Fields Institute Communications
Volume **00**, 0000

Algebraic tori in cryptography

Karl Rubin
Department of Mathematics, Stanford University, Stanford CA 94305, USA
rubin@math.stanford.edu

Alice Silverberg
Department of Mathematics, Ohio State University, Columbus OH 43210, USA
silver@math.ohio-state.edu

Abstract. We give a mathematical interpretation in terms of algebraic tori of Lucas-based cryptosystems, XTR, and the conjectural generalizations in [2]. We show that the varieties underlying these systems are quotients of algebraic tori by actions of products of symmetric groups. Further, we use these varieties to disprove conjectures from [2].

1 Introduction

In a series of papers culminating in [7], Edouard Lucas introduced and explored the properties of certain recurrent sequences that became known as Lucas functions. Since then, generalizations and applications of Lucas functions have been studied (see [17, 18, 20]), and public key discrete log based cryptosystems (such as LUC) have been based on them (see [8, 12, 13, 19, 1]). The Lucas functions arise when studying quadratic field extensions. Cryptographic applications of generalizations to cubic and sextic field extensions are given in [4] and [3, 6], respectively. The cryptosystem in [6] is called XTR. An approach for constructing a generalization of these cryptosystems to the case of degree 30 extensions is suggested in [3, 2]. The idea of these cryptosystems is to represent certain elements of $\mathbb{F}_{q^n}^\times$ (for $n = 2$, 6, and 30, respectively) using only $\varphi(n)$ elements of $\mathbb{F}_q$, and do a variant of the Diffie-Hellman key exchange protocol. For XTR and LUC, traces are used to represent the elements. In [2], symmetric functions are proposed in place of the trace (which is the first symmetric function).

In [11] we use algebraic tori to construct public key cryptosystems. These systems are based on the discrete log problem in a subgroup of $\mathbb{F}_{q^n}^\times$ in which the elements can be represented by only $\varphi(n)$ elements of $\mathbb{F}_q$. However, unlike LUC, XTR, and the conjectured system of [2], our systems make direct use of the group structure of an algebraic torus, thereby allowing cryptographic applications (such as ElGamal) that depend not only on exponentiation but also on multiplication.

Rubin was partially supported by NSF grant DMS-0140378.

In [11] we also give examples that disprove the open conjectures from [2] and show that the approach suggested there cannot succeed.

In this paper we give the mathematics, based on the theory of algebraic tori, underlying the cryptosystems and counterexamples in [11], and give an algebro-geometric interpretation of the Lucas-based and XTR cryptosystems and the conjectured generalization. We show that the latter systems are not directly based on an algebraic group, but are in fact based on quotients of algebraic tori by actions of products of symmetric groups.

In §2 we define the tori $\mathcal{T}_L$ we are interested in, and give their basic properties. In §3 we consider actions of permutation groups on tori. We define a variety $\mathcal{X}_F$ in terms of the torus $\mathcal{T}_L$, and show that it is birationally equivalent to a quotient of $\mathcal{T}_L$ by a group action. In §4 we interpret the underlying sets in LUC, XTR, and "beyond" in terms of these varieties. In §5 we study the function fields of the varieties $\mathcal{X}_F$ in the case of degree 30 extensions, and prove that they are not generated by symmetric functions as was proposed in [2].

Note that [10] gives another example, this time in the context of elliptic curves rather than multiplicative groups of fields, where the Weil restriction of scalars is used to obtain $n\log(q)$ bits of security from $\varphi(n)\log(q)$ bit keys.

2 Algebraic tori

Fix a field k, and let k_s be a fixed separable closure of k. Let $\mathbb{A}^d$ denote d-dimensional affine space and let $\mathbb{G}_m$ denote the multiplicative group. If V is a variety and D is a finite set, write

$$V^D := \bigoplus_{\delta\in D} V \cong V^{|D|}.$$

If D is a group, then D acts on V^D by permuting the summands. Write

$$\mathbb{A}^D := (\mathbb{A}^1)^D = \bigoplus_{\delta\in D} \mathbb{A}^1.$$

If G is a group and H is a subgroup, define a norm map $\mathbf{N}_H : \mathbb{G}_m^G \to \mathbb{G}_m^{G/H}$ by $(\alpha_g)_{g\in G} \mapsto (\prod_{\gamma\in gH}\alpha_\gamma)_{gH\in G/H}$ and let

$$\mathbb{T}_G := \ker\big[\mathbb{G}_m^G \xrightarrow{\oplus\mathbf{N}_H} \bigoplus_{1\neq H\subseteq G} \mathbb{G}_m^{G/H}\big].$$

Definition 2.1 An *algebraic torus* T (over k) is an algebraic group defined over k that is isomorphic over k_s to $\mathbb{G}_m^d$, where d is necessarily the dimension of T. If $k\subseteq L\subseteq k_s$ and T is isomorphic to $\mathbb{G}_m^d$ over L, then one says that L *splits* T.

Good references for algebraic tori are [9, 14].

The *character module* $\widehat{T}$ of a torus T is the group $\mathrm{Hom}_{k_s}(T,\mathbb{G}_m)$, which has a natural (continuous) action of $G_k := \mathrm{Gal}(k_s/k)$ (and of $\mathrm{Gal}(L/k)$ for any field L that splits T). Since $\mathrm{Hom}(\mathbb{G}_m,\mathbb{G}_m)=\mathbb{Z}$, as abelian groups we have $\widehat{T}\cong\mathbb{Z}^d$. If T and T' are tori, then there is a natural bijection between $\mathrm{Hom}_k(T,T')$ and $\mathrm{Hom}_{G_k}(\widehat{T'},\widehat{T})$. In particular, the tori T and T' are isomorphic over k if and only if $\widehat{T'}$ and $\widehat{T}$ are isomorphic as G_k-modules. If L is the fixed field of the kernel of the action of G_k on $\widehat{T}$, then L is the minimal splitting field of T.

