Torus-Based Cryptography

Karl Rubin[1]* and Alice Silverberg[2]

[1] Department of Mathematics
Stanford University
Stanford CA, USA
rubin@math.stanford.edu

[2] Department of Mathematics
Ohio State University
Columbus, OH, USA
silver@math.ohio-state.edu

Abstract. We introduce the concept of torus-based cryptography, give a new public key system called CEILIDH, and compare it to other discrete log based systems including Lucas-based systems and XTR. Like those systems, we obtain small key sizes. While Lucas-based systems and XTR are essentially restricted to exponentiation, we are able to perform multiplication as well. We also disprove the open conjectures from [2], and give a new algebro-geometric interpretation of the approach in that paper and of LUC and XTR.

1 Introduction

This paper accomplishes several goals. We introduce a new concept, namely torus-based cryptography, and give a new torus-based public key cryptosystem that we call CEILIDH. We compare CEILIDH with other discrete log based systems, and show that it improves on Diffie-Hellman and Lucas-based systems and has some advantages over XTR. Moreover, we show how to use the mathematics underlying XTR and Lucas-based systems to interpret them in terms of algebraic tori. We also show that a certain conjecture about algebraic tori has as a consequence new torus-based cryptosystems that would generalize and improve on CEILIDH and XTR. Further, we disprove the open conjectures from [2], and thereby show that the approach to generalizing XTR that was suggested in [2] cannot succeed.

The Lucas-based systems, the cubic field system in [5], and XTR have the discrete log security of the field $\mathbb{F}_{p^n}$, for $n = 2$, 3, and 6, resp., while the data required to be transmitted consists of $\varphi(n)$ elements of $\mathbb{F}_p$. Since these systems have $n \log p$ bits of security when exchanging $\varphi(n) \log p$ bits of information, they are more efficient than Diffie-Hellman by a factor of $n/\varphi(n) = 2$, $3/2$, and 3, respectively. See [10, 15, 16, 20, 21, 1] for Lucas-based systems and LUC, and [3, 7, 8] for XTR and related work.

* Rubin was partially supported by NSF grant DMS-0140378.

What makes discrete log based cryptosystems work is that they are based on the mathematics of algebraic groups. An algebraic group is both a group and an algebraic variety. The group structure allows you to multiply and exponentiate. The variety structure allows you to express all elements and operations in terms of polynomials, and therefore in a form that can be efficiently handled by a computer.

In classical Diffie-Hellman, the underlying algebraic group is $\mathbb{G}_m$, the multiplicative group. Algebraic tori (not to be confused with complex tori of elliptic curve fame) are generalizations of the multiplicative group. By definition, an algebraic torus is an algebraic variety that over some extension field is isomorphic to $(\mathbb{G}_m)^d$, namely, d copies of the multiplicative group. For the tori we consider, the group operation is just the usual multiplication in a (larger) finite field.

The cryptosystems based on algebraic tori introduced in this paper accomplish the same goal as Lucas-based systems, XTR, and [5] of attaining the full security of the field $\mathbb{F}_{p^n}$ while requiring the transmission of only $\varphi(n)$ elements of $\mathbb{F}_p$. However, they additionally take advantage of the fact that an algebraic torus is a multiplicative group. For every n one can define an algebraic torus T_n with the property that $T_n(\mathbb{F}_p)$ consists of the elements in $\mathbb{F}_{p^n}^\times$ whose norms are 1 down to every intermediate subfield. This torus T_n has dimension $\varphi(n)$. When the torus is "rational", then its elements can be compactly represented by $\varphi(n)$ elements of $\mathbb{F}_p$. Doing cryptography inside this subgroup of $\mathbb{F}_{p^n}^\times$ has the security of the Diffie-Hellman problem in $\mathbb{F}_{p^n}^\times$ (see Lemma 7 below), but only $\varphi(n)$ elements of $\mathbb{F}_p$ need to be transmitted.

The CEILIDH[1] public key system is Compact, Efficient, Improves on LUC, and Improves on Diffie-Hellman. It also has some advantages over XTR. The system is based on the 2-dimensional algebraic torus T_6. The CEILIDH system does discrete log cryptography in a subgroup of $\mathbb{F}_{p^6}^\times$ while representing the elements in $\mathbb{F}_p^2$, giving a savings comparable to that of XTR, and having exactly the same security proof. While XTR and the Lucas-based cryptosystems are essentially restricted to exponentiation, CEILIDH allows full use of multiplication, thereby enabling a wider range of applications. In particular, where XTR uses a hybrid ElGamal encryption scheme that exchanges a key and then does symmetric encryption with that shared key, CEILIDH can do an exact analogue of (non-hybrid) ElGamal, since it has group multiplication at its disposal. Because of this multiplication, any cryptographic application that can be done in an arbitrary group can be done in a torus-based cryptosystem such as CEILIDH.

We also show that XTR, rather than being based on the torus T_6, is based on a quotient of this torus by the symmetric group S_3. The reason that XTR does not have a straightforward multiplication is that this quotient variety is not a group. (We note, however, that XTR has additional features that permit efficient computations.)

We exhibit a similar, but easier, construction based on the 1-dimensional torus T_2, obtaining a system similar to LUC but with the advantage of being

[1] The Scots Gaelic word *ceilidh*, pronounced "kayley", means a traditional Scottish gathering. This paper is dedicated to the memory of a cat named Ceilidh.

able to efficiently perform the group operation (in fact, directly in $\mathbb{F}_p$). This system has the security of $\mathbb{F}_{p^2}$ while transmitting elements of the field $\mathbb{F}_p$ itself.

The next case where $n/\varphi(n)$ is "large" is when $n = 30$ (and $\varphi(n) = 8$). Here, the 8-dimensional torus T_{30} is not known to be rational, though this is believed to be the case. An explicit rational parametrization of T_{30} would give a compact representation of this group by 8 elements of $\mathbb{F}_p$, with the security of the field $\mathbb{F}_{p^{30}}$. It would also refute the statement made in the abstract to [2] that "it is unlikely that such a compact representation of elements can be achieved in extension fields of degree thirty."

Conjectures were made in [2] suggesting a way to generalize LUC and XTR to obtain the security of the field $\mathbb{F}_{p^{30}}$ while transmitting only 8 elements of $\mathbb{F}_p$. In addition to showing that a rational parametrization of the torus T_{30} would accomplish this, we also show that the method suggested in [2] for doing this cannot. The reason is that, reinterpreting the conjectures in [2] in the language of algebraic tori, they say that the coordinate ring of the quotient of T_{30} by a certain product of symmetric groups is generated by the first 8 of the symmetric functions on 30 elements. (This would generalize the fact that the coordinate ring of T_6/S_3 is generated by the trace, which is what enables the success of XTR.) In §2 we disprove the open conjectures from [2]. This confirms the idea in [2] that the approach in [2] is unlikely to work.

