Cryptogr🌹phy and elliptic c🌹rves : a 25-year «l🌹ve» (?) st🌹ry

Marc Girault
(formerly with France Telecom/Orange Labs R&D)

INDOCRYPT Conference, **New Delhi**, 13-16 December 2009

Many thanks to

- **Bimal Roy** and **Nicolas Sendrier** (and all the program committee) for this invitation
- The **organization committee** for kind arrangements and organization

Contents

1. What looks like **cryptology** in 1985 ?
2. The irruption of **elliptic curves** (1985-1989)
3. **ECC** incubation period (1990-1999)
4. The **pairing** tornado (2000-2009)
5. Applications
6. Experts' opinions
7. Conclusion (?)

1. What looks like cryptology in 1985 ?

80's : effervescence years

- DES and RSA recent and undisputed crypto-stars
- One new scheme (and nearly one broken…) per day
- Birth of IACR (International Association for Cryptologic Research)
- Birth of Crypto, Eurocrypt, JoC

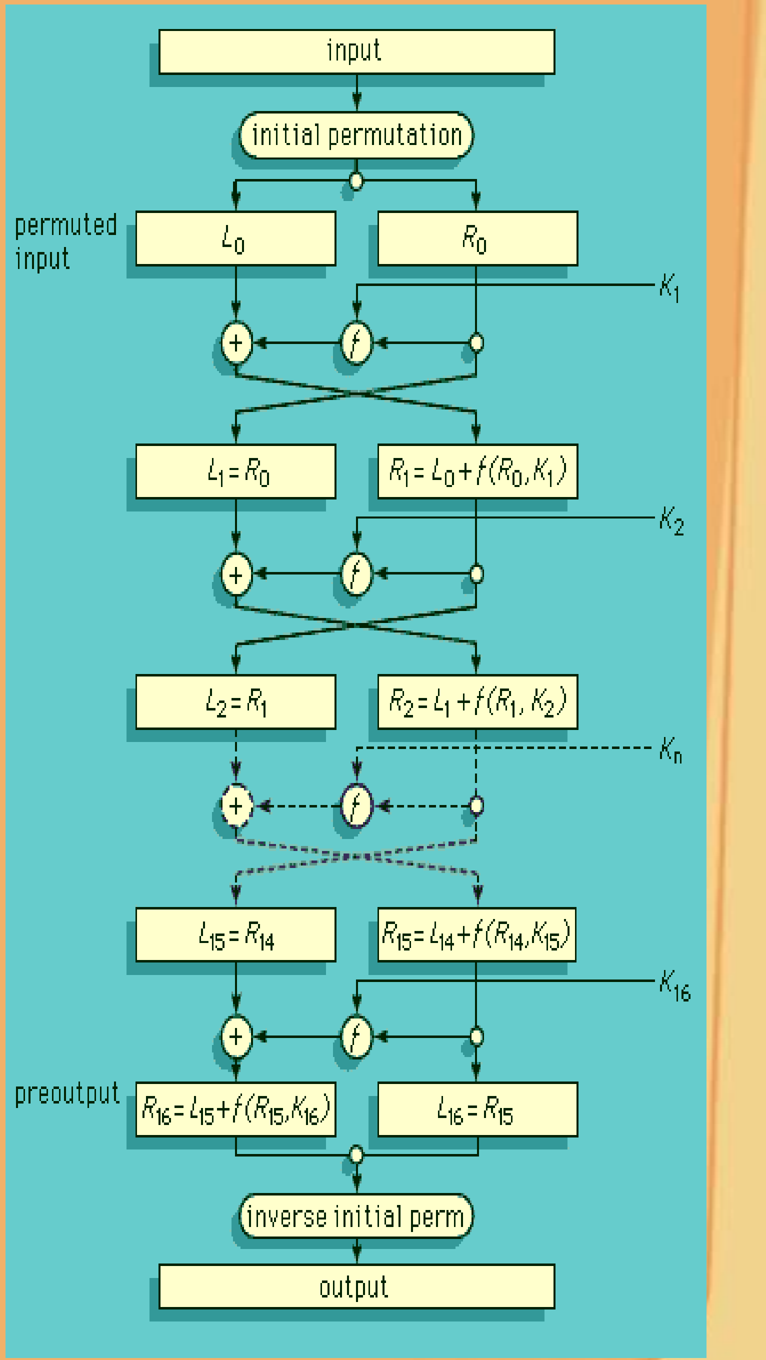
More precisely, on 1st of January 1985…

DES : the glory (1)

- Sound foundations
  (Luby-Rackoff)

