

Algebraic Torus-Based Cryptography

Jason E. Gower

`gower@ima.umn.edu`

Institute for Mathematics and its Applications

University of Minnesota

November 7, 2006

Symmetric Key Encryption

Private communication over an **insecure channel**: Alice and Bob want to communicate privately, but Eve can obtain a copy of everything they send to each other.

Alice and Bob agree (in public) to use a particular **symmetric key encryption scheme** that will allow them both to encrypt/decrypt messages so long as they are using the same encryption/decryption key K .

They need to agree on the value of K , after which they can communicate using the insecure channel.

Alice and Bob have reduced their problem to finding a way to share a private key K without Eve finding out the value of K .

Diffie-Hellman Key Exchange

Usually K is an element of a cyclic group $G = \langle g \rangle$ of prime order p , with $p \approx 2^{160}$. In this case, Alice and Bob can use the [Diffie-Hellman key exchange protocol](#):

1. Alice picks a random integer $a \in [1, p]$ and computes $\alpha = g^a$, while Bob picks a random integer $b \in [1, p]$ and computes $\beta = g^b$. (Alice keeps a private and Bob keeps b private.)
2. Alice sends α to Bob and Bob sends β to Alice.
3. Alice computes β^a and Bob computes α^b . They now share the private key $K = g^{ab}$.

[Diffie-Hellman problem](#): Given the values of g , g^a and g^b , compute g^{ab} .

Security assumption: DHP is computationally difficult.

Diffie-Hellman & Discrete Logarithm Problems

The difficulty of DHP is unknown, though it has resisted at least 30 years of attack.

Note that if Eve can efficiently compute **discrete logarithms** in G , then she can solve DHP:

1. First she computes $a = \log_g(\alpha)$ and $b = \log_g(\beta)$.
2. With a , b and g she can now compute g^{ab} .

Discrete Logarithm problem: Given the values of g and g^x , compute x .

Clearly DHP is no harder than DLP.

Open Question: Are DHP and DLP equivalent?

Pollard Rho

The best group-independent attack on DLP is the [Pollard Rho](#) algorithm.

Let $h = g^x$, randomly partition $G = G_1 \cup G_2 \cup G_3$ and define $f : G \rightarrow G$ by:

$$f(z) = \begin{cases} zh, & \text{if } z \in G_1; \\ zg, & \text{if } z \in G_2; \\ z^2, & \text{if } z \in G_3. \end{cases}$$

Let $a_0 = b_0 = h$ and define sequences $a_i = f(a_{i-1})$ and $b_i = f(f(b_{i-1}))$ for $i \geq 1$. Note that $b_i = a_{2i}$ and $a_i = g^{r_i x + s_i}$ for some r_i, s_i .

If we ever find $a_i = b_i$, then $r_i x + s_i \equiv r_{2i} x + s_{2i} \pmod{p}$. If we also have $r_i \not\equiv r_{2i} \pmod{p}$, then we can solve for x .

We expect to find x with Pollard Rho after $O(\sqrt{p})$ steps.

Index Calculus

Another good algorithm for DLP is the [Index Calculus](#) algorithm.

Pick a [factor base](#) $\{g_1, \dots, g_r\} \subset G$ over which most elements of G can easily be factored. For random $j \in \mathbb{Z}/p\mathbb{Z}$, compute g^j and try to write

$$g^j = \prod_{i=1}^r g_i^{e_{ij}}, \quad \text{hence} \quad j \equiv \sum_{i=1}^r e_{ij} \log_g(g_i) \pmod{p}.$$

Once we have more than r of these linear congruences, we should be able to solve for the unknowns $\log_g(g_1), \dots, \log_g(g_r)$.

Now randomly pick $k \in \mathbb{Z}/p\mathbb{Z}$, compute hg^k and try to write

$$hg^k = \prod_{i=1}^r g_i^{f_{ik}}, \quad \text{hence} \quad x = -k + \sum_{i=1}^r f_{ik} \log_g(g_i) \pmod{p}.$$

The performance of index calculus is group-dependent: subexponential for \mathbb{F}_{q^n} , but not for elliptic curves.

