

ACTIONS, COMMUTATOR IDENTITIES, AND THE ALGEBRAIC ERASERTM

Iris Anshel

31 Peter Lynas Ct. Tenafly, NJ 07670, USA

Michael Anshel

City College of New York, New York, NY 10031, USA

Dorian Goldfeld*

Columbia University, Department of Mathematics, New York, NY 10027

Dedicated to Tony Gaglione on his 60th birthday.

Abstract : An algebraic structure arising in the formulation of a lightweight key agreement protocol yields a new concept of commutator whose identities are quite traditional

1. Introduction

In [AAGL] the authors introduced a key agreement protocol for public-key cryptography suitable for implementation on lightweight platforms, that is, those subject to severe cost and resource constraints. Careful examination reveals a hidden notion of commutator possessing identities analogous to those formulated by P. Hall, W. Magnus, E. Witt. The question as to whether or not these eminent mathematicians of the twentieth century developed the theory of commutators for cryptographic purposes was raised in [AG]. Our method is to formulate the necessary mathematical primitives as monoid (group) actions and then identify the objects of interest. We conclude by inviting the reader to explore a certain action in the context of

*The authors would like to thank SecureRF for its support of this research

nonhopfian groups. This paper is dedicated to Professor Anthony Gaglione on his 60th Birthday.

2. The Algebraic EraserTM and its Key Agreement Protocol:

Let M, N denote monoids (or groups), and let

$$\Pi : M \rightarrow N,$$

be a homomorphism. In addition, let S denote a monoid (or group) which acts on M on the left as a monoid of endomorphisms (or a group of automorphisms), i.e., $S \rightarrow \text{End}(M)$, where we view $\text{End}(M)$ as a monoid. The action of $s \in S$ on $m \in M$, is denoted by ${}^s m$, and the semidirect product of M and S , denoted $M \rtimes S$, is the monoid (or group) constructed in the classical manner:

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

The Algebraic EraserTM is, in essence, a right action of $M \rtimes S$ in the direct product $N \times S$ (viewed as a set), together with some additional apparatus which allows for cryptographic applications. The action \mathbf{E} is specified as follows:

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

is given by

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

In practice we often use the more compact notation,

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

That \mathbf{E} is a right action follows from the elementary computation with the operation \star : given $(n, s) \in N \times S$ and $(m_1, s_1), (m_2, s_2) \in M \rtimes S$ then

$$\begin{aligned} ((n, s) \star (m_1, s_1)) \star (m_2, s_2) &= (n \Pi({}^s m_1), s s_1) \star (m_2, s_2) \\ &= (n \Pi({}^s m_1) \Pi({}^{s s_1} m_2), s s_1 s_2) = (n \Pi({}^s m_1 {}^{s s_1} m_2), s s_1 s_2) \\ &= (n \Pi({}^s (m_1 {}^{s s_1} m_2)), s s_1 s_2) = (n, s) \star ((m_1, s_1) (m_2, s_2)). \end{aligned}$$

From the point of view of effective computation, the identity above allows us to compute \star iteratively, which will be useful for applications. In particular, observing that $(1, 1) \star (m, s) = (\Pi(m), s)$ for all $(m, s) \in M \rtimes S$, if one

expressed an element (m, s) as a product in $M \rtimes S$, then $(\Pi(m), s)$ can be computed in stages.

Associated to the action \mathbf{E} , and crucial to encryption applications, is the concept of \mathbf{E} -commuting which is defined as follows: two submonoids (or subgroups) of $A, B \leq M \rtimes S$ are said to \mathbf{E} -commute provided that for all $(a, s_a) \in A, (b, s_b) \in B$

$$(1) \quad (\Pi(a), s_a) \star (b, s_b) = (\Pi(b), s_b) \star (a, s_a).$$

With the above notations in place, the *Algebraic Eraser* \mathbf{E} is defined to be the compilation of the above data,

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

The term *algebraic eraser* is a fitting description of our structure $(M \rtimes S, N, \Pi, \mathbf{E}, A, B)$ in that given $(n, s) \in N \times S$, and $(m_1, s_1) \in M \rtimes S$, knowledge of

$$(n, s) \star (m_1, s_1),$$

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} specified we are in a position to introduce an associated key agreement protocol. Referring to the protocol users as Alice and Bob, each user is assigned a submonoid of N , $N_A, N_B \leq N$ respectively so that N_A and N_B commute. Furthermore we view the \mathbf{E} -commuting submonoids A and B as assigned to Alice and Bob, respectively. With all these choices in place Alice and Bob can choose their respective private keys as follows:

$$A_{\text{Private}} = (n_a, (w_a, s_a)) \quad B_{\text{Private}} = (n_b, (w_b, s_b))$$

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

$$(w_a, s_a) = (a_1, s_{a_1})(a_2, s_{a_2}) \cdots (a_k, s_{a_k}) \in A \leq M \rtimes S,$$

and

$$(w_b, s_b) = (b_1, s_{b_1})(b_2, s_{b_2}) \cdots (b_\ell, s_{b_\ell}) \in B \leq M \rtimes S.$$

