Bivariate Polynomials Modulo Composites and Their Applications

Dan Boneh and Henry Corrigan-Gibbs
Stanford University

ASIACRYPT — 8 December 2014

Crypto's Bread and Butter

Let $N = pq$ be an RSA modulus of unknown factorization.

Crypto's Bread and Butter

Let $N = pq$ be an RSA modulus of unknown factorization.

i.e., p and q are large
distinct random primes

Crypto's Bread and Butter

Let $N = pq$ be an RSA modulus of unknown factorization.

Crypto's Bread and Butter

Let $N = pq$ be an RSA modulus of unknown factorization.

Question

Given a fixed polynomial $f \in \mathbb{Z}[x]$ and $c \leftarrow_R \mathbb{Z}_N$

How hard is it to solve:

$$f(x) = c \mod N \quad ?$$

Crypto's Bread and Butter

When $f(x) = x^2$, solving

$$x^2 = c \mod N$$

is as hard as factoring N [Rabin '79]

Crypto's Bread and Butter

When $f(x) = x^2$, solving

$$x^2 = c \mod N$$

is as hard as factoring N [Rabin '79]

When $f(x) = x^3$, solving

$$x^3 = c \mod N$$

is the RSA problem [Rivest-Shamir-Adleman '78]

Crypto's Bread and Butter

When $f(x) = x^2$, solving

$$x^2 = c \mod N$$

is as hard as factoring N [Rabin '79]

When $f(x) = x^3$, solving

$$x^3 = c \mod N$$

is the RSA problem [Rivest-Shamir-Adleman '78]

When $f \in \mathbb{Z}_N[x]$ is random (of fixed degree), solving:

$$f(x) = 0 \mod N$$

is as hard as factoring N [Schwenk-Eisfeld '96]

A Natural Extension: Bivariates

Question

Fix a *bivariate* polynomial $f \in \mathbb{Z}[x, y]$, choose $c \leftarrow_R \mathbb{Z}_N$

For which f is it hard to solve:

$$f(x, y) = c \mod N \quad ?$$

A Natural Extension: Bivariates

Question

Fix a *bivariate* polynomial $f \in \mathbb{Z}[x, y]$, choose $c \leftarrow_R \mathbb{Z}_N$

For which f is it hard to solve:

$$f(x, y) = c \mod N \quad ?$$

When does $f(x, y) \bmod N$ have interesting cryptographic properties?

A Natural Extension: Bivariates

Question

Fix a *bivariate* polynomial $f \in \mathbb{Z}[x, y]$, choose $c \leftarrow_R \mathbb{Z}_N$

For which f is it hard to solve:

$$f(x, y) = c \mod N \quad ?$$

When does $f(x, y) \bmod N$ have interesting cryptographic properties?

Subject of this talk

Immediate Application

From the **discrete log problem**. . .

$$M = g^m$$

Immediate Application

From the **discrete log problem**. . .

$$M = g^m$$

. . . we get a commitment scheme:

$$C(m; r) = g^m h^r$$

[Pedersen '91]

Immediate Application

From the **discrete log problem**…

$$M = g^m$$

…we get a commitment scheme:

$$C(m; r) = g^m h^r$$

[Pedersen '91]

From the **RSA problem**…

$$M = m^3 \mod N$$

Immediate Application

From the **discrete log problem**…

$$M = g^m$$

…we get a commitment scheme:

$$C(m; r) = g^m h^r$$

[Pedersen '91]

From the **RSA problem**…

$$M = m^3 \mod N$$

…do we get a commitment scheme?

$$C(m; r) = m^3 + 2r^3 \bmod N$$

Immediate Application

From the **discrete log problem**…

$$M = g^m$$

…we get a commitment scheme:

$$C(m;r) = g^m h^r$$

[Pedersen '91]

From the **RSA problem**…

$$M = m^3 \mod N$$

…do we get a

Or maybe m^4? m^5?

$$C(m;r) = m^3 + 2r^3 \bmod N$$

Immediate Application

From the **discrete log problem**. . .

$$M = g^m$$

. . . we get a commitment scheme:

$$C(m; r) = g^m h^r$$

[Pedersen '91]

From the **RSA problem**. . .

$$M = m^3 \mod N$$

. . . do we get a commitment scheme?

