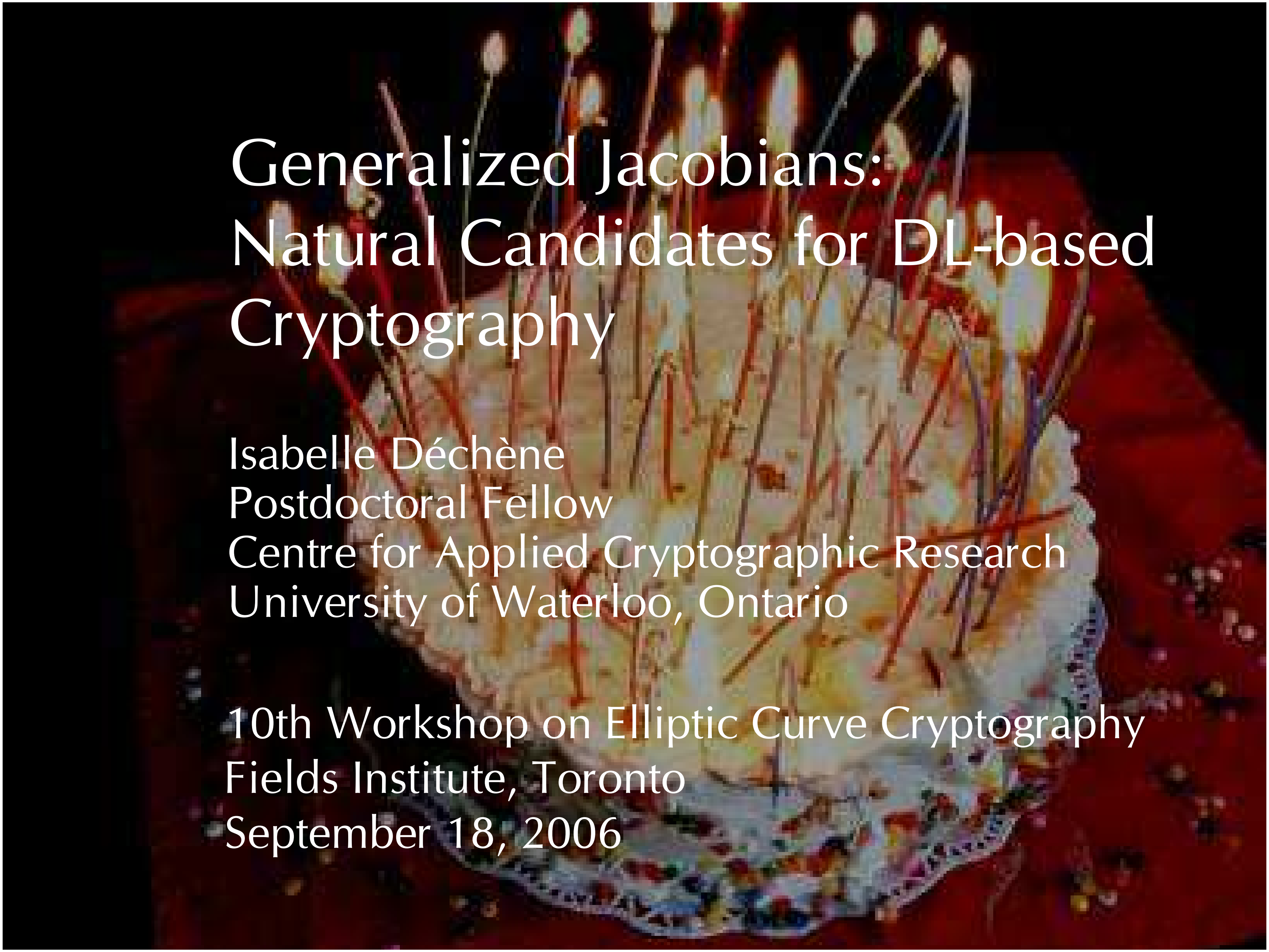
Huge thanks to Edlyn Teske for presenting my talk at ANTS in Berlin.

Special thanks also goes to everyone who signed the postcard…
It was greatly appreciated!!!



# Generalized Jacobians: Natural Candidates for DL-based Cryptography

Isabelle Déchène
Postdoctoral Fellow
Centre for Applied Cryptographic Research
University of Waterloo, Ontario

10th Workshop on Elliptic Curve Cryptography
Fields Institute, Toronto
September 18, 2006

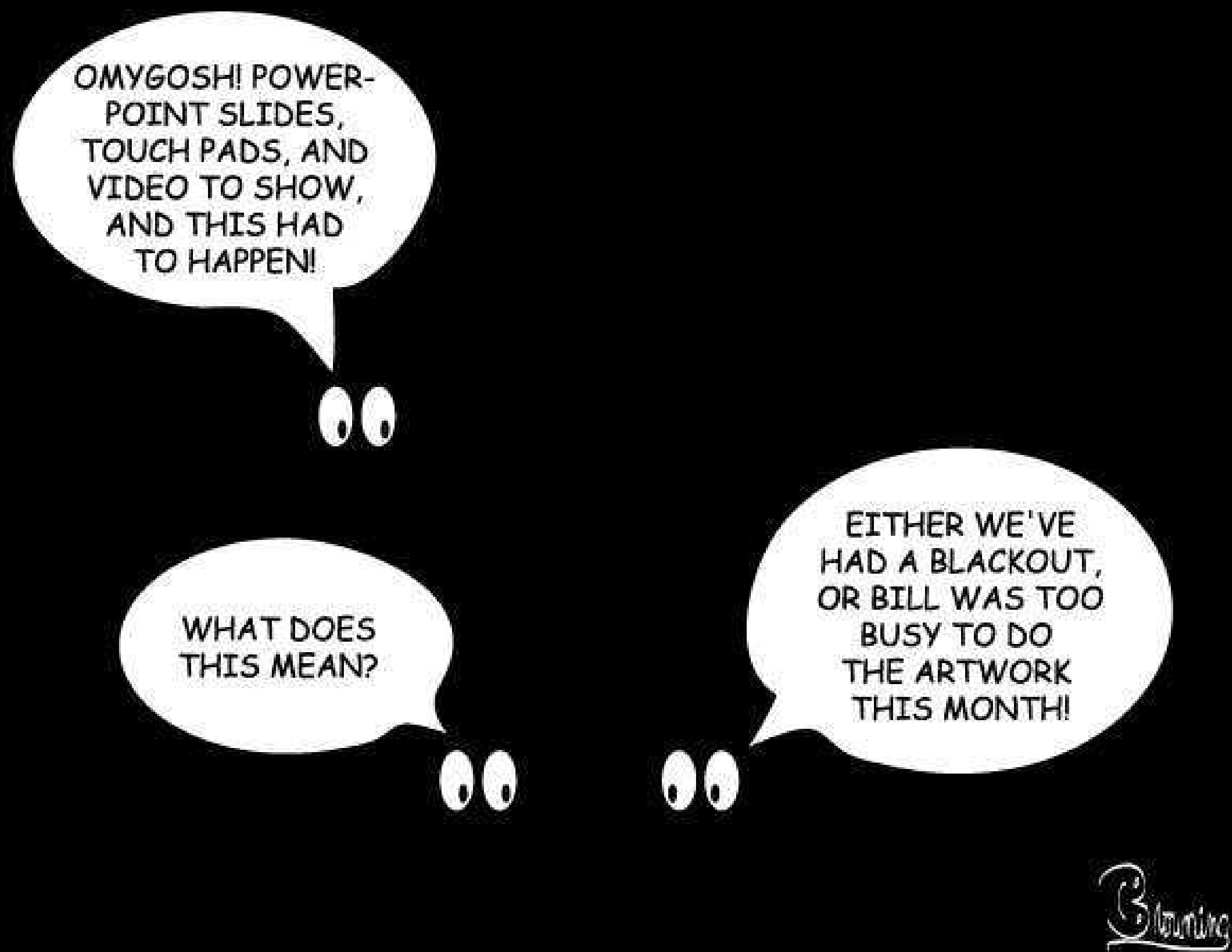
# ECC 2003 at the University of Waterloo

My first ECC Workshop made me *really* grasp the importance of abelian varieties in cryptography, like elliptic curves and Jacobians of hyperelliptic curves.

That of course raises the following question:

*Are there any other algebraic groups that one could use for crypto applications?*

# SAC 2003 at Carleton University



# CRYPTO 2003

At CRYPTO 2003, Alice Silverberg presented her joint work with Karl Rubin on Torus-based Cryptography.

