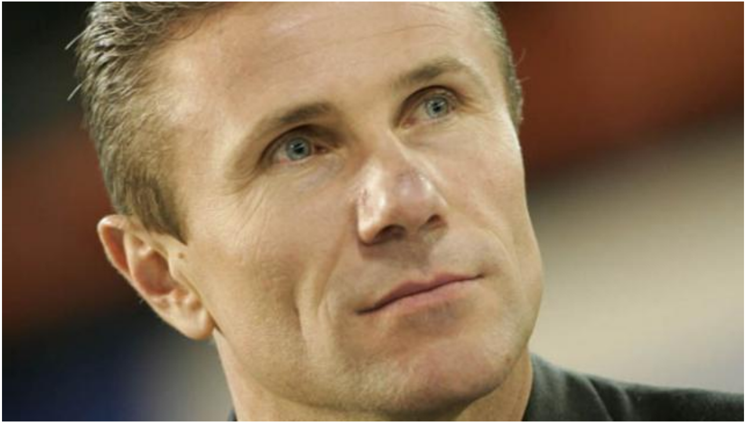
The relationship between some guy and cryptography

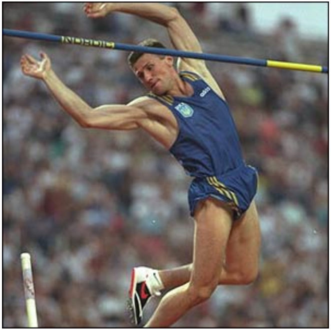
Răzvan Bărbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé, Marion Videau, Paul Zimmermann

Caramel/Inria/Loria

Who's this ?



Hint



Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

- 1987: 6.03m

Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

- 1987: 6.03m
- 1988: 6.05m

Serguei Bubka, pole vault champion

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m

Multiple WR holder.
(18 outdoor, 17 indoor)

Serguei Bubka, pole vault champion

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m

Multiple WR holder.
(18 outdoor, 17 indoor)

Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m
- 1991: 6.08m

Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m
- 1991: 6.08m
- 1991: 6.09m

Serguei Bubka, pole vault champion

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m
- 1991: 6.08m
- 1991: 6.09m
- 1991: 6.10m

Multiple WR holder.
(18 outdoor, 17 indoor)

Serguei Bubka, pole vault champion

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m
- 1991: 6.08m
- 1991: 6.09m
- 1991: 6.10m
- 1992: 6.11m

Multiple WR holder.
(18 outdoor, 17 indoor)

Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m
- 1991: 6.08m
- 1991: 6.09m
- 1991: 6.10m
- 1992: 6.11m
- 1992: 6.12m

Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m
- 1991: 6.08m
- 1991: 6.09m
- 1991: 6.10m
- 1992: 6.11m
- 1992: 6.12m
- 1992: 6.13m

Serguei Bubka, pole vault champion

Multiple WR holder.
(18 outdoor, 17 indoor)

- 1987: 6.03m
- 1988: 6.05m
- 1988: 6.06m
- 1991: 6.07m
- 1991: 6.08m
- 1991: 6.09m
- 1991: 6.10m
- 1992: 6.11m
- 1992: 6.12m
- 1992: 6.13m
- 1994: 6.14m

Link with crypto

6.14m is in the whereabouts of a crypto record.

Link with crypto

6.14m is in the whereabouts of a crypto record.

- Record for characteristic 2 DLP: 2^{613} (Joux, Lercier, 2005). (This is a prime degree extension).

Link with crypto

6.14m is in the whereabouts of a crypto record.

- Record for characteristic 2 DLP: 2^{613} (Joux, Lercier, 2005). (This is a prime degree extension).
- It's an old record, really.

Link with crypto

6.14m is in the whereabouts of a crypto record.

- Record for characteristic 2 DLP: 2^{613} (Joux, Lercier, 2005). (This is a prime degree extension).
- It's an old record, really.

What do you do in the plane ? Think about the rump session.

Link with crypto

6.14m is in the whereabouts of a crypto record.

- Record for characteristic 2 DLP: 2^{613} (Joux, Lercier, 2005). (This is a prime degree extension).
- It's an old record, really.

What do you do in the plane ? Think about the rump session.

- Have to update this record. Do it the Bubka way.

DL in a day in $\mathbb{F}_{2^{619}}$

$\#\mathbb{F}_{2^{619}}^{\times}$ has a 217-bit prime factor q.
Solving DLP mod q in $\mathbb{F}_{2^{619}}$ with FFS takes:

- Poly selection: ϵ. (Bărbulescu, Zimmermann)
- Sieve: < 200 core-hours. (Detrey, Gaudry, Videau)
- Filtering; ϵ. (Bouvier, Zimmermann)
- Matrix: 17h on a GPU, $+1$h CPU (Jeljeli, Thomé)
- Descent: not done yet (lazy guys).

DL in a day in $\mathbb{F}_{2^{619}}$

$\#\mathbb{F}_{2^{619}}^{\times}$ has a 217-bit prime factor q.
Solving DLP mod q in $\mathbb{F}_{2^{619}}$ with FFS takes:

- Poly selection: ϵ. (Bărbulescu, Zimmermann)
- Sieve: < 200 core-hours. (Detrey, Gaudry, Videau)
- Filtering; ϵ. (Bouvier, Zimmermann)
- Matrix: 17h on a GPU, +1h CPU (Jeljeli, Thomé)
- Descent: not done yet (lazy guys).

Business plan:

- Tons of trivial records to do next: 641, 643, ...
- Unfortunately there's no \$1M USD prize offered with each.

Result commitment

Abbreviation: `0x7` denotes $t^2 + t + 1$.

$$\begin{aligned} f &= x^6 + (\mathtt{0x7})x^5 + (\mathtt{0x6})x + (\mathtt{0x152A}), \\ g &= x + (t^{104} + \mathtt{0x6DBB}). \end{aligned}$$

(we like being stupid, and chose degree 6)
$\mathbb{F}_{2^{619}}$ defined by the adequate factor of $\mathrm{Res}_x(f, g)$.

$$\begin{aligned} \log_z(z+1) &\equiv \text{0xAF2374196F73B923A2CBDBCF33CBADF86FFB681C989185917F9E58} \mod q, \\ \log_z(z^2+z+1) &\equiv \text{0x8266B9C22ED99B8F3292AA11C2DD7BEF2B68703B869A1A6D7030C} \mod q, \\ \log_z(z^3+z+1) &\equiv \text{0xA3124184BF58FE05D05F3489612B37DD7A25D700CE14630FE82104} \mod q, \\ &\dots \end{aligned}$$