$$C(m; r) = m^3 + 2r^3 \bmod N$$

Immediate Application

From the **discrete log problem**…

$$M = g^m$$

…we get a commitment scheme:

$$C(m; r) = g^m h^r$$

[Pedersen '91]

From the **RSA problem**…

$$M = m^3 \mod N$$

…do we get a commitment scheme?

$$\cancel{C(m; r) = m^3 + 2r^3 \bmod N}$$

Overview

Motivation

Classifying Polynomials
- One way functions
- Second preimage resistance
- Collision Resistance

Applications

Conclusion

Classifying Polynomials

Useful cryptographic properties of $f(x, y) \bmod N$:

- one-wayness
- second preimage resistance
- collision resistance

Classifying Polynomials

Useful cryptographic properties of $f(x, y) \bmod N$:

- one-wayness
- second preimage resistance
- collision resistance

Question

Which polynomials $f \in \mathbb{Z}[x, y]$ define functions $\bmod N$ with these properties?

To understand properties of

$$c \leftarrow f(x, y) \bmod N,$$

look at the properties of

$$f(x, y) = c \quad \in \mathbb{Q}.$$

Our Approach

Fact

If it's easy to find *rational* solutions to

$$f(x, y) = c \qquad \in \mathbb{Q}$$

then, for random RSA moduli N, it's easy find solutions to

$$f(x, y) = c \mod N.$$

Our Approach

Fact

If it's easy to find *rational* so

Find solution
and reduce it $\bmod N$.

$$f(x, y) = c \qquad \in \mathbb{Q}$$

then, for random RSA moduli N, it's easy find solutions to

$$f(x, y) = c \mod N.$$

Our Approach

Fact

If it's easy to find *rational* solutions to

$$f(x, y) = c \qquad \in \mathbb{Q}$$

then, for random RSA moduli N, it's easy find solutions to

$$f(x, y) = c \mod N.$$

Our Approach

Fact

If it's easy to find *rational* solutions to

$$f(x, y) = c \qquad \in \mathbb{Q}$$

then, for random RSA moduli N, it's easy find solutions to

$$f(x, y) = c \mod N.$$

Question

Is this the *only* way to find solutions $\bmod N$?

Our Approach

Fact

If it's easy to find *rational* solutions to

$$f(x, y) = c \qquad \in \mathbb{Q}$$

then, for random RSA moduli N, it's easy find solutions to

$$f(x, y$$

Can compute $+$,$-$,$*$,$/$.
Not $\sqrt{x}$.

Question

Is this the *only* way to find solutions $\bmod N$?

Our Approach

Fact

If it's easy to find *rational* solutions to

$$f(x,y) = c \qquad \in \mathbb{Q}$$

then, for random RSA moduli N, it's easy find solutions to

$$f(x,y) = c \mod N.$$

Question

Is this the *only* way to find solutions $\mathrm{mod}\ N$?

Our Approach

Fact

If it's easy to find *rational* solutions to

$$f(x, y) = c \qquad \in \mathbb{Q}$$

then, for random RSA moduli N, it's easy find solutions to

$$f(x, y) = c \mod N.$$

Question

Is this the *only* way to find solutions $\bmod N$?

More generally: Are rational properties of f *sufficient* to get cryptographic properties $\bmod N$?

One Wayness

Example

You want this to be a OWF. **Is it?**

$$f(x, y) = x^2 - 5y^2 + 3xy \mod N$$

One Wayness

Example

You want this to be a OWF. **Is it?**

$$f(x, y) = x^2 - 5y^2 + 3xy \mod N$$

No! The curve $f(x, y) = c$ is of genus zero over $\mathbb{Q}$, so can efficiently invert the OWF. [Pollard-Schnorr '87]

One Wayness

Example

You want this to be a OWF. **Is it?**

$$f(x, y) = x^2 - 5y^2 + 3xy \mod N$$

No! The curve $f(x, y) = c$ is of genus zero over $\mathbb{Q}$, so can efficiently invert the OWF. [Pollard-Schnorr '87]

OSS'84 sigs (broken) relied on the hardness of a related problem.