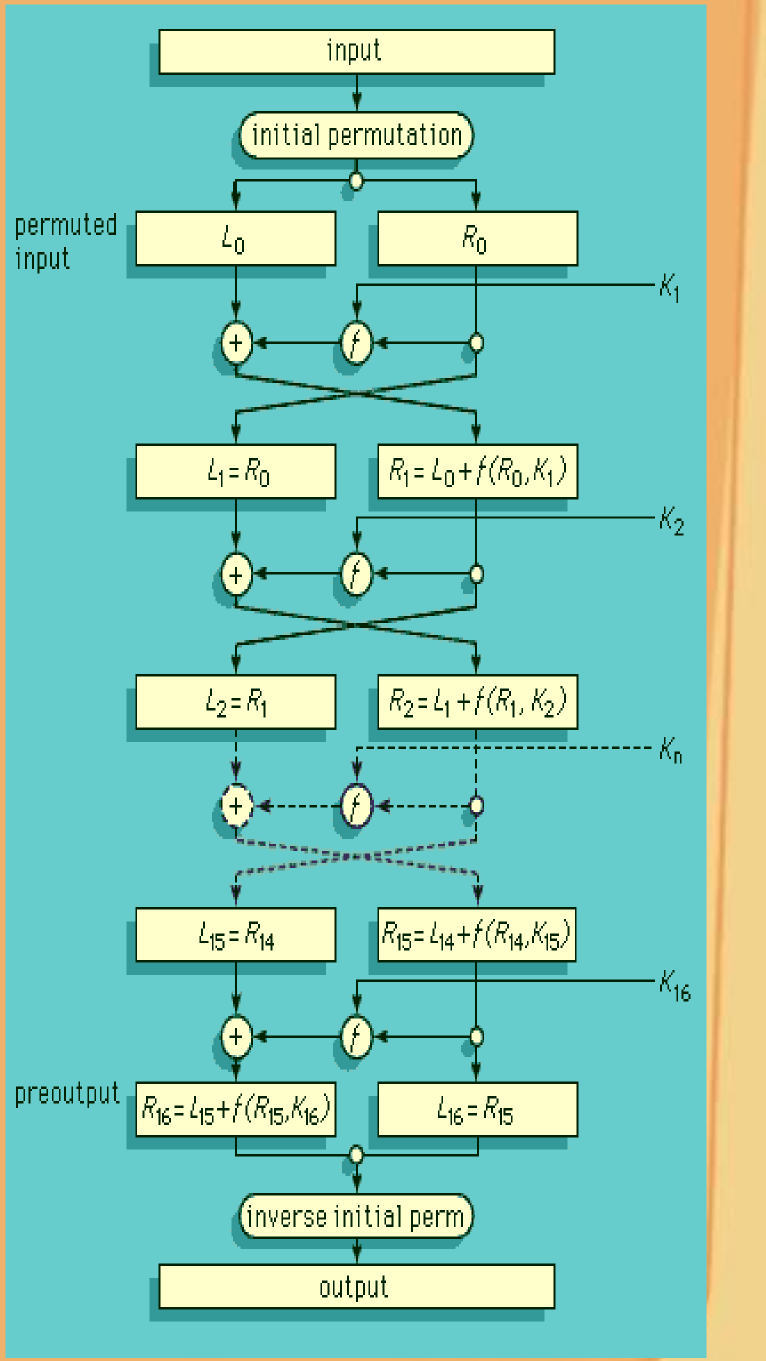
- Exhaustive research believed to be “unfeasible”

- Building block for hashing and MAC-ing
  (Matyas-Meyer, Davies-Price)



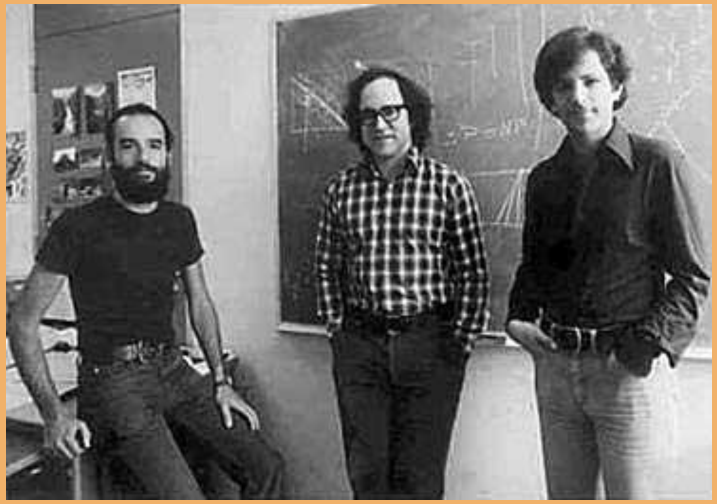
DES : the glory (2)

