On the Balasubramanian-Koblitz Results

Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute, Kolkata
India
palash@isical.ac.in

Institute of Mathematical Sciences,
22nd February 2012

As Part of
Number Theory Year Celebration
and
Felicitation of Professor R. Balasubramanian

The Paper

This talk is about the following paper.

R. Balasubramanian and N. Koblitz. The improbability than an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, 11 (2):141–145, 1998. (**Submitted** November 1995.)

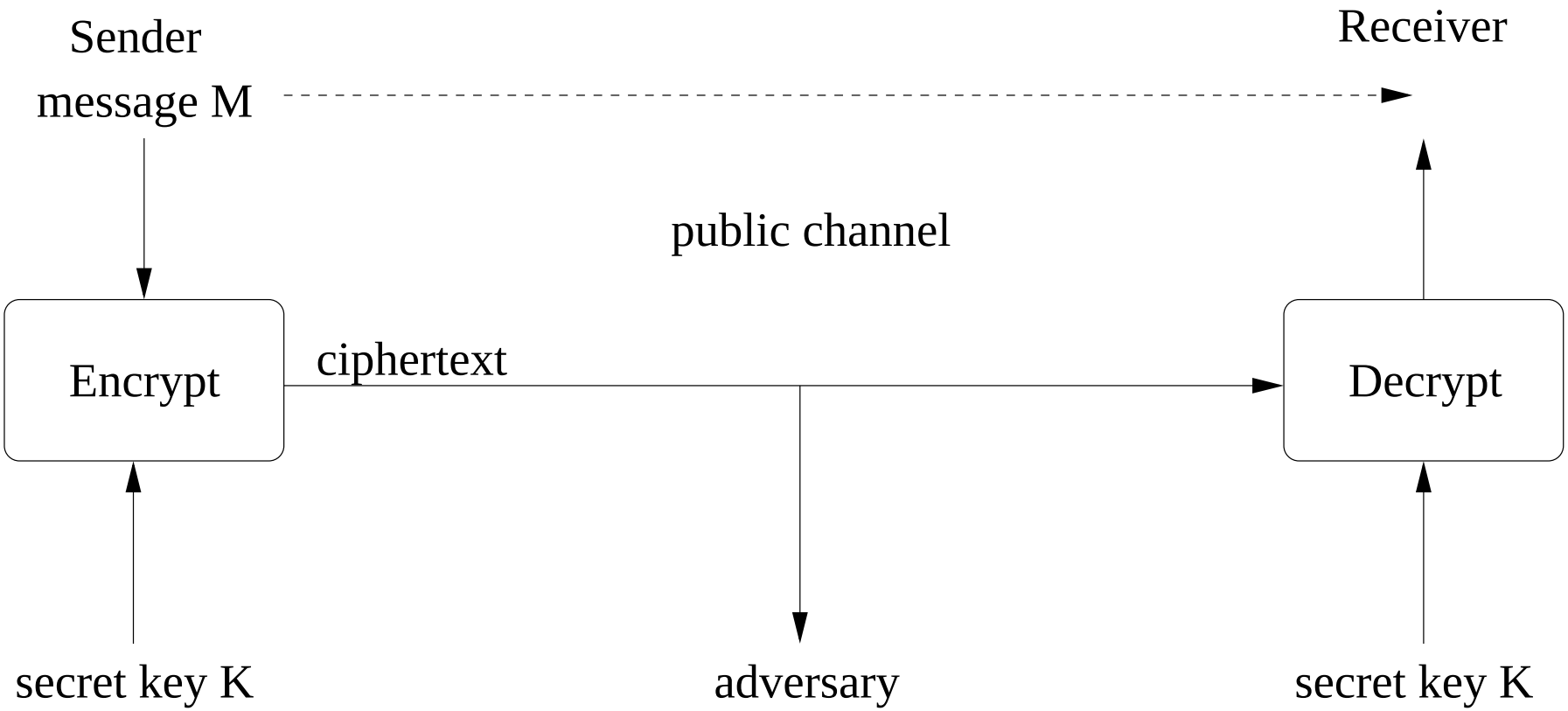
Overview of the Presentation

- A bit of cryptography.
- Elliptic curve discrete log problem.
- Balasubramanian-Koblitz reassurance.