One Wayness

Classify polynomials $f \in \mathbb{Z}[x, y]$ according to the *genus* of $f(x, y) - c = 0$ for most $c \in \mathbb{Z}_N$

One Wayness

Classify polynomials $f \in \mathbb{Z}[x, y]$ according to the *genus* of $f(x, y) - c = 0$ for most $c \in \mathbb{Z}_N$

Genus	**Type**	**Easy to invert $\mathrm{mod}\ N$?**
0	"rational"	Yes
1	"elliptic"	**?**
≥ 2		**?**

One Wayness

Classify polynomials $f \in \mathbb{Z}[x, y]$ according to the *genus* of $f(x, y) - c = 0$ for most $c \in \mathbb{Z}_N$

Genus	**Type**	**Easy to invert** $\mathrm{mod}\ N$**?**
0	"rational"	Yes
1	"elliptic"	**?**
≥ 2		**?**

Necessary Condition: For f to give rise to OWF, curve $f(x, y) - c = 0$ must have genus > 0 for almost all c.

Second Preimage Resistance

Definition: Given a point $(x, y) \leftarrow_R \mathbb{Z}_N^2$, should be hard to find a *second* point (x', y') such that:

$$f(x, y) = f(x', y') \bmod N$$

Second Preimage Resistance

Definition: Given a point $(x, y) \leftarrow_R \mathbb{Z}_N^2$, should be hard to find a *second* point (x', y') such that:

$$f(x, y) = f(x', y') \bmod N$$

Breaking SPR is only as hard as finding a *second* rational point on the curve $f(x, y) = c$.

Second Preimage Resistance

Definition: Given a point $(x, y) \leftarrow_R \mathbb{Z}_N^2$, should be hard to find a *second* point (x', y') such that:

$$f(x, y) = f(x', y') \bmod N$$

Breaking SPR is only as hard as finding a *second* rational point on the curve $f(x, y) = c$.

Necessary Condition: For f to be SPR, curve $f(x, y) = c$ must have no non-trivial rational mapping $(x, y) \mapsto (x', y')$ for almost all c.

Second Preimage Resistance

Definition: Given a point $(x, y) \leftarrow_R \mathbb{Z}_N^2$, should be hard to find a *second* point (x', y') such that:

$$f(x, y) = f(x', y') \bmod N$$

Details are in the paper

Breaking SPR is o *second* rational point on the curve $f($

Necessary Condition: For f to be SPR, curve $f(x, y) = c$ must have no non-trivial rational mapping $(x, y) \mapsto (x', y')$ for almost all c.

Collision Resistance

Definition: f is *collision resistant* if it is computationally hard to find $(x, y) \neq (x', y') \in \mathbb{Z}_N^2$ such that

$$f(x, y) = f(x', y') \mod N.$$

Collision Resistance

Definition: f is *collision resistant* if it is computationally hard to find $(x, y) \neq (x', y') \in \mathbb{Z}_N^2$ such that

$$f(x, y) = f(x', y') \mod N.$$

Definition: A function $f : \mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{Q}$ is *injective* if

$$f(x, y) = f(x', y') \qquad \Longrightarrow \qquad (x, y) = (x', y').$$

Collision Resistance

Fact

$f(x, y)$ is **NOT** an injective map $\implies$ $f(x, y)$ is **NOT** CR $\bmod N$

Collision Resistance

Find “collision” in $\mathbb{Q}$ and reduce it $\bmod N$.

Fact

$f(x, y)$ is **NOT** an injective map	$\Longrightarrow$	$f(x, y)$ is **NOT** CR $\bmod N$

Collision Resistance

Fact

$f(x, y)$ is **NOT** an injective map $\implies$ $f(x, y)$ is **NOT** CR $\bmod N$

Collision Resistance

Fact

$f(x,y)$ is **NOT** an injective map $\implies$ $f(x,y)$ is **NOT** CR $\bmod N$

Open Question

$f(x,y)$ **IS** an injective map $\overset{?}{\implies}$ $f(x,y)$ **IS** CR $\bmod N$

Injective Polynomials

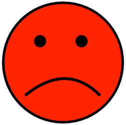
Question

Does there exist a low-degree poly $f(x, y)$ that induces an *injective* map $\mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{Q}$?

Injective Polynomials

Question

Does there exist a low-degree poly $f(x, y)$ that induces an *injective* map $\mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{Q}$?

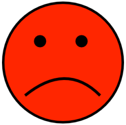


This is an open problem in number theory.

