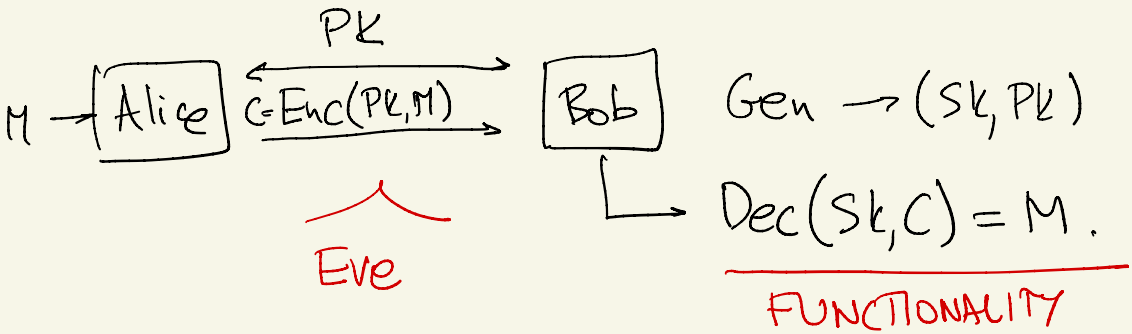
PUBLIC-KEY ENCRYPTION



PKE IS (s,ε)-MESSAGE-INDISTINGUISHABLE

$\forall M, M'$ $(PK, Enc(PK, M))$, $(PK, Enc(PK, M'))$ ARE (s,ε)-INDISTINGUISHABLE.

(s,ε)-SIMULATABLE IN SIZE t: $\exists$ Sim S.T. Sim IS (s,ε)-IND FROM $(PK, Enc(PK,M))$

PERFECTLY OR STAT. SECURE PKE CANNOT EXIST EVEN WITH VERY LARGE KEYS.

PKE FOR 1 MESSAGE → PKE FOR q MESSAGES

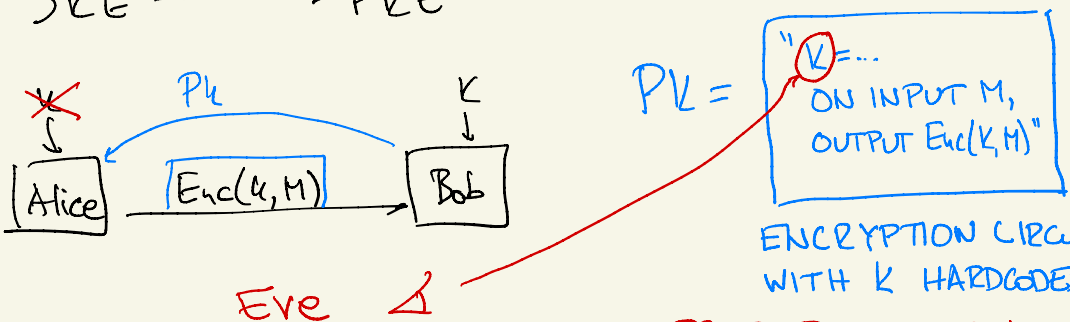
A $(PK, Enc(PK,M_1), Enc(PK,M_2))$ Eve CAN COMPUTE ON HER OWN

B $(PK, Enc(PK,M_1), Enc(PK,M_2'))$ D

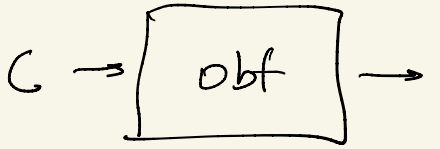
C $(PK, Enc(PK,M_1'), