Applying number theory and algebraic geometry to cryptography

Alice Silverberg

October 8, 2005

AMS Meeting, Bard College

Goal

We will discuss some ways to use algebraic tori, elliptic curves, and abelian varieties to

- better understand some known cryptosystems,
- make them more efficient,
- create new efficient cryptosystems,
- attack the security of known cryptosystems.

Talk Outline

- Discrete Log Based Cryptography (Diffie-Hellman, El Gamal)
- Improvements (LUC, XTR, $\mathbb{T}_2$, CEILIDH, and beyond)
- Mathematical Interpretation via Algebraic Tori
- Elliptic Curve Analogue

Finite fields

$\mathbb{F}_q$ is the finite field with q elements.

Finite fields

$\mathbb{F}_q$ is the finite field with q elements.

$\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$, a group under multiplication.

Finite fields

$\mathbb{F}_q$ is the finite field with q elements.

$\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$, a group under multiplication.

$$|\mathbb{F}_q^\times| = q - 1$$

Finite fields

$\mathbb{F}_q$ is the finite field with q elements.

$\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$, a group under multiplication.

$$|\mathbb{F}_q^\times| = q - 1$$

The multiplicative group $\mathbb{F}_q^\times$ is cyclic.

$$\mathbb{F}_q^\times = \{g, g^2, g^3, \ldots, g^{q-1} = 1\}$$

for some $g \in \mathbb{F}_q^\times$.

Diffie-Hellman Key Agreement (1976)

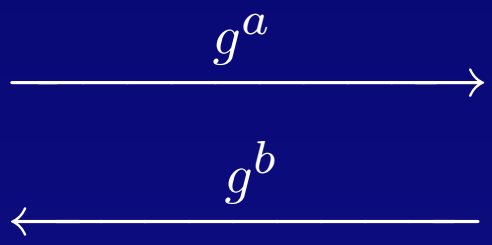
	ALICE	BOB
secrets:	a	b

Diffie-Hellman Key Agreement (1976)

	ALICE		BOB
secrets:	a		b
		$\xrightarrow{\quad g^a \quad}$	

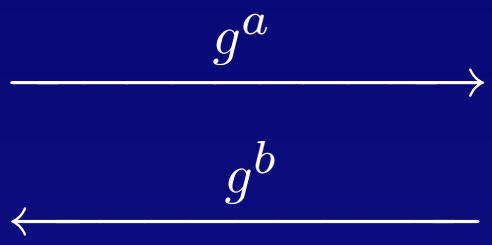
Diffie-Hellman Key Agreement (1976)

	ALICE	BOB
secrets:	a	b



Diffie-Hellman Key Agreement (1976)

	ALICE	BOB
secrets:	a	b



They share $g^{ab} = (g^b)^a = (g^a)^b$.

Diffie-Hellman Key Agreement (1976)

	ALICE		BOB
secrets:	a		b
		$\xrightarrow{\quad g^a \quad}$	
		$\xleftarrow{\quad g^b \quad}$	

They share $g^{ab} = (g^b)^a = (g^a)^b$.

Diffie-Hellman Problem:

Given g, g^a, and g^b, find g^{ab}.

Diffie-Hellman Key Agreement (1976)

	ALICE		BOB
secrets:	a		b
		$\xrightarrow{\quad g^a \quad}$	
		$\xleftarrow{\quad g^b \quad}$	

They share $g^{ab} = (g^b)^a = (g^a)^b$.

Diffie-Hellman Problem:

Given g, g^a, and g^b, find g^{ab}.

Discrete Logarithm Problem:

Given g and g^a, find a.

Cryptographic Security

For a general cyclic group of order q, there are attacks on the Discrete Logarithm Problem that run in time exponential in $\log q$.

For $\mathbb{F}_q^\times$, there are attacks on the Discrete Logarithm Problem that are subexponential in $\log q$.

Cryptographic Security

For a general cyclic group of order q, there are attacks on the Discrete Logarithm Problem that run in time exponential in $\log q$.

For $\mathbb{F}_q^\times$, there are attacks on the Discrete Logarithm Problem that are subexponential in $\log q$.

The goal is to find groups of a given size (suitable for cryptography) for which the smallest $\mathbb{F}_q^\times$ they embed in is large.

Cryptographic Security

For a general cyclic group of order q, there are attacks on the Discrete Logarithm Problem that run in time exponential in $\log q$.

For $\mathbb{F}_q^\times$, there are attacks on the Discrete Logarithm Problem that are subexponential in $\log q$.

The goal is to find groups of a given size (suitable for cryptography) for which the smallest $\mathbb{F}_q^\times$ they embed in is large. (Also need the group order to have a large prime divisor.)

Our Finite Field Goals

Use $\mathbb{F}_{q^n}^{\times}$ to improve the efficiency by a factor of $n/\varphi(n)$, where φ is Euler's phi function.

Our Finite Field Goals

Use $\mathbb{F}_{q^n}^\times$ to improve the efficiency by a factor of $n/\varphi(n)$, where φ is Euler's phi function.

Find a subgroup of $\mathbb{F}_{q^n}^\times$ of size about $q^{\varphi(n)}$ in which the Discrete Logarithm Problem is about as secure as in $\mathbb{F}_{q^n}^\times$, and efficiently represent the elements of the subgroup.

Our Finite Field Goals

Use $\mathbb{F}_{q^n}^\times$ to improve the efficiency by a factor of $n/\varphi(n)$, where φ is Euler's phi function.

Find a subgroup of $\mathbb{F}_{q^n}^\times$ of size about $q^{\varphi(n)}$ in which the Discrete Logarithm Problem is about as secure as in $\mathbb{F}_{q^n}^\times$, and efficiently represent the elements of the subgroup.