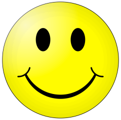
Injective Polynomials

Question

Does there exist a low-degree poly $f(x, y)$ that induces an *injective* map $\mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{Q}$?



This is an open problem in number theory.



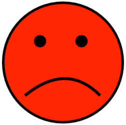
But a 15-year-old conjecture says that $f_{\text{Zag}}(x, y) = x^7 + 3y^7$ is injective over $\mathbb{Q} \times \mathbb{Q}$

[Zagier, as reported by Poonen 2009]

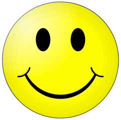
Injective Polynomials

Question

Does there exist a low-degree poly $f(x, y)$ that induces an *injective* map $\mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{Q}$?



This is an open problem in number theory.



But a 15-year-old conjecture says that $f_{\text{Zag}}(x, y) = x^7 + 3y^7$ is injective over $\mathbb{Q} \times \mathbb{Q}$

[Zagier, as reported by Poonen 2009]

$x^7 + 3y^7$ is the **actual** polynomial, not a toy example.

Injective Polynomials

Conjecture [Zagier]

The following is an injective function mapping $\mathbb{Q}^2 \mapsto \mathbb{Q}$:

$$f_{\mathsf{Zag}}(x, y) = x^7 + 3y^7$$

Injective Polynomials

Conjecture [Zagier]

The following is an injective function mapping $\mathbb{Q}^2 \mapsto \mathbb{Q}$:

$$f_{\mathsf{Zag}}(x, y) = x^7 + 3y^7$$

Remark

By Merkle-Damgård:

$$f_{\mathsf{Zag}}(x, y) \text{ injective} \implies g(x, y, z) = x^7 + 3(y^7 + 3z^7)^7 \text{ injective}$$

Injective Polynomials

Conjecture [Zagier]

The following is an injective function mapping $\mathbb{Q}^2 \mapsto \mathbb{Q}$:

$$f_{\mathsf{Zag}}(x, y) = x^7 + 3y^7$$

Remark

By Merkle-Damgård:

$$f_{\mathsf{Zag}}(x, y) \text{ injective} \implies g(x, y, z) = x^7 + 3(y^7 + 3z^7)^7 \text{ injective}$$

We get injective maps on $\mathbb{Q}^4, \mathbb{Q}^5, \ldots$ for free!

Collision Resistance

Since the only apparent way to find collisions in $f \bmod N$ is to find $\mathbb{Q}$ collisions…

Collision Resistance

Since the only apparent way to find collisions in $f \bmod N$ is to find $\mathbb{Q}$ collisions...

and since Zagier conjectures that f_{Zag} is injective (i.e., has no collisions) over $\mathbb{Q}^2$...

Collision Resistance

Since the only apparent way to find collisions in $f \bmod N$ is to find $\mathbb{Q}$ collisions…

and since Zagier conjectures that f_{Zag} is injective (i.e., has no collisions) over $\mathbb{Q}^2$…

Assumption

The function $f_{\mathsf{Zag}}(x, y) = x^7 + 3y^7 \bmod N$ is CR.

Collision Resistance

Since the only apparent way to find collisions in $f \bmod N$ is to find $\mathbb{Q}$ collisions...

and since Zagier conjectures that f_{Zag} is injective (i.e., has no collisions) over $\mathbb{Q}^2$...

Assumption

The function $f_{\mathsf{Zag}}(x, y) = x^7 + 3y^7 \bmod N$ is CR.

Now, what can we do
with this assumption?

Overview

Commitment Scheme

One of the most common tools in crypto protocols

Commitment Scheme

One of the most common tools in crypto protocols

$\mathsf{Commit}(m) \rightarrow (c, r)$. Generate a commitment c to m using randomness r.

$\mathsf{Open}(c, m, r) \rightarrow \{0, 1\}$. Test whether (m, r) is a valid opening of c.

Commitment Scheme

One of the most common tools in crypto protocols

Commit$(m) \to (c, r)$. Generate a commitment c to m using randomness r.

Open$(c, m, r) \to \{0, 1\}$. Test whether (m, r) is a valid opening of c.

Hiding. For any two messages m and m':

$$\mathsf{Commit}(m, r) \approx_s \mathsf{Commit}(m', r')$$

Binding. Cannot open a commitment two different ways.