Section 2 gives counterexamples to the open questions in [2]. Section 3 gives background on algebraic tori, defines the tori T_n, shows that $T_n(\mathbb{F}_q)$ is the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$, and shows that the security of cryptosystems based on this group is the discrete log security of $\mathbb{F}_{q^n}^\times$. Section 4 discusses rational parametrizations and compact representations, while §5 gives explicit rational parametrizations of T_6 and T_2. In §6 we introduce torus-based cryptography, and give the CEILIDH system (based on the torus T_6), a system based on T_2, and conjectured systems based on T_n for all n (most interesting for $n = 30$ or 210). In §7 we reinterpret the Lucas-based cryptosystems, XTR, and the point of view in [2] in terms of algebraic tori, and compare these systems to our torus-based systems.

Note that [12] gives another example, this time in the context of elliptic curves rather than multiplicative groups of fields, where the Weil restriction of scalars is used to obtain $n\log(q)$ bits of security from $\varphi(n)\log(q)$ bit transmissions.

1.1 Notation

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a prime power. Write φ for the Euler φ-function. Write Φ_n for the n-th cyclotomic polynomial, and let $G_{q,n}$ be the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$. Let $\mathbb{A}^n$ denote n-dimensional affine space, i.e., the variety whose $\mathbb{F}_q$-points are $\mathbb{F}_q^n$ for every q.

2 Counterexamples to the Open Questions in [2]

Four conjectures are stated in [2]. The two "strong" conjectures are disproved there. Here we disprove the two remaining conjectures (Conjectures 1 and 3 of

[2], which are also called (d,e)-**BPV** and n-**BPV**). In fact, we do better. We give examples that show not only that the conjectures are false, but also that weaker forms of the conjectures (i.e., with less stringent conclusions) are also false.

Fix an integer $n > 1$, a prime power q, and a factorization $n = de$ with $e > 1$. Recall that $G_{q,n}$ is the subgroup of $\mathbb{F}_{q^n}^{\times}$ of order $\Phi_n(q)$, where Φ_n is the n-th cyclotomic polynomial. Let $S_{q,n}$ be the set of elements of $G_{q,n}$ not contained in any proper subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$. For $h \in G_{q,n}$, let $P_h^{(d)}$ be the characteristic polynomial of h over $\mathbb{F}_{q^d}$, and define functions $a_j : G_{q,n} \to \mathbb{F}_{q^d}$ by

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

Then $a_0(h) = (-1)^e$, and if also n is even then

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

for all $j \in \{1, \ldots, e-1\}$ (see for example Theorem 1 of [2]).

The following conjecture is a *consequence* of Conjecture (d,e)-**BPV** of [2].

Conjecture (p,d,e)-**BPV**$'$ **([2])** *Let* $u = \lceil \varphi(n)/d \rceil$. *There are polynomials* $Q_1, \ldots, Q_{e-u-1} \in \mathbb{Z}[x_1, \ldots, x_u]$ *such that for all* $h \in S_{p,n}$ *and* $j \in \{1, \ldots, e-u-1\}$,

$$a_j(h) = Q_j(a_{e-u}(h), \ldots, a_{e-1}(h)).$$

We will prove below the following result.

Theorem 1 *Conjecture* (p,d,e)-**BPV**$'$ *is false when* (p,d,e) *is any one of the triples* $(7,1,30), (7,2,15), (11,1,30), (11,2,15)$.

If $n > 1$ is fixed, then Conjecture n-**BPV** of [2] 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. Since $(d, n/d)$-**BPV** implies $(p, d, n/d)$-**BPV**$'$ for every p, the following is an immediate consequence of Theorem 1.

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

Remark 3 The case $n = 30$ is particularly relevant for cryptographic applications, because this is the smallest value of n for which $n/\varphi(n) > 3$. If Conjecture 30-**BPV** of [2] were true it would have had cryptographic applications.

Proof of Theorem 1. If Conjecture (p,d,e)-**BPV**$'$ were true, then for every $h \in S_{p,n}$ the values $a_{e-u}(h), \ldots, a_{e-1}(h)$ would determine $a_j(h)$ for *every* j. We will disprove Conjecture (p,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 $j < e - u$.

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 [2] we have $S_{p,30} = G_{p,30} - \{1\}$. We 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 we 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: $n = 30$, $e = 30$, $d = 1$. Then $u = \lceil \varphi(n)/d \rceil = 8$. 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 (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. The examples in Table 1 disprove Conjecture $(7,1,30)$-**BPV′** and the examples in Table 2 disprove Conjecture $(11,1,30)$-**BPV′**.

$h \setminus j$	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 $h \in G_{11,30}$

Case 2: $n = 30$, $e = 15$, $d = 2$. Then $u = \lceil \varphi(n)/d \rceil = 4$. For $h \in S_{p,30} = G_{p,30} - \{1\}$ and $1 \le j \le 14$ we have $a_j(h) = \overline{a_{15-j}}(h)$ by (1), where $\overline{a}$ denotes conjugation in $\mathbb{F}_{p^2}$. Thus we need only consider $a_j(h)$ for $8 \le j \le 14$. 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 disprove Conjecture $(7,2,15)$-**BPV′** and the examples in Table 4 disprove Conjecture $(11,2,15)$-**BPV′**.

This concludes the proof of Theorem 1.

$h \setminus j$	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}	$6+6i$	$\mathbf{5}$	$\mathbf{5}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{6}$	$\mathbf{2}$
g^{5348}	$6+i$	$\mathbf{5}$	$\mathbf{5}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{6}$	$\mathbf{2}$

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}	$10+i$	$10i$	$3+3i$	$\boldsymbol{1+4i}$	$\boldsymbol{8+9i}$	$\boldsymbol{5+4i}$	$\mathbf{9}$
g^{18196}	$6+8i$	$9+10i$	$8+i$	$\boldsymbol{1+4i}$	$\boldsymbol{8+9i}$	$\boldsymbol{5+4i}$	$\mathbf{9}$

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

Remark 4 Using these examples and some algebraic geometry, we prove in Theorem 5.3 of [13] that Conjectures $(p, 1, 30)$-$\mathbf{BPV}'$ and $(p, 2, 15)$-$\mathbf{BPV}'$ are each false for almost every prime p.

Remark 5 For $d = 1$ and $e = 30$, the last two lines of Table 1 (resp., Table 2) show that even the larger collection of values $a_{18}(h)$, $a_{20}(h)$, ..., $a_{29}(h)$ (resp., $a_{21}(h)$, ..., $a_{29}(h)$) 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 $a_9(h)$, ..., $a_{14}(h)$ 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 $a_8(h), \ldots, a_{14}(h)$ determines the other three.

3 Algebraic Tori

Good references for algebraic tori are [11, 17].