If M/K is a finite Galois extension and V is a variety defined over M, write $\mathrm{Res}_{M/K}V$ for the Weil restriction of scalars of V from M to K. Then $\mathrm{Res}_{M/K}V$ is a variety defined over K. The next proposition, which follows from the universal

property of $\mathrm{Res}_{M/K}V$, summarizes the properties we need. See §1.3 of [16] or §3.12 of [14] for the definition and properties of the restriction of scalars.

Proposition 2.2 *Suppose M/K is a finite Galois extension and V is a variety defined over K. Let $H = \mathrm{Gal}(M/K)$. Then:*

(i) *for every field F containing K, there is a functorial bijection*
$$(\mathrm{Res}_{M/K}V)(F) \cong V(F \otimes_K M),$$

(ii) *there are functorial morphisms $\pi_\gamma : \mathrm{Res}_{M/K}V \to V$ for every $\gamma \in H$, defined over M, such that the direct sum*
$$\oplus\pi_\gamma : \mathrm{Res}_{M/K}V \xrightarrow{\sim} V^H$$
is an isomorphism defined over M,

(iii) *H acts on $\mathrm{Res}_{M/K}V$ (i.e., there is a homomorphism $H \to \mathrm{Aut}_K(\mathrm{Res}_{M/K}V)$) compatibly with the isomorphisms of* (i) *and* (ii)*, where in* (i)*, H acts on the second factor of $F \otimes_K M$,*

(iv) *if V is an algebraic group, then so is $\mathrm{Res}_{M/K}V$, and the maps above all preserve the group structure as well.*

From now on suppose L is a finite Galois extension of k and $k \subseteq F \subseteq L$. Let
$$H := \mathrm{Gal}(L/F) \subseteq G := \mathrm{Gal}(L/k), \quad e := |H| = [L : F], \quad n := |G| = [L : k].$$
For $1 \le i \le e$ let $\sigma_{i,F}$ denote the composition
$$\sigma_{i,F} : \mathrm{Res}_{L/F}\mathbb{A}^1 \xrightarrow{\sim} \mathbb{A}^H \longrightarrow \mathbb{A}^1 \tag{2.1}$$
where the first map is the isomorphism (defined over L) of Proposition 2.2(ii) and the second map is the i-th symmetric polynomial of the e projection maps $\mathbb{A}^H \to \mathbb{A}^1$. Define
$$\mathcal{G}_F := \mathrm{Res}_{F/k}\mathbb{G}_m \subset \mathrm{Res}_{F/k}\mathbb{A}^1 =: \mathcal{A}_F.$$
Then $\mathcal{G}_F$ is an algebraic torus with character module $\widehat{\mathcal{G}_F} = \mathbb{Z}[G/H]$. By Proposition 2.2(i) we have an isomorphism
$$\mathcal{G}_L(k) \cong \mathbb{G}_m(L) = L^\times. \tag{2.2}$$
The next result follows from Proposition 2.2.

Proposition 2.3 (i) *The maps $\sigma_{i,k} : \mathcal{A}_L \longrightarrow \mathbb{A}^1$ are defined over k.*

(ii) *For every $1 \le i \le e$ there is a commutative diagram*
$$\begin{array}{ccc} \mathcal{A}_L(k) & \xrightarrow{\sigma_{i,k}} & \mathbb{A}^1(k) \\ \cong\downarrow & & \downarrow\cong \\ L & \xrightarrow{\sigma_{i,k}} & k \end{array}$$
where the bottom map $\sigma_{i,k}$ sends $\alpha \in L^\times$ to the i-th symmetric polynomial evaluated on the set of G-conjugates of α, and the left map is defined by Proposition 2.2(i) with $M = L$, $K = k$, and $V = \mathbb{A}^1$.

Denote $\sigma_{e,F}$ and $\sigma_{1,F}$ by $\mathbf{N}_{L/F}$ and $\mathbf{Tr}_{L/F}$, respectively; Proposition 2.3(ii) shows that these correspond to the usual norm and trace maps on $\mathcal{A}_L(k) \cong L$. Applying $\mathrm{Res}_{F/k}$ to (2.1) and using that $\mathrm{Res}_{F/k}\mathrm{Res}_{L/F}\mathbb{A}^1 = \mathcal{A}_L$, we obtain maps
$$\tilde{\sigma}_{i,F} : \mathcal{A}_L \longrightarrow \mathcal{A}_F$$
for $1 \le i \le e$. As above we write $\mathbf{N}_{L/F,k} = \tilde{\sigma}_{e,F}$, and $\mathbf{Tr}_{L/F,k} = \tilde{\sigma}_{1,F}$.

Definition 2.4 We define $\mathcal{T}_L$ (or $\mathcal{T}_{L/k}$ when it is necessary to denote the dependence on the ground field k) to be the intersection of the kernels of the restrictions to $\mathcal{G}_L$ of the norm maps $\mathbf{N}_{L/M,k}$, for all subfields $k \subseteq M \subsetneq L$; i.e.,

$$\mathcal{T}_{L/k} = \mathcal{T}_L = \ker\big[\mathcal{G}_L \xrightarrow{\oplus \mathbf{N}_{L/M,k}} \bigoplus_{k \subseteq M \subsetneq L} \mathcal{G}_M\big].$$

Proposition 2.3(ii) implies that

$$\mathcal{T}_L(k) \cong \{\alpha \in L^\times : N_{L/M}(\alpha) = 1 \text{ whenever } k \subseteq M \subsetneq L\}. \tag{2.3}$$

Remark 2.5 By Lemma 7 of [11], if $k = \mathbb{F}_q$ and $L = \mathbb{F}_{q^n}$, then (2.3) identifies $\mathcal{T}_L(k)$ with the cyclic subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$, where Φ_n is the n-th cyclotomic polynomial.

