key is at most

$$(n^2 + n)\log_2(p). \tag{11}$$

Next, we examine the running time of the algorithm and show that it is essentially linear in the number of generators g in the private key. We shall obtain a crude estimate of the running time in terms of elementary processor operation. By an elementary processor operation we mean either a search and replace operation or a multiplication/addition/subtraction/involving two bits. It is convenient to make the simplifying assumption that each matrix $x_k(t)$ $(k = 1, 2, \ldots, \lambda)$ occurring in the generator $(x_k(t), s_k)$ differs from the identity matrix in at most ℓ entries and that each of these entries is a Laurent polynomial in $\mathbb{F}_p(t)$ where the Laurent polynomial itself has at most ρ terms of degree at most d. For example, the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & t_1 - 2t_2^{-1} - t_2 + t_2^3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 3 + 2t_1 & 0 & 0 & 2 \end{pmatrix}$$

differs from the identity matrix in exactly 3 entries and each of these entries involves Laurent polynomials of at most 4 terms of degree at most 3. The degree is defined to be the absolute value of the largest power, i.e., t_2^{-4} has degree 4. Given an element

$$(x(t), s) \in M \rtimes S$$

and a generator

$$(x_j(t), s_j)$$

of $M \rtimes S$, the most expensive and time consuming operation of the protocol is the computation of

$$(x(t), s) \star (x_j(t), s_j) = \Big(x(t) \cdot \Pi\left({}^s x_j(t)\right),\ ss_j\Big).$$

First of all, the multiplication of permutations ss_j can be done in n search and replace operations, so this is clearly linear in the number of generators g. Second, the computation of ${}^s x_j(t)$ requires at most $\ell\rho$ search and replace operations. The computation of $\Pi\left({}^s x_j(t)\right)$ requires an additional $\ell\rho$ search and replace operations followed by at most $\ell\rho d$ computations in $\mathbb{F}_p$. Finally, the computation of $x(t) \cdot \Pi\left({}^s x_j(t)\right)$ involves at most $n\ell$ multiplications and additions in $\mathbb{F}_p$. This gives an upper bound of $n + 2\ell\rho + 2\ell\rho d(\log_2 p)^2 + 2n\ell(\log_2 p)^2$ elementary operations for each of the g generators. In the final step of the key agreement protocol, it is necessary to multiply two $n \times n$ matrices over $\mathbb{F}_p$. This will take $n^3(\log_2 p)^2$ operations. Assuming that the conjugating element z is made up of g_z generators, the total estimate for the running time of the algorithm is:

$$n^3(\log_2 p)^2 \ + \ (g + 2g_z) \cdot \Big(n + 2\ell\rho + 2\ell\rho d(\log_2 p)^2 + 2n\ell(\log_2 p)^2\Big). \tag{12}$$

One may also give estimates for the memory size (fixed and rewriteable) needed to run the protocol.

§5. The Colored Burau Key Agreement Protocol (CBKAP):

Fix an integer $n \geq 7$, and let $t = (t_1, \ldots, t_n)$. Define

$$x_1(t) = \begin{pmatrix} -t_1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix},$$

and for $i = 2, \ldots n-1$, let

$$x_i(t) := \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & t_i & -t_i & 1 \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}.$$

which is the identity matrix except for the i^{th} row where it has successive entries $t_i, -t_i, 1$ with $-t_i$ on the diagonal. For each $i = 1, 2, \ldots, n-1$, we define

$$s_i \;=\; (i \;\; i+1)$$

which is just the transposition (element of the symmetric group S_n) which interchanges i and $i+1$. The elements $\big(x_i(t), s_i\big)$, for $i = 1, 2, \ldots, n-1$, satisfy the braid relations and hence determine a representation of the braid group (see [AAG2]). Next, fix a prime $p > n$, then the set of pairs

$$\Big\{ \big(x_1(t), s_1\big), \ldots, \big(x_{n-1}(t), s_{n-1}\big) \Big\}$$

will generate the semidirect product $M \rtimes S$ with $S = S_n$ and $M \subset GL(n, \mathbb{F}_p)$. We call the group $M \rtimes S$ the colored Burau group. The general key agreement protocol given in §4, with this choice of M, is termed the colored Burau key agreement protocol (CBKAP). If we choose $\tau = (\tau_1, \tau_2, \ldots, \tau_n)$ with $1 \leq \tau_i < p$ for $1 \leq i \leq n$ then one may easily check that Assumption τ of §4 is satisfied.