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

$$A_{\text{Public}} = (n_a, 1) \star (w_a, s_a) = (n_a \Pi(w_a), s_a) = ((n_a, 1) \star (a_1, s_{a_1})) \star (a_2, s_{a_2}) \star \cdots \in N \times S,$$

$$B_{\text{Public}} = (n_b, 1) \star (w_b, s_b) = (n_b \Pi(w_b), s_b) = ((n_b, \text{id}) \star (b_1, s_{b_1})) \star (b_2, s_{b_2}) \star \cdots \in N \times S.$$

With this done Alice and Bob are now each in a position to compute the shared secret: Alice computes

$$(n_a, 1) \cdot (B_{\text{Public}} \star (w_a, s_a)) = (n_a n_b, 1) \cdot ((\Pi(w_b), s_b) \star (w_a, s_a))$$

(here \cdot denoted multiplication in $N \times S$), Bob computes

$$(n_b, 1) \cdot (A_{\text{Public}} \star (w_b, s_b)) = (n_b n_a, 1) \cdot ((\Pi(w_a), s_a) \star (w_b, s_b)).$$

The assumption that A and B \mathbf{E} -commute and N_A and N_B commute, implies that the two expressions above, computed individually by Bob and Alice, coincide, and the exchanged key is given by

$$(n_a n_b \Pi(w_b^{s_b} w_a), s_b s_a) = (n_b n_a \Pi(w_a^{s_a} w_b), s_a s_b)$$

Specific and detailed implementations of the above protocol can be found in [AAGL]. It should be noted that use of commuting monoids and the \mathbf{E} -commuting structures A, B represents an application of a Shamir 3-pass specialized to this context.

3. Related Algebraic Constructions

The Algebraic Eraser TM , \mathbf{E} , $(M \rtimes S, N, \Pi, \mathbf{E}, A, B)$ and its associate key agreement protocol lend themselves naturally to various traditional 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 \mathbf{E} -commuting condition.

As a first example of a categorical construction, we can define the direct product of two algebraic erasers, \mathbf{E}_1 and \mathbf{E}_2 , in a natural way: Next

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

Next, given a submonoid $H \leq M$ which is S invariant, there is a natural sub structure of $(M \rtimes S, N, \Pi, \mathbf{E}, A, B)$ to consider; by restricting the functions Π and \mathbf{E} , and taking suitable intersections we obtain,

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

where $\Pi \downarrow_H$ denotes the restriction of Π to H .

Finally the concept of a image of an algebraic eraser TM can be approached by starting with a homomorphism $\Psi : N \rightarrow N_0$ and considering the algebraic eraser TM

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

where $\Psi \circ \Pi$, denotes the composite of Ψ and Π , and \mathbf{E}_0 denotes the new action. We leave it to the reader to proceed with this categorical exploration.

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 , $S \leq \text{Aut}(G)$, then the hypothesis of \mathbf{E} -commuting takes the following form. Elements in the subgroups $A, B \leq G \rtimes S$ can be written as

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

where $a, b \in G$ and $\alpha, \beta \in \text{Aut}(G)$. The function Π can be assumed to take the form $G \rightarrow G/K$, and thus \mathbf{E} -multiplication takes the form,

$$(gK, \alpha) \star (h, \beta) = (g\alpha(h)K, \beta \circ \alpha).$$

Elements $(a, \alpha), (b, \beta)$ \mathbf{E} -commute provided identity (1) holds, which in this case takes the form

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

The first component of this identity leads naturally to the following generalization of the classical commutator. Given elements $x, y \in G$, and $\alpha, \beta \in \text{Aut}(G)$, we define the doubly twisted commutator by

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

Clearly when $\alpha, \beta = \text{id}$ we are reduced to the familiar classical definition. Letting

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

be the associated doubly twisted conjugate, then we have the following analogues of the various classical commutator identities (see [MKS]).

Theorem 3.1. *With the notation as above, the following identities hold:*

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

$$(ii) C(\alpha, \beta, xy, z) = \Omega(\text{id}, \beta, x, C(\alpha, \beta, y, z)) C(\text{id}, \text{id}, \beta(x), \alpha(z))$$

$$(iii) C(\alpha, \beta, x, yz) = C(\text{id}, \text{id}, x, y) \Omega(\text{id}, \alpha, y, C(\alpha, \beta, x, z))$$

(iv) *(identity of Hall-Witt type, see [MKS])*

$$y^{-1} C(\text{id}, \alpha, C(\alpha, \alpha, y, \alpha(x^{-1})), \alpha(z^{-1})) y$$

$$\cdot z^{-1} C(\text{id}, \alpha, C(\alpha, \alpha, z, \alpha(y^{-1})), \alpha^2(x^{-1})) z$$

$$\cdot \alpha(x^{-1}) C(\text{id}, \alpha, C(\alpha, \alpha^2, \alpha(x), z^{-1}), \alpha(y^{-1})) \alpha(x) = 1$$

