Using primitive subgroups to do more with fewer bits

K. Rubin[1⋆] and A. 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. This paper gives a survey of some ways to improve the efficiency of discrete log-based cryptography by using the restriction of scalars and the geometry and arithmetic of algebraic tori and abelian varieties.

1 Introduction

This paper is a survey, intended to be readable by both mathematicians and cryptographers, of some of the results in [24–26], along with a new result in §3.6. It can be viewed as a sequel to the Brouwer-Pellikaan-Verheul paper "Doing more with fewer bits" [8].

The overall objective is to provide greater efficiency for the same security. The idea is to shorten transmissions by a factor of $\frac{n}{\varphi(n)}$, by going from a finite field $\mathbb{F}_q$ up to the larger field $\mathbb{F}_{q^n}$, and using "primitive subgroups". Here, $\varphi(n)$ is the Euler φ-function. Note that $n/\varphi(n)$ goes to infinity (very slowly), as n goes to infinity.

The first goal is to obtain the same security as the classical Diffie-Hellman and ElGamal cryptosystems, while sending shorter transmissions. More precisely, the goal is to do discrete log-based cryptography, relying on the security of $\mathbb{F}_{q^n}^\times$, while transmitting only $\varphi(n)$ elements of $\mathbb{F}_q$, instead of n elements of $\mathbb{F}_q$ (i.e., one element of $\mathbb{F}_{q^n}$). We use algebraic tori. The next goal is to improve pairing-based cryptosystems. Here, we use elliptic curves E and primitive subgroups of $E(\mathbb{F}_{q^n})$.

As pointed out by Dan Bernstein, the techniques discussed here can be viewed as "compression" techniques, adding more flexibility for the user, who might

⋆ Rubin was partially supported by NSF grant DMS-0140378.
⋆⋆ Silverberg thanks NSA for support, and the ANTS VI organizers for inviting her to speak.

choose to send compressed information when the network is the bottleneck and uncompressed information when computational power is the bottleneck.

In §2 we discuss some background and past results on compressing the transmissions in discrete log-based cryptography for the multiplicative group. In §3 we give an exposition of torus-based cryptography; we give a new implementation of CEILIDH in §3.6. In §4 we show how to compress the transmissions in pairing-based cryptosystems. In §5 we discuss some of the underlying mathematics, including an elementary introduction to the Weil restriction of scalars; we define "primitive subgroup" in §5.5. In §6 we discuss the mathematics underlying torus-based cryptography, and interpret some earlier systems in terms of quotients of algebraic tori.

For technical details, see the original papers. See also [11] (especially §3.2) for the use of primitive subgroups in cryptography.

Acknowledgments: The authors thank Dan Bernstein, Steven Galbraith, and Paul Leyland for helpful comments on a draft of the paper.

2 Some background

We first recall the classical Diffie-Hellman key agreement scheme [10, 21].

2.1 Classical Diffie-Hellman

In classical Diffie-Hellman key agreement, a large finite field $\mathbb{F}_q$ is public ($q \approx 2^{1024}$), as is an element $g \in \mathbb{F}_q^\times$ of large (public) multiplicative order ℓ ($> 2^{160}$). Alice chooses a private integer a, random in the interval between 1 and $\ell - 1$, and Bob similarly chooses a private integer b.

- Alice sends g^a to Bob.
- Bob sends g^b to Alice.
- They share $g^{ab} = (g^a)^b = (g^b)^a$.

Tautologically, the security is based on the difficulty of the Diffie-Hellman Problem in $\mathbb{F}_q^\times$.

Note that when this is performed using $\mathbb{F}_{q^n}$ in place of $\mathbb{F}_q$, then the transmissions are elements of $\mathbb{F}_{q^n}$ (i.e., n elements of $\mathbb{F}_q$). If one can do Diffie-Hellman transmitting only $\varphi(n)$ elements of $\mathbb{F}_q$ while relying on security coming from $\mathbb{F}_{q^n}^\times$, then one would like to have $n\log(q)$ large for high security, and $\varphi(n)\log(q)$ small for high bandwidth efficiency. In particular, for maximal efficiency per unit of security (i.e., to achieve a system that is $\frac{n}{\varphi(n)}$ times as efficient as Diffie-Hellman), one would like $\frac{n}{\varphi(n)}$ to be as large as possible. Thus, the most useful n's to consider are those in the sequence

$$1, \quad 2, \quad 2 \cdot 3 = 6, \quad 2 \cdot 3 \cdot 5 = 30, \quad 2 \cdot 3 \cdot 5 \cdot 7 = 210, \quad \ldots$$

(whose i-th entry is the product of the first $i - 1$ primes). We will discuss some ways to do this, below.

2.2 A brief tour of some history

As noted in [17, 8], one can achieve greater efficiency per unit of security by choosing g in the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$, where $\Phi_n(x)$ is the n-th cyclotomic polynomial. (The polynomial $\Phi_n(x)$ has integer coefficients, and its (complex) roots are the primitive n-th roots of unity.)

Diffie-Hellman key agreement is based on the full multiplicative group $\mathbb{F}_q^\times$, which is a group of order $q-1 = \Phi_1(q)$.

In [22, 31, 32, 28, 29, 25], analogues of the classical Diffie-Hellman key agreement scheme are introduced that rely on the security of $\mathbb{F}_{p^2}^\times$ while transmitting only one element of $\mathbb{F}_p$. One now takes the element g to lie in the subgroup of $\mathbb{F}_{p^2}^\times$ of order $p+1$ $(= \Phi_2(p))$. Since $n = 2$, we have $n/\varphi(n) = 2$, and achieve twice the efficiency of Diffie-Hellman for comparable security. The papers [22, 31, 32, 28, 29] use Lucas sequences [20], to give what are known as Lucas-based cryptosystems. See [4] for a critique of [28, 29]. In [25] (see §3.4 below) we introduced the $\mathbb{T}_2$-cryptosystem,

which is a torus-based system. It is related to the Lucas-based cryptosystems (see §6.5 below), and has some advantages over them.

The Gong-Harn system [13] uses linear feedback shift register sequences. In this case $n = 3$, so $n/\varphi(n) = 1.5$. This cryptosystem relies on the security of $\mathbb{F}_{p^3}^\times$ while transmitting only two elements of $\mathbb{F}_p$, using the subgroup of $\mathbb{F}_{p^3}^\times$ of order $p^2 + p + 1$ $(= \Phi_3(p))$.

The case where $n = 6$ (so $n/\varphi(n) = 3$) is considered in [8], [19] (the XTR system), and [25] (the CEILIDH system). These systems give three times the efficiency of Diffie-Hellman, for the same security. They rely on the security of $\mathbb{F}_{p^6}^\times$ while transmitting only two elements of $\mathbb{F}_p$, using the subgroup of $\mathbb{F}_{p^6}^\times$ of order $p^2 - p + 1$ $(= \Phi_6(p))$.

Arjen Lenstra [18] has asked whether one can use $n = 30$ to do better than XTR. Note that $\varphi(30) = 8$ and

$$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$$

Building on a conjecture in [8], conjectures for arbitrary n were given in [6]. Those conjectures were disproved in [6, 25, 26], and it was proposed in [25, 26] that a conjecture of Voskresenskii should replace those conjectures.

2.3 Classical ElGamal encryption

As before, the public information is a large finite field $\mathbb{F}_q$ and an element $g \in \mathbb{F}_q^\times$ of order ℓ, along with q and ℓ.
Alice's private key: an integer a, random in the interval $[1, \ell - 1]$
Alice's public key: $P_A = g^a \in \mathbb{F}_q$

- Bob represents the message M in $\langle g \rangle$ and chooses a random integer r between 1 and $\ell - 1$. Bob send Alice the ciphertext (c, d) where $c = g^r$ and $d = M \cdot P_A^r$.
- To decrypt a ciphertext (c, d), Alice computes

$$d \cdot c^{-a} = M \cdot (g^a)^r \cdot (g^r)^{-a} = M.$$

2.4 Classical ElGamal signatures

With public information as before, also fix a public cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/\ell\mathbb{Z}$ (i.e., H takes bit strings to integers modulo ℓ, is easy to compute and hard to invert, and its images look "random").
Alice's private key: an integer a, random in the interval $[1, \ell - 1]$
Alice's public key: $P_A = g^a \in \mathbb{F}_q$

- 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 $c = g^r$ and $d = r^{-1}(H(M) - aH(g^r)) \pmod{\ell}$.
- Bob accepts Alice's signature if and only if

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

  in the field $\mathbb{F}_q$.

