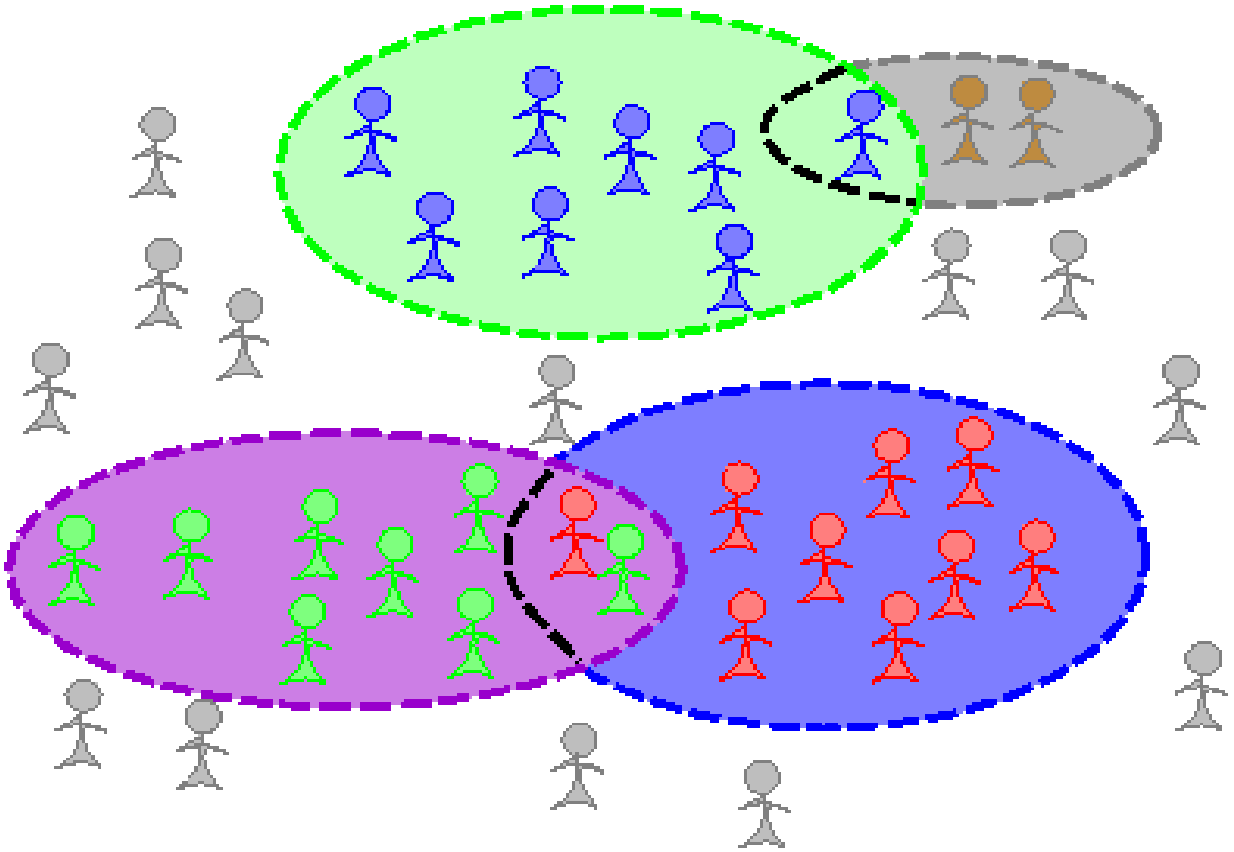
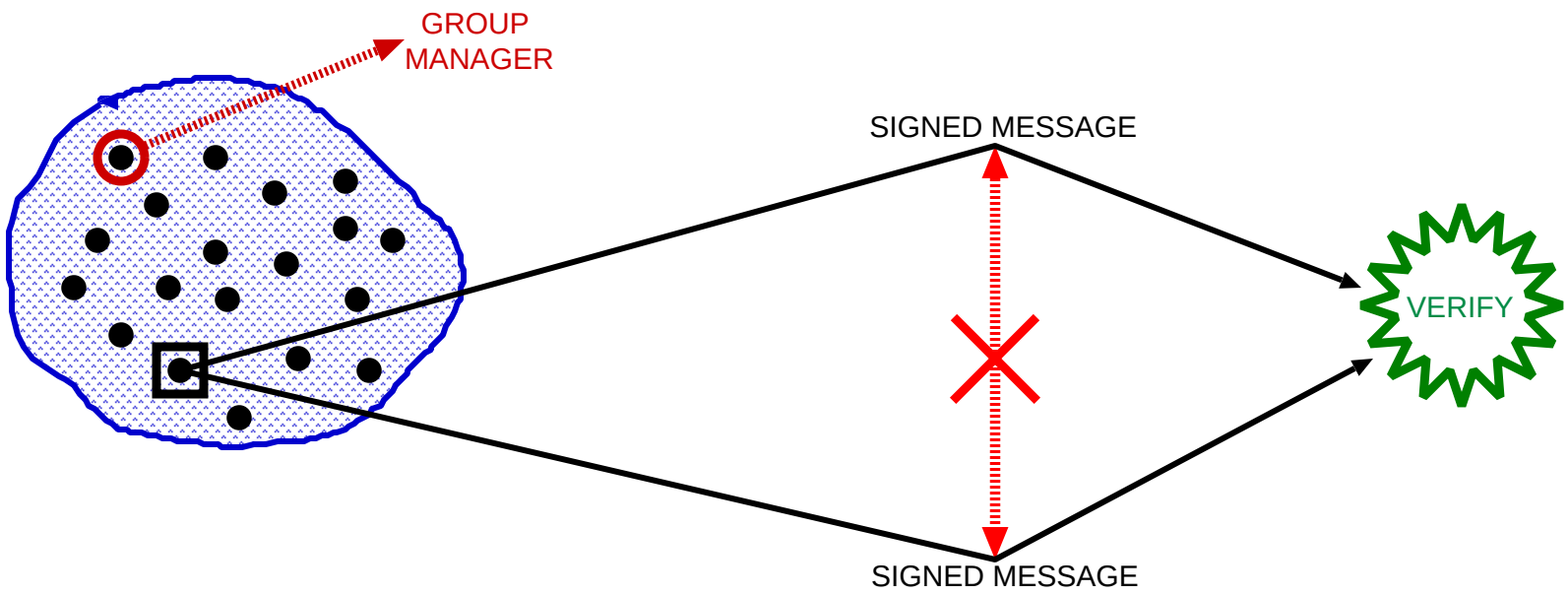
Efficient Group Signature Schemes