Groups for Diffie-Hellman

The most popular groups for Diffie-Hellman come from:

- **Finite fields:** The multiplicative group \mathbb{F}^\times of a finite field \mathbb{F} .
- **Elliptic curves:** The additive group $E(\mathbb{F})$ of \mathbb{F} -points on an elliptic curve E , where \mathbb{F} is a finite field.
- **Hyperelliptic curves:** The jacobian of a low-genus hyperelliptic curve.

We will consider groups arising as **algebraic tori** (Rubin & Silverberg) ...

Weil Restriction of Scalars

Let L/K be finite and separable with $[L : K] = n$. If V is an algebraic group defined over L , then $\text{Res}_{L/K} V$ denotes the **Weil restriction of scalars** from L down to K .

Example: $V = \{(x, y) \in \mathbb{C}^2 \mid xy = 1\} \cong \mathbb{C}^\times$. To find $\text{Res}_{\mathbb{C}/\mathbb{R}} V$, let $x = x_1 + ix_2, y = y_1 + iy_2$, substitute in, and multiply out:

$$1 = xy = (x_1 + ix_2)(y_1 + iy_2) = (x_1y_1 - x_2y_2) + i(x_1y_2 + x_2y_1).$$

Equating coefficients yields:

$$\text{Res}_{\mathbb{C}/\mathbb{R}} V = \{(x_1, x_2, y_1, y_2) \in \mathbb{C}^4 \mid x_1y_1 - x_2y_2 - 1 = 0 = x_1y_2 + x_2y_1\}.$$

We will need the following property of the Weil restriction:

$$(\text{Res}_{L/K} V)(K) \cong V(L).$$

The Multiplicative Group and Algebraic Tori

Let \mathbb{G}_m be the **multiplicative group** defined by

$$\mathbb{G}_m(L) = \{(x, y) \in L^2 \mid xy = 1\} \cong L^\times,$$

where L is any field.

From what we have seen, it follows that

$$(\text{Res}_{L/K} \mathbb{G}_m)(K) \cong \mathbb{G}_m(L) \cong L^\times.$$

An **algebraic torus** is an algebraic group (defined over K) that splits into a product of multiplicative groups over some extension L/K .

Examples of algebraic tori are:

- \mathbb{G}_m^r , for any positive integer r ;
- $\text{Res}_{L/K} \mathbb{G}_m$ defined over K , splits over L .

Primitive Subgroups

For any F with $K \subseteq F \subsetneq L$, let $N_{L/F} : L \rightarrow F$ be the usual norm map. There is a corresponding map $\mathcal{N}_{L/F} : \text{Res}_{L/K} \mathbb{G}_m \rightarrow \text{Res}_{F/K} \mathbb{G}_m$ such that the following diagram commutes:

$$\begin{array}{ccc}
 (\text{Res}_{L/K} \mathbb{G}_m)(K) & \xrightarrow{\mathcal{N}_{L/F}} & (\text{Res}_{F/K} \mathbb{G}_m)(K) \\
 \cong \downarrow & & \downarrow \cong \\
 L^\times & \xrightarrow{N_{L/F}} & F^\times
 \end{array}$$

Define the **primitive subgroup** of $\text{Res}_{L/K} \mathbb{G}_m$ by:

$$T_n = \ker \left[\text{Res}_{L/K} \mathbb{G}_m \xrightarrow{\bigoplus \mathcal{N}_{L/F}} \bigoplus \text{Res}_{F/K} \mathbb{G}_m \right].$$

It can be shown that T_n is a $\varphi(n)$ -dimensional algebraic torus, where φ is the Euler totient function.

