

Others

Pascal Lafourcade

Université Joseph Fourier, Verimag

9th December 2009

Last Time

- ▶ Diffie-Hellman
- ▶ Security Notions
- ▶ OAEP
- ▶ El Gamal

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

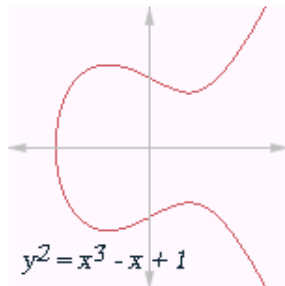
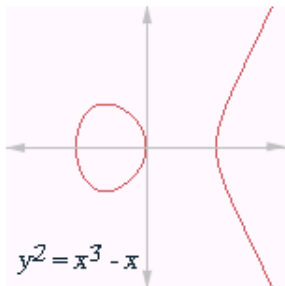
MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

Introduction

$$y^2 = x^3 + ax + b$$



$E(K) = \{(x, y) \text{ such that } y^2 = x^3 + ax + b\}$ plus an extra point
“at infinite”

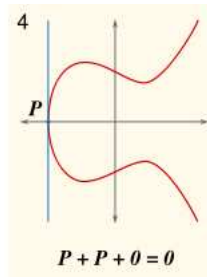
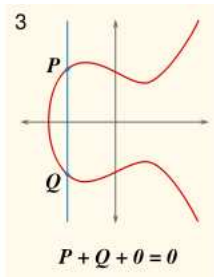
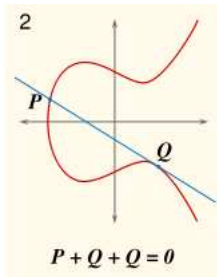
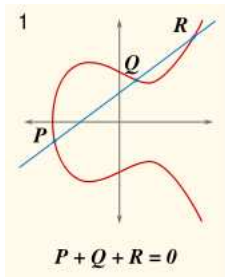
Weierstrass form if $\Delta = -16(4a^3 + 27b^2) \neq 0$ (if K is not of
characteristic 2 or 3).

Laws

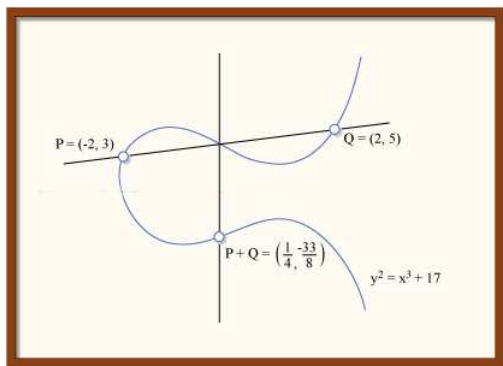
Theorem

- ▶ Addition law on $E(K)$
 - ▶ Associativity: $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$
 - ▶ Commutativity: $P_1 + P_2 = P_2 + P_1$
 - ▶ Neutral element is ∞ : $P + \infty = P$
 - ▶ Inverse: Given P on E , there exists P' on E with $P + P' = \infty$ (usually denoted $-P$)
- ▶ Three aligned points sum to neutral element often denoted zero

Laws



Addition



$$P + R + Q = 0 \Rightarrow R = -(P + Q)$$

$$R + S + 0 = 0 \Rightarrow R = -S$$

“Elliptic Discrete Logarithm”

Hard Problem

Finding k , given P and $Q = kP$. is computationally intractable for large values of k .

Cryptosystem: ECDH

Alice's key is (d_A, Q_A) where $Q_A = d_A G$.

DH like Protocol

1. Alice sends Q_A, G to Bob.
2. Bob computes $k = d_B Q_A$.
3. Bob sends to Alice Q_B
4. Alice computes $k = d_A Q_B$.

The shared key is x_k (the x coordinate of the point).

The number calculated by both parties is equal, because
 $k = d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A = k$.

ECDSA (Digital Signature Algorithm) I

Alice private key d_A and a public key Q_A (where $Q_A = d_A G$).

Signature generation algorithm

1. Calculate $e = \text{HASH}(m)$, where HASH is a cryptographic hash function, such as SHA-1.
2. Select a random integer k from $[1, n - 1]$.
3. Calculate $r = x_1 \pmod n$, where $(x_1, y_1) = kG$.
If $r = 0$, go back to step 2.
4. Calculate $s = k^{-1}(e + rd_A) \pmod n$.
If $s = 0$, go back to step 2.
5. The signature is the pair (r, s) .