- Widely implemented and used
  - Software and hardware
  - Banks, credit cards…
- Neither theoretical nor practical concurrent
  - LFSR not trustworthy



RSA : towards the glory (1)

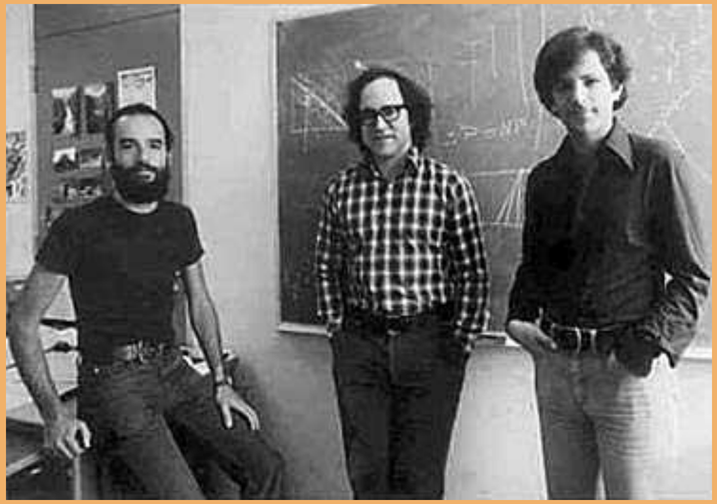
- Factoring algorithms not too destructive (quadratic sieve, Pollard, p–1, p+1,…)
  - ➔ 320 bits are enough



- Many weaknesses are pointed out however :
  - Not only they can be avoided…
  - …but some of them can even be turned into advantages (ex. blind signatures)

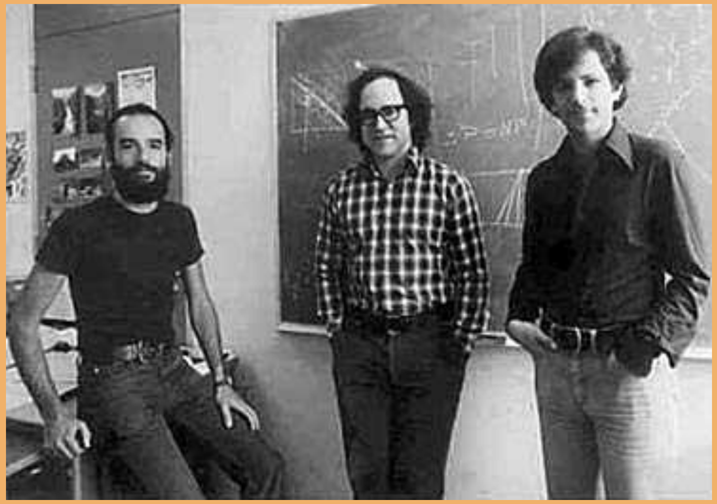
RSA : towards the glory (2)

- The main concurrent (knapsack, Merkle-Hellman) has been (almost) fully broken
  - Shamir
  - then Brickell, Odlyzko,…
  - first and brilliant demonstration of LLL devastating effects in crypto



RSA : towards the glory (3)

- The least significant bit(s) is (are) secure (Abadi-Chor-Goldreich-Goldwasser Hastad-Schnorr)



- Towards massive usage
  - reasonably efficient implementations
  - real applications (ex. static authentication of bank cards in France)

Discrete logarithm

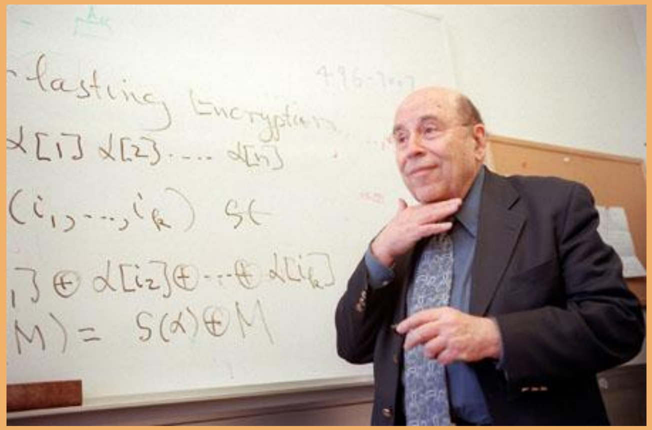
- DL algorithms not too destructive (index-calculus,…)
  - ➔ 320 bits are enough

- Diffie-Hellman very popular

- El-Gamal schemes are rather considered as alternatives of RSA

Other (factoring-based)

- Encryption and Signature
  - *Rabin* (exponent 2 RSA’s variant)
  - *Williams*’ variants



- Signature
  - *OSS* (Ong-Schnorr-Shamir, broken)
  - *E-Sign* (Okamoto-Shiraishi, broken with exponents 2 and 3)
  - *Shamir* (identity-based)

Other (quantum-related)

- Code – based encryption
  - *McEliece*
  - First (alive) PQ-algorithm !

