COMPRESSION IN FINITE FIELDS AND TORUS-BASED CRYPTOGRAPHY

K. RUBIN AND A. SILVERBERG

This paper is dedicated to the memory of the cat Ceilidh.

Abstract. We present efficient compression algorithms for subgroups of multiplicative groups of finite fields, we use our compression algorithms to construct efficient public key cryptosystems called $\mathbb{T}_2$ and CEILIDH, we disprove some conjectures, and we use the theory of algebraic tori to give a better understanding of our cryptosystems, the Lucas-based, XTR and Gong-Harn cryptosystems, and conjectured generalizations.

1. Introduction

In this paper we present efficient compression algorithms for the elements of the subgroup of order q^2-q+1 in $\mathbb{F}_{q^6}^\times$, the multiplicative group of the finite field with q^6 elements, and for the elements of the subgroup of order $q+1$ in $\mathbb{F}_{q^2}^\times$. We use our compression algorithms to create efficient public key cryptosystems, called CEILIDH and $\mathbb{T}_2$. We also disprove some conjectures from [4] about efficient compression in $\mathbb{F}_{q^n}^\times$. In addition, we show that our compression algorithms, Lucas-based, XTR, Gong-Harn compression, and conjectural generalizations rely on the mathematical properties of algebraic tori, which are concepts from algebraic geometry that are generalizations of the multiplicative group of a field. We believe that studying and understanding the mathematics that underlies the associated cryptosystems is a useful aid to better understand their properties and their security.

Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial, i.e., the monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$ whose complex roots are exactly the primitive n-th roots of unity. The multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$ is a cyclic group of order $q-1 = \Phi_1(q)$. Note that

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \quad \text{so} \quad |\mathbb{F}_{q^n}^\times| = q^n - 1 = \prod_{d|n} \Phi_d(q).$$

For example,

$$|\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1) = \Phi_2(q)\Phi_1(q),$$
$$|\mathbb{F}_{q^6}^\times| = q^6 - 1 = (q^2-q+1)(q^2+q+1)(q+1)(q-1) = \Phi_6(q)\Phi_3(q)\Phi_2(q)\Phi_1(q).$$

2000 *Mathematics Subject Classification.* 94A60, 68P25, 14G50, 11T71.

Key words and phrases. multiplicative groups, compression, torus-based cryptography, CEILIDH.

Preliminary versions of parts of this paper appeared in the proceedings of Crypto 2003 [28], the conference in honour of the 60th birthday of Hugh Cowie Williams [29], and ANTS VI [30].

Rubin is supported by NSF grant DMS-0457481 and Silverberg is supported by NSA grants H98230-05-1-0044 and H9823-07-1-0039. We thank the referees for helpful comments.

Let $G_{q,n}$ denote the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$.

In Diffie-Hellman key agreement, a finite field $\mathbb{F}_q$ and an element $g \in G_{q,1} = \mathbb{F}_q^\times$ are public. Alice (resp., Bob) transmits g^a (resp., g^b), where a (resp., b) is Alice's (resp., Bob's) secret. Then Alice and Bob share the secret $g^{ab} = (g^a)^b = (g^b)^a$.

When doing cryptography in the multiplicative group of a finite field $\mathbb{F}_{q^n}$, mathematically one is taking the $\mathbb{F}_{q^n}$-points of the multiplicative group $\mathbb{G}_m$, which is the same as the $\mathbb{F}_q$-points of the restriction of scalars $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$. This restriction of scalars decomposes (up to isogeny) as a product of algebraic tori that we will denote $\mathbb{T}_d$, one for each divisor d of n. Thus when doing cryptography in $\mathbb{F}_{q^n}^\times$, one is reduced to studying the tori $\mathbb{T}_d$. The torus $\mathbb{T}_d$ is an algebraic group over $\mathbb{F}_q$ of dimension $\varphi(d)$ whose $\mathbb{F}_q$-points form the group $G_{q,d}$ defined above. Being an algebraic torus just means that over an extension field (in this case, $\mathbb{F}_{q^d}$) the algebraic variety is isomorphic to a product of copies of the multiplicative group $\mathbb{G}_m$. Since $\mathbb{T}_d(\mathbb{F}_q) \cong G_{q,d} \subseteq \mathbb{F}_{q^d}^\times$, the subgroup $\mathbb{T}_d(\mathbb{F}_q)$ is subject to index calculus attacks on $\mathbb{F}_{q^d}^\times$; so if $d < n$, then $\mathbb{T}_d$ does not inherit the full security of $\mathbb{F}_{q^n}^\times$. Since almost no element of $\mathbb{T}_n(\mathbb{F}_q)$ lies in a proper subfield of $\mathbb{F}_{q^n}$, the torus $\mathbb{T}_n$ can be viewed as the cryptographically most significant part of $\mathbb{F}_{q^n}^\times$.

Since $\dim(\mathbb{T}_n) = \varphi(n)$, when the transmitted information comes from the group $G_{q,n} = \mathbb{T}_n(\mathbb{F}_q)$ one would hope to be able to compress transmissions down to $\varphi(n)\log q$ bits, rather than the $n \log q$ bits one must use for arbitrary elements of $\mathbb{F}_{q^n}^\times$. In other words, one would like to find an efficiently computable "compression" function f, defined on almost all of $G_{q,n}$, with values in $\mathbb{F}_q^{\varphi(n)}$, such that

(i) $f(h)$ and a determine $f(h^a)$,
(ii) $f(g)$ and $f(h)$ determine $f(gh)$,
(iii) f has an efficiently computable inverse j (a "decompression" map), defined on almost all of $\mathbb{F}_q^{\varphi(n)}$.

This would improve the efficiency of transmissions of group elements for discrete log based cryptography on $\mathbb{F}_{q^n}^\times$ by a factor of $n/\varphi(n)$.

We represent this with a diagram:

$$\begin{tikzcd}
\mathbb{F}_q^{\varphi(n)} \arrow[rr, dashed, bend left, "j"] & & G_{q,n} \arrow[ll, dashed, bend left, "f"]
\end{tikzcd} \tag{1.1}$$

where the dotted arrows signify that f and j need not be defined everywhere; they might be undefined on a "small" number of elements.

Whenever one has a compression map f with a corresponding decompression map j as above, the following protocols give generalized Diffie-Hellman key agreement and ElGamal encryption and signature schemes for the group $G_{q,n}$. Note that such maps f and j allow one to compress and decompress transmissions not only for Diffie-Hellman and ElGamal, but also for any cryptosystem whose security relies on the difficulty of the discrete logarithm problem in the multiplicative group $\mathbb{F}_{q^n}^\times$.

Choose $g \in G_{q,n}$ whose order ℓ is divisible by a large prime number (having chosen a prime power q such that $\Phi_n(q)$ has a large prime divisor).

Torus-based Diffie-Hellman key agreement:

Alice chooses an integer a randomly in the interval $[1, \ell - 1]$. Similarly, Bob chooses a random integer b from the same range.

- Alice sends $P_A := f(g^a) \in \mathbb{F}_q^{\varphi(n)}$ to Bob.
- Bob sends $P_B := f(g^b) \in \mathbb{F}_q^{\varphi(n)}$ to Alice.
- They share $(j(P_B))^a = g^{ab} = (j(P_A))^b$, and also $f(g^{ab})$.

Torus-based ElGamal encryption:
Alice's private key: an integer a, random in the interval $[1, \ell - 1]$.
Alice's public key: $P_A := f(g^a) \in \mathbb{F}_q^{\varphi(n)}$.

- Bob represents the message M in $\langle g \rangle$ and picks a random r between 1 and $\ell - 1$. The ciphertext is (c, d) where $c = f(g^r)$ and $d = f(M \cdot j(P_A)^r)$.
- To decrypt a ciphertext (c, d), Alice computes $M = j(d) \cdot j(c)^{-a}$.

As pointed out by a referee, in practice one would use hybrid encryption rather than textbook ElGamal, in which case a symmetric encryption key would be derived from $f(j(P_A)^r)$.

Torus-based ElGamal signatures:
Fix a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/\ell\mathbb{Z}$ (i.e., the function is easy to compute but hard to invert) and a key derivation function $h : \mathbb{F}_q^{\varphi(n)} \to \mathbb{Z}/\ell\mathbb{Z}$.
Alice's private key: an integer a, random in the interval $[1, \ell - 1]$.
Alice's public key: $P_A := f(g^a) \in \mathbb{F}_q^{\varphi(n)}$.

- To sign a message $M \in \{0,1\}^*$, Alice chooses a random integer r between 1 and $\ell - 1$ with $\gcd(r, \ell) = 1$. Alice's signature on M is (c, d) where $c = f(g^r) \in \mathbb{F}_q^{\varphi(n)}$ and $d = r^{-1}(H(M) - ah(c)) \pmod{\ell}$.
- Bob accepts Alice's signature if and only if

$$g^{H(M)} = j(P_A)^{h(c)} \cdot j(c)^d.$$

The signature length is $\varphi(n)\log_2(q) + \log_2(\ell)$ bits, as opposed to $n \log_2(q) + \log_2(\ell)$ bits in the classical ElGamal signature scheme over $\mathbb{F}_{q^n}$.

Examples of compression functions f that satisfy (i) above (but not (ii) or (iii)) are the trace functions used in the XTR and Lucas-based cryptosystems, which we now recall. (See also [19, 2].)

Lucas-based cryptosystems [25, 39, 40, 34, 35, 3], including LUC, are based on Lucas functions [23]. One way to interpret them is that they compress elements of $G_{q,2} \subset \mathbb{F}_{q^2}^\times$ using the trace map $\mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ defined by $\mathrm{Tr}(x) = x + x^q$. In Lucas-based key agreement, Alice and Bob transmit $\mathrm{Tr}(g^a)$ and $\mathrm{Tr}(g^b)$, respectively, where $g \in G_{q,2}$. It turns out that Alice and Bob each have enough information to reconstruct $\mathrm{Tr}(g^{ab})$. Each party transmits only one element of $\mathbb{F}_q$, rather than one element of $\mathbb{F}_{q^2}$, thereby doubling the efficiency over Diffie-Hellman per unit of security against attacks on the discrete log problem in $\langle g \rangle \subset \mathbb{F}_{q^2}^\times$.

The Gong-Harn cryptosystem [10], which is based on linear feedback shift registers, can be viewed as using two symmetric functions to compress elements of $G_{q,3} \subset \mathbb{F}_{q^3}^\times$, namely the trace map $\mathrm{Tr} : \mathbb{F}_{q^3} \to \mathbb{F}_q$ defined by $\mathrm{Tr}(x) = x + x^q + x^{q^2}$ and the map $\sigma_2 : \mathbb{F}_{q^3} \to \mathbb{F}_q$ defined by $\sigma_2(x) = x \cdot x^q + x \cdot x^{q^2} + x^q \cdot x^{q^2}$. These are two of the three symmetric functions on $\{x, x^q, x^{q^2}\}$; the third is the norm map: $x \mapsto x \cdot x^q \cdot x^{q^2}$, which sends $G_{q,3}$ to 1. In Gong-Harn key agreement, Alice (resp., Bob) transmits $(\mathrm{Tr}(g^a), \sigma_2(g^a))$ (resp., $(\mathrm{Tr}(g^b), \sigma_2(g^b))$), where $g \in G_{q,3}$. It turns out that Alice and Bob each have enough information to reconstruct $\mathrm{Tr}(g^{ab})$ and $\sigma_2(g^{ab})$. Each party transmits only two elements of $\mathbb{F}_q$, rather than one element of

$\mathbb{F}_{q^3}$, thereby improving efficiency over Diffie-Hellman by a factor of $3/2 = 3/\varphi(3)$ per unit of security against attacks on the discrete log problem in $\langle g \rangle \subset \mathbb{F}_{q^3}^{\times}$.

Brouwer-Pellikaan-Verheul [5] and XTR [21] use the trace map $\mathrm{Tr} : \mathbb{F}_{q^6} \to \mathbb{F}_{q^2}$ defined by $\mathrm{Tr}(x) = x + x^{q^2} + x^{q^4}$ to compress elements of $G_{q,6} \subset \mathbb{F}_{q^6}^{\times}$. In XTR key agreement, Alice and Bob transmit $\mathrm{Tr}(g^a)$ and $\mathrm{Tr}(g^b)$, respectively, where $g \in G_{q,6}$. It turns out that they each have enough information to reconstruct a shared secret $\mathrm{Tr}(g^{ab})$. Each party transmits only one element of $\mathbb{F}_{q^2}$, rather than one element of $\mathbb{F}_{q^6}$, thereby tripling the efficiency over Diffie-Hellman per unit of security against attacks on the discrete log problem in $\langle g \rangle \subset \mathbb{F}_{q^6}^{\times}$. Brouwer, Pellikaan, and Verheul [5] asked whether this can be extended to larger n to represent elements of $G_{q,n}$ by $\varphi(n)$ elements of $\mathbb{F}_q$. In [4], Bosma, Hutton, and Verheul state precise conjectures on extending the above systems to larger n.

In XTR, the Gong-Harn cryptosystem, and the Lucas-based cryptosystems, Alice can compute $f(g^{ab})$ from $f(g^b)$ and a, for a suitable f coming from symmetric functions. In other words, these cryptosystems can exponentiate, as is needed for doing (analogues of) Diffie-Hellman. However, they cannot multiply in a straightforward way, as is needed for a direct use of ElGamal, since, for example, $\mathrm{Tr}(g)$ and $\mathrm{Tr}(h)$ do not determine $\mathrm{Tr}(gh)$. For example, for XTR, $\mathrm{Tr}(h) = \mathrm{Tr}(h^{q^2})$ for every h, but it is not the case in general that $\mathrm{Tr}(hg) = \mathrm{Tr}(h^{q^2}g)$ for all $g, h \in G_{q,6}$. However, if one orders the Galois conjugates and transmits a couple of extra bits to specify which conjugate has been chosen, then one can reconstruct an element of $G_{q,6}$ from its trace.

In §§2–3 below we present our compression algorithms. We construct explicit maps f and j as in (1.1) when $n = 2$ and 6, and obtain the $\mathbb{T}_2$ and CEILIDH (or $\mathbb{T}_6$) cryptosystems. We show that they can be explained and implemented in an elementary way without any knowledge of algebraic geometry or algebraic tori (only basic definitions of finite fields are required).

We give background on algebraic tori in §4, and study the algebraic tori $\mathbb{T}_n$ in §5. In §6 we consider rationality results and conjectures for the tori $\mathbb{T}_n$, since whenever the torus $\mathbb{T}_n$ is rational over $\mathbb{F}_q$, compression and decompression maps f and j exist for $G_{q,n}$. In particular, we explain the mathematics that we used to obtain the CEILIDH compression algorithm, and prove that it works. We briefly mention stable rationality in §7. In §8 we discuss security considerations.

In §9.1 we study group actions on tori, in order to give in §9.2 and §10 a deeper mathematical understanding of the Lucas-based systems, XTR, Gong-Harn, and the Bosma-Hutton-Verheul conjectural cryptosystems of [4]. We define an action of certain symmetric groups on the tori $\mathbb{T}_n$, and show (with S_e denoting the symmetric group on e letters) that:

- the Lucas-based cryptosystems are “based on” the quotient variety $\mathbb{T}_2/S_2$,
- the Gong-Harn cryptosystem is based on the quotient variety $\mathbb{T}_3/S_3$,
- XTR is based on the quotient variety $\mathbb{T}_6/S_3$,
- conjectural cryptosystems of Bosma-Hutton-Verheul would rely on the quotient varieties $\mathbb{T}_{30}/(S_3 \times S_5)$ or $\mathbb{T}_{30}/(S_2 \times S_3 \times S_5)$.