The isomorphism $\mathcal{G}_L \xrightarrow{\sim} \mathbb{G}_m^G$ of Proposition 2.2(ii) (defined over L) restricts to an isomorphism $\mathcal{T}_L \xrightarrow{\sim} \mathbb{T}_G$ defined over L. For L/k cyclic, Proposition 2.6 below constructs an explicit isomorphism between $\mathbb{T}_G$ and $\mathbb{G}_m^{\varphi(n)}$, and thus shows that $\mathcal{T}_L$ is a torus of dimension $\varphi(n)$ split by L. If L/k is abelian but not cyclic, then an argument similar to the proof of Proposition 2.6 shows that $\mathcal{T}_L$ is finite, i.e., is an algebraic group of dimension zero.

Proposition 2.6 *Suppose G is cyclic, and write $G = \prod_{i=1}^t G_i$ where G_i is cyclic of order $p_i^{a_i} > 1$. For every i let H_i denote the cyclic subgroup of G_i of order p_i, fix a set C_i of coset representatives of G_i/H_i, let $\Gamma_i = G_i - C_i$, and let $\Gamma = \prod_i \Gamma_i \subset G$. Then the composition*

$$\mathbb{T}_G \hookrightarrow \mathbb{G}_m^G \twoheadrightarrow \mathbb{G}_m^\Gamma$$

is an isomorphism.

Proof For $\beta \in \mathbb{G}_m^G$ we have that $\beta \in \mathbb{T}_G$ if and only if $\mathbf{N}_{H_i}(\beta) = 1$ for every i, and therefore

$$\mathbb{T}_G = \{(\beta_\gamma)_{\gamma \in G} : \prod_{\tau \in H_i} \beta_{\gamma\tau} = 1 \text{ for every } \gamma \in G \text{ and } 1 \le i \le t\}. \tag{2.4}$$

We will construct a section $\mathbb{G}_m^\Gamma \hookrightarrow \mathbb{G}_m^G$, with image $\mathbb{T}_G$. Take $\alpha = (\alpha_\gamma)_{\gamma \in \Gamma} \in \mathbb{G}_m^\Gamma$. For $\gamma \in G$, write $\gamma = \gamma_1 \cdots \gamma_t$ with $\gamma_i \in G_i$, let $I_\gamma = \{i : \gamma_i \in C_i\}$, let $D_\gamma = \prod_{i \in I_\gamma}(H_i - \{1\})$, and define

$$\beta_\gamma = \big(\prod_{\tau \in D_\gamma} \alpha_{\gamma\tau}\big)^{(-1)^{|I_\gamma|}}. \tag{2.5}$$

Note that $\gamma\tau \in \Gamma$ for every $\tau \in D_\gamma$. If $\gamma \in \Gamma$, then I_γ is empty, $D_\gamma = 1$, and $\beta_\gamma = \alpha_\gamma$.

We claim that $(\beta_\gamma)_{\gamma \in G} \in \mathbb{T}_G$. Fix $\gamma = \gamma_1 \cdots \gamma_t \in G$ and fix j with $1 \le j \le t$. By the definition of C_j, the set $H_j\gamma_j \cap C_j$ consists of a single element w_j. Let $\eta_j = w_j\gamma_j^{-1} \in H_j$. If $\delta \in H_j - \{\eta_j\}$, then $I_{\gamma\eta_j} = I_{\gamma\delta} \coprod \{j\}$, $D_{\gamma\eta_j} = D_{\gamma\delta} \times (H_j - \{1\})$, and $D_{\gamma\delta}$ is independent of δ. Write D' for $D_{\gamma\delta}$. Then using (2.5),

$$\beta_{\gamma\eta_j} = \big(\prod_{\tau \in D_{\gamma\eta_j}} \alpha_{\gamma\eta_j\tau}\big)^{(-1)^{|I_{\gamma\eta_j}|}} = \big(\prod_{\tau \in D'} \prod_{\delta \in H_j - \{1\}} \alpha_{\gamma\eta_j\tau\delta}\big)^{(-1)^{|I_{\gamma\eta_j}|}} = \prod_{\delta \in H_j - \{\eta_j\}} \beta_{\gamma\delta}^{-1}.$$

Thus $\prod_{\delta \in H_j} \beta_{\gamma\delta} = 1$, so $(\beta_\gamma)_{\gamma \in G} \in \mathbb{T}_G$.

This shows that the map $\mathbb{T}_G \to \mathbb{G}_m^\Gamma$ is surjective. We will now show injectivity. Suppose that $(\beta_\gamma)_{\gamma\in G} \in \mathbb{T}_G$ and $\beta_\gamma = 1$ for every $\gamma \in \Gamma$. We will prove that $\beta_\gamma = 1$ for every $\gamma \in G$, by induction on $|I_\gamma|$. If $|I_\gamma| = 0$, then $\gamma_i \in \Gamma_i$ for all i, so $\gamma \in \Gamma$ and $\beta_\gamma = 1$. If $|I_\gamma| = r \geq 1$, write $\gamma = \gamma_1 \cdots \gamma_t$ with $\gamma_j \notin \Gamma_j$ for some j. Then

$$1 = \prod_{\tau\in H_j} \beta_{\gamma\tau} = \beta_\gamma \prod_{\tau\in H_j - \{1\}} \beta_{\gamma\tau}. \tag{2.6}$$

If $\tau \in H_j - \{1\}$, then $\gamma_j\tau \in \Gamma_j$, so $|I_{\gamma\tau}| \leq r-1$, and by induction we have $\beta_{\gamma\tau} = 1$. By (2.6), we have $\beta_\gamma = 1$. □

The following lemma summarizes some additional facts about $\mathcal{T}_L$. See §5.1 of Chapter 2 of [14].

