The group of signed quadratic residues and applications

Dennis Hofheinz (CWI)
Eike Kiltz (CWI)

Quadratic residues

- $QR_N := \{ x \in Z_N^* \mid \exists y \in Z_N^* : x = y^2 \bmod N \}$
- Extremely useful for cryptography:
  - Deciding membership in QR_N supposedly hard
    - Goldwasser-Micali, (Benaloh/Naccache-Stern)/...
  - Computing witness for membership (i.e., square root) equivalent to factoring N
    - Rabin/Blum-Blum-Shub/Blum-Goldwasser/...

Quadratic residues

- But: Membership in QR_N can be problematic
  - Example: PKE with ciphertexts in QR_N
  - Problem: decryption cannot distinguish QR_N-ciphertexts from $(Z_N^*\backslash QR_N)$-ciphertexts
  - Decryption simulation becomes harder (what if Dec($-C^*$) is requested?)
- Ad-hoc solution: use homomorphic properties and square every incoming group element

Signed quadratic residues

- More elegant: use *signed* quadratic residues

$$QR_N^+ := \{\ |x|\ |\ x \in QR_N\ \}$$

- Membership problem in QR_N^+ easy (Blum N)
  - $QR_N^+ = J_N^+ = \{\ |x|\ |$ Jacobi symbol $(x/N)=1\ \}$
    - Map f: $J_N \to QR_N$, $f(x)=x^2 \bmod N$ has kernel ± 1
- Finding square roots still as hard as factoring
- Gap group!
- Considered by [FS2000], but not explored

Our results

- Consider QR_N^+ for Hybrid ElGamal (DHIES)
- Results:
  - RO model: DHIES is IND-CCA under factoring
    - Difficulty: reject inconsistent ciphertexts in sim.
    - Idea: show Strong Diffie-Hellman holds in QR_N^+
  - Standard model: DHIES is IND-CCA under higher residuosity assumption
    - Difficulty: reject inconsistent ciphertexts in sim.
    - Idea: use entropic hash proof systems
- Note: one scheme, two models, two results!

Hybrid ElGamal (DHIES)

- Key generation:

$$pk = (G, g, X = g^x, H) \qquad sk = (G, x, H)$$

- Encryption ((E,D) denotes IND-CCA SKE):

$$\mathrm{Enc}_{pk}(M) = (Y = g^y, S = \mathrm{E}_K(M)) \;\; \text{for} \;\; K = H(Y, X^y)$$

- Decryption: $\mathrm{Dec}_{sk}(Y,S)$ computes $K = H(Y, Y^x)$
  decrypts $M = \mathrm{D}_K(S)$

Our results

- Consider QR_N^+ for Hybrid ElGamal (DHIES)
- Results:
  - RO model: DHIES is IND-CCA under factoring
    - Difficulty: reject inconsistent ciphertexts in sim.
    - Idea: show Strong Diffie-Hellman holds in QR_N^+
  - Standard model: DHIES is IND-CCA under higher residuosity assumption
    - Difficulty: reject inconsistent ciphertexts in sim.
    - Idea: use entropic hash proof systems
- Note: one scheme, two models, two results!

DHIES in the RO model

- [ABR01,CS03]: DHIES IND-CCA under SDH
  - Idea: RO statistically separates challenge key
  - Sim. must connect *H*-queries and keys (SDH)
- Strong Diffie-Hellman (SDH) problem:

CDH: given g, $X=g^x$, $Y=g^y$, compute g^{xy}

SDH: like CDH, but with access to $DH_x(\cdot)$:

$$DH_x(Y^*,Z^*)=1 \text{ iff } Z^*=(Y^*)^x$$

DHIES in the RO model

- [S85]: CDH in QR_N is as hard as factoring
  - Idea: turn CDH adversary into root extractor
    given square $h \in QR_N$, set up:

$$g := h^2, \qquad X := hg^a \qquad Y := hg^b$$

so

$$g^{xy} = g^{(a+1/2)(b+1/2)} = g^{ab+(a+b)/2+1/4} = h^{2ab+a+b} h^{1/2}$$

  - No obvious way to simulate DH-oracle (SDH)
  - Reason: queries may be in $Z_N^*\backslash QR_N$

DHIES in the RO model

- Our simulation: given square $h \in QR_N^+$, set up

$$g := h^2, \qquad X := hg^a \qquad Y := hg^b$$

- Given a DH_x query (Y^*, Z^*), need to test for

$$Z^* = (Y^*)^x$$

$$\Leftrightarrow \qquad Z^* = (Y^*)^{a+1/2}$$

$$\Leftrightarrow \qquad (Z^*)^2 = (Y^*)^{2a+1}$$

(all operations in QR_N^+)

Our results

- Consider QR_N^+ for Hybrid ElGamal (DHIES)
- Results:
  - RO model: DHIES is IND-CCA under factoring
    - Difficulty: reject inconsistent ciphertexts in sim.
    - Idea: show Strong Diffie-Hellman holds in QR_N^+
  - Standard model: DHIES is IND-CCA under higher residuosity assumption
    - Difficulty: reject inconsistent ciphertexts in sim.
    - Idea: use entropic hash proof systems
- Note: one scheme, two models, two results!

DHIES in the standard model

- Recall $pk = (G, g, X{=}g^x, H)$, sk=(G, x, H)
- Idea 1: replace g in proof with subgroup gen.
  - Consequence: *pk* does not determine *x*
- Idea 2: implement *H* as UHF
  - Consequence: decryption $K{=}H(Y, Y^x)$ extracts
  - Key *K* looks uniform if $Y \notin \langle g \rangle$ (so $Y^x \notin \langle g \rangle$)
- KEM part is entropic HPS (hence IND-CCA)!

Conclusion

- Signed quadratic residues useful (gap!) group
- Simplifies existing proofs ([L02,CS03,HK09])...
- ...and gives new handles (Hybrid ElGamal)