These quotient varieties are *not* groups. This is why the Lucas-based systems, Gong-Harn, and XTR do not have straightforward multiplication. However:

- Diffie-Hellman is based on the algebraic group (and algebraic torus) $\mathbb{T}_1 = \mathbb{G}_m$,

- the $\mathbb{T}_2$-cryptosystem is based on the algebraic group (and algebraic torus) $\mathbb{T}_2$,
- CEILIDH is based on the algebraic group (and algebraic torus) $\mathbb{T}_6$,
- the (sometimes conjectural) $\mathbb{T}_n$-cryptosystems are based on the algebraic group (and algebraic torus) $\mathbb{T}_n$.

We therefore called the $\mathbb{T}_n$-cryptosystems "torus-based cryptosystems". (Later authors used our terminology more generally to refer to any cryptosystem using the group $G_{q,n}$ for some q and n, even ones based on quotients of tori.)

In §10 we disprove conjectures from [4], and thereby show that symmetric polynomials are not the correct functions to use for compression in $G_{q,n}$ when n has at least 3 distinct prime divisors.

Security and parameter selection for CEILIDH are exactly the same as for XTR. The advantage of the CEILIDH (resp., $\mathbb{T}_2$) cryptosystem over XTR (resp., LUC) is that CEILIDH and $\mathbb{T}_2$ make full use of the multiplication in the group $G_{q,n}$ (for $n = 6$ and 2). This is especially useful for signature schemes. However XTR and LUC have computational efficiency advantages over CEILIDH and $\mathbb{T}_2$ (key agreement can be performed with fewer operations). See [11] for a comparison of CEILIDH and XTR.

Since the pairings in pairing-based cryptography take values in the algebraic tori considered here, our torus-based cryptography techniques can be used to improve the efficiency of pairing-based cryptography by compressing pairing values [33, 12].

In [31] we study analogues in the setting of elliptic curves and abelian varieties.

2. $\mathbb{T}_2$ compression and the $\mathbb{T}_2$-cryptosystem

Let $n = 2$ and let q be a prime power. One can write $\mathbb{F}_{q^2} = \mathbb{F}_q(\delta)$ for some $\delta \in \mathbb{F}_{q^2}^\times$ with $D := \delta^2 \in \mathbb{F}_q^\times$ if q is odd and $D := \delta^2 + \delta \in \mathbb{F}_q^\times$ if q is even. Since $\delta^q = -\delta$ if q is odd and $\delta^q = \delta + 1$ if q is even, we have

$$\begin{aligned} G_{q,2} &= \{a + b\delta : a, b \in \mathbb{F}_q \text{ and } (a + b\delta)^{q+1} = 1\} \\ &= \begin{cases} \{a + b\delta : a, b \in \mathbb{F}_q \text{ and } a^2 - Db^2 = 1\} & \text{if } q \text{ is odd,} \\ \{a + b\delta : a, b \in \mathbb{F}_q \text{ and } a^2 + Db^2 + ab = 1\} & \text{if } q \text{ is even.} \end{cases} \end{aligned}$$

Hilbert's Theorem 90 leads naturally to the following maps f and j. Define a compression map

$$f : G_{q,2} - \{1, -1\} \to \mathbb{F}_q \qquad \text{by} \qquad f(c + d\delta) = \frac{1 + c}{d}$$

and define a decompression map

$$j : \mathbb{F}_q \to G_{q,2} \quad \text{by} \quad j(a) = \frac{a + \delta}{a + \delta^q} = \begin{cases} \frac{a+\delta}{a-\delta} & \text{if } q \text{ is odd,} \\ \frac{a+\delta}{a+\delta+1} & \text{if } q \text{ is even.} \end{cases}$$

It is easy to check that f and j are inverse maps where they are defined, and if $a, b \in \mathbb{F}_q$ and $a \neq -b$ (respectively, $a \neq b + 1$) then

$$\begin{aligned} j(a)j(b) &= j\big(\tfrac{ab+D}{a+b}\big) \quad \text{if } q \text{ is odd,} \\ j(a)j(b) &= j\big(\tfrac{ab+D}{a+b+1}\big) \quad \text{if } q \text{ is even.} \end{aligned}$$

To do $\mathbb{T}_2$-cryptography, use f to represent the elements of $G_{q,2} - \{1, -1\}$ in $\mathbb{F}_q$, and do all multiplications and exponentiations directly in $\mathbb{F}_q$ (without needing to use j), using the operation on (most of) $\mathbb{F}_q$:

$$a * b = \frac{ab+D}{a+b}, \qquad \text{respectively} \qquad a * b = \frac{ab+D}{a+b+1}$$

if q is odd, respectively even.

3. CEILIDH compression and the CEILIDH public key system

The acronym **CEILIDH** (pronounced "cayley", like the Scottish Gaelic word ceilidh) stands for **C**ompact, **E**fficient, **I**mproves on **L**UC, **I**mproves on **D**iffie-**H**ellman. The CEILIDH key agreement (resp., encryption, resp., signature) scheme is torus-based Diffie-Hellman (resp., ElGamal encryption, resp., ElGamal signatures) in the case $n = 6$.

3.1. CEILIDH compression algorithm.

When $n = 6$, we can generate explicit examples of maps f and j at will. Next we give our algorithm for doing so. In §6 below we will give a proof that it works and explain the mathematics behind it.

For a polynomial h in two variables with coefficients in $\mathbb{F}_q$, let

$$V(h) = \{(a,b) \in \mathbb{F}_q^2 : h(a,b) = 0\}.$$

Fix a prime power q. Fix $x \in \mathbb{F}_{q^2} - \mathbb{F}_q$, so $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$, and choose a basis $\{\alpha_1, \alpha_2, \alpha_3\}$ of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$. Then $\{\alpha_1, \alpha_2, \alpha_3, x\alpha_1, x\alpha_2, x\alpha_3\}$ is a basis of $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$. Let $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$ be the element of order 2, i.e., $\sigma(z) = z^{q^3}$. Define a map $j_0 : \mathbb{F}_q^3 \hookrightarrow \mathbb{F}_{q^6}^\times$ by

$$j_0(u,v,w) = \frac{\gamma + x}{\gamma + \sigma(x)}$$

where $\gamma = u\alpha_1 + v\alpha_2 + w\alpha_3$. Let

$$U = \{(u,v,w) \in \mathbb{F}_q^3 : N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(j_0(u,v,w)) = 1\}.$$

A calculation in Mathematica shows that U is a hypersurface in $\mathbb{F}_q^3$ defined by a quadratic equation in u, v, w. Fix a point $\beta = (\beta_1, \beta_2, \beta_3) \in U(\mathbb{F}_q)$. Adjust the basis $\{\alpha_1, \alpha_2, \alpha_3\}$ if necessary, to ensure that the tangent plane at β to the surface U is $u = \beta_1$. If $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$, then the intersection of U with the line $\beta + t(1,a,b)$ consists of two points, namely β and a point $g(a,b) \in U$ of the form $\beta + \frac{1}{h(a,b)}(1,a,b)$ where $h(a,b) \in \mathbb{F}_q[a,b]$ is an explicit polynomial that can be computed using Mathematica. The map g is an isomorphism

$$g : \mathbb{F}_q^2 - V(h) \xrightarrow{\sim} U - \{\beta\},$$

and $j_0 \circ g$ defines an isomorphism

$$j : \mathbb{F}_q^2 - V(h) \xrightarrow{\sim} G_{q,6} - \{1, j_0(\beta)\}.$$

For the inverse isomorphism, suppose that $t = c + dx \in G_{q,6} - \{1, j_0(\beta)\}$ with $c, d \in \mathbb{F}_{q^3}$. Write $(1+c)/d = u\alpha_1 + v\alpha_2 + w\alpha_3$ with $u, v, w \in \mathbb{F}_q$, and define

$$f(t) = \left(\frac{v - \beta_2}{u - \beta_1}, \frac{w - \beta_3}{u - \beta_1}\right).$$

Then $f : G_{q,6} - \{1, j_0(\beta)\} \xrightarrow{\sim} \mathbb{F}_q^2 - V(h)$ satisfies $f \circ j = \mathrm{id}$ and $j \circ f = \mathrm{id}$.

3.2. **Explicit examples of maps f and j.** Using the above algorithm, we produce explicit examples, where ζ_m denotes an m-th root of unity in $\overline{\mathbb{F}}_q$.

Example 3.1. To ensure that $\mathbb{F}_{q^6} = \mathbb{F}_q(\zeta_9)$, restrict to prime powers $q \equiv 2$ or $5 \pmod 9$. Let $x = \zeta_3$ and let $(\alpha_1, \alpha_2, \alpha_3) = (1, \zeta_9 + \zeta_9^{-1}, \zeta_9^2 + \zeta_9^{-2})$. The hypersurface U is given by the quadratic equation $u^2 - u - v^2 + vw - w^2 = 0$. Let $\beta = (0, 0, 0)$. The above algorithm gives a map $j : \mathbb{F}_q^2 \to G_{q,6}$ defined by

$$j(a, b) = (r + s\zeta_3)/(r + s\zeta_3^2)$$

where

$$r = 1 + a(\zeta_9 + \zeta_9^{-1}) + b(\zeta_9^2 + \zeta_9^{-2}), \quad s = h(a, b) = 1 - a^2 - b^2 + ab,$$

and a map $f : G_{q,6} - \{1, \zeta_3^2\} \xrightarrow{\sim} \mathbb{F}_q^2 - V(h)$ defined by $f(t) = (v/u, w/u)$ where $t = c + d\zeta_3$ with $c, d \in \mathbb{F}_{q^3}$ and $(1 + c)/d = u + v(\zeta_9 + \zeta_9^{-1}) + w(\zeta_9^2 + \zeta_9^{-2})$ with $u, v, w \in \mathbb{F}_q$.

Example 3.2. In order to ensure that $\mathbb{F}_{q^6} = \mathbb{F}_q(\zeta_7)$, restrict to prime powers $q \equiv 3$ or $5 \pmod 7$. We can then let $x = \sqrt{-7}$, $\beta = (1, 0, 2)$, and $(\alpha_1, \alpha_2, \alpha_3) = (1, \zeta_7 + \zeta_7^{-1}, \zeta_7^2 + \zeta_7^{-2} + 1)$. The above algorithm outputs a map $j : \mathbb{F}_q^2 \to G_{q,6}$ defined by $j(a, b) = (r + s\sqrt{-7})/(r - s\sqrt{-7})$ where

$$s = h(a, b) = (2a^2 + b^2 - ab + 2a - 4b - 3)/14,$$
$$r = h(a, b) + 1 + a(\zeta_7 + \zeta_7^{-1}) + (2h(a, b) + b)(\zeta_7^2 + \zeta_7^{-2} + 1),$$

and a map $f : G_{q,6} - \{1, \zeta_7^2\} \xrightarrow{\sim} \mathbb{F}_q^2 - V(h)$ defined by

$$f(t) = \Big(\frac{v}{u-1}, \frac{w-2}{u-1}\Big)$$

where $t = c + d\sqrt{-7}$ with $c, d \in \mathbb{F}_{q^3}$ and $(1+c)/d = u + v(\zeta_7 + \zeta_7^{-1}) + w(\zeta_7^2 + \zeta_7^{-2} + 1)$ with $u, v, w \in \mathbb{F}_q$. Here U is defined by $3u^2 - 2uv - 2v^2 + 4uw + vw - w^2 = 7$.

Example 3.3. Let q be an odd prime power congruent to 2, 6, 7, or 11 (mod 13), and let $z = \zeta_{13} + \zeta_{13}^{-1}$. Then $\mathbb{F}_{q^{12}} = \mathbb{F}_q(\zeta_{13})$ and $\mathbb{F}_{q^6} = \mathbb{F}_q(z)$. Let $x = \sqrt{13}$, let $\beta = (-1, 0, 3)$, let $y = \zeta_{13} + \zeta_{13}^{-1} + \zeta_{13}^5 + \zeta_{13}^{-5} \in \mathbb{F}_{q^3}$, and let $(\alpha_1, \alpha_2, \alpha_3) = (y^2, y + \frac{y^2}{2}, 1)$. The above algorithm outputs a map $j : \mathbb{F}_q^2 \to G_{q,6}$ defined by $j(a, b) = (r - s\sqrt{13})/(r + s\sqrt{13})$ where

$$\begin{aligned} r = {} & (3(a^2 + b^2) + 7ab + 34a + 18b + 40)y^2 + 26ay - \\ & \qquad (21a(3 + b) + 9(a^2 + b^2) + 28b + 42), \\ s = {} & 3(a^2 + b^2) + 7ab + 21a + 18b + 14, \end{aligned}$$

and a map $f : G_{q,6} - \{1, -2z^5 + 6z^3 - 4z - 1\} \to \mathbb{F}_q^2$ defined by

$$f(t) = \Big(\frac{v}{u+1}, \frac{w-3}{u+1}\Big)$$

where $t = c + d\sqrt{13}$ with $c, d \in \mathbb{F}_{q^3}$ and $(1 + c)/d = uy^2 + v(y + \frac{y^2}{2}) + w$ with $u, v, w \in \mathbb{F}_q$. Here U is defined by $14u^2 + 21uv + 3v^2 + 18uw + 7vw + 3w^2 = -13$.

4. Algebraic tori

In this section we briefly introduce algebraic tori, in order to explain the mathematics underlying compression algorithms for $G_{q,n} \subseteq \mathbb{F}_{q^n}^\times$.

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 together with a morphism

$$\eta : \mathrm{Res}_{M/k}V \to V \tag{4.1}$$

defined over M that induces an isomorphism

$$\eta : (\mathrm{Res}_{M/k}V)(k) \xrightarrow{\sim} V(M). \tag{4.2}$$

A precise technical definition is that the restriction of scalars $\mathrm{Res}_{M/k}V$ is uniquely defined by the universal property that for every scheme X over k (and therefore every variety X over k) and every morphism $f : X \to V$, there exists a unique morphism $f_0 : X \to \mathrm{Res}_{M/k}V$ such that $\eta \circ f_0 = f$. See §1.3 of [38] or §3.12 of [36] for more on the restriction of scalars.

If V is an algebraic 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. Let $\mathbb{A}^d$ denote d-dimensional affine space (so $\mathbb{A}^d(k) = k^d$), and let $\mathbb{A}^D := (\mathbb{A}^1)^D$.

If V is defined over k and $\Gamma = \mathrm{Gal}(M/k)$, then the morphism η of (4.1) induces an isomorphism

$$\bigoplus_{\gamma \in \Gamma} \eta^\gamma : \mathrm{Res}_{M/k}V \xrightarrow{\sim} V^\Gamma \tag{4.3}$$

defined over M (see §1.3 of [38]), where $\eta^\gamma : \mathrm{Res}_{M/k}V \to V$ is the morphism defined by applying γ to the coefficients of the rational functions that define η.

Let $\mathbb{G}_m$ denote the multiplicative group over a field k. Then $\mathbb{G}_m$ $(\subset \mathbb{A}^1)$ is an algebraic group over k such that $\mathbb{G}_m(F) = F^\times$ for all extension fields F of k.

Definition 4.1. An *algebraic torus* over a field k is an algebraic group over k that over some larger field is isomorphic to a product of copies of $\mathbb{G}_m$. A field over which the torus becomes isomorphic to a product of multiplicative groups is called a *splitting field* for the torus; one says that the torus *splits* over that field.

Good references for algebraic tori are [26, 36].

Example 4.2.
(i) For every positive integer n, $\mathbb{G}_m^n$ is an n-dimensional algebraic torus.
(ii) If L/k is an extension of degree n, then $\mathrm{Res}_{L/k}\mathbb{G}_m$ is an n-dimensional algebraic torus over k that splits over L (by (4.3) with $V = \mathbb{G}_m$).

5. The algebraic tori $\mathbb{T}_{L/k}$ and $\mathbb{T}_n$

Next we define the algebraic tori that underlie the XTR, Gong-Harn, Lucas-based, $\mathbb{T}_2$, and CEILIDH cryptosystems, and give some of their basic properties.