Lemma 2.7 (i) *If L/k is cyclic, then $\widehat{\mathcal{T}_L} \cong \mathbb{Z}[\zeta_n]$, where a generator of G acts on $\mathbb{Z}[\zeta_n]$ via multiplication by a primitive n-th root of unity ζ_n.*

(ii) *There is an isomorphism $\mathcal{T}_L \cong \mathcal{G}_L / \prod_{k\subseteq M\subsetneq L} \mathcal{G}_M$ defined over k, where we use Proposition 2.2(ii) to view each $\mathcal{G}_F$ as an algebraic subgroup of $\mathcal{G}_L$.*

(iii) *If L/k is abelian and T is a torus that splits over L, then there are cyclic extensions L_i of k in L and a surjective map $T \twoheadrightarrow \prod_i \mathcal{T}_{L_i}$ with finite kernel.*

(iv) *If L/k is cyclic, $k \subset F \subset L$, and every prime dividing $[F:k]$ divides $[L:F]$, then $\mathcal{T}_{L/k} = \mathrm{Res}_{F/k}\mathcal{T}_{L/F}$.*

Remark 2.8 By Lemma 2.7(iii) and (iv), every algebraic torus that splits over an abelian extension of k is isogenous to some $\prod \mathrm{Res}_{F_i/k}\mathcal{T}_{L_i/F_i}$ where each L_i/k is cyclic and $[L_i : F_i]$ is square-free. Therefore once we assume that L/k is abelian, we might as well assume that L/k is cyclic and n is square-free.

An algebraic torus T of dimension d is *rational* if T is birationally isomorphic to $\mathbb{A}^d$. In [11] we show that explicit birational isomorphisms (in both directions) between $\mathcal{T}_L$ and $\mathbb{A}^{\varphi(n)}$, where $L = \mathbb{F}_{q^n}$, lead to cryptosystems with $\varphi(n)\log(q)$ bit keys whose security is based on the difficulty of the discrete log problem in $\mathbb{F}_{q^n}^\times$.

Conjecture 2.9 ([14, 15]) *If L/k is cyclic, then the torus $\mathcal{T}_L$ is rational.*

The conjecture is true if n is a prime power (see Chapter 2 of [14]) or a product of two prime powers ([5]; see also §6.3 of [14]). In [11] we gave explicit rational parametrizations for $\mathcal{T}_L$ when $n = 2$ and 6, and used them to construct public key cryptosystems. When n is divisible by more than two distinct primes the question of the rationality of $\mathcal{T}_L$ is still open. The paper [15] claims to give a proof of the conjecture in characteristic zero, but the proof is flawed. Even the case $n = 30$ is open.

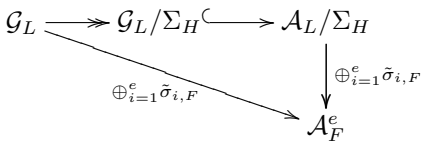
3 Group actions on tori

For this section L/k is a (finite) cyclic extension and for simplicity we assume n is square-free. Recall that $k \subseteq F \subseteq L$, $G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/F)$, $n = |G|$, $e = |H|$. Write $G = \prod G_i$, with the G_i cyclic groups of (distinct) prime order.

Definition 3.1 Let Σ_H denote the group of permutations of the set H. Since n is square-free, there is a unique subgroup $J \subseteq G$ such that $G = H \times J$. This decomposition induces an inclusion $\Sigma_H \subseteq \Sigma_G$, and hence an action of Σ_H on $\mathbb{A}^G$ by permuting the summands. The isomorphism of Proposition 2.2(ii) gives an action of Σ_H on $\mathcal{A}_L$ as well, i.e., we have $\Sigma_H \hookrightarrow \mathrm{Aut}_k(\mathbb{A}^G) \hookrightarrow \mathrm{Aut}_L(\mathcal{A}_L)$. This action of Σ_H preserves $\mathbb{G}_m^G$ and $\mathcal{G}_L$, giving an action on those tori as well.

The quotient varieties $\mathbb{A}^G/\Sigma_H$, $\mathbb{G}_m^G/\Sigma_H$, $\mathcal{A}_L/\Sigma_H$, and $\mathcal{G}_L/\Sigma_H$ are all defined over k.

Proposition 3.2 *The maps $\tilde{\sigma}_{i,F}$ for $1 \le i \le e$ factor through $\mathcal{A}_L/\Sigma_H$ and induce a commutative diagram*



where the right-hand vertical map is an isomorphism.

Proof That the $\tilde{\sigma}_{i,F}$ factor through $\mathcal{A}_L/\Sigma_H$ is clear. The only thing to prove is that the right-hand map is an isomorphism. Since $\tilde{\sigma}_{i,F}$ is obtained from $\sigma_{i,F}$ by applying $\mathrm{Res}_{F/k}$, it suffices to consider the case $F = k$, so $e = n$. Over L, using the identification $\mathcal{A}_L \cong \mathbb{A}^G$ of Proposition 2.2(ii), the right-hand map corresponds to the inclusion of coordinate rings $L[s_1, \dots, s_n] \hookrightarrow L[\dots, x_\gamma, \dots]^{\Sigma_G}$ where the s_i are the symmetric polynomials in indeterminates $\{x_\gamma : \gamma \in G\}$, Σ_G acts by permuting the x_γ, and $L[\dots, x_\gamma, \dots]^{\Sigma_G}$ is the ring of Σ_G-invariant polynomials. That this inclusion is an isomorphism is a standard Galois theory exercise. Thus the right-hand map is an isomorphism. □

Definition 3.3 Let $\mathcal{X}_F$ denote the image of $\mathcal{T}_L$ in $\mathcal{G}_L/\Sigma_H$, and let $\mathbb{X}_H$ denote the image of $\mathbb{T}_G$ in $\mathbb{G}_m^G/\Sigma_H$.