This talk had a crucial influence on my perception of DL-based crypto…

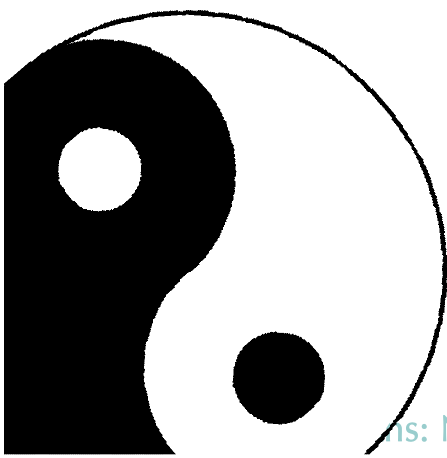
- On one hand, *Jacobians of curves* (of small genus) gained the favor of many over the years, mostly because of the smaller key size needed.
- On the other hand, *algebraic tori* offer the really neat advantage of compactly representing elements…

# Initial Observation

So it seems that these two sub-families of algebraic groups somehow have *complementary* cryptographic properties…

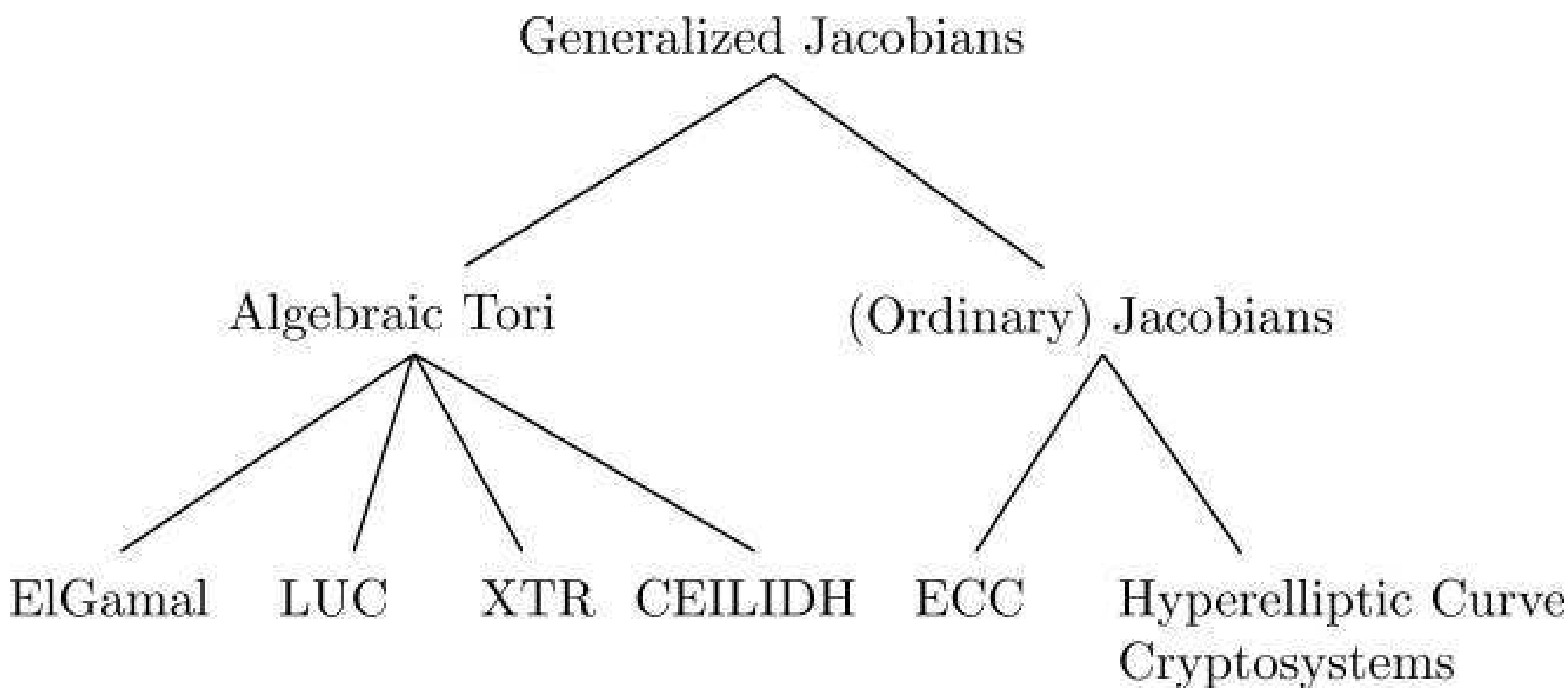
From a mathematical point of view, however, they can both be seen as two realizations of a *single* concept:

## Generalized Jacobians



As a result, several existing DL-based cryptosystems possess an underlying structure that can be naturally reinterpreted in terms of generalized Jacobians…

# Relation between DL-based Cryptosystems & Generalized Jacobians



# The Current Snapshot

All generalized Jacobians that are currently used in DL-based cryptography precisely fall under two categories:

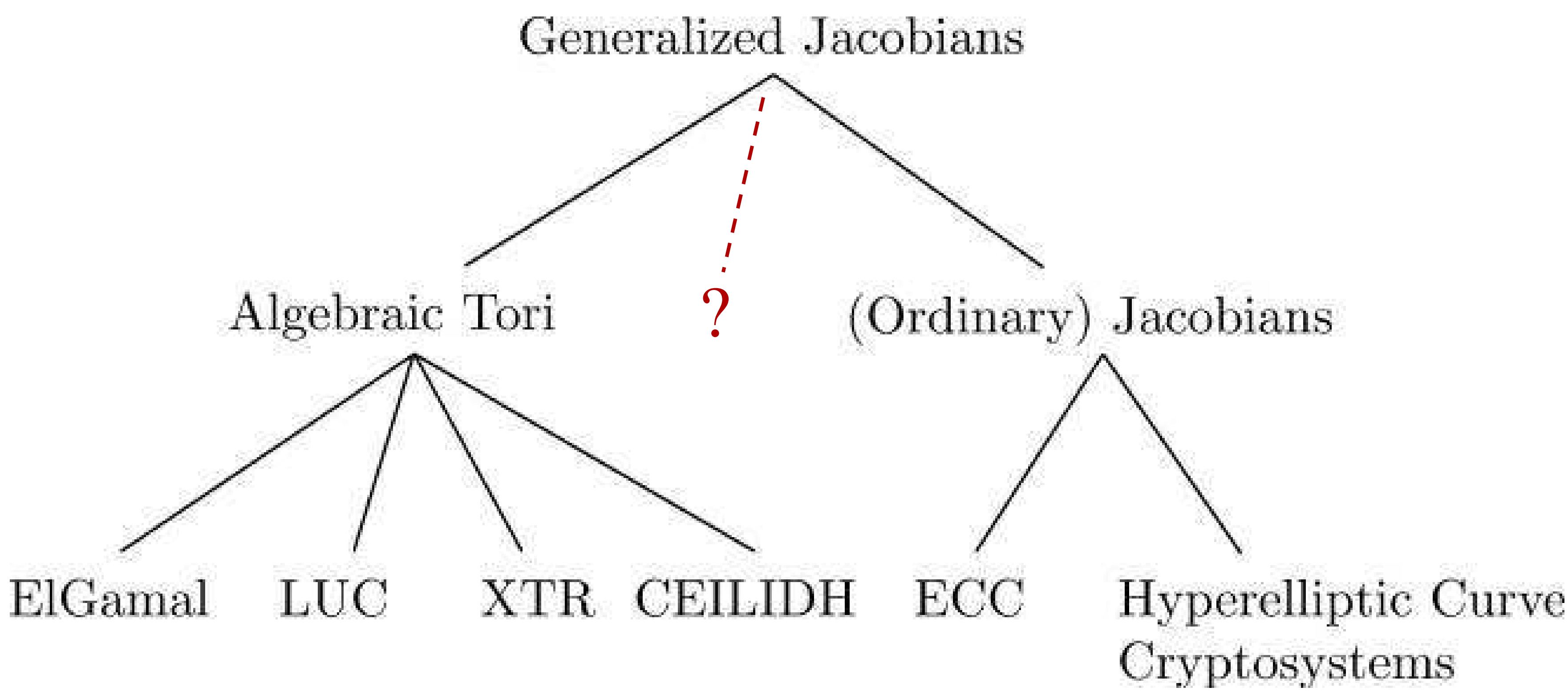
- (Usual) Jacobians
- Algebraic Tori

# The Natural Question

*Is it possible to use a generalized Jacobian*
*that is neither a usual Jacobian*
*nor an algebraic torus*
*for DL-based cryptography?*

An affirmative answer would then widen the class of algebraic groups that are of interest in public-key cryptography.