Suppose L/k is a finite Galois extension and $n := [L : k]$ is square-free. Suppose $k \subseteq F \subseteq L$, and let $G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/F)$, and $e = |H|$. For $1 \le i \le e$ let $\sigma_{i,F}$ denote the composition

$$\sigma_{i,F} : \mathrm{Res}_{L/F}\mathbb{A}^1 \xrightarrow{\sim} \mathbb{A}^H \longrightarrow \mathbb{A}^1 \tag{5.1}$$

where the first map is the isomorphism (defined over L) coming from (4.3) and the second map is the i-th symmetric polynomial of the e projection maps $\mathbb{A}^H \to \mathbb{A}^1$. (Recall that the first symmetric polynomial of $x_1, \ldots, x_e$ is $\sum_{i=1}^{e} x_i$, the second is $\sum_{i<j} x_i x_j$, and the e-th is $\prod_{i=1}^{e} x_i$.)

The next lemma will used to define the algebraic tori $\mathbb{T}_{L/k}$ and prove properties about them.

Lemma 5.1. (i) *The maps $\sigma_{i,k} : \mathrm{Res}_{L/k}\mathbb{A}^1 \longrightarrow \mathbb{A}^1$ are defined over k.*

(ii) *For every $1 \le i \le n$ the following diagram is commutative:*

$$\begin{tikzcd}
(\mathrm{Res}_{L/k}\mathbb{A}^1)(k) \arrow[r, "\sigma_{i,k}"] \arrow[d, "\cong"'] & \mathbb{A}^1(k) \arrow[d, "\cong"'] \\
L \arrow[r, "\sigma_{i,k}"] & k
\end{tikzcd}$$

where the bottom map $\sigma_{i,k}$ sends $\alpha \in L$ to the i-th symmetric polynomial evaluated on the set of G-conjugates of α, the right map is the natural identification, and the left map is the composition of (4.2) *with the natural identification $\mathbb{A}^1(L) \cong L$.*

Proof. Part (i) follows since symmetric functions are symmetric, while (ii) follows from the definitions and the fact that $(\eta(v))^\sigma = \eta^\sigma(v)$ for all $v \in (\mathrm{Res}_{L/k}\mathbb{A}^1)(k)$ and $\sigma \in \mathrm{Gal}(L/k)$. □

Lemma 5.1(ii) shows that $\sigma_{n,k}$ and $\sigma_{1,k}$ correspond to the usual norm and trace maps from $(\mathrm{Res}_{L/k}\mathbb{A}^1)(k) \cong L$ to k. Applying $\mathrm{Res}_{F/k}$ to (5.1) and using that $\mathrm{Res}_{L/k}\mathbb{A}^1 = \mathrm{Res}_{F/k}(\mathrm{Res}_{L/F}\mathbb{A}^1)$, we obtain maps

$$\tilde{\sigma}_{i,F} : \mathrm{Res}_{L/k}\mathbb{A}^1 \longrightarrow \mathrm{Res}_{F/k}\mathbb{A}^1 \tag{5.2}$$

for $1 \le i \le e$. Let $\mathrm{N}_{L/F,k} := \tilde{\sigma}_{e,F}$ and $\mathrm{Tr}_{L/F,k} := \tilde{\sigma}_{1,F}$.

Definition 5.2. Define $\mathbb{T}_{L/k}$ by

$$\mathbb{T}_{L/k} := \ker\bigl[\mathrm{Res}_{L/k}\mathbb{G}_m \xrightarrow{\oplus \mathrm{N}_{L/M,k}} \bigoplus_{k \subseteq M \subsetneq L} \mathrm{Res}_{M/k}\mathbb{G}_m\bigr].$$

Let $\mathbb{T}_n$ (or $\mathbb{T}_{n,q}$) denote $\mathbb{T}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

By definition, $\mathbb{T}_{L/k}$ is a subvariety and algebraic subgroup of $\mathrm{Res}_{L/k}\mathbb{G}_m$, defined over k. When L/k is abelian but not cyclic, then the algebraic group $\mathbb{T}_{L/k}$ has dimension zero (see Proposition 5.3 of [24]). Lemmas 5.4 and 5.6 below show that when L/k is cyclic, then $\mathbb{T}_{L/k}$ is isomorphic over L to $\mathbb{G}_m^{\varphi(n)}$, and thus $\mathbb{T}_{L/k}$ is an algebraic torus of dimension $\varphi(n)$ that splits over L. When L/k is cyclic, $\mathbb{T}_{L/k}$ is the variety V_L defined in §5 of [24] with $V = \mathbb{G}_m$ (see Remark 5.11 of [24]). We first need some notation, which will also be used in §§9–10.

Definition 5.3. If Γ is a finite group and Δ is a subgroup, let Γ/Δ denote the coset space. Letting σ_i denote the i-th symmetric function, for $i = 1, \ldots, |\Delta|$ define

$$s_i : \mathbb{A}^\Gamma \to \mathbb{A}^{\Gamma/\Delta} \quad \text{by} \quad (\alpha_g)_{g\in\Gamma} \mapsto (\sigma_i(\{\alpha_\gamma : \gamma \in g\Delta\}))_{g\Delta\in\Gamma/\Delta}.$$

Let $\mathbb{N}_\Delta$ be the restriction of $s_{|\Delta|}$ to $\mathbb{G}_m^\Gamma$, i.e.,

$$\mathbb{N}_\Delta : \mathbb{G}_m^\Gamma \to \mathbb{G}_m^{\Gamma/\Delta}, \qquad (\alpha_g)_{g\in\Gamma} \mapsto (\prod_{\gamma\in g\Delta} \alpha_\gamma)_{g\Delta\in\Gamma/\Delta},$$

and let

$$\begin{aligned}\mathbb{T}_\Gamma :&= \ker\bigl[\mathbb{G}_m^\Gamma \xrightarrow{\oplus \mathbb{N}_\Delta} \bigoplus_{1 \neq \Delta \subseteq \Gamma} \mathbb{G}_m^{\Gamma/\Delta}\bigr] \\ &= \{(x_g)_{g \in \Gamma} : \prod_{h \in \Delta} x_{gh} = 1 \text{ for all } g \in \Gamma \text{ and all subgroups } \Delta \neq 1 \text{ of } \Gamma\}.\end{aligned}$$

Viewing $\mathbb{G}_m$ as an algebraic group over a field k, then $\mathbb{T}_\Gamma$ is an algebraic group over k. The next lemma, which we will use repeatedly, follows directly from the definitions of $\mathbb{T}_{L/k}$ and $\mathbb{T}_G$.

Lemma 5.4. *The isomorphism* $\mathrm{Res}_{L/k}\mathbb{G}_m \xrightarrow{\sim} \mathbb{G}_m^G$ *given by* (4.3) *(with* $V = \mathbb{G}_m$*) restricts to an isomorphism* $\mathbb{T}_{L/k} \xrightarrow{\sim} \mathbb{T}_G$ *(defined over* L*).*

The next result is used to prove Lemma 5.6 and Proposition 5.8 below. For a proof, see for example Theorem 1 of [6] or Theorem 2 of [32]. We thank D. Bernstein and H. Lenstra for pointing out these references.

Lemma 5.5. *For every positive integer* n, $\Phi_n(x)$ *and the set*

$$\left\{\frac{x^n - 1}{x^t - 1} : t \mid n \text{ and } 1 \leq t \neq n\right\}$$

generate the same ideal of $\mathbb{Z}[x]$.

Lemma 5.6 is used to prove Theorems 5.7 and 10.9 below. Its proof can be ignored by the casual reader.

Lemma 5.6. *Suppose* Γ *is a cyclic group of squarefree order. Let* Ω *be the subset of* Γ *consisting of all generators of* Γ*. The projection map* $\mathbb{G}_m^\Gamma \twoheadrightarrow \mathbb{G}_m^\Omega$ *restricts to an isomorphism* $\mathbb{T}_\Gamma \xrightarrow{\sim} \mathbb{G}_m^\Omega$ *of algebraic groups over* k.

Proof. Let $m = |\Gamma|$. If Δ is a subgroup of Γ, let $N_\Delta := \sum_{h \in \Delta} h$. Let I denote the ideal of $\mathbb{Z}[\Gamma]$ generated by $\{N_\Delta : \Delta \neq 1 \text{ is a subgroup of } \Gamma\}$. The map $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\Gamma], \mathbb{G}_m) \to \mathbb{G}_m^\Gamma$ defined by $\phi \mapsto (\phi(g))_{g \in \Gamma}$ induces a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{Z}[\Gamma]/I, \mathbb{G}_m) \arrow[r, hook] \arrow[d, "\cong"] & \mathrm{Hom}(\mathbb{Z}[\Gamma], \mathbb{G}_m) \arrow[r, two heads] \arrow[d, "\cong"] & \mathrm{Hom}(\oplus_{\gamma \in \Omega}\mathbb{Z}\gamma, \mathbb{G}_m) \arrow[d, "\cong"] \\
\mathbb{T}_\Gamma \arrow[r, hook] & \mathbb{G}_m^\Gamma \arrow[r, two heads] & \mathbb{G}_m^\Omega
\end{tikzcd}$$

where the vertical maps are group isomorphisms and the top and bottom rows are the natural maps. For each $g \in \Gamma$, let $\bar{g}$ denote its image in $\mathbb{Z}[\Gamma]/I$. Let τ denote a generator of Γ. Since Γ is cyclic, $\tau \mapsto x$ induces an isomorphism $\mathbb{Z}[\Gamma] \xrightarrow{\sim} \mathbb{Z}[x]/(x^m - 1)\mathbb{Z}[x]$. By Lemma 5.5, this map induces an isomorphism $\mathbb{Z}[\Gamma]/I \xrightarrow{\sim} \mathbb{Z}[x]/\Phi_m(x)\mathbb{Z}[x] \cong \mathbb{Z}[\zeta_m]$ that sends τ to ζ_m. Since m is squarefree, the primitive m-th roots of unity form a $\mathbb{Z}$-basis for $\mathbb{Z}[\zeta_m]$ (see for example [22]), i.e., $\mathbb{Z}[\zeta_m] = \oplus_{a \in R}\mathbb{Z}\zeta_m^a$, where $R := (\mathbb{Z}/m\mathbb{Z})^\times$. It follows that $\mathbb{Z}[\Gamma]/I = \oplus_{a \in R}\mathbb{Z}\bar{\tau}^a = \oplus_{\gamma \in \Omega}\mathbb{Z}\bar{\gamma}$. This says exactly that the natural group homomorphism $\oplus_{\gamma \in \Omega}\mathbb{Z}\gamma \to \mathbb{Z}[\Gamma]/I$ is an isomorphism. Therefore the composition in the top line of the commutative diagram is an isomorphism. Thus the composition in the bottom line of the diagram is an isomorphism, as desired. □

If V and W are algebraic groups over k, a homomorphism $f : V \to W$ is an *isogeny* over k if f is surjective and defined over k and $\dim(V) = \dim(W)$. If an isogeny between V and W exists we say V and W are *isogenous* over k.

Theorem 5.7. *If L/k is a cyclic extension of degree n, then*

(i) $\mathbb{T}_{L/k}$ *is an algebraic torus of dimension $\varphi(n)$ that splits over L;*

(ii) *letting $\mathrm{N}_{L/M}$ denote the usual norm map from L to M, then*

$$\mathbb{T}_{L/k}(k) \cong \{\alpha \in L^{\times} : \mathrm{N}_{L/M}(\alpha) = 1 \textit{ for all } k \subseteq M \subsetneq L\};$$

(iii) $\mathrm{Res}_{L/k}\mathbb{G}_m$ *is isogenous over k to $\oplus_M \mathbb{T}_{M/k}$, where M runs over all intermediate extensions $k \subseteq M \subseteq L$.*

Proof. By Lemma 5.4, $\mathbb{T}_{L/k}$ is isomorphic over L to $\mathbb{T}_G$, which by Lemma 5.6 is isomorphic over k to $\mathbb{G}_m^{\varphi(n)}$. This gives (i). Part (ii) follows from Lemma 5.1(ii) with $i = n$. For (iii), see pp. 60–61 of [36], or Theorem 5.2 of [24]. □

Recall that $G_{q,n}$ is the subgroup of $\mathbb{F}_{q^n}^{\times}$ of order $\Phi_n(q)$.

Proposition 5.8. (i) $\mathbb{T}_n(\mathbb{F}_q) \cong G_{q,n}$.

(ii) $G_{q,n} = \{\alpha \in \mathbb{F}_{q^n}^{\times} : \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^t}}(\alpha) = 1$ *for all $t|n$ with $t \neq n$*$\}$.

(iii) $\#\mathbb{T}_n(\mathbb{F}_q) = \Phi_n(q)$.

Proof. The cyclic group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is generated by the Frobenius automorphism $\alpha \mapsto \alpha^q$. Hence if t divides n, then $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^t}}(\alpha) = \alpha^{(q^n-1)/(q^t-1)}$ for all $\alpha \in \mathbb{F}_{q^n}$. Thus by Theorem 5.7(ii),

$$\begin{aligned}\mathbb{T}_n(\mathbb{F}_q) &\cong \{\alpha \in \mathbb{F}_{q^n}^{\times} : \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^t}}(\alpha) = 1 \text{ for all } t|n \text{ with } t \neq n\} \\ &= \{\alpha \in \mathbb{F}_{q^n}^{\times} : \alpha^c = 1\}\end{aligned}$$

where $c = \gcd\{(q^n-1)/(q^t-1) : t \mid n \text{ and } t \neq n\}$. By Lemma 5.5, $c = \Phi_n(q)$. Now (i) and (ii) follow from the definition of $G_{q,n}$, and (iii) follows from (i). □

6. Rationality and the $\mathbb{T}_n$-cryptosystem

We will recall what it means for a variety to be rational. This concept is useful since whenever an algebraic torus is rational, there exist compression and decompression maps. We give a mathematical explanation for why the torus $\mathbb{T}_6$ that underlies CEILIDH (and XTR) is rational, that proves the correctness of the algorithm in §3.1 and the formulas in §3.2. We also discuss generalizing CEILIDH and XTR.

Definition 6.1. A *rational* map between algebraic varieties is a function defined by quotients of polynomials that is defined almost everywhere (i.e., on a Zariski open set). A *birational isomorphism* between algebraic varieties is a rational map that has a rational inverse (the maps are inverses wherever both are defined). A d-dimensional variety over k is *rational* over k if it is birationally isomorphic over k to $\mathbb{A}^d$.

Note that birational isomorphisms of algebraic groups are not necessarily group isomorphisms. Further, rational maps are not necessarily functions — they might fail to be defined on a lower dimensional set.

If $\mathbb{T}_n$ is rational over k (i.e., birationally isomorphic over k to $\mathbb{A}^{\varphi(n)}$), then by Proposition 5.8(i), almost all elements of $G_{q,n}$ can be represented by $\varphi(n)$ elements of $\mathbb{F}_q$, and we obtain efficient "$\mathbb{T}_n$-cryptosystems" using the "torus-based" protocols given in the introduction.

The sets $G_{q,n}$ and $\mathbb{F}_q^{\varphi(n)}$ are of size approximately $q^{\varphi(n)}$. The "bad" sets where the maps f or j are not defined lie in algebraic subvarieties of dimension at most

$\varphi(n) - 1$, and therefore have at most $cq^{\varphi(n)-1}$ elements for some constant c. Thus the probability that an element lands in the bad set is at worst c/q, which will be small for large q. In any given case the bad sets might be even smaller. In the examples in §3, the maps j are defined on all of $\mathbb{F}_q^2$, and the maps f are defined at all but 2 elements of $G_{q,6}$.

