HOMOMORPHIC ENCRYPTION

El Gamal ENCRYPTION $\quad Enc(Pk, M) = (g^R, Pk^R \cdot M)$

$Enc(Pk, M') = (g^{R'}, Pk^{R'} \cdot M')$

ENCRYPTION OF $M \cdot M' \longleftarrow (g^{R+R'}, Pk^{R+R'}(M \cdot M'))$

HOMOMORPHISM

VOTING $\quad x_1, \dots, x_n \in \{1, 0, -1\}$

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n$$

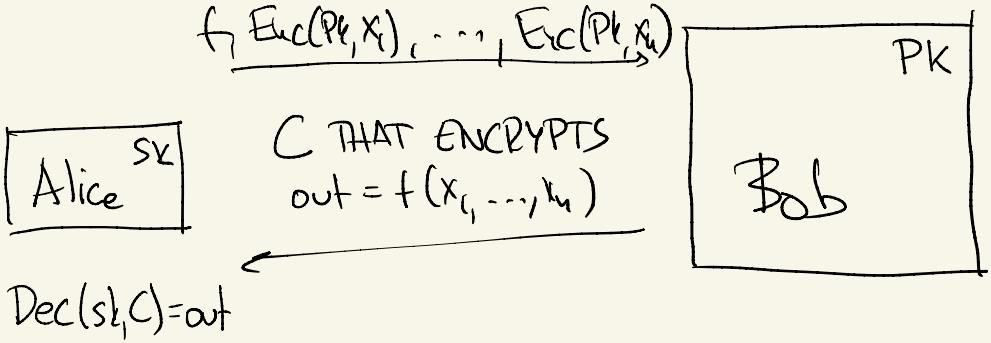
ELECTION COMMITTEE: $(sk, Pk = g^{sk})$ FOR El Gamal ENCRYPTION