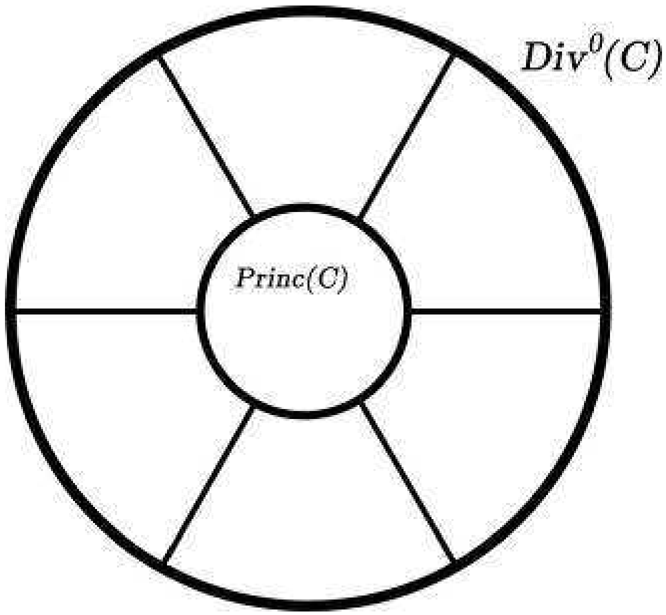
# The Natural Question



# Constructing a Generalized Jacobian

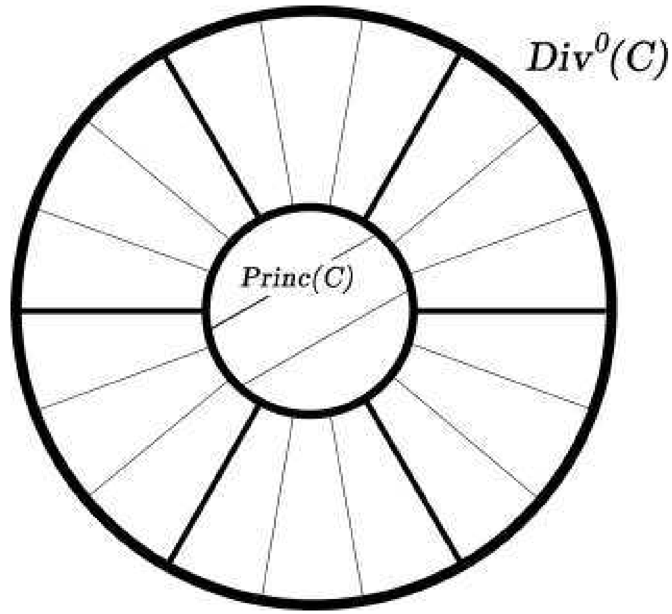
1. Start with your favorite algebraic curve.
2. Consider its divisors of degree zero.
3. (Cleverly) define an equivalence relation on them.
4. Find a canonical representative for each class.

# Usual vs Generalized Jacobians




Usual Jacobians

Linear equivalence




Generalized Jacobians

$\mathfrak{m}$–equivalence

# Why are Jacobians Useful?

Say the points of your favorite curve $C$ do *not* form a group…

*Then how can we create a group out of a set of elements?*

Consider the free abelian group on the set of points of $C$!

$$
\begin{array}{r}
3(P_1) - 5(P_2) + 0(P_3) - 9(P_4) + \ldots \\
+\ 0(P_1) - 3(P_2) - 1(P_3) + 3(P_4) + \ldots \\
\hline
3(P_1) - 8(P_2) - 1(P_3) - 6(P_4) + \ldots
\end{array}
$$

# Divisors

Let $C$ be a smooth curve defined over an (algebraically closed) field $K$.

A *divisor* on $C$ is a formal sum of the form

$$D = \sum_{P \in C} n_P (P)$$

where each $n_P$ is an integer and finitely many of them are nonzero.

The addition of two such divisors is thus given by

$$\sum_{P \in C} n_P (P) + \sum_{P \in C} m_P (P) = \sum_{P \in C} (n_P + m_P)(P)$$

# Divisors

The group formed by these divisors is denoted $\mathrm{Div}(C)$, and its identity element is

$$\mathbf{0} = \sum_{P \in C} 0(P)$$

The *degree* of the divisor $D$ is the integer

$$\deg(D) = \sum_{P \in C} n_P$$

The divisors of degree zero form a subgroup denoted by $\mathrm{Div}^0(C)$.

# Principal Divisors

The *divisor of a function* $f \in K(C)^*$ is

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)(P)$$

where $\operatorname{ord}_P(f)$ is the *order of vanishing* at $P$:

- If $\operatorname{ord}_P(f) < 0$, then $f$ has a *pole* of order $-\operatorname{ord}_P(f)$ at $P$,
- If $\operatorname{ord}_P(f) = 0$, then $f$ is defined and nonzero at $P$,
- If $\operatorname{ord}_P(f) > 0$, then $f$ has a *zero* of order $\operatorname{ord}_P(f)$ at $P$.

These special divisors are called *principal divisors*.

# Linear Equivalence

Now let $D_1, D_2 \in \mathrm{Div}(C)$ be given.

If $D_1 - D_2$ is a principal divisor, then we say that $D_1$ and $D_2$ are *linearly equivalent*, and we write

$$D_1 \sim D_2.$$

Equivalence classes of divisors of degree zero form a group denoted $\mathrm{Pic}^0(C)$.

Lastly, the Jacobian of $C$ is an abelian variety isomorphic (as a group) to $\mathrm{Pic}^0(C)$.

# Main Property of $\mathfrak{m}$-equivalent Divisors

Let $C$ be a smooth curve defined over an (algebraically closed) field $K$.

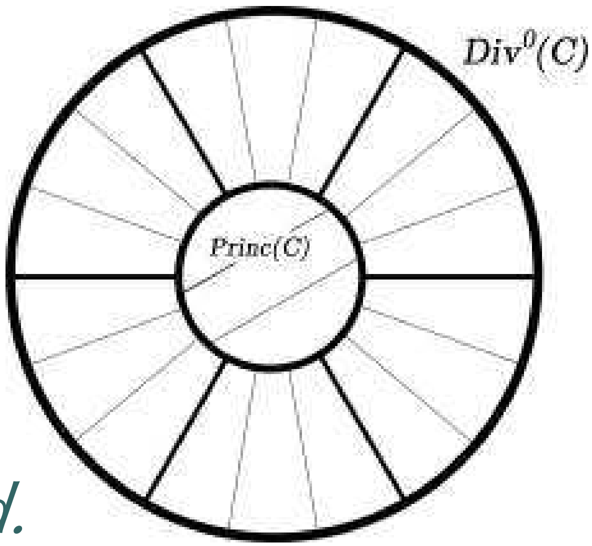
*If two divisors are $\mathfrak{m}$–equivalent, then they are linearly equivalent as well.*

Thus,

$$D_1 \sim_{\mathfrak{m}} D_2$$

if and only if

$\exists f \in K(C)^*$ such that $D_1 - D_2 = \mathrm{div}(f)$,
*plus an extra condition to be determined.*



# Modulus $\mathfrak{m}$

We can impose an extra condition by looking at the *behavior* of $f$ at some specific points of $C$, say $P_0, P_1, \ldots, P_r$.

Thus fix a positive divisor

$$\mathfrak{m} = m_0(P_0) + m_1(P_1) + \ldots + m_r(P_r),$$

thereafter called a *modulus*, and denote its support by $S_{\mathfrak{m}}$.