Primitive Subgroups (continued)

The set of K -points of T_n is then:

$$T_n(K) = \{\alpha \in L^\times \mid N_{L/F}(\alpha) = 1, \text{ for all } F \text{ with } K \subseteq F \subsetneq L\}.$$

We are interested in the case of $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^n}$.

It is not hard to show that:

- $T_n(\mathbb{F}_q) = \{\alpha \in \mathbb{F}_{q^n}^\times \mid \alpha^{\Phi_n(q)} = 1\}$, where Φ_n is the n -th cyclotomic polynomial;
- If $\alpha \in T_n(\mathbb{F}_q)$ is an element of prime order not dividing n , then α does not lie in a proper subfield of \mathbb{F}_{q^n} .

Since $T_n(\mathbb{F}_q)$ does not lie in any proper subfield of \mathbb{F}_{q^n} , $T_n(\mathbb{F}_q)$ can be thought of as the “cryptographically strongest” proper subgroup of $\mathbb{F}_{q^n}^\times$.

Cardinality of $T_n(\mathbb{F}_q)$

The cardinality of $T_n(\mathbb{F}_q)$ must be either a large prime or divisible by a large prime to be of any cryptographic use.

Bateman-Horn Conjecture (1962): Let $f_1, \dots, f_k \in \mathbb{Z}[x]$ be distinct monic irreducibles s.t. no prime divides every element of the set $\{f(m) \mid m \in \mathbb{Z}\}$, where $f = f_1 \cdots f_k$. For every positive integer N , define $Q(f_1, \dots, f_k; N)$ to be the number of positive integers $m \in [1, N]$ s.t. $f_1(m), \dots, f_k(m)$ are all prime. Then $Q(f_1, \dots, f_k; N) \sim \frac{C(f_1, \dots, f_k)}{d_1 \cdots d_k} \sum_{j=2}^N (\log j)^{-k}$, where $d_i = \deg f_i$.

If q is a prime and n is not a prime power, then use BH with $f_1 = x$ and $f_2 = \Phi_n(x)$. If $q = p^r$ for some prime p and every prime dividing r also divides n , then use BH with $f_1 = x$ and $f_2 = \Phi_{rn}(x) = \Phi_n(x^r)$.

There should be many cryptographically interesting choices for q and n .

Compact Representation of $T_n(\mathbb{F}_q)$

A d -dimensional variety V over K is **rational** over K if it is birationally isomorphic to \mathbb{A}^d .

In other words, there exist nonempty Zariski open sets $U \subset V$, $W \subset \mathbb{A}^d$, a rational mapping $\rho : U \rightarrow W$, and a rational inverse $\psi : W \rightarrow U$.

This gives us a **rational parametrization** of V .

Since T_n is $\varphi(n)$ -dimensional, we have a **compact representation**; elements of $T_n(\mathbb{F}_q)$ can be represented with $\varphi(n)$ elements of \mathbb{F}_q , as opposed to the n elements of \mathbb{F}_q usually needed to represent elements of \mathbb{F}_{q^n} .

Let $X = V - U$. Then $\dim X \leq d - 1$, so $|X(K)| = O(q^{d-1})$. The fraction of elements of $V(K)$ “missed” by the parametrization is $O(1/q)$.

Cryptographically interesting cases will have large q .

Rationality of $T_n(\mathbb{F}_q)$

Cryptographically interesting cases are when $n/\varphi(n)$ is large; i.e.,
 $n = 2, 6, 30, 210, \dots$

Conjecture (Voskresenskii, circa 1977): $T_n(\mathbb{F}_q)$ is rational.

Voskresenskii showed that the conjecture is true if n is a prime power or a product of two prime powers, so we know T_2 and T_6 are rational.

In fact, explicit parameterizations are available for T_2 and T_6 .

Open Question: Can we prove the conjecture for all n ?

Open Question: Can we find parameterizations for T_{30} and T_{210} ?

Stable Rationality of $T_n(\mathbb{F}_q)$

A variety V over K is **stably rational** over K if $V \times \mathbb{A}^r$ is rational for some positive integer r .