Definition 6 An *algebraic torus* T over $\mathbb{F}_q$ is an algebraic group defined over $\mathbb{F}_q$ that over some finite extension field is isomorphic to $(\mathbb{G}_m)^d$, where $\mathbb{G}_m$ is the multiplicative group and d is necessarily the dimension of T. If T is isomorphic to $(\mathbb{G}_m)^d$ over $\mathbb{F}_{q^n}$, then one says that $\mathbb{F}_{q^n}$ *splits* T.

Let $k = \mathbb{F}_q$ and $L = \mathbb{F}_{q^n}$. Writing $\mathrm{Res}_{L/k}$ for the Weil restriction of scalars from L to k (see §3.12 of [17] or §1.3 of [19] for the definition and properties), then

$\mathrm{Res}_{L/k}\mathbb{G}_m$ is a torus. The universal property of the Weil restriction of scalars gives an isomorphism:

$$(\mathrm{Res}_{L/k}\mathbb{G}_m)(k) \cong \mathbb{G}_m(L) = L^\times. \tag{2}$$

If $k \subset F \subset L$ then the universal property also gives a norm map:

$$\mathrm{Res}_{L/k}\mathbb{G}_m \xrightarrow{N_{L/F}} \mathrm{Res}_{F/k}\mathbb{G}_m$$

which makes the following diagram commute:

$$\begin{tikzcd}
(\mathrm{Res}_{L/k}\mathbb{G}_m)(k) \arrow[r, "N_{L/F}"] \arrow[d, "\cong"'] & (\mathrm{Res}_{F/k}\mathbb{G}_m)(k) \arrow[d, "\cong"'] \\
L^\times \arrow[r, "N_{L/F}"] & F^\times
\end{tikzcd} \tag{3}$$

(recall that the norm of an element is the product of its conjugates).

Define the torus T_n to be the intersection of the kernels of the norm maps $N_{L/F}$, for all subfields $k \subset F \subsetneq L$.

$$T_n := \ker\left[\mathrm{Res}_{L/k}\mathbb{G}_m \xrightarrow{\oplus N_{L/F}} \bigoplus_{k\subseteq F\subsetneq L} \mathrm{Res}_{F/k}\mathbb{G}_m\right].$$

By (3), for k-points we have:

$$T_n(k) \cong \{\alpha \in L^\times : N_{L/F}(\alpha) = 1 \text{ whenever } k \subset F \subsetneq L\}. \tag{4}$$

The dimension of T_n is $\varphi(n)$ (see [17]).

The group $T_n(\mathbb{F}_q)$ is a subgroup of the multiplicative group $\mathbb{F}_{q^n}^\times$. Lemma 7 below identifies $T_n(\mathbb{F}_q)$ with the cyclic subgroup $G_{q,n} \subset \mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$, and shows that the security of discrete log-based cryptosystems on the group T_n is really that of the multiplicative group of $\mathbb{F}_{q^n}$ and not any smaller field.

Lemma 7 *(i)* $T_n(\mathbb{F}_q) \cong G_{q,n}$.
(ii) $\#T_n(\mathbb{F}_q) = \Phi_n(q)$.
(iii) If $h \in T_n(\mathbb{F}_q)$ is an element of prime order not dividing n, then h does not lie in a proper subfield of $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Proof. The group $\mathbb{F}_{q^n}^\times$ is cyclic of order $q^n - 1$, and $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is generated by the Frobenius automorphism which sends $x \in \mathbb{F}_{q^n}^\times$ to x^q. Hence if t divides n, then $N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^t}}(x) = x^{(q^n-1)/(q^t-1)}$. Thus by (4),

$$T_n(\mathbb{F}_q) \cong \{x \in \mathbb{F}_{q^n}^\times : x^c = 1\} \tag{5}$$

where $c = \gcd\{(q^n-1)/(q^t-1) : t \mid n \text{ and } t \neq n\}$. Since $q^t - 1 = \prod_{j|t} \Phi_j(q)$, we have that $\Phi_n(q)$ divides c. There are polynomials $a_t(u) \in \mathbb{Z}[u]$ such that

$$\sum_{t|n, t\neq n} a_t(u)\frac{u^n-1}{u^t-1} = \Phi_n(u)$$

(see for example Theorem 1 of [4] or Theorem 2 of [14][2]), and so c divides $\Phi_n(q)$ as well. Thus $c = \Phi_n(q)$, so $T_n(\mathbb{F}_q) \cong G_{q,n}$ by (5) and the definition of $G_{q,n}$. Part (ii) follows from (i). Part (iii) now follows from Lemma 1 of [2].

4 Rationality of Tori and Compact Representations

Definition 8 Suppose T is an algebraic torus over $\mathbb{F}_q$ of dimension d. Then T is *rational* if and only if there is a birational map $\rho : T \to \mathbb{A}^d$ defined over $\mathbb{F}_q$. In other words, T is rational if and only if, after embedding T in an affine space $\mathbb{A}^t$, there are Zariski open subsets $W \subset T$ and $U \subset \mathbb{A}^d$, and (rational) functions $\rho_1, \ldots, \rho_d \in \mathbb{F}_q(x_1, \ldots, x_t)$ and $\psi_1, \ldots, \psi_t \in \mathbb{F}_q(y_1, \ldots, y_d)$ such that $\rho = (\rho_1, \ldots, \rho_d) : W \to U$ and $\psi = (\psi_1, \ldots, \psi_t) : U \to W$ are inverse isomorphisms. Call such a map ρ a *rational parametrization* of T.

A rational parametrization of a torus T gives a *compact representation* of the group $T(\mathbb{F}_q)$, i.e., a way to represent every element of the subset $W(\mathbb{F}_q) \subset T(\mathbb{F}_q)$ by d coordinates in $\mathbb{F}_q$. In general this is "best possible" (in terms of the number of coordinates), since a rational variety of dimension d has approximately q^d points over $\mathbb{F}_q$, and thus cannot be represented by fewer than d elements of $\mathbb{F}_q$.

Letting $X = T - W$, then $\dim(X) \leq d - 1$, so $|X(\mathbb{F}_q)| = O(q^{d-1})$. Thus the fraction of elements in $T(\mathbb{F}_q)$ that are "missed" by a compact representation is $|X(\mathbb{F}_q)|/|T(\mathbb{F}_q)| = O(1/q)$. For cryptographically interesting values of q this will be very small, and in special cases (by describing X explicitly as in the examples below) we obtain an even better bound.

Conjecture 9 (Voskresenskii [17]) *The torus T_n is rational.*

The conjecture is true for n if n is a prime power (see Chapter 2 of [17]) or a product of two prime powers ([6]; see also §6.3 of [17]). In the next section we will exhibit explicit rational parametrizations when $n = 6$ and 2.

When n is divisible by more than two distinct primes the conjecture is still open. Note that [18] claims a proof of a result that would imply that for every n, T_n is rational over $\mathbb{F}_q$ for almost all q. However, there is a serious flaw in the proof. Even the case $n = 30$, which would have interesting cryptographic applications, is not settled.