In order to implement the CBKAP with the above choice of M it is necessary to effectively choose the matrix m_0, the elements $z \in M \rtimes S$, and

$$x_{a_1}(t), \ldots, x_{a_\mu(t)},\; x_{b_1}(t), \ldots, x_{b_\nu}(t) \in M.$$

With regard to the matrix m_0 one can begin by generating a random matrix from $GL(N, \mathbb{F}_p)$ and test to see if this matrix has an irreducible characteristic polynomial over $\mathbb{F}_p$. If it does not we simply choose another random matrix and repeat the process. Appendix A contains a Mathematica program that performs this task which heuristically runs quickly and is always successful. The resulting matrix m_0 then has an easily calculable multiplicative order because m_0 is diagonalizable over $\mathbb{F}_p$. The non-zero entries of the diagonal matrix will lie in $\mathbb{F}_{p^n}$ and be the roots of the characteristic polynomial. With pobability better than $1/2$, each of these roots will have order $p^n - 1$, and so the matrix m_0 will likewise have order $p^n - 1$. If the roots have a lower order, we again discard and choose a new m_0. Eventually a suitible m_0 will be found.

We now turn to the task of choosing the elements $z \in M \rtimes S$ and

$$x_{a_1}(t), \ldots, x_{a_\mu}(t),\ x_{b_1}(t), \ldots, x_{b_\nu}(t)\ \in\ M.$$

Assuming that we do not want either party to be able to obtain the other's key, a trusted third party (TTP) will be performing the algorithm. If one wishes to design a system which allows for a "master key" then the TTP would simply be one of the users who would then be in possession of the "master key."

The TTP performs the following actions to establish two commuting sets of generators in the braid group. By the representation described above, this produces two **E**–commuting sets of generators in the colored Burau group. Note that these two sets can then be made public and used by any two parties that wish to establish, secretly, a common key. Thus the TTP need only be called upon once.

Let $B_n = \{b_1, \ldots, b_{n-1}\}$ be the Artin representation of the braid group on n strings. Recall that the left canonical form of a braid word may be written as a power of the fundamental braid times a sequence of short braid words, called permutation braids. For further details see [B]. To further shorten the lengths of keys, any even power of the fundamental braid can be ommitted since it is a central element. For the same reason, any odd power of the fundamental braid can simply be replaced by the fundamental braid itself. This will considerably shorten the sequences of integers representing keys.

TTP Algorithm:

(1) *Choose two secret subsets* $BL = \{b_{\ell_1}, \ldots b_{\ell_\alpha}\}$, $BR = \{b_{r_1}, \ldots b_{r_\beta}\}$ *of the set of generators of* B_n, *where* $|\ell_i - r_j| \geq 2$ *for all* $1 \leq i \leq \ell_\alpha$ *and* $1 \leq j \leq r_\beta$.

(2) *Choose a secret element* $z \in B_n$.

(3) *Choose words* $\{w_1, \ldots, w_\gamma\}$ *of bounded length from BL.*

(4) *Choose words* $\{v_1, \ldots, v_\gamma\}$ *of bounded length from BR.*

(5) *For* $1 \leq i \leq \gamma$*:*

(a) *calculate the left normal form of* zw_iz^{-1} *and reduce the result modulo the square of the fundamental braid;*

(b) *set* w_i' *equal to the sequence of integers that corresponds to the element calculated in (a);*

(c) *calculate the left normal form of* zv_iz^{-1} *and reduce the result modulo the square of the fundamental braid;*

(d) *set* v_i' *equal to the sequence of integers that corresponds to the element calculated in (c).*

(5) *Publish the two sets* $\{w_1', \ldots, w_\gamma'\}$ *and* $\{v_1', \ldots, v_\gamma'\}$.