Next we give the mathematics that proves that the algorithm of §3.1 is correct. Suppose L/k is a cyclic degree 6 extension, and F_2 (resp., F_3) are the quadratic (resp., cubic) extensions of k in L:

$$\begin{tikzcd}
& L \arrow[dl, dash] \arrow[dr, dash] & \\
F_2 \arrow[dr, dash, "2"'] & & F_3 \arrow[dl, dash, "3"] \\
& k &
\end{tikzcd}$$

The one-dimensional algebraic torus $\mathbb{T}_{L/F_3}$ is, by definition, the kernel of the norm map $N_{L/F_3} : L \to F_3$. Let $\mathbb{T} := \mathrm{Res}_{F_3/k}(\mathbb{T}_{L/F_3})$. Then $\mathbb{T}$ is an algebraic torus over k of dimension 3. As in §2, the torus $\mathbb{T}_{L/F_3}$, corresponding to the quadratic extension L/F_3, is rational over k (i.e., is birationally isomorphic over k to $\mathbb{A}^1$), and thus the torus $\mathbb{T}$ is rational over k (i.e., birationally isomorphic over k to $\mathbb{A}^3$). The two-dimensional torus $\mathbb{T}_{L/k}$ is the hypersurface cut out by the equation $\mathrm{N}_{L/F_2} = 1$ inside the torus $\mathbb{T}$, where N_{L/F_2} denotes the norm map from L to F_2. This hypersurface is defined by a quadratic equation that can be used to parametrize the hypersurface. When $k = \mathbb{F}_q$, then the above says that $\mathbb{T}_{6,q}$ is the 2-dimensional subvariety of the 3-dimensional torus $\mathrm{Res}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\mathbb{T}_{2,q^3})$ that is cut out by the equation $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} = 1$.

Fix $x \in F_2 - k$, so $F_2 = k(x)$, and choose a basis $\{\alpha_1, \alpha_2, \alpha_3\}$ of F_3 over k. Then $\{\alpha_1, \alpha_2, \alpha_3, x\alpha_1, x\alpha_2, x\alpha_3\}$ is a basis of L over k. Let $\sigma \in \mathrm{Gal}(L/k)$ be the element of order 2. Define a (one-to-one) map $j_0 : \mathbb{A}^3(k) \hookrightarrow L^\times$ by

$$j_0(u, v, w) = \frac{\gamma + x}{\gamma + \sigma(x)}$$

where $\gamma = u\alpha_1 + v\alpha_2 + w\alpha_3$. Then $N_{L/F_3}(j_0(\mathbf{u})) = 1$ for every $\mathbf{u} = (u, v, w)$. Let

$$U = \{\mathbf{u} \in \mathbb{A}^3 : N_{L/F_2}(j_0(\mathbf{u})) = 1\}.$$

By Definition 5.2, $j_0(\mathbf{u}) \in \mathbb{T}_{L/k}$ if and only if $u \in U$, so restricting j_0 to U gives a morphism

$$j_0 : U \to \mathbb{T}_{L/k} - \{1\}. \tag{6.1}$$

We will next define a birational map from $\mathbb{A}^2$ to U. A calculation in Mathematica shows that U is a hypersurface in $\mathbb{A}^3$ defined by a quadratic equation in u, v, w. Fix a point $\beta = (\beta_1, \beta_2, \beta_3) \in U(k)$. By adjusting the basis $\{\alpha_1, \alpha_2, \alpha_3\}$ if necessary, we can assume without loss of generality that the tangent plane at β to the surface U is the plane $u = \beta_1$. If $(a, b) \in k \times k$, then the intersection of U with the line $\beta + t(1, a, b)$ consists of two points, namely β and $g(a, b) = \beta + \frac{1}{h(a,b)}(1, a, b)$ for some $h(a, b) \in k[a, b]$. The map g defines a morphism

$$g : \mathbb{A}^2 - V(h) \to U - \{\beta\}, \tag{6.2}$$

so $j_0 \circ g$ defines a morphism

$$j : \mathbb{A}^2 - V(h) \to \mathbb{T}_{L/k} - \{1, j_0(\beta)\}. \tag{6.3}$$

For the inverse, write $t = c + dx \in \mathbb{T}_{L/k}(k) - \{1, j_0(\beta)\}$ with $c, d \in F_3$. One checks easily that $d \neq 0$, and if $\gamma = (1+c)/d$ then $\gamma/\sigma(\gamma) = t$. Write $(1+c)/d = u\alpha_1 + v\alpha_2 + w\alpha_3$ with $u_i \in k$, and define

$$f(t) = \left(\frac{v-\beta_2}{u-\beta_1}, \frac{w-\beta_3}{u-\beta_1}\right).$$

It follows from the discussion above that $f : \mathbb{T}_{L/k} - \{1, j_0(\beta)\} \xrightarrow{\sim} \mathbb{A}^2 - V(h)$ satisfies $f \circ j = \mathrm{id}$ and $j \circ f = \mathrm{id}$, so (6.1), (6.2), and (6.3) are isomorphisms and we obtain the following.

Theorem 6.2. *The above maps f and j induce inverse birational isomorphisms over k between $\mathbb{T}_{L/k}$ and $\mathbb{A}^2$.*

Note that in the examples in §3.2, the coefficients of the rational maps f and j are independent of q.

Remark 6.3. While the choice of j_0 on first glance might look obvious, in fact replacing j_0 by the seemingly just as obvious $j_1(u, v, w) = (\gamma x + 1)/(\gamma\sigma(x) + 1)$ leads to a hypersurface U defined by a cubic, rather than a quadratic, that does not seem to easily lead to a parametrization, and thus does not easily lead to efficient functions f and j. This is especially relevant when trying to generalize to the case of $n = 30$, where it is not at all clear how to correctly choose a generalization of j_0.

Arjen Lenstra [20] asked whether XTR can be generalized to obtain more security (see also [5]). The next interesting case after $n = 6$ (i.e., the first case where $n/\varphi(n) > 6/\varphi(6) = 3$) is when $n = 30$, where finding efficient generalizations of the XTR or CEILIDH compression/decompression maps is an open question. (However, see the next section for other techniques.) The following problem is discussed in §§5–6 of [36], and can be viewed as giving a general mathematical framework for the question of extending XTR and CEILIDH.

Voskresenskiĭ's Conjecture. *If L/k is a finite cyclic extension of fields, then $\mathbb{T}_{L/k}$ is rational over k; i.e., if $n = [L : k]$, there is a birational isomorphism over k*

$$\mathbb{T}_{L/k} \dashrightarrow \mathbb{A}^{\varphi(n)}.$$

By work of Klyachko and Voskresenskiĭ, this conjecture is known to hold when n is a product of at most two prime powers ([17]; see also §6.3 of [36]). In §3.2 and §2 above we gave explicit birational isomorphisms in some cases where $n = 6$ and 2. A $\mathbb{T}_n$-cryptosystem arises for every n for which Voskresenskiĭ's Conjecture is true over a finite field with efficiently computable birational maps.

When n is divisible by more than two distinct primes, Voskresenskiĭ's Conjecture is still an open question (despite a claim to the contrary in [37]). In particular, the conjecture is not known when $n = 30 = 2 \cdot 3 \cdot 5$.

7. Stable rationality

In Definition 7.1 below we give the definition of stable rationality. One reason that Voskresenskiĭ's Conjecture would be difficult to disprove is that the tori $\mathbb{T}_{L/k}$ (for L/k cyclic) are known to always be stably rational over k (see the Corollary on p. 61 of [36]), and it seems to be very difficult to prove the non-rationality of a stably rational torus. Although the stable rationality of $\mathbb{T}_{L/k}$ does not enable one to represent elements of $G_{q,n}$ in $\mathbb{F}_q^{\varphi(n)}$, it does allow one to represent elements of $G_{q,n}\times\mathbb{F}_q^r$ in $\mathbb{F}_q^{\varphi(n)+r}$ for a suitable r. In the language of the mathematical framework of this paper, the paper [8] of van Dijk and Woodruff can be viewed as a way to make clever use of the stable rationality of the algebraic tori $\mathbb{T}_n$ by encoding the message to be encrypted or signed in the extra affine piece $\mathbb{A}^r$.

Definition 7.1. A variety V over k is called *stably rational* over k if $V \times \mathbb{A}^r$ is rational over k for some $r \geq 0$ (i.e., $V \times \mathbb{A}^r$ is birationally isomorphic over k to $\mathbb{A}^s$ for some r and s).

In [8], van Dijk and Woodruff used the polynomial identity

$$\Phi_n(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)}$$

to obtain an "almost bijection" between $G_{q,n}\times\mathbb{F}_q^r$ and $\mathbb{F}_q^s$ where

$$r = \sum_{d|n,\mu(n/d)=-1} d, \qquad s = \sum_{d|n,\mu(n/d)=1} d.$$

In particular, this gave an "almost bijection" between $G_{q,30}\times\mathbb{F}_q^{32}$ and $\mathbb{F}_q^{40}$, from which they obtained public key cryptosystems. In [7], the rationality of $\mathbb{T}_6$, the ideas of [8], and the polynomial identity

$$\Phi_n(x)\prod_{i=2}^{r-1}\Phi_{p_1\cdots p_i}(x^{p_{i+2}\cdots p_r}) = \Phi_{p_1p_2}(x^{p_3\cdots p_r}),$$

where $n = p_1\cdots p_r$ is a product of $r \geq 2$ distinct primes, are used to obtain an "almost bijection" between $G_{q,n}\times\mathbb{F}_q^{n/3-\varphi(n)}$ and $\mathbb{F}_q^{n/3}$ if n is divisible by 6, giving a useful "almost bijection" between $G_{q,30}\times\mathbb{F}_q^2$ and $\mathbb{F}_q^{10}$. This improves the efficiency of the cryptosystems in [8].

It is an open question to find a birational isomorphism over $\mathbb{F}_q$ between $\mathbb{T}_{30}\times\mathbb{A}^1$ and $\mathbb{A}^9$ (or to prove its non-existence).

8. Security considerations

The map $\alpha \mapsto (\alpha^{(q^n-1)/\Phi_t(q)})_{t|n}$ gives a homomorphism

$$\mathbb{F}_{q^n}^\times \cong (\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m)(\mathbb{F}_q) \to \bigoplus_{t|n}\mathbb{T}_t(\mathbb{F}_q) \cong \bigoplus_{t|n} G_{q,t} = G_{q,n} \oplus \bigoplus_{\substack{t|n\\ t\neq n}} G_{q,t}$$

whose kernel and cokernel have orders whose prime divisors all divide n. We have $G_{q,t} \subseteq \mathbb{F}_{q^t}^\times$ for all t, so for $t|n$ and $t < n$ the elements of the subgroups $G_{q,t}$ lie in a strictly smaller field than $\mathbb{F}_{q^n}$, and are therefore vulnerable to attacks on the discrete logarithm problem in $\mathbb{F}_{q^t}^\times$, for $t|n$ with $t < n$. By Lemma 1 of [4], if $h \in G_{q,n}$ is an element of prime order not dividing n, then $\mathbb{F}_q(h) = \mathbb{F}_{q^n}$, i.e., almost none of the elements of $G_{q,n}$ lie in a proper subfield of $\mathbb{F}_{q^n}$.

Part (ii) of the following result shows that the finite cyclic group $G_{q,n} = \mathbb{T}_n(\mathbb{F}_q)$ is as cryptographically secure as $\mathbb{F}_{q^n}^\times$ against the known subexponential attacks on the discrete logarithm problem.

Proposition 8.1. *Suppose p is a prime, m and n are positive integers, $q = p^m$, and $(n,q) \neq (6,2)$. Then:*

(i) $\min\{k \in \mathbb{Z}^+ : \Phi_n(q)$ *divides* $p^k - 1\} = mn;$

(ii) *the smallest extension F of $\mathbb{F}_p$ such that $G_{q,n} \subseteq F^\times$ is $\mathbb{F}_{q^n}$.*

Proof. Let k be the smallest positive integer such that $\Phi_n(q)$ divides $p^k - 1$. Since $\Phi_n(q)$ divides $q^n - 1$, we have $k \le mn$. First suppose $mn > 2$. Since $(n, q) \neq (6, 2)$, it follows from a result of Zsigmondy (see Theorem 8.3, §IX of [14]) that $\Phi_{mn}(p)$ has a prime divisor ℓ that does not divide mn. By Lemma 4 of [27], mn is the order of p modulo ℓ. Since ℓ divides $\Phi_{mn}(p)$, which divides $\Phi_n(p^m)$, which divides $p^k - 1$, we have $mn \le k$. Thus $k = mn$, as desired. If $n = 1$, then clearly $k = m$. If $n = 2$ and $m = 1$, then clearly $k = 2$. This gives (i). Part (ii) follows from (i) since $|G_{q,n}| = \Phi_n(q)$ and $q^n = p^{mn}$. □

In a 2004 preprint, Kohel [18] suggests attacking cryptography on $G_{q,n}$ by using the fact that when n is odd and relatively prime to q, the tori $\mathbb{T}_n$ and $\mathbb{T}_{2n}$ are subschemes of the generalized Jacobian of a singular hyperelliptic curve $y^2 = cxf(x)^2$, where $f(x) \in \mathbb{F}_q[x]$ is irreducible of degree n. This seems like an interesting point of view that needs to be fleshed out and studied more fully.

Gaudry introduced a new probabilistic index calculus attack on the discrete logarithm problem for abelian varieties in his 2004 preprint [9]. Granger-Vercauteren [13] did an analogue of Gaudry's attack for the multiplicative group $\mathbb{G}_m$, which gives an attack on a subgroup of $\mathbb{F}_{q^6}^\times$ whose order is a 160-bit prime that is faster than Pollard ρ (which has complexity $O(\sqrt{q})$) when q is a sufficiently large fifth power (and therefore this attack applies also to subgroups of $\mathbb{F}_{q^{30}}^\times$), but has not been compared to index calculus attacks.

Joux et al. [15, 16] recently obtained efficient variants of the function field and number field sieve that bring the complexity of these attacks on the discrete log problem in $\mathbb{F}_{p^n}^\times$ to $L_{p^n}(1/3)$ for all finite fields $\mathbb{F}_{p^n}$, including the intermediate range where only $L_{p^n}(1/2)$ was previously known. They point out that the tori $\mathbb{T}_2$ and $\mathbb{T}_6$, which underlie LUC, XTR, and CEILIDH, appear to be safe from such attacks, as are cryptosystems based on the difficulty of the discrete log problem in $\mathbb{T}_{30}$ over $\mathbb{F}_p$ for 64-bit primes p, but not for 32-bit p.

To summarize, CEILIDH and XTR seem to be safe from known attacks, if one takes the parameter q to be a prime of at least 170 ($\approx \frac{1024}{6}$) bits. For $\mathbb{T}_{30}$-cryptosystems, Joux recommends taking 64-bit primes q to avoid all known attacks.

9. Interpreting discrete log cryptosystems in terms of quotients of tori

We will show that the XTR, Gong-Harn, and Lucas-based cryptosystems are based on the rationality of certain quotients of algebraic tori by the action of certain (finite) symmetric groups. In particular, Theorems 9.7 and 9.8, and the definition of the maps $\tilde{\sigma}_{i,F}$ in (5.2), show that the Lucas-based, Gong-Harn, and XTR cryptosystems are "based on" the quotient varieties $\mathbb{T}_2/S_2$, $\mathbb{T}_3/S_3$, and $\mathbb{T}_6/S_3$, respectively, and the conjectural "Looking beyond XTR" systems in [4] would be based on the quotient varieties $\mathbb{T}_{30}/(S_3 \times S_5)$ or $\mathbb{T}_{30}/(S_2 \times S_3 \times S_5)$, where S_r denotes the symmetric group on r letters, and the actions of these symmetric groups on $\mathbb{T}_n$ are defined in §9.1 below. Theorem 9.11 shows that $\mathbb{T}_2/S_2$, $\mathbb{T}_3/S_3$, and $\mathbb{T}_6/S_3$ are rational varieties (and that is why the cryptosystems have efficient compression).