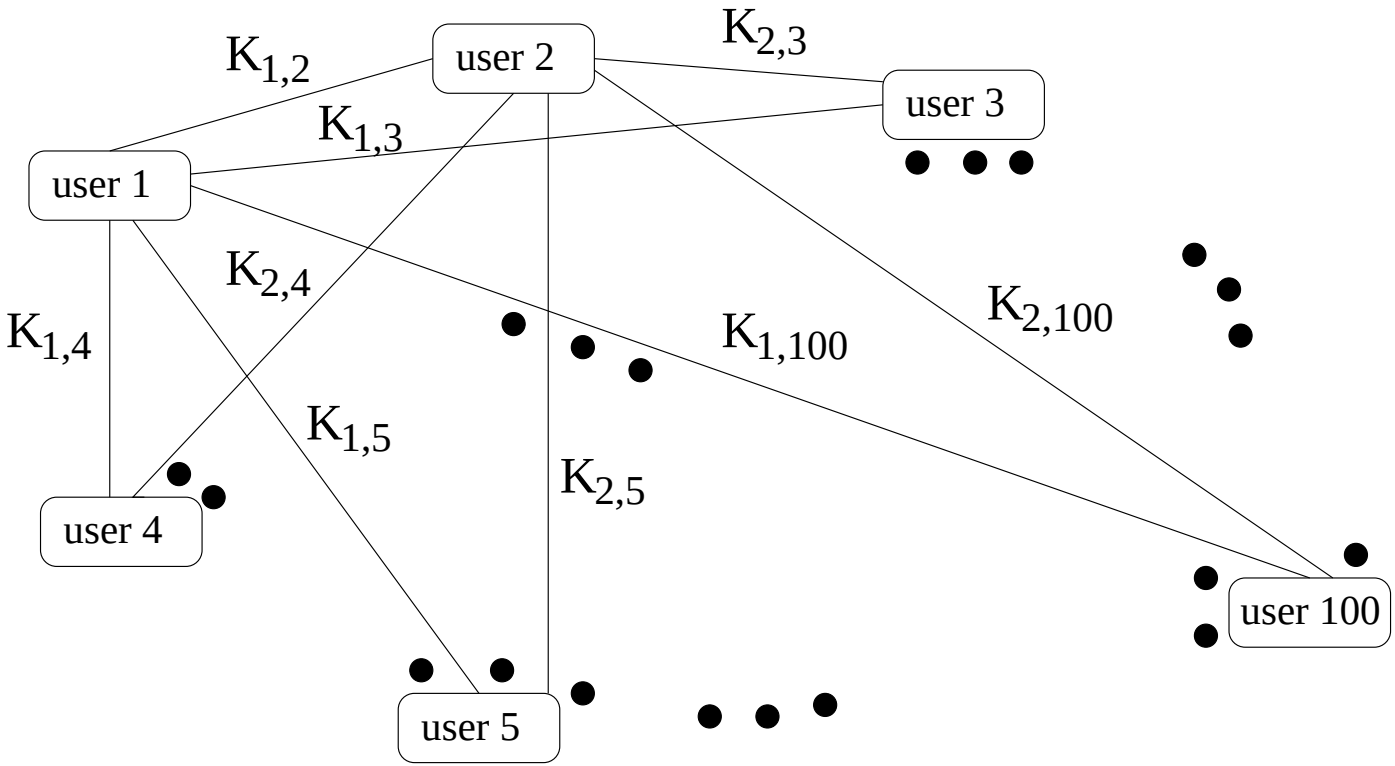
Overview of the Presentation

- A bit of cryptography.
- Elliptic curve discrete log problem.
- Balasubramanian-Koblitz reassurance.
- Pairing-based cryptography.
- Balasubramanian-Koblitz sufficient condition on embedding degree.