VOTE x_i : $Enc(PK, x_i) = (g^R, Pk^R \cdot g^{x_i})$

HOMOMORPHISM : $\prod$ VOTES $= (g^{R^*}, Pk^{R^*} g^{\sum x_i})$

1978 RAD: IS THERE SECURE Enc THAT SUPPORT HOMOMORPHIC X AND +?

SECURE OUTSOURCING

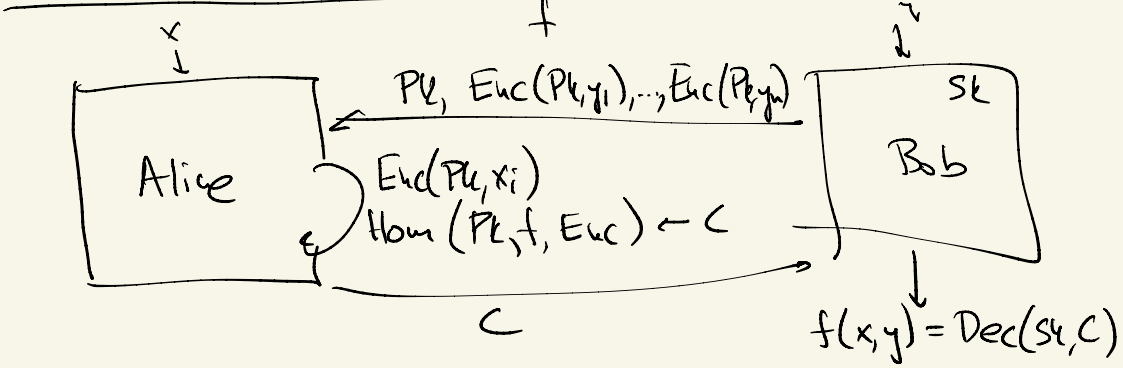


WEAK HOMOMORPHIC EVALUTOR IS AN ALGORITHM Hom

$$Hom(Pk, f, Enc(Pk, x_1), \dots, Enc(Pk, x_n)) = C$$

SUCH THAT $Dec(Sk, C) = f(x_1, \dots, x_n)$

SECURE 2 PARTY COMPUTATION



STRONG HOMOMORPHIC EVALUATOR IF R.V.S

$(PK, Enc(PK,x_1), \dots, Enc(PK,x_n), C)$ IS ε-CLOSE

TO $(PK, Enc(PK,x_1), \dots, Enc(PK,x_n), Enc(PK,y))$

WHERE $y = f(x_1, \dots, x_n)$ AND $C = Hom(PK, f, \cdot)$

STATISTICAL

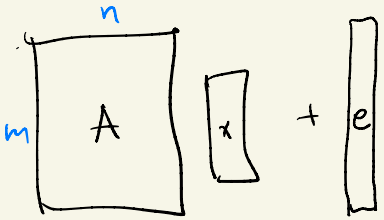
HOW TO BUILD FULLY HOMOMORPHIC ENCRYPTION

LWE ASSUMPTION $(A, Ax+e)$ IND FROM (A,r)

A RANDOM MATRIX WITH $\mathbb{Z}_q$ ENTRIES

x " VECTOR

e SHORT RANDOM VECTOR IN $\mathbb{Z}_q$



e IS b-BOUNDED

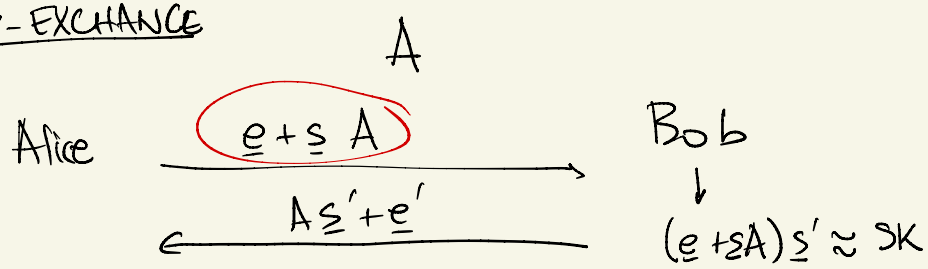
THINK OF $b = O(n)$

WHILE q = EXPONENTIAL IN n.

e, f = b-BOUNDED $\quad e^T \cdot f$ = mb-BOUNDED poly(n)

SHORT-LWE: $(A, Ax+e)$ IND FROM (A,r).

KEY-EXCHANGE



SHARED KEY $\approx \underline{s}A\underline{s}'$

PUBLIC-KEY ENCRYPTION

$$\underline{sk} = [\underline{s}, -1] \quad , \quad PK = \begin{bmatrix} A \\ \underline{e} + \underline{s}A \end{bmatrix}$$

$$\underline{sk} \cdot PK = \underline{s}A - (\underline{e} + \underline{s}A) = -\underline{e} \quad \text{SHORT}$$

$$Enc(PK, m) = PK \cdot \underline{x} + \begin{bmatrix} \underline{e}' \\ \underline{e}'' \end{bmatrix} + \begin{bmatrix} 0 \\ \underline{m} \end{bmatrix} \qquad \underline{m} \in \{0,1\}$$

$$Dec(\underline{sk}, C) = \underline{sk} \cdot C \quad (+ \text{ A LITTLE MORE WORK})$$

$$\underline{sk} \cdot C = \underbrace{\underline{sk} \cdot PK}_{-\underline{e}} \cdot \underline{x} + \underline{sk} \cdot \begin{bmatrix} \underline{e}' \\ \underline{e}'' \end{bmatrix} + [\underline{s} \; -1] \begin{bmatrix} 0 \\ \underline{m} \end{bmatrix}$$

$$= \underline{\text{short}} - \underline{m}$$

SECURITY: PK IS C.I. FROM RANDOM MATRIX R

REGEV ENCRYPTION

$sk = [s \ \ -1] \qquad PK = \begin{matrix} n \\ \end{matrix}\begin{matrix} m \\ \end{matrix}\begin{bmatrix} A \\ e + sA \end{bmatrix}$

$sk \cdot PK = -e$ (sk IS ALMOST IN LEFT NULLSPACE OF PK)