Remark 1 Note that Diffie-Hellman key agreement only requires exponentiations (i.e., computing powers of elements in the group generated by g), while the ElGamal encryption and signature schemes require multiplications in the finite field (i.e., $M \cdot P_A^r$, $c^{-a} \cdot d$, and $P_A^{H(c)} \cdot c^d$).

2.5 Using XTR to illustrate the idea

We give an illustration, in the case $n = 6$, of the idea behind [8, 13, 19] and the Lucas-based cryptosystems.

XTR is short for ECSTR, which stands for *Efficient Compact Subgroup Trace Representation*.

The *trace* is the trace map from $\mathbb{F}_{p^6}$ to $\mathbb{F}_{p^2}$, which is defined by

$$\mathrm{Tr}(h) = h + h^{p^2} + h^{p^4} = h + \sigma(h) + \sigma^2(h),$$

where σ generates the Galois group $\mathrm{Gal}(\mathbb{F}_{p^6}/\mathbb{F}_{p^2})$. (Note that $h^{p^6} = h$.)

The *subgroup* is the subgroup of $\mathbb{F}_{p^6}^\times$ of order $p^2 - p + 1 = \Phi_6(p)$. Choose a generator g of this subgroup.

- Alice sends $\mathrm{Tr}(g^a)$ to Bob.
- Bob sends $\mathrm{Tr}(g^b)$ to Alice.
- They share $\mathrm{Tr}(g^{ab})$.

Since the transmissions are elements of $\mathbb{F}_{p^2}$, Alice and Bob are sending 2 ($= \varphi(6)$) elements of $\mathbb{F}_p$, rather than 6 elements of $\mathbb{F}_p$ (i.e., one element of $\mathbb{F}_{p^6}$, as would be the case in classical Diffie-Hellman over the field $\mathbb{F}_{p^6}$). The point is that the trace gives an *efficient compact representation* of elements in the subgroup $\langle g \rangle$.

We claim that Alice and Bob now share $\mathrm{Tr}(g^{ab}) \in \mathbb{F}_{p^2}$. This is proved in [19], where an efficient way to compute $\mathrm{Tr}(g^{ab})$ is given. Let's convince ourselves that

Alice and Bob really do have enough information to compute $\mathrm{Tr}(g^{ab})$. Suppose that h is an element of the subgroup of $\mathbb{F}_{p^6}^{\times}$ of order $p^2 - p + 1$. Let

$$C_h = \{h, \sigma(h), \sigma^2(h)\}.$$

The three elementary symmetric polynomials of the set C_h are:

$$\begin{aligned}
\Pi_1(C_h) &= h + \sigma(h) + \sigma^2(h) = \mathrm{Tr}(h), \\
\Pi_2(C_h) &= h \cdot \sigma(h) + h \cdot \sigma^2(h) + \sigma(h) \cdot \sigma^2(h) = \mathrm{Tr}(h \cdot \sigma(h)), \\
\Pi_3(C_h) &= h \cdot \sigma(h) \cdot \sigma^2(h) = \mathrm{N}(h),
\end{aligned}$$

where $\mathrm{N} : \mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ is the norm map. It turns out that if h is in the subgroup of order $p^2 - p + 1$, then $\Pi_2(C_h) = \mathrm{Tr}(h)^p$ and $\Pi_3(C_h) = 1$.

Thus, knowing $\mathrm{Tr}(h)$ is equivalent to knowing the values of all the elementary symmetric polynomials of C_h, which is equivalent to knowing the set C_h. However, if you know C_h and you know a, then you know C_{h^a}, just by taking every element of C_h to the power a. But we have already noted that knowing C_{h^a} is equivalent to knowing $\mathrm{Tr}(h^a)$.

To sum up, if h is in the subgroup of $\mathbb{F}_{p^6}^{\times}$ of order $p^2 - p + 1$, then a and $\mathrm{Tr}(h)$ together determine $\mathrm{Tr}(h^a)$. Since Alice knows $\mathrm{Tr}(g^b)$ and a, she has enough information to compute $\mathrm{Tr}((g^b)^a)$, and similarly Bob can compute $\mathrm{Tr}((g^a)^b)$.

Note that knowing C_h is equivalent to knowing the characteristic polynomial of h over $\mathbb{F}_{p^2}$, since that characteristic polynomial is

$$\prod_{c \in C_h} (X - c) = X^3 - \Pi_1(C_h)X^2 + \Pi_2(C_h)X - \Pi_3(C_h).$$

Remark 2 In XTR [19], the Gong-Harn system [13], and the Lucas-based cryptosystems, Alice can compute $f(g^{ab})$ from $f(g^b)$ and a, for a suitable function f (usually a trace). In other words, these cryptosystems can exponentiate, as is needed for doing (analogues of) Diffie-Hellman. However, they cannot multiply in a straightforward way. If you know $\mathrm{Tr}(g)$ and $\mathrm{Tr}(h)$, that does not give you enough information to compute $\mathrm{Tr}(gh)$, since C_g and C_h do not determine the set C_{gh} (knowing only C_g and C_h, you do not have enough information to distinguish C_{gh} from $C_{g \cdot \sigma(h)}$, for example). These are examples of "lossy" compression. If one orders the conjugates of h and transmits a couple of extra bits to specify which conjugate h is, then one can reconstruct h from $\mathrm{Tr}(h)$, and perform multiplications in $\mathbb{F}_{p^6}$.

3 Torus-Based Cryptography

The goal is to find a computable function f satisfying the following properties:

- the number of bits needed to represent $f(h)$ is less than the number of bits needed to represent h (ideally, $f(h)$ is $\frac{\varphi(n)}{n}$ as long as h),

- $f(h)$ and a determine $f(h^a)$ and h^a,
- $f(g)$ and $f(h)$ determine $f(gh)$ and gh,
- f is defined on almost all elements of the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$.

Note that these conditions imply that f has a computable inverse function.

From now on, fix a square-free integer n and a prime power q. (Square-free means that the only square that divides n is 1.)

Definition 3 Let T_n denote the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$.

Example 4 (i) Diffie-Hellman is based on the group $T_1 = \mathbb{F}_q^\times$.
(ii) If q is not a power of 2, one can write $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{d})$. Then

$$\begin{aligned} T_2 &= \{a + b\sqrt{d} : a, b \in \mathbb{F}_q \text{ and } (a + b\sqrt{d})^{q+1} = 1\} \\ &= \{a + b\sqrt{d} : a, b \in \mathbb{F}_q \text{ and } a^2 - db^2 = 1\} \subset \mathbb{F}_{q^2}^\times, \end{aligned}$$

since $(a + b\sqrt{d})^q = a - b\sqrt{d}$.

Choose a prime power q of about $1024/n$ bits, such that $\Phi_n(q)$ is divisible by a large prime. Choose $g \in T_n$ whose order ℓ is divisible by that large prime. Suppose for now that one has efficiently computable maps

$$\mathbb{F}_q^{\varphi(n)} \underset{f}{\overset{j}{\rightleftarrows}} T_n \tag{1}$$

that are inverses of each other. The dotted arrows signify that these maps need not be defined everywhere; they might be undefined at a "small" number of elements. In §3.4, §3.6, §6.3, and [25] we discuss the maps f and j, and give explicit examples. The following protocols are generalized Diffie-Hellman and ElGamal [21], using the subgroup T_n of $\mathbb{F}_{q^n}^\times$. In §3.7 below we discuss how to represent the message in $\langle g \rangle$. Note that the maps f and j allow one to compress transmissions not only for Diffie-Hellman and ElGamal, but also for any discrete log-based system that can use a general group.

