Lecture 12

Tuesday, 10 January 2023 08:22

homomorphism : structure preserving map

let:
$\varphi : A \to B$
$\circ : A \times A \to A$
$\bullet : B \times B \to B$

φ is homomorphic if $\forall a, b \in A : \varphi(a) \bullet \varphi(b) = \varphi(a \circ b)$

today : $\varphi = Enc$

for ElGamal: $\circ = \cdot$ in G

$\mathbb{Z}_p^*$ $p = 2q+1$

decisional DH problem is hard $\Rightarrow$ $x, y, z \xleftarrow{R} \mathbb{Z}_q : g^x, g^y, g^{xy} \equiv g^x, g^y, g^z$

IND-CCA2 security is undecidable for any homomorphic encryption scheme

ElGamal is IND-CPA
and IND-CCA1 secure
(under reasonable assumption)

all sensible homomorphic schemes are re-randomizable

CGS voting system

assume trusted authority A generates keypairs
voters V_i submits (=multiplies) encrypted vote with signature

$g^{r_i}, (g^x)^{r_i} \cdot g^{v_i}$ $v_i \in \{0, 1\}$

$\prod_{i \in V} g^{r_i}$, $\prod_{i \in V} g^{r_i \cdot a + v_i}$

$g^{\sum r_i}$, $g^{a \cdot \sum r_i + \sum v_i}$

works if all parties are honest
solution: require collusion of multiple parties
but: may allow abstention especially by last party to publish data, who knows whether he likes the result

fully homomorphic encryption
$\downarrow$
need ability to run arbitrary circuits
$\downarrow$
early: lattice-based but noisy

encrypt secret key with public key
$\downarrow$
encrypt ciphertext a second time
$\downarrow$
run decryption homomorphically $\rightarrow$ reduces noise

Zero-knowledge proofs: verifier learns nothing new / non-trivial from proof

correctness honestly generated proof for true statement is accepted
soundness no valid proof for false statement
zero-knowledge proof can be simulated for false statement so that result is indistinguishable from real proof