Proof. We give selective verifications leaving the remainder to the interested reader. The identity (i) uses the fact that, in general, $(\alpha(x))^{-1} = \alpha(x^{-1})$:

$$\begin{aligned} C(\alpha, \beta, x, y)^{-1} &= \alpha(y^{-1})^{-1} \beta(x^{-1})^{-1} y^{-1} x^{-1} \\ &\quad \alpha(y) \beta(x) y^{-1} x^{-1} \\ &= C(\beta^{-1}, \alpha^{-1}, \alpha(y), \beta(x)) \end{aligned}$$

To prove (ii) we begin with the expression on the right:

$$\begin{aligned} &\Omega(\text{id}, \beta, x, C(\alpha, \beta, y, z)) C(\text{id}, \text{id}, \beta(x), \alpha(z)) \\ &= x C(\alpha, \beta, y, z) \beta(x)^{-1} \beta(x) \alpha(x) \beta(x)^{-1} \alpha(x)^{-1} \\ &= xy z \beta(y)^{-1} \alpha(z)^{-1} \underline{\beta(x)^{-1} \beta(x)} \alpha(z) \beta(x)^{-1} \alpha(z)^{-1} \\ &= xy z \beta(y)^{-1} \underline{\alpha(z)^{-1} \alpha(z)} \beta(x)^{-1} \alpha(z)^{-1} \\ &= xy z \beta(y^{-1} x^{-1}) \alpha(z)^{-1} \\ &= xy z \beta(xy)^{-1} \alpha(z)^{-1} \\ &= C(\alpha, \beta, xy, z) \end{aligned}$$

Our third identity is, of course, similar. The final identity is equally elementary: expanding

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

we obtain

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

Expanding further we obtain:

$$\begin{aligned}
& y^{-1}y\alpha(x^{-1})\alpha(y^{-1})\alpha^2(x)\alpha(z^{-1})\alpha^3(x^{-1}) \\
& \cdot \alpha^2(y)\alpha^2(x)\alpha(y^{-1})\alpha(z)yz^{-1}zy^{-1}\alpha(z^{-1})\alpha(y)\alpha^2(x^{-1})\alpha^2(y^{-1}) \\
& \cdot \alpha^2(z)\alpha(y)\alpha(z^{-1})\alpha^2(x)z\alpha(x^{-1})\alpha(x)z^{-1}\alpha^2(x^{-1})\alpha(z)\alpha(y^{-1})\alpha^2(z^{-1}) \\
& \cdot \alpha^3(x)\alpha(z)\alpha^2(x^{-1})\alpha(y)\alpha(x).
\end{aligned}$$

The second and the third lines reduce to the identity, leading to a final cascade of cancellations and the desired identity. \square

To conclude this discussion we again focus on the case of a group G , assuming this time that $S \rightarrow \text{Aut}(G)$ and N coincides with G , i.e.,

$$\Pi : G \rightarrow G.$$

In this case the Algebraic EraserTM yields a right action of the semidirect product $G \rtimes S$ on *itself* (viewed as a set)

$$(g, s) \star (g_1, s_1) = (g\Pi(sg_1), ss_1)$$

which can be viewed as a twist of the classical right regular representation. Here an element (g, s) is fixed by the element (g_1, s_1) provided that

$$(g, s) \star (g_1, s_1) = (g, s) \iff \Pi(sg_1) = 1, \text{ and } s_1 = 1.$$

Thus the stabilizer of the element (g, s) is directly related to the kernel of the endomorphism Π ,

$$\begin{aligned}
\text{Stab}(g, s) &= \{(g_1, 1) \mid g_1 \in \ker(\Pi)\} \\
&= \{(g_1, 1) \mid g_1 \in {}^{s^{-1}}\ker(\Pi)\}.
\end{aligned}$$

In fact the set of stabilizers coincides with the orbit of the action of S (on the left) on $\ker(\Pi)$. As with any action the set (see [R]) $G \rtimes S$ is a disjoint union of the orbits of the action and there is a natural bijection between the orbit of a element (g, s) ,

$$\text{Orb}(g, s) = \{(g\Pi(sg_1), ss_1) \mid (g_1, s_1) \in G \rtimes S\}$$

and the right cosets

$$G \rtimes S \text{ mod}(\text{Stab}(g, s)).$$

In the case $\ker(\Pi)$ is trivial then the stabilizers are themselves trivial. When $\ker(\Pi)$ is not trivial, the case of a nonhopfian group comes to mind, the situation becomes for more complex and merits further study. It would be of interest to use a non-hopfian group as a basis for the key agreement protocol introduced in this paper.

4. References

[AAGL] Anshel, I., Anshel, M., Goldfeld, D., Lemieux, S., Key agreement, the algebraic eraserTM, and lightweight cryptography, **Contemporary Mathematics**, 418, 2006.

[AG] Anshel, M., Gaglione, A. M., **The search for origins of the commutator calculus**, Contemporary Mathematics, 421, 2006.

[MKS] Magnus, Wilhelm, Karrass, Abraham, Solitar, Donald *Combinatorial group theory, Presentations of groups in terms of generators and relations*, Reprint of the 1976 second edition. Dover Publications, Inc., Mineola, NY, 2004.

[R] Robinson, Derek J. S., *A Course in the Theory of Groups*, Second Edition, Springer-Verlag, 1995.