Want $n/\varphi(n)$ large. Optimal n: $1, 2, 6, 30, \ldots$

Lucas-based Key Agreement (1980's and 1990's)

$\mathbb{F}_q \subset \mathbb{F}_{q^2}$ $\qquad$ $|\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1)$

Take $g \in \mathbb{F}_{q^2}^\times$ of order $q+1$.

Lucas-based Key Agreement (1980's and 1990's)

$\mathbb{F}_q \subset \mathbb{F}_{q^2}$ $\qquad$ $|\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1)$

Take $g \in \mathbb{F}_{q^2}^\times$ of order $q+1$.

$\mathrm{Tr} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q$,

Lucas-based Key Agreement (1980's and 1990's)

$\mathbb{F}_q \subset \mathbb{F}_{q^2}$ $\qquad$ $|\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1)$

Take $g \in \mathbb{F}_{q^2}^\times$ of order $q+1$.

$\mathrm{Tr} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q, \quad x \mapsto x + x^q$

Lucas-based Key Agreement (1980's and 1990's)

$\mathbb{F}_q \subset \mathbb{F}_{q^2}$ $\qquad$ $|\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1)$

Take $g \in \mathbb{F}_{q^2}^\times$ of order $q+1$.

$\mathrm{Tr} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q, \quad x \mapsto x + x^q$

	ALICE	BOB
secrets:	a	b

Lucas-based Key Agreement (1980's and 1990's)

$\mathbb{F}_q \subset \mathbb{F}_{q^2}$ $\qquad |\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1)$

Take $g \in \mathbb{F}_{q^2}^\times$ of order $q+1$.

$\mathrm{Tr} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q, \quad x \mapsto x + x^q$

	ALICE		BOB
secrets:	a		b
		$\xrightarrow{\mathrm{Tr}(g^a)}$	

Lucas-based Key Agreement (1980's and 1990's)

$\mathbb{F}_q \subset \mathbb{F}_{q^2}$ $\qquad |\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1)$

Take $g \in \mathbb{F}_{q^2}^\times$ of order $q+1$.

$\mathrm{Tr} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q, \quad x \mapsto x + x^q$

	ALICE		BOB
secrets:	a		b
		$\mathrm{Tr}(g^a) \longrightarrow$	
		$\leftarrow \mathrm{Tr}(g^b)$	

Lucas-based Key Agreement (1980's and 1990's)

$\mathbb{F}_q \subset \mathbb{F}_{q^2}$ $\qquad |\mathbb{F}_{q^2}^\times| = q^2 - 1 = (q+1)(q-1)$

Take $g \in \mathbb{F}_{q^2}^\times$ of order $q+1$.

$\mathrm{Tr} : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q, \quad x \mapsto x + x^q$

	ALICE		BOB
secrets:	a		b
		$\xrightarrow{\mathrm{Tr}(g^a)}$	
		$\xleftarrow{\mathrm{Tr}(g^b)}$	

They share $\mathrm{Tr}(g^{ab})$. (Exercise!)

Lucas-based Key Agreement

The security is based on the difficulty of the Diffie-Hellman Problem in $\mathbb{F}_{q^2}^{\times}$.

Each party transmits only one element of $\mathbb{F}_q$ (rather than one element of $\mathbb{F}_{q^2}$).

This doubles the efficiency.

W. Müller & W. Nöbauer (1981)
H. C. Williams (1985)
P. Smith (1993): **LUC**

XTR (2000)

$$|\mathbb{F}_{q^6}^{\times}| = q^6 - 1 = (q^2 - q + 1)(q^2 + q + 1)(q^2 - 1)$$

Take $g \in \mathbb{F}_{q^6}^{\times}$ of order $q^2 - q + 1$.

$$\mathrm{Tr} : \mathbb{F}_{q^6} \longrightarrow \mathbb{F}_{q^2}, \qquad x \mapsto x + x^{q^2} + x^{q^4}$$

	ALICE		BOB
secrets:	a		b
		$\mathrm{Tr}(g^a)$ $\longrightarrow$	
		$\longleftarrow$ $\mathrm{Tr}(g^b)$	

They share $\mathrm{Tr}(g^{ab})$. (Exercise)

XTR (2000)

The security is based on the difficulty of the Diffie-Hellman Problem in $\mathbb{F}_{q^6}^{\times}$ (note that g does not lie in any proper subfield of $\mathbb{F}_{q^6}$).

Each party transmits only one element of $\mathbb{F}_{q^2}$.

This triples the efficiency.

A. Brouwer, R. Pellikaan, & E. Verheul (1999)
A. Lenstra & E. Verheul (2000)

Gong-Harn Key Agreement (1999)

$|\mathbb{F}_{q^3}^{\times}| = q^3 - 1 = (q^2 + q + 1)(q - 1)$

Take $g \in \mathbb{F}_{q^3}^{\times}$ of order $q^2 + q + 1$.

$\mathrm{Tr} : \mathbb{F}_{q^3} \longrightarrow \mathbb{F}_q, \quad x \mapsto x + x^q + x^{q^2}$

$\gamma : \mathbb{F}_{q^3} \longrightarrow \mathbb{F}_q, \quad x \mapsto x \cdot x^q + x \cdot x^{q^2} + x^q \cdot x^{q^2}$

(2 of the 3 symmetric functions on $\{x, x^q, x^{q^2}\}$)

Gong-Harn Key Agreement (1999)

	ALICE		BOB
secrets:	a		b
		$\xrightarrow{\mathrm{Tr}(g^a),\gamma(g^a)}$	
		$\xleftarrow{\mathrm{Tr}(g^b),\gamma(g^b)}$	

They share $\mathrm{Tr}(g^{ab})$ and $\gamma(g^{ab})$. (Exercise)

The security is based on the difficulty of the Diffie-Hellman Problem in $\mathbb{F}_{q^3}^{\times}$.

