A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and its Applications

Emmanuel Bresson (CELAR),
Dario Catalano (ENS),
David Pointcheval (ENS)

Contents

- Introduction, related work
- A PKC with double trapdoor
  - Descrition of our scheme
  - Security of the new scheme
- An efficient trapdoor commitment
  - Properties of the scheme
- Variants
- Conclusion

Prior Work

- El Gamal's cryptosystem (1984)
  - Based on the Diffie-Hellman problem modulo a prime number p.
- Paillier's cryptosystem (1999)
  - Based on Composite Residuosity problem modulo $N=pq$.
- Cramer-Shoup scheme (2002)
  - Cryptosystem allowing two trapdoors

Our Results

- A new variant of Cramer-Shoup '02 PKC
  - Additively homomorphic
  - Allows for a double trapdoor mechanism
  - Based on Diffie-Hellman modulo an RSA number
  - Can be turned IND-CCA2 secure easily
- A perfectly hiding commitment
  - Trapdoor based on factoring
  - Efficient online/offline trade-off
- A new Gap group (not based on EC)
- New Diffie-Hellman variant assumptions

Preliminaries

- Work in G=QR(N^2), with $N=pq=(2p'+1)(2q'+1)$
  - $|G|=\lambda(N^2)/2=pp'qq'=N\,\lambda(N)/2$
  - G is cyclic, we denote by g a generator
  - If $x\in G$ has order N, there exists k, s.t. $x=(1+kN)$
  - If $x\in Z_{N^2}$ has order N, then $x\in$ G since $x=(1+tkN)^2$

    with t the inverse of 2 mod N

Assumptions

- The Partial Discrete Logarithm Problem
  - Given g^a mod N^2, find a mod N
  - Can be solved efficiently given the factorization of N
  - Assumed to be hard otherwise
- The Diffie-Hellman Problem modulo a composite
  - Given g^x, g^y mod N^2, distinguish g^{xy} mod N^2 from a random in G
  - Can be solved efficiently given the factorization of N
  - Assumed to be hard otherwise

A Gap-problem

- An algorithmic problem whose computational version is hard, while decisional version is easy
- The Diffie-Hellman problem modulo N^2
  - DDH is easy when given the factorization
  - It does not help computing the value of g^{xy} mod N^2
- Not based on elliptic curves

Our cryptosystem

- Key generation
  - $N=pq$, safe-prime, $G=\langle g \rangle$ and $h=g^a$ mod N^2.
- Encryption of $m \in Z_N$
  - Pick $r \in Z_{N^2}$, set $A=g^r$ mod N^2, $B=h^r(1+mN)$ mod N^2
- Decryption using a
  - Compute B/A^a-1mod N^2, and divide by N (in Z)
- Decryption using the factorization
  - Compute a mod N and r mod N, set $\gamma = ar$ mod N
  - Compute $D=(B/g^\gamma)^\lambda = 1+mN\lambda$ mod N^2
  - Denoting $\pi=\lambda^{-1}$mod N, recover $m=(D-1)\pi / N$

Remarks on the scheme

- Comparison of the two trapdoors:
  - The discrete logarithm a can be used only to decrypt ciphertexts generated using the corresponding public key (that is, $h=g^a$)
  - The master key (factorization) can be used to decrypt a ciphertext generated w.r.t. arbitrary public keys.
- Drawback:
  - When trying to decrypt an incorrectly generated ciphertext, the first method detects the fault, while the master key outputs a ''invalid'' plaintext

One-wayness of the scheme

- The Lift Diffie-Hellman Problem:
  - Given $X=g^x \bmod N^2$, $Y=g^y \bmod N^2$, $Z=g^{xy} \bmod N$, find $Z \bmod N^2$
  - This problem is not easier than the Partial DL Problem
- Theorem:
  - The one-wayness of the cryptosystem is equivalent to the Lift Diffie-Hellman problem

Semantic Security

- Decisional Diffie-Hellman Problem modulo N^2:
  - Given $X=g^x \bmod N^2$, $Y=g^y \bmod N^2$, $Z=g^z \bmod N^2$, decide if $z=xy \bmod \mathrm{ord}(\mathsf{G})$ or not
  - This problem is not harder than factoring
- Theorem:
  - If the DDH assumption holds in Z_{N^2}, the scheme is semantically secure in the standard model

A new trapdoor commitment scheme

- Trapdoor commitments
  - Given a public key *pk*, and a randomness *r*, commit to a message *m*
  - Trapdoor property: given a commitment on *m* using random *r*, together with a trapdoor *sk*, find for any message *m'*, a random string *r'* that leads to the same commitment
- On-line / off-line commitments
  - A preprocessing stage is done **before** knowing *m*
  - The length of the commitment should not increase

The scheme

- Key generation
  - Same as for the cryptosystem
- Committing a message $m \in Z_N$
  - Pick $r \in Z_{N\lambda(N)/2}$, and set $C = h^r(1+mN) \bmod N^2$
- Preprocessing
  - h^r can be precomputed; this is only one exponentiation
  - The on-line cost is only two multiplications

Properties and security

- Trapdoor:
  - Let $h^\lambda = (1+kN) \bmod N^2$, and $d = k^{-1} \bmod N$
  - Given m, m' and r, the following value

    $$r' = r + (m-m')d\lambda \mod N\lambda/2$$

  leads to the same value of the commitment
- Perfectly hiding, computationally binding
  - If r is uniformly distributed over $Z_{N\lambda/2}$, h^r is uniformly distributed over G, and so is the commitment
- Security of the scheme
  - One shows that if (m,r) and (m',r') commit identically, then $r-r'$ should be a multiple of $\lambda(N)/2$

Variants and applications

- On-line/off-line signatures based on factoring
  - Off-line: commit-and-sign a random message (m', r')
  - On-line: when given the message to sign m, use the trapdoor to find a random r for a collision (m,r)
- A "lite" cryptosystem:
  - Choose r in Z_N rather than in Z_{N^2}
  - Security is based on a so-called Small Diffie-Hellman problem
  - The decryption using factorization is simplified

Conclusion

- Summary
  - two new schemes:cryptosystem, commitment
  - new problems: variants of Diffie-Hellman, ''gap''-problem
- Further research in progress
  - improvments
  - other applications