Classical View of Cryptography



The Key Management Problem



- There are $\binom{100}{2}$ bi-directional links.
- Each link has an associated secret key.
- Each user has to maintain the secrecy of 99 keys.

Change 100 to larger n to see the immensity of the problem!

Diffie-Hellman Public Key Agreement

How to agree upon a secret through public discussion?

Diffie-Hellman Public Key Agreement

How to agree upon a secret through public discussion?

Cyclic group $G = \{1, g, g^2, \ldots, g^{p-1}\}$

Alice		Bob
1. Choose secret a;		1. Choose secret b;
2. Compute g^a;		2. Compute g^b;
	send g^a →	
	← send g^b	
3. Compute $K=(g^b)^a=g^{ab}$		3. Compute $K=(g^a)^b=g^{ab}$

Computationally Hard Problems

Computational Diffie-Hellman Problem.

Given (g, g^a, g^b) compute g^{ab}.

Discrete Logarithm Problem.

Given $(g, h = g^a)$ compute $a \stackrel{\Delta}{=} \log_g h$.

Computationally Hard Problems

Computational Diffie-Hellman Problem.

Given (g, g^a, g^b) compute g^{ab}.

Discrete Logarithm Problem.

Given $(g, h = g^a)$ compute $a \stackrel{\Delta}{=} \log_g h$.

If DL can be solved, then CDH can be solved

Computationally Hard Problems

Computational Diffie-Hellman Problem.

Given (g, g^a, g^b) compute g^{ab}.

Discrete Logarithm Problem.

Given $(g, h = g^a)$ compute $a \stackrel{\Delta}{=} \log_g h$.

If DL can be solved, then CDH can be solved
and then DH-KA can be 'broken'.

Computationally Hard Problems

Computational Diffie-Hellman Problem.

$$\text{Given } (g, g^a, g^b) \text{ compute } g^{ab}.$$

Discrete Logarithm Problem.

$$\text{Given } (g, h = g^a) \text{ compute } a \stackrel{\Delta}{=} \log_g h.$$

If DL can be solved, then CDH can be solved
and then DH-KA can be 'broken'.

Necessary criterion for security: Choose the group order p to be large enough so that solving DLP becomes infeasible.

Computationally Hard Problems

Computational Diffie-Hellman Problem.

$$\text{Given } (g, g^a, g^b) \text{ compute } g^{ab}.$$

Discrete Logarithm Problem.

$$\text{Given } (g, h = g^a) \text{ compute } a \stackrel{\Delta}{=} \log_g h.$$

If DL can be solved, then CDH can be solved
and then DH-KA can be 'broken'.

Necessary criterion for security: Choose the group order p to be large enough so that solving DLP becomes infeasible.

Efficiency issue: Working with a larger group will slow down the computations.

Generic Methods for Solving DLP

Brute Force: Given (g, h), for each $a \in \{0, \ldots, p-1\}$ compute g^a and check whether this is equal to h.

- Requires p exponentiations (in the worst case).

Generic Methods for Solving DLP

Brute Force: Given (g, h), for each $a \in \{0, \ldots, p-1\}$ compute g^a and check whether this is equal to h.

- Requires p exponentiations (in the worst case).

Pollard's Rho: A clever method that ensures that a can be found with high probability using about $\sqrt{p}$ steps.

Generic Methods for Solving DLP

Brute Force: Given (g, h), for each $a \in \{0, \ldots, p-1\}$ compute g^a and check whether this is equal to h.

- Requires p exponentiations (in the worst case).

Pollard's Rho: A clever method that ensures that a can be found with high probability using about $\sqrt{p}$ steps.