Each party transmits only 2 element of $\mathbb{F}_q$.

El Gamal Encryption (1985)

Alice's private key: a
Alice's public key: g^a

El Gamal Encryption (1985)

Alice's private key: a
Alice's public key: g^a

- Bob represents the message M as a power of g, and picks a random r. The ciphertext is

$$(g^r, M \cdot (g^a)^r).$$

El Gamal Encryption (1985)

Alice's private key: a
Alice's public key: g^a

- Bob represents the message M as a power of g, and picks a random r. The ciphertext is

$$(g^r, M \cdot (g^a)^r).$$

- To decrypt a ciphertext (c, d), Alice computes $M = d \cdot c^{-a}$.

XTR

XTR and LUC work because $\mathrm{Tr}(g^a)$ and b determine $\mathrm{Tr}(g^{ab})$.

XTR

XTR and LUC work because $\mathrm{Tr}(g^a)$ and b determine $\mathrm{Tr}(g^{ab})$.

In other words, XTR and LUC can exponentiate.

XTR

XTR and LUC work because $\mathrm{Tr}(g^a)$ and b determine $\mathrm{Tr}(g^{ab})$.

In other words, XTR and LUC can exponentiate.

However, XTR and LUC cannot multiply:

XTR

XTR and LUC work because $\mathrm{Tr}(g^a)$ and b determine $\mathrm{Tr}(g^{ab})$.

In other words, XTR and LUC can exponentiate.

However, XTR and LUC cannot multiply:

$\mathrm{Tr}(h)$ and $\mathrm{Tr}(k)$ do not determine $\mathrm{Tr}(hk)$.

XTR

XTR and LUC work because $\mathrm{Tr}(g^a)$ and b determine $\mathrm{Tr}(g^{ab})$.

In other words, XTR and LUC can exponentiate.

However, XTR and LUC cannot multiply:

$\mathrm{Tr}(h)$ and $\mathrm{Tr}(k)$ do not determine $\mathrm{Tr}(hk)$.

To do efficient El Gamal encryption and signatures, one needs to be able to multiply.

XTR

XTR and LUC work because $\mathrm{Tr}(g^a)$ and b determine $\mathrm{Tr}(g^{ab})$.

In other words, XTR and LUC can exponentiate.

However, XTR and LUC cannot multiply:

$\mathrm{Tr}(h)$ and $\mathrm{Tr}(k)$ do not determine $\mathrm{Tr}(hk)$.

To do efficient El Gamal encryption and signatures, one needs to be able to multiply.

The CEILIDH cryptosystem can multiply and exponentiate.

XTR

XTR = **ECSTR** =

Efficient Compact Subgroup Trace Representation

Silverberg, AMS Bard

CEILIDH

CEILIDH is Compact, Efficient, Improves on LUC, and Improves on Diffie-Hellman

Silverberg, AMS Bard

CEILIDH can multiply; LUC and XTR can't

Silverberg, AMS Bard

CEILIDH (2003, Rubin & Silverberg)

As in XTR, take $g \in \mathbb{F}_{q^6}^{\times}$ of order $q^2 - q + 1$.

Let

$$G_6 = \{g, g^2, \ldots, g^{q^2-q+1} = 1\}.$$

CEILIDH (2003, Rubin & Silverberg)

We found an efficiently computable "compression" function f, satisfying the following properties:

- $f : G_6 \dashrightarrow \mathbb{F}_q \times \mathbb{F}_q$ is defined almost everywhere,
- can compute $f(g^{ab})$ from $f(g^a)$ and b,
- can compute $f(hk)$ from $f(h)$ and $f(k)$,
- f has an efficiently computable inverse

$$j : \mathbb{F}_q \times \mathbb{F}_q \to G_6.$$

CEILIDH

Use $f : G_6 \dashrightarrow \mathbb{F}_q \times \mathbb{F}_q$ to compress powers of $g \in \mathbb{F}_{q^6}^{\times}$.

Use $j : \mathbb{F}_q \times \mathbb{F}_q \longrightarrow G_6$ to decompress elements of $\mathbb{F}_q \times \mathbb{F}_q$, in order to use the group law in $G_6 \subset \mathbb{F}_{q^6}^{\times}$.

CEILIDH Diffie-Hellman Key Agreement

	ALICE	BOB
secrets:	a	b

CEILIDH Diffie-Hellman Key Agreement

	ALICE		BOB
secrets:	a		b
		$\xrightarrow{f(g^a)}$	

CEILIDH Diffie-Hellman Key Agreement

	ALICE		BOB
secrets:	a		b
		$f(g^a)$ $\longrightarrow$	
		$\longleftarrow$ $f(g^b)$	

CEILIDH Diffie-Hellman Key Agreement

	ALICE		BOB
secrets:	a		b
		$f(g^a)$ $\longrightarrow$	
		$\longleftarrow$ $f(g^b)$	

They share $f(g^{ab})$.

CEILIDH El Gamal Encryption

Alice's private key: a
Alice's public key: $f(g^a) \in \mathbb{F}_q^2$

- Bob represents the message M as a power of g, and picks a random r. The ciphertext is

$$(f(g^r), f(M \cdot j(f(g^a))^r)).$$

- To decrypt a ciphertext (c, d), Alice computes $M = j(d) \cdot j(c)^{-a}$.