More precisely, for XTR, information exchanged corresponds to a $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$-conjugacy class of $G_{q,6}$, which by Theorems 9.7 and 9.8 corresponds to an element of $\mathbb{T}_6/S_3$. The cryptosystem XTR takes advantage of the fact that $\mathbb{T}_6/S_3$ is rational, and the trace map from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^2}$ induces a morphism and birational isomorphism $\mathbb{T}_6/S_3 \to \mathbb{A}^2(= \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\mathbb{A}^1)$ over $\mathbb{F}_p$ as in Theorem 9.11, and therefore gives a compact representation of $\mathbb{T}_6/S_3$ (i.e., an element of $(\mathbb{T}_6/S_3)(\mathbb{F}_q)$ is represented by two elements of $\mathbb{F}_q$). The set of equivalence classes $\mathbb{T}_6/S_3$ is not a group, because multiplication in $\mathbb{T}_6$ does not send S_3-orbits to S_3-orbits. This explains why XTR does not have a straightforward way to multiply. However, exponentiation in $\mathbb{T}_6$ does send S_3-orbit to S_3-orbits, and it induces a well-defined exponentiation in $\mathbb{T}_6/S_3$, and therefore in the set $\Lambda(\mathbb{F}_q, \mathbb{F}_{q^2}, \mathbb{F}_{q^6})$ of XTR traces (defined below).

Similarly for Lucas-based cryptosystems, the elements being exchanged correspond to elements of $\mathbb{T}_2/S_2$, and the trace map from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ induces a morphism and birational isomorphism $\mathbb{T}_2/S_2 \to \mathbb{A}^1$ over $\mathbb{F}_p$.

From now on, L/k is a finite cyclic extension, $n := [L : k]$ is square-free,

$$k \subseteq F \subseteq L, \quad G := \mathrm{Gal}(L/k), \quad H := \mathrm{Gal}(L/F), \quad e := |H|, \quad d := n/e.$$

We define an algebraic variety $\mathcal{X}_F$ that underlies XTR, Gong-Harn, and the Lucas-based cryptosystems (with $k = \mathbb{F}_q$ and $(F, L) = (\mathbb{F}_{q^2}, \mathbb{F}_{q^6})$, $(\mathbb{F}_q, \mathbb{F}_{q^3})$, and $(F_q, \mathbb{F}_{q^2})$, respectively). Theorem 9.11 below shows that in those cases, $\mathcal{X}_F$ is rational. Theorem 9.11 can be viewed as a rephrasing of a result in [5]. Phrasing Theorem 9.11 in terms of quotients of algebraic tori and birational isomorphisms makes precise the underlying mathematics. This was useful to us both in helping us find counterexamples in more general cases (see §10), and in helping to see what ideas might be necessary to obtain correct and useful generalizations.

When $(k, F, L) = (\mathbb{F}_q, \mathbb{F}_{q^n}, \mathbb{F}_{q^n})$, then $(n, d, e) = (n, n, 1)$ and the varieties $\mathcal{X}_F$ and $\mathbb{T}_n/S_e$ are $\mathbb{T}_n$ itself, corresponding to the $\mathbb{T}_n$-cryptosystems ($\mathbb{T}_2$ is the case $(n, d, e) = (2, 2, 1)$ and CEILIDH is the case $(6, 6, 1)$). An effective proof of Voskresenskiĭ's Conjecture would provide a birational isomorphism between $\mathbb{T}_n$ and $\mathbb{A}^{\varphi(n)}$.

Because the details become more technical from this point on, we recommend that the casual reader ignore the proofs, lemmas, and propositions, and concentrate on the definitions, theorem statements, and examples.

9.1. **Group actions on tori.** We next define actions of symmetric groups on the tori $\mathbb{T}_{L/k}$. If Γ is a finite set, let Σ_Γ denote the group of permutations of Γ. As an abstract group, Σ_G (resp., Σ_H) is the symmetric group S_n (resp., S_e). Since n is square-free, there is a unique subgroup $J \subseteq G$ such that $G = H \times J$. This decomposition induces inclusions $\Sigma_H \subseteq \Sigma_G \subseteq \mathrm{Aut}_k(\mathbb{A}^G)$ and $\Sigma_H \subseteq \Sigma_G \subseteq \mathrm{Aut}_k(\mathbb{G}_m^G)$. More concretely, the action of $\pi \in \Sigma_H = S_e$ on $\mathbb{A}^G = \mathbb{A}^n$ is $(x_i)_{i\in\mathbb{Z}/n\mathbb{Z}} \mapsto (x_{\pi^{-1}(i)})_{i\in\mathbb{Z}/n\mathbb{Z}}$ where S_e acts on $G = \mathbb{Z}/n\mathbb{Z}$ via the decomposition $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$, with trivial action on the second factor. See also Examples 9.3 and 9.4 below. We have

$$\mathbb{A}^n = \mathbb{A}^G \underset{L}{\cong} \mathrm{Res}_{L/k}\mathbb{A}^1 \supset \mathrm{Res}_{L/k}\mathbb{G}_m \supset \mathbb{T}_{L/k}.$$

The action of Σ_H on $\mathrm{Res}_{L/k}\mathbb{A}^1 \cong \mathbb{A}^G$ sends $\mathrm{Res}_{L/k}\mathbb{G}_m$ to $\mathrm{Res}_{L/k}\mathbb{G}_m$. The images of Σ_H in $\mathrm{Aut}_L(\mathrm{Res}_{L/k}\mathbb{A}^1) \cong \mathrm{Aut}_L(\mathbb{A}^G)$ and in $\mathrm{Aut}_L(\mathrm{Res}_{L/k}\mathbb{G}_m) \cong \mathrm{Aut}_L(\mathbb{G}_m^G)$ are stable under the action of $\mathrm{Gal}(L/k)$ (by Corollary 1.7(i) of [24] with $\mathcal{I} = \mathcal{J} = \mathbb{Z}[G]$ and $V = \mathbb{G}_a = \mathbb{A}^1$ and $V = \mathbb{G}_m$ and Proposition 4.1 of [24] with $\mathcal{O} = \mathbb{Z}$ and $V = \mathbb{G}_a$ and $\mathbb{G}_m$), and it follows that the quotient varieties $\mathbb{A}^G/\Sigma_H$, $(\mathrm{Res}_{L/k}\mathbb{A}^1)/\Sigma_H$, and $(\mathrm{Res}_{L/k}\mathbb{G}_m)/\Sigma_H$ are all defined over k.

Recall the maps $\tilde{\sigma}_{i,F}$ from (5.2). We will make repeated use of the following lemma.

Lemma 9.1 (Proposition 3.2 of [29])**.** *The maps $\tilde{\sigma}_{i,F}$ for $1 \leq i \leq e$ factor through $(\mathrm{Res}_{L/k}\mathbb{A}^1)/\Sigma_H$ and induce a commutative diagram*

$$\begin{tikzcd}
\mathrm{Res}_{L/k}\mathbb{G}_m \arrow[r, two heads] \arrow[drr, "\oplus_{i=1}^{e}\tilde{\sigma}_{i,F}"'] & (\mathrm{Res}_{L/k}\mathbb{G}_m)/\Sigma_H \arrow[r, hook] & (\mathrm{Res}_{L/k}\mathbb{A}^1)/\Sigma_H \arrow[d, "\oplus_{i=1}^{e}\tilde{\sigma}_{i,F}"] \\
 & & (\mathrm{Res}_{F/k}\mathbb{A}^1)^e
\end{tikzcd}$$

where the right-hand vertical map is an isomorphism over k.

If e is divisible by two or more primes, then the action of Σ_H on $\mathrm{Res}_{L/k}\mathbb{G}_m$ does not send $\mathbb{T}_{L/k}$ to itself. We illustrate this concretely in Examples 9.3 and 9.4 below. The following result, which is used in Theorem 9.7 below, tells us which elements of Σ_G do send $\mathbb{T}_{L/k}$ to itself. In particular, Lemma 9.2 shows that if p is a prime divisor of n, then the action of S_p on $\mathbb{A}^n$ $(= \mathbb{A}^G)$ does take $\mathbb{T}_n$ to itself.

Write $G = \prod G_i$, with the G_i cyclic groups of (distinct) prime order.

Lemma 9.2. *If $\sigma \in \Sigma_G$, then $\sigma(\mathbb{T}_{L/k}) \subseteq \mathbb{T}_{L/k}$ if and only if $\sigma \in \prod_i \Sigma_{G_i}$.*

Proof. This follows from Theorem 7.3 of [24]; see also Lemma 3.5 of [29]. □

The following examples give concrete realizations of the tori $\mathbb{T}_n$, that allow explicit computation, and show how the symmetric groups act.

Example 9.3. Let $n = e = 6$ and $d = 1$, and let

$$\Gamma = \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \supset \Omega = (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \cong (\mathbb{Z}/6\mathbb{Z})^\times.$$

By Definition 5.3, $\mathbb{T}_\Gamma \subset \mathbb{G}_m^\Gamma \xrightarrow{\sim} \mathbb{G}_m^6$ can be identified with the 2×3 matrices over $\mathbb{G}_m$ for which each row and column product is 1. By Lemma 5.4 we have $\mathbb{T}_6 \cong \mathbb{T}_\Gamma$ over $\mathbb{F}_{q^6}$, and by Lemma 5.6 we have $\mathbb{G}_m^2 \cong \mathbb{G}_m^\Omega \xrightarrow{\sim} \mathbb{T}_\Gamma \subset \mathbb{G}_m^\Gamma \xrightarrow{\sim} \mathbb{G}_m^6$ via

$$(x_1, x_2) \mapsto \begin{pmatrix} x_1 & x_2 & (x_1x_2)^{-1} \\ x_1^{-1} & x_2^{-1} & x_1x_2 \end{pmatrix}.$$

The action of S_2 interchanges the rows, and the action of S_3 permutes the columns of the 2×3 matrix. However, the action of S_6 on $\mathbb{G}_m^\Gamma = \mathbb{G}_m^6$ does not take $\mathbb{T}_\Gamma$ into itself (i.e., there are permutations of the 6 matrix entries that do not give a matrix of the same form). Thus, the action of S_6 does not take $\mathbb{T}_6$ into itself.

Example 9.4. More generally, if $n = pq$ and

$$\Gamma = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \supset \Omega = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

then by Definition 5.3, $\mathbb{T}_\Gamma \subset \mathbb{G}_m^\Gamma \xrightarrow{\sim} \mathbb{G}_m^n$ can be identified with the $p \times q$ matrices over $\mathbb{G}_m$ for which each row and column product is 1. By Lemma 5.4 we have $\mathbb{T}_n \cong \mathbb{T}_\Gamma$ over $\mathbb{F}_{q^n}$, and by Lemma 5.6 we have $\mathbb{G}_m^{(p-1)(q-1)} \cong \mathbb{G}_m^\Omega \xrightarrow{\sim} \mathbb{T}_\Gamma \subset \mathbb{G}_m^\Gamma \xrightarrow{\sim} \mathbb{G}_m^n$ via $(x_{i,j})_{1 \leq i \leq p-1, 1 \leq j \leq q-1} \mapsto$

$$\begin{pmatrix}
x_{1,1} & x_{1,2} & \cdots & x_{1,q-1} & (\prod_{\ell=1}^{q-1} x_{1,\ell})^{-1} \\
x_{2,1} & x_{2,2} & \cdots & x_{2,q-1} & (\prod_{\ell=1}^{q-1} x_{2,\ell})^{-1} \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
x_{p-1,1} & x_{p-1,2} & \cdots & x_{p-1,q-1} & (\prod_{\ell=1}^{q-1} x_{p-1,\ell})^{-1} \\
(\prod_{k=1}^{p-1} x_{k,1})^{-1} & (\prod_{k=1}^{p-1} x_{k,2})^{-1} & \cdots & (\prod_{k=1}^{p-1} x_{k,q-1})^{-1} & \prod_{\ell=1}^{q-1}\prod_{k=1}^{p-1} x_{k,\ell}
\end{pmatrix}.$$

Now S_p acts on $\mathbb{T}_\Gamma$ by permuting the rows of the matrix, and S_q acts by permuting the columns. However, the action of S_n on $\mathbb{G}_m^\Gamma = \mathbb{G}_m^n$ does not take $\mathbb{T}_\Gamma$ into itself, so does not take $\mathbb{T}_n$ into itself. More generally, taking $n = p_1p_2\cdots p_r$, one can represent $\mathbb{T}_\Gamma$ via a $p_1 \times \cdots \times p_r$ multi-dimensional matrix. The proof of Lemma 5.6 can be viewed as a coordinate-free version of this representation.

Definition 9.5. Let $\mathcal{X}_F$ denote the image of $\mathbb{T}_{L/k}$ in $(\mathrm{Res}_{L/k}\mathbb{G}_m)/\Sigma_H$. Let $\mathbb{X}_H$ be the image of $\mathbb{T}_G$ under the map $\mathbb{G}_m^G \twoheadrightarrow \mathbb{G}_m^G/\Sigma_H$, with Σ_H acting on $\mathbb{G}_m^G$ by permuting the factors as above.

It follows from Lemma 5.6 that $\mathbb{T}_G$ and $\mathbb{T}_{L/k}$, and thus $\mathbb{X}_H$ and $\mathcal{X}_F$, are absolutely irreducible.

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

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

More concretely, letting $e = p_1 \cdots p_r$ be the prime factorization of the squarefree positive integer e, and letting $S'_e := S_{p_1} \times \cdots \times S_{p_r}$, then $\Sigma'_H = S'_e$. Note that when e is prime, then $S'_e = \Sigma'_H = \Sigma_H = S_e$. By Lemma 9.2, $\Sigma'_H \subseteq \mathrm{Aut}_{k_s}(\mathbb{T}_{L/k})$. Clearly the map $\mathbb{T}_{L/k} \to \mathcal{X}_F$ factors through $\mathbb{T}_{L/k}/\Sigma'_H$. When $k = \mathbb{F}_q$, we will denote $\mathbb{T}_{L/k}/\Sigma'_H$ by $\mathbb{T}_n/S'_e$.

The next lemma is used to prove Theorem 9.7.

Lemma 9.6. *Suppose Y is an affine variety defined over k, and X is an irreducible affine subvariety of Y defined over k. Suppose $\mathrm{Aut}_{k_s}(Y)$ contains a finite group Σ, and let $\Sigma_0 = \{\gamma \in \Sigma : \gamma(X) \subseteq X\}$. Then the natural map $X/\Sigma_0 \to Y/\Sigma$ induces a birational isomorphism over k from X/Σ_0 to its image in Y/Σ.*

Proof. If $g \in \Sigma$, let $U_g = X - g^{-1}(X)$. Let $U = \cap_{g\in\Sigma-\Sigma_0} U_g$. Then U is a non-empty Zariski-open subset of X. By the definition of U, the natural map $X/\Sigma_0 \to Y/\Sigma$ is injective on the image of U in X/Σ_0, proving the desired result. □

Theorem 9.7. *The natural map $\mathbb{T}_{L/k}/\Sigma'_H \to \mathcal{X}_F$ is a birational isomorphism over k.*

Proof. By Lemmas 9.6 and 9.2, the natural map $\mathbb{T}_{L/k}/\Sigma'_H \to (\mathrm{Res}_{L/k}\mathbb{G}_m)/\Sigma_H$ induces a birational isomorphism to $\mathcal{X}_F$. □

The next result will be used to prove Theorems 10.5 and 10.9.