Representing an element of the group requires at least $\lceil \log_2 p \rceil$ bits. So both algorithms require time which is exponential in $\log p$.

Groups Obtained From Finite Fields

- A subgroup of order p of the multiplicative group of a finite field $\mathbb{F}$.
- There are two parameters: p and $\#\mathbb{F}$.
- Representing an element of the field requires $\lceil \log_2 \#\mathbb{F} \rceil$ bits.
- Pollard's rho requires $O(p^{1/2})$ time.

Groups Obtained From Finite Fields

- A subgroup of order p of the multiplicative group of a finite field $\mathbb{F}$.
- There are two parameters: p and $\#\mathbb{F}$.
- Representing an element of the field requires $\lceil \log_2 \#\mathbb{F} \rceil$ bits.
- Pollard's rho requires $O(p^{1/2})$ time.

Sub-exponential algorithm for DLP: runtime

$$O\left(\exp\left((\log \#\mathbb{F})^{c}(\log\log \#\mathbb{F})^{1-c}\right)\right).$$

Groups Obtained From Finite Fields

- A subgroup of order p of the multiplicative group of a finite field $\mathbb{F}$.
- There are two parameters: p and $\#\mathbb{F}$.
- Representing an element of the field requires $\lceil \log_2 \#\mathbb{F} \rceil$ bits.
- Pollard's rho requires $O(p^{1/2})$ time.

Sub-exponential algorithm for DLP: runtime

$$O\left(\exp\left((\log \#\mathbb{F})^{c}(\log\log \#\mathbb{F})^{1-c}\right)\right).$$

- To ensure that solving DLP takes about 2^{80} time, p should be about 2^{160} and $\#\mathbb{F}$ should be about 2^{1500}.
- Field elements would be represented using about 1500 bits.

Groups of Points on an Elliptic Curve

Suggested independently by Koblitz and Miller in 1985.

- Assume $\mathrm{char}(\mathbb{F}) \neq 2, 3$: simplied Weierstraß form:

$$y^2 = x^3 + ax + b \qquad (*)$$

$a, b \in \mathbb{F}$ and $4a^3 + 27b^2 \neq 0$.

- Points (x, y) satisfying $(*)$ form a group under a suitably defined addition law.

Groups of Points on an Elliptic Curve

Suggested independently by Koblitz and Miller in 1985.

- Assume $\mathrm{char}(\mathbb{F}) \neq 2, 3$: simplied Weierstraß form:

$$y^2 = x^3 + ax + b \qquad (*)$$

  $a, b \in \mathbb{F}$ and $4a^3 + 27b^2 \neq 0$.
  - Points (x, y) satisfying $(*)$ form a group under a suitably defined addition law.
- Cryptography is done over a suitable prime order subgroup.
- No known sub-exponential algorithm for the discrete log problem.
- So, choose parameter sizes to just protect against Pollard's rho.
- Leads to smaller key sizes and faster encryption/decryption algorithms.

Bilinear Maps

Let G_1, G_2: (additive) cyclic groups; G_T: (multiplicative) cyclic group.

$$e : G_1 \times G_2 \rightarrow G_T.$$

- $e(P, Q_1 + Q_2) = e(P, Q_1) \times e(P, Q_2)$.
- $e(P_1 + P_2, Q) = e(P_1, Q) \times e(P_2, Q)$.

Bilinear Maps

Let G_1, G_2: (additive) cyclic groups; G_T: (multiplicative) cyclic group.

$$e : G_1 \times G_2 \rightarrow G_T.$$

- $e(P, Q_1 + Q_2) = e(P, Q_1) \times e(P, Q_2)$.
- $e(P_1 + P_2, Q) = e(P_1, Q) \times e(P_2, Q)$.

For any $a, b \in \mathbb{Z}_p$, $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$.