The $\mathbb{T}_2$ cryptosystem

It's even easier to do the analogous thing with $\mathbb{F}_{q^2}$, instead of $\mathbb{F}_{q^6}$.

The $\mathbb{T}_2$ cryptosystem

It's even easier to do the analogous thing with $\mathbb{F}_{q^2}$, instead of $\mathbb{F}_{q^6}$.

As was the case for the Lucas-based cryptosystems, take $g \in \mathbb{F}_{q^2}^{\times}$ of order $q+1$.

Let

$$G_2 = \{g, g^2, \ldots, g^{q+1} = 1\}.$$

Write

$$\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{D}).$$

The $\mathbb{T}_2$ cryptosystem

$$G_2 - \{1, -1\} \xrightarrow{f} \mathbb{F}_q$$

$$a + b\sqrt{D} \xmapsto{f} \frac{1+a}{b}$$

$$G_2 \xleftarrow{j} \mathbb{F}_q$$

$$\frac{\alpha+\sqrt{D}}{\alpha-\sqrt{D}} \xleftarrow{j} \alpha$$

The $\mathbb{T}_2$ cryptosystem

$$G_2 - \{1, -1\} \xrightarrow{f} \mathbb{F}_q$$

$$a + b\sqrt{D} \xmapsto{f} \frac{1+a}{b}$$

$$G_2 \xleftarrow{j} \mathbb{F}_q$$

$$\frac{\alpha+\sqrt{D}}{\alpha-\sqrt{D}} \xleftarrow{j} \alpha$$

To do Diffie-Hellman and El Gamal, use the group law on G_2, and use f to efficiently represent the elements of G_2 in $\mathbb{F}_q$.

The $\mathbb{T}_2$ cryptosystem

There's no need to decompress elements of $\mathbb{F}_q$, since one can use

$$j(\alpha)j(\beta) = j\left(\frac{\alpha\beta + D}{\alpha + \beta}\right)$$

to translate G_2's multiplication to $\mathbb{F}_q$.

Can do everything in $\mathbb{F}_q$, without using $\mathbb{F}_{q^2}$.

An example of CEILIDH

Choose a prime power $q \equiv 2$ or $5 \pmod 9$.

Let $\zeta_9 \in \mathbb{F}_{q^6}$ be a primitive ninth root of 1 and let $\zeta_3 = \zeta_9^3$.

We'll define

$$G_6 - \{1, \zeta_3^2\} \xrightarrow{f} \mathbb{F}_q \times \mathbb{F}_q$$

$$G_6 \xleftarrow{j} \mathbb{F}_q \times \mathbb{F}_q$$

An example of CEILIDH

$$a + b\zeta_3 \xrightarrow{\ f\ } \left(\frac{u}{w}, \frac{v}{w}\right)$$

$$\frac{s+r\zeta_3}{s+r\zeta_3^2} \xleftarrow{\ j\ } (x, y)$$

where $a, b \in \mathbb{F}_{q^3}$,

$$\frac{1+a}{b} = w + u(\zeta_9 + \zeta_9^{-1}) + v(\zeta_9^2 + \zeta_9^{-2}),$$

$$r = 1 - x^2 - y^2 + xy,$$

$$s = 1 + x(\zeta_9 + \zeta_9^{-1}) + y(\zeta_9^2 + \zeta_9^{-2}).$$

Beyond XTR

A. Lenstra and others asked if one can use symmetric polynomials to generalize XTR to $\mathbb{F}_{q^{30}}$ and beyond.

In "Looking beyond XTR", W. Bosma, J. Hutton, & E. Verheul (2002) gave some precise conjectures for 30 and beyond, involving symmetric polynomials.

Beyond XTR

A. Lenstra and others asked if one can use symmetric polynomials to generalize XTR to $\mathbb{F}_{q^{30}}$ and beyond.

In "Looking beyond XTR", W. Bosma, J. Hutton, & E. Verheul (2002) gave some precise conjectures for 30 and beyond, involving symmetric polynomials.

K. Rubin and I disproved the conjectures and showed that symmetric functions are not the right functions to consider.

Cyclotomic Polynomials

Let Φ_n denote the n-th cyclotomic polynomial:

$$\Phi_1(x) = x - 1,$$

$$\Phi_2(x) = x + 1,$$

$$\Phi_6(x) = x^2 - x + 1,$$

$$\deg(\Phi_n(x)) = \varphi(n),$$

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \quad \Rightarrow \quad \Phi_n(q) | (q^n - 1) = |\mathbb{F}_{q^n}^{\times}|$$

Beyond XTR and CEILIDH

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

Beyond XTR and CEILIDH

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

Goal: represent (most) elements of G_n using $\varphi(n)$ elements of $\mathbb{F}_q$, to give an efficiency gain of $n/\varphi(n)$.

Beyond XTR and CEILIDH

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

Goal: represent (most) elements of G_n using $\varphi(n)$ elements of $\mathbb{F}_q$, to give an efficiency gain of $n/\varphi(n)$.

The Lucas-based crytosystems and the $\mathbb{T}_2$ cryptosystem do this for $n = 2$; here $n/\varphi(n) = 2$.

Beyond XTR and CEILIDH

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

Goal: represent (most) elements of G_n using $\varphi(n)$ elements of $\mathbb{F}_q$, to give an efficiency gain of $n/\varphi(n)$.

The Lucas-based crytosystems and the $\mathbb{T}_2$ cryptosystem do this for $n = 2$; here $n/\varphi(n) = 2$.

XTR and CEILIDH do this for $n = 6$; here $n/\varphi(n) = 3$.

