a quick quiz on cricket & crypto

7 questions in 7 minutes

Craig Costello

2014 – ECC Rump Session

Chennai, India

Question 1

The favourite to win next year’s cricket world cup is:

Question 1

The favourite to win next year’s cricket world cup is:

a) USA

Question 1

The favourite to win next year’s cricket world cup is:

a) USA

b) South Africa

Question 1

The favourite to win next year’s cricket world cup is:

a) USA

b) South Africa

c) India

Question 1

The favourite to win next year’s cricket world cup is:

a) USA

b) South Africa

c) India

d) Australia

Answer 1

The favourite to win next year's cricket world cup is:

~~a) USA~~

~~b) South Africa~~

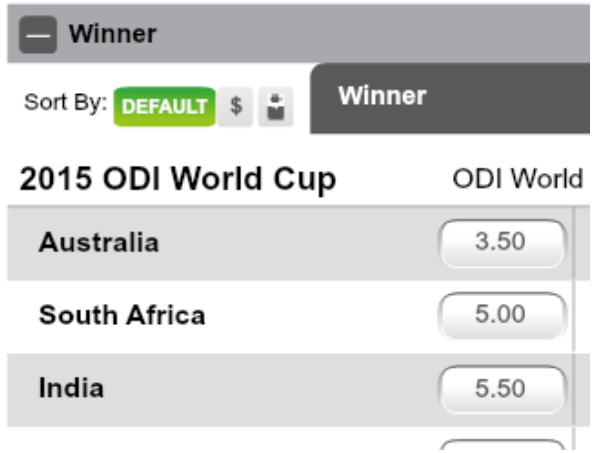
~~c) India~~

d) Australia

source: indiabet.com
8th October, 2014

Event Winner	
Lines Available	**Odds**
Australia	4.00
India	4.50
South Africa	5.00
England	8.00

source: tabsportsbet.com.au
8th October 2014



Winner	
Sort By: DEFAULT $	Winner
2015 ODI World Cup	ODI World
Australia	3.50
South Africa	5.00
India	5.50

Question 2

You want to work as fast as possible in the Jacobian group of a genus 2 curve, so you choose to cast the Mumford coordinates $(q, r, s, t) \leftrightarrow (x^2 + qx + r, sx + t)$ into projective space by introducing an additional coordinate.

Which projective space (weightings) do you choose?

Question 2

You want to work as fast as possible in the Jacobian group of a genus 2 curve, so you choose to cast the Mumford coordinates $(q, r, s, t) \leftrightarrow (x^2 + qx + r, sx + t)$ into projective space by introducing an additional coordinate.

Which projective space (weightings) do you choose?

a) $(\lambda^2\, Q : \lambda^2\, R : \lambda^3\, S : \lambda^3\, T : \lambda^1 Z) \in P(2, 2, 3, 3, 1)$

to follow Lange‘05

Question 2

You want to work as fast as possible in the Jacobian group of a genus 2 curve, so you choose to cast the Mumford coordinates $(q, r, s, t) \leftrightarrow (x^2 + qx + r, sx + t)$ into projective space by introducing an additional coordinate.

Which projective space (weightings) do you choose?

a) $(\lambda^2\, Q : \lambda^2\, R : \lambda^3\, S : \lambda^3\, T : \lambda^1 Z) \in P(2, 2, 3, 3, 1)$

to follow Lange'05

b) $(\lambda^1\, Q : \lambda^1\, R : \lambda^1\, S : \lambda^1\, T : \lambda^1 Z) \in P(1, 1, 1, 1, 1)$

to follow C-Lauter'11

Question 2

You want to work as fast as possible in the Jacobian group of a genus 2 curve, so you choose to cast the Mumford coordinates $(q, r, s, t) \leftrightarrow (x^2 + qx + r, sx + t)$ into projective space by introducing an additional coordinate.

Which projective space (weightings) do you choose?

a) $(\lambda^2 Q : \lambda^2 R : \lambda^3 S : \lambda^3 T : \lambda^1 Z) \in P(2, 2, 3, 3, 1)$

to follow Lange'05

b) $(\lambda^1 Q : \lambda^1 R : \lambda^1 S : \lambda^1 T : \lambda^1 Z) \in P(1, 1, 1, 1, 1)$

to follow C-Lauter'11

c) $(\lambda^2 Q : \lambda^4 R : \lambda^3 S : \lambda^5 T : \lambda^1 Z) \in P(2, 4, 3, 5, 1)$

you want each coordinate to feel special with its own individual weighting

Question 2

You want to work as fast as possible in the Jacobian group of a genus 2 curve, so you choose to cast the Mumford coordinates $(q, r, s, t) \leftrightarrow (x^2 + qx + r, sx + t)$ into projective space by introducing an additional coordinate.