- Quantum – based key exchange
  - Theory (Bennett-Brassard, Crépeau)
  - Practice : not yet

Foundations

- Well advanced (Goldwasser, Goldreich, Levin, Micali, Yao,…)
  - One-way (trapdoor) functions
  - Hardcore bits
  - Indistinguishability
  - Probabilistic encipherment
  - Semantic security
  - PRNG (Blum-Blum-Shub) and PRNF
  - Oblivious transfer
  - Signatures : *next year* (Goldwasser-Micali-Rivest)

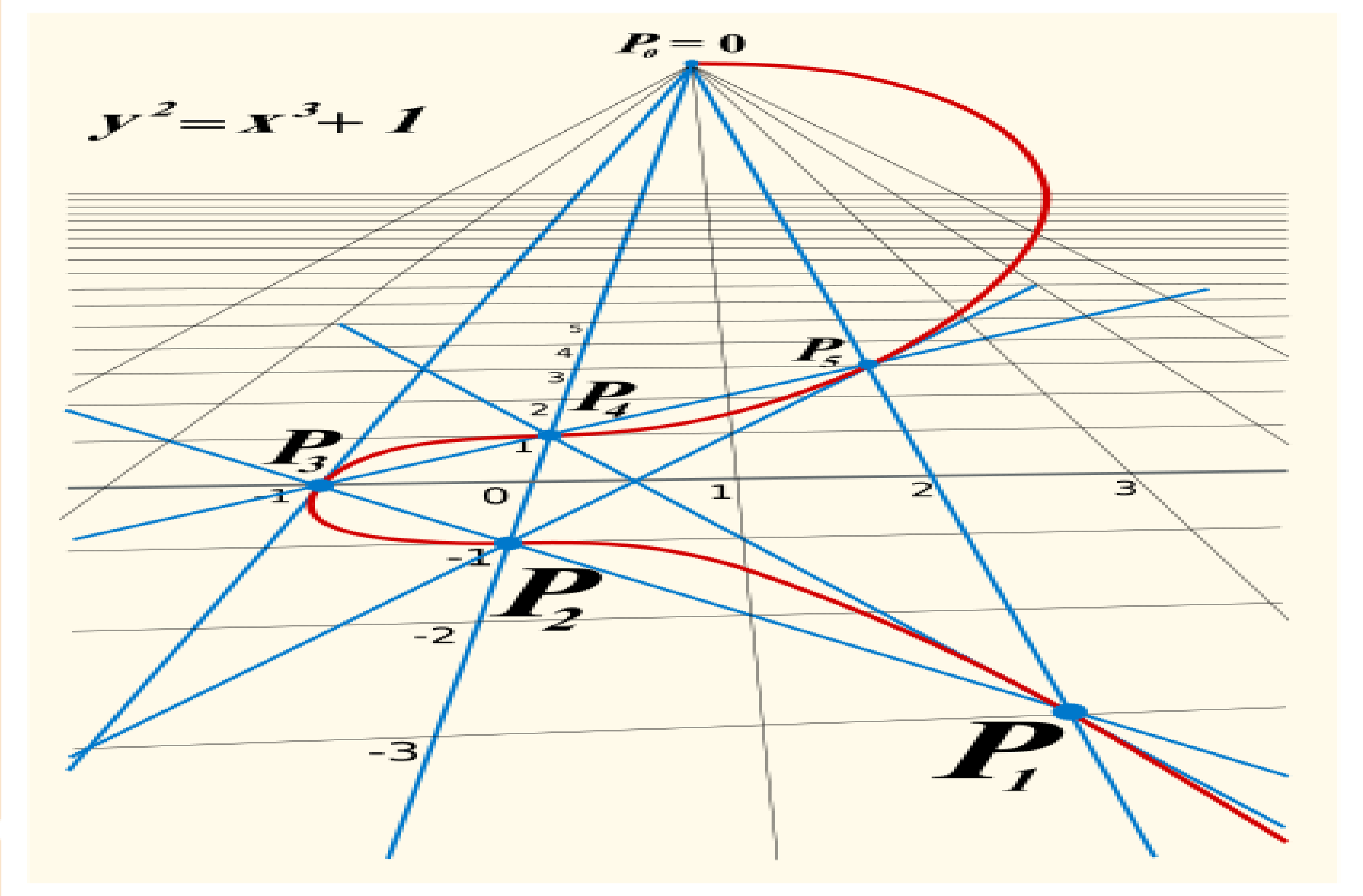
1985 : the **best** millenium since 1977 ?