Beyond XTR and CEILIDH

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

Goal: represent (most) elements of G_n using $\varphi(n)$ elements of $\mathbb{F}_q$, to give an efficiency gain of $n/\varphi(n)$.

The Lucas-based crytosystems and the $\mathbb{T}_2$ cryptosystem do this for $n = 2$; here $n/\varphi(n) = 2$.

XTR and CEILIDH do this for $n = 6$; here $n/\varphi(n) = 3$.

The next interesting case is $n = 30$; here $n/\varphi(n) = 30/8 = 3.75$.

Beyond XTR and CEILIDH

It is not known how to usefully represent (most) elements of G_{30} using 8 elements of $\mathbb{F}_q$.

Beyond XTR and CEILIDH

It is not known how to usefully represent (most) elements of G_{30} using 8 elements of $\mathbb{F}_q$.

However, for all n there is an A such that (most) elements of $G_n \times \mathbb{F}_q^A$ can be represented using $\varphi(n) + A$ elements of $\mathbb{F}_q$.

Beyond XTR and CEILIDH

It is not known how to usefully represent (most) elements of G_{30} using 8 elements of $\mathbb{F}_q$.

However, for all n there is an A such that (most) elements of $G_n \times \mathbb{F}_q^A$ can be represented using $\varphi(n) + A$ elements of $\mathbb{F}_q$.

M. van Dijk and D. Woodruff (2004) found a clever way to use the "excess" $\mathbb{F}_q^A$ to encode the message being encrypted or signed, so that it doesn't go to waste.

van Dijk-Woodruff's Asymptotically Optimal Cryptosystems

They use

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

where $\mu(m) = (-1)^r$ if m is a product of r distinct primes, to obtain an "almost bijection" between $G_n \times \mathbb{F}_q^A$ and $\mathbb{F}_q^B$, with $A = \sum_{d|n, \mu(n/d)=-1} d$ and $B = \sum_{d|n, \mu(n/d)=1} d$.

van Dijk-Woodruff's Asymptotically Optimal Cryptosystems

They use

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

where $\mu(m) = (-1)^r$ if m is a product of r distinct primes, to obtain an "almost bijection" between $G_n \times \mathbb{F}_q^A$ and $\mathbb{F}_q^B$, with $A = \sum_{d|n, \mu(n/d)=-1} d$ and $B = \sum_{d|n, \mu(n/d)=1} d$.

This gives an "almost bijection" between $G_{30} \times \mathbb{F}_q^{32}$ and $\mathbb{F}_q^{40}$.

van Dijk-Granger-Page-Rubin-Silverberg-Stam-Woodruff (2005)

We obtain an "almost bijection" between $G_n \times \mathbb{F}_q^{n/3-\varphi(n)}$ and $\mathbb{F}_q^{n/3}$, and thus an "almost bijection" between $G_{30} \times \mathbb{F}_q^2$ and $\mathbb{F}_q^{10}$.

We obtain this using CEILIDH and the equation:

$$\Phi_n(x) \prod_{i=2}^{r-1} \Phi_{p_1 \cdots p_i}(x^{p_{i+2} \cdots p_r}) = \Phi_{p_1 p_2}(x^{p_3 \cdots p_r})$$

for $n = p_1 \cdots p_r$ a product of $r \geq 2$ distinct primes.

Attacks on Discrete Log in $\mathbb{F}_{q^n}^\times$

Granger and Vercauteren (2005), using ideas of Gaudry in the elliptic curve case, exploit the efficient representation of elements of G_2 and G_6 to mount a new kind of attack on the Discrete Logarithm Problem in fields of the form $\mathbb{F}_{q^{2m}}^\times$ and $\mathbb{F}_{q^{6m}}^\times$ for large m.

Torus-based Cryptography

Diffie-Hellman, El Gamal, the $\mathbb{T}_2$ cryptosystem, and CEILIDH are based on certain algebraic groups, i.e., groups that are defined by polynomials. This allows these systems to make full use of the multiplication.

Torus-based Cryptography

Diffie-Hellman, El Gamal, the $\mathbb{T}_2$ cryptosystem, and CEILIDH are based on certain algebraic groups, i.e., groups that are defined by polynomials. This allows these systems to make full use of the multiplication. The algebraic groups are algebraic tori.

Torus-based Cryptography

Diffie-Hellman, El Gamal, the $\mathbb{T}_2$ cryptosystem, and CEILIDH are based on certain algebraic groups, i.e., groups that are defined by polynomials. This allows these systems to make full use of the multiplication. The algebraic groups are algebraic tori.

The Lucas-based cryptosystems and XTR are based on algebraic varieties that are *not* groups. They are quotients of algebraic tori by the action of symmetric groups.

Weil Restriction of Scalars

From now on:

L/k is a cyclic extension of square-free degree n.

E.g., $k = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$.

G is a commutative algebraic group over k (e.g., the multiplicative group $\mathbb{G}_m$ or an elliptic curve).

$\mathrm{Res}_{L/k}G$ is a commutative algebraic group over k such that

$$(\mathrm{Res}_{L/k}G)(k) = G(L).$$

Example: $\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m$

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

The multiplicative group $\mathbb{G}_m$ is defined by $xy = 1$.

Example: $\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m$

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

The multiplicative group $\mathbb{G}_m$ is defined by $xy = 1$.