Which projective space (weightings) do you choose?

a) $(\lambda^2 Q : \lambda^2 R : \lambda^3 S : \lambda^3 T : \lambda^1 Z) \in P(2, 2, 3, 3, 1)$

to follow Lange‘05

b) $(\lambda^1 Q : \lambda^1 R : \lambda^1 S : \lambda^1 T : \lambda^1 Z) \in P(1, 1, 1, 1, 1)$

to follow C-Lauter‘11

c) $(\lambda^2 Q : \lambda^4 R : \lambda^3 S : \lambda^5 T : \lambda^1 Z) \in P(2, 4, 3, 5, 1)$

you want each coordinate to feel special with its own individual weighting

d) None of the above

Answer 2

You want to work as fast as possible in the Jacobian group of a genus 2 curve, so you choose to cast the Mumford coordinates $(q, r, s, t) \leftrightarrow (x^2 + qx + r, sx + t)$ into projective space by introducing an additional coordinate.

Which projective space (weightings) do you choose?

~~a) $(\lambda^2 Q : \lambda^2 R : \lambda^3 S : \lambda^3 T : \lambda^1 Z) \in P(2, 2, 3, 3, 1)$~~

~~to follow Lange'05~~

~~b) $(\lambda^1 Q : \lambda^1 R : \lambda^1 S : \lambda^1 T : \lambda^1 Z) \in P(1, 1, 1, 1, 1)$~~

~~to follow C-Lauter'11~~

c) $\left(\lambda^2 Q : \lambda^4 R : \lambda^3 S : \lambda^5 T : \lambda^1 Z\right) \in P(2, 4, 3, 5, 1)$

you want each coordinate to feel special with its own individual weighting

~~d) None of the above~~

Source

up to $1.29\times$ faster to work in $\boldsymbol{P(2,4,3,5,1)}$!!!

Jacobian Coordinates on Genus 2 Curves

Hisil-C

to appear

at Asiacrypt 2014

http://eprint.iacr.org/2014/xxx.pdf

Question 3

The greatest test cricket batsman of all time is:

Question 3

The greatest test cricket batsman of all time is:

a) None of the below

Question 3

The greatest test cricket batsman of all time is:

a) None of the below

b) Brian Lara (West Indies)

Question 3

The greatest test cricket batsman of all time is:

a) None of the below

b) Brian Lara (West Indies)

c) Sachin Tendulkar (India)

Question 3

The greatest test cricket batsman of all time is:

a) None of the below

b) Brian Lara (West Indies)

c) Sachin Tendulkar (India)

d) Greg Chappell (Australia)

Answer 3

The greatest test cricket batsman of all time is:

a) None of the below

~~b) Brian Lara (West Indies)~~

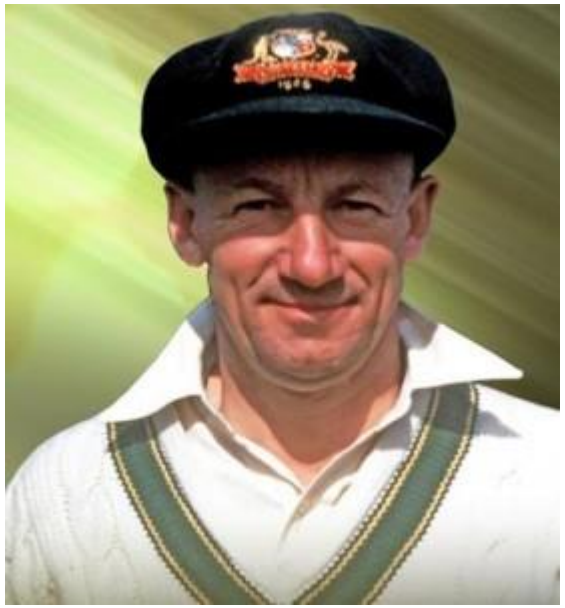
~~c) Sachin Tendulkar (India)~~

~~d) Greg Chappell (Australia)~~

Source

wikipedia

Sir Donald Bradman



Career Test average leaders [edit]

Top 20 retired Test batsmen [edit]