Theorem 9.8. *Fix an isomorphism $(\phi_1, \ldots, \phi_d) : \mathrm{Res}_{F/k}\mathbb{A}^1 \xrightarrow{\sim} \mathbb{A}^d$ over k (for example, by fixing a k-basis of F). Then 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 Lemma 9.1, the function field $k((\mathrm{Res}_{L/k}\mathbb{A}^1)/\Sigma_H)$ is generated by the maps $\phi_j \circ \tilde{\sigma}_{i,F}$. Since $\mathcal{X}_F$ is a subvariety of $(\mathrm{Res}_{L/k}\mathbb{A}^1)/\Sigma_H$, the restrictions of those maps to $\mathcal{X}_F$ generate $k(\mathcal{X}_F)$. □

Remark 9.9. Let $G_{L/k} \subseteq L^\times$ be the image of $\mathbb{T}_{L/k}(k)$ under the map of Theorem 5.7(ii) and let $\rho : \mathbb{T}_{L/k} \to \mathcal{X}_F$ be the natural map. Then Theorem 9.8 (combined with Lemma 5.1) shows that ρ induces a one-to-one correspondence between the $\mathrm{Gal}(L/F)$-orbits of $G_{L/k}$ and the subset $\rho(\mathbb{T}_{L/k}(k))$ of $\mathcal{X}_F(k)$. In particular, the $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})$-orbits of $G_{q,n}$ are in bijection with the image of $\mathbb{T}_n(\mathbb{F}_q)$ in $\mathcal{X}_{\mathbb{F}_{q^d}}(\mathbb{F}_q)$. When $n = 6$, $k = \mathbb{F}_q$, and $F = \mathbb{F}_{q^2}$, the map $\mathrm{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_q}\mathbb{G}_m \to (\mathrm{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_q}\mathbb{G}_m)/S_3$

induces $\rho : \mathbb{T}_6 \to \mathbb{T}_6/S_3 = \mathcal{X}_F$, a (generically) 6-to-1 map. However, for the induced map on $\mathbb{F}_q$-points $\rho : \mathbb{T}_6(\mathbb{F}_q) \to \mathcal{X}_F(\mathbb{F}_q)$, almost all non-empty fibers have size 3, corresponding to $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$-orbits in $G_{q,6}$.

9.2. **Interpreting XTR, Gong-Harn, and Lucas-based systems.**

Theorem 9.11 below can be viewed as a rephrasing, in the language of this paper, of a result in §5 of [5] (see also Proposition 1 of [4]) that says that the minimal polynomial over $\mathbb{F}_{q^d}$ of an element of $G_{p,n}$ can be represented using $\varphi(n)\log_2(p)$ bits, if $d = 1$ or 2 and e is prime.

With notation k, L, F, G, H, n, e, and d as before, let $u = \lceil \varphi(n)/d \rceil$. There is a commutative diagram

$$\begin{tikzcd}
\mathbb{T}_{L/k} \arrow[r, phantom, "\subseteq"] \arrow[d] & \mathrm{Res}_{L/k}\mathbb{G}_m \arrow[r, hook] & \mathrm{Res}_{L/k}\mathbb{A}^1 \arrow[r, "\sim"] \arrow[dl] \arrow[d, "\oplus_{i=1}^{u}\tilde{\sigma}_{i,F}"] & \mathbb{A}^G \arrow[d, "\oplus_{i=1}^{u} s_i"] \\
\mathbb{T}_{L/k}/\Sigma'_H \arrow[r] & (\mathrm{Res}_{L/k}\mathbb{A}^1)/\Sigma'_H \arrow[r] & (\mathrm{Res}_{F/k}\mathbb{A}^1)^u \arrow[r, "\sim"] & (\mathbb{A}^{G/H})^u
\end{tikzcd}$$

where the top and bottom isomorphisms are defined over L and F, respectively, and the functions s_i were defined in Definition 5.3. Let

$$\lambda_F := (\tilde{\sigma}_{1,F}, \ldots, \tilde{\sigma}_{u,F}) : \mathbb{T}_{L/k}/\Sigma'_H \to (\mathrm{Res}_{F/k}\mathbb{A}^1)^u \tag{9.1}$$

denote the composition in the bottom row, and let

$$\Lambda(k, F, L) := \{\lambda_F(\alpha) : \alpha \in \mathbb{T}_{L/k}(k)\} \subseteq (\mathrm{Res}_{F/k}\mathbb{A}^1)^u(k) \cong F^u.$$

Note that $\Lambda(\mathbb{F}_q, \mathbb{F}_{q^d}, \mathbb{F}_{q^n}) = \{(\sigma_1(\alpha), \ldots, \sigma_u(\alpha)) : \alpha \in G_{q,n}\} \subseteq (\mathbb{F}_{q^d})^{\lceil \varphi(n)/d \rceil}$ where $\sigma_i(\alpha)$ is the i-th symmetric function on $\{\alpha^\gamma : \gamma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})\}$. The Lucas-based and XTR cryptosystems correspond to the cases $(n, d, e) = (2, 1, 2)$ and $(6, 2, 3)$, respectively. In these two cases, λ_F is essentially the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^d}$, and $\Lambda(\mathbb{F}_q, \mathbb{F}_{q^d}, \mathbb{F}_{q^n})$ is the set of traces used in the Lucas-based systems and XTR, respectively. Further, when $(n, d, e) = (3, 1, 3)$, then $\Lambda(\mathbb{F}_q, \mathbb{F}_{q^d}, \mathbb{F}_{q^n})$ is the set of values that occur in the Gong-Harn cryptosystem. In Theorem 10.5 below we will show that a conjecture in [4] on how to generalize XTR would imply that λ_F is always a birational isomorphism.

The following result, which will be used to prove Theorem 10.9, gives equivalent conditions for λ_F to be a birational isomorphism.

Proposition 9.10. (i) *The isomorphism $\mathbb{T}_{L/k} \xrightarrow{\sim} \mathbb{T}_G$ of Lemma 5.4 induces an isomorphism $\mathcal{X}_F \xrightarrow{\sim} \mathbb{X}_H$ defined over F.*

(ii) *Lemma 9.1 remains true when $\mathrm{Res}_{L/k}\mathbb{G}_m$, $\mathrm{Res}_{L/k}\mathbb{A}^1$, and $\tilde{\sigma}_{i,F}$ are replaced by $\mathbb{G}_m^G$, $\mathbb{A}^G$, and s_i, respectively, where the s_i were defined in Definition 5.3.*

(iii) *There is a commutative diagram, with maps defined over F,*

$$\begin{tikzcd}
\mathcal{X}_F \arrow[r, "\sim"] \arrow[d, "\oplus_{i=1}^{e}\tilde{\sigma}_{i,F}"'] & \mathbb{X}_H \arrow[d, "\oplus_{i=1}^{e} s_i"] \\
(\mathrm{Res}_{F/k}\mathbb{A}^1)^e \arrow[r, "\sim"] & (\mathbb{A}^{G/H})^e
\end{tikzcd}$$

where the top map is the isomorphism of (i), the bottom isomorphism is given by the e-th power of (4.3) *(with $V = \mathbb{A}^1$), and the left map is induced by the map of Lemma 9.1.*

(iv) *There is a commutative diagram*

$$\begin{tikzcd}
\mathbb{T}_{L/k}/\Sigma'_H \arrow[r] \arrow[dr, "\lambda_F"'] & \mathcal{X}_F \arrow[r, "\sim"] \arrow[d, "\oplus_{i=1}^{u}\tilde{\sigma}_{i,F}"] & \mathbb{X}_H \arrow[d, "\oplus_{i=1}^{u}s_i"] \\
& (\mathrm{Res}_{F/k}\mathbb{A}^1)^u \arrow[r, "\sim"] & (\mathbb{A}^{G/H})^u
\end{tikzcd}$$

where the top left map is the birational isomorphism of Theorem 9.7, the top right map is from (i), and the bottom map is the u-th power of (4.3).

(v) *The following are equivalent:*

(a) λ_F *is a birational isomorphism,*

(b) $\oplus_{i=1}^{u}\tilde{\sigma}_{i,F}$ *is a birational isomorphism,*

(c) $\oplus_{i=1}^{u}s_i$ *is a birational isomorphism.*

Proof. Part (i) follows from Lemma 5.4, (4.3), and the definitions of $\mathcal{X}_F$ and $\mathbb{X}_H$. Part (ii) follows from (4.3). Part (iii) now follows immediately, while (iv) follows from Theorem 9.7 and the definition of λ_F. Part (v) follows from (iv) and the fact that being a birational isomorphism is invariant under change of base field. □

Theorem 9.11. *Suppose e is prime, and $d = 1$ or 2. Then λ_F is a birational isomorphism and injective morphism*

$$\mathbb{T}_{L/k}/\Sigma'_H \hookrightarrow (\mathrm{Res}_{F/k}\mathbb{A}^1)^{\varphi(n)/d} \quad (\cong \mathbb{A}^{\varphi(n)})$$

such that $\Lambda(k, F, L)$ is the image of the composition

$$\mathbb{T}_{L/k}(k) \longrightarrow (\mathbb{T}_{L/k}/\Sigma'_H)(k) \hookrightarrow (\mathrm{Res}_{F/k}\mathbb{A}^1)^{\varphi(n)/d}(k) \cong F^{\varphi(n)/d}.$$

In this way, $\Lambda(k, F, L)$ can be naturally identified with the image of $\mathbb{T}_{L/k}(k)$ in $(\mathbb{T}_{L/k}/\Sigma'_H)(k)$.

Proof. By definition, $\Lambda(k, F, L)$ is the image of the composition

$$\mathbb{T}_{L/k}(k) \to (\mathbb{T}_{L/k}/\Sigma'_H)(k) \to (\mathrm{Res}_{F/k}\mathbb{A}^1)^u(k) \cong F^u.$$

When d divides $\varphi(n)$, then $\mathbb{T}_{L/k}$ and $(\mathrm{Res}_{F/k}\mathbb{A}^1)^u$ are both $\varphi(n)$-dimensional varieties over k. Thus to prove the theorem we need only show that when $d = 1$ or 2 and e is prime then λ_F is injective. By Lemma 9.1,

$$(\tilde{\sigma}_{1,F}, \dots, \tilde{\sigma}_{e,F}) : (\mathrm{Res}_{F/k}\mathbb{A}^1)/\Sigma_H \xrightarrow{\sim} (\mathrm{Res}_{F/k}\mathbb{A}^1)^e. \tag{9.2}$$

Suppose e is prime. Then $\Sigma'_H = \Sigma_H$, and $\mathbb{T}_{L/k}/\Sigma'_H$ is a subvariety of $\mathrm{Res}_{F/k}\mathbb{A}^1/\Sigma_H$.

Suppose first that $d = 1$. By the definitions of $\mathbb{T}_{L/k}$ and $\tilde{\sigma}_{e,F}$, we have $\tilde{\sigma}_{e,F} = \mathrm{N}_{L/F,k} = 1$ on $\mathbb{T}_{L/k}$. Thus $(\tilde{\sigma}_{1,F}, \dots, \tilde{\sigma}_{e,F}) = (\lambda_F, 1)$ on $\mathbb{T}_{L/k}$. The injectivity of λ_F follows from the injectivity of (9.2).

Now suppose that $d = 2$ (so e is an odd prime). Let M denote the degree e extension of k in L and let ρ denote the element of order 2 in G. We have $\mathrm{N}_{L/M,k}(g) = g \cdot g^\rho$ and $\mathrm{N}_{L/M,k} = 1$ on $\mathbb{T}_{L/k}$. Thus ρ is the same as inversion on $\mathbb{T}_{L/k}$. By definition,

$$\tilde{\sigma}_{i,F}(g_1, \dots, g_e) = \sum_{\substack{S \subseteq \{1,\dots,e\} \\ |S| = i}} \prod_{j \in S} g_j, \qquad \frac{\tilde{\sigma}_{e-i,F}}{\tilde{\sigma}_{e,F}}(g_1, \dots, g_e) = \sum_{\substack{S \subseteq \{1,\dots,e\} \\ |S| = i}} \prod_{j \in S} g_j^{-1}.$$

Since ρ is inversion on $\mathbb{T}_{L/k}$ and $\tilde{\sigma}_{e,F} = 1$ on $\mathbb{T}_{L/k}$, we have $\tilde{\sigma}_{i,F}^{\rho} = \tilde{\sigma}_{e-i,F}/\tilde{\sigma}_{e,F} = \tilde{\sigma}_{e-i,F}$ on $\mathbb{T}_{L/k}$. Thus

$$(\tilde{\sigma}_{1,F}, \ldots, \tilde{\sigma}_{e,F}) = (\tilde{\sigma}_{1,F}, \ldots, \tilde{\sigma}_{(e-1)/2,F}, \tilde{\sigma}^{\rho}_{(e-1)/2,F}, \ldots, \tilde{\sigma}^{\rho}_{1,F}, 1)$$

on $\mathbb{T}_{L/k}$. Since $\lambda_F = (\tilde{\sigma}_{1,F}, \ldots, \tilde{\sigma}_{(e-1)/2,F})$, the injectivity of λ_F again follows from (9.2). □

10. "Looking beyond XTR"

Arjen Lenstra [20] asked if one can use $n = 30$ to do better than XTR. The Bosma-Hutton-Verheul paper "Looking beyond XTR" [4], building on a conjecture in [5], asked whether, for $n > 6$, some set of elementary symmetric polynomials can be used in place of the trace. In particular, [4] asked whether one can recover the values of all the elementary symmetric polynomials (i.e., the entire characteristic polynomial) for $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})$ from the first $\lceil \varphi(n)/d \rceil$ of them (this was already answered in the affirmative in [5] when $(d, n/d) = (1, \ell)$ or $(2, \ell)$ with ℓ prime). If this were true, one could use the first $\lceil \varphi(n)/d \rceil$ elementary symmetric polynomials on the set of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})$-conjugates of an element $h \in G_{q,n}$ to compress h, representing it via $\varphi(n)$ elements of $\mathbb{F}_q$.

Of the four conjectures stated in [4], the two "strong" conjectures were disproved there. In Theorem 10.1 and Corollary 10.2 below we disprove the two remaining conjectures (Conjectures 1 and 3 of [4], which were also called (d, e)-**BPV** and n-**BPV** in [4]). In fact we can do better. We have constructed examples that show not only that the conjectures are false, but also that weakening the conjectures does not help. In particular, when $n = 30$ and $p = 7$, we can show that:

- for $d = 1$, no 8 ($= \varphi(n)/d$) elementary symmetric polynomials determine *any* of the remaining ones, except for those determined by the symmetry of the characteristic polynomial,
- for $d = 1$, no 10 elementary symmetric polynomials determine *all* of them;
- for $d = 2$, no 4 ($= \varphi(n)/d$) elementary symmetric polynomials determine all of them.

Rationality of the varieties $\mathbb{T}_n/S'_n$ (or more generally the varieties $\mathbb{T}_n/S'_e$) would imply the conjecture in [5] that characteristic polynomials (i.e., Galois-conjugacy classes) of elements of $G_{p,n}$ can be represented using $\varphi(n)\log_2(p)$ bits. We see in Theorem 10.5 below that the conjectures in [4] would imply the stronger statement (when d divides $\varphi(n)$) that the map $\lambda_{\mathbb{F}_{q^d}}$ of (9.1) is a (morphism and) birational isomorphism

$$\mathbb{T}_n/S'_e \to (\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q} \mathbb{A}^1)^{\varphi(n)/d} \cong \mathbb{A}^{\varphi(n)}.$$

Theorem 9.11 above showed this is true when e is a prime and $d = 1$ or 2. In particular, it is true when (d, e) is $(1, 1)$ (Diffie-Hellman), $(1, 2)$ (Lucas-based systems), $(1, 3)$ (Gong-Harn), and $(2, 3)$ (XTR). Theorem 10.9 below shows that this is false for $(d, e) = (1, 30)$ and $(2, 15)$ in all but at most finitely many characteristics p, i.e., the first eight elementary symmetric polynomials do not induce a birational isomorphism $\mathbb{T}_{30}/S'_{30} = \mathbb{T}_{30}/(S_2 \times S_3 \times S_5) \to \mathbb{A}^8$ over $\mathbb{F}_p$, and the first four elementary symmetric polynomials on the $\mathrm{Gal}(\mathbb{F}_{p^{30}}/\mathbb{F}_{p^2})$-conjugates of an element in $\mathbb{T}_{30}$ do not induce a birational isomorphism $\mathbb{T}_{30}/S'_{15} = \mathbb{T}_{30}/(S_3 \times S_5) \to (\mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p} \mathbb{A}^1)^4 \cong \mathbb{A}^8$ over $\mathbb{F}_p$. In summary, elementary symmetric polynomials are not the correct functions to use.