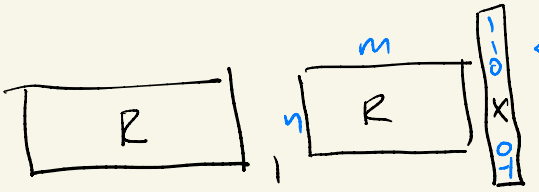
$Enc(PK, u) = PK \cdot \underline{x} + \begin{bmatrix} 0 \\ u \end{bmatrix}$ FOR RANDOM $\underline{x} \sim \{-1,0,1\}^m$

$sk \cdot C = sk \cdot PK \cdot \underline{x} + [s \ -1]\begin{bmatrix} 0 \\ u \end{bmatrix} = \underbrace{-e \cdot \underline{x}}_{\text{SHORT}} - u$

SECURITY:

$(PK, Enc(PK, m))$ C.I. $(R, Enc(R, u))$ (R RANDOM)

$= (R, R\underline{x} + \begin{bmatrix} 0 \\ u \end{bmatrix})$



$m > n \log q \rightarrow x$ HAS AS MUCH ENTROPY AS A RANDOM VECTOR IN $\mathbb{Z}_q^n$

LEFTOVER HASH LEMMA: (R, Rx) IS ε-CLOSE TO (R, r) (r IND OF R) IF $m > n \log q + 2\log\frac{1}{\varepsilon}$.

SO $(PK, Enc(PK, m))$ C.I. $(R, r + \begin{bmatrix} 0 \\ u \end{bmatrix}) \equiv (R, r)$

SIMULATABLE WITHOUT KNOWING u

SECURITY DOES NOT DEPEND ON HOW u IS ENCODED (THOUGH FUNCTIONALITY DOES)

ALTERNATIVE ENCODING

$$Enc(Pk, m) = Pk \cdot \underline{x} + \begin{bmatrix} m \\ 0 \end{bmatrix} \leftarrow G(m)$$

$$sk \cdot \left(Pk \cdot \underline{x} + \begin{bmatrix} m \\ 0 \end{bmatrix} \right) = -\underline{e} + m \cdot sk_1$$

CAN STILL DECRYPT BECAUSE sk_1 IS TYPICALLY NOT TOO SMALL

CAN ALSO DO

$$Enc(Pk, m) = (Pk \cdot \underline{x}_1 + G_1(m), Pk \cdot \underline{x}_2 + G_2(m), \dots, Pk \cdot \underline{x}_n + G_n(m))$$

$$= Pk \cdot \underline{X} + m \cdot \underline{I}$$ CIPHERTEXT IS A MATRIX

$$\underline{X} = [\underline{x}_1 \cdots \underline{x}_n]$$

$$sk \cdot \overbrace{(Pk \cdot \underline{X} + m \cdot \underline{I})}^{C}$$

$$= -\underline{e} \cdot \underline{X} + sk \cdot m \cdot \underline{I}$$

$$= \underline{e}' + m \cdot sk$$

$sk \cdot C = m \cdot sk + \underline{e}$ C ENCRYPTS m

$sk \cdot C' = m' \cdot sk + \underline{e}'$ C' ENCRYPTS m'

$$sk \cdot (C + C') = (m + m')\, sk + (\underline{e} + \underline{e}')$$

$C + C'$ ENCRYPTS $m + m'$ (BUT NOISE DOUBLES)

$$sk\, C \cdot C' = m \cdot sk \cdot C' = m \cdot m' \cdot sk$$

IF $\underline{e}, \underline{e}' = 0 \rightarrow$ $C \cdot C'$ WOULD ENCRYPT $m \cdot m'$

$$sk \cdot C \cdot C' = (\underline{u} \cdot sk + \underline{e}) \cdot C'$$
$$= \underline{u} \cdot sk \cdot C' + \underline{e} \cdot C'$$
$$= \underline{u} \cdot (\underline{u}' \cdot sk + \underline{e}') + \underline{e} C'$$
$$= \underline{u}\,\underline{u}' \cdot sk + \underline{u} \cdot \underline{e} + \underline{e} \cdot C'$$

SHORT NOT SHORT

IDEA: REPLACE C' WITH ITS BIT DECOMPOSITION.