5 Explicit Rational Parametrizations

5.1 Rational Parametrization of T_6

Next we obtain an explicit rational parametrization of the torus T_6, thereby giving a compact representation of $T_6(\mathbb{F}_q)$. More precisely, we will show that T_6 is birationally isomorphic to $\mathbb{A}^2$, and therefore every element of $T_6(\mathbb{F}_q)$ can be represented by two elements of $\mathbb{F}_q$.

[2] The authors thank D. Bernstein and H. Lenstra for pointing out references [4, 14].

Fix $x \in \mathbb{F}_{q^2} - \mathbb{F}_q$, so $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$, and choose an $\mathbb{F}_q$-basis $\{\alpha_1, \alpha_2, \alpha_3\}$ of $\mathbb{F}_{q^3}$. Then $\{\alpha_1, \alpha_2, \alpha_3, x\alpha_1, x\alpha_2, x\alpha_3\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^6}$. Let $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$ be the element of order 2. Define a (one-to-one) map $\psi_0 : \mathbb{A}^3(\mathbb{F}_q) \hookrightarrow \mathbb{F}_{q^6}^\times$ by

$$\psi_0(u_1, u_2, u_3) = \frac{\gamma + x}{\gamma + \sigma(x)}$$

where $\gamma = u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3$. Then $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(\psi_0(\mathbf{u})) = 1$ for every $\mathbf{u} = (u_1, u_2, u_3)$. Let $U = \{\mathbf{u} \in \mathbb{A}^3 : N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\psi_0(\mathbf{u})) = 1\}$. By (4), $\psi_0(\mathbf{u}) \in T_6(\mathbb{F}_q)$ if and only if $u \in U$, so restricting ψ_0 to U gives a morphism $\psi_0 : U \to T_6$. It follows from Hilbert's Theorem 90 that every element of $T_6(\mathbb{F}_q) - \{1\}$ is in the image of ψ_0, so ψ_0 defines an isomorphism

$$\psi_0 : U \xrightarrow{\sim} T_6 - \{1\}.$$

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_1, u_2, u_3. Fix a point $\mathbf{a} = (a_1, a_2, a_3) \in U(\mathbb{F}_q)$. By adjusting the basis $\{\alpha_1, \alpha_2, \alpha_3\}$ of $\mathbb{F}_{q^6}$ if necessary, we can assume without loss of generality that the tangent plane at $\mathbf{a}$ to the surface U is the plane $u_1 = a_1$. If $(v_1, v_2) \in \mathbb{F}_q \times \mathbb{F}_q$, then the intersection of U with the line $\mathbf{a} + t(1, v_1, v_2)$ consists of two points, namely $\mathbf{a}$ and a point of the form $\mathbf{a} + \frac{1}{f(v_1,v_2)}(1, v_1, v_2)$ where $f(v_1, v_2) \in \mathbb{F}_q[v_1, v_2]$ is an explicit polynomial that we computed in Mathematica. The map that takes (v_1, v_2) to this latter point is an isomorphism

$$g : \mathbb{A}^2 - V(f) \xrightarrow{\sim} U - \{\mathbf{a}\},$$

where $V(f)$ denotes the subvariety of $\mathbb{A}^2$ defined by $f(v_1, v_2) = 0$. Thus $\psi_0 \circ g$ defines an isomorphism

$$\psi : \mathbb{A}^2 - V(f) \xrightarrow{\sim} T_6 - \{1, \psi_0(\mathbf{a})\}.$$

For the inverse isomorphism, suppose that $\beta = \beta_1 + \beta_2 x \in T_6(\mathbb{F}_q) - \{1, \psi_0(\mathbf{a})\}$ with $\beta_1, \beta_2 \in \mathbb{F}_{q^3}$. One checks easily that $\beta_2 \neq 0$, and if $\gamma = (1 + \beta_1)/\beta_2$ then $\gamma/\sigma(\gamma) = \beta$. Write $(1 + \beta_1)/\beta_2 = u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3$ with $u_i \in \mathbb{F}_q$, and define

$$\rho(\beta) = \left(\frac{u_2 - a_2}{u_1 - a_1}, \frac{u_3 - a_3}{u_1 - a_1} \right).$$

It follows from the discussion above that $\rho : T_6(\mathbb{F}_q) - \{1, \psi_0(\mathbf{a})\} \xrightarrow{\sim} \mathbb{A}^2 - V(f)$ is the inverse of the isomorphism ψ. We obtain the following.

Theorem 10 *The above maps ρ and ψ induce inverse birational maps between T_6 and $\mathbb{A}^2$.*

To implement the CEILIDH system, one must choose a finite field $\mathbb{F}_q$ and compute the rational maps ρ and ψ explicitly. We do this in two families of examples. Note that in each family the coefficients of the rational maps ρ and ψ are independent of q. When $(n, q) = 1$, write ζ_n for a primitive n-th root of unity.

Example 11 Fix $q \equiv 2$ or $5 \pmod 9$. Let $x = \zeta_3$ and $y = \zeta_9 + \zeta_9^{-1}$. Then $\mathbb{F}_{q^6} = \mathbb{F}_q(\zeta_9)$, $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$, and $\mathbb{F}_{q^3} = \mathbb{F}_q(y)$. The basis we take for $\mathbb{F}_{q^3}$ is $\{1, y, y^2 - 2\}$, and we take $\mathbf{a} = (0, 0, 0)$. Then $\psi_0(\mathbf{a}) = \zeta_3^2$, and a calculation gives $f(v_1, v_2) = 1 - v_1^2 - v_2^2 + v_1 v_2$. Thus

$$\psi(v_1, v_2) = \frac{1 + v_1 y + v_2(y^2 - 2) + f(v_1, v_2)x}{1 + v_1 y + v_2(y^2 - 2) + f(v_1, v_2)x^2}.$$

For $\beta = \beta_1 + \beta_2 x \in T_6(\mathbb{F}_q) - \{1, \zeta_3^2\}$, we have

$$\rho(\beta) = (u_2/u_1, u_3/u_1) \quad \text{where } (1 + \beta_1)/\beta_2 = u_1 + u_2 y + u_3(y^2 - 2).$$

