**Edwards Curve:**

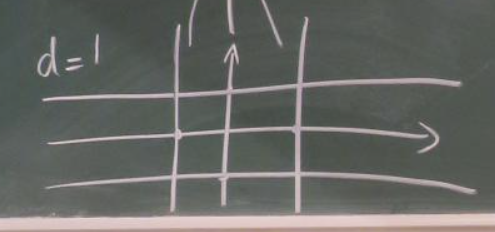
 

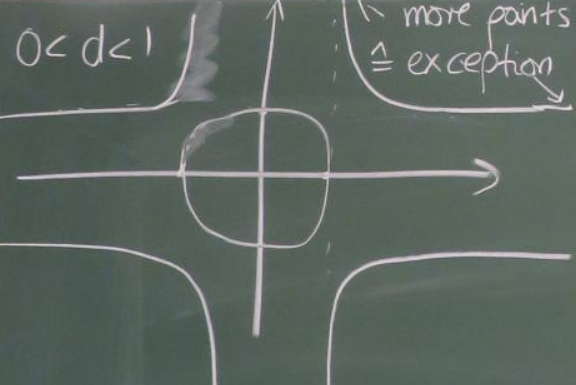
(x1,y1)+(x2,y2)=

neutral element (0,1) and -(x,y)=(-x,y), (0,-1) has order 2, (±1,0) has order 4.

There are no exceptions over Fp for p>2 and d a non-square.



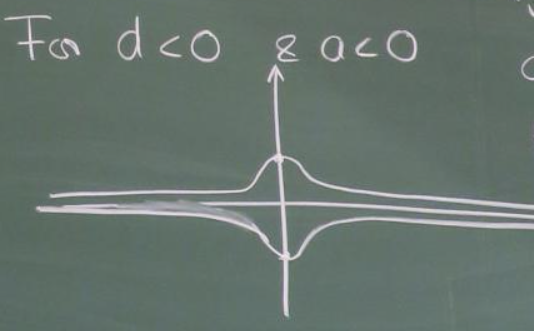


when , the points (±b,±b), exist, with order 8.

**Twisted Edwards Curve:**



. (x1,y1)+(x2,y2)=



**Short Weierstrass Curve:**

,

Adding:

(x1,y1)+(x2,y2)=(x,y)



Doubling:

2(x1,y1) =(x,y)



**Special:**



**Montgomery curve**



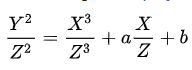
Adding:



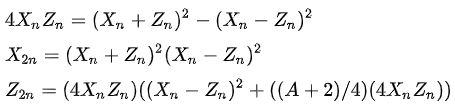


Doubling:



(X:Y:Z) x=X/Z and y=Y/Z





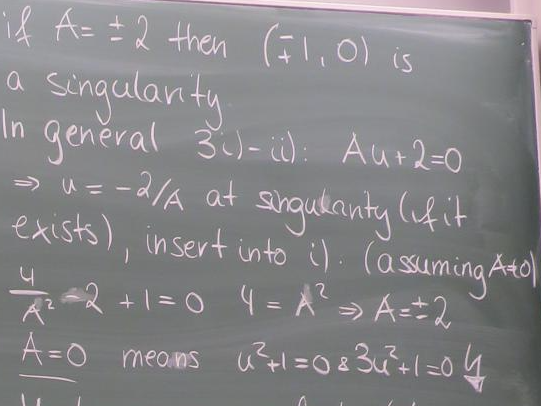
**Twisted Edwards** curve are biracially equivalent to **Montgomery** curve:

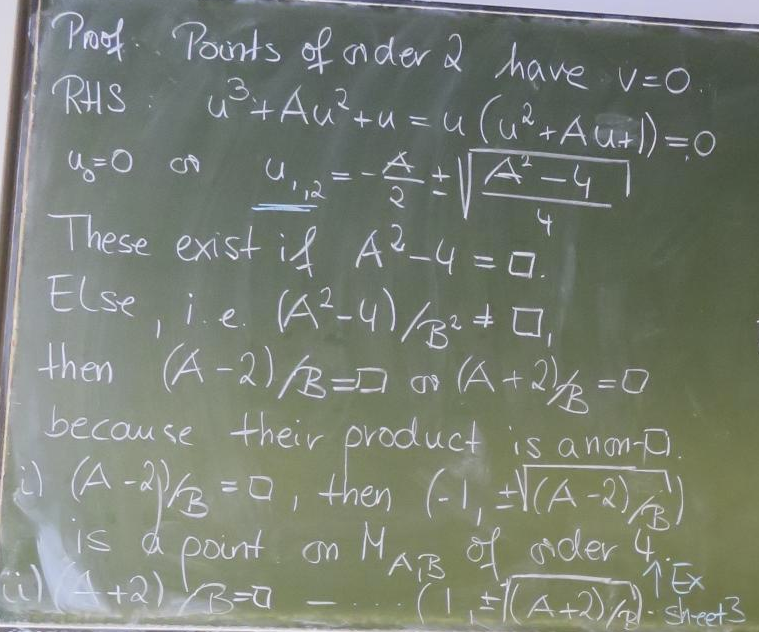
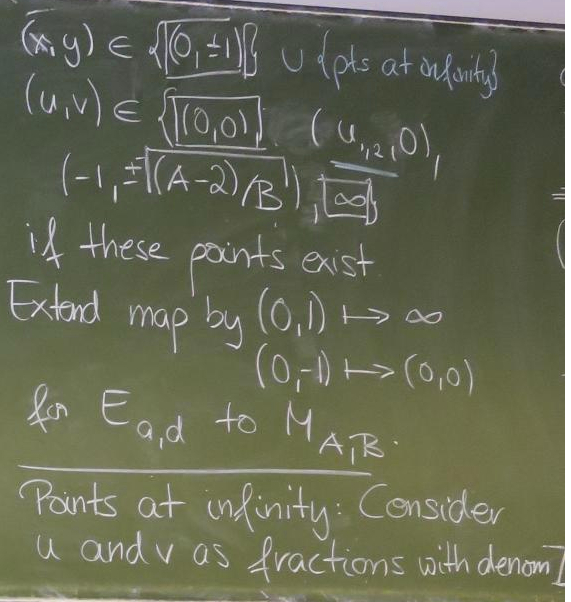
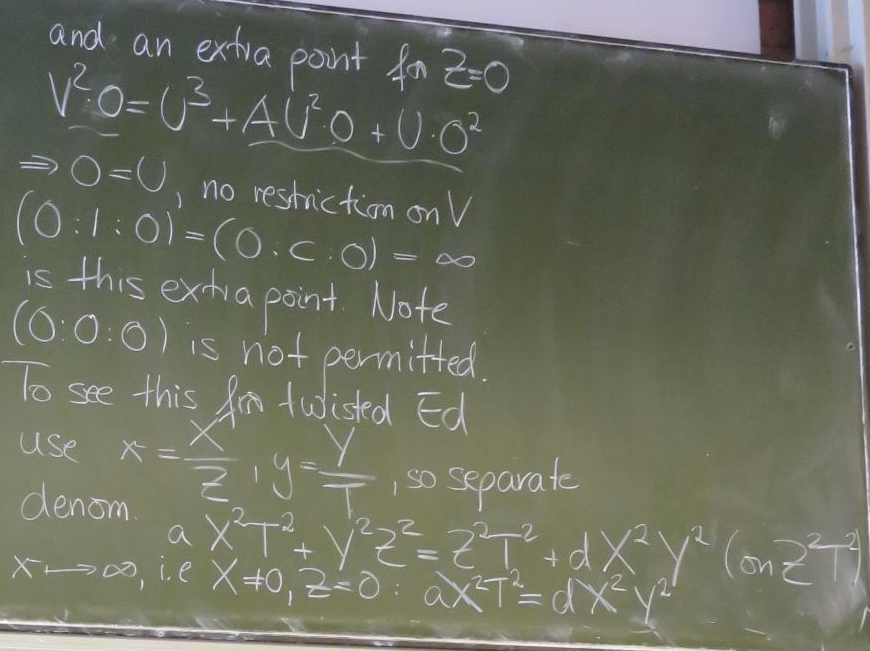
(x,y) to (u,v)

 , 

If the characteristic of the field is not 2 or 3 then any elliptic curve in long Weierstrass form is isomorphic to one in short Weierstrass form.

the curve is nonsingular if A is not 2 or -2



**Preimage resistance (PRE)**:

Given y∈H({0,1}∗) finding x∈{0,1}∗ with H(x)=y is hard.

**Second preimage resistance (SPR):**

Given x∈{0,1}∗ finding x’∈{0,1}∗ with and H(x)=H(x’) is hard.

**Collision resistance (CR)**:

Finding x, x’∈{0,1}∗ with and H(x)=H(x’) is hard.



**birthday paradox:** given a set of t(≥10) elements take a sample of size k(drawn with repetition) in order to get a probability ≥½ on a collision (i.e. an element drawn at least twice) k has to be >1.2 𝑡. 