Rank	Batsman	Tests	Innings	not out	Runs	Highest	Career average	Career span
1	Don Bradman	52	80	10	6996	334	99.94	1928-1948
2	Graeme Pollock	23	41	4	2256	274	60.97	1963–1970
3	George Headley	22	40	4	2190	270*	60.83	1930–1954
4	Herbert Sutcliffe	54	84	9	4555	194	60.73	1924–1935
5	Eddie Paynter	20	31	5	1540	243	59.23	1931–1939
6	Ken Barrington	82	131	15	6806	256	58.67	1955–1968
7	Everton Weekes	48	81	5	4455	207	58.61	1948–1958
8	Wally Hammond	85	140	16	7249	336*	58.45	1927–1947
9	Garfield Sobers	93	160	21	8032	365*	57.78	1954–1974
10	Jack Hobbs	61	102	7	5410	211	56.94	1908–1930
11	C.L. Walcott	44	74	7	3798	220	56.68	1948–1960
12	L. Hutton	79	138	15	6971	364	56.67	1937–1955
13	Jacques Kallis	166	280	40	13289	224	55.37	1995–2013
14	G.E. Tyldesley	14	20	2	990	122	55.00	1921–1929
15	C.A. Davis	15	29	5	1301	183	54.20	1968–1973
16	V.G. Kambli	17	21	2	1084	227*	54.20	1993–1995
17	G.S. Chappell	87	151	19	7110	247*	53.86	1970–1984
18	Dudley Nourse	34	62	7	2960	231	53.81	1935–1951
19	Sachin Tendulkar	200	329	33	15921	248*	53.78	1989–2013
20	B.C. Lara	131	232	6	11953	400*	52.88	1990–2006

Question 4

You want to implement a fast and secure cryptographic pairing at the 128-bit security level. Naturally you choose the BN parameterization

$$p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$$
$$n = 36u^4 + 36u^3 + 18u^2 + 6u + 1$$

to get your curve E/F_p with prime order n. But which u value would you choose?

Question 4

You want to implement a fast and secure cryptographic pairing at the 128-bit security level. Naturally you choose the BN parameterization

$$p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$$
$$n = 36u^4 + 36u^3 + 18u^2 + 6u + 1$$

to get your curve E/F_p with prime order n. But which u value would you choose?

a) $u = 2^{62} + 2^{59} + 2^{55} + 2^{15} + 2^{10} - 1$

(gives 254-bit primes p and n)

Question 4

You want to implement a fast and secure cryptographic pairing at the 128-bit security level. Naturally you choose the BN parameterization

$$p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$$
$$n = 36u^4 + 36u^3 + 18u^2 + 6u + 1$$

to get your curve E/F_p with prime order n. But which u value would you choose?

a) $u = 2^{62} + 2^{59} + 2^{55} + 2^{15} + 2^{10} - 1$

(gives 254-bit primes p and n)

b) $u = -(2^{62} + 2^{55} + 1)$

(also gives 254-bit primes p and n, but better NAF-weight, faster pairing, and same as in Microsoft, MIRACL, RELIC, PandA, etc libraries

Question 4

You want to implement a fast and secure cryptographic pairing at the 128-bit security level. Naturally you choose the BN parameterization

$$p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$$
$$n = 36u^4 + 36u^3 + 18u^2 + 6u + 1$$

to get your curve E/F_p with prime order n. But which u value would you choose?

a) $u = 2^{62} + 2^{59} + 2^{55} + 2^{15} + 2^{10} - 1$

(gives 254-bit primes p and n)

b) $u = -(2^{62} + 2^{55} + 1)$

(also gives 254-bit primes p and n, but better NAF-weight, faster pairing, and same as in Microsoft, MIRACL, RELIC, PandA, etc libraries

c) none of the above

Question 4

You want to implement a fast and secure cryptographic pairing at the 128-bit security level. Naturally you choose the BN parameterization

$$p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$$
$$n = 36u^4 + 36u^3 + 18u^2 + 6u + 1$$

to get your curve E/F_p with prime order n. But which u value would you choose?

a) $\boldsymbol{u = 2^{62} + 2^{59} + 2^{55} + 2^{15} + 2^{10} - 1}$

(gives 254-bit primes p and n)

~~b)~~ ~~$u = -(2^{62} + 2^{55} + 1)$~~

~~(also gives 254-bit primes p and n, but better NAF-weight, faster pairing, and same as in Microsoft, MIRACL, RELIC, PandA, etc libraries~~