Example 12 Fix $q \equiv 3$ or $5 \pmod 7$. Let $x = \sqrt{-7}$ and $y = \zeta_7 + \zeta_7^{-1}$. Then $\mathbb{F}_{q^6} = \mathbb{F}_q(\zeta_7)$, $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$, and $\mathbb{F}_{q^3} = \mathbb{F}_q(y)$. The basis we take for $\mathbb{F}_{q^3}$ is $\{1, y, y^2 - 1\}$, and we take $\mathbf{a} = (1, 0, 2)$. A calculation gives $f(v_1, v_2) = (2v_1^2 + v_2^2 - v_1 v_2 + 2v_1 - 4v_2 - 3)/14$. Thus

$$\psi(v_1, v_2) = \frac{\gamma + f(v_1, v_2)x}{\gamma - f(v_1, v_2)x}$$

where $\gamma = f(v_1, v_2) + 1 + v_1 y + (2f(v_1, v_2) + v_2)(y^2 - 1)$. If $\beta = \beta_1 + \beta_2 x \in T_6(\mathbb{F}_q) - \{1, \psi_0(\mathbf{a})\}$, then

$$\rho(\beta) = \Big(\frac{u_2}{u_1 - 1}, \frac{u_3 - 2}{u_1 - 1}\Big) \quad \text{where } (1 + \beta_1)/\beta_2 = u_1 + u_2 y + u_3(y^2 - 1).$$

5.2 Rational Parametrization of T_2

We give an explicit birational isomorphism between T_2 and $\mathbb{P}^1$. For simplicity we assume that q is not a power of 2, and we write $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{d})$ for some non-square $d \in \mathbb{F}_q^\times$. Let σ be the non-trivial automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$, so $\sigma(\sqrt{d}) = -\sqrt{d}$.

Define a map $\psi : \mathbb{A}^1(\mathbb{F}_q) \to T_2(\mathbb{F}_q)$ by

$$\psi(a) = \frac{a + \sqrt{d}}{a - \sqrt{d}} = \frac{a^2 + d}{a^2 - d} + \frac{2a}{a^2 - d}\sqrt{d}.$$

Conversely, suppose $\beta = \beta_1 + \beta_2\sqrt{d} \in T_2(\mathbb{F}_q)$, with $\beta \neq \pm 1$ (so $\beta_2 \neq 0$). Then

$$\beta = \frac{1 + \beta}{1 + \sigma(\beta)} = \psi\Big(\frac{1 + \beta_1}{\beta_2}\Big).$$

Thus if we let $\rho(\beta) = (1 + \beta_1)/\beta_2$, then ρ and ψ define inverse isomorphisms

$$\begin{tikzcd} T_2 - \{\pm 1\} \arrow[r, bend left, "\rho"] & \mathbb{A}^1 - \{0\} \arrow[l, bend left, "\psi"] \end{tikzcd} .$$

In fact, these maps extend naturally to give an isomorphism $T_2(\mathbb{F}_q) \xrightarrow{\sim} \mathbb{F}_q \cup \{\infty\}$ by sending 1 to ∞ and -1 to 0. A simple calculation shows that if $a, b \in \mathbb{F}_q$ and $a \neq -b$, then

$$\psi(a)\psi(b) = \psi\Big(\frac{ab+d}{a+b}\Big). \tag{6}$$

Therefore instead of doing cryptography in the subgroup T_2 of $\mathbb{F}_{q^2}$, we can do all operations (i.e., multiplications and exponentiations in T_2) directly in $\mathbb{F}_q$ itself, where now multiplication in T_2 has been translated into the map $(a,b) \mapsto \frac{ab+d}{a+b}$ from $\mathbb{F}_q \times \mathbb{F}_q$ to $\mathbb{F}_q$.

6 Torus-Based Cryptosystems

Next we introduce public key cryptosystems based on a torus T_n with a rational parametrization. The case $n = 6$ is the CEILIDH system. By Lemma 7(iii), $T_n(\mathbb{F}_q)$ has the same cryptographic security as $\mathbb{F}_{q^n}^\times$. However, thanks to the compact representation that allows us to represent an element of $T_n(\mathbb{F}_q)$ by $\varphi(n)$ elements of $\mathbb{F}_q$, the size of any data represented by a group element is decreased by a factor of $\varphi(n)/n$ compared to classical cryptosystems using $\mathbb{F}_{q^n}^\times$. This give an improvement of a factor of 3 (resp., 2) using CEILIDH (resp., T_2).

Any discrete log based cryptosystem for a general group can be done using a torus T_n with a rational parametrization. Below we describe torus-based versions of Diffie-Hellman key exchange, ElGamal encryption, and ElGamal signatures. Other examples where this can be done in a straightforward way include DSA and Nyberg-Rueppel signatures (see also §5 of [8]).

Note that it is easy to turn any torus-based cryptosystem into an RSA-like system whose security is based on the difficulty of factoring, analogous to the LUC system of [15]. Here, one views the torus T_n over a ring $\mathbb{Z}/N\mathbb{Z}$. However, as shown in [1], such RSA-based systems do not seem to have significant advantages over RSA.

Parameter selection: Choose a prime power q and an integer n such that the torus T_n over $\mathbb{F}_q$ has an explicit rational parametrization, $n\log(q) \approx 1024$ (to obtain 1024 bit security), and $\Phi_n(q)$ is divisible by a prime ℓ that has at least 160 bits. Let $m = \varphi(n)$, and fix a birational map $\rho : T_n(\mathbb{F}_q) \to \mathbb{F}_q^m$ and its inverse ψ. Choose $\alpha \in T_n$ of order ℓ (taking an arbitrary element of $\mathbb{F}_{q^n}^\times$ and raising it to the power $(q^n-1)/\ell$ will usually work), and let $g = \rho(\alpha) \in \mathbb{F}_q^m$. Note that n is a small number (2, 6, . . .). For the protocols below, the public data is n, q, ρ, ψ, ℓ, and either g or $\alpha = \psi(g)$.

Key agreement scheme (torus-based Diffie-Hellman):

1. Alice chooses a random integer a in the range $1 \le a \le \ell - 1$. She computes $P_A := \rho(\alpha^a) \in \mathbb{F}_q^m$ and sends it to Bob.
2. Bob chooses a random integer b in the range $1 \le b \le \ell - 1$. He computes $P_B := \rho(\alpha^b) \in \mathbb{F}_q^m$ and sends it to Alice.
3. Alice computes $\rho(\psi(P_B)^a) \in \mathbb{F}_q^m$.
4. Bob computes $\rho(\psi(P_A)^b) \in \mathbb{F}_q^m$.

Since $\psi \circ \rho$ is the identity, we have $\rho(\psi(P_B)^a) = \rho(\alpha^{ab}) = \rho(\psi(P_A)^b)$, and this is Alice's and Bob's shared secret.

Encryption scheme (torus-based ElGamal encryption):

1. **Key Generation:** Alice chooses a random integer a in the range $1 \leq a \leq \ell - 1$ as her private key. Her public key is $P_A := \rho(\alpha^a) \in \mathbb{F}_q^m$.
2. **Encryption:** Bob represents the message M as an element of the group generated by α, selects a random integer k in the range $1 \leq k \leq \ell - 1$, computes $\gamma = \rho(\alpha^k) \in \mathbb{F}_q^m$ and $\delta = \rho(M\psi(P_A)^k) \in \mathbb{F}_q^m$, and sends the ciphertext (γ, δ) to Alice.
3. **Decryption:** Alice computes $M = \psi(\delta)\psi(\gamma)^{-a}$.