**Merkle-Damgård construction**

Given: •compression function: 

Goal: •Hash function: 

intermediate hash values (length n) as CF input and output

message blocks as second input of CF

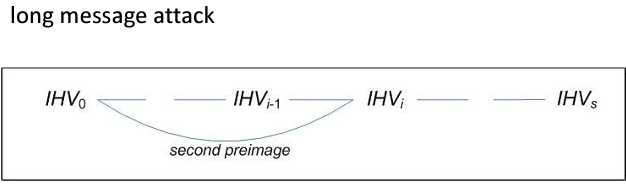
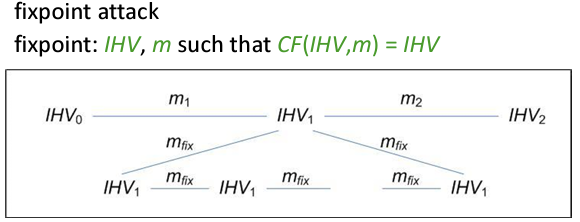
start with fixed initial IHV0 (a.k.a. IV= initialization vector)

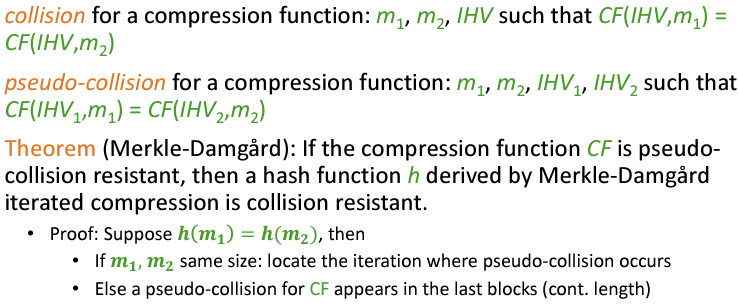
iterate CF : IHV1= CF(IHV0,m1), IHV2= CF(IHV1,m2), …, IHVs= CF(IHVs-1,ms),

• take h(m) = IHVs as hash value

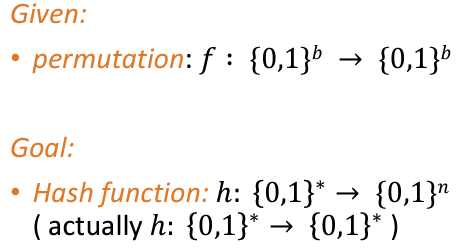
**advantages:** • this design makes streaming possible • hash function analysis becomes compression function analysis • analysis easier because domain of CFis finite

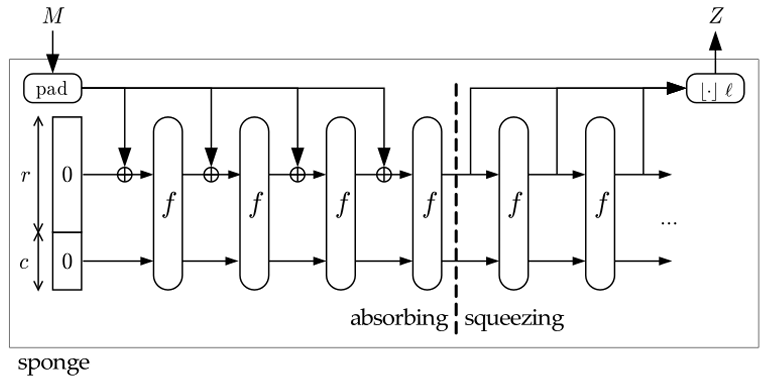
**non-ambiguous padding:** add one 1-bit and as many 0-bits as necessary to fill the final block





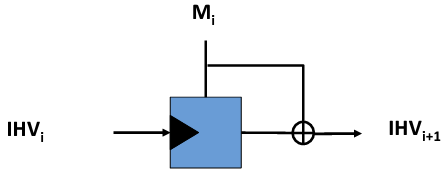
**Sponge:**



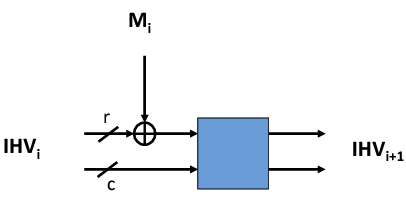


**Theorem** (Indifferentiability from a random oracle): If f is a random permutation, the expected complexity for differentiating a sponge from a random oracle is 

**Block-Cipher-based designs**

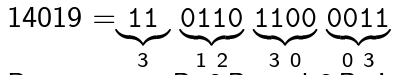
tradition

Permutation-based designs

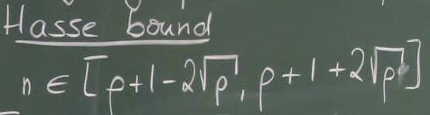


Important: NEVER hand out last c bits of IHV!