ECDSA (Digital Signature Algorithm) II

Signature verification algorithm

1. Verify that r and s are integers in $[1, n - 1]$.
If not, the signature is invalid.
2. Calculate $e = \text{HASH}(m)$, where HASH is the same function used in the signature generation.
3. Calculate $w = s^{-1} \pmod{n}$.
4. Calculate $u_1 = ew \pmod{n}$ and $u_2 = rw \pmod{n}$.
5. Calculate $(x_1, y_1) = u_1G + u_2Q_A$.
6. The signature is valid if $r = x_1 \pmod{n}$, invalid otherwise.

ECDSA (Digital Signature Algorithm)

$$s = k^{-1}(e + rd_A) \pmod{n}$$

Hence

$$k = s^{-1}(e + rd_A) \pmod{n} = w(e + rd_A) = we + wrd_A = u_1 + u_2d_A$$

since $w = s^{-1}$, $u_1 = we$ and $u_2 = wr$

$$(x_1, y_1) = u_1G + u_2Q_A$$

$$\text{Hence } (x_1, y_1) = u_1G + u_2d_AG = kG$$

$$\text{because } Q_A = d_AG \text{ and } k = u_1 + u_2d_A$$

We conclude that $r = x_1 \pmod{n}$ by construction.

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

Public Key History

- ▶ Diffie-Hellman 1976
- ▶ Rivest-Shamir-Adleman RSA 1978
- ▶ El Gamal 1985
- ▶ ECC by Neal Koblitz and Victor S. Miller in 1985.
- ▶ ...

Post-Quantum Computer Birth

The New York Times

April 26, 2077

RSA Broken

All Internet secured web sites are closed due to lack of security. Quantum computer produces a revolution in Internet Security. Most of the considered Hard problems are any more Hard, specially factoring integers becomes a problem solvable in polynomial time. Breaking these would have significant ramifications for electronic privacy and security.

Idea: Break Factorization with Quantum Computer

Definition

The order of $a \in Z_N^*$ modulo N is the smallest integer $r > 0$ such that $a^r = 1 \pmod{N}$

For example, order of 4 mod 7 is 3: $4^1 = 4$, $4^2 = 16 = 2$,
 $4^3 = 64 = 1 \pmod{7}$.

Main Reduction

Factoring reduces to order-finding.

Reduction

- ▶ If $a^r = 1 \pmod{N}$, then N divides $a^r - 1$.
- ▶ If r even, $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$.
- ▶ If N is product of two or more primes, $\gcd(a^{r/2} - 1, N)$ is a nontrivial factor of N with probability at least $1/2$.

Factorization: Shor Algorithm 1994

Idea: Reduce factoring to period-finding

Shor Algorithm

Repeat $O(\log n)$ times:

- ▶ Generate random $a \in \{1, \dots, N - 1\}$;
- ▶ Check if $(a, N) = 1$;
- ▶ $r = \text{order}(a)$;
- ▶ If r even, check $(a^{r/2} - 1, N)$.

Using Simon's algorithm then period finding with a quantum computer is "easy" (1994)

What is dead?

- ▶ RSA: Dead.
- ▶ DSA: Dead.
- ▶ ECDSA: Dead.
- ▶ ECC in general: Dead.
- ▶ HECC in general: Dead.
- ▶ BuchmannWilliams: Dead.
- ▶ Class groups in general: Dead.

What are the alternatives?

- ▶ Secret-key cryptography. Example: 1998 DaemenRijmen Rijndael cipher, AES.
- ▶ Hash-based cryptography. Example: 1979 Merkle hash-tree public-key signature system.
- ▶ Lattice-based cryptography. Example: 1998 NTRU.
- ▶ Multivariate-quadratic-equations cryptography. Example: 1996 Patarin HFE Public-key signature system.
- ▶ Code-based cryptography. Example: 1978 McEliece hidden-Goppa-code public-key encryption system.