Signature scheme (torus-based ElGamal signatures):

1. **Key Generation:** Alice chooses a random integer a in the range $1 \leq a \leq \ell - 1$ as her private key. Her public key is $P_A := \rho(\alpha^a) \in \mathbb{F}_q^m$. The system requires a public cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/\ell\mathbb{Z}$.
2. **Signature Generation:** Alice selects a random integer k in the range $1 \leq k \leq \ell - 1$, computes $\gamma = \rho(\alpha^k) \in \mathbb{F}_q^m$ and $\delta = k^{-1}(H(M) - aH(\gamma)) \pmod{\ell}$. Alice's signature on the message M is the pair (γ, δ).
3. **Verification:** Bob accepts Alice's signature (γ, δ) on M if and only if
$$\psi(P_A)^{H(\gamma)}\psi(\gamma)^\delta = \alpha^{H(M)}$$
in T_n.

The torus-based encryption scheme is the generalized ElGamal protocol (see p. 297 of [9]) applied to T_n, and the torus-based signature scheme is the generalized ElGamal signature scheme (see p. 458 of [9]) for the group T_n, where the maps ρ and ψ are used to go back and forth between the group law on T_n and the compact representation in $\mathbb{F}_q^m$.

Diffie-Hellman and ElGamal fail when any of the computed quantities is 1 or a small power of the generator, and RSA fails when one obtains something that is not relatively prime to the modulus. Similarly, a torus-based cryptosystem fails when one tries to apply ρ or ψ to a point where the map is not defined. Since there are very few such points (none for T_2 and only two for T_6 in the examples in §5), the probability of this occurring is negligible, and can ignored (or such points can be checked for and discarded). Lemma 7 shows that torus-based cryptosystems have exactly the same security as that of a multiplicative group $\mathbb{F}_{q^n}^\times$, and an attack on a T_n-cryptosystem gives an attack on an $\mathbb{F}_{q^n}^\times$.

Note that the shared key sizes for key agreement, the public key and ciphertext sizes for encryption, and the public key sizes for the signature schemes are all $\varphi(n)/n$ as long as those for the corresponding classical schemes, for the same security. Further, torus-based signatures have $\varphi(n)\log(q) + \log(\ell)$ bits, while the corresponding classical ElGamal signature scheme with the same security using a subgroup of order ℓ has $n\log(q) + \log(\ell)$ bit signatures.

The CEILIDH key exchange, encryption, and signature schemes are the above protocols with $n = 6$ and with ρ and ψ as in §5.1. Note that $\Phi_6(q) = q^2 - q + 1$ and $m = 2$, and q and ℓ can be chosen as in XTR.

The T_2 key exchange, encryption, and signature schemes are the above protocols with $n = 2$ and with ρ and ψ as in §5.2. However, we obtain an extra savings in the T_2 case, since there is no need to go back and forth between T_2 and $\mathbb{F}_q$ using the functions ρ and ψ. Using (6), all the group computations can be done directly and simply in $\mathbb{F}_q$, rather than in the group $T_2(\mathbb{F}_q)$.

The T_n cryptosystem uses the above protocols, whenever we have an n for which the torus T_n has an explicit and efficiently computable rational parametrization ρ and inverse map ψ. Conjecture 9 states that for every n, the torus T_n is rational. This is most interesting in the case $n = 30 = 2 \cdot 3 \cdot 5$, where $n/\varphi(n) = 3\frac{3}{4}$, but might also be of interest when $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$, where $n/\varphi(n) = 4\frac{3}{8}$. An explicit rational parametrization of the 8-dimensional torus T_{30} (analogous to the maps ρ and ψ of the CEILIDH and T_2 systems) would allow us to represent elements of $T_{30}(\mathbb{F}_q)$ by 8 elements of $\mathbb{F}_q$.

7 Understanding LUC, XTR, and "Beyond" in Terms of Tori

The Lucas-based systems, the cubic field system in [5], and XTR have the security of $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, and $\mathbb{F}_{p^6}$, respectively, while representing elements in $\mathbb{F}_p$, $\mathbb{F}_p^2$, and $\mathbb{F}_{p^2}$, respectively. However, unlike the above torus-based systems, they do not make full use of the field multiplication. Here, we give a conceptual framework that explains why. We interpret these schemes in terms of varieties that are quotients of tori, and compare these schemes to the torus-based schemes of §3.

Consider two cases: $n = 2$ (the LUC case) and $n = 6$ (the XTR case). (It is straightforward to do the cubic case of [5] similarly.) Let F be $\mathbb{F}_q$ in the LUC case and $\mathbb{F}_{q^2}$ in the XTR case. Let $t = [\mathbb{F}_{q^n} : F]$, so $t = 2$ for LUC and $t = 3$ for XTR. In LUC and XTR, instead of $g \in G_{q,n}$ one considers the trace

$$Tr(g) := Tr_{\mathbb{F}_{q^n}/F}(g) \in F,$$

where the trace is the sum of the conjugates. One can show that for $g \in G_{q,n}$, the trace $Tr(g)$ determines the entire characteristic polynomial of g over F. In other words, knowing the trace of g is equivalent to knowing its unordered set of conjugates (but not the conjugates themselves). Let

$$C_g = \{g^\tau : \tau \in \mathrm{Gal}(\mathbb{F}_{q^n}/F)\},$$

the set of Galois conjugates of g.

Given a set $C = \{c_1, \ldots, c_t\} \subset \mathbb{F}_{q^n}$, let $C^{(j)} = \{c_1^j, \ldots, c_t^j\}$. If $C = C_g$, then $C^{(j)} = C_{g^j}$. In place of exponentiation ($g \mapsto g^j$), the XTR and LUC systems compute $Tr(g^j)$ from $Tr(g)$. In the above interpretation, they compute C_{g^j} from C_g, without needing to distinguish between the elements of C_g.

On the other hand, given sets of conjugates $\{g_1, \ldots, g_t\}$ and $\{h_1, \ldots, h_t\}$, it is not possible (without additional information) to multiply them to produce a new set of conjugates, because we do not know if we are looking for $C_{g_1h_1}$, or

$C_{g_1h_2}$, for example, which will be different. Therefore, XTR and LUC do not have straightforward multiplication algorithms.

However, XTR includes a partial multiplication algorithm (see Algorithm 2.4.8 of [7]). Given $Tr(g)$, $Tr(g^{j-1})$, $Tr(g^j)$, $Tr(g^{j+1})$, and a and b, the algorithm outputs $Tr(g^{a+bj})$. Thus for an XTR-based system, any transmission of data that needs to be multiplied requires sending three times as much data, effectively negating the improvement of $3 = 6/\varphi(6)$ that comes from XTR's compact representation. An analogous situation holds true for the signature scheme LUCELG DS in [16].