$$\underline{D}(5) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \qquad \underline{D}: \mathbb{Z}_q \to \{0,1\}^{\lceil \log q \rceil}$$

$$\underline{D}\left(\begin{bmatrix} 3 & 2 \\ 0 & 7 \end{bmatrix}\right) = \begin{bmatrix} \underline{D}(3) & \underline{D}(2) \\ \underline{D}(0) & \underline{D}(7) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$$

$$5 = (1\ 2\ 4)\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

INVERSE D^+ IS LINEAR: $D^+\begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} = x_0 + 2x_1 + 4x_2$

WHEN X IS A MATRIX D^+X IS LEFT MULT. BY

$$D^+ = \begin{bmatrix} 4 & 2 & 1 & & & \\ & & & 4 & 2 & 1 \end{bmatrix}$$

$$\boxed{D^+ \cdot \underline{D}(C) = C}$$

$$Enc(PK, \underline{m}) = PK \cdot \underline{X} + \underline{m} \cdot \underline{I}$$

CHANGE TO

$$Enc(PK, \underline{m}) = PK \cdot \underline{X} + m \cdot \underline{D}^+$$

FUNCTIONALITY, SECURITY IS PRESERVED

$$sk \cdot C = sk \cdot PK \cdot \underline{X} + sk \cdot \underline{m} \cdot \underline{D}^+$$
$$= \underline{e} + \underline{m} \cdot sk \cdot \underline{D}^+$$

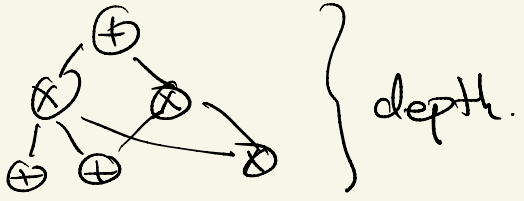
IF C, C' ENCRYPT $\underline{m}, \underline{m}'$ $\rightarrow$ $C + C'$ ENCRYPTS $\underline{m} + \underline{m}'$.

Claim. $C \cdot \underline{D}(C')$ ENCRYPTS $\underline{m} \cdot \underline{m}'$.

$$sk \cdot C \cdot \underline{D}(C') = (\underline{m} \cdot sk \cdot \underline{D}^+ + \underline{e})\, \underline{D}(C')$$
$$= \underline{m} \cdot sk \cdot \underline{D}^+ \underline{D}(C') + \underline{short}$$
$$= \underline{m} \cdot sk \cdot C' + \underline{short}$$
$$= \underline{m} \cdot (sk\, \underline{m}' \underline{D}^+ + \underline{e}') + \underline{short}$$
$$= \underline{m} \cdot \underline{m}' \cdot sk\, \underline{D}^+ + \underline{short}$$

NOISE ROUGHLY GROWS BY A FACTOR OF n.

CKT OF DEPTH d $\rightarrow$ NOISE BECOMES $\approx n^{depth}$



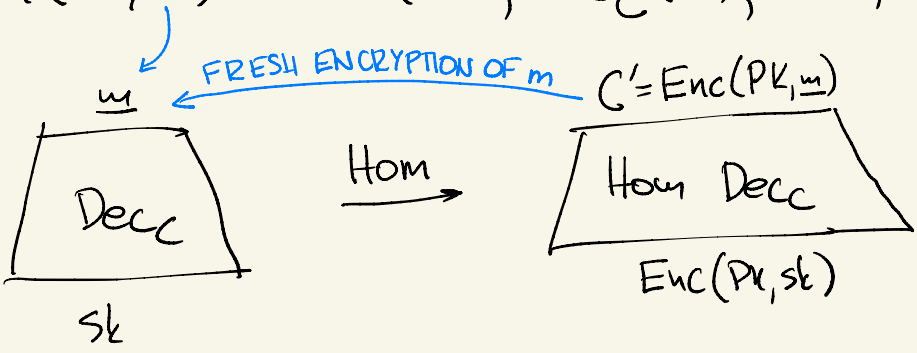
SUMMARY SCHEME WORKS FOR SUFFICIENTLY SHALLOW CIRCUITS.