Post-Quantum Cryptography

Workshop in 2006, 2008 and PQCrypto 2010:

The Third International Workshop on Post-Quantum Cryptography

Darmstadt, Germany, May 25-28, 2010

<http://pqc2010.cased.de/>

- ▶ Code-based cryptosystems
- ▶ MPKC, or multivariate public key cryptography
- ▶ Hash-based cryptography
- ▶ Lattice-based cryptosystems

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

Quantum Channel

- ▶ A quantum communication channel which allows quantum states to be transmitted: In the case of photons this channel is generally either an optical fibre or simply free space.
- ▶ In addition they communicate via a public classical channel, for example using radio waves or the internet.
- ▶ Neither of these channels need to be secure; the protocol is designed with the assumption that an eavesdropper (referred to as Eve) can interfere in any way with both.

Quantum

Using photon polarization states to transmit the information.



- ▶ No cloning theorem
- ▶ Reading a photon will change his state.

BB84 is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984.

BB84 (I)

Alice sends photons with one of the four polarizations, which she chooses at random.



For each photon, Bob chooses at random the type of measurement: either the rectilinear type (+) or the diagonal type (X).



Bob records the result of his measurements but keeps it a secret.

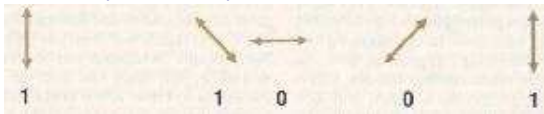


BB84 (II)

After the transmission, Bob tells Alice the measurement types he used (but not his results) and Alice tells him which were correct for the photons she sent. This exchange may be overheard.



Alice and Bob keep all cases in which Bob should have measured the correct polarization. These cases are then translated into bits (1s and 0s) to define the key.



Intruder Detection

- ▶ Alice and Bob compare a subset of remaining bit strings.
- ▶ Eavesdropper should have introduced error on Bob's side
- ▶ If more than p bits differ they abort the key and try again

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

NTRU Public Key Cryptosystem

- ▶ Designed in 1996 by Joseph H. Silverman, Jeffrey Hoffstein, Jill Pipher and Daniel Lieman, at Brown University.
- ▶ Ntru is short for N -th degree truncated polynomial ring, or in mathematical notation $R[x]/(x^N - 1)$. ("Number Theorists aRe Us" and "Number Theory Research Unit")

Base ring $\mathbb{Z}/p\mathbb{Z}$

It consists of all truncated polynomials of degree $N - 1$ having integer coefficients:

$$a = a_0 + a_1X + a_2X^2 + a_3X^3 + \dots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$$

Multiplication is more-or-less as usual, except that X^N is replaced by 1, X^{N+1} is replaced by X , X^{N+2} is replaced by X^2 , and so on.

NTRU: Parameters

Parameters

- ▶ N : the polynomials in the truncated polynomial ring have degree $N-1$.
- ▶ q : large modulus, usually, the coefficients of the truncated polynomials will be reduced mod q .
- ▶ p : small modulus. As the final step in decryption, the coefficients of the message are reduced mod p .

$\gcd(p, q) = 1$	N	q	p
<i>ModerateSecurity</i>	167	128	3
<i>StandardSecurity</i>	251	128	3
<i>HighSecurity</i>	347	128	3
<i>HighestSecurity</i>	503	256	3

NTRU: Key Generation

- ▶ Security parameters N, p, q
- ▶ Two "small" random polynomials f and g in R .
- ▶ Compute the inverse f_q of f modulo q and the inverse f_p of f modulo p :
 $f * f_q = 1 \pmod{q}$ and $f * f_p = 1 \pmod{p}$.
- ▶ Private key : (f, f_p)
- ▶ Public key : $h = p * f_q * g \pmod{q}$

In a small polynomial, the coefficients are much smaller than q .

NTRU: Cryptosystem

Encryption

Let m be a small polynomial mod q of the plain text and r be a random small polynomial.

$$e = r * h + m \pmod{q}$$

Decryption

- ▶ $a = f * e \pmod{q} = f * (r * h + m) \pmod{q}$
 $= f * (r * pf_q * g + m) \pmod{q}$ since $h = pf_q * g \pmod{q}$
 $= pr * g + f * m \pmod{q}$ since $f * f_q = 1 \pmod{q}$
- ▶ $b = a \pmod{p} = f * m \pmod{p}$
- ▶ $f_p * b = f_p * f * m = m \pmod{p}$

25 time faster than RSA.