3.1 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 $f(g^{ab})$.

3.2 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 $M = j(d) \cdot j(c)^{-a}$.

3.3 Torus-based ElGamal signatures

Fix a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/\ell\mathbb{Z}$.
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 $\mathbb{F}_{q^n}$.

3.4 The $\mathbb{T}_2$-cryptosystem

Here, $n = 2$. Choose a prime power q that has about 512 bits, and such that $\frac{q+1}{2}$ is a prime. One can write $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{d})$ for some non-square $d \in \mathbb{F}_q^\times$. Define

$$j : \mathbb{F}_q \to T_2 \qquad \text{by} \qquad j(a) = \frac{a + \sqrt{d}}{a - \sqrt{d}}.$$

Define an inverse map (defined on $T_2 - \{1, -1\}$):

$$f : T_2 \dashrightarrow \mathbb{F}_q \qquad \text{by} \qquad f(a + b\sqrt{d}) = \frac{1 + a}{b}.$$

It is easy to check that if $a, b \in \mathbb{F}_q$ and $a \neq -b$, then

$$j(a)j(b) = j\big(\frac{ab + d}{a + b}\big).$$

In the $\mathbb{T}_2$-cryptosystem, one does Diffie-Hellman key agreement and ElGamal encryption and signatures, using the group law on the group T_2, while representing the elements in $\mathbb{F}_q$. Here, it is not necessary to go back and forth between $\mathbb{F}_q$ and T_2, since the previous equation translates T_2's multiplication to $\mathbb{F}_q$, i.e., multiplication in T_2 translates into the following operation on $\mathbb{F}_q$:

$$(a, b) \mapsto \frac{ab + d}{a + b},$$

giving a way to compose elements of $\mathbb{F}_q$ without having to pass to T_2 each time.

3.5 The CEILIDH public key system

The acronym **CEILIDH** (pronounced "cayley") 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 $n = 6$.

Examples 11 and 12 of [25] give explicit examples of maps f and j (called ρ and ψ there) when $n = 6$. We give a new example in §3.6 (and use it in §3.7).

3.6 An explicit example of maps f and j

Take an odd prime power q congruent to 2, 6, 7, or 11 (mod 13) and such that $\Phi_6(q)$ is prime. Then $\mathbb{F}_q(\zeta_{13}) \cong \mathbb{F}_{q^{12}}$, where ζ_{13} is a primitive 13-th root of unity, and $\mathbb{F}_q(z) \cong \mathbb{F}_{q^6}$, where $z = \zeta_{13} + \zeta_{13}^{-1}$. Let

$$y = \zeta_{13} + \zeta_{13}^{-1} + \zeta_{13}^{5} + \zeta_{13}^{-5} \in \mathbb{F}_{q^3}.$$

For $u, v \in \mathbb{F}_q$, define

$$j(u,v) = \frac{r - s\sqrt{13}}{r + s\sqrt{13}} \in T_6$$

where

$$r = (3(u^2+v^2) + 7uv + 34u + 18v + 40)y^2 + 26uy \\ - (21u(3+v) + 9(u^2+v^2) + 28v + 42),$$

$$s = 3(u^2+v^2) + 7uv + 21u + 18v + 14.$$

For $t \in T_6$, define

$$f(t) = \Big(\frac{u}{w+1}, \frac{v-3}{w+1}\Big) \in \mathbb{F}_q^2,$$

with

$$t = a + b\sqrt{13} \quad \text{and} \quad \frac{1+a}{b} = wy^2 + u\Big(y + \frac{y^2}{2}\Big) + v$$

where t is written with respect to the basis $\{1, \sqrt{13}\}$ for $\mathbb{F}_{q^6}/\mathbb{F}_{q^3}$, with a, $b \in \mathbb{F}_{q^3} = \mathbb{F}_q(y)$, and $\frac{1+a}{b}$ is written with respect to the basis $\{y^2, y + \frac{y^2}{2}, 1\}$ for $\mathbb{F}_{q^3}/\mathbb{F}_q$, with u, v, $w \in \mathbb{F}_q$.

Then f and j are inverses. The map $j : \mathbb{F}_q^2 \to T_6$ is defined on all of $\mathbb{F}_q^2$. The map $f : T_6 \dashrightarrow \mathbb{F}_q^2$ is defined except at 1 and $-2z^5 + 6z^3 - 4z - 1 \in T_6$.

3.7 Representing elements of $\mathbb{F}_q^{\varphi(n)}$ in $\langle g \rangle$

For torus-based ElGamal encryption, how does one represent a message as an element of $\langle g \rangle$? First, represent the message as an element M in $\mathbb{F}_q^{\varphi(n)}$.

If g is taken to be a generator of T_n, then taking $j(M)$ represents the message in $\langle g \rangle$ (where j is as in (1)). Note that g is a generator of T_n whenever $\Phi_n(q)$ is prime.

If g is taken to be in an index s subgroup of T_n for some small integer s, then by adding a few bits of redundancy to M, after at most a few tries one obtains an M such that $j(M)$ is in $\langle g \rangle$. If g has order ℓ, one can test whether $j(M)$ is in $\langle g \rangle$ by checking whether $j(M)^\ell = 1$.

How does one represent the message in $\langle g \rangle$ when $n = 6$?

Take a prime r and an odd prime power q such that the order of $q \pmod r$ is divisible by 6 but is not 6 itself, and such that $\Phi_6(q)$ is prime. (One expects, but cannot prove, that there are infinitely many such q; it is not hard to find some in a suitable range for cryptography, e.g., such that q has about 170 bits, to get 1024-bit security.) These conditions ensure that $\mathbb{F}_q(\zeta_r)$ contains $\mathbb{F}_{q^6}$, where ζ_r is a primitive r-th root of unity. (Note that if the order of $q \pmod r$ is 6, then $\Phi_6(q)$ is divisible by 6, so is not prime. Note also that the condition that the order of $q \pmod r$ is divisible by 6 implies that $r \equiv 1 \pmod 6$.) In the case $r = 13$, one can use the example given in §3.6. Here, one represents the message in $\mathbb{F}_q^2$, and uses the map j to put it in the prime order group $T_6 = \langle g \rangle$.

In Example 11 of [25], we have $q \equiv 2$ or $5 \pmod 9$. Here, $\Phi_6(q)$ is divisible by 3. One can choose the prime power q so that $\Phi_6(q)/3$ is prime. If one takes g to have order $\Phi_6(q)$, then $j(M)$ is in $\langle g \rangle = T_6$.

Similarly for Example 12 of [25], we have $q \equiv 3$ or $5 \pmod 7$. Now $\Phi_6(q)$ is divisible by 7. One can choose q so that $\Phi_6(q)/7$ is prime. If g is taken to have order $\Phi_6(q)$, then $j(M) \in \langle g \rangle = T_6$.

The following sample parameters are all the primes q between $2^{170} - 10^5$ and $2^{170} + 10^5$ such that $q^2 - q + 1$ is prime and q has order 12 modulo 13:

$$1496577676626844588240573268701473812127674923933621,$$
$$1496577676626844588240573268701473812127674923946773,$$
$$1496577676626844588240573268701473812127674923949251,$$
$$1496577676626844588240573268701473812127674924018047,$$
$$1496577676626844588240573268701473812127674924027533.$$

3.8 Comparison between CEILIDH and XTR

The security of CEILIDH is exactly the same as that of XTR, with the same security proof; they both rely on the security of the "hardest" subgroup of $\mathbb{F}_{q^6}^\times$ (see §3.11). Parameter selection for CEILIDH is exactly the same as for XTR.