Corollary 3.4 *Fix an isomorphism $\phi = (\phi_1, \dots, \phi_d) : \mathcal{A}_F \xrightarrow{\sim} \mathbb{A}^d$ where $d = [F : k]$ (for example, by fixing a k-basis of F). The function field $k(\mathcal{X}_F)$ is generated by the symmetric functions $\{\phi_j \circ \tilde{\sigma}_{i,F} : 1 \le i \le e, 1 \le j \le d\}$.*

Proof By Proposition 3.2, the maps $\phi_j \circ \tilde{\sigma}_{i,F}$ generate $k(\mathcal{A}_L/\Sigma_H)$. Since $\mathcal{X}_F$ is a subvariety of $\mathcal{A}_L/\Sigma_H$, the restrictions of those maps to $\mathcal{X}_F$ generate $k(\mathcal{X}_F)$. □

If e is divisible by two distinct primes, then the action of Σ_H on $\mathcal{G}_L$ does not preserve $\mathcal{T}_L$. However, we have the following result

Lemma 3.5 *The action of Σ_{G_i} on $\mathcal{G}_L$ preserves $\mathcal{T}_L$.*

Proof Since the action of Σ_G on $\mathcal{G}_L$ is defined from the action on $\mathbb{G}_m^G$, it suffices to show that every $\tau \in \Sigma_{G_i}$ preserves $\mathbb{T}_G$. By (2.4), it suffices to show that for every $(\alpha_\gamma)_{\gamma \in G} \in \mathbb{T}_G$, every $\gamma = \gamma_1 \cdots \gamma_t \in G_1 \cdots G_t = G$, and every j, we have $\prod_{\sigma \in G_j} \alpha_{\tau(\gamma\sigma)} = 1$ for every $\gamma \in G$. Since $\tau \in \Sigma_{G_i}$, we have $\prod_{\sigma \in G_i} \alpha_{\tau(\gamma\sigma)} = \prod_{\sigma \in G_i} \alpha_{(\gamma\gamma_i^{-1})\tau(\gamma_i\sigma)} = \prod_{\sigma \in G_i} \alpha_{(\gamma\gamma_i^{-1})\sigma} = 1$. If $j \ne i$, then $\prod_{\sigma \in G_j} \alpha_{\tau(\gamma\sigma)} = \prod_{\sigma \in G_j} \alpha_{\tau(\gamma)\sigma} = 1$. □

Write $H = \prod H_i$ with $\{H_i\} \subseteq \{G_i\}$, and define

$$\Sigma'_H := \prod_i \Sigma_{H_i} \subseteq \Sigma_H.$$

Clearly the map $\mathcal{T}_L \to \mathcal{X}_F$ factors through $\mathcal{T}_L/\Sigma'_H$.

Proposition 3.6 *If $\sigma \in \Sigma_H$ and $\sigma(\mathbb{T}_G) \subseteq \mathbb{T}_G$, then $\sigma \in \Sigma'_H$.*

Proof Since $\Sigma'_G \cap \Sigma_H = \Sigma'_H$, it suffices to prove the result with $H = G$. Suppose that $\sigma \in \Sigma_G$ and $\sigma(\mathbb{T}_G) \subseteq \mathbb{T}_G$. Order the G_i so that $|G_i| < |G_{i+1}|$. Write $\pi_i : G \to G_i$ for the projection map, and for $g \in G$ let $g_i = \pi_i(g)$. We will first show that $\sigma(\eta G_i) = \sigma(\eta)G_i$ for all $\eta \in G$ and all i.

Take j minimal so that there exists an $\eta \in G$ with $\sigma(\eta G_j) \neq \sigma(\eta)G_j$. Since Σ'_G acts transitively on G, there exist τ_1, $\tau_2 \in \Sigma'_G$ so that $\tau_1(\sigma(\eta)) = 1$ and $\tau_2(1) = \eta$. Replacing σ by $\tau_1\sigma\tau_2$, we may assume that $\eta = 1$, $\sigma(1) = 1$, $\sigma(G_j) \neq G_j$, and

$$\sigma(g \prod_{i<j} G_i) = \sigma(g) \prod_{i<j} G_i \quad \text{for all } g \in G. \tag{3.1}$$

For every i, fix an element $\delta^{(i)} \in G_i$ such that:

$$\delta^{(i)} \in \begin{cases} G_i - \pi_i(\sigma(G_j)) & \text{if } i > j, \\ G_j - \sigma(G_j) & \text{if } i = j, \\ G_i - \{1, \pi_i(\sigma(G_j) \cap \delta^{(j)} \prod_{i<j} G_i)\} & \text{if } 1 < i < j, \\ G_i - \{1\} & \text{if } 1 = i < j. \end{cases}$$

(Note that $\sigma(G_j) \cap \delta^{(j)} \prod_{i<j} G_i$ has at most one element, since by (3.1), if $g, g' \in G_j$ and $g \neq g'$, then $\sigma(g) \prod_{i<j} G_i \neq \sigma(g') \prod_{i<j} G_i$. Since $i > 1$, we have $|G_i| \geq 3$.)

Define $f : G \to \{-1, 0, 1\}$ by $f(g) = \prod f_i(g_i)$ where $f_i : G_i \to \{-1, 0, 1\}$ is defined by $f_i(1) = 1$, $f_i(\delta^{(i)}) = -1$, and $f_i(h) = 0$ otherwise. Fix any $x \in \mathbb{G}_m - \{\pm 1\}$ and define $\alpha = (\alpha_\gamma)_{\gamma \in G} \in \mathbb{G}_m^G$ by $\alpha_\gamma = x^{f(\gamma)}$. It follows from (2.4) that $\alpha \in \mathbb{T}_G$. We will show that $\sigma(\alpha) \notin \mathbb{T}_G$.