NTRU: Security

- ▶ Jaulmes and Joux presented at Crypto '00 a simple chosen-ciphertext attack against NTRU as originally described.
- ▶ This led Hoffstein and Silverman to propose three encryption padding schemes more or less based on previous work by Fujisaki and Okamoto on strengthening encryption schemes. It was claimed that these three padding schemes made NTRU secure against adaptive chosen-ciphertext attacks (IND-CCA) in the random oracle model.
- ▶ “Analysis and Improvements of NTRU Encryption Paddings”. Phong Nguyen and David Pointcheval In CRYPTO '02. It turns out that the first one is not even semantically secure (IND-CPA). The second and third ones can be proven IND-CCA-secure in the random oracle model, under however rather unusual assumptions.

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

Problem

Given the following set of equations E

$$y_1 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_5 + x_3x_4 + x_3x_5$$

$$y_2 = x_1x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_2x_5 + x_3x_4 + x_4x_5$$

$$y_3 = x_1x_2 + x_1x_4 + x_2x_3 + x_4 + x_5$$

$$y_4 = x_1x_5 + x_3x_5 + x_2x_3 + x_2x_4 + x_3x_4$$

$$y_5 = x_1x_2 + x_1x_3 + x_1x_5 + x_2x_5 + x_4x_5$$

From x_i and E it is easy to compute y_i .

Given values of y_i and E it is hard to get x_i . Until now, only exhaustive method is known to solve this problem.

Cryptography based on MQ

Some particular systems are easy to solve (using for instance Gauss Elimination)

Using a one-to-one transformation we transform such system to a general one. Knowing this transformation is similar to knowing the trapdoor like in RSA knowing p and q of n .

Existing MQ Schemes

- ▶ UOV: Unbalanced Oil and Vinegar 1997 by J. Patarin
- ▶ STS: Sepwise Triangular Systems 1993 Coppersmith, Stern, Vaudenay
- ▶ MIA: Tsutomu Matsumoto and Ideki Imai 1985
- ▶ HFE: Hidden Field Equations J. Patarin 1996
- ▶ QUARTZ (New)
- ▶ SFLASH (New)

Unbalanced Oil and Vinegar

Idea

Oil variables h_i and Vinegar variables v_i .

Quadratic variables are composed only of:

- ▶ $v_i v_j$
- ▶ $v_i h_j$

But NEVER of $h_i h_j$

Using Gauss elimination it is easy to solve the original problem.

This system F is hidden by linear bijective transformations P and S that constitute the private key $(PoFoS)$.

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

What are error-correcting codes?

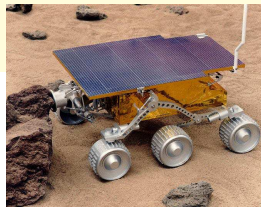
Propose to correct errors when communication is noisy.

- ▶ Add redundancy to transmitted information.
- ▶ Correct corrupted data, if enough information is received.

Stronger than Checksum or CRC (only detect problem)

Applications

- ▶ DVD, CD
- ▶ Cell-phones
- ▶ Radio transmissions
- ▶ Mars Pathfinder ...



Linear Codes

Oldest family of corrector codes:

- ▶ Block Codes
- ▶ Defined by a Generator Matrix ($c = m.G$):

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

- ▶ 00 → 0000 | 10 → 10110
- ▶ 01 → 01011 | 11 → 11101

Example

$$'a' = 97 = 0110001$$

$$01|10|00|01 \rightarrow 01011|10110|00000|01011$$

Terminology

- ▶ The code C is vectorial space generated by G of size $k \times n$.
- ▶ Dimension k is the dimension of C .
- ▶ The length n of a code is the length of a code word, i.e. the number of columns of G .
- ▶ Hamming weight of a word is the number of non zero bits.
- ▶ Minimal distance d is minimal Hamming distance between two words.
- ▶ The ratio $r = \frac{k}{n}$ is the transmission rate.

Decoding

- ▶ Transmitter sends $c = mG$, but receiver gets $c' = c + e$
- ▶ Decoding is recovering c from c' .
- ▶ We denote $[n, k, d]$ a code of length n , dimension k and minimal distance d .

Example : Repetition Code

- ▶ Each bit is repeated d times
- ▶ 10100 is coded by 111000111000000
- ▶ This code is $[d, 1, d]$ with $\frac{1}{d}$ transmission rate (too small).