The advantage of the $\mathbb{T}_2$-cryptosystem and CEILIDH over LUC and XTR is that $\mathbb{T}_2$ and CEILIDH make full use of the multiplication in the group T_n (for $n = 2$ and 6). This is especially useful for signature schemes. XTR is efficient for key agreement and hybrid encryption (i.e., using a Diffie-Hellman-like protocol to exchange a secret key, and using symmetric key encryption, not public key encryption). CEILIDH can do efficient key agreement, public key (i.e., non-hybrid) encryption, and signatures.

XTR has computational efficiency advantages over CEILIDH (key agreement can be performed with fewer operations).

3.9 Conjectural $\mathbb{T}_n$-cryptosystems

Whenever f and j exist as in (1), one has a "$\mathbb{T}_n$-cryptosystem", or $\mathbb{T}_n$ compression technique. As in §3.1–§3.3, use f to compactly represent transmissions in $\mathbb{F}_q^{\varphi(n)}$, and use j to send elements of $\mathbb{F}_q^{\varphi(n)}$ to the group T_n, where group operations can be performed.

3.10 Parameter selection when $n = 30$

For torus-based ElGamal signatures, finding good parameters when $n = 30$ amounts to finding prime powers q of about $1024/30 \approx 35$ bits such that $\Phi_{30}(q)$ has a prime factor ℓ of about 160 bits. Here is a method for doing this:

- choose a 20–30 bit prime $p \equiv 1 \pmod{30}$,
- find the $x_1, \ldots, x_8$ with $1 < x_i < p$ whose orders modulo p are 30,
- find 35-bit primes q congruent to some $x_i \pmod{p}$,
- factor out small ($<$ 90–100 bits) prime divisors from the integer $\Phi_{30}(q)/p$,
- see if what is left is a prime of about 160-bits.

Paul Leyland suggested doing the factorization step by using the Elliptic Curve Method optimized for 90 – 100 bit factors. Using this, he can obtain a few examples per hour on a laptop.

Note that the parameters are like Diffie-Hellman parameters — they do not need to be changed often, and the same q and g can be used for all users.

The table below gives some pairs of primes q and ℓ where q has 35 bits, ℓ has 160 or 161 bits, and ℓ divides $\Phi_{30}(q)$. One expects there to be about

$$717267168(\ln(161) - \ln(160)) \approx 4.47 \times 10^6$$

35-bit primes q such that $\Phi_{30}(q)$ has a 160-bit prime divisor (717267168 is the number of 35-bit primes).

q	ℓ
18849585563	272182927859864576322913555520387538121502585025 1
18859507111	114537755221368933480888080324760842570059669044 1
18918018433	219106745795716727328046841332619652274532411091 1
18937704077	262291755042381695663904065040214531479808197573 1
19020912667	200990794418851110984328610785636238856973693866 1
19096959863	267035151876706532221284669668629842146809482048 1
19123281371	108973197908118946508340328579176521332245379629 1
19200181867	138210800774622478229271644425457049475314218430 1
19241156549	129263193059394202841488838668457192230868038341 1

3.11 Security

The security of all the systems discussed thus far is the discrete log security of the "hardest" subgroup of $\mathbb{F}_{q^n}^\times$, in the following sense. The group $\mathbb{F}_{q^n}^\times$ is "almost the same" as the direct product

$$\prod_{d|n} T_d \quad = \quad T_n \times \prod_{\substack{d|n \\ d \neq n}} T_d$$

(there are homomorphisms between them for which the prime divisors of the orders of the kernel and cokernel all divide n); see pp. 60–61 of [30].

We have $T_d \subset \mathbb{F}_{q^d}^\times$ for all d, so for $d < n$ the elements of these subgroups lie in a strictly smaller field than $\mathbb{F}_{q^n}$. Therefore, these groups T_d are weaker for cryptographic purposes — they are vulnerable to attacks on the discrete logarithm problem in $\mathbb{F}_{q^d}^\times$, where now $d < n$.

Almost none of the elements of T_n lie in a smaller field than $\mathbb{F}_{q^n}$ (see Lemma 1 of [6]). Therefore, T_n can be viewed as the cryptographically strongest subgroup of $\mathbb{F}_{q^n}^\times$.

4 Improving Pairing-Based Cryptography

Inspired by and building on a paper of Galbraith [12], in [24] we use the theory of supersingular abelian varieties to improve the efficiency of pairing-based cryptosystems.

Pairing-based cryptography was conceived of independently by Joux [14] and by Sakai, Ohgishi, and Kasahara [27]. There are numerous applications of pairing-based cryptography, including tripartite Diffie-Hellman, identity-based encryption, and short signatures. See [1] for numerous references and information.

The Boneh-Lynn-Shacham (BLS) short signature scheme [5] uses pairings associated with elliptic curves. The question of whether one can use abelian varieties (which are higher dimensional generalizations of elliptic curves) to obtain shorter signatures was stated as an open problem in [5], and answered in the affirmative in [24]. While we arrived at our method (see §4.2 below) for compressing BLS signatures by studying the arithmetic of abelian varieties, in fact our final algorithm can be performed entirely using elliptic curve arithmetic, without going to higher dimensional abelian varieties.

The Rubin-Silverberg (RS) modification of the BLS signature scheme multiplies the security of BLS signatures by n while multiplying the signature size by $\varphi(n)$. Implementations when $n = 3$ and $n = 5$ are given in [24]. We give an example when $n = 5$ in §4.2 below.

Our methods can be used to improve the bandwidth efficiency of any pairing-based cryptosystem, not just the BLS signature scheme.

4.1 BLS short signature scheme

We give an example of the Boneh-Lynn-Shacham signature scheme, with fixed parameters.

Let $q = 3^{97}$. Consider the elliptic curve $E^+ : y^2 = x^3 - x + 1$ over $\mathbb{F}_q$, and take $P \in E^+(\mathbb{F}_q)$ of (prime) order

$$\ell = 27268651890582610107749607981349761871714627 21.$$

Note that $\#E^+(\mathbb{F}_q) = 7\ell$.

Use a pairing

$$e\colon \langle P\rangle \times \langle P\rangle \to \mathbb{F}_{q^6}^{\times}$$

that satisfies

$$e(aP, bP) = e(P, P)^{ab} \quad \text{for every } a, b \in \mathbb{Z},$$
$$e(P, P) \neq 1.$$

One can use a modified Weil or Tate pairing [15].

The public information is q, E^+, P, ℓ, e, and a cryptographic hash function

$$H\colon \{0,1\}^* \to \langle P\rangle.$$

Alice's private key: an integer a, random in the interval $[1, \ell]$
Alice's public key: $P_A = aP$

- To sign a message $M \in \{0,1\}^*$, Alice computes $P_M = H(M)$ and $aP_M = (s,t) \in \langle P\rangle$.
- Alice's signature is $s \in \mathbb{F}_q$ (and 1 bit to recover the sign of t).
- To verify the signature, Bob computes

$$t = \pm\sqrt{s^3 - s + 1} \in \mathbb{F}_q,$$

lets

$$P' = (s,t)\ (= aP_M),$$

and checks that

$$e(P, P') = e(P_A, P_M).$$

4.2 RS compression of BLS signatures

We give an example with fixed parameters, with $n = 5$. Let $q' = 3^{19}$ and let $q = (q')^5 = 3^{95}$. Consider the elliptic curve $E^- : y^2 = x^3 - x - 1$, and take $P \in E^-(\mathbb{F}_q)$ of (prime) order

$$\ell = 67332385860403367623388769605995 21.$$

Note that

$$\#E^-(\mathbb{F}_q) = 271 \cdot 1162320517 \cdot \ell,$$
$$\#E^-(\mathbb{F}_{3^5}) = 271, \qquad \#E^-(\mathbb{F}_{q'}) = 1162320517.$$

Take a pairing e and a hash function H as before. Let σ be a generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q'})$. For $Q \in E^-(\mathbb{F}_q)$,

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(Q) = Q + \sigma(Q) + \sigma^2(Q) + \sigma^3(Q) + \sigma^4(Q).$$