**Fixed window method**





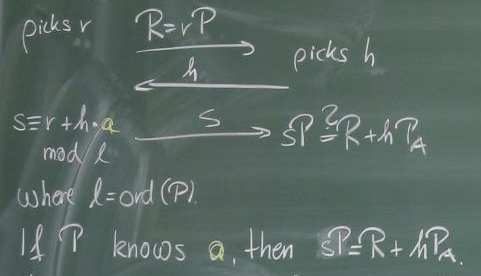


If N is the number of points on the elliptic curve E over a finite field with q elements, then Hasse's result states that

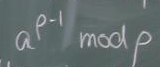


properties of signatures: authenticity, integrity, and non-repudiation, meaning that the message really came from the sender, was not modified, and the sender cannot claim not to have sent it.

**Schnorr**



**Fermat’s Prime test**

 not 1, not prime. If 1, maybe Carmichel number.

**RSA：**

Public key (n,e), Private key (n,d)



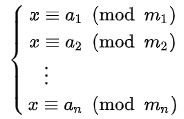
**CRT for RSA:**



See next



**CRT:**

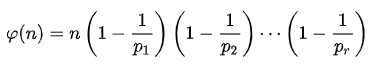




**Euler phi Function**

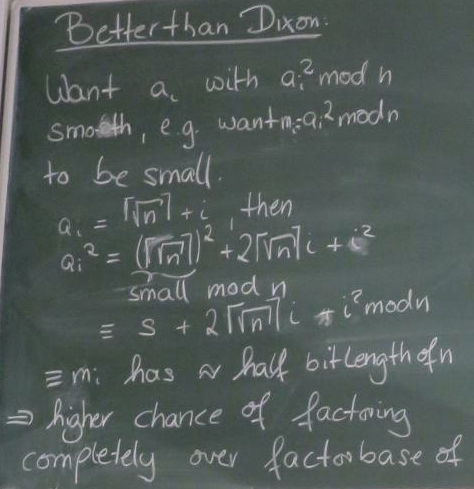




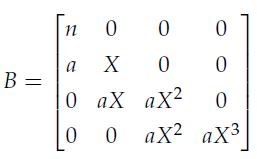




**Dixion:**



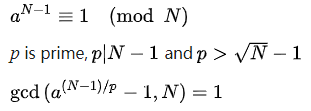
Coppersmith method:



See hw.6 & article

**Pocklington primality test**

Let N>1 be an integer, and suppose there exist natural numbers a and p such that

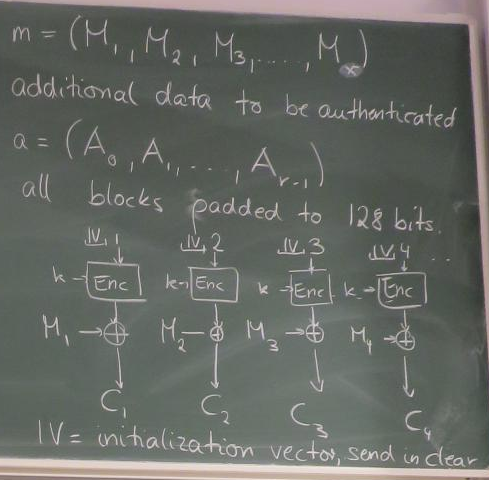


Then N is a prime.

**Miller-Rabin test**

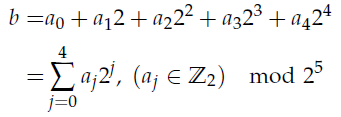
1. 令 n - 1 = 2k q，其中 k > 0，q 为奇数，随机选取整数 a，1 < a < n - 1
2. 若 aq mod n = 1，则 n 有可能是素数
3. 取整数 j，0 ≤ j < k，若存在 a^2^j mod n = n - 1，则 n 有可能是素数；否则，n为合数

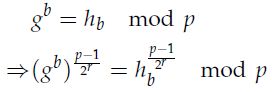
**Block Cipher**

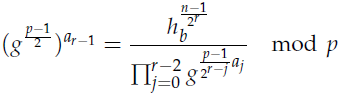


**Pohlig-Hellman:**









See hw.5.

**Pollard-Rho for DLP**



**Pollard-Rho for factoring**



**Pollard p-1**

By Femat Primality Test



So, if p-1 only has small factors (it is B-power smooth), we can choose , then



 is a factor.

判定椭圆曲线：