Only used for very noisy channel.

Terminology II

Parity check matrix

- ▶ H is orthogonal matrix to G of size $(n - k) \times n$
- ▶ $c \in C$ iff $Hc = 0$

Syndrome of error

$$S = Hc' = H(c + e) = Hc + He = He$$

Hard Problems

Syndrome decoding is NP-complet [Berlekamp, McEliece, van Tilborg 1978]

- ▶ Input: Matrix H , syndrome S and a weight w .
- ▶ Problem: Find e of weight w with $He^t = S$.

Parametrized Bounded Decoding is NP-complet for all f raisonnable

- ▶ Input: Matrix H of size $r \times n$, syndrome S .
- ▶ Problem: Find e of weight $f(r, n)$ with $He^t = S$.

Example: Hamming code

It is a $[2^l - 1, 2^l - 1 - l, 3]$ code. For $l = 3$ it is $[7, 4, 3]$ code

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Minimal distance is 3 then no code words of weight 1 or 2
Can correct exactly one error.

Other Codes: Reed-Solomon 1960, V.D. Goppa 1970, McEliece 1978.

Mc Eliece Public key Cryptosystem

Using Goppa Code.

Key Generation

- ▶ Generate a Goppa code $T(g, L)$ and his generator matrix G
- ▶ Compute $G' = QGP$, G' s the pubic key, Q and P constitue the private key.

Encryption

- ▶ Compute $c = mG'$ and generate error e of weight t
- ▶ Transmit $c + e$

Mc Eliece Public key Cryptosystem

Decryption of $c + e$ (valid)

- ▶ $c' = (c + e)P^{-1} = mQGPP^{-1} + eP^{-1} = (mQ)G + e'$
- ▶ Decode e' in $T(g, l)$ and find mQ
- ▶ Use Q^{-1} to find m

Variant proposed by Niederreiter in 1986.

Outline

Elliptic Curves

Post Quantum Cryptography

Quantum Cryptography

Lattices (NTRU)

MQ (Multivariable Quadratic)

Codes (McEliece)

Conclusion

Summary of our 4 Lectures

- ▶ Classical Symmetric and Asymmetric Encryption
 - ▶ DES, AES, IDEA ...
 - ▶ RSA, ElGamal, EC
- ▶ Hash functions (SHA-1, MD5 ...)
- ▶ Security Notions
 - ▶ OW
 - ▶ IND-CPA, IND-CCA1 and IND-CCA2.
 - ▶ NM-CPA, NM-CCA1 and NM-CCA2.
- ▶ Other encryption primitives
 - ▶ Quantum cryptography BB84
 - ▶ NTRU
 - ▶ MQ
 - ▶ Code based crypto-system

Applications ... using protocols for Security Policy, Secure communication, Mobile Phone, E-Banking, E-vote, E-Cash, E-commerce ...

Exercise

Find an attack on CBC encryption mode with counter IV against IND-CPA.

Cipher-block chaining (CBC)

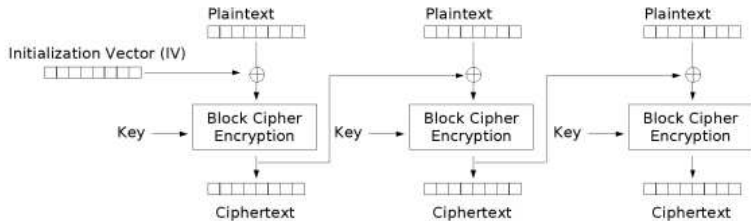
If the first block has index 1, the mathematical formula for CBC encryption is

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

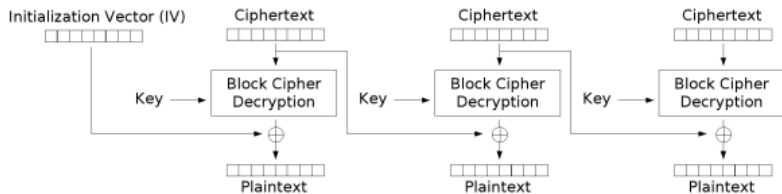
while the mathematical formula for CBC decryption is

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$$

CBC has been the most commonly used mode of operation.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Thank you for your attention

Questions ?