Let

$$A_0 = \{Q \in E^-(\mathbb{F}_q) : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(Q) = \mathcal{O}_{E^-}\},$$

the "trace-0 subgroup" of $E^-(\mathbb{F}_q)$. Then A_0 has order $271 \cdot \ell$. Since P has order ℓ, we have $P \in A_0$.
Alice's private key: an integer a, random in the interval $[1, \ell]$
Alice's public key: $P_A = aP$

- To sign M, as before, Alice computes $P_M = H(M)$ and $aP_M = (s, t)$.
- Letting $(s_0, s_1, s_2, s_3, s_4)$ be the coordinates of s with respect to a basis for $\mathbb{F}_q$ over $\mathbb{F}_{q'}$, Alice's signature is (s_1, s_2, s_3, s_4) (and 6 bits to recover s_0 and t).
- To verify the signature, Bob first uses that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(P) = \mathcal{O}_{E^-}$ to reconstruct s_0 (see below).
- Bob then, as before, computes

$$t = \pm\sqrt{s^3 - s - 1} \in \mathbb{F}_q,$$

lets

$$P' = (s, t) \ (= aP_M),$$

and checks that

$$e(P, P') = e(P_A, P_M).$$

The process of reconstructing s_0 and t from s_1, s_2, s_3, s_4 is as follows. The input is $(s_1, s_2, s_3, s_4) \in \mathbb{F}_{q'}^4$ and the output will be $s_0, t \in \mathbb{F}_{q'}$. Viewing $\mathbb{F}_q$ as $\mathbb{F}_{q'}(z)$ with $z^5 - z + 1 = 0$, let $c = S + \sum_{i=1}^4 s_i z^i$ and define $a_0, \cdots, a_4 \in \mathbb{F}_{q'}[S]$ by

$$\prod_{i=0}^{4}(Y - \sigma^i(c)) = Y^5 + a_4Y^4 + a_3Y^3 + a_2Y^2 + a_1Y + a_0.$$

The trace-0 condition can (eventually) be reduced to finding simultaneous solutions of $p_1 = 0$ and $p_2 = 0$, where p_1 and p_2 are as follows:

$$\begin{aligned} p_1 = X^8 - a_4X^7 + (1 + a_4^2 - a_3)X^6 + (a_4 - a_4^3 - a_2)X^5 + (a_4 - a_4^2 + a_4^4 - a_3 - a_4a_2)X^4 \\ + (1 - a_4 + a_4^2 - a_4^5 - a_3 + a_4^3a_3 + a_2 - a_3a_2 + a_0)X^3 \\ + (-1 + a_4^2 - a_4^3 + a_4^4 + a_4^6 + a_3 + a_4a_3 - a_3^2 - a_3^3 - a_2 - a_4^3a_2 + a_4a_3a_2 + a_2^2)X^2 \\ + (-1 - a_4^2 - a_4^3 - a_4^4 - a_4^5 - a_4^7 + a_3 + a_4a_3 - a_4^2a_3 - a_4^3a_3 - a_3^2 \\ - a_4a_3^2 + a_4a_3^3 - a_2 - a_4^2a_2 - a_4^4a_2 + a_3a_2 - a_4^2a_3a_2 - a_3^2a_2)X \\ + 1 - a_4^2 - a_4^6 + a_4^8 + a_3 - a_4^6a_3 + a_3^3 - a_4^2a_3^3 + a_3^4, \end{aligned}$$

$$p_2 = X^6 - X^4 + (-1 - a_4 - a_4^3 + a_2)X^3 + (-1 + a_4^2 - a_3 - a_4a_2 + a_1)X^2 \\ + (-1 - a_4 + a_4^2 + a_4^3 - a_3 - a_4a_3 - a_2 + a_4^2a_2 - a_3a_2)X - 1 + a_4^6 - a_3^3.$$

Taking the resultant of p_1 and p_2 eliminates the variable X, and gives a degree 27 polynomial $h \in \mathbb{F}_{q'}[S]$ that has s_0 as a root. The extra 6 bits allow one to decide which root of h to take for s_0, and to determine t. The polynomial $h(S)$ is of the form $h_1(S^3 - S)$ for a certain degree 9 polynomial $h_1(S) \in \mathbb{F}_{q'}[S]$, and this simplifies finding the roots of h. See §5.1 of [24] for an explanation of this reconstruction step.

RS compression was arrived at by studying the Weil restriction of scalars of elliptic curves (which are abelian varieties), and understanding the theory of abelian varieties. In §5.7 we discuss some of the underlying mathematics.

Remark 5 In elliptic curve point compression and in BLS, an elliptic curve point (x, y) is compressed to its x-coordinate, giving lossy compression. One can transmit an extra bit that determines the y-coordinate, in order to fully reconstruct the point. The signature (s_1, s_2, s_3, s_4) above is similarly an example of lossy compression; the extra 6 bits and the reconstruction step allow one to fully recover the elliptic curve point (s, t).

4.3 Comparison

RS compression (§4.2) produces signatures that are roughly $\frac{4}{5}$ as large as BLS signatures with comparable security. In both cases, the security is based on the difficulty of the Elliptic Curve Diffie-Hellman Problem in $\langle P \rangle$. RS signing is no more work than for BLS. Compared with BLS, RS verification requires an additional reconstruction step to recover s_0. For applications in which the verifier is powerful, this is not a significant problem.

Note that RS compression (like BLS) only uses elliptic curve arithmetic, and does not use any abelian variety arithmetic.

Bernstein and Bleichenbacher have compressed RSA and Rabin signatures ([2, 3]). In Table 1 below, BCR stands for Bleichenbacher's Compressed Rabin signatures, DSA is the Digital Signature Algorithm, and ECDSA is the Elliptic Curve Digital Signature Algorithm. In the middle column of Table 1, the signatures are all scaled to 1024-bit RSA security. In the remaining columns the signatures are scaled to the MOV security of the RS scheme. The MOV security refers to attacks on the discrete log problem in $\mathbb{F}_{q^6}^{\times}$. The DL security refers to generic attacks on the group $\langle P \rangle$; the relevant value for DL security is $\log_2(\ell)$-bits, where ℓ is the order of P. (See [5, 24].)

There is an RS scheme similar to the one in §4.2 (see §5.2 of [24]) that uses elliptic curves over binary fields $\mathbb{F}_{2^w}$. Working over binary fields might yield some efficiency advantages. However, due to Coppersmith's attack on the discrete log problem in low characteristic [9], larger parameters should be used.

To achieve the flexibility of higher characteristic, in §6 of [24] we suggest the use of (Jacobian varieties of) certain twists of Fermat curves. In a recent preprint giving an expanded version of [5], Boneh, Lynn, and Shacham suggest using MNT elliptic curves.

system			
RSA	904	1024	2045
BCR	452	512	1024
DSA		320	
ECDSA		320	
BLS	152	172	342
RS	127	143	279

Table 1. Signature lengths, in bits, for comparable MOV security

5 The underlying mathematics

5.1 Varieties and algebraic groups

Definition 6 Loosely speaking, an *algebraic variety* (over a field k) is the solution set of a system of polynomial equations (whose coefficients are in k). An *algebraic group* (or *group variety*) over a field k is a variety over k such that the group law and the inverse map are quotients of polynomials whose coefficients are in k.

5.2 The Weil restriction of scalars

Suppose that V is a variety over a field L. This means that V is the solution set of a system of polynomial equations $f_i(x_1, \ldots, x_r) = 0$, $1 \leq i \leq s$, where the polynomials f_i have coefficients in the field L. Suppose k is a subfield of L, and n is the degree of L over k. Fix a basis $\{v_1, \ldots, v_n\}$ for L over k. Write $x_i = \sum_{j=1}^{n} y_{ij} v_j$ with variables y_{ij}. Substitute this into the equations $f_i(x_1, \ldots, x_r) = 0$. Multiplying out, writing everything with respect to the basis $\{v_1, \ldots, v_n\}$, and equating coefficients, one obtains a system of polynomials in the variables $\{y_{ij}\}$, with coefficients in the field k. The variety defined by these new equations is denoted $\mathrm{Res}_{L/k} V$, and is called the (Weil) restriction of scalars from L down to k. It is a variety over k with the property that its k-points are the L-points of V:

$$(\mathrm{Res}_{L/k} V)(k) \cong V(L).$$

Its dimension is $n \cdot \dim(V)$. See for example §3.12 in Chapter 1 of [30] for more information.