Theorem (Voskresenskii, circa 1977): $T_n(\mathbb{F}_q)$ is stably rational.

van Dijk and Woodruff: constructions with $r = \sum_{d|n, \mu(\frac{n}{d})=-1} d$, where μ is the Möbius function.

- $n = 30 \implies \phi(n) = 8, r = 32$
- $n = 210 \implies \phi(n) = 48, r = 264$

Later, van Dijk *et al.* construct representations with $n = 30, r = 2$ and $n = 210, r = 22$.

Open Question: Can we find constructions with even smaller values of r ?

Rationality of $T_2(\mathbb{F}_q)$

Suppose q is not a power of two, and pick any non-square $d \in \mathbb{F}_q^\times$ so that we can write $\mathbb{F}_{q^2} = \mathbb{F}_q[\sqrt{d}]$.

Define $\psi : \mathbb{F}_q - \{0\} \rightarrow T_2(\mathbb{F}_q) - \{\pm 1\}$ by

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

Clearly, $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\psi(a)) = 1$ for all $a \in \mathbb{F}_q$.

Define $\rho : T_2(\mathbb{F}_q) - \{\pm 1\} \rightarrow \mathbb{F}_q - \{0\}$ by

$$\rho(a + b\sqrt{d}) = \frac{1 + a}{b}.$$

We can extend this birational isomorphism to one between $T_n(\mathbb{F}_q)$ and $\mathbb{P}^1(\mathbb{F}_q)$ by defining $\psi(0) = -1$, $\rho(-1) = 0$ and $\psi(\infty) = 1$, $\rho(1) = \infty$.

Rationality of $T_2(\mathbb{F}_q)$ (continued)

Note that

$$\psi(a)\psi(b) = \psi\left(\frac{ab+d}{a+b}\right),$$

so it is not necessary to pass back and forth between $T_n(\mathbb{F}_q)$ and $\mathbb{P}^1(\mathbb{F}_q)$.

Since we have a nice formula for multiplication (not just exponentiation), we can (efficiently) do more cryptography than just the Diffie-Hellman key exchange (i.e., ElGamal public key encryption and authentication).

Rationality of $T_6(\mathbb{F}_q)$

Fix $x \in \mathbb{F}_{q^2} - \mathbb{F}_q$ so that $\mathbb{F}_{q^2} = \mathbb{F}_q(x)$. Pick 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 $\sigma \in \text{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_q)$ be an element of order two.

Define $\psi_0 : \mathbb{A}^3(\mathbb{F}_q) \hookrightarrow \mathbb{F}_{q^6}^\times$ by

$$\psi_0(u) = \frac{\gamma + x}{\gamma + \sigma(x)},$$

where $u = (u_1, u_2, u_3) \in \mathbb{A}^3(\mathbb{F}_q)$ and $\gamma = u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3 \in \mathbb{F}_{q^3}$.

Then $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(\psi_0(u)) = 1$ for every u .

Let $U = \{u \in \mathbb{A}^3(\mathbb{F}_q) \mid N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\psi_0(u)) = 1\}$. Then $\psi_0(u) \in T_6(\mathbb{F}_q)$ iff $u \in U$, so restricting ψ_0 to U gives a morphism $\psi_0 : U \rightarrow T_6(\mathbb{F}_q)$.

Hilbert's Theorem 90 implies that every element of $T_6(\mathbb{F}_q) - \{1\}$ is in $\text{im}(\psi_0)$, so $\psi_0 : U \rightarrow T_6(\mathbb{F}_q) - \{1\}$ is an isomorphism.

Rationality of $T_6(\mathbb{F}_q)$ (continued)

Any computational algebra package can be used to show that U is a hypersurface in $\mathbb{A}^3(\mathbb{F}_q)$ defined by a degree two equation in u_1, u_2, u_3 .