Write
$\mathbb{F}_9 = \mathbb{F}_3(\sqrt{-1}), x = x_1 + x_2\sqrt{-1}, y = y_1 + y_2\sqrt{-1}$,
substitute into $xy = 1$, and equate coefficients to obtain defining equations for $\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m$:

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

Primitive Subgroups

The primitive subgroup $G_{L/k} \subset \mathrm{Res}_{L/k}G$ is

$$G_{L/k} := \ker\Big[\mathrm{Res}_{L/k}G \xrightarrow{\oplus \mathrm{N}_{L/F}} \bigoplus_{k\subseteq F\subsetneq L} \mathrm{Res}_{F/k}G\Big].$$

Primitive Subgroups

The primitive subgroup $G_{L/k} \subset \mathrm{Res}_{L/k}G$ is

$$G_{L/k} := \ker\Big[\mathrm{Res}_{L/k}G \xrightarrow{\oplus \mathrm{N}_{L/F}} \bigoplus_{k\subseteq F\subsetneq L} \mathrm{Res}_{F/k}G\Big].$$

$G_{L/k}$ is a commutative algebraic group over k whose dimension is $\varphi(n)\dim(G)$.

Primitive Subgroups

The primitive subgroup $G_{L/k} \subset \mathrm{Res}_{L/k}G$ is

$$G_{L/k} := \ker\Big[\mathrm{Res}_{L/k}G \xrightarrow{\oplus \mathrm{N}_{L/F}} \bigoplus_{k\subseteq F\subsetneq L} \mathrm{Res}_{F/k}G\Big].$$

$G_{L/k}$ is a commutative algebraic group over k whose dimension is $\varphi(n)\dim(G)$.

$$\mathrm{Res}_{L/k}G \sim \bigoplus_{k\subseteq F\subseteq L} G_{F/k} = G \times \cdots \times G_{L/k}$$

Example: $(\mathbb{G}_m)_{\mathbb{F}_9/\mathbb{F}_3}$

$$\begin{aligned} \mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m &\sim (\mathbb{G}_m)_{\mathbb{F}_3/\mathbb{F}_3} \times (\mathbb{G}_m)_{\mathbb{F}_9/\mathbb{F}_3} \\ &= \mathbb{G}_m \times \ker(\mathrm{N}_{\mathbb{F}_9/\mathbb{F}_3}) \end{aligned}$$

Example: $(\mathbb{G}_m)_{\mathbb{F}_9/\mathbb{F}_3}$

$$\begin{aligned}\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m &\sim (\mathbb{G}_m)_{\mathbb{F}_3/\mathbb{F}_3} \times (\mathbb{G}_m)_{\mathbb{F}_9/\mathbb{F}_3} \\ &= \mathbb{G}_m \times \ker(\mathrm{N}_{\mathbb{F}_9/\mathbb{F}_3})\end{aligned}$$

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

$$(xx_1, xx_2, x^{-1}x_1, -x^{-1}x_2) \longmapsto (x, x_1 + x_2\sqrt{-1})$$

Both compositions are squaring.

Example: $(\mathbb{G}_m)_{\mathbb{F}_9/\mathbb{F}_3}$

$$\begin{aligned}\mathrm{Res}_{\mathbb{F}_9/\mathbb{F}_3}\mathbb{G}_m &\sim (\mathbb{G}_m)_{\mathbb{F}_3/\mathbb{F}_3} \times (\mathbb{G}_m)_{\mathbb{F}_9/\mathbb{F}_3} \\ &= \mathbb{G}_m \times \ker(\mathrm{N}_{\mathbb{F}_9/\mathbb{F}_3})\end{aligned}$$

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

$$(xx_1, xx_2, x^{-1}x_1, -x^{-1}x_2) \longmapsto (x, x_1 + x_2\sqrt{-1})$$

Both compositions are squaring.

$(\mathbb{G}_m)_{\mathbb{F}_9/\mathbb{F}_3}$ is a one-dimensional algebraic torus.

Algebraic tori

An *algebraic torus* over k is an algebraic group over k that over some larger field is isomorphic to a product of multiplicative groups $\mathbb{G}_m$.

Algebraic tori

An *algebraic torus* over k is an algebraic group over k that over some larger field is isomorphic to a product of multiplicative groups $\mathbb{G}_m$.

$\mathrm{Res}_{L/k}\mathbb{G}_m$ is an algebraic torus of dimension n.

Algebraic tori

An *algebraic torus* over k is an algebraic group over k that over some larger field is isomorphic to a product of multiplicative groups $\mathbb{G}_m$.

$\mathrm{Res}_{L/k}\mathbb{G}_m$ is an algebraic torus of dimension n.

$(\mathbb{G}_m)_{L/k}$ is an algebraic torus of dimension $\varphi(n)$.

Algebraic tori

An *algebraic torus* over k is an algebraic group over k that over some larger field is isomorphic to a product of multiplicative groups $\mathbb{G}_m$.

$\mathrm{Res}_{L/k}\mathbb{G}_m$ is an algebraic torus of dimension n.

$(\mathbb{G}_m)_{L/k}$ is an algebraic torus of dimension $\varphi(n)$.

From now on, let $L = \mathbb{F}_{q^n}$ and $k = \mathbb{F}_q$, and let

$$\mathbb{T}_{q,n} = (\mathbb{G}_m)_{L/k}.$$

Algebraic tori

$\mathbb{T}_{q,n}(\mathbb{F}_q) = G_n$, the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$.

Algebraic tori

$\mathbb{T}_{q,n}(\mathbb{F}_q) = G_n$, the subgroup of $\mathbb{F}_{q^n}^\times$ of order $\Phi_n(q)$.

If p is prime divisor of n, then there is an action of the symmetric group S_p on the torus $\mathbb{T}_{q,n}$.