Bilinear Maps

Let G_1, G_2: (additive) cyclic groups; G_T: (multiplicative) cyclic group.

$$e : G_1 \times G_2 \rightarrow G_T.$$

- $e(P, Q_1 + Q_2) = e(P, Q_1) \times e(P, Q_2)$.
- $e(P_1 + P_2, Q) = e(P_1, Q) \times e(P_2, Q)$.

$$\text{For any } a, b \in \mathbb{Z}_p,\ e(aP_1, bP_2) = e(P_1, P_2)^{ab}.$$

- The only known examples of e arise from Weil and Tate pairings where G_1 and G_2 are sub-groups of a group of points on an elliptic curve and G_T is a subgroup of the multiplicative group of a finite field $\mathbb{F}$.

Menezes-Okamoto-Vanstone Reduction

Suppose $G_1 = \langle P_1 \rangle$ and $G_2 = \langle P_2 \rangle$.

DLP in G_1: Given (P_1, Q_1) find a such that $Q_1 = aP_1$.

Menezes-Okamoto-Vanstone Reduction

Suppose $G_1 = \langle P_1 \rangle$ and $G_2 = \langle P_2 \rangle$.

DLP in G_1: Given (P_1, Q_1) find a such that $Q_1 = aP_1$.

Transferring to DLP on G_T:
Let $g = e(P_1, P_2)$ and $h = (Q_1, P_2)$. If $h = g^a$, then $Q_1 = aP_1$.

Instead of solving DLP on G_1, it is sufficient to solve DLP on G_T.

Menezes-Okamoto-Vanstone Reduction

Suppose $G_1 = \langle P_1 \rangle$ and $G_2 = \langle P_2 \rangle$.

DLP in G_1: Given (P_1, Q_1) find a such that $Q_1 = aP_1$.

Transferring to DLP on G_T:
Let $g = e(P_1, P_2)$ and $h = (Q_1, P_2)$. If $h = g^a$, then $Q_1 = aP_1$.

Instead of solving DLP on G_1, it is sufficient to solve DLP on G_T.

G_T is a subgroup of the multiplicative group of a finite field $\mathbb{F}$.

To solve DLP in G_1 one can use a sub-exponential algorithm over $\mathbb{F}$.

If $\#\mathbb{F}$ is not much larger than $\#G_1$, then DLP in G_1 is not much harder than the DLP in $\mathbb{F}$.

Embedding Degree

Suppose G_1 is a subgroup of $E[\mathbb{F}_q]$ Then for the embedding, $\#\mathbb{F}$ should be q^k such that $p = \#G_1$ divides $q^k - 1$.

- This is clearly a necessary condition.
- The parameter k is called the embedding degree.

Embedding Degree

Suppose G_1 is a subgroup of $E[\mathbb{F}_q]$ Then for the embedding, $\#\mathbb{F}$ should be q^k such that $p = \#G_1$ divides $q^k - 1$.

- This is clearly a necessary condition.
- The parameter k is called the embedding degree.

Crucial question: How large is k?

Embedding Degree

Suppose G_1 is a subgroup of $E[\mathbb{F}_q]$ Then for the embedding, $\#\mathbb{F}$ should be q^k such that $p = \#G_1$ divides $q^k - 1$.

- This is clearly a necessary condition.
- The parameter k is called the embedding degree.

Crucial question: How large is k?

If k is not too large, then DLP over elliptic curves is not much harder than DLP over finite fields.

For supersingular curves, this is indeed true ($k \leq 6$).

The question is how hard is this for randomly chosen elliptic curves?

Balasubramanian-Koblitz Reassurance

Theorem 2 (simplified statement): Suppose q is a prime. Then the probability that for a randomly chosen elliptic curve having a subgroup of size p (another prime), the probability that $p|q^k - 1$ for some $k < (\log q)^2$ is less than $(\log q)^{9+\varepsilon} q^{-1}$.