Commitment Scheme

Public params: RSA modulus N s.t. $\gcd(\phi(N), 7) = 1$

$\mathsf{Commit}(m) \to (c, r)$

Pick $r \leftarrow_R \mathbb{Z}_N$.

Return $f_{\mathsf{Zag}}(m, r) = m^7 + 3r^7 \bmod N$.

$\mathsf{Open}(c, m, r) \to \{0, 1\}$

Check that $c \stackrel{?}{=} f_{\mathsf{Zag}}(m, r) \bmod N$.

Commitment Scheme

Public params: RSA modulus N s.t. gc

Efficient! Only a few mults.

$\mathsf{Commit}(m) \to (c, r)$

Pick $r \leftarrow_R \mathbb{Z}_N$.

Return $f_{\mathsf{Zag}}(m, r) = m^7 + 3r^7 \bmod N$.

$\mathsf{Open}(c, m, r) \to \{0, 1\}$

Check that $c \stackrel{?}{=} f_{\mathsf{Zag}}(m, r) \bmod N$.

Commitment Scheme

Public params: RSA modulus N s.t. $\gcd(\phi(N), 7) = 1$

Commit$(m) \to (c, r)$

Pick $r \leftarrow_R \mathbb{Z}_N$.

Return $f_{\mathsf{Zag}}(m, r) = m^7 + 3r^7 \bmod N$.

Open$(c, m, r) \to \{0, 1\}$

Check that $c \stackrel{?}{=} f_{\mathsf{Zag}}(m, r) \bmod N$.

Commitment Scheme

Public params: RSA modulus N s.t. $\gcd(\phi(N), 7) = 1$

Commit$(m) \rightarrow (c, r)$

Pick $r \leftarrow_R \mathbb{Z}_N$.

Return $f_{\mathsf{Zag}}(m, r) = m^7 + 3r^7 \bmod N$.

Open$(c, m, r) \rightarrow \{0, 1\}$

Check that $c \stackrel{?}{=} f_{\mathsf{Zag}}(m, r) \bmod N$.

Security

Commitment Scheme

Public params: RSA modulus N s.t. $\gcd(\phi(N), 7) = 1$

Commit$(m) \to (c, r)$

Pick $r \leftarrow_R \mathbb{Z}_N$.

Return $f_{\mathsf{Zag}}(m, r) = m^7 + 3r^7 \bmod N$.

Open$(c, m, r) \to \{0, 1\}$

Check that $c \stackrel{?}{=} f_{\mathsf{Zag}}(m, r) \bmod N$.

Security

- Hiding: Follows because m is blinded with random element $3r^7$

Commitment Scheme

Public params: RSA modulus N s.t. $\gcd(\phi(N), 7) = 1$

Commit$(m) \to (c, r)$
Pick $r \leftarrow_R \mathbb{Z}_N$.
Return $f_{\mathsf{Zag}}(m, r) = m^7 + 3r^7 \bmod N$.

Open$(c, m, r) \to \{0, 1\}$
Check that $c \stackrel{?}{=} f_{\mathsf{Zag}}(m, r) \bmod N$.

Security

- Hiding: Follows because m is blinded with random element $3r^7$
- Binding: Violating the binding property implies finding a collision in $f_{\mathsf{Zag}} \bmod N$

ZK Proofs on "Nested" Commitments

Given Pedersen commitments:

$$\mathsf{Commit}(m), \mathsf{Commit}(r), \mathsf{Commit}(c)$$

can prove in *succinct* ZK that $c = m^7 + 3r^7 \bmod N$.

ZK Proofs on "Nested" Commitments

Given Pedersen commitments:

$$\mathsf{Commit}(m), \mathsf{Commit}(r), \mathsf{Commit}(c)$$

can prove in *succinct* ZK that $c = m^7 + 3r^7 \bmod N$.

- $\rightarrow$ Prove that committed values (c, m, r) are themselves the opening of a commitment
- $\rightarrow$ Uses standard D.log ZKPoK techniques

ZK Proofs on “Nested” Commitments

Given Pedersen commitments:

$$\mathsf{Commit}(m), \mathsf{Commit}(r), \mathsf{Commit}(c)$$

can prove in *succinct* ZK that $c = m^7 + 3r^7 \bmod N$.