Algebraic tori

$\mathbb{T}_{q,n}(\mathbb{F}_q) = G_n$, the subgroup of $\mathbb{F}_{q^n}^{\times}$ of order $\Phi_n(q)$.

If p is prime divisor of n, then there is an action of the symmetric group S_p on the torus $\mathbb{T}_{q,n}$.

XTR is based on the quotient variety $\mathbb{T}_{q,6}/S_3$.

Algebraic tori

$\mathbb{T}_{q,n}(\mathbb{F}_q) = G_n$, the subgroup of $\mathbb{F}_{q^n}^{\times}$ of order $\Phi_n(q)$.

If p is prime divisor of n, then there is an action of the symmetric group S_p on the torus $\mathbb{T}_{q,n}$.

XTR is based on the quotient variety $\mathbb{T}_{q,6}/S_3$.

The Lucas-based cryptosystems are based on $\mathbb{T}_{q,2}/S_2$.

Algebraic tori

$\mathbb{T}_{q,n}(\mathbb{F}_q) = G_n$, the subgroup of $\mathbb{F}_{q^n}^{\times}$ of order $\Phi_n(q)$.

If p is prime divisor of n, then there is an action of the symmetric group S_p on the torus $\mathbb{T}_{q,n}$.

XTR is based on the quotient variety $\mathbb{T}_{q,6}/S_3$.

The Lucas-based cryptosystems are based on $\mathbb{T}_{q,2}/S_2$.

Gong-Harn is based on the $\mathbb{T}_{q,3}/S_3$.

Algebraic tori

$\mathbb{T}_{q,n}(\mathbb{F}_q) = G_n$, the subgroup of $\mathbb{F}_{q^n}^{\times}$ of order $\Phi_n(q)$.

If p is prime divisor of n, then there is an action of the symmetric group S_p on the torus $\mathbb{T}_{q,n}$.

XTR is based on the quotient variety $\mathbb{T}_{q,6}/S_3$.

The Lucas-based cryptosystems are based on $\mathbb{T}_{q,2}/S_2$.

Gong-Harn is based on the $\mathbb{T}_{q,3}/S_3$.

The conjectured systems in "Looking beyond XTR" are based on $\mathbb{T}_{q,30}/(S_2 \times S_3 \times S_5)$ and $\mathbb{T}_{q,30}/(S_3 \times S_5)$.

Algebraic tori

Diffie-Hellman is based on $\mathbb{T}_{q,1} = \mathbb{G}_m$.

Algebraic tori

Diffie-Hellman is based on $\mathbb{T}_{q,1} = \mathbb{G}_m$.

The $\mathbb{T}_2$-cryptosystem is based on $\mathbb{T}_{q,2}$.

Algebraic tori

Diffie-Hellman is based on $\mathbb{T}_{q,1} = \mathbb{G}_m$.

The $\mathbb{T}_2$-cryptosystem is based on $\mathbb{T}_{q,2}$.

CEILIDH is based on the algebraic torus $\mathbb{T}_{q,6}$.

Algebraic tori

Diffie-Hellman is based on $\mathbb{T}_{q,1} = \mathbb{G}_m$.

The $\mathbb{T}_2$-cryptosystem is based on $\mathbb{T}_{q,2}$.

CEILIDH is based on the algebraic torus $\mathbb{T}_{q,6}$.

The maps f and j are birational isomorphisms between the torus and affine space of the same dimension.

Algebraic tori

Diffie-Hellman is based on $\mathbb{T}_{q,1} = \mathbb{G}_m$.

The $\mathbb{T}_2$-cryptosystem is based on $\mathbb{T}_{q,2}$.

CEILIDH is based on the algebraic torus $\mathbb{T}_{q,6}$.

The maps f and j are birational isomorphisms between the torus and affine space of the same dimension.

Fact (Klyachko): The tori $\mathbb{T}_{q,n}$ are rational (i.e., birationally isomorphic to affine space) whenever n is divisible by at most 2 distinct primes.

Voskresenskii's Conjecture

The tori $\mathbb{T}_{q,n}$ are rational; i.e., there is a birational isomorphism

$$\mathbb{T}_{q,n} \quad \dashleftarrow\!\!\dashrightarrow \quad \mathbb{A}^{\varphi(n)}.$$

Voskresenskii's Conjecture

The tori $\mathbb{T}_{q,n}$ are rational; i.e., there is a birational isomorphism

$$\mathbb{T}_{q,n} \quad \dashleftarrow\!\!\dashrightarrow \quad \mathbb{A}^{\varphi(n)}.$$

Not known for $n = 30$.

Asymptotically Optimal Communication for Torus-Based Cryptography

M. van Dijk and Woodruff got around Voskresenskii's Conjecture by using only that the torus $\mathbb{T}_{q,n}$ is stably rational, i.e., $\mathbb{T}_{q,n} \times \mathbb{A}^A$ is birationally isomorphic to $\mathbb{A}^B$ for some A and B.

Elliptic Curves

An elliptic curve E over a finite field $\mathbb{F}_q$ is a nonsingular curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with the a_i's in $\mathbb{F}_q$.

Elliptic Curves

An elliptic curve E over a finite field $\mathbb{F}_q$ is a nonsingular curve of the form

$$y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6$$

with the a_i's in $\mathbb{F}_q$.

One can define a natural addition law on the $\mathbb{F}_q$-solutions so that, along with the point at infinity, they form an abelian group $E(\mathbb{F}_q)$ of order $\approx q$.

Elliptic Curve Cryptography

- V. Miller, 1985.
- N. Koblitz, 1987.

In place of the group $\mathbb{F}_q^\times$, use $E(\mathbb{F}_q)$
(in Diffie-Hellman, El Gamal, etc.).