Balasubramanian-Koblitz Reassurance

Theorem 2 (simplified statement): Suppose q is a prime. Then the probability that for a randomly chosen elliptic curve having a subgroup of size p (another prime), the probability that $p|q^k - 1$ for some $k < (\log q)^2$ is less than $(\log q)^{9+\varepsilon} q^{-1}$.

Example: if q is a 160-bit prime, then the probability that the embedding degree is less than $(160)^2$ is less than roughly $(160)^9/2^{160} < 2^{-88}$.

Balasubramanian-Koblitz Reassurance

- With high probability, the embedding degree is ‘large’.
- In other words, with high probability, the size of the field $\mathbb{F}$ will be q^k with $k > (\log q)^2$.
- An algorithm which is sub-exponential in q^k will actually be exponential in p.

Balasubramanian-Koblitz Reassurance

- With high probability, the embedding degree is 'large'.
- In other words, with high probability, the size of the field $\mathbb{F}$ will be q^k with $k > (\log q)^2$.
- An algorithm which is sub-exponential in q^k will actually be exponential in p.

So, randomly chosen elliptic curves are safe from MOV reduction attacks.

This had and continues to have important implications for both theoretical and industrial applications of elliptic curve cryptography.

Pairing-Based Cryptography

$e : G_1 \times G_2 \to G_T$ satisfying $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$.

Pairing-Based Cryptography

$$e : G_1 \times G_2 \to G_T \qquad \text{satisfying } e(aP_1, bP_2) = e(P_1, P_2)^{ab}.$$

Provides an interesting tool to construct cryptographic primitives.

- Joux (2000): 3-party 1-round key agreement.
- Sakai-Ohgishi-Kasahara (2000): identity-based key agreement.
- Boneh-Franklin (2001): identity-based encryption.
- More than one decade of research.

Pairing-Based Cryptography

$$e : G_1 \times G_2 \to G_T \qquad \text{satisfying } e(aP_1, bP_2) = e(P_1, P_2)^{ab}.$$

Provides an interesting tool to construct cryptographic primitives.

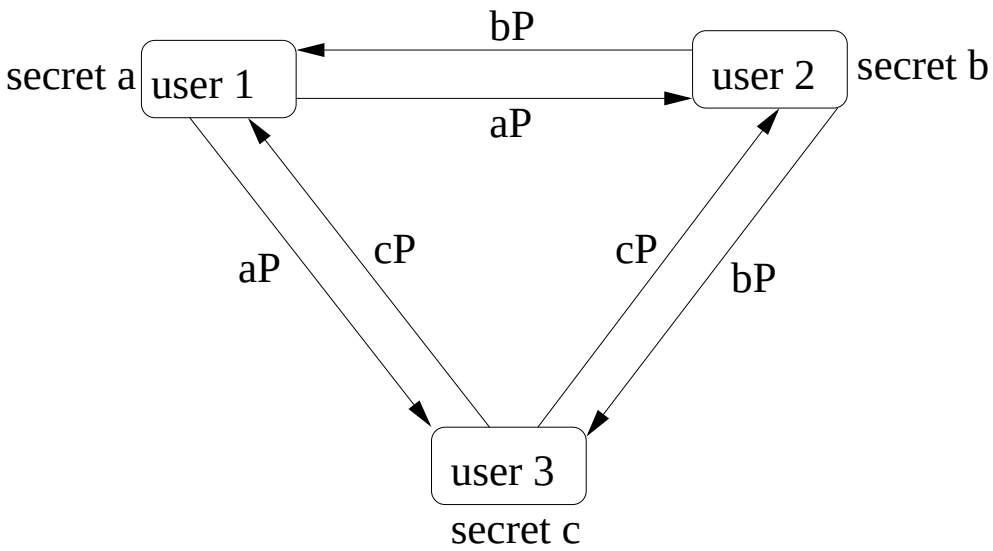
- Joux (2000): 3-party 1-round key agreement.
- Sakai-Ohgishi-Kasahara (2000): identity-based key agreement.
- Boneh-Franklin (2001): identity-based encryption.
- More than one decade of research.