- Two major breakthroughs
  - **Zero-knowledge** (Goldwasser-Micali-Rackoff)
  - **Elliptic curves** for cryptanalysis (H.W. Lenstra) and cryptography (V. Miller, Koblitz)

- Both worlds meet the year after
  - Primality algorithm (Goldwasser-Kilian)

2. The irruption of elliptic curves (1985 - 1989)

What’s an "elliptic curve" ?



ECM (1)

On 14 February **1985**, H.W. Lenstra, Jr. sends to Henri Cohen :

Cher Henri,

Best regards

Hendrik

ELLIPTIC CURVE FACTORIZATION

This is a new integer factoring method with running time $L^{1+o(1)}$. It detects small prime factors first.

It is derived from the Pollard p -1-method by replacing the multiplicative group by a random elliptic curve.

(...)

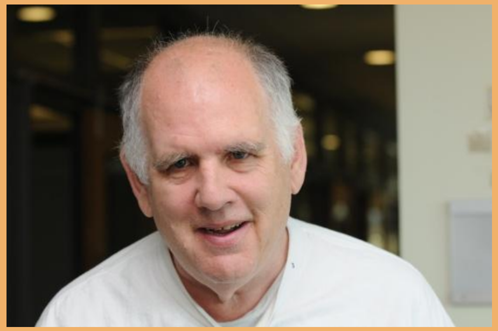
ECM (2)

On 29 June **1985**, John M. Pollard sends to Don Hunter :

> Dear Don,
>
> Here are some opinions about the 'elliptic curve' (EC) method. (...)
>
> The relationship with p+/-1 is as follows. In 'p-1', we get q=p-1 always, so there is no point in making more than one attempt.(...)But in EC, we are likely to get different q each time.(...)
>
> A possible line now is that we do not bother with ANY conditions in RSA ! (I predict that there will be one school that maintains this... I am not sure whether I belong).(...)
>
> *With compliments,* ***John M. Pollard***

ECM (3)

- Lenstra's paper is published at Computational Number Theory Conference, Arcata (CA), August **1985**
- Along with Montgomery's factorization of the 74-digit number $(5^{106}+1)/2$ in two factors, one close to 10^{22}



- Today the record is $\mathbf{10^{381}+1}$, whose smallest prime factor is 67 digits or 222 bits (Dodson, August **2006**)

(1)

- At CRYPTO'**85** Conference, V. Miller suggests to use Diffie-Hellman key agreement protocol with elliptic curves

ECC is born !!!

(2)

Koblitz independently has the same idea while staying in Russia (published in **1987**)

- In **1988**, he extends it to Jacobians of Hyper-Elliptic Curves
  - Crypto’88 then JoC, Vol.1, N°3, 1989 (the first paper about ECC in this revue)
- In **1991**, he will propose practical curves for implementation (known as Koblitz curves)

(3)

- Many people are skeptical
  - « *Too complicated !* »
  - (variant) « *Too much structure !* »
  - Addition of points not faster than modular exponentation
  - No EC-RSA

(4)

- As a result
  - No related paper at **1986** and **1987** at Eurocrypt or Crypto conference
- Even later
  - No treatment of ECC in 2nd edition of Schneier's «Applied cryptography» (**1996 !**)
  - The same in «Handbook of Applied Cryptography» (**1997 !**)

(5)

- Nonetheless :

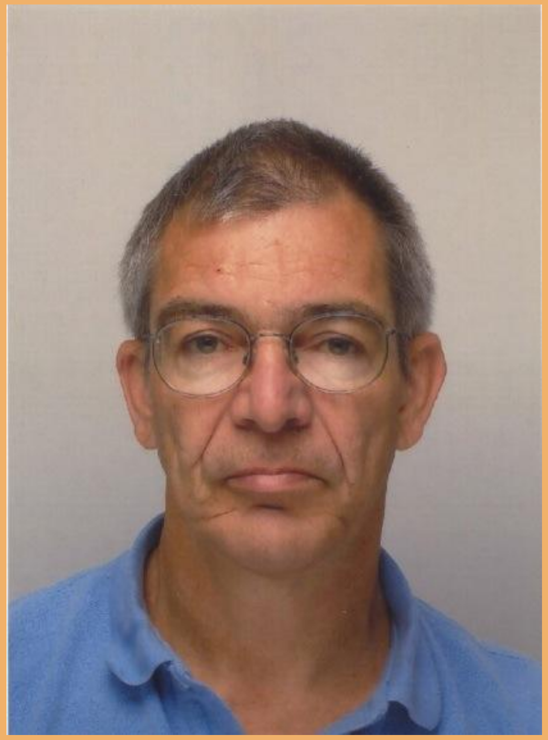
  As soon as **1985**, Agnew, Mullin and Vanstone are visionary and fund

