

Cryptography research at ICHEC

Neil Costigan

School of Computing, Dublin City University.

neil.costigan@computing.dcu.ie

PhD student.

Supervisor : - Prof Michael Scott.

IRCSET funded.





Talk Overview

- Public Key Cryptography 101.
- Research topics in Public Key Cryptography.
- Searching for Pairing friendly curves.
- Post-quantum computing Cryptography.



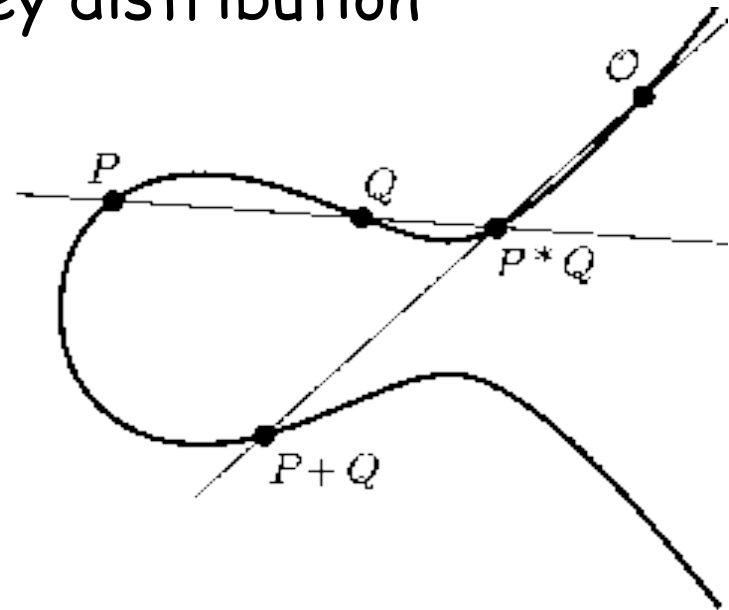
Public Key Crypto 101

- Early 70's technology.
- Used in
 - network security protocols
 - authentication
 - digital signatures
- Based on hard problems...
 - RSA / large primes
 - Elliptic Curve (ECC) / discrete log problem
 - McEliece / Error correcting codes

Why ECC ?

- Equivalent security with less computation overhead.
- Often used in mobile, embedded, and sensor networks for power characteristics.
- Pairings can help solve key distribution problem.

- $E(\mathbb{F}_p m) : y^2 = x^3 + Ax + B$
- $E(\mathbb{F}_2 m) : y^2 + y = x^3 + x + b$
- $E(\mathbb{F}_3 m) : y^2 = x^3 - x + b$





Pairings / IBE / PKI

Cryptographic pairings are primitives for security applications.

Pairings used for identity based encryption (IBE)

IBE Vs traditional PKI...

- Its easier to get people to use keys
- Its easier to manage keys
- Its easier to integrate into existing products
- New properties enable new features



Pairing friendly curves...

Not all elliptic curves are equal.

- Low embedding degree
- Large prime-order subgroup
- Rare

What we are speaking of is

- Security levels
- **Efficiency.** ie for low power.