Fix an integer $n > 1$, a prime p, and a factorization $n = de$ with $e > 1$. For $h \in G_{p,n}$, let $P_h^{(d)}$ be the characteristic polynomial of h over $\mathbb{F}_{p^d}$, and define functions $a_j : G_{p,n} \to \mathbb{F}_{p^d}$ by

$$P_h^{(d)}(X) = X^e + a_{e-1}(h)X^{e-1} + \cdots + a_1(h)X + a_0(h).$$

Then $a_0(h) = (-1)^e$. If n is even then

$$a_j(h) = (-1)^e (a_{e-j}(h))^{p^{n/2}} \tag{10.1}$$

for all $j \in \{1, \ldots, e-1\}$ (see for example Theorem 1 of [4] or the proof of Theorem 9.11 above). Let

$$S_{p,n} = \{h \in G_{p,n} : \mathbb{F}_p(h) = \mathbb{F}_{p^n}\}.$$

Next we state Conjectures 1 and 3 (also called (d,e)-**BPV** and n-**BPV**, resp.) of [4].

Conjecture (d,e)**-BPV.** *Let $n = de$ with $e > 1$. Then $\lceil \varphi(n)/d \rceil$ is the smallest positive integer u for which there are polynomials*

$$Q_j \in \mathbb{Z}[X_1^{(0)}, \ldots, X_1^{(d-1)}, X_2^{(0)}, \ldots, X_2^{(d-1)}, \ldots, X_u^{(d-1)}, \ldots, X_u^{(d-1)}],$$

for all $1 \le j \le e-u-1$, such that for every prime p and every $h \in S_{p,n}$,

$$a_j(h) = \bar{Q}_j(a_{e-1}, a_{e-1}^p, \ldots, a_{e-1}^{p^{d-1}}, a_{e-2}, a_{e-2}^p, \ldots, a_{e-2}^{p^{d-1}}, \ldots, a_{e-u}, a_{e-u}^p, \ldots, a_{e-u}^{p^{d-1}})$$

where $\bar{Q}_j$ denotes Q_j with coefficients taken modulo p.

Conjecture n**-BPV.** *Suppose $1 < n \in \mathbb{Z}$. Then n has a divisor d such that d divides $\varphi(n)$ and Conjecture $(d, n/d)$-**BPV** holds.*

Theorem 10.1. *Conjecture (d,e)-**BPV** is false when $(d,e) = (1,30)$ and $(2,15)$.*

Proof. Let $u = \lceil \varphi(n)/d \rceil$. Conjecture (d,e)-**BPV** would imply there are polynomials $Q_1, \ldots, Q_{e-u-1} \in \mathbb{Z}[x_1, \ldots, x_u]$ such that $a_j(h) = Q_j(a_{e-u}(h), \ldots, a_{e-1}(h))$ for all primes p, $h \in S_{p,n}$, and $j \in \{1, \ldots, e-u-1\}$; so for each p and h the values $a_{e-u}(h), \ldots, a_{e-1}(h)$ would determine $a_j(h)$ for *every* j. We will disprove Conjecture (d,e)-**BPV** by exhibiting two elements $h, h' \in S_{p,n}$ such that $a_j(h) = a_j(h')$ whenever $e-u \le j \le e-1$ but $a_j(h) \ne a_j(h')$ for at least one $j < e-u$, with $p = 7$ and 11.

Let $n = 30$, and $p = 7$ or 11. Note that $\Phi_{30}(7) = 6568801$ (a prime) and $\Phi_{30}(11) = 31 \times 7537711$. Since $\Phi_{30}(p)$ is relatively prime to 30, by Lemma 1 of [4] we have $S_{p,30} = G_{p,30} - \{1\}$. View the field $\mathbb{F}_{p^{30}}$ as $\mathbb{F}_p[x]/f(x)$ with an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$, and fix a generator g of $G_{p,n}$. Specifically, let $r = (p^{30}-1)/\Phi_{30}(p)$ and let

$$\begin{aligned} f(x) &= x^{30} + x^2 + x + 5, & g &= x^r, & &\text{if } p = 7,\\ f(x) &= x^{30} + 2x^2 + 1, & g &= (x+1)^r, & &\text{if } p = 11. \end{aligned}$$

Case 1: $d = 1$, $e = 30$. Then $u = \lceil \varphi(n)/d \rceil = \varphi(30) = 8$. For $h \in S_{p,30} = G_{p,30} - \{1\}$ and $1 \le j \le 29$ we have $a_j(h) = a_{30-j}(h)$ by (10.1), so we need only consider $a_j(h)$ for $15 \le j \le 29$. By constructing a table of g^i and their characteristic polynomials $P_{g^i}^{(d)}$ for $i = 1, 2, \ldots$, and checking for matching coefficients, we found the examples in Tables 1 and 2 below. The examples in Table 1 (resp., Table 2) disprove Conjecture $(1,30)$-**BPV** with $p = 7$ (resp., 11).

Case 2: $d = 2$, $e = 15$. Then $u = \lceil \varphi(n)/d \rceil = \varphi(30)/2 = 4$. For $h \in S_{p,30} = G_{p,30} - \{1\}$ and $1 \leq j \leq 14$ we have $a_j(h) = \bar{a}_{15-j}(h)$ by (10.1), where $\bar{a}$ denotes conjugation in $\mathbb{F}_{p^2}$. Thus we need only consider $a_j(h)$ for $8 \leq j \leq 14$. View $\mathbb{F}_{p^2}$ as $\mathbb{F}_p(i)$ where $i^2 = -1$. A computer search as above leads to the examples in Tables 3 and 4. The examples in Table 3 (resp., Table 4) disprove Conjecture $(2, 15)$-**BPV** with $p = 7$ (resp., 11). □

$h \setminus j$	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
g^{2754}	3	2	0	6	4	4	2	**5**	**4**	**0**	**2**	**2**	**1**	**4**	**4**
g^{6182}	5	4	4	5	5	3	1	**5**	**4**	**0**	**2**	**2**	**1**	**4**	**4**
g^{5374}	2	0	5	**2**	1	**6**	**4**	**6**	**1**	**1**	**5**	**6**	**4**	**2**	**6**
g^{23251}	4	2	0	**2**	3	**6**	**4**	**6**	**1**	**1**	**5**	**6**	**4**	**2**	**6**

TABLE 1. Values of $a_j(h) \in \mathbb{F}_7$ for several $h \in G_{7,30}$

$h \setminus j$	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
g^{7525}	**10**	**2**	9	7	7	5	6	**9**	**2**	**1**	**8**	**10**	**4**	**1**	**10**
g^{31624}	**10**	**2**	2	4	2	3	10	**9**	**2**	**1**	**8**	**10**	**4**	**1**	**10**
g^{46208}	9	9	6	10	6	10	**10**	**8**	**1**	**3**	**2**	**7**	**4**	**6**	**5**
g^{46907}	7	8	0	0	1	7	**10**	**8**	**1**	**3**	**2**	**7**	**4**	**6**	**5**

TABLE 2. Values of $a_j(h) \in \mathbb{F}_{11}$ for several $h \in G_{11,30}$

$h \setminus j$	8	9	10	11	12	13	14
g^{173}	$4+4i$	$5+i$	$1+6i$	$\boldsymbol{4i}$	$\boldsymbol{2+3i}$	$\boldsymbol{6+3i}$	$\boldsymbol{3+i}$
g^{2669}	6	$6+3i$	$5+i$	$\boldsymbol{4i}$	$\boldsymbol{2+3i}$	$\boldsymbol{6+3i}$	$\boldsymbol{3+i}$
g^{764}	$6+6i$	**5**	**5**	**0**	**0**	**6**	**2**
g^{5348}	$6+i$	**5**	**5**	**0**	**0**	**6**	**2**

TABLE 3. Values of $a_j(h) \in \mathbb{F}_{49}$ for certain $h \in G_{7,30}$

$h \setminus j$	8	9	10	11	12	13	14
g^{9034}	$10+i$	$10i$	$3+3i$	$\boldsymbol{1+4i}$	$\boldsymbol{8+9i}$	$\boldsymbol{5+4i}$	**9**
g^{18196}	$6+8i$	$9+10i$	$8+i$	$\boldsymbol{1+4i}$	$\boldsymbol{8+9i}$	$\boldsymbol{5+4i}$	**9**

TABLE 4. Values of $a_j(h) \in \mathbb{F}_{121}$ for certain $h \in G_{11,30}$

If $n > 1$ is fixed, then Conjecture n-**BPV** of [4] says that there exists a divisor d of both n and $\varphi(n)$ such that $(d, n/d)$-**BPV** holds. Since $\gcd(30, \varphi(30)) = 2$, when $n = 30$ we need only consider $d = 1$ and 2. The following is an immediate consequence of Theorem 10.1.

Corollary 10.2. *Conjectures* $(1,30)$-**BPV**, $(2,15)$-**BPV**, *and* 30-**BPV** *of* [4] *are false. Thus, Conjectures 1 and 3 of* [4] *are both false.*

Remark 10.3. For $d = 1$ and $e = 30$, the last two lines of Table 1 (resp., Table 2) show that even the larger collection of values $a_{18}(h)$, $a_{20}(h)$, $\dots$, $a_{29}(h)$ (resp., $a_{21}(h)$, $\dots$, $a_{29}(h)$) does not determine any of the other values when $p = 7$ (resp., $p = 11$). We also found that no 8 coefficients determine all the rest; we found 64 pairs of elements so that given any set of 8 coefficients, one of these 64 pairs match up on these coefficients but not everywhere. In fact, we computed additional examples that show that when $p = 7$, no ten coefficients determine all the rest. We also show that when $p = 7$ no set of eight coefficients determines even one additional coefficient.

Suppose now $d = 2$, $e = 15$, and $p = 7$. Then the last two lines of Table 3 show that even the larger collection of values $a_9(h)$, $\dots$, $a_{14}(h)$ does not determine the remaining value $a_8(h) \in \mathbb{F}_{49}$. We have computed additional examples that show that *no* choice of four of the values $a_8(h), \dots, a_{14}(h)$ determines the other three.

The next lemma is used to prove Theorem 10.5 (and Lemma 10.6) below.

Lemma 10.4. *Suppose L/k is a cyclic extension of degree n, and τ is a generator of $G := \mathrm{Gal}(L/k)$. Then the natural ring homomorphism $\gamma : \mathbb{Z}[G] \to \mathrm{End}(\mathbb{T}_{L/k})$ has kernel $(\Phi_n(\tau))$.*

Proof. This follows from Proposition 4.2(iii) and Lemma 5.4 of [24]. □

Theorem 10.5. *Suppose k is a prime field ($\mathbb{Q}$ or $\mathbb{F}_p$), n is a square-free integer, L/k is a cyclic extension of degree n, $k \subseteq F \subseteq L$, $d := [F : k]$, and $e := [L : F]$. Suppose d divides $\varphi(n)$. Then Conjecture* (d,e)-**BPV** *of* [4] *implies that the map λ_F defined in* (9.1) *is a birational isomorphism.*

Proof. Let $u = \varphi(n)/d$. Since $\dim(\mathcal{X}_F) = \dim((\mathrm{Res}_{F/k}\mathbb{A}^1)^u)$, it suffices to show that λ_F induces a surjective map on function fields $k((\mathrm{Res}_{F/k}\mathbb{A}^1)^u) \to k(\mathcal{X}_F)$. Fix an isomorphism $(\phi_1, \dots, \phi_d) : \mathrm{Res}_{F/k}\mathbb{A}^1 \xrightarrow{\sim} \mathbb{A}^d$ over k. Since $\{\phi_j \circ \tilde{\sigma}_{i,F} : 1 \le i \le e, 1 \le j \le d\}$ generates $k(\mathcal{X}_F)$ by Theorem 9.8, it suffices to show that for all $1 \le i \le e$ and $1 \le j \le d$ there is a $g_{i,j} \in k((\mathrm{Res}_{F/k}\mathbb{A}^1)^u)$ such that $g_{i,j} \circ \lambda_F = \phi_j \circ \tilde{\sigma}_{i,F}$.

For $1 \le j \le d$, let $t_j : (\mathrm{Res}_{F/k}\mathbb{A}^1)^u \to \mathrm{Res}_{F/k}\mathbb{A}^1$ be the j-th projection. Then $t_i \circ \lambda_F = \tilde{\sigma}_{i,F}$. With Q_i from Conjecture (d,e)-**BPV** and writing $[\tau^i]$ for $\gamma(\tau^i)$ with τ and γ as in Lemma 10.4, for $1 \le i \le e$ define $f_i : \mathbb{T}_{L/k} \to \mathrm{Res}_{F/k}\mathbb{A}^1$ by

$$f_i = \tilde{\sigma}_{i,F} -$$
$$Q_i(\tilde{\sigma}_{e-1,F}, [\tau]\circ\tilde{\sigma}_{e-1,F}, [\tau^2]\circ\tilde{\sigma}_{e-1,F}, \dots, [\tau^{d-1}]\circ\tilde{\sigma}_{e-1,F}, \tilde{\sigma}_{e-2,F}, \dots, [\tau^{d-1}]\circ\tilde{\sigma}_{e-u,F}).$$

We show below that $f_i = 0$. The desired result then follows by taking

$$g_{i,j} := \phi_j \circ Q_i(t_1, [\tau] \circ t_1, \dots, [\tau^{d-1}] \circ t_1, t_2, [\tau] \circ t_2, \dots, [\tau^{d-1}] \circ t_{e-u}).$$

First suppose $k = \mathbb{Q}$. Viewing $\mathbb{T}_{L/\mathbb{Q}}(\mathbb{Q}) \subseteq L^\times$ via Theorem 5.7(ii), let $A_L := \{\alpha \in \mathbb{T}_{L/\mathbb{Q}}(\mathbb{Q}) : L = \mathbb{Q}(\alpha)\}$. Fix any $\alpha \in A_L$. Let $S(\alpha)$ be the set of all primes ℓ such that $\mathrm{Frob}_\ell(L/\mathbb{Q}) = \tau$, α is integral at ℓ, and ℓ does not divide the discriminant of the minimal polynomial for α over $\mathbb{Q}$. Let $\mathcal{O}_L$ denote the ring of integers of the number field L. Since $\mathrm{Frob}_\ell(L/\mathbb{Q}) = \tau$, we have $\mathcal{O}_L/\ell\mathcal{O}_L \cong \mathbb{F}_{\ell^n}$. Since α is integral at ℓ, and ℓ does not divide the discriminant of α's minimal polynomial, we have $\mathbb{F}_{\ell^n} = \mathbb{F}_\ell(\tilde{\alpha})$ where $\tilde{\alpha}$ is the image of α under $(\mathcal{O}_L)_{(\ell)} \to \mathcal{O}_L/\ell\mathcal{O}_L$, with $(\mathcal{O}_L)_{(\ell)}$

the localization. Conjecture (d,e)-**BPV** implies $\mathrm{ord}_\ell(f_i(\alpha)) > 0$ for all $\ell \in S(\alpha)$. Since $S(\alpha)$ is an infinite set (by the Cebotarev density theorem), $f_i(\alpha) = 0$. Lemma 10.6(ii) below shows that A_L is Zariski-dense in $\mathbb{T}_{L/\mathbb{Q}}$; therefore $f_i = 0$.

Now suppose $k = \mathbb{F}_p$. Let L' be any cyclic extension of $\mathbb{Q}$ of degree n for which p is inert, and let F' be the subfield of L' of degree d over $\mathbb{Q}$. Since p is inert, the residue field of F' at p is $\mathbb{F}_{p^d} = F$. The map f_i is the reduction modulo p of the f_i defined in characteristic zero, and thus is 0. □

The previous proof made use of the following lemma.