# Congruence Modulo $\mathfrak{m}$

If a function $f \in K(C)^*$ is such that

$$\operatorname{ord}_{P_i}(1-f) \geq m_i \text{ for each } P_i \in S_{\mathfrak{m}},$$

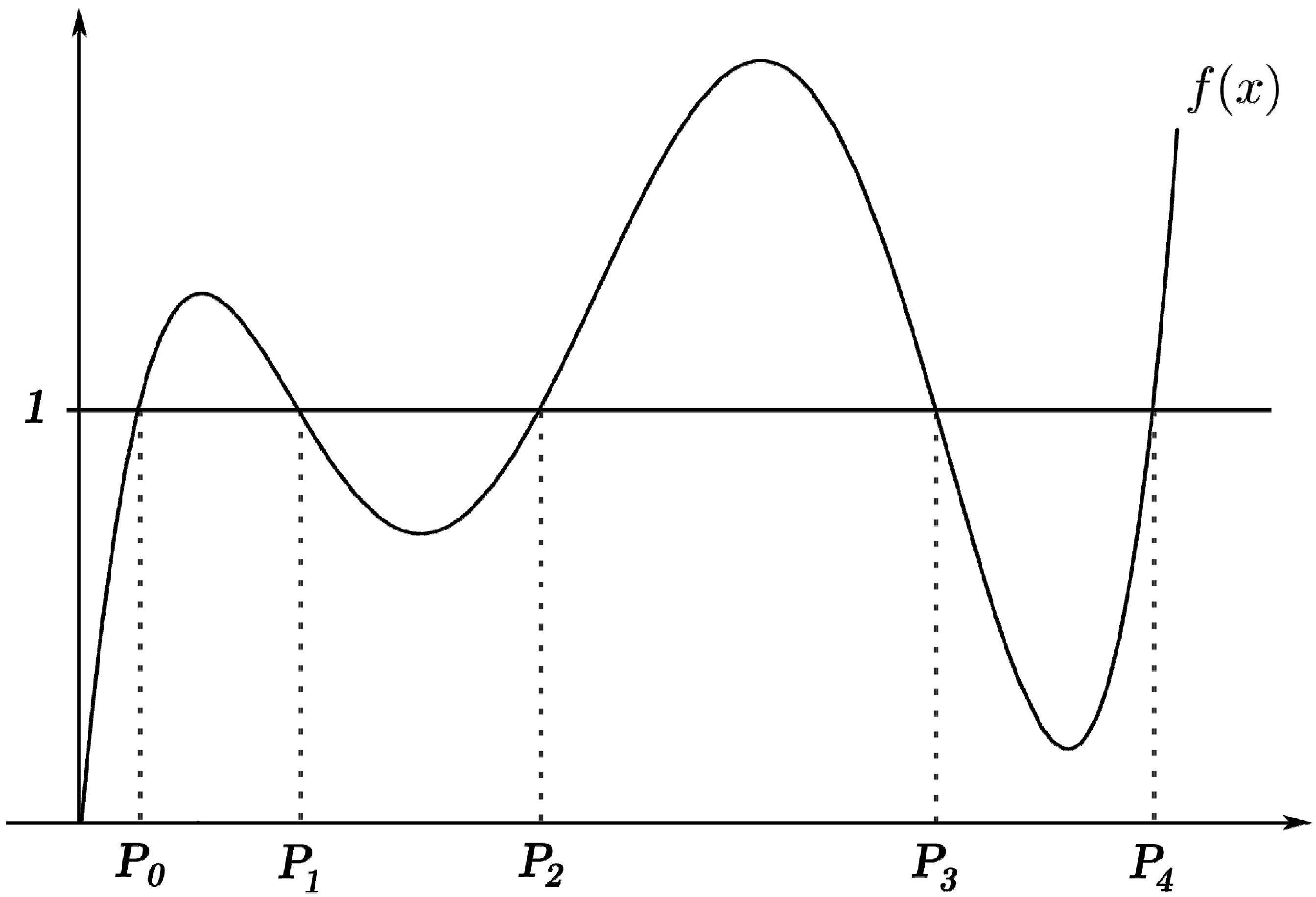
then we say that

*$f$ is congruent to 1 modulo $\mathfrak{m}$*

and we write

$$f \equiv 1 \bmod \mathfrak{m}.$$

# Visual Interpretation



# Defining $\mathfrak{m}$-equivalence and $\mathrm{Pic}^0_{\mathfrak{m}}(C)$

Let $\mathfrak{m}$ be an effective divisor with support $S_{\mathfrak{m}}$ and let $D_1$ and $D_2$ be two divisors prime to $S_{\mathfrak{m}}$. We say that $D_1$ and $D_2$ are $\mathfrak{m}$–*equivalent,* and write $D_1 \sim_{\mathfrak{m}} D_2$ if

$$\exists f \in K(C)^* \text{ such that}$$

$$\mathrm{div}(f) = D_1 - D_2 \text{ and } f \equiv 1 \bmod \mathfrak{m}.$$

The $\mathfrak{m}$-equivalence classes of divisors of degree zero that are prime to $S_{\mathfrak{m}}$ form a group denoted $\mathrm{Pic}^0_{\mathfrak{m}}(C)$.

# Existence of Generalized Jacobians

## Theorem (Rosenlicht)

Let $C$ be a smooth algebraic curve defined over an algebraically closed field $K$.

Then for every modulus $\mathfrak{m}$, there exists a commutative algebraic group $J_{\mathfrak{m}}$ isomorphic to $\mathrm{Pic}^0{}_{\mathfrak{m}}(C)$.

## Definition

The algebraic group $J_{\mathfrak{m}}$ is called the *generalized Jacobian* of $C$ with respect to the modulus $\mathfrak{m}$.

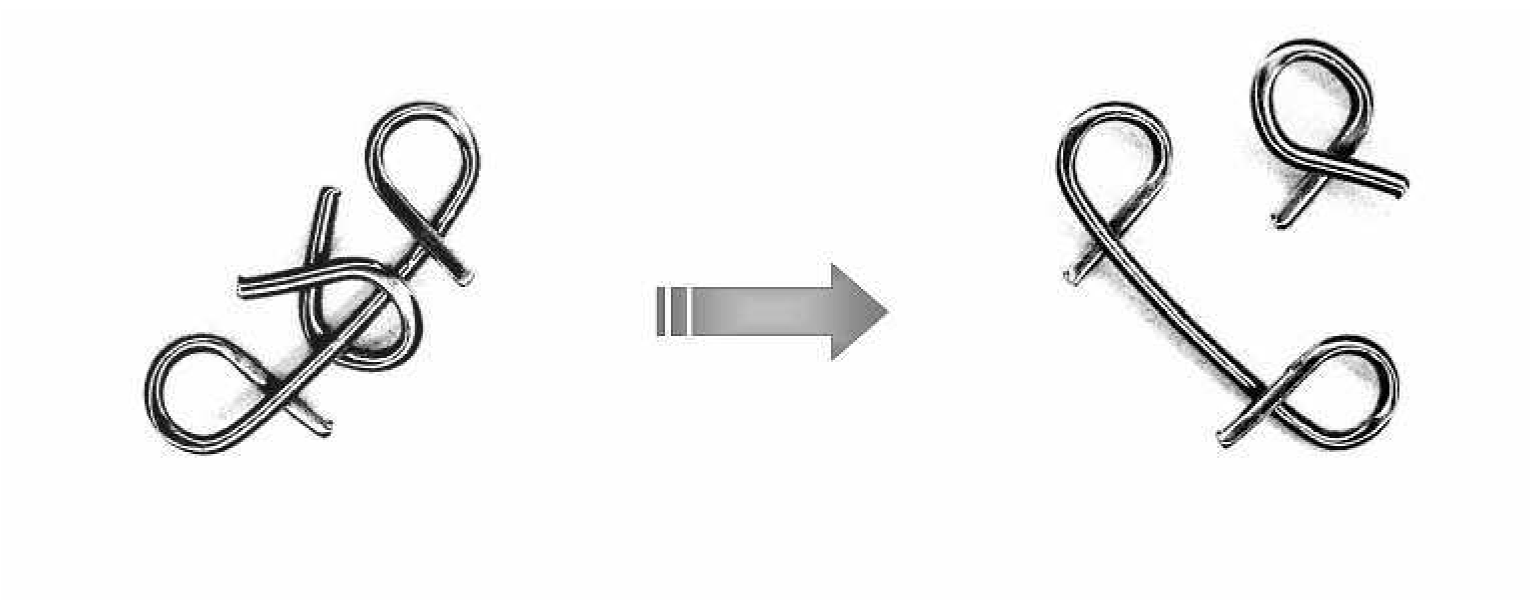
# How to Choose a Good Candidate?

The canonical choice is then to consider the generalized Jacobian of an elliptic curve $E$ with respect to a modulus formed by only two distinct points of $E$.