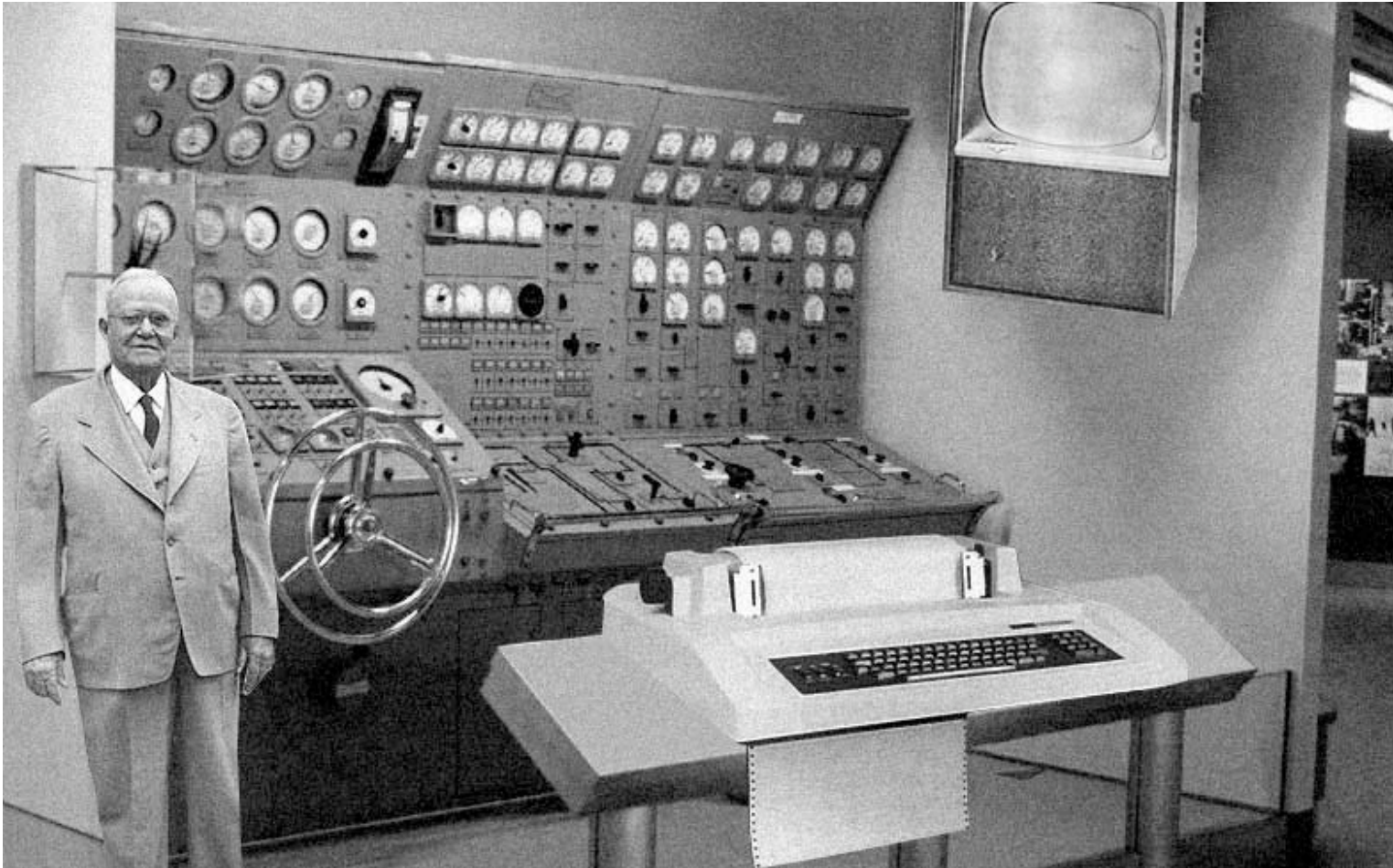


Finding pairing friendly curves

- Number of computational expensive 'tests'
- Can be pre-computed.
- Idea is a 'reference book' of curves.

- Brute Force Search.
- C++/MPI based over NTL and GMP.

Roll your own ...









Result...

- ~30,000 cpu hours
- Found new curves ! 😊
- No new families 😞
- No 'better' curves 😞
- Verify known curves !



McEliece

- Quantum computing and Crypto.
- Hot topic of crypto research.
- Recent paper* described theoretical attack.
- Factor of 5000 then by Factor of 2.
- Predicted 1400 days on a single Intel 2 Quad Q6600. That's 5600 core-days or 2^{58} CPU cycles

*Attacking and defending the McEliece cryptosystem. Daniel J. Bernstein, Tanja Lange, Christiane Peters. Technische Universiteit Eindhoven. PQCrypto2008



McEliece Practical Attack

- 200 computers involved, with about 300 cores. Ad hoc setup.
- Holland, US, France, Taiwan, Ireland.
- Computation finished in under 90 days most of the cores put in far fewer than 90 days of work.
- Some of which were considerably slower than a Core 2
- Used about 8000 core-days.



Luck of the Irish ?

- 2nd October 2008...
- Error vector found by Walton cluster at SFI/HEA Irish Centre of High-End Computing (ICHEC) 😊
- Total was 200,000 cpu hours worldwide
- We used 8,000 on Walton.



Thank you !

Questions ?

Numbers...