DENOISING: $Den(PK, C) = C'$

- C' ENCRYPTS SAME CIPHERTEXT AS C
- IF $sk \cdot C = \underline{m} \cdot sk \cdot D^+ + \underline{e}$ FOR b^+-BDD $\underline{e}$
  THEN $sk \cdot C' = \underline{m}\ sk \cdot D^+ + \underline{e}'$ FOR b^--BDD $\underline{e}'$

WHERE $b^- < b^+$.

$$Den(PK, C) = Hom(PK, Dec_C(sk), Enc(PK, sk))$$



NOISE IN C' ONLY DEPENDS ON DEPTH OF Dec_C CIRCUIT AND NOT AT ALL ON NOISE IN C

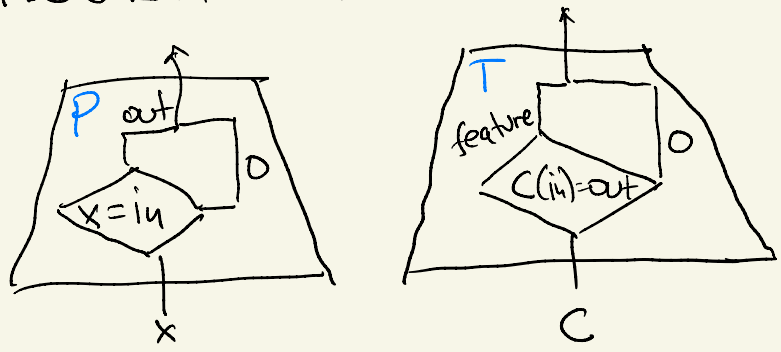
HOMOMORPHIC EVAL OF Dec_C $\rightarrow$
HOMOMORPHIC EVAL OF ARBITRARY CIRCUIT!

IMPOSSIBILITY OF OBFUSCATION

$C \longrightarrow Obf(C)$ SAME FUNCTIONALITY

LEARNER GIVEN CODE OF $Obf(C)$ CAN BE SIMULATED USING ORACLE ACCESS

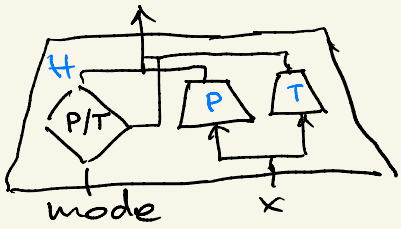
LEARNER ADVANTAGE: CAN TAKE CIRCUIT AND INPUT INTO ANOTHER CIRCUIT (PROGRAM ANALYSIS)



in, out, feature ARE SECRET KEYS

LEARNER CAN EXTRACT feature BY RUNNING $Obf(T)$ ON $Obf(P)$, BUT ORACLE ACCESS UNLIKELY TO REVEAL in, out, OR feature

OBFUSCATION OF 2 CIRCUITS IMPOSSIBLE; WHAT ABOUT 1 CIRCUIT? IDEA



LEARNER NEEDS TO SET x = CODE OF $H(P,\cdot)$ TOO BIG TO FIT!

WE CAN MAKE THIS WORK BY OUTSOURCING COMPUTATION OF T TO LEARNER

H: node
- I → OUTPUT $PK, Enc(PK, in)$
- P → OUTPUT out IF $x = in$
- T → OUTPUT feature IF $Dec(sk, z) = out$

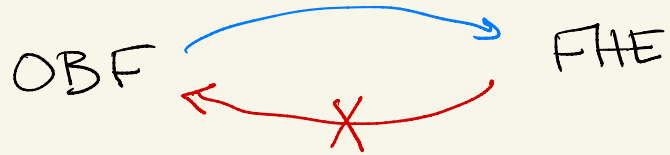
LEARNER: $H(I) \rightarrow PK, Enc(PK, in)$

$Hom(PK, H(P), Enc(PK, in)) \rightarrow Enc(PK, out)$

$H(T, Enc(PK, out)) \rightarrow$ feature

SIMULATOR CANNOT FIND ANY INFO ABOUT in BECAUSE $Enc(PK, in)$ IS SIMULATABLE → SMALL CHANCE OF GUESSING FEATURE.

CONCLUSION: IF FHE EXISTS OBF DOESN'T. IN FACT FHE CAN BE BUILT FROM OBF (WITHOUT EXTRA ASSUMPTIONS) SO



AND OBF CANNOT EXIST!