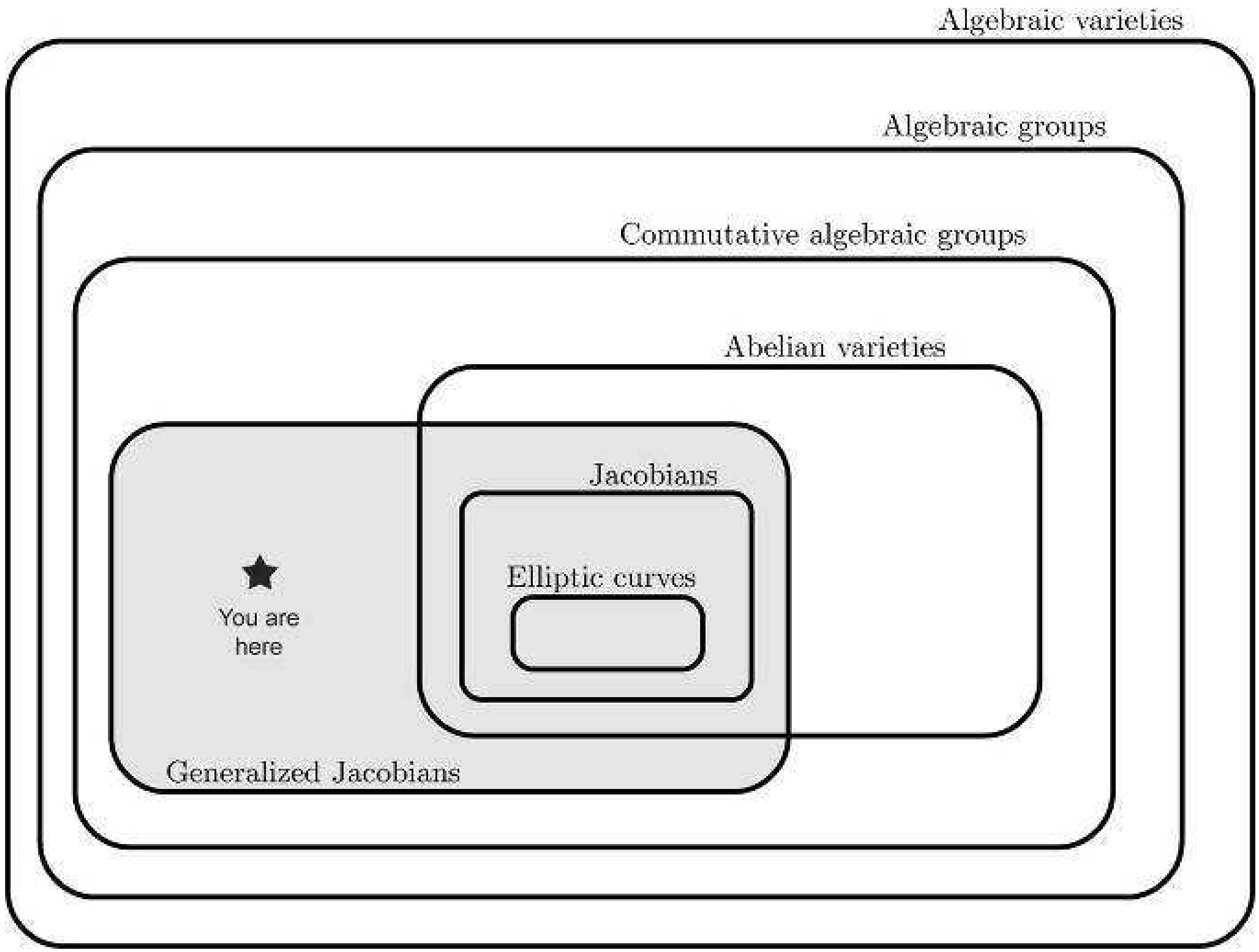
We have in this case that the corresponding generalized Jacobian is an extension of $E$ by the multiplicative group $\mathbb{G}_{\mathrm{m}}$.

# Just Like a Ringwire Puzzle...

That is, we can naively picture this object as an elliptic curve intertwined, in a natural and nontrivial fashion, with a finite field.



# Generalized Jacobians in Perspective



# Setup

Let $\mathbb{F}_q$ be the finite field with $q$ elements and let $K$ be a fixed algebraic closure of $\mathbb{F}_q$.

Let $E$ be a smooth elliptic curve defined over $\mathbb{F}_q$ and $B \in E(\mathbb{F}_q)$ be a given basepoint of prime order $l$.

Let also

$$\mathfrak{m} = (M) + (N),$$

where $M$ and $N$ are distinct points of $E(\mathbb{F}_{q^r})$ such that $M, N \notin \langle B \rangle$.

# Basic Requirements

Necessary conditions for a group $G$ to be suitable for cryptographic applications:

- ✓ The elements of $G$ can be easily represented in a compact form,
- ✓ The group operation can be performed efficiently,
- ✓ The DLP in $G$ is believed to be intractable, and
- ✓ The group order can be efficiently computed.

# Compact Representation of the Elements

Since $J_\mathfrak{m}$ is here an *extension* of $E$ by $\mathbb{G}_\mathrm{m}$, we have the exact sequence

$$0 \to \mathbb{G}_\mathrm{m} \to J_\mathfrak{m} \to E \to 0$$

Hence, there is a bijection of *sets* between $J_\mathfrak{m}$ and $\mathbb{G}_\mathrm{m} \times E$.

The existence of this bijection suffices to compactly represent the elements.

However, an *explicit* bijection

$$\psi : \mathrm{Pic}^0{}_\mathfrak{m}(E) \ \to \ \mathbb{G}_\mathrm{m} \times E$$

would allow us to "transport" the known group law on $\mathrm{Pic}^0{}_\mathfrak{m}(E)$ to $\mathbb{G}_\mathrm{m} \times E$.

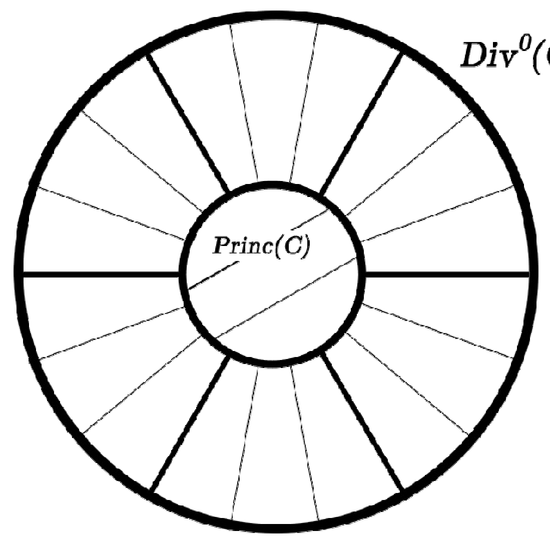
# How to label each $\mathfrak{m}$-equivalence class?

Given a degree zero divisor $D$ of disjoint support with $\mathfrak{m}$, we need to find $k \in \mathbb{G}_{\mathrm{m}}$ and $S \in E$ such that

$$[D]_{\mathfrak{m}} \text{ corresponds to } (k, S).$$

The easy part is the determination of $S$.

Indeed, it follows from the Abel-Jacobi Theorem.



# A Corollary of the Abel-Jacobi Theorem

Let $E$ be a smooth elliptic curve defined over a field $K$ and let

$$D_1 = \sum_{P \in E} n_P(P),\ D_2 = \sum_{P \in E} m_P(P) \in \mathrm{Div}(E)$$

be given. Then,

$$D_1 \sim D_2$$

if and only if

$$\deg(D_1) = \deg(D_2) \text{ and } \sum_{P \in E} n_P P = \sum_{P \in E} m_P P.$$

# Natural candidate for $S$

If $D = \sum_{P \in E} n_P(P)$, then we can set $S = \sum_{P \in E} n_P P$.

So $D \sim (S) - (\mathcal{O})$, which means that $\exists f \in K(E)^*$ such that

$$\mathrm{div}(f) = D - (S) + (\mathcal{O}).$$

It now remains to determine $k$.

As we will see, the value of $k$ will involve $f(M)$ and $f(N)$.

If $S \neq M, N$, then we are safe since $\mathrm{ord}_M(f) = \mathrm{ord}_N(f) = 0$.

If $S = M$ or $N$, then remark that we also have

$$D \sim (S+T) - (T) \text{ for any } T \in E.$$

So we simply choose $T$ such that $T \neq \mathcal{O}, M, N, M-N, N-M$.

# The Intuition Behind the Value of $k$

Say $S \neq M, N$ and let $D_1 = (S) - (\mathcal{O}) + \mathrm{div}(f_1)$ and $D_2 = (S) - (\mathcal{O}) + \mathrm{div}(f_2)$ be given. Then, $D_1 - D_2 = \mathrm{div}(f_1/f_2)$. Hence, $D_1 \sim_{\mathfrak{m}} D_2$

iff $\exists f \in K(C)^*$ such that $\mathrm{div}(f_1/f_2) = \mathrm{div}(f)$ and $f \equiv 1 \bmod \mathfrak{m}$.

iff $\exists c \in K^*$ such that $f_1/f_2 = cf$, $\mathrm{ord}_M(1-f) \geq 1$, $\mathrm{ord}_N(1-f) \geq 1$.

iff $\exists c \in K^*$ such that $f_1/f_2 = cf$ and $f(M) = f(N) = 1$.

iff $\exists c \in K^*$ such that $\dfrac{f_1(M)}{f_2(M)} = \dfrac{f_1(N)}{f_2(N)} = c$.

iff $\dfrac{f_1(M)}{f_1(N)} = \dfrac{f_2(M)}{f_2(N)}$.