5.3 The multiplicative group $\mathbb{G}_m$

Diffie-Hellman is based on the multiplicative group, denoted $\mathbb{G}_m$. Over any field F, the F-points on $\mathbb{G}_m$ are

$$\mathbb{G}_m(F) = F^\times = F - \{0\},$$

the multiplicative group of invertible elements of the field F. The algebraic variety $\mathbb{G}_m$ is defined by the equation $xy = 1$, i.e., it consists of the elements x such that there exists a y with $xy = 1$. It is an algebraic group over any field k. We will view $\mathbb{G}_m$ as an algebraic group over the field $\mathbb{F}_q$.

5.4 The restriction of scalars $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$

The Weil restriction of scalars $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$ is an algebraic variety (in fact, an algebraic group) over $\mathbb{F}_q$. We have

$$(\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m)(\mathbb{F}_q) \cong \mathbb{F}_{q^n}^\times.$$

Example 7 To find equations defining the two-dimensional algebraic variety $\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m$, write $\mathbb{F}_9 = \mathbb{F}_3(\sqrt{-1})$, and write $x = x_1 + x_2\sqrt{-1}$ and $y = y_1 + y_2\sqrt{-1}$. Substituting into $xy = 1$ and equating coefficients gives the equations:

$$x_1y_1 - x_2y_2 = 1, \qquad x_1y_2 + x_2y_1 = 0.$$

5.5 The primitive subgroup G_0

Suppose that G is a commutative algebraic group over a field k. In the cases of interest to us, V will be the multiplicative group $\mathbb{G}_m$ or an elliptic curve. For now, we write G's group operation as multiplication.

If L is a field that is a finite extension of k, define the *primitive subgroup* G_0 of $\mathrm{Res}_{L/k}G$ to be

$$G_0 = \ker[\mathrm{Res}_{L/k}G \xrightarrow{\oplus \mathrm{N}_{L/F}} \bigoplus_{k\subseteq F\subsetneq L} \mathrm{Res}_{F/k}G],$$

where the norm maps $\mathrm{N}_{L/F}$ induce the usual norm maps

$$\mathrm{N}_{L/F} : G(L) \to G(F), \qquad x \mapsto \prod_{\sigma\in\mathrm{Gal}(L/F)} \sigma(x).$$

Then G_0 is an algebraic group over k, and $G_0(k)$ consists of all elements of $G(L)$ whose norm down $G(F)$ is the identity, for every intermediate field F with $F \neq L$.

The group $\mathrm{Res}_{L/k}G$ is "almost the same" as the product $G \times G_0$ (there are homomorphisms between them with "small" kernel and cokernel).

5.6 The algebraic torus $\mathbb{T}_n$

Let $\mathbb{T}_n$ (or $\mathbb{T}_{n,q}$ when it is important to keep track of the ground field) denote the primitive subgroup of $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$, i.e.,

$$\mathbb{T}_n = \mathbb{T}_{n,q} = \ker\big[\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\ \mathbb{G}_m \xrightarrow{\oplus \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}} \bigoplus_{\substack{d\mid n\\ d\neq n}} \mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\ \mathbb{G}_m\big].$$

By definition, $\mathbb{T}_n(\mathbb{F}_q)$ is the group of elements of $\mathbb{F}_{q^n}^\times$ that have norm 1 down to every intermediate field $\mathbb{F}_{q^d}$ (for $d \neq n$). By Lemma 7 of [25],

$$\mathbb{T}_n(\mathbb{F}_q) = T_n. \tag{2}$$

Example 8 Continuing Example 7, where $q = 3$ and $n = 2$, it is easy to write down embeddings:

$$\mathbb{G}_m \hookrightarrow \mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m, \quad x \mapsto (x, 0, x^{-1}, 0),$$

$$\mathbb{T}_2 \hookrightarrow \mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m, \quad x_1 + x_2\sqrt{-1} \mapsto (x_1, x_2, x_1, -x_2).$$

The compositions (in both orders) of the resulting map

$$\mathbb{G}_m \times \mathbb{T}_2 \to \mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m$$

with the map

$$\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m \to \mathbb{G}_m \times \mathbb{T}_2$$

defined by

$$(x_1, x_2, y_1, y_2) \mapsto (x_1^2 + x_2^2, x_1y_1 + x_2y_2 + 2x_2y_1\sqrt{-1})$$

are the squaring maps. Thus, $\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m$ is "almost the same" as $\mathbb{G}_m \times \mathbb{T}_2$.

5.7 The trace-0 subgroup of $\mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_{q'}}(E^-)$

Abelian varieties are, by definition, projective algebraic groups. Elliptic curves are exactly the one-dimensional abelian varieties.

With E^-, q', q, ℓ, and P as in §4.2, let

$$B = \mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_{q'}}(E^-),$$

and let A be the primitive subgroup of B:

$$A = \ker[B \xrightarrow{\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_{q'}}} E^-].$$

Then A and B are abelian varieties over $\mathbb{F}_{q'}$ of dimensions 4 and 5, respectively, and B is isogenous to $E^- \times A$. (See also §3.2 of [11].) The abelian variety A is simple. Since the group law on an abelian variety is written additively, the norm map now corresponds to the sum of the conjugates, i.e., the trace defined in §4.2. We have

$$\begin{array}{ccc} \langle P \rangle \subset A_0 = \{Q \in E^-(\mathbb{F}_q) : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(Q) = \mathcal{O}_{E^-}\} & \cong & A(\mathbb{F}_{q'}) \\ \cap & & \cap \\ E^-(\mathbb{F}_q) & & \cong B(\mathbb{F}_{q'}) \end{array}$$

Note that the underlying four-dimensional abelian variety A is invisible in the algorithms in §4.2.

6 Cryptographic applications of algebraic tori and their quotients

We give an exposition of some of the mathematics underlying torus-based cryptography (i.e., the $\mathbb{T}_n$-cryptosystems) and the cryptosystems discussed in §2. We discuss how the latter schemes are based on quotients of tori by the actions of symmetric groups.

6.1 Algebraic tori

Definition 9 An *algebraic torus* is an algebraic group that over some larger field is a product of multiplicative groups. 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. See [23, 30] for expositions.

Example 10 (i) For every positive integer r, $\mathbb{G}_m^r$ is an r-dimensional algebraic torus.

(ii) $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$ is an n-dimensional algebraic torus over $\mathbb{F}_q$ that splits over $\mathbb{F}_{q^n}$.

By Proposition 2.6 of [26], the group $\mathbb{T}_n$ defined in §5.6 is a $\varphi(n)$-dimensional torus.

6.2 Rationality and birational isomorphisms

If r is a positive integer, write $\mathbb{A}^r$ for affine r-space. For any field F, we have $\mathbb{A}^r(F) = F^r$, the direct sum of r copies of F.

Definition 11 A *rational* map between algebraic varieties is a function defined by polynomials or quotients of polynomials that is defined almost everywhere. 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 is *rational* if it is birationally isomorphic to $\mathbb{A}^d$.

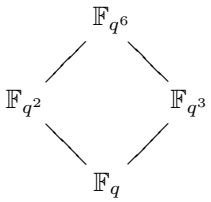
Note that birational isomorphisms are not necessarily group isomorphisms. Note also that rational maps are not necessarily functions — they might fail to be defined on a lower dimensional set.

By (2), if $\mathbb{T}_n$ is rational (i.e., birationally isomorphic to $\mathbb{A}^{\varphi(n)}$), then almost all elements of T_n can be represented by $\varphi(n)$ elements of $\mathbb{F}_q$.