~~c)~~ ~~none of the above~~

Answer 4

Subgroup security in pairing-based cryptography
Barreto-C-Misoczki-Naehrig-Pereira-Zanon
to appear on
cryptology eprint archive
http://eprint.iacr.org/2014/???.pdf

BN curve	$\lvert E(F_p)\rvert$	$\lvert E'(F_{p^2})\rvert$	$\lvert G_{\Phi_k(p)}\rvert$
$u = 2^{62} + 2^{59} + 2^{55} + 2^{15} + 2^{10} - 1$	p_{254}	$p_{254} \cdot p'_{254}$	$p_{254} \cdot p_{762}$
~~$u = -(2^{62} + 2^{55} + 1)$~~	p_{254}	$p_{254} \cdot c_{96} \cdot p_{158}$	$p_{254} \cdot c_{79} \cdot c_{681}$

p_i : i-bit prime, c_i: i-bit composite

≈7% slowdown in pairing (nowhere else), but thwarts subgroup attacks!

Question 5

Who is the most successful world cup cricket nation of all time?

Question 5

Who is the most successful world cup cricket nation of all time?

a) not Australia

Question 5

Who is the most successful world cup cricket nation of all time?

a) not Australia

b) Australia, whose record 4 world cup wins is twice as many as any other country and includes the incredible 1999-2003-2007 three-peat

Answer 5

Who is the most successful world cup cricket nation of all time?

~~a)~~ ~~not Australia~~

b) Australia, whose record 4 world cup wins is twice as many as any other country and includes the incredible 1999-2003-2007 three-peat

source: history

Question 6

You don’t think a large-scale quantum computer exists today, but you think it will in the future. You also believe there’s an adversary out there holding onto your precious traffic until that day comes. What key-agreement/signature primitives do you opt for in the TLS ciphersuite?

Question 6

You don’t think a large-scale quantum computer exists today, but you think it will in the future. You also believe there’s an adversary out there holding onto your precious traffic until that day comes. What key-agreement/signature primitives do you opt for in the TLS ciphersuite?

a) ECC for key agreement, ECC for signing

Question 6

You don’t think a large-scale quantum computer exists today, but you think it will in the future. You also believe there’s an adversary out there holding onto your precious traffic until that day comes. What key-agreement/signature primitives do you opt for in the TLS ciphersuite?

a) ECC for key agreement, ECC for signing
b) (R)-LWE for key agreement, (R)-LWE for signing

Question 6

You don’t think a large-scale quantum computer exists today, but you think it will in the future. You also believe there’s an adversary out there holding onto your precious traffic until that day comes. What key-agreement/signature primitives do you opt for in the TLS ciphersuite?

a) ECC for key agreement, ECC for signing
b) (R)-LWE for key agreement, (R)-LWE for signing
c) ECC for key agreement, RSA for signing

Question 6

You don’t think a large-scale quantum computer exists today, but you think it will in the future. You also believe there’s an adversary out there holding onto your precious traffic until that day comes. What key-agreement/signature primitives do you opt for in the TLS ciphersuite?

a) ECC for key agreement, ECC for signing
b) (R)-LWE for key agreement, (R)-LWE for signing
c) ECC for key agreement, RSA for signing
d) (R)-LWE for key agreement, ECC for signing

Question 6

You don’t think a large-scale quantum computer exists today, but you think it will in the future. You also believe there’s an adversary out there holding onto your precious traffic until that day comes. What key-agreement/signature primitives do you opt for in the TLS ciphersuite?

a) ECC for key agreement, ECC for signing
b) (R)-LWE for key agreement, (R)-LWE for signing
c) ECC for key agreement, RSA for signing
d) (R)-LWE for key agreement, ECC for signing
e) (R)-LWE for key agreement, RSA for signing

Answer 6

You don’t think a large-scale quantum computer exists today, but you think it will in the future. You also believe there’s an adversary out there holding onto your precious traffic until that day comes. What key-agreement/signature primitives do you opt for in the TLS ciphersuite?