We therefore suspect that $k_1 = \dfrac{f_1(M)}{f_1(N)}$ and $k_2 = \dfrac{f_2(M)}{f_2(N)}$.

# Explicit Bijection between $\mathrm{Pic}^0_{\mathfrak{m}}(E)$ and $\mathbb{G}_m \times E$

Theorem

Let $T \in E$ be given such that $T \neq \mathcal{O}, M, N, M-N, N-M$.

Let also $\psi: \mathrm{Pic}^0_{\mathfrak{m}}(E) \to \mathbb{G}_m \times E$

$$[D]_{\mathfrak{m}} \mapsto (k, S)$$

be such that the $\mathfrak{m}$-equivalence class of $D = \sum_{P\in E} n_P(P)$ corresponds to $S = \sum_{P\in E} n_P P$ and $k = f(M)/f(N)$, where $f \in K(E)^*$ is any function satisfying

$$\mathrm{div}(f) = \begin{cases} D-(S)+(\mathcal{O}) & \text{if } S \neq M, N \\ D-(S+T)+(T) & \text{otherwise.} \end{cases}$$

Then, $\psi$ is a well-defined bijection of sets.

# Inferring the Group Law

This explicit bijection of sets thus induces a group law on $\mathbb{G}_m \times E$ :

$$\begin{array}{rcc} \mathrm{Pic}^0{}_{\mathfrak{m}}(E) & \rightarrow & \mathbb{G}_m \times E \\ [D_1]_{\mathfrak{m}} & \mapsto & (k_1, P_1) \\ [D_2]_{\mathfrak{m}} & \mapsto & (k_2, P_2) \\ [D_1]_{\mathfrak{m}} + [D_2]_{\mathfrak{m}} & \mapsto & ? \end{array}$$

# Group Law for *B*-unrelated Moduli

## Theorem

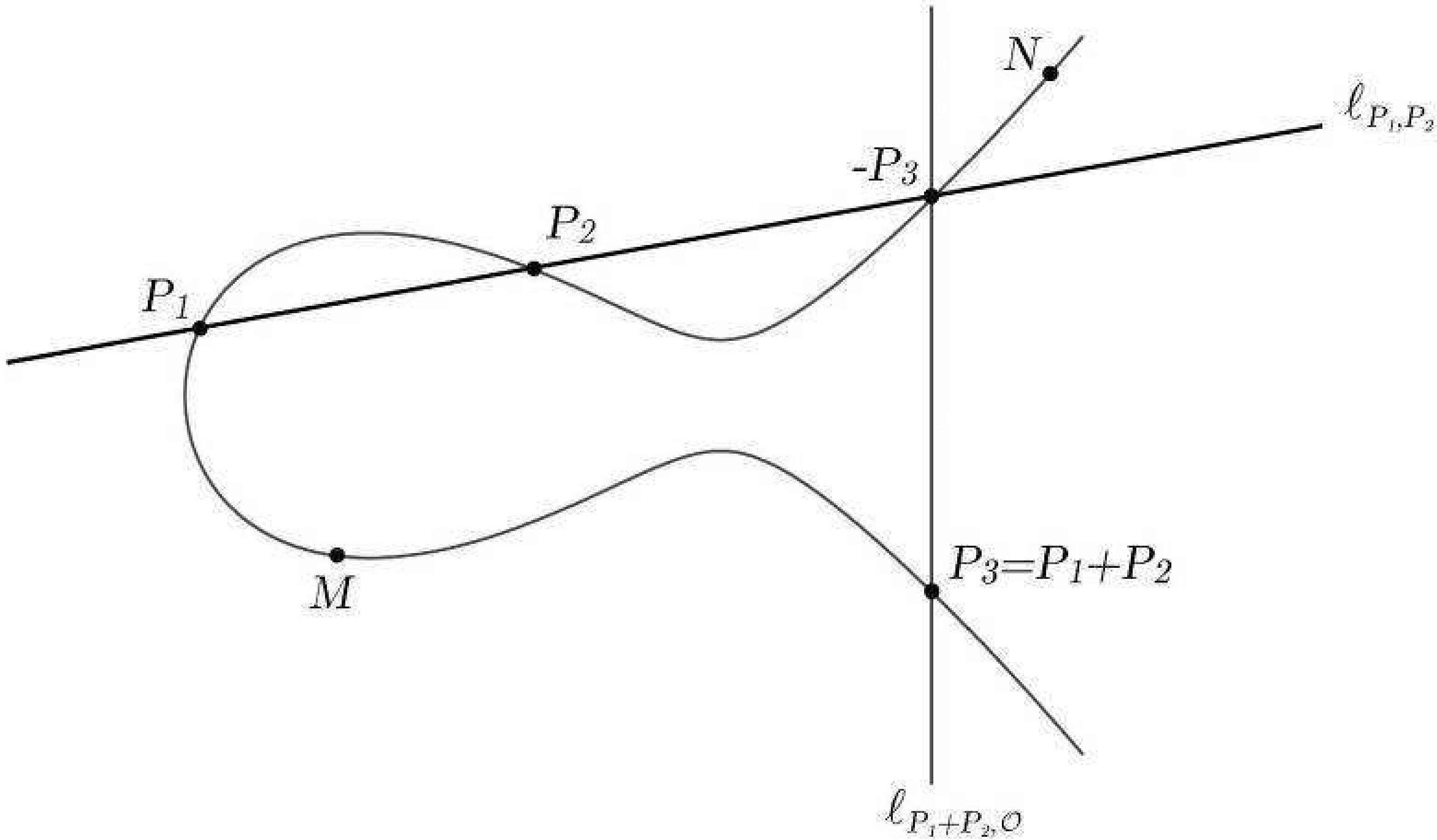
Let $(k_1, P_1)$ and $(k_2, P_2)$ be elements of $J_{\mathfrak{m}}$ such that $P_1, P_2, \pm(P_1+P_2) \notin \{M,N\}$. Then,

$$(k_1, P_1) + (k_2, P_2) = (k_1 \cdot k_2 \cdot \mathbf{c}_{\mathfrak{m}}(P_1, P_2)\ ,\ P_1 + P_2),$$

where $\mathbf{c}_{\mathfrak{m}} : E \times E \to \mathbb{G}_{\mathfrak{m}}$ is the 2-cocycle given by

$$\mathbf{c}_{\mathfrak{m}}(P_1, P_2) = \frac{\ell_{P_1,P_2}(M) \cdot \ell_{P_1+P_2,\mathcal{O}}(N)}{\ell_{P_1+P_2,\mathcal{O}}(M) \cdot \ell_{P_1,P_2}(N)}$$

# Group Law



# Corollaries

- $(1, \mathcal{O})$ is the identity element of $J_{\mathfrak{m}}$
- $\mathbf{c}_{\mathfrak{m}}(P_1, P_2) = \mathbf{c}_{\mathfrak{m}}(P_2, P_1)$
- $-(k, P) = \left( \frac{1}{k} \cdot \frac{\ell_{P,\mathcal{O}}(N)}{\ell_{P,\mathcal{O}}(M)}, -P \right)$
- $\mathbb{F}_{q^r}^{*} \times \langle B \rangle$ is a subgroup of $J_{\mathfrak{m}}$
- $(k_1, \mathcal{O}) + (k_2, P) = (k_1 \cdot k_2, P)$

# Relating three different DLPs

## Lemma

For $k \in \mathbb{F}^*_{q^r}$, $P \in \langle B \rangle$ and a positive integer $n$,
let $n_0 = n \bmod l$ , $n_1 = \lfloor n/l \rfloor$, $l(k, P) = (\lambda\ , \mathcal{O})$ and

$n_0(k, P) = (\nu_{n_0}\ , n_0 P)$.

