Introduction to Cryptology

Lecture-13
Public-Key Cryptography
Knapsack one-way function, Elliptic-Curve System

17.05.2023, v48

Outlines

- Historical Overview !
- Knapsack One Way Function (OWF)
- Elliptic Curve Cryptography
- Summary of OWF's

Knapsack Public-Key Crypto-System 1978

Ralph Merkle
Berkeley → Stanford University

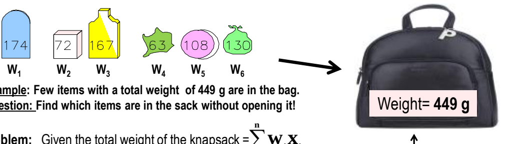
Published similar concept to Diffie-Hellmann system as a student at Berkeley University
"Secure communications over insecure channels"
Commun ACM, April 1978 (Berkeley Univ.), submitted Aug. 1975

Martin Hellman
Stanford University

Based on: **Knapsack problem as a One-Way Function**

Knapsack Problem as a One-Way Function*

Example: Given the following 6 items, each with its own weight:



Example: Few items with a total weight of 449 g are in the bag.
Question: Find which items are in the sack without opening it!

Weight = $\sum_{i=1}^{n} W_i X_i$

Problem: Given the total weight of the knapsack = $\sum_{i=1}^{n} W_i X_i$

Find the binary vector X = [x_1, x_2 ......], where x_i = {0,1}

Solution : X = [1 0 1 0 1 0]

- There is no algorithm known for finding X !!! (in the public literature

- The solution is easy if the knapsack is **superincreasing**

A Knapsack is a superincreasing one : if any W_i is greater than the sum of all other smaller weights.

Example: the binary weight system $2^0, 2^1, 2^2 \ldots 2^{n-1}$ = 1, 2, 4, 8, 16 … are used to represent an integer of n-bits

* Ref. J. Massey

Merkle-Hellmann Crypto System (1978)*

(Broken by Shamir 1984)

1. Multiply each weight by u= 113 in Z_{199}

secret key is u = (m, u) = (199,113)
Where gcd (199,113)=1

2	5	8	17	35	71	select an easy knapsack
27	167	108	130	174	63	Convert to hard knapsack

2. Permute locations and publish → 174 27 167 63 108 130 published knapsack

Public key

Encrypt: X = [1 0 1 0 1 0] Plaintext

Y = 174 + 167 + 108 = **449** Cryptogram

118 = 113^{-1} in Z_{199}

Decrypt : Y′ = u^{-1} . Y = 118 . **449** mod 199 = **48** in Z_{199}

from **Y′ =48** find x′ = [0 1 1 0 1 0] in the easy knapsack

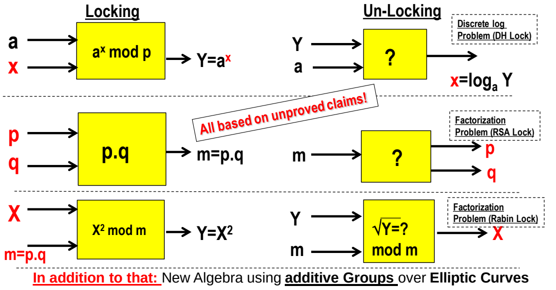
permute to get the original message **X = [1 0 1 0 1 0]**

Conditions : gcd (u , m) = 1 and m > Σ W_i

* source. J. Massey

Summary: Widely Used Claimed One-Way Functions (OWF) /(Locks) are from Number Theory

Summary of "still claimed" ***One-way Functions (OWF) we introduced so far***



In addition to that: New Algebra using **additive Groups** over **Elliptic Curves**

Elliptic Curve Based Crypto-systems

Background: We introduced so far using the **multiplicative cyclic group** of the exponents of a primitive element for building a system in which the discrete logarithm is not computable

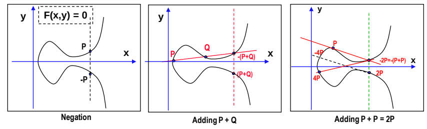
α was selected as a ***primitive element*** in GF(p) or GF(2^m) having the maximum possible multiplicative order in GF.

Thus $\{\alpha^1 \;\; \alpha^2 \;\; \alpha^3 \; .... \; \alpha^n = 1\}$ is a **cyclic group including all non-zero field elements**.

Claimed unsolved problem: If we know α^i, we do not know how to find i without exhaustive search (discrete logarithm problem).
The basic arithmetic used was modular multiplication (or exponentiation modulo p or mod p(x)).

Question:
Are there other similar groups offering less complex arithmetic with similar cryptographic properties?
The answer is yes with the following proposed algebra:
An **additive groups** is defined by addition in in an ***elliptic curve*** system over GF(p) or GF(2^m).
was suggested independently by Neal Koblitz and Victor S. Miller n 1985.

Elliptic Curve: Other Additive Group for Cryptosystems



An Additive Group of order n was found using a primitive point **P having the large additive order n which can generate a large group**. That is

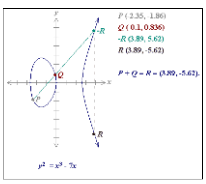
P + P + P ....+ P = **n P** = e where e is the neutral element of the group.

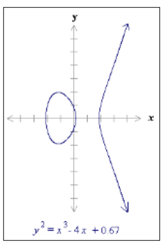
n-times (n is very large)

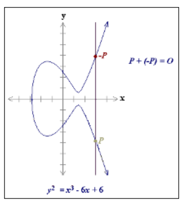
In this group it is still claimed that we do not know how to divide!.
Example: if we know that Y = 5 P and we know P and Y, we do not know how to find 5 = Y/P.

