Notes on “A Practical Cryptanalysis of the Algebraic Eraser”
Elijah Soria

Let KEY denote the paper “Key Agreement, the Algebraic Eraser^{TM}, and Lightweight Cryptography”.

1. Notation
   - $\mathbb{F}$ is a finite field of small order. S_n is the symmetric group on n elements. $N = \mathrm{GL}_n(\mathbb{F})$ is the general linear group over $\mathbb{F}$.
   - M is a subgroup of $\mathrm{GL}_n(\mathbb{F}(t_1, \ldots, t_n))$, where the t_i's are algebraically independent commuting indeterminates, such that M is contained in the subgroup of $\mathrm{GL}_n(\mathbb{F}(t_1, \ldots, t_n))$ of matrices whose determinant can be written as $a\mathbf{t}$ for some non-zero element $a \in \mathbb{F}$ and some, possibly empty, word $\mathbf{t}$ in the elements t_i and their inverses.
   - $\overline{M}$ is the subgroup of $\mathrm{GL}_n(\mathbb{F}(t_1, \ldots, t_n))$ generated by permuting the indeterminants of M in all possible ways.
     - S_n acts on $\overline{M}$ by permuting the indeterminants t_i.
   - $\varphi : \overline{M} \to \mathrm{GL}_n(\mathbb{F}(t_1, \ldots, t_n))$ is the evaluation homomorphism, where the evaluation elements are the non-zero elements $\tau_1, \ldots, \tau_n \in \mathbb{F}$.
     - This function is denoted as $\Pi : M \to N$ in KEY.
   - The semidirect product $\overline{M} \rtimes S_n$ has the operation defined as

     $$(a, g)(b, h) = (a^g b, gh)$$

     for all $(a, g), (b, h) \in \overline{M} \rtimes S_n$ where ${}^g a$ is the left action of $g \in S_n$ on $a \in \overline{M}$.
   - In the CBKAP, C and D (i.e. $C = D$) are the subgroups of $\mathrm{GL}_n(\mathbb{F})$ consisting of all invertible matrices of the form $l_0 + l_1\kappa + \cdots + l_r\kappa^r$ where κ is a fixed matrix, $l_i \in \mathbb{F}$, and $r \geq 0$.
     - *In this paper, C and D are only assumed to be subgroups of $GL_n(\mathbb{F})$ that commute element wise: $cd = dc$ for all $c \in C$ and $d \in D$...Well actually, in Section 4 they assume that $C = Alg^*(C)$, a more general assumption.*
     - C and D are denoted as N_A and N_B in KEY.
   - $\Omega = \mathrm{GL}_n(\mathbb{F}) \times S_n$. *This is denoted as $N \times S$ in KEY section 4.*
   - $\widehat{S_n} = \overline{M} \rtimes S_n$. *This is denoted as $M \rtimes S$ in KEY section 4.*
   - $* : \Omega \times \widehat{S_n} \to \Omega$ is defined as

     $$(s, g) * (b, h) = (s\varphi({}^g b), gh)$$

for all $(s,g) \in \Omega$ and $(b,h) \in \widehat{S_n}$. *This is the Algebraic Eraser function defined in KEY, so $*$-commuting makes sense.*

- $\bullet : \mathrm{GL}_n(\mathbb{F}) \times \Omega \to \Omega$ is defined as

$$x \bullet (s,g) = (xs, g)$$

for all $x \in \mathrm{GL}_n(\mathbb{F})$ and all $(s,g) \in \Omega$.

- Let A and B be subgroups of $\widehat{S_n}$ that $*$-commute: for all $(a,g) \in A$, $(b,h) \in B$, and $\omega = (x_\omega, s_\omega) \in \Omega$,

$$(\omega*(a,g))*(b,h) = (x_\omega\varphi({}^{s_\omega}a), s_\omega g)*(b,h) = (x_\omega\varphi({}^{s_\omega}b), s_\omega h)*(a,g) = (\omega*(b,h))*(a,g)$$

2. Proposed Attack

- For an arbitrary group $H \subseteq M_n(\mathbb{F}_q)$, we write $\mathrm{Alg}(H)$ for the set of all $\mathbb{F}_q$-linear combinations of matrices in H. We write $\mathrm{Alg}^*(H)$ for the set of all invertible matrices in $\mathrm{Alg}(H)$.
- Let $C = \mathrm{Alg}^*(C)$. Let $\kappa_1, \kappa_2, \ldots, \kappa_r \in C$ be a basis for $\mathrm{Alg}(C)$.
- Let $P \trianglelefteq A$ be defined as (the pure subgroup)

$$P = \{(\alpha, g) \in A : g = e\}.$$

- Let $Q \leq N$ be $Q = \mathrm{Alg}^*(\varphi(P))$. This implies that for all $\alpha' \in Q$,

$$\alpha' = \sum_{i=1}^{k} l_i \varphi(\alpha_i)$$

where $k \geq 0$, $l_i \in \mathbb{F}_q$, and $(\alpha_i, e) \in P$.

- Eve finds elements $\tilde{c} \in C$, $\alpha' \in Q$ and $(\tilde{a}, g) \in \widehat{G}$ such that

$$(p,g) = \tilde{c} \bullet (\alpha', e) * (\tilde{a}, g)$$

and elements $(\alpha_i, e) \in P$ and $l_i \in \mathbb{F}_q$ such that

$$\sum_{i=1}^{k} l_i \varphi(\alpha_i) = \alpha'.$$

If Eve finds this it is GAME OVER FOR ALICE AND BOB.