The maps f and j in §3 are only birational. The sets T_n and $\mathbb{F}_q^{\varphi(n)}$ are of size approximately $q^{\varphi(n)}$. The "bad" sets where f and j are not defined correspond to 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. For example, in §3.6 the bad sets have 2 and 0 elements, respectively.

6.3 Obtaining the rational maps f and j

How were the maps in Examples 11 and 12 of [25] and in §3.6 above arrived at? The idea is as follows.



The one-dimensional torus $\mathbb{T}_{2,q^3}$ is, by definition, the kernel of the norm map $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}$. The torus

$$\mathcal{T} := \mathrm{Res}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\mathbb{T}_{2,q^3})$$

has dimension 3. As in §3.4, the torus $\mathbb{T}_{2,q^3}$ is rational (i.e., is birationally isomorphic to $\mathbb{A}^1$), and thus the torus $\mathcal{T}$ is rational (i.e., birationally isomorphic to $\mathbb{A}^3$). The two-dimensional torus $\mathbb{T}_6$ is the hypersurface cut out by the equation $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} = 1$ inside the torus $\mathcal{T}$. This hypersurface is defined by a quadratic equation that can be used to parametrize the hypersurface. We gave examples of this in Examples 11 and 12 of [25]. Section 3.6 gives an additional example.

6.4 A group action on the torus

Next, we define actions of symmetric groups on the tori $\mathbb{T}_n$. Suppose e is a divisor of n, and let $d = n/e$. Since n is square-free, we have $\gcd(e, d) = 1$, so

$$\mathbb{Z}/n\mathbb{Z} \quad \cong \quad \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}.$$

The symmetric group on e letters, S_e, acts on $\mathbb{Z}/e\mathbb{Z}$. Extend this action to an action of S_e on $\mathbb{Z}/n\mathbb{Z}$, by acting trivially on $\mathbb{Z}/d\mathbb{Z}$. Now define an action of S_e on $\mathbb{A}^n$ $(= \mathbb{A}^{\mathbb{Z}/n\mathbb{Z}})$ as follows. For $\pi \in S_e$,

$$(x_i)_{i\in\mathbb{Z}/n\mathbb{Z}} \quad \mapsto \quad (x_{\pi^{-1}(i)})_{i\in\mathbb{Z}/n\mathbb{Z}}.$$

We have

$$\mathbb{A}^n \underset{\mathbb{F}_{q^n}}{\cong} \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{A}^1 \supset \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m \supset \mathbb{T}_n.$$

The action of S_e on $\mathbb{A}^n$ preserves $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$. However, it does not necessarily preserve the torus $\mathbb{T}_n$.

Theorem 12 (Lemma 3.5 of [26]) *If p is a prime divisor of n, then the above action of S_p on $\mathbb{A}^n$ preserves the torus $\mathbb{T}_n$.*

6.5 Interpreting the other systems in terms of quotients of tori

- The Lucas-based cryptosystems are "based on" the quotient variety $\mathbb{T}_2/S_2$.
- The Gong-Harn system is based on the quotient variety $\mathbb{T}_3/S_3$.
- XTR is based on the quotient variety $\mathbb{T}_6/S_3$.
- Conjectural "Looking beyond XTR" systems would rely on the quotient variety $\mathbb{T}_{30}/(S_3 \times S_5)$ 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 and XTR do not do straightforward multiplication.

- The $\mathbb{T}_2$-cryptosystem is based on the group (and torus) $\mathbb{T}_2$.
- CEILIDH is based on the group (and torus) $\mathbb{T}_6$.

– The (sometimes conjectural) $\mathbb{T}_n$-cryptosystems are based on the group (and torus) $\mathbb{T}_n$.

We therefore call the $\mathbb{T}_n$-cryptosystems "torus-based cryptosystems".

What do we mean when we say that these systems are "based on" certain algebraic varieties?

XTR works because the variety $\mathbb{T}_6/S_3$ is rational, and the trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ induces a birational isomorphism:

$$\mathbb{T}_6/S_3 \ \dashrightarrow \ \mathbb{A}^2 = \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\mathbb{A}^1.$$

Similarly for the Lucas-based cryptosystems, the trace map $\mathbb{F}_{p^2} \to \mathbb{F}_p$ induces a birational isomorphism:

$$\mathbb{T}_2/S_2 \ \dashrightarrow \ \mathbb{A}^1.$$

More precisely, let $B_{(d,e)}$ denote the image of $\mathbb{T}_n$ in $(\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m)/S_e$ (where $n = de$). By Theorem 3.7 of [26], $B_{(d,e)}$ is birationally isomorphic to $\mathbb{T}_n/(S_{p_1} \times \cdots \times S_{p_r})$ where $e = p_1 \cdots p_r$ is the prime factorization of e. Note that the quotient map $\mathbb{T}_n \to \mathbb{T}_n/S_e$ induces a (non-surjective) map on $\mathbb{F}_q$-points:

$$T_n = \mathbb{T}_n(\mathbb{F}_q) \to (\mathbb{T}_n/S_e)(\mathbb{F}_q).$$

Let

$$\mathrm{XTR}(d,e) = \{\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(\alpha) : \alpha \in T_n\} \subset \mathbb{F}_{q^d}.$$

When $(d,e) = (1,2)$ or $(2,3)$, then $\mathrm{XTR}(d,e)$ is the set of traces that occur in the Lucas-based systems and XTR, respectively. In these two cases, $\mathrm{XTR}(d,e)$ can be naturally identified with the image of $\mathbb{T}_n(\mathbb{F}_q)$ in $(\mathbb{T}_n/S_e)(\mathbb{F}_q)$. More precisely (see Theorem 13 of [25]), when $(d,e) = (1,2)$ or $(2,3)$, the trace map $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$ induces a birational embedding

$$\mathbb{T}_n/S_e \hookrightarrow \mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\mathbb{A}^1$$

such that $\mathrm{XTR}(d,e)$ is the image of the composition

$$T_n = \mathbb{T}_n(\mathbb{F}_q) \longrightarrow (\mathbb{T}_n/S_e)(\mathbb{F}_q) \hookrightarrow (\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\mathbb{A}^1)(\mathbb{F}_q) \cong \mathbb{F}_{q^d}.$$

6.6 "Looking beyond XTR"

The paper "Looking beyond XTR" [6], building on a conjecture in [8], asks whether, for $n > 6$, some set of elementary symmetric polynomials can be used in place of the trace. In particular, [6] asks whether, when $d \mid n$ and $d \mid \varphi(n)$, 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 $\varphi(n)/d$ of them (this was already answered in the affirmative in some cases in [8, 13]). If this were true, one could use the first $\varphi(n)/d$ elementary symmetric polynomials on

the set of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})$-conjugates of an element $h \in T_n$ to represent h by $\varphi(n)$ elements of $\mathbb{F}_q$. More generally, [6] asks whether, for $d \mid n$, one can recover the entire characteristic polynomial over $\mathbb{F}_{p^d}$ from its first $\lceil \varphi(n)/d \rceil$ coefficients.

The answer is no. In particular, in [25] we show that when $n = 30$ and $p = 7$, then:

- for $d = 1$, no 8 $(= \varphi(n)/d)$ elementary symmetric polynomials determine *any* of the remaining ones (except 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.

Reinterpreted in terms of algebraic tori, the conjectures in [6] imply (see [26]) that the first eight elementary symmetric polynomials induce a birational isomorphism over $\mathbb{F}_p$:

$$\mathbb{T}_{30}/(S_2 \times S_3 \times S_5) \dashrightarrow \mathbb{A}^8,$$

and the first four elementary symmetric polynomials on the $\mathrm{Gal}(\mathbb{F}_{p^{30}}/\mathbb{F}_{p^2})$-conjugates of an element in T_{30} induce a birational isomorphism over $\mathbb{F}_p$:

$$\mathbb{T}_{30}/(S_3 \times S_5) \dashrightarrow \mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p} \mathbb{A}^4 \cong \mathbb{A}^8.$$

In [26] we prove that these statements are both false, for all but possibly finitely many primes p.