Then,

$$n\ (k, P) = (\nu_{n_0} \cdot \lambda^{n_1}, n_0 P).$$

# The Natural Solution to this DLP

| $\mathbb{F}_{q^r}^*$ | $E$ |
| --- | --- |
| | $n_0 P$ |
| | $\downarrow$ |
| | $n_0$ |
| | $\downarrow$ |
| $\nu_{n_0} \cdot \lambda^{n_1}$ | $\nu_{n_0}$ |
| $\downarrow$ | |
| $\lambda^{n_1}$ | |
| $\downarrow$ | |
| $n_1$ | |

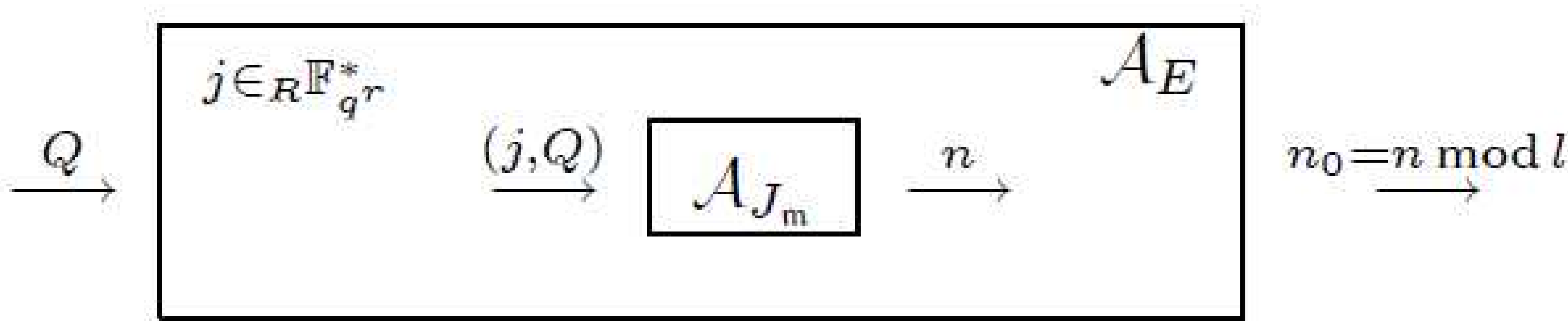
# Reductions among DLPs

## Proposition

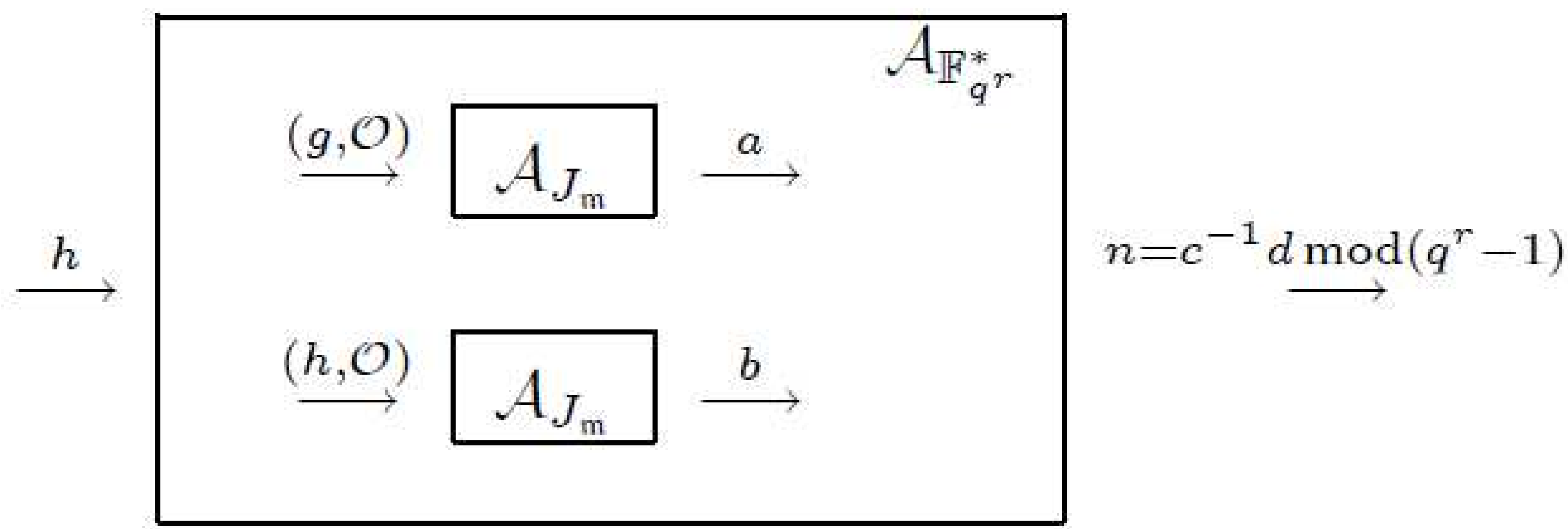
Let $E$ be a smooth elliptic curve over $\mathbb{F}_q$, $B \in E(\mathbb{F}_q)$ be a point of prime order $l$, $\mathfrak{m}=(M)+(N)$ be a $B$-unrelated modulus, where $M$ and $N$ are distinct points of $E(\mathbb{F}_{q^r})$ such that $\mathbb{F}^*_{q^r} \times \langle B \rangle$ is a cyclic subgroup of $J_{\mathfrak{m}}$.

Then, the DLP in this subgroup is at least as hard as the DLP in $\langle B \rangle \subseteq E(\mathbb{F}_q)$ and at least as hard as the DLP in $\mathbb{F}^*_{q^r}$.

# Converting an Instance of the DLP in $\langle B \rangle$ into one in $\mathbb{F}_{q^r}^{*} \times \langle B \rangle$



# Converting an Instance of the DLP in $\mathbb{F}_{q^r}^*$ into Two Instances in $\mathbb{F}_{q^r}^* \times \langle B \rangle$



# Reductions among DLPs

So from a practical point of view, these results imply that even though this generalized Jacobian is a newcomer in cryptography, we already know that solving this DLP *cannot be easier* than extracting discrete logarithms in two of the most studied groups used in DL-based cryptography today…

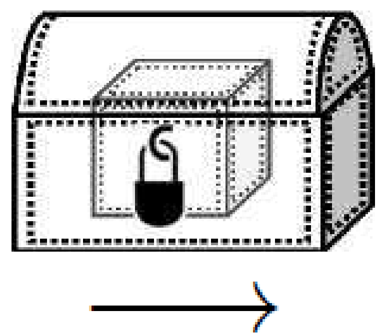
# A Cryptosystem with Two Safes...

## Alice

Put message $m$ in safe $S_1$ and lock it

Put $S_1$ within the safe $S_0$

Lock $S_0$ and send it to Bob



## Bob

Open safe $S_0$ to recover the closed safe $S_1$

Unlock $S_1$ and retrieve $m$

*Is it possible to crack the two locks simultaneously?*

That is, to extract the discrete logarithms in the elliptic curve and in the finite field in *parallel* ?

# A Solution à la Pohlig-Hellman

Since the order of our group is $(q^r - 1)l$, then we can try to retrieve

$$n_0 = n \bmod l \text{ and } n_2 = n \bmod (q^r - 1)$$

in parallel, and then combine them using the Chinese remainder theorem.

This method thus requires that $l$ does *not* divide $q^r - 1$.

# Computing $n_2$

Let $(j,Q) = n(k, P)$ be the instance of the DLP to be solved.

First compute $l(j,Q)$, which will equal, say, $(j', \mathcal{O})$.

We now have:

$$(j', \mathcal{O}) = l(j,Q) = l \cdot n(k,P) = n \cdot l(k,P) = n(\lambda, \mathcal{O}) = (\lambda^{n_2}, \mathcal{O}).$$

Since $j'$ and $\lambda$ are known, it thus suffices to solve the following DLP in the finite field:

$$j' = \lambda^{n_2}.$$

# Pairing-based Cryptography

Now, the case where $l$ divides $q^r - 1$ corresponds to the curves used in pairing-based crypto, where $r$ is the embedding degree.

In that case, if we try to mimic Pohlig-Hellman and explicitly write down each intermediate step, the sequence of operations *still* contains the sequential computation of a DL in the elliptic curve followed by one in the finite field.

It is still an open problem to decide if the natural sequential solution is optimal in this case.