Cryptographic significance: If a secret key K is multiplied by a known element P to get Y=KP.
If Y is publish with P, K is not possible to be found as it is not known how to compute K= Y/P .
This is equivalent to the discreet logarithm computation problem. The used algebra is over GF(p) or GF(2^m)

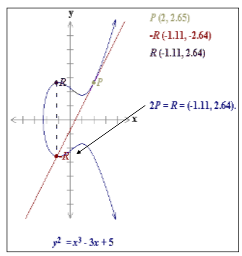
EC- Examples in real fields 1/2

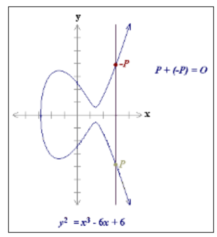






EC- Examples in real fields 2/2





Adding the points P and -P

The line through P and -P is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and -P cannot be added as previously to get the "neutral point" 0. Therefore, the elliptic curve group includes the neutral element point at infinity 0. By definition, P + (-P) = 0. As a result of this equation, P + 0 = P is in the elliptic curve group. 0 is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity.

Standardized Elliptic Curve Algebra over GF (IEEE 1363/D8)

Used Koblitz Elliptic Curve equation (curves):

$$y^2 + xy = x^3 + a \cdot x^2 + b$$

Addition in Elliptic Curve over GF (2^n)
(n should be prime for higher security)
x, y are elements in GF(2^n)

Adding two point: P + Q

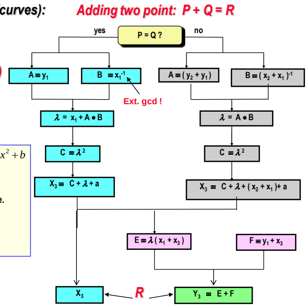
E is an Elliptic Curve (Koblitz) : $y^2 + xy = x^3 + a \cdot x^2 + b$
with $\mathbf{b} \neq 0$ (IEEE 1363/D8, 10.1999)

P = (x_1,y_1) and Q = (x_2,y_2) are two points on the curve.

The sum is R= P ⊕ Q , where R= (x_3,y_3) is computed according to the right flow chart

If P = (x, y)
then -P = (x, -y)

Adding two point: P + Q = R

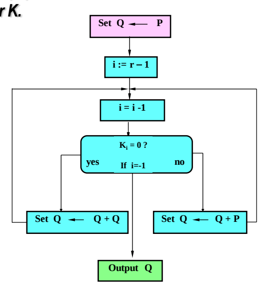


Multiplication in Elliptic Curve over GF (2^n)

How to multiply a point P by the scalar K.
Computing Q = K . P

Double & Add technique

1. Convert K into the binary form:
   K = ($k_r k_{r-1}$...... $k_1 k_0$) with k_r (MSB) = 1;
2. Set : Q ⟵ P
3. for *i* from *r – 1* down to 0 do
   a) Set: Q ⟵ Q + Q
   b) If k_i = 1, then Set: Q ⟵ Q + P
4. Output Q.



Double & Add Multiplication Algorithm

Why Elliptic Curve Cryptosystems ECC ?

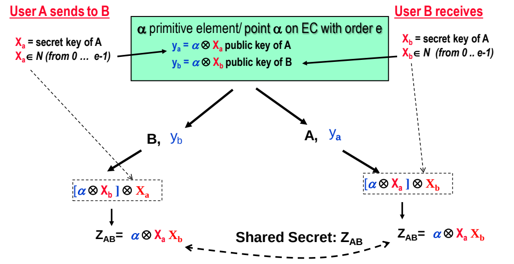
Key length and security motivations

Claimed key length for RSA, DSA and ECC for similar security level

Symmetric scheme (key size in bits)	ECC-based scheme (size of n in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

ECC system is still claimed to exhibit higher security level for the same key length!

Conventional Diffie-Hellman Public Key Distribution System Using Additive Groups over Elliptic Curves

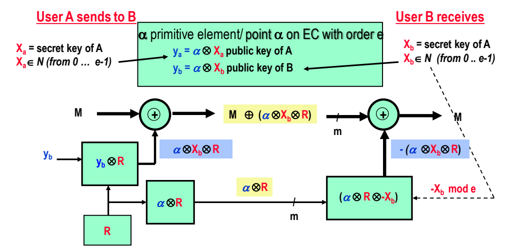


El-Gamal Crypto-System

Using Additive Groups over Elliptic Curves (EC) Algebra Over GF (2^n) or GF(p)

Neal Koblitz[1] and Victor S. Miller[2] in 1985

System mapping: Substitute addition instead of multiplication and multiplication instead of exponentiation! Same can be done for any discrete log based cryptosystem like Diffie-Helman tec. ..



Random Generator creates R = 0 … e-1, a new R is needed for every message (p is α 's order)

Sample ECC NIST Standards

ECC Koblitz Curve: $E: y^2 + x\,y = x^3 + x^2 + b$, $E_a: y^2 + x\,y = x^3 + a\,x^2 + 1$

Over GF(p) special primes p

Curve name	Bits in p
ANSSI FRP256v1	256
BN(2, 254)	254
brainpoolP256t1	256
Curve1174	251
Curve25519	255
Curve383187	383
E-222	222
E-382	382
E-521	521
Ed448	448
M-211	221
M-383	383
M-511	511
NIST P-224	224
NIST P-256	256
NIST P-384	384
secp256k1	256

Over GF(2^n) n is selected as a prime integer!

Irreducible Polynomial	Bits
$p(t) = t^{163} + t^7 + t + t^3 + 1$	163
$p(t) = t^{233} + t^{74} + 1$ (Trinomial)	233
$p(t) = t^{283} + t^{12} + t^7 + t^5 + 1$	283
$p(t) = t^{409} + t^{87} + 1$ (Trinomial)	409