Suppose $\tau \in G_j$. If $\sigma(\tau) \in G_j - \{1\}$, then $\sigma(\tau) \notin \{1, \delta^{(j)}\}$, since $\delta^{(j)} \notin \sigma(G_j)$. Thus $f(\sigma(\tau)) = 0$. Suppose $\sigma(\tau) \notin G_j$ and $f(\sigma(\tau)) \neq 0$. Then $\sigma(\tau)_i \in \{1, \delta^{(i)}\}$ for all i. If $i > j$, then $\delta^{(i)} \notin \pi_i(\sigma(G_j))$, so $\sigma(\tau)_i \neq \delta^{(i)}$. Thus $\sigma(\tau)_i = 1$ for all $i > j$. If $\sigma(\tau)_j = 1$, then (again using (3.1)) $\tau = 1$. But we assumed $\sigma(\tau) \notin G_j$. Thus $\sigma(\tau)_j = \delta^{(j)}$, and $\sigma(\tau) \in \sigma(G_j) \cap \delta^{(j)} \prod_{i<j} G_i$. Since $\sigma(\tau) \notin G_j$, it follows from the definition of $\delta^{(i)}$ for $1 < i < j$ that $\sigma(\tau) = \delta^{(1)}\delta^{(j)}$ and $j > 1$. Thus, $f(\sigma(\tau)) = 1$. Since $f(\sigma(1)) = 1$, it follows that $\sum_{\tau \in G_j} f(\sigma(\tau)) = 1$ or 2. Thus, $\prod_{\tau \in G_j} \alpha_{\sigma(\tau)} = x$ or x^2, and thus is not 1. It follows from (2.4) that $\sigma(\alpha) \notin \mathbb{T}_G$, contradicting our assumption.

Thus $\sigma(\eta G_i) = \sigma(\eta)G_i$ for all $\eta \in G$ and all i. It follows easily that $\sigma(g) = \prod_i (\pi_i \circ \sigma_i)(\pi_i(g))$ for all $g \in G$, where σ_i is the restriction of σ to G_i. This means that $\sigma \in \Sigma'_G$. □

Theorem 3.7 *The induced map $\mathcal{T}_L/\Sigma'_H \to \mathcal{X}_F$ is a birational isomorphism.*

Proof The property of being a birational isomorphism is preserved under change of base field, so (using Proposition 2.2(ii)) it suffices to show that the map $\mathbb{T}_G/\Sigma'_H \to \mathbb{X}_H \subset \mathbb{G}_m^G/\Sigma_H$ is generically one-to-one. Suppose $x = (x_\gamma)_{\gamma \in G}$ is a generic point of $\mathbb{T}_G(\Omega)$ for some large field Ω, so the x_γ satisfy no multiplicative relations other than the ones that define $\mathbb{T}_G$, and suppose $\sigma(x) \in \mathbb{T}_G(\Omega)$ for some $\sigma \in \Sigma_H$. Then $\sigma \in \Sigma'_H$ by Proposition 3.6, and the theorem follows. □

4 Understanding LUC, XTR, and "beyond" in terms of tori

In the LUC and XTR algorithms, instead of $g \in \mathcal{T}_L$ one considers the trace $\mathrm{Tr}_{L/F}(g) \in F$. In these special cases (i.e., $(n, e) = (2, 2)$ or $(6, 3)$), for $g \in \mathcal{T}_L$, the trace $\mathrm{Tr}(g) := \mathrm{Tr}_{L/F}(g)$ determines the full characteristic polynomial of g over

F. Thus knowing the trace of g is equivalent to knowing its set of conjugates $C_g := \{\tau(g) : \tau \in \mathrm{Gal}(L/F)\}$.

Given a set $C = \{c_1, \dots, c_t\} \subseteq L$, let $C^{(j)} = \{c_1^j, \dots, c_t^j\}$. If $C = C_g$, then $C^{(j)} = C_{g^j}$. In place of exponentiation ($g \mapsto g^j$), XTR and LUC compute $\mathrm{Tr}(g^j)$ from $\mathrm{Tr}(g)$. In the above interpretation, they compute C_{g^j} from C_g, without needing to distinguish between the elements of C_g. On the other hand, given sets of conjugates $\{g_1, \dots, g_t\}$ and $\{h_1, \dots, h_t\}$, it is not possible (without additional information) to multiply them to produce a new set of conjugates, because we do not know if we are looking for $C_{g_1 h_1}$ or $C_{g_1 h_2}$, for example, which will be different. In other words, $\mathrm{Tr}(g)$ and $\mathrm{Tr}(h)$ do not uniquely determine $\mathrm{Tr}(gh)$. Thus XTR and LUC do not have straightforward multiplication algorithms.

Suppose n is a square-free integer and e is a divisor of n. Let $d = n/e$, $k = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$, and $F = \mathbb{F}_{q^d}$. Then the variety $\mathcal{X}_F$ and the torus $\mathcal{T}_L$ defined in this paper are the variety $B_{(d,e)}$ and the torus T_n, respectively, of [11]. We showed in Theorem 13 of [11] that the sets of traces used in LUC and XTR can be viewed naturally as subsets of $\mathcal{X}_F(k) = B_{(d,e)}(k)$, with $(d,e) = (1,2)$ and $(2,3)$, respectively. If the variety $B_{(d,e)}$ is rational, then one can represent elements of $B_{(d,e)}(k)$ using only $\varphi(n)\log q$ bits, and use them to do cryptography. This was done for $(d,e) = (1,2)$ in LUC, for $(d,e) = (1,3)$ in [4], for $(d,e) = (2,3)$ in XTR, and for $(d,e) = (2,1)$ and $(6,1)$ in the T_2 and CEILIDH cryptosystems of [11]. The T_n cryptosystems in [11] are the cases $(d,e) = (n,1)$. (They are conjectural when n is divisible by more than two primes, because it is not known whether such tori $B_{(n,1)}$ are rational.)

Theorem 3.7 implies that $B_{(d,e)}$ is birationally isomorphic to $T_n/\prod_{\text{primes } \ell \mid e} S_\ell$, where the symmetric group on ℓ letters, S_ℓ, is identified with $\Sigma_{\mathrm{Gal}(L/M)}$ where $M = \mathbb{F}_{q^{n/\ell}}$. In particular,

$$B_{(1,2)} \sim T_2/S_2, \quad B_{(1,3)} \sim T_3/S_3, \quad B_{(2,3)} \sim T_6/S_3, \quad B_{(n,1)} \sim T_n,$$

$$B_{(1,30)} \sim T_{30}/(S_2 \times S_3 \times S_5), \quad B_{(2,15)} \sim T_{30}/(S_3 \times S_5).$$

The variety $B_{(d,e)}$ is not generally a group. However, when $e = 1$, then $B_{(d,e)}$ is the torus T_n, which is a group. This is why the torus-based cryptosystems of [11] can take advantage of both multiplication and exponentiation, while LUC and XTR are exponentiation-based.