  certicom™

  which today holds 450 patents !!!

Besides, still in **1985**

- Schoof discovers a polynomial algorithm for counting points of $E(F_q)$



- Complexity is initially in $O(\log^{5+\varepsilon} q)$

Primality (1)

- Before 1984, *no efficient primality algorithm is known* (only compositeness algorithms) and nobody knows if there is
- In **1984**, Cohen and Lenstra had proposed the efficient but non-polynomial *Jacobi sums* algorithm
- In **1986,** G. Miller comes with a polynomial (under RH) but non-efficient algorithm

Primality (2)

- In **1986**, by using elliptic curves, Goldwasser and Kilian exhibit a probabilistic algorithm which is both efficient and polynomial (under a reasonable conjecture)

- In **1986** Adleman and Huang skip the conjecture by working on Jacobians of hyper-elliptic curves of genus 2 :
- **PRIMES is in RP !**

Note also…

- **1986** : EC used for PRNG (Kaliski)
- **1987** : Unified addition law (Montgomery)
- **1989** : First chip implementation (Agnew-Mullin-Vanstone)

3. **ECC** incubation period (1990 - 1999)

90’s are (for cryptology in general) years of *maturity*

90's : Maturity years (1)

- Cryptanalysts refine their tools
  - Differential (Biham-Shamir) and linear (Gilbert, Matsui) cryptanalysis
  - NFS algorithm for factoring and DL (BLP after Pollard)
  - Flaws in modes of operation (Preneel-Van Orschoot)
  - Fault and side-channel attacks (Kocher)
  - And plenty of others… (Coppersmith)

- But cryptographers too !
  - Provable security (Bellare – Rogaway, Pointcheval – Stern)

90's : Maturity years (2)

- Symmetric crypto
  - Many new schemes (FEAL, IDEA, RC family,…)
  - Some of them (FEAL,…) do not resist the differential cryptanalysis…nor the linear one !
  - DES does resist and dies in its bed
  - Hash (MD family, SHA-1,…) and MAC
  - Design criteria made rigorous : AES competition is rough

90's : Maturity years (3)

- Asymmetric crypto (*traditional*)
  - Efficient implementations (RSA in a smart card !)
  - DSA (from NIST) fails in superseding RSA
  - RSA and DH conquer the Net
  - Zero-knowledge remains a hot topic

90's : Maturity years (4)

- Asymmetric crypto (*alternative*)
  - Non-traditional (today called Post-Quantum) cryptology emerges
  - PKP-based (Shamir)
  - Code-based (Niederreiter, Stern)
  - Multivariate-based (Patarin, after Matsumoto-Imaï 88)
  - Lattice-based encryption scheme (NTRU, Ajtai)
  - Other more exotic (Courtois, Pointcheval,…)

90's : Maturity years (5)

- New conferences
  - General and IACR-sponsored : Asiacrypt (Auscrypt †)
  - Specialized and IACR-approved : FSE, PKC, CHES
  - Other : ICICS, ISISC, ACISP, ACNS, CTRSA,…

90's : Maturity years (6)

- Standardization
  - ISO (ANSI)
  - IEEE
  - IETF
  - NIST
  - PKCS (RSA), SECG (Certicom)
  - EMV (Europay-Mastercard-Visa)

90’s are for ECC years of *incubation*

90’s and ECC in brief (1)

- Discrete Logarithm problem
  - confirmed as being (apparently) exponential
  - subexponential in one special case

- DSA’s revenge on RSA
  - Research of an analog of RSA essentially failed
  - EC-DSA becomes an “icon” of ECC
  - MQV, an improvement of EC-DH, also.