More generally, we have

$$\mathbb{T}_n \twoheadrightarrow B_{(d,e)} \hookrightarrow (\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q} \mathbb{A}^1)^e \cong \mathbb{A}^n,$$

where the middle map $\oplus_{i=1}^{e} s_i$ is induced by the e elementary symmetric polynomials $s_1, \ldots, s_e$ on $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})$-conjugacy classes. (Recall that $B_{(d,e)}$ was defined at the end of §6.5, and $de = n$.)

The conjectures in [6] would imply that, when d divides $\varphi(n)$, then the first $\varphi(n)/d$ functions $s_1, \ldots, s_{\varphi(n)/d}$ induce a birational isomorphism

$$B_{(d,e)} \dashrightarrow (\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q} \mathbb{A}^1)^{\varphi(n)/d} \cong \mathbb{A}^{\varphi(n)}.$$

This is true when the pairs (d, e) are $(1, 1)$ (this is Diffie-Hellman), $(1, 2)$ (Lucas-based systems), $(1, 3)$ (Gong-Harn), and $(2, 3)$ (XTR). It is also true (see [8]) when ℓ is a prime and $(d, e) = (1, \ell)$ or $(2, \ell)$. As noted above, we showed in [25, 26] that this is false for $(d, e) = (1, 30)$ and $(2, 15)$ (in all but at most finitely many characteristics).

When $(d, e) = (n, 1)$, the underlying variety $B_{(d,e)}$ is $\mathbb{T}_n$ itself, corresponding to the $\mathbb{T}_n$-cryptosystems.

In summary, elementary symmetric polynomials are not the correct functions to use. In the next section we state a conjecture (of Voskresenskii) that seems to be closer to the truth.

6.7 Voskresenskii's Conjecture

Conjecture 13 (Voskresenskii) *$\mathbb{T}_n$ is rational; i.e., for every n, there is a birational isomorphism*

$$\mathbb{T}_n \dashrightarrow \mathbb{A}^{\varphi(n)}.$$

The conjecture is true, and not difficult to prove, if n is a prime power [30]. The conjecture was proved by Klyachko [16] when n is a product of two prime powers. Explicit birational isomorphisms are given in §5 of [25] and §3.6 above (see also §3.4 above), in the cases $n = 2$ and 6. A $\mathbb{T}_n$-cryptosystem arises for every n for which Voskresenskii's Conjecture is true with efficiently computable birational maps.

When n is divisible by more than two distinct primes, Voskresenskii's Conjecture is still an open question. In particular, the conjecture is not known when $n = 30 = 2 \cdot 3 \cdot 5$. We have tried unsuccessfully to construct a birational isomorphism between $\mathbb{T}_{30}$ and $\mathbb{A}^8$. It would be interesting to know whether Voskresenskii's Conjecture is true or false when $n = 30$. We have been able to construct explicit rational maps of low degree in this case, which might be useful if no birational map exists. For example, an s-to-1 map from $\mathbb{T}_{30}$ to $\mathbb{A}^8$ would provide a lossy compression scheme, and would allow one to represent elements of T_{30} in $\mathbb{F}_q^8 \times \{1, \ldots, s\}$.

Rationality of the varieties $B(1, n)$ (or more generally the varieties $B(d, e)$) would imply the conjecture in [8].

6.8 Stable rationality

One reason that Voskresenskii's Conjecture would be difficult to disprove is that the tori $\mathbb{T}_n$ are known to always be stably rational over $\mathbb{F}_q$ (see the Corollary on p. 61 of [30]).

Definition 14 A variety V over k is called *stably rational* over k if for some r and s, $V \times \mathbb{A}^r$ is birationally isomorphic over k to $\mathbb{A}^s$ (i.e., $V \times \mathbb{A}^r$ is rational for some $r \geq 0$).

Although the stable rationality of $\mathbb{T}_n$ does not allow one to represent elements of T_n in $\mathbb{F}_q^{\varphi(n)}$, it does allow one to represent elements of $T_n \times \mathbb{F}_q^r$ in $\mathbb{F}_q^s$ for suitable r and s, and this might be useful.

7 Open problems

Some goals for the future are:

- Improve the efficiency of CEILIDH.
- Obtain more efficient key agreement, encryption, and signature schemes, by generalizing to $\mathbb{T}_{30}$-cryptosystems:
  - find explicit and efficient birational isomorphisms f and j between $\mathbb{T}_{30}$ and $\mathbb{A}^8$, if such exist,

  - look for special attacks on the discrete log problem in $\mathbb{F}_{q^{30}}^{\times}$.
- Use non-supersingular (i.e., ordinary) abelian varieties to further improve pairing-based cryptography.

Progress has been made on the last point in the case of elliptic curves; see for example [7].

References

1. P. Barreto, *Pairing-based crypto lounge*: `http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html`
2. D. Bernstein, *A state-of-the-art public-key signature system*, `http://cr.yp.to/sigs.html`
3. D. Bleichenbacher, *Compressing Rabin Signatures*, in Topics in Cryptology — CT-RSA 2004, Lect. Notes in Comp. Sci. **2964**, Springer, Berlin, 2004, 126–128.
4. 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.
5. D. Boneh, B. Lynn, H. Shacham, *Short signatures from the Weil pairing*, in Advances in Cryptology — Asiacrypt 2001, Lect. Notes in Comp. Sci. **2248**, Springer, Berlin, 2001, 514–532.
6. 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.
7. F. Brezing, A. Weng, *Elliptic curves suitable for pairing based cryptography*, Cryptology ePrint Archive, Report 2003/143.
8. 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.
9. D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic two*, IEEE Trans. Inform. Theory **30** (1984), 587–594.
10. W. Diffie, M. E. Hellman, *New Directions in Cryptography*, IEEE Trans. Inform. Theory **22** (1976), 644–654.
11. G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, in Finite fields and applications (Augsburg, 1999). Springer, Berlin, 2001, 128–161.
12. S. Galbraith, *Supersingular curves in cryptography*, in Advances in Cryptology — Asiacrypt 2001, Lect. Notes in Comp. Sci. **2248**, Springer, Berlin, 2001, 495–513.
13. G. Gong, L. Harn, *Public-key cryptosystems based on cubic finite field extensions*, IEEE Trans. Inform. Theory **45** (1999), 2601–2605.
14. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, in Algorithmic Number Theory Symposium (ANTS-IV), Lect. Notes in Comp. Sci. **1838**, Springer, Berlin, 2000, 385–394.
15. A. Joux, *The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems*, in Algorithm Number Theory Symposium (ANTS-V), Lect. Notes in Comp. Sci. **2369**, Springer, Berlin, 2002, 20–32.
16. 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).

17. 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.
18. A. K. Lenstra, *The XTR public key system*, lecture at MSRI Number-Theoretic Cryptography Workshop, October 20, 2000.
19. 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.
20. E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–239, 289–321.
21. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of applied cryptography, CRC Press, Boca Raton, FL, 1997.
22. W. B. Müller, W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. **16** (1981), 71–76.
23. T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. **74** (1961), 101–139.
24. 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.
25. K. Rubin, A. Silverberg, *Torus-based cryptography*, in Advances in Cryptology — CRYPTO 2003, Lect. Notes in Comp. Sci. **2729** (2003), Springer, Berlin, 2003, 349–365.
26. 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, AMS, Providence, RI, 2004.
27. R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystems based on pairing*, SCIS2000 (The 2000 Symposium on Cryptography and Information Security), Okinawa, Japan, January 26–28, 2000, C20.
28. 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.
29. 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.
30. V. E. Voskresenskii, Algebraic groups and their birational invariants, Translations of Mathematical Monographs **179**, AMS, Providence, RI, 1998.
31. H. C. Williams, *A $p+1$ method of factoring*, Math. Comp. **39** (1982), 225–234.
32. H. C. Williams, *Some public-key crypto-functions as intractable as factorization*, Cryptologia **9** (1985), 223–237.