Lemma 10.6. *Suppose k is an infinite field, and L is a cyclic extension of k of finite square-free degree. Let $\iota : \mathbb{T}_{L/k}(k) \hookrightarrow L^\times$ be the inclusion of Theorem 5.7(ii) and let $A_L = \{\alpha \in \mathbb{T}_{L/k}(k) : L = k(\iota(\alpha))\}$. Then*

(i) *$\mathbb{T}_{L/k}(k)$ is Zariski-dense in $\mathbb{T}_{L/k}$, and*
(ii) *A_L is Zariski-dense in $\mathbb{T}_{L/k}$.*

Proof. By Theorem 5.7(iii), there is a surjective morphism f over k from $\mathrm{Res}_{L/k}\mathbb{G}_m$ onto the connected algebraic group $\mathbb{T}_{L/k}$. Since k is infinite and $\mathrm{Res}_{L/k}\mathbb{G}_m$ is rational, $(\mathrm{Res}_{L/k}\mathbb{G}_m)(k)$ is Zariski dense in $\mathrm{Res}_{L/k}\mathbb{G}_m$. If U is a non-empty open subset of $\mathbb{T}_{L/k}$, then $f^{-1}(U)$ is a non-empty open subset of $\mathrm{Res}_{L/k}\mathbb{G}_m$, so contains an $x \in (\mathrm{Res}_{L/k}\mathbb{G}_m)(k)$. Then $f(x) \in \mathbb{T}_{L/k}(k) \cap U$. Now (i) follows.

Let τ be a generator of $G := \mathrm{Gal}(L/k)$ and let $n = |G|$. Let $\omega = \prod_{i=1}^{n-1}(1-\tau^i) \in \mathbb{Z}[G]$ and let $W := \ker \gamma(\omega) \subseteq \mathbb{T}_{L/k}$, with γ as in Lemma 10.4. Then W is closed. Since $\prod_{i=1}^{n-1}(1-x^i)$ is not divisible by $\Phi_n(x)$, Lemma 10.4 implies that $\gamma(\omega) \neq 0$, so $W \neq \mathbb{T}_{L/k}$. Suppose $\beta \in \mathbb{T}_{L/k}(k) - A_L$. By the definition of A_L, $L \neq k(\iota(\beta))$, so there is a $j \in \{1, \ldots, n-1\}$ such that $\tau^j(\iota(\beta)) = \iota(\beta)$. Thus $\gamma(\tau^j)(\beta) = \beta$, so $\beta \in W(k)$. Thus $\mathbb{T}_{L/k}(k) - A_L \subseteq W(k)$, so $A_L \cup W(k) = \mathbb{T}_{L/k}(k)$. Let A be the Zariski closure of A_L in $\mathbb{T}_{L/k}$. Then $\mathbb{T}_{L/k}(k) \subseteq A(k) \cup W(k)$. By (i), $\mathbb{T}_{L/k} = A \cup W$. Since $\mathbb{T}_{L/k}$ is irreducible and $W \neq \mathbb{T}_{L/k}$, we have $A = \mathbb{T}_{L/k}$, giving (ii). □

Our next goal (Theorem 10.9) is to show that the conjectures in [4] are false when $n = 30$ in almost all characteristics. Since we do not know whether $\mathbb{T}_{30}$ is rational, we cannot find nice coordinates on $\mathbb{T}_{30}$. However, by Lemma 5.4, $\mathbb{T}_{30}$ is isomorphic over $\mathbb{F}_{q^{30}}$ to $\mathbb{T}_G$, which is isomorphic to $\mathbb{G}_m^8$ by Lemma 5.6. Using explicit coordinates on $\mathbb{G}_m^8$, we can take derivatives with respect to these coordinates, as we do below in the proof of Proposition 10.8. We do not know a direct proof of Theorem 10.9, without going through Proposition 10.8.

Suppose Γ is a cyclic group of order 30, and Δ is a subgroup of Γ of index $d = 1$ or 2. Let $u = \lceil \varphi(n)/d \rceil$, and let

$$\mathbf{s}_\Delta := (s_1, \ldots, s_u) : \mathbb{X}_\Gamma \longrightarrow (\mathbb{A}^{\Gamma/\Delta})^u.$$

The idea of the proof of Proposition 10.8 is as follows. Suppose for simplicity that $d = 1$, so $\Delta = \Gamma$. We showed in Theorem 10.1 that $\lambda_{\mathbb{F}_7}$ is not injective. Using the counterexample to injectivity constructed there, and the diagram of Proposition 9.10(iv), we deduce (via the computation of a derivative and Hensel's Lemma) that $\mathbf{s}_\Gamma$ over $\mathbb{Q}_7$ is generically not injective, so in particular $\mathbf{s}_\Gamma$ over $\mathbb{Q}_7$ is not a birational isomorphism. It follows that $\mathbf{s}_\Gamma$ over $\mathbb{Q}$ is not a birational isomorphism. Reducing mod ℓ shows that $\mathbf{s}_\Gamma$ over $\mathbb{F}_\ell$ is not a birational isomorphism for all but finitely many primes ℓ.

Lemma 10.7. *With notation as in Definition 5.3, the function field $k(\mathbb{X}_\Delta)$ is generated by the symmetric functions $\{s_i : 1 \le i \le |\Delta|\}$.*

Proof. Apply Theorem 9.8, Proposition 9.10, and Lemma 5.4. □

Proposition 10.8. *Fix a field k. There is a finite set P of prime numbers such that if $\mathrm{char}(k) \notin P$, Γ is a cyclic group of order 30, and Δ is a subgroup of Γ of index 1 or 2, then the morphism $\mathbf{s}_\Delta$ is not a birational isomorphism.*

Proof. Suppose that $\Delta = \Gamma$. The proof when $[\Gamma : \Delta] = 2$ is exactly analogous. Let $\mathbf{s} := \mathbf{s}_\Gamma$. Note that if Ω is an extension field of k, then the morphism $\mathbf{s}$ is a birational isomorphism over k if and only if it is a birational isomorphism over Ω.

Lemma 5.6 gives an isomorphism $\mathbb{G}_m^8 \xrightarrow{\sim} \mathbb{T}_\Gamma \subseteq \mathbb{G}_m^\Gamma$. Let $t_1, \ldots, t_8$ be the coordinates on $\mathbb{T}_\Gamma$ induced by this isomorphism. Viewing the restrictions of $s_1, \ldots, s_8$ to $\mathbb{T}_\Gamma$ as rational functions of $t_1, \ldots, t_8$, let $J : \mathbb{T}_\Gamma \to \mathbb{A}^1$ be the Jacobian determinant $\det\big(\frac{\partial s_i}{\partial t_j}\big)_{i,j=1,\ldots,8}$.

Let $\mathbf{x}$ and $\mathbf{y}$ be the image in $\mathbb{T}_\Gamma$, under the isomorphism of Lemma 5.4, of the first two entries in Table 1 (respectively, Table 3 in the case $[\Gamma : \Delta] = 2$). Then $\mathbf{x}$ and $\mathbf{y}$ are two elements of $\mathbb{T}_\Gamma(\mathbb{F}_{7^{30}})$, distinct modulo the action of Σ_Γ (since the first 2 rows of the table differ), such that $\mathbf{s}(\mathbf{x}) = \mathbf{s}(\mathbf{y})$ (since the first 8 entries agree). We computed further that $J(\mathbf{x}) \ne 0$ and $J(\mathbf{y}) \ne 0$.

Set $\beta = \mathbf{s}(\mathbf{x}) = \mathbf{s}(\mathbf{y}) \in (\mathbb{F}_{7^{30}})^8$, and let $\tilde{L}$ be the unramified extension of $\mathbb{Q}_7$ of degree 30. Since $J(\mathbf{x}) \ne 0$ and $J(\mathbf{y}) \ne 0$, by Hensel's Lemma for every lift $\tilde{\beta}$ of β to $\tilde{L}^8$ we can find unique lifts $\tilde{\mathbf{x}}$ of $\mathbf{x}$ and $\tilde{\mathbf{y}}$ of $\mathbf{y}$ to $\mathbb{T}_\Gamma(\tilde{L})$ such that $\mathbf{s}(\tilde{\mathbf{x}}) = \mathbf{s}(\tilde{\mathbf{y}}) = \tilde{\beta}$. 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. Note that we have shown that $\mathbb{Q}(\mathbb{X}_\Gamma)$ is a finite nontrivial extension of $\mathbb{Q}(\mathbb{A}^8)$.

Let $A := \mathbb{Z}[x_1, \ldots, x_8] \subset \mathbb{Q}(\mathbb{A}^8) \subset \mathbb{Q}(\mathbb{X}_\Gamma)$ and $B := \mathbb{Z}[s_1, \ldots, s_{30}]$. Note that A is a subring of B via the map induced by $x_i \mapsto s_i$. The field of fractions $\mathrm{Frac}(B)$ of B is $\mathbb{Q}(\mathbb{X}_\Gamma)$ by Lemma 10.7. Since this field is a finite nontrivial extension of $\mathrm{Frac}(A) = \mathbb{Q}(\mathbb{A}^8)$, we can choose $0 \ne f \in A$ such that $B' := B[1/f]$ is integral over $A' := A[1/f]$ and $A' \ne B'$.

Let P be the (finite) set of prime numbers that divide f in A. Suppose $p \notin P$. Then pA' is a prime ideal of A'. Since $B/pB = \mathbb{F}_p[s_1, \ldots, s_{30}] \subseteq \mathbb{F}_p(\mathbb{X}_\Gamma)$, B/pB is an integral domain, so pB is a prime ideal of B. Since B' is integral over A', p does not divide f in B, so pB' is a prime ideal of B'. Let $A'_{(p)}$ (resp., $B'_{(p)}$) denote the localization of A' (resp., B') at pA' (resp., pB'). Then

$$\mathrm{Frac}(A'_{(p)}) = \mathrm{Frac}(A') = \mathbb{Q}(\mathbb{A}^8) \ne \mathbb{Q}(\mathbb{X}_\Gamma) = \mathrm{Frac}(B') = \mathrm{Frac}(B'_{(p)}). \qquad (10.2)$$

Since $A'_{(p)}$ is a Noetherian local domain of dimension one and its maximal ideal $pA'_{(p)}$ is principal, by Proposition 9.2 of [1], $A'_{(p)}$ is a principal ideal domain. It follows that $B'_{(p)}$ is a free $A'_{(p)}$-module, of rank > 1 by (10.2). Thus

$$\mathbb{F}_p(x_1, \ldots, x_8) = \mathrm{Frac}(A'/pA') = A'_{(p)}/pA'_{(p)} \ne$$
$$B'_{(p)} \otimes_{A'_{(p)}} (A'_{(p)}/pA'_{(p)}) = B'_{(p)}/pB'_{(p)} = \mathrm{Frac}(B'/pB') = \mathbb{F}_p(\mathbb{X}_\Gamma).$$

Thus $\mathbf{s}$ is not a birational isomorphism over $\mathbb{F}_p$, and the same holds with $\mathbb{F}_p$ replaced by any field of characteristic p. □

Theorem 10.9. *Fix a field k. There is a finite set P of prime numbers such that if* $\operatorname{char}(k) \notin P$*, L/k is cyclic of degree* 30*, and $k \subseteq F \subseteq L$ with $[F : k] = 1$ or* 2*, then the morphism λ_F is not a birational isomorphism.*

Proof. With $\Gamma = \operatorname{Gal}(L/k)$ and $\Delta = \operatorname{Gal}(L/F)$, apply Propositions 9.10(iv,v) and 10.8. □

Theorems 10.9 and 10.5 show that Conjectures $(1, 30)$-**BPV** and $(2, 15)$-**BPV** of [4] are false in all but finitely many characteristics.

References

[1] M. F. Atiyah, I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, Mass., 1969.

[2] E. Bach, J. Shallit, *Factoring with cyclotomic polynomials*, Math. Comp. **52** (1989), 201–219.

[3] 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**, Springer, Berlin, 1995, 386–396.

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

[5] 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**, Springer, Berlin, 1999, 321–332.

[6] N. G. de Bruijn, *On the factorization of cyclic groups*, Nederl. Akad. Wetensch. Proc. Ser. A **56** (= Indagationes Math. **15**) (1953), 370–377.

[7] M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, D. Woodruff, *Practical cryptography in high dimensional tori*, in Advances in Cryptology — EUROCRYPT 2005, Lect. Notes in Comp. Sci. **3494**, Springer, Berlin, 2005, 234–250.

[8] M. van Dijk, D. Woodruff, *Asymptotically optimal communication for torus-based cryptography*, in Advances in Cryptology — CRYPTO 2004, Lect. Notes in Comp. Sci. **3152**, Springer, Berlin, 2004, 157–178.

[9] P. Gaudry, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, Cryptology ePrint Archive, Report 2004/073, `http://eprint.iacr.org/2004/073`.

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

[11] R. Granger, D. Page, M. Stam, *A comparison of CEILIDH and XTR*, in Algorithmic Number Theory (ANTS VI), Lect. Notes in Comp. Sci. **3076**, Springer, Berlin, 2004, 235–249.

[12] R. Granger, D. Page, M. Stam, *On small characteristic algebraic tori in pairing based cryptography*, LMS Journal of Computation and Mathematics **9** (2006), 64–85.

[13] R. Granger, F. Vercauteren, *On the discrete logarithm problem on algebraic tori*, in Advances in Cryptology — CRYPTO 2005, Lect. Notes in Comp. Sci. **3621**, Springer, Berlin, 2005, 66–85.

[14] B. Huppert, N. Blackburn, Finite groups II, Springer, Berlin-New York, 1982.

[15] A. Joux, R. Lercier, *The function field sieve in the medium prime case*, in Advances in Cryptology — Eurocrypt 2006, Lect. Notes in Comp. Sci. **4004**, Springer, Berlin, 2006, 254–270.

[16] A. Joux, R. Lercier, N. Smart, F. Vercauteren, *The number field sieve in the medium prime case*, in Advances in Cryptology — CRYPTO 2006, Lect. Notes in Comp. Sci. **4117**, Springer, Berlin, 2006, 323–341.

[17] 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).

[18] D. Kohel, *Constructive and destructive facets of torus-based cryptography*, `http://echidna.maths.usyd.edu.au/~kohel/doc/torus.ps`, 2004, preprint.

[19] A. K. Lenstra, *Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields*, in Information Security and Privacy, Proc. ACISP '97, Lect. Notes in Comp. Sci. **1270**, Springer, Berlin, 1997, 127–138.

[20] A. K. Lenstra, *The XTR public key system*, lecture at MSRI Number-Theoretic Cryptography Workshop, October 20, 2000.

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

[22] H.-W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149.

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

[24] B. Mazur, K. Rubin, A. Silverberg, *Twisting commutative algebraic groups*, J. Alg. **314**, (2007), 419–438.

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

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

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

[28] K. Rubin, A. Silverberg, *Torus-based cryptography*, in Advances in Cryptology — CRYPTO 2003, Lect. Notes in Comp. Sci. **2729**, Springer, Berlin, 2003, 349–365.

[29] K. Rubin, A. Silverberg, *Algebraic tori in cryptography*, in High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications Series **41**, AMS, Providence, RI (2004), 317–326.

[30] K. Rubin, A. Silverberg, *Using primitive subgroups to do more with fewer bits*, in Algorithmic Number Theory (ANTS VI), Lect. Notes in Comp. Sci. **3076**, Springer, 2004, 18–41.

[31] K. Rubin, A. Silverberg, *Using abelian varieties to improve pairing-based cryptography*, preprint.

[32] I. J. Schoenberg, *A note on the cyclotomic polynomial*, Mathematika **11** (1964), 131–136.

[33] M. Scott, P. S. L. M. Barreto, *Compressed pairings*, Advances in Cryptology — CRYPTO 2004, Lect. Notes in Comp. Sci. **3152**, Springer, Berlin, 2004, 140–156.

[34] 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, North-Holland, Amsterdam, 1993, 103–117.

[35] 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**, Springer, Berlin, 1995, 357–364.

[36] V. E. Voskresenskiĭ, Algebraic groups and their birational invariants, Translations of Mathematical Monographs **179**, AMS, Providence, RI, 1998.

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

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

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

[40] H. C. Williams, *Some public-key crypto-functions as intractable as factorization*, Cryptologia **9** (1985), 223–237.

Mathematics Department, University of California at Irvine, Irvine, CA 92697 USA
E-mail address: krubin@uci.edu
E-mail address: asilverb@uci.edu