- Counting points
  - Major improvements of Schoof’s algorithm → SEA

90's and ECC in brief (2)

- Primality
  - Major improvements of Goldwasser-Kilian → ECPP
- Implementation
  - Speeding up computations (possibly on special curves)
  - Software and hardware realizations (including smart cards)
- Standardization
  - IEEE, FIPS, ANSI, ISO, Certicom…

Discrete logarithm problem (1)

Major result

- **1993** : Don’t use supersingular curves !!! (Menezes-Okamoto-Vanstone)
  - First apparition of pairings in crypto (Weil pairing)
  - The second will be in **1994** (Tate pairing with an attack by Frey-Rück)

Discrete logarithm problem (2)

- **1995** : Don’t use anomalous curves !!!
  - Semaev, Satoh-Araki , Smart
- **1998** : Don’t use any elliptic curve at all !!!
  - xedni calculus (Silverman)
  - **1999** : **April fool !!** (Koblitz et al.)

Analog of RSA

- **1991** : EC over Z/nZ (Koyama-Maurer-Okamoto-Vanstone)
- **1993** : Optimisations of RSA-analog (Demytko)
- **1997** : No clear advantage on RSA itself (Joye)

Analog of DSA

- **1992** : EC-DSA (Vanstone)
- **1998** : ISO *and* NIST standards

(later)

- **2000** : IEEE P1363-a
- **2002** : Proof of security in the generic model (Brown)

Analog of DH

- Remember : EC-DH was proposed by Miller in **1985**
- **1995** : MQV (Menezes-Qu-Vanstone)
- **1998** : MQV standardized in IEEE
- **2005** : HMQV

Point counting

- **1990** : GF(2^m) (Koblitz)
- **1995** : SEA (Schoof-Elkies-Atkin)
  - works in $O(\log^{4+\varepsilon} q)$ after many improvements
  - Atkin, Couveignes, Dewaghe, Elkies, Lercier, Morain, Mueller, Schoof,…
- **1997** : GF(2^{155}) (Lercier, Morain)

CM curves and primality

(CM = Complex Multiplication)

- **1991** : Construction on GF(2^m) (Koblitz)
- **1991** : Construction on GF(p) (Morain)
- **1993** : ECPP (Morain-Atkin)
- **2001** : ECPP record (Morain) : $\mathbf{907^{694} + 694^{907}}$

  (2578 decimal digits)

Implementations

- **1992** : Acceleration of scalar multiplication (Meier-Staffelbach)
- **1992** : Software (Harper-Menezes-Vanstone)
- **1993** : Hardware (Menezes-Vanstone)
- **1995** : DH on GF(2^{155}) in software (Schroeppel-Orman-O'Malley-Spatscheck)

Odds and ends

- **1992** : 15 curves (including 5 Koblitz curves) standardized by NIST
- **1997** : first ECC conference in Waterloo
- **1997-8** : Certicom
  - proposes *challenges* and prizes
  - launches *Security Builder Crypto*, first commercial product based on ECC
  - starts own standardization with *SECG*

Personal feeling

- At this time (1999), my feeling is that
  - RSA or DH key length will not *by itself* pose a problem for long
  - Signature production time *might* pose a problem, but which can be solved with ZK schemes (Fiat-Shamir, GQ, Schnorr)
  - Alternative crypto is seriously growing
  - As a consequence, ECC could be the **wasted generation…**

4. The pairing **tornado** (2000 - 2009)

(Sorry : no time for

summarizing 2000’s for

cryptology in general)

Joux's time bomb

- **2000** : Three-party Diffie-Hellman key agreement
  - thanks to Weil pairing
  - $e(aP,bP)^c = e(bP,cP)^a = e(cP,aP)^b = e(P,P)^{abc}$

(see also earlier work by Sahai et al.)

Then Boneh et al.

- **2001** : Identity-based encryption (Boneh-Franklin)
- **2001** : Short signatures (Boneh-Lynn-Sacham)
- **2004** : Short group signatures (Boneh-Boyen)
- Followed by incredibly many other schemes

see Tanja Lange's survey at Asiacrypt 2005

Cryptology fully revisited but… (1)

- Theoretical hardness of underlying problems is questionable
- Many strange assumptions

Cryptology fully revisited but… (2)

- Practical feasibility of pairings is questionable
- ***See Gouvea & Lopez' paper this morning***

Cryptology fully revisited but… (3)

- Is identity-based cryptography useful at all ?
  - (apparently) flexible from user's viewpoint
  - (actually) horrible from key distribution viewpoint

Discrete log problem

- No theoretical breakthrough
- **ECC2p-109** broken in **2002** and **ECC2-109** in **2004** (Monico et al.)
- Next : **ECC2K**-130
  - Believed by european E-Crypt II partners to be breakable in one year
  - ***see Dan Bernstein’s invited talk tomorrow***

Suitable curves/forms (1)

- Another hot topic of 2000's is to find suitables curves and/or representations for
  - *accelerating* computation
  - or *countering* side-channel attacks
  - or both

- To achieve the second goal, unified addition laws are attractive (remember Montgomery's one in **1987**)

Suitable curves/forms (2)

Have been particularly analysed during **2000's**

- Weierstrass form (Brier-Joye)
- Jacobi form (Liardet-Smart)
- Hessian form (Joye-Quisquater)
- Edwards curves (Bernstein-Lange)
- MNT curves (Miyaji-Nakabayashi-Takano)
- BN curves (Barretto-Naehrig)
- etc.