To "compress" an elliptic curve point (x, y), drop the y-coordinate and send a bit that allows y to be reconstructed from x and the equation for E.

Rubin-Silverberg EC Point Compression

E an elliptic curve over k, $n = [L : k]$ prime:

$$\mathrm{Res}_{L/k} E \sim E \times E_{L/k} = E \times \ker(\mathrm{Tr}_{L/k})$$

Rubin-Silverberg EC Point Compression

E an elliptic curve over k, $n = [L : k]$ prime:

$$\mathrm{Res}_{L/k} E \sim E \times E_{L/k} = E \times \ker(\mathrm{Tr}_{L/k})$$

If $P = (x, y) \in E_{L/k}(k) \subset E(L)$, write
$x = \sum_{i=1}^{n} x_i e_i$ wrt a basis $\{e_1, \ldots, e_n\}$ for L/k.

Rubin-Silverberg EC Point Compression

E an elliptic curve over k, $n = [L : k]$ prime:

$$\mathrm{Res}_{L/k} E \sim E \times E_{L/k} = E \times \ker(\mathrm{Tr}_{L/k})$$

If $P = (x, y) \in E_{L/k}(k) \subset E(L)$, write $x = \sum_{i=1}^{n} x_i e_i$ wrt a basis $\{e_1, \ldots, e_n\}$ for L/k.

Compress P to $(x_2, \ldots, x_n)$, and send a few extra bits that allow reconstruction of P from $(x_2, \ldots, x_n)$, the equation for E, and the equation $\mathrm{Tr}(P) = 0$.

Rubin-Silverberg EC Point Compression

E an elliptic curve over k, $n = [L : k]$ prime:

$$\mathrm{Res}_{L/k} E \sim E \times E_{L/k} = E \times \ker(\mathrm{Tr}_{L/k})$$

If $P = (x, y) \in E_{L/k}(k) \subset E(L)$, write $x = \sum_{i=1}^{n} x_i e_i$ wrt a basis $\{e_1, \ldots, e_n\}$ for L/k.

Compress P to $(x_2, \ldots, x_n)$, and send a few extra bits that allow reconstruction of P from $(x_2, \ldots, x_n)$, the equation for E, and the equation $\mathrm{Tr}(P) = 0$.

We can do this efficiently when $n = 2, 3$, or 5.

Rubin-Silverberg EC Point Compression

In other words, we are finding explicit rational maps of small degree

$$E_{L/k} \longrightarrow \mathbb{A}^{n-1}$$

over k.

Cryptographic Security

If G is a commutative algebraic group over $k = \mathbb{F}_q$, let $c(G, k)$ be the smallest c such that every cyclic subgroup of $G(k)$ embeds in $\mathbb{F}_{q^c}^{\times}$.

Cryptographic Security

If G is a commutative algebraic group over $k = \mathbb{F}_q$, let $c(G, k)$ be the smallest c such that every cyclic subgroup of $G(k)$ embeds in $\mathbb{F}_{q^c}^{\times}$.

$c(G_{L/k}, k) = c(G, L)$ for $G = \mathbb{G}_m$ or a supersingular elliptic curve E over k with $(n, 2qc(E, k)) = 1$, where $n = [L : k]$.

Cryptographic Security

If G is a commutative algebraic group over $k = \mathbb{F}_q$, let $c(G, k)$ be the smallest c such that every cyclic subgroup of $G(k)$ embeds in $\mathbb{F}_{q^c}^{\times}$.

$c(G_{L/k}, k) = c(G, L)$ for $G = \mathbb{G}_m$ or a supersingular elliptic curve E over k with $(n, 2qc(E, k)) = 1$, where $n = [L : k]$.

Thus in these cases, the subgroup $G_{L/k}(k)$ is as secure as $G(L)$ against the classical subexponential attacks on the Discrete Logarithm Problem in finite fields, and is smaller.

Abelian Varieties

The fact that this works in the elliptic curve case can be proved using abelian varieties.

An abelian variety is a connected projective algebraic group.

The one-dimensional abelian varieties are exactly the elliptic curves.

Our results were inspired by earlier work of S. Galbraith.

Attacks on Discrete Log in $E(\mathbb{F}_{q^n})$

Gaudry recently exploited the Weil restriction of scalars to mount a new kind of attack on the Discrete Logarithm Problem in $E(\mathbb{F}_{q^n})$ for certain n.

The future

- Find a birational isomorphism between $\mathbb{T}_{q,30}$ and $\mathbb{A}^8$.
- Study attacks on the Discrete Logarithm Problem that use the torus structure (understand current ones and find new ones).
- Find good decompression algorithms for primitive subgroups of elliptic curves when $n > 5$.

Some references

Supersingular abelian varieties in cryptology, Rubin & Silverberg, CRYPTO 2002

Torus-based cryptography, Rubin & Silverberg, CRYPTO 2003

Using primitive subgroups to do more with fewer bits, Rubin & Silverberg, ANTS VI, 2004

Asymptotically Optimal Communication for Torus-Based Cryptography, van Dijk & Woodruff, CRYPTO 2004

Some references

Practical Cryptography in High Dimensional Tori, van Dijk, Granger, Page, Rubin, Silverberg, Stam & Woodruff, EUROCRYPT 2005

On the discrete logarithm problem on algebraic tori, Granger & Vercauteren, CRYPTO 2005

Index calculus for abelian varieties and the elliptic curve discrete logarithm problem, Gaudry, preprint

Applying number theory and algebraic geometry to cryptography

Alice Silverberg

October 8, 2005

AMS Meeting, Bard College