Conjectured cryptosystems for other (d,e) are discussed in [2]. The questions in [2] can be interpreted in the language of the present paper as questions about the morphism from $B_{(d,e)}$ to $\mathbb{A}^{\varphi(n)}$ induced by the first $\lceil \varphi(n)/d \rceil$ symmetric functions on the $\mathrm{Gal}(L/F)$-conjugates. The examples in [11] show that when $(d,e) = (1,30)$ or $(2,15)$, then these symmetric functions do not generate the coordinate ring of $B_{(d,e)}$. Theorem 5.3 below shows that these functions do not even generate the function field, so the corresponding morphisms are not birational isomorphisms, and do not give short representations of elements of $B_{(d,e)}$.

5 "Beyond" XTR

In §2 of [11] we answered the open questions from [2] by giving numerical counterexamples. Here we give an algebro-geometric context for these examples, and prove stronger results than those proved in [11]. In [2] it is asked whether, for elements of the order $\Phi_n(p)$ subgroup of $\mathbb{F}_{p^n}^\times$ that do not lie in any proper subfield, it is possible to recover the entire minimal polynomial over a subfield $\mathbb{F}_{p^d}$ from the

first $\lceil \varphi(n)/d \rceil$ symmetric polynomials. Retaining the notation of §3 above, then Conjectures 1 and 3 of [2] would imply, respectively, the following two statements.

Statement 5.1 *Suppose that $k = \mathbb{F}_p$, $L = \mathbb{F}_{p^n}$, and $F = \mathbb{F}_{p^d}$ with $d \mid n$ and $d \neq n$, and fix an isomorphism $\phi = (\phi_1, \ldots, \phi_d) : \mathcal{A}_F \xrightarrow{\sim} \mathbb{A}^d$. Then the function field $k(\mathcal{X}_F)$ is generated by $\{\phi_j \circ \tilde{\sigma}_{i,F} : 1 \leq i \leq \lceil \varphi(n)/d \rceil, 1 \leq j \leq d\}$.*

Statement 5.2 *If $n \in \mathbb{Z}^+$ then there is a $d \in \mathbb{Z}^+$ dividing both n and $\varphi(n)$ such that Statement 5.1 holds with that n and d, for every prime p.*

As shown in §5 of [3], Statements 5.1 and 5.2 are true when $d = 1$ or 2 and n/d is prime. The next theorem shows that Statements 5.1 and 5.2 are false when $n = 30$ (with $d = 1$ and 2 in Statement 5.1).

Theorem 5.3 *There is a finite set P of prime numbers such that if $\mathrm{char}(k) \notin P$, L/k is cyclic of degree 30, $k \subseteq F \subseteq L$ with $d := [F : k] = 1$ or 2, and $\phi = (\phi_1, \ldots, \phi_d) : \mathcal{A}_F \xrightarrow{\sim} \mathbb{A}^d$ is an isomorphism, then the function field $k(\mathcal{X}_F)$ is not generated by $\{\phi_j \circ \tilde{\sigma}_{i,F} : 1 \leq i \leq \lceil 8/d \rceil, 1 \leq j \leq d\}$.*

Proof Suppose that $F = k$. The proof when F/k is quadratic is exactly analogous. Note that $k(\mathcal{X}_k)$ is generated by $\tilde{\sigma}_{1,k}, \ldots, \tilde{\sigma}_{8,k}$ if and only if the morphism $\oplus_{i=1}^8 \sigma_{i,k} : \mathcal{X}_k \to \mathbb{A}^8$ is a birational isomorphism, and for an extension field Ω of L this holds if and only if this is a birational isomorphism over Ω.

Given G, a cyclic group of order 30, Proposition 2.6 gives an isomorphism $\psi : \mathbb{G}_m^8 \xrightarrow{\sim} \mathbb{T}_G \subseteq \mathbb{G}_m^G$. Let $t_1, \ldots, t_8$ be the coordinates on $\mathbb{T}_G$ induced by this isomorphism, let $s_1, \ldots, s_{30}$ be the rational functions of $t_1, \ldots, t_8$ that are the compositions of ψ with the symmetric polynomials on $\mathbb{G}_m^G$, and let $J : \mathbb{T}_G \to \mathbb{A}^1$ be the Jacobian determinant of the map $\mathbf{s} = (s_1, \ldots, s_8) : \mathbb{X}_G \to \mathbb{A}^8$; i.e., $J = \det\left(\frac{\partial s_i}{\partial t_j}\right)$.

By a computer search we found points $\mathbf{x}, \mathbf{y} \in \mathbb{T}_G(\mathbb{F}_{7^{30}})$, distinct modulo the action of Σ_G, such that $\mathbf{s}(\mathbf{x}) = \mathbf{s}(\mathbf{y})$. See §2 of [11] for the details of this computation; we take $\mathbf{x}$ and $\mathbf{y}$ to be the first two entries in Table 1 (respectively, Table 3 in the case $[F : k] = 2$). We computed further that $J(\mathbf{x}) \neq 0$ and $J(\mathbf{y}) \neq 0$.