Odds and ends

- Counting points
  - new "p-adic" methods initiated by Satoh in **2000** and Mestre in **2001**
  - Allow to count points of a curve on GF(2^{155}) in less than one second (Lercier-Lubicz)
- HECC : don't use genus more than three (Gaudry)

and last but not least

- Support of ECC by NSA (so-called suite B)

And what about primality ?

PRIMES is in P

(of course !)

Agraval-Kayal-Saxena 2002

(but this has nothing to do with elliptic curves)

5. Applications

DRM

- Microsoft
  - Windows Media Player 2009
- Apple
  - Fair play (in progress)
- MARLIN standard (Open Source, supported by Sony,Toshiba, Samsung, Hitachi, Panasonic,...)
- Liquidplay

Internet

- IPSEC
- S-MIME
- TLS
- OpenSSL and NSS/Mozilla (with Sun support)

RIM

- Blackberry (ECC 256, near to RSA and DH-3072)
- Bought Certicom this year

Smart cards and RFID

- ECC implemented in many smart cards
- Electronic passports (tags with crypto-processors)
  - ECC in option (along with RSA)
  - Germany opted for ECC
- Lightweight (without microprocessors)
  - ≈10000 GE's (not so bad)

6. Two experts’ opinions

For the past 5 years or more there have been **no significant new results** on the elliptic curve discrete logarithm problem (ECDLP). There are at least two possible interpretations of this fact :

Steven Galbraith

1) Everyone has been working on **pairing-based cryptography** and has stopped looking at the ECDLP.

Steven Galbraith

2) Research progress on the ECDLP has **stabilised**, in much the same way that progress on factoring has been stable for the last 15 or more years. This interpretation suggests that the **ECDLP is indeed a hard computational problem.**

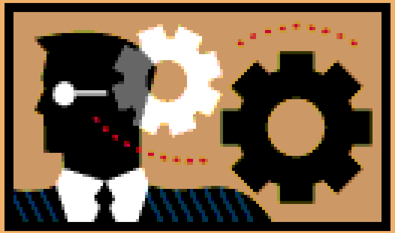
Steven Galbraith

In any case, the lack of any significant progress on the ECDLP in recent years further supports my opinion that **elliptic curve cryptosystems are a secure choice for public key cryptography**

Steven Galbraith

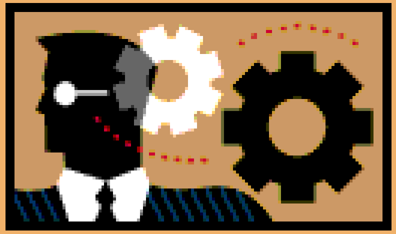
Today, **all is ready for switching from RSA to ECC**. Only missing is the « spark » which will push the industrials to move. In France, the Agency for Security of Information Systems encourages the industrials to use ECC.

Ludovic Flament (transl. M. Girault)



ECC sounds « **modern** » and becomes more and more **familiar** out of the cryptographic community. **I think that the transition will occur within five years.**

Ludovic Flament (transl. M. Girault)



7. Conclusion (?)

- ***Considering that***
  - At the eve of its 25-year birthday, ECC is now (theoretically and practically) very mature
  - ECC is supported by several national agencies
  - ECC has already interfered in several key products, applications or standards
  - ECC is on the starting-blocks, ready for invasion
  - PQ crypto seems to mark time
  - Quantum computers still are long-term technology

- *I undersigned Marc Girault*
  - Declare to be in possession of my mental faculties
  - Request authorization of (partially) reversing my past opinion
  - Am today (15th of December 2009) inclined to believe that

ECC may be the next crypto generation

M. Girault

Nonetheless

Since doubt survives, let me kindly suggest the program committee to invite me again at

INDOCRYPT 2034

- Special credits and/or thanks to
  - *L. Flament*
  - *S. Galbraith*
  - *M. Joye*
  - *F. Laguillaumie*
  - *R. Lercier*
  - *F. Morain*
  - *N. Sendrier*