- $\rightarrow$ Prove that committed values (c, m, r) are themselves the opening of a commitment
- $\rightarrow$ Uses standard D.log ZKPoK techniques

WHY WOULD YOU EVER WANT TO DO THAT?!

ZK Proofs on “Nested” Commitments

Given Pedersen commitments:

$$\mathsf{Commit}(m), \mathsf{Commit}(r), \mathsf{Commit}(c)$$

can prove in *succinct* ZK that $c = m^7 + 3r^7 \bmod N$.

→ Prove that committed values (c, m, r) are themselves the opening of a commitment

→ Uses standard D.log ZKPoK techniques

WHY WOULD YOU EVER WANT TO DO THAT?!

Useful for:

- short anonymous Bitcoins, [Miers et al. 2013, Ben-Sasson et al, 2014]
- anonymous authentication, [Benaloh-De Mare ’93, Barić-Pfitz. ’97, C-L 2002]
- set membership proofs, [Camenisch-Chaabouni-Shelat 2008]
- etc.

Chameleon Hash

[Gennaro-Halevi-Rabin ’99, Krawczyk-Rabin 2000, Bellare-Ristov 2008]

Definition: a hash function $H(m, r)$ such that

- without “trapdoor,” it’s hard to find collisions in H
- given (h, m), can use the “trapdoor,” to find r s.t.

$$h = H(m, r)$$

- for any m, m' and for random r, r':

$$H(m, r) \approx_s H(m', r')$$

Chameleon Hash

[Gennaro-Halevi-Rabin '99, Krawczyk-Rabin 2000, Bellare-Ristov 2008]

Definition: a hash function $H(m, r)$ such that

- without "trapdoor," it's hard to find collisions in H
- given (h, m), can use the "trapdoor," to find r s.t.

$$h = H(m, r)$$

- for any m, m' and for random r, r':

$$H(m, r) \approx_s H(m', r')$$

Construction

- Hash function is $H(m, r) = m^7 + 3r^7 \bmod N$
- "Trapdoor" is the factorization of N

Other Applications

Others...

- "Accumulator" [Merkle '89]
- Signature scheme [Goldwasser-Micali-Rivest '88]

Other Applications

Others. . .

- "Accumulator" [Merkle '89]
- Signature scheme [Goldwasser-Micali-Rivest '88]
- **[Your application here]**

Overview

Recap

We reason about properties of $f(x, y) \bmod N$ by looking at the properties of $f(x, y) = c$ over the rationals.

Crypto Property	**Algebraic Property**

Recap

We reason about properties of $f(x, y) \bmod N$ by looking at the properties of $f(x, y) = c$ over the rationals.

Crypto Property	**Algebraic Property**
One-wayness	genus $g > 0$

Recap

We reason about properties of $f(x, y) \bmod N$ by looking at the properties of $f(x, y) = c$ over the rationals.

Crypto Property	**Algebraic Property**
One-wayness	genus $g > 0$
2nd-preimage resistant	No $\mathbb{Q}$ maps

Recap

We reason about properties of $f(x, y) \bmod N$ by looking at the properties of $f(x, y) = c$ over the rationals.

Crypto Property	**Algebraic Property**
One-wayness	genus $g > 0$
2nd-preimage resistant	No $\mathbb{Q}$ maps
Collision-resistant	Injective on $\mathbb{Q} \times \mathbb{Q}$

Conclusion

- Can we prove in a generic ring model that $x^7 + 3y^7$ is collision resistant $\bmod N$? [Aggarwal-Maurer 2009]

Conclusion

- Can we prove in a generic ring model that $x^7 + 3y^7$ is collision resistant $\bmod N$? [Aggarwal-Maurer 2009]
- What other applications are there for bivariates $\bmod N$?

Conclusion

- Can we prove in a generic ring model that $x^7 + 3y^7$ is collision resistant $\bmod N$? [Aggarwal-Maurer 2009]
- What other applications are there for bivariates $\bmod N$?

Conclusion

- Can we prove in a generic ring model that $x^7 + 3y^7$ is collision resistant $\bmod N$? [Aggarwal-Maurer 2009]
- What other applications are there for bivariates $\bmod N$?

Thanks to Antoine Joux, Bjorn Poonen, Don Zagier, Joe Zimmerman, and Steven Galbraith for helpful comments and suggestions.