# The Bottlenecks...

$$\#\left(\mathbb{F}_{q^r}^{*} \times \langle B \rangle\right) = d \cdot l^{\alpha}, \text{ where } \alpha \geq 2 \text{ and } l \nmid d.$$

$$\begin{cases} n_d = n \bmod d \\ n_\alpha = n \bmod l^\alpha \end{cases}$$

DLP in $\mathbb{F}_{q^r}^{*}$

$$n_\alpha = n_0 + n_1 l + n_2 l^2 + \ldots + n_{\alpha-1} l^{\alpha-1}$$

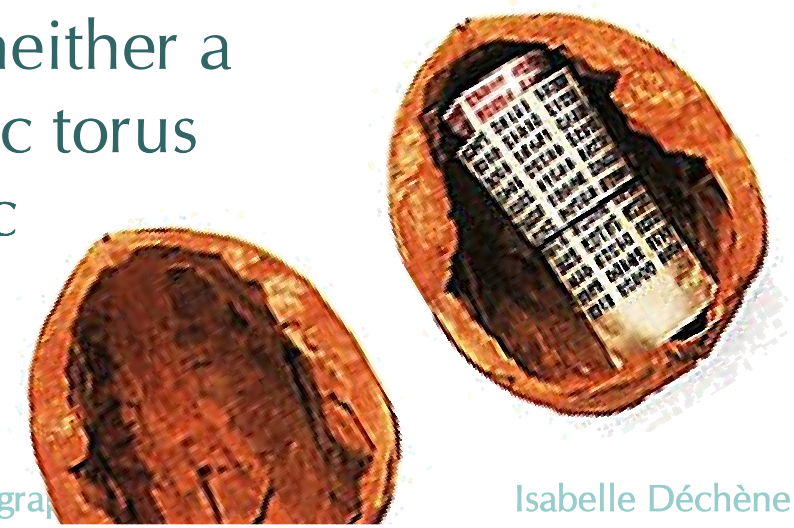
DLP in $E$

DLP in $\mathbb{F}_{q^r}^{*}$

# In a Nutshell…

We have seen in this talk how the generalized Jacobian of an elliptic curve with respect to a modulus $\mathfrak{m} = (M) + (N)$ fulfills the main conditions for a group to be suitable for DL-based cryptography.

This provides the first example of a generalized Jacobian which is neither a (usual) Jacobian nor an algebraic torus that is suitable for cryptographic applications.

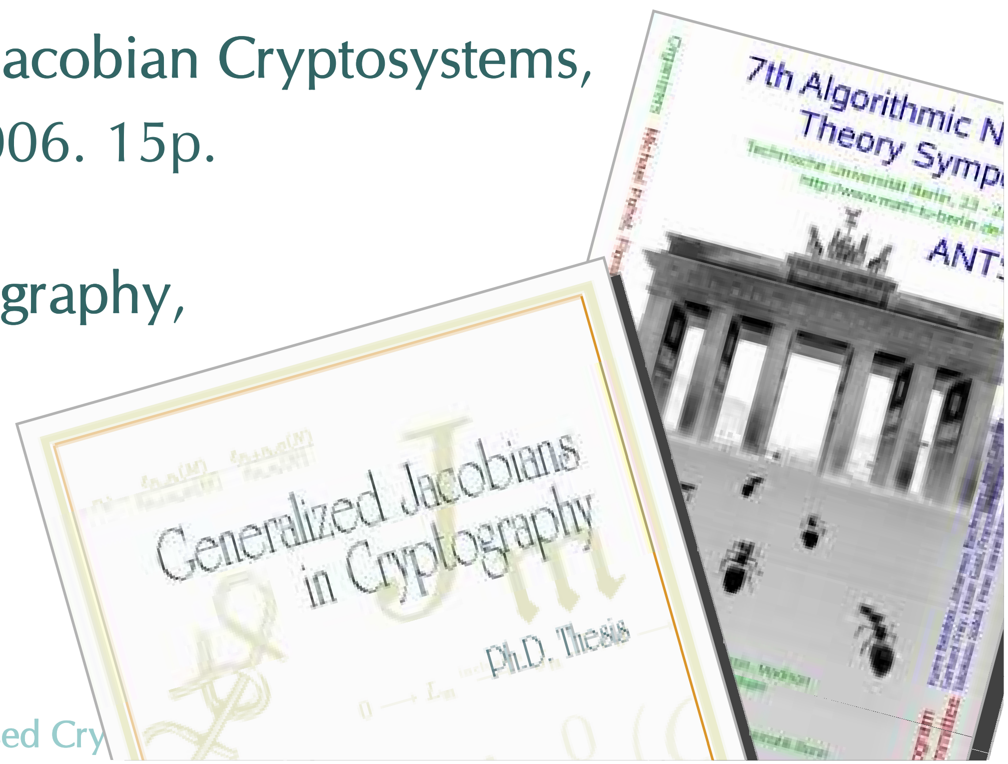


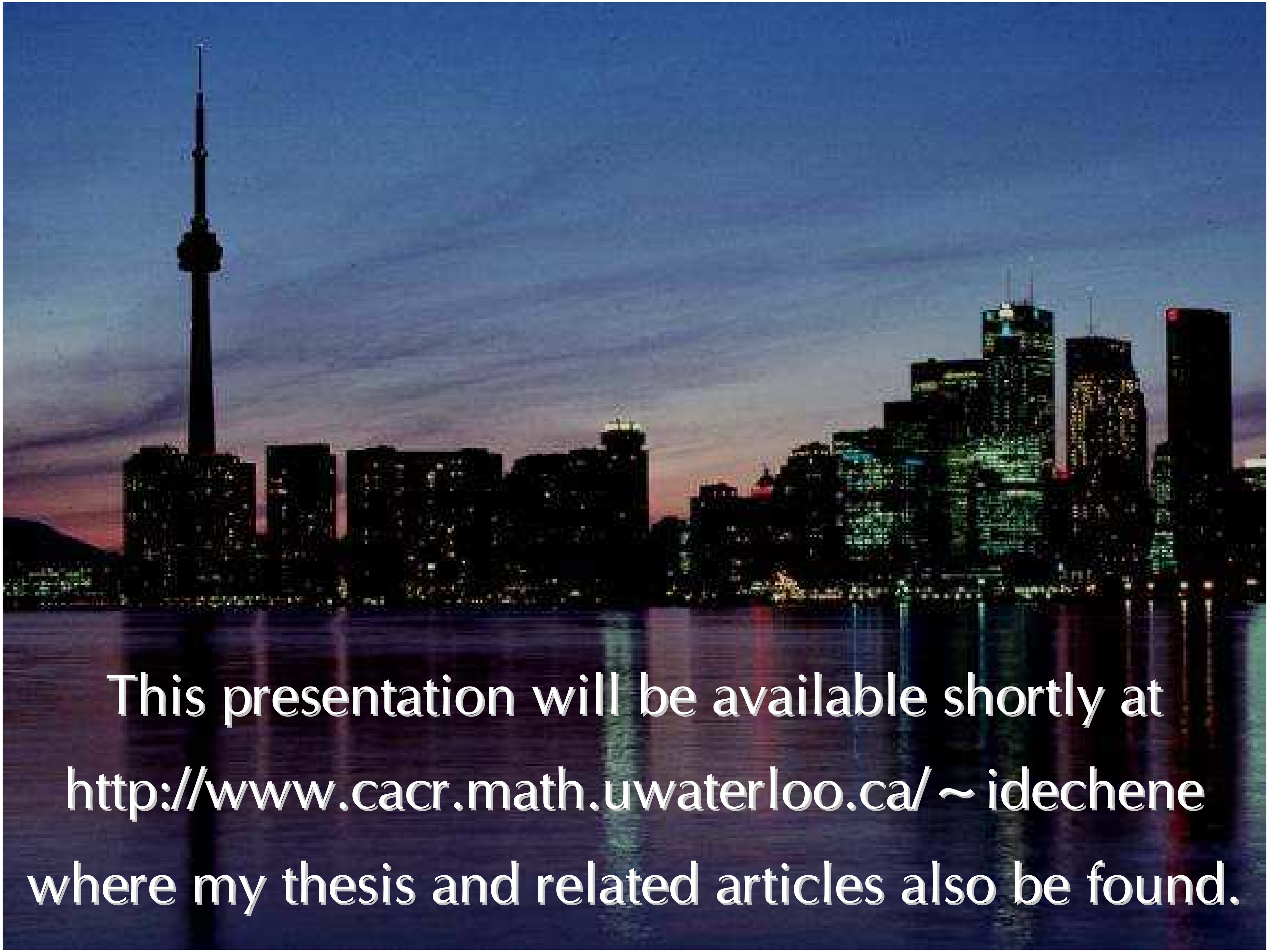
# References for this Talk

- **Arithmetic of Generalized Jacobians**, In Algorithmic Number Theory Symposium - ANTS VII, LNCS Volume 4076, Springer, 2006, pp. 421-435.

- **On the Security of Generalized Jacobian Cryptosystems**, CACR Technical Report, June 2006. 15p.

- **Generalized Jacobians in Cryptography**, Ph.D. Thesis, McGill University, Montreal, Canada, 2005, 203 p.




This presentation will be available shortly at
http://www.cacr.math.uwaterloo.ca/~idechene
where my thesis and related articles also be found.