Set $\mathbf{a} = \mathbf{s}(\mathbf{x}) = \mathbf{s}(\mathbf{y}) \in (\mathbb{F}_{7^{30}})^8$, and let $\tilde{L}$ be the unramified extension of $\mathbb{Q}_7$ of degree 30. By Hensel's Lemma, for every lift $\tilde{\mathbf{a}}$ of $\mathbf{a}$ to $\tilde{L}^8$ we can find unique lifts $\tilde{\mathbf{x}}$ of $\mathbf{x}$ and $\tilde{\mathbf{y}}$ of $\mathbf{y}$ to $\mathbb{T}_G(\tilde{L})$ such that $\mathbf{s}(\tilde{\mathbf{x}}) = \mathbf{s}(\tilde{\mathbf{y}}) = \tilde{\mathbf{a}}$. Thus there is an open (in the 7-adic topology) subset $U \subseteq \tilde{L}^8$ contained in the image of $\mathbf{s}$, over which $\mathbf{s}$ is not one-to-one. It follows that as an algebraic map over $\tilde{L}$, $\mathbf{s}$ is dominant and $\deg(\mathbf{s}) > 1$. Therefore $\mathbf{s}$ is not a birational isomorphism over $\tilde{L}$. The theorem now follows for all k of characteristic zero.

Let $A := \mathbb{Z}[x_1, \ldots, x_8]$ and $B := \mathbb{Z}[s_1, \ldots, s_{30}]$, identifying A with a subring of B via the map induced by $x_i \mapsto s_i$. The field of fractions $\mathrm{Frac}(B)$ of B is $\mathbb{Q}(\mathbb{X}_G)$ by Corollary 3.4. We proved above that this field is a finite nontrivial extension of $\mathrm{Frac}(A) = \mathbb{Q}(\mathbb{A}^8)$. We can therefore choose $0 \neq f \in A$ such that $B' := B[1/f]$ is integral over $A' := A[1/f]$, and $A' \neq B'$.

Let P be the (finite) set of prime numbers that divide f in A. Suppose $p \notin P$. Then pA' (resp., pB') is a prime ideal of A' (resp., B'), and the localizations $A'_{(p)}$ and $B'_{(p)}$ are not equal. By Nakayama's Lemma, $\mathbb{F}_p(x_1, \ldots, x_8) = \mathrm{Frac}(A'/pA') = A'_{(p)}/pA'_{(p)} \neq B'_{(p)}/pB'_{(p)} = \mathrm{Frac}(B'/pB') = \mathbb{F}_p(\mathbb{X}_G)$. Thus $s_1, \ldots, s_8$ do not generate $\mathbb{F}_p(\mathbb{X}_G)$, and the same holds with $\mathbb{F}_p$ replaced by any field of characteristic p. □

Remark 5.4 In fact, our computer computations give additional examples which show that no ten (respectively, four) of the symmetric functions generate the coordinate ring of $\mathcal{X}_F$ over $\overline{\mathbb{F}}_7$ (for $[F : k] = 1$ or 2, respectively).

References

[1] D. Bleichenbacher, W. Bosma, A. K. Lenstra, *Some remarks on Lucas-based cryptosystems*, in Advances in cryptology — CRYPTO '95, Lect. Notes in Comp. Sci. **963** (1995), Springer, Berlin, 386–396.

[2] W. Bosma, J. Hutton, E. R. Verheul, *Looking beyond XTR*, in Advances in cryptology — Asiacrypt 2002, Lect. Notes in Comp. Sci. **2501** (2002), Springer, Berlin, 46–63.

[3] A. E. Brouwer, R. Pellikaan, E. R. Verheul, *Doing more with fewer bits*, in Advances in cryptology — Asiacrypt '99, Lect. Notes in Comp. Sci. **1716** (1999), Springer, Berlin, 321–332.

[4] G. Gong, L. Harn, *Public-key cryptosystems based on cubic finite field extensions*, IEEE Trans. Inform. Theory **45** (1999), 2601–2605.

[5] A. A. Klyachko, *On the rationality of tori with cyclic splitting field*, in Arithmetic and geometry of varieties, Kuybyshev Univ. Press, Kuybyshev, 1988, 73–78 (Russian).

[6] A. K. Lenstra, E. R. Verheul, *The XTR public key system*, in Advances in cryptology — CRYPTO 2000, Lect. Notes in Comp. Sci. **1880** (2000), Springer, Berlin, 1–19.

[7] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–239, 289–321.

[8] W. B. Müller, W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. **16** (1981), 71–76.

[9] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. **74** (1961), 101–139.

[10] K. Rubin, A. Silverberg, *Supersingular abelian varieties in cryptology*, in Advances in cryptology — CRYPTO 2002, Lect. Notes in Comp. Sci. **2442** (2002), Springer, Berlin, 336–353.

[11] ———, *Torus-based cryptography*, to appear in Advances in cryptology — CRYPTO 2003, Lect. Notes in Comp. Sci. (2003), Springer, Berlin.

[12] P. J. Smith, M. J. J. Lennon, *LUC: A New Public Key System*, in Proceedings of the IFIP TC11 Ninth International Conference on Information Security IFIP/Sec'93 (ed. E. G. Dougall), North-Holland, Amsterdam, 1993, 103–117.

[13] P. Smith, C. Skinner, *A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms*, in Advances in cryptology — Asiacrypt 1994, Lect. Notes in Comp. Sci. **917** (1995), 357–364.

[14] V. E. Voskresenskii, Algebraic groups and their birational invariants, Translations of Mathematical Monographs **179**, American Mathematical Society, Providence, RI, 1998.

[15] ———, *Stably rational algebraic tori*, Les XXèmes Journées Arithmétiques (Limoges, 1997), J. Théor. Nombres Bordeaux **11** (1999), 263–268.

[16] A. Weil, Adeles and algebraic groups, Progress in Math. **23**, Birkhäuser, Boston, 1982.

[17] H. C. Williams, *On a generalization of the Lucas functions*, Acta Arith. **20** (1972), 33–51.

[18] ———, *A $p+1$ method of factoring*, Math. Comp. **39** (1982), 225–234.

[19] ———, *Some public-key crypto-functions as intractable as factorization*, Cryptologia **9** (1985). 223–237.

[20] ———, *Édouard Lucas and primality testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts **22**, John Wiley & Sons, Inc., New York, 1998.