Giuseppe Ateniese and Gene Tsudik
USC Information Sciences Institute
ateniese@ISI.EDU
gts@ISI.EDU

Group Signature



- Unforgeability, Anonymity, Unlinkability, Exculpability, Traceability

- Efficiency and Size (group PK, signature)

Basic Phases

- SETUP: -(n,v,a,Y,Z)-

-> n = pq, p=2p'+1 q=2q'+1;
-> v, gcd(v,(p-1)(q-1))=1;
-> a, of large mult. order mod both p,q;
-> Y, a^(-y);
-> Z, a^z;

- JOIN:

-> send a^x, v<x gcd(v,x)=1;
-> group certificate: A=a^[(x+y)/v];
-> store significant information in the membership table;

Basic Phases

- SIGN:

  -> T1 = A a^r

  -> T2 = A^{-1} (Z a^{-1})^r

  -> Construct:

  SKLOG1 = SKLOG(m,a^(x+rv),a);

  SKLOG2 = SKLOG(m,a^(zr),a^z);

  -> Send {T1,T2,SKLOG1,SKLOG2};

- VERIFY:

  -> W1 = (T1^v) Y (= a^(x+rv));

  -> W2 = (T1 T2) (= a^(rz)= Z^r);

  -> check SKLOG1 and SKLOG2 with W1, W2;

- OPEN:

  -> ID = (T1)^(z-1) $T2^{-1}$= A^z;

Coalitions and Previous Works

- C./S. crypto'97:

  -> group certificate: A=(a^x + 1)^d, d=1/e;

- Some attacks: (a^x+1) = a^x(1+a^-x)

  -> if x = ke, from a^k (1+a^-x)^d

  ==> (a^-x +1)^d;

  -> User 1 registers (a^x + 1)^d

  User 2 registers (a^-x +1)^d

  ==> a^(xd)

  User 3 registers (a^(-cx) +1)^d

  ==> (a^(cx) +1)^d

  -> a^(C1 X1 d), ... , a^(Cn Xn d)

  ==> (a^(Ci1Xi1+...+CipXip) +1)^d

Our Approach and On-going Work

- Cross-check by several group certificates

- How many ?

- Pooling shares is only a specific form of coalition