The CEILIDH system, since its operations take place in the group $G_{q,6}$, can do both multiplication and exponentiation, while taking full advantage of the compact representation for transmitting data. In particular, XTR-ElGamal encryption is key exchange followed by symmetric encryption with the shared key, while CEILIDH has full-fledged ElGamal encryption and signature schemes.

In the torus-based systems above, the information being exchanged is (a compact representation of) an element of a torus T_n. Further, the computations that are performed are multiplications in this group. We will see below that for XTR, the information being exchanged corresponds to an element of the quotient of T_6 by a certain action of the symmetric group on three letters, S_3. Similarly for LUC, the elements being exchanged correspond to elements of T_2/S_2. The set of equivalence classes T_6/S_3 is not a group, because multiplication in T_6 does not preserve S_3-orbits. This explains why XTR does not have a straightforward way to multiply. However, exponentiation in T_6 *does* preserve S_3-orbits, and it induces a well-defined exponentiation in T_6/S_3, and therefore in the set of XTR traces (the set $\mathrm{XTR}(q)$ defined below).

What XTR takes advantage of is the fact that the quotient variety T_6/S_3 is rational, and the trace map to the quadratic subfield gives an explicit rational parametrization. This rational parametrization embeds T_6/S_3 in $\mathbb{A}^2$, as shown in Theorem 13 below, and therefore gives a compact representation of T_6/S_3.

Let $k = \mathbb{F}_q$, $L = \mathbb{F}_{q^6}$, and $F = \mathbb{F}_{q^2}$. If G is a group and V is a variety, then G acts on $\oplus_{\gamma \in G} V$ by permuting the factors. We have

$$\mathrm{Res}_{L/k}\mathbb{G}_m \xrightarrow{\sim} \bigoplus_{\gamma \in \mathrm{Gal}(L/k)} \mathbb{G}_m \xrightarrow{\sim} \Big(\bigoplus_{\gamma \in \mathrm{Gal}(F/k)} \mathbb{G}_m\Big)^3 \tag{7}$$

where the first isomorphism is defined over L and preserves the action of the Galois group $\mathrm{Gal}(L/k)$ on both sides. The symmetric group S_3 acts naturally on $(\oplus_{\gamma \in \mathrm{Gal}(F/k)}\mathbb{G}_m)^3$. Pulling back this action via the above composition defines an action of S_3 on $\mathrm{Res}_{L/k}\mathbb{G}_m$ that preserves the torus $T_6 \subset \mathrm{Res}_{L/k}\mathbb{G}_m$. The quotient map $T_6 \to T_6/S_3$ induces a (non-surjective) map on k-points $T_6(k) \to (T_6/S_3)(k)$. Let

$$\mathrm{XTR}(q) = \{Tr_{L/F}(\alpha) : \alpha \in T_6(k)\} \subset F,$$

the set of traces used in XTR.

Theorem 13 *The set* $\mathrm{XTR}(q)$ *can be naturally identified with the image of* $T_6(k)$ *in* $(T_6/S_3)(k)$*. More precisely, there is a birational embedding*

$$T_6/S_3 \hookrightarrow \mathrm{Res}_{F/k}\mathbb{A}^1 \cong \mathbb{A}^2$$

such that $\mathrm{XTR}(q)$ *is the image of the composition*

$$T_6(k) \longrightarrow (T_6/S_3)(k) \hookrightarrow (\mathrm{Res}_{F/k}\mathbb{A}^1)(k) \cong F.$$

Proof. Let $k = \mathbb{F}_q$, $L = \mathbb{F}_{q^6}$, and $F = \mathbb{F}_{q^2}$. We have a commutative diagram (see (7))

$$\begin{tikzcd} T_6 \arrow[r, hook] & \mathrm{Res}_{L/k}\mathbb{G}_m \arrow[r, hook] & \mathrm{Res}_{L/k}\mathbb{A}^1 \arrow[r, "\sim"] \arrow[d, "Tr_{L/F}"] & \Big(\bigoplus_{\gamma\in\mathrm{Gal}(F/k)} \mathbb{A}^1\Big)^3 \arrow[d] \\ & & \mathrm{Res}_{F/k}\mathbb{A}^1 \arrow[r, "\sim"] & \bigoplus_{\gamma\in\mathrm{Gal}(F/k)} \mathbb{A}^1 \end{tikzcd} \tag{8}$$

where the top and bottom isomorphisms are defined over L and F, respectively, and the right vertical map is the "trace" map $(\alpha_1, \alpha_2, \alpha_3) \mapsto \alpha_1 + \alpha_2 + \alpha_3$.

The morphism $Tr_{L/F} : \mathrm{Res}_{L/k}\mathbb{A}^1 \to \mathrm{Res}_{F/k}\mathbb{A}^1$ of (8) factors through the quotient $(\mathrm{Res}_{L/k}\mathbb{A}^1)/S_3$, so by restriction it induces a morphism $Tr : T_6/S_3 \to \mathrm{Res}_{F/k}\mathbb{A}^1$. By definition $\mathrm{XTR}(q)$ is the image of the composition $T_6(k) \to (T_6/S_3)(k) \to (\mathrm{Res}_{F/k}\mathbb{A}^1)(k) \cong F$, and T_6 and $\mathrm{Res}_{F/k}\mathbb{A}^1$ are both 2-dimensional varieties, so to prove the theorem we need only show that $Tr : T_6/S_3 \to \mathrm{Res}_{F/k}\mathbb{A}^1$ is injective. Suppose $g \in T_6(\bar{k})$. Using (7) we can view $g = (g_1, g_2, g_3) \in (\oplus_{\gamma\in\mathrm{Gal}(F/k)}\bar{k}^\times)^3$. Let σ be the non-trivial element of $\mathrm{Gal}(F/k)$. Since $g \in T_6(\bar{k})$, we have $g_1g_2g_3 = N_{L/F}(g) = 1$ and $g_i g_i^\sigma = 1$ for $i = 1, 2, 3$ by the definition of T_6. Hence we also have

$$g_1g_2 + g_1g_3 + g_2g_3 = 1/g_3 + 1/g_2 + 1/g_1 = g_3^\sigma + g_2^\sigma + g_1^\sigma = Tr(g)^\sigma.$$

Thus the trace of g determines all the symmetric functions of $\{g_1, g_2, g_3\}$. Hence if $h = (h_1, h_2, h_3) \in T_6(\bar{k})$ and $Tr(h) = Tr(g)$, then $\{h_1, h_2, h_3\} = \{g_1, g_2, g_3\}$, i.e., h and g are in the same orbit under the action of S_3. Thus Tr is injective.