Fix a point $a = (a_1, a_2, a_3) \in U$ and, by adjusting the basis $\{\alpha_1, \alpha_2, \alpha_3\}$ of \mathbb{F}_{q^6} if necessary, assume that the tangent plane at a to the surface U is the plane $u_1 = a_1$.

Let $(v_1, v_2) \in \mathbb{F}_q \times \mathbb{F}_q$. The intersection of U with the line $a + t(1, v_1, v_2)$ consists of two points: a and a point of the form $a + \frac{1}{f(v_1, v_2)}(1, v_1, v_2)$, where $f(v_1, v_2) \in \mathbb{F}_q[v_1, v_2]$ can be computed by any computational algebra package.

The map $g : \mathbb{A}^2(\mathbb{F}_q) - V(f) \rightarrow U - \{a\}$ defined by

$$g(v_1, v_2) = a + \frac{1}{f(v_1, v_2)}(1, v_1, v_2),$$

where $V(f) = \{(v_1, v_2) \in \mathbb{A}^2(\mathbb{F}_q) \mid f(v_1, v_2) = 0\}$, is an isomorphism.

Rationality of $T_6(\mathbb{F}_q)$ (continued)

Finally, we have the isomorphism

$\psi : \mathbb{A}^2(\mathbb{F}_q) - V(f) \rightarrow T_6(\mathbb{F}_q) - \{1, \psi_0(a)\}$ given by

$$\psi = \psi_0 \circ g.$$

For the inverse, pick $\beta = \beta_1 + \beta_2 x \in T_6(\mathbb{F}_q) - \{1, \psi_0(a)\}$, where $\beta_1, \beta_2 \in \mathbb{F}_{q^3}$. It is easy to check that $\beta_2 \neq 0$.

Let $\gamma = \frac{1+\beta_1}{\beta_2}$. This is an element of \mathbb{F}_{q^3} , so find $u_1, u_2, u_3 \in \mathbb{F}_q$ s.t. $\gamma = u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3$.

Define $\rho : T_6(\mathbb{F}_q) - \{1, \psi_0(a)\} \rightarrow \mathbb{A}^2(\mathbb{F}_q) - V(f)$ by

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

It follows that ρ is the inverse of the isomorphism ψ .

Explicit Example of $T_6(\mathbb{F}_q)$

Fix $q \equiv 2, 5 \pmod{9}$. For $\gcd(n, q) = 1$, let ζ_n be a primitive n^{th} root of 1.

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 $\mathbb{F}_{q^3} = \mathbb{F}_q(y)$. Choose the \mathbb{F}_q -basis $\{1, y, y^2 - 2\}$ of \mathbb{F}_{q^3} . Pick $a = (0, 0, 0)$ so that $\psi_0(a) = \zeta_3^2$.

In this case we compute $f(v_1, v_2) = 1 - v_1^2 - v_2^2 + v_1v_2$, and the isomorphism $\psi : \mathbb{A}^2(\mathbb{F}_q) - V(f) \rightarrow T_6(\mathbb{F}_q) - \{1, \zeta_3^2\}$ is given by:

$$\psi(v_1, v_2) = \frac{1 + v_1y + v_2(y^2 - 2) + xf(v_1, v_2)}{1 + v_1y + v_2(y^2 - 2) + x^2f(v_1, v_2)}.$$

The inverse $\rho : T_6(\mathbb{F}_q) - \{1, \zeta_3^2\} \rightarrow \mathbb{A}^2(\mathbb{F}_q) - V(f)$ is given by:

$$\rho \left(\frac{u_2}{u_1}, \frac{u_3}{u_1} \right),$$

where $\beta = \beta_1 + \beta_2x \in T_6(\mathbb{F}_q) - \{1, \zeta_3^2\}$ and $\frac{1+\beta_1}{\beta_2} = u_1 + u_2y + u_3(y^2 - 2)$.

Diffie-Hellman in $T_n(\mathbb{F}_q)$

Choose a prime p and an integer n s.t. $T_n(\mathbb{F}_p)$ has an explicit rational parametrization, $n \log p \approx 1024$, and $\Phi_n(p)$ is a prime with at least 160 bits. Let ρ, ψ be the maps of the given parametrization.