Reason: Pairings can be used to construct cryptographic primitives which cannot be otherwise constructed.

Joux's 3-Party 1-Round KA (2000)

$$G = \langle P \rangle; e : G \times G \to G_T$$

(Assume symmetric pairing, i.e., $G_1 = G_2 = G$.)



$$\begin{aligned} e(P,P)^{abc} &= e(bP,cP)^{a} \text{ (user 1 computes)} \\ &= e(aP,cP)^{b} \text{ (user 2 computes)} \\ &= e(aP,bP)^{c} \text{ (user 3 computes).} \end{aligned}$$

More Hard Problems

Bilinear Diffie-Hellman Problem.

Given (P, aP, bP, cP) compute $e(P, P)^{abc}$.

More Hard Problems

Bilinear Diffie-Hellman Problem.

$$\text{Given } (P, aP, bP, cP) \text{ compute } e(P, P)^{abc}.$$

Solving DLP in either G or G_T will lead to a solution to the BDH problem.

So, for the scheme to be secure DLP should be hard in both G and G_T.

If the embedding degree is too large, then computations over G_T will be too slow.

So the embedding degree will have to be small.

Implementing Pairing-Based Cryptography

If the embedding degree is too large, then computations over G_T will be too slow.

So the embedding degree will have to be small.

Sub-exponential algorithms will apply.

Increase parameter sizes to compensate.

Pairing-Friendly Curves

From the BK result, ‘random’ curves will have high embedding degrees.

So, one needs methods to construct curves with low to moderate embedding degrees.

Pairing-Friendly Curves

From the BK result, ‘random’ curves will have high embedding degrees.

So, one needs methods to construct curves with low to moderate embedding degrees.

As mentioned earlier, a necessary condition on k is that $p|q^k - 1$.

But, is this sufficient?

Balasubramanian-Koblitz Sufficient Condition

Theorem 1 (simplified): If $p \not| q - 1$ and $p | q^k - 1$, then an elliptic curve group of order p can be embedded into the field $\mathbb{F}$ where $\#\mathbb{F} = q^k$.

Balasubramanian-Koblitz Sufficient Condition

Theorem 1 (simplified): If $p \not| q-1$ and $p|q^k-1$, then an elliptic curve group of order p can be embedded into the field $\mathbb{F}$ where $\#\mathbb{F} = q^k$.

The following fact is a by product of the proof.

Fact 1: If $p \not| q-1$ and $p|q^k-1$, then $E(\mathbb{F}_{q^k})$ contains a point Q of order p which is linearly independent of a point P of order p in $E(\mathbb{F}_q)$.

Balasubramanian-Koblitz Sufficient Condition

Theorem 1 (simplified): If $p \not| q-1$ and $p|q^k-1$, then an elliptic curve group of order p can be embedded into the field $\mathbb{F}$ where $\#\mathbb{F} = q^k$.

The following fact is a by product of the proof.

Fact 1: If $p \not| q-1$ and $p|q^k-1$, then $E(\mathbb{F}_{q^k})$ contains a point Q of order p which is linearly independent of a point P of order p in $E(\mathbb{F}_q)$.

- Theorem 1 has simplified the task of finding pairing-friendly curves.
- Fact 1 has considerably helped in designing efficient algorithms for computing pairings.

Summary

- The cryptographic motivation for studying the discrete logarithm problem.
- Sub-exponential algorithms and its effects on parameter sizes and efficiency of computations.
- MOV Reduction.
- Balasubramanian-Koblitz reassurance about the non-applicability of the MOV reduction to ‘random’ elliptic curves.
- Pairing based cryptography.
- Balasubramanian-Koblitz sufficient condition for embedding an elliptic curve into a finite field.

Thank you for your attention!