~~a) ECC for key agreement, ECC for signing~~

~~b) (R)-LWE for key agreement, (R)-LWE for signing~~

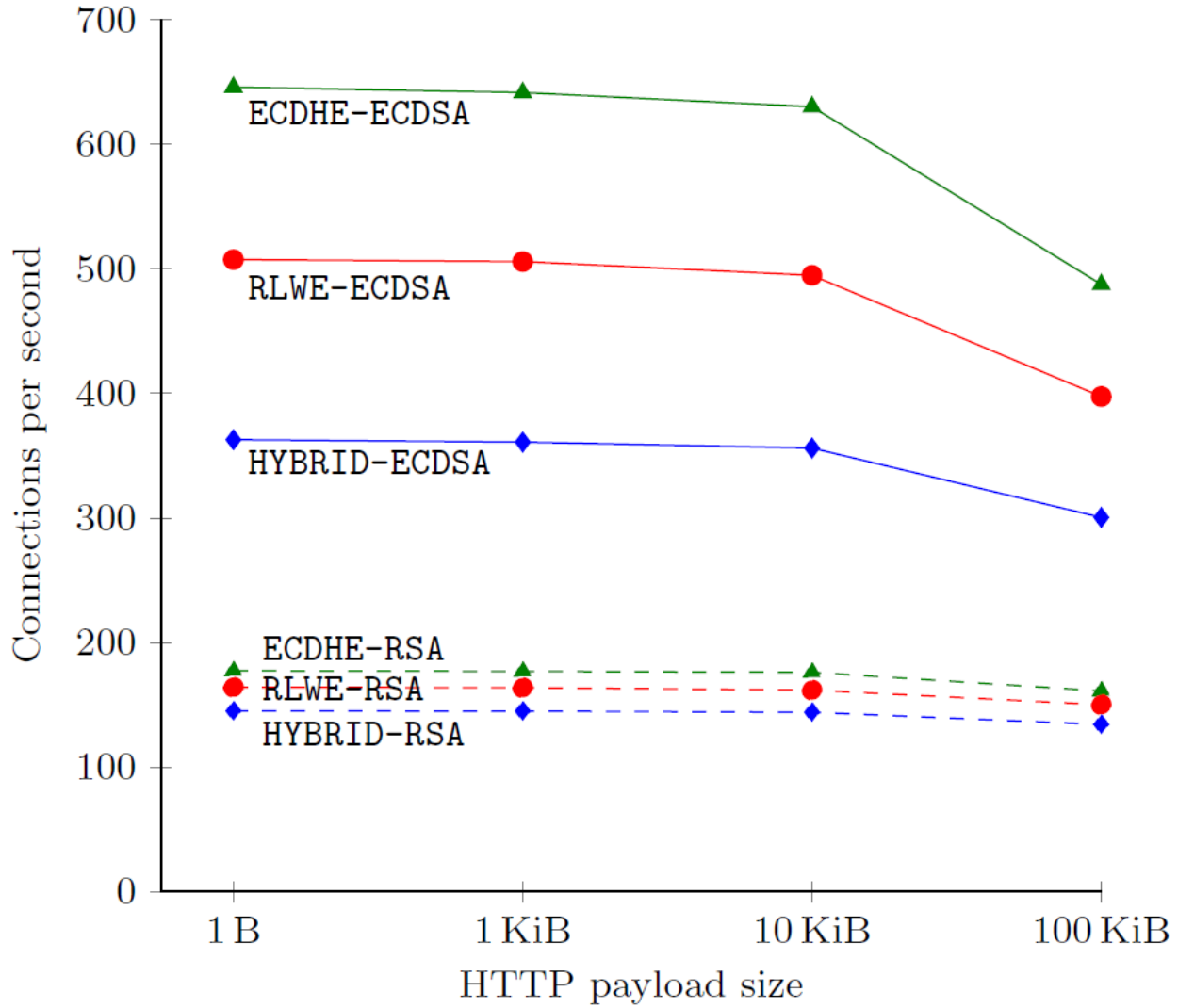
~~c) ECC for key agreement, RSA for signing~~

d) (R)-LWE for key agreement, ECC for signing

~~e) (R)-LWE for key agreement, RSA for signing~~

Answer 6

Post-quantum key exchange for the TLS protocol from the ring learning with errors problem
Bos-C-Naehrig-Stebila
http://eprint.iacr.org/2014/599.pdf



`RLWE-ECDSA-AES128-GCM-SHA256`

506 HTTPS connections per second for 10KiB payload

(only 21% slower than ECDHE-ECDSA in OpenSSL)

Question 7

In the Australia-India rivalry, who has won the Border-Gavaskar trophy more times?

Question 7

In the Australia-India rivalry, who has won the Border-Gavaskar trophy more times?

a) Australia

Question 7

In the Australia-India rivalry, who has won the Border-Gavaskar trophy more times?

a) Australia

b) India

Question 7

In the Australia-India rivalry, who has won the Border-Gavaskar trophy more times?

~~a) Australia~~

b) India