Choose a random $\alpha \in T_n(\mathbb{F}_p)$ and let $g = \rho(\alpha) \in \mathbb{F}_p^{\varphi(n)}$.

Public data: n, p, ρ, ψ and either g or $\alpha = \psi(g)$.

The Diffie-Hellman key exchange proceeds as follows:

1. Alice picks a random integer $a \in [1, \Phi_n(p)]$ and computes $P_A = \rho(\alpha^a)$. Meanwhile, Bob picks a random integer $b \in [1, \Phi_n(p)]$ and computes $P_B = \rho(\alpha^b)$. (Recall that $P_A, P_B \in \mathbb{F}_p^{\varphi(n)}$.)
2. Alice sends P_A to Bob, while Bob sends P_B to Alice.
3. Alice computes $\rho(\psi(P_B)^a)$, while Bob computes $\rho(\psi(P_A)^b)$. They now share the private key $K = \rho(\alpha^{ab}) \in \mathbb{F}_q^{\varphi(n)}$.

Diffie-Hellman in $T_n(\mathbb{F}_q)$

Why do they share K ? Using $\psi \circ \rho = id$, we see that:

$$\rho(\psi(P_B)^a) = \rho((\alpha^b)^a) = \rho(\alpha^{ab}) = \rho((\alpha^a)^b) = \rho(\psi(P_A)^b).$$

Other applications of T_n include:

1. **ElGamal encryption/authentication**: Previously mentioned.
2. **Discrete logarithm-based voting schemes**: Improved communication and bulletin board size, but increased computational workload.
3. **Mix-nets**: Use torus-based ElGamal encryption to create savings in re-encrypting mix-nets.
4. **Pairing-based cryptography**: Tripartite Diffie-Hellman, identity-based encryption, short signatures.

Open Question: Other applications for T_n ?

Attacks on $T_n(\mathbb{F}_q)$

So far the best choices seem to be Pollard Rho in $T_n(\mathbb{F}_q)$, and index calculus in \mathbb{F}_{q^n} or $T_n(\mathbb{F}_q)$.

We have seen that Pollard Rho is exponential, while index calculus in \mathbb{F}_{q^n} is subexponential.

Granger & Vercauteren have developed an index calculus algorithm for $T_n(\mathbb{F}_{q^m})$ that outperforms Pollard Rho when $n = 2, m \geq 5$, and when $n = 6, m \geq 3$.

Open Question: Can these methods be improved?

Further Reading

- *Torus-Based Cryptography*, K. Rubin and A. Silverberg. Proc. of CRYPTO 2003, LNCS, vol. 2729, pp. 349–365, Springer, 2003.
- *Algebraic Tori in Cryptography*, K. Rubin and A. Silverberg. High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Institute Communication Series, vol. 41, pp. 317–326, AMS, 2004.
- *Using Primitive Subgroups to Do More with Fewer Bits*, K. Rubin and A. Silverberg. Proc. of ANTS VI, LNCS, vol. 3076, pp. 18–41, Springer, 2004.
- *Practical Cryptography in High Dimensional Tori*, M. van Dijk *et al.* Proc. of EUROCRYPT 2005, LNCS, vol. 3494, pp. 234–250, Springer, 2005.
- *Algebraic Groups and Their Birational Invariants*, V. E. Voskresenskiĭ. Translations of Mathematical Monographs, vol. 179, AMS, 1998.
- *The Bateman-Horn Conjecture and the Cardinality of the Primitive Subgroup of a Finite Field*, J. E. Gower. Manuscript, seven pages, 2006.
- *On the Discrete Logarithm Problem on Algebraic Tori*, R. Granger and F. Vercauteren. Proc. of CRYPTO 2005, LNCS, vol. 3621, pp. 66–85, Springer, 2005.