Similarly for LUC, the trace map induces a birational embedding $T_2/S_2 \hookrightarrow \mathbb{A}^1$, the variety T_2/S_2 is not a group, and

$$\mathrm{LUC}(q) = \{Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) : \alpha \in T_2(k)\} \subset \mathbb{F}_q$$

is the image of $T_2(\mathbb{F}_q)$ under the trace map $T_2 \to T_2/S_2 \hookrightarrow \mathbb{A}^1$.

7.1 Beyond XTR

As in [2] and §2 above, let $n = de$. Assume that n is square-free, and let $k = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$, and $F = \mathbb{F}_{q^d}$. We have

$$T_n \subset \mathrm{Res}_{L/k}\mathbb{G}_m \xrightarrow{\sim} \bigoplus_{\gamma\in\mathrm{Gal}(L/k)} \mathbb{G}_m \xrightarrow{\sim} \Big(\bigoplus_{\gamma\in\mathrm{Gal}(F_\ell/k)} \mathbb{G}_m\Big)^\ell \xrightarrow{\sim} \Big(\bigoplus_{\gamma\in\mathrm{Gal}(F/k)} \mathbb{G}_m\Big)^e$$

where the first isomorphism is defined over L and preserves the action of the Galois group $\mathrm{Gal}(L/k)$ on both sides, ℓ is any prime divisor of n, and $F_\ell = \mathbb{F}_{q^{n/\ell}}$. The symmetric group S_e acts naturally on $(\oplus_{\gamma \in \mathrm{Gal}(F/k)} \mathbb{G}_m)^e$. Pulling back this action via the above composition defines an action of S_e on $\mathrm{Res}_{L/k}\mathbb{G}_m$. Note that this action does not necessarily preserve the torus T_n. Similarly, S_ℓ acts naturally on $(\oplus_{\gamma \in \mathrm{Gal}(F_\ell/k)} \mathbb{G}_m)^\ell$. Since $N_{L/F_\ell}(g) = 1$ for every $g \in T_n$, it follows that T_n is in fact fixed under the induced action of S_ℓ.

Definition 14 Let $B_{(d,e)}$ denote the image of T_n in $(\mathrm{Res}_{L/k}\mathbb{G}_m)/S_e$.

If the variety $B_{(d,e)}$ is rational, then one can do cryptography. For example, this was done for the cases $(d,e) = (6,1)$ and $(2,1)$ in this paper (CEILIDH and T_2, respectively), for $(1,2)$ in the LUC papers, and for $(2,3)$ in XTR. Note that $(1,1)$ gives the usual Diffie-Hellman. Our (conjectural when n is a product of more than two primes) T_n cryptosystems are the cases $(n,1)$, and [2] discusses the cases $(d,e) = (1,30)$ and $(2,15)$. The variety $B_{(d,e)}$ is not generally a group. However, when $e = 1$, then $B_{(d,e)} = T_n$ which is a group.

Theorem 3.7 of [13] shows that the variety $B_{(d,e)}$ is birationally isomorphic to the quotient of T_n by the action of $\prod_{\text{primes } \ell \mid e} S_\ell$. Thus, the conjectures in [2] can be interpreted in this language as asking about the rationality of the varieties $T_{30}/(S_3 \times S_5)$ and $T_{30}/(S_2 \times S_3 \times S_5)$, and asking in particular if the morphisms from $B_{(1,30)}$ (resp., $B_{(2,15)}$) to $\mathbb{A}^8$ induced by the first $8/d$ (for $d = 1$ or 2, respectively) symmetric functions for the field extension L/F define rational parametrizations. We saw in §2 that these symmetric functions do not generate the coordinate ring of $B_{(1,30)}$ (resp., $B_{(2,15)}$).

The definitions in §3 can be easily extended to apply to an arbitrary cyclic extension L/k, not necessarily of finite fields. In particular, for $k = \mathbb{Q}$ and L a cyclic degree 30 extension of $\mathbb{Q}$, consider the above morphisms from characteristic zero versions of $B_{(1,30)}$ and $B_{(2,15)}$ to $\mathbb{A}^8$. We show in [13] that these maps are not birational, and (by reducing mod p) that for all but finitely many primes p, Conjecture $(p,1,30)$-$\mathbf{BPV}'$ (resp., Conjecture $(p,2,15)$-$\mathbf{BPV}'$) is false (see Remark 4 above).

References

1. D. Bleichenbacher, W. Bosma, A. K. Lenstra, *Some remarks on Lucas-based cryptosystems*, in Advances in cryptology — CRYPTO '95, Lect. Notes in Comp. Sci. **963**, Springer, Berlin, 1995, 386–396.
2. W. Bosma, J. Hutton, E. R. Verheul, *Looking beyond XTR*, in Advances in Cryptology — Asiacrypt 2002, Lect. Notes in Comp. Sci. **2501**, Springer, Berlin, 2002, 46–63.
3. A. E. Brouwer, R. Pellikaan, E. R. Verheul, *Doing more with fewer bits*, in Advances in Cryptology — Asiacrypt '99, Lect. Notes in Comp. Sci. **1716**, Springer, Berlin, 1999, 321–332.
4. N. G. de Bruijn, *On the factorization of cyclic groups*, Nederl. Akad. Wetensch. Proc. Ser. A **56** (= Indagationes Math. **15**) (1953), 370–377.

5. G. Gong, L. Harn, *Public-key cryptosystems based on cubic finite field extensions*, IEEE Trans. Inform. Theory **45** (1999), 2601–2605.
6. 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).
7. 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.
8. A. K. Lenstra, E. R. Verheul, *An overview of the XTR public key system*, in Public-key cryptography and computational number theory (Warsaw, 2000), de Gruyter, Berlin, 2001, 151–180.
9. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of applied cryptography, CRC Press, Boca Raton, FL, 1997.
10. W. B. Müller, W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. **16** (1981), 71–76.
11. T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. **74** (1961), 101–139.
12. 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.
13. K. Rubin, A. Silverberg, *Algebraic tori in cryptography*, to appear in High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications Series, American Mathematical Society, Providence, RI.
14. I. J. Schoenberg, *A note on the cyclotomic polynomial*, Mathematika **11** (1964), 131–136.
15. 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.
16. 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.
17. V. E. Voskresenskii, Algebraic groups and their birational invariants, Translations of Mathematical Monographs **179**, American Mathematical Society, Providence, RI, 1998.
18. V. E. Voskresenskii, *Stably rational algebraic tori*, Les XXèmes Journées Arithmétiques (Limoges, 1997), J. Théor. Nombres Bordeaux **11** (1999), 263–268.
19. A. Weil. Adeles and algebraic groups. Progress in Math. **23**, Birkhäuser, Boston (1982).
20. H. C. Williams, *A $p+1$ method of factoring*, Math. Comp. **39** (1982), 225–234.
21. H. C. Williams, *Some public-key crypto-functions as intractable as factorization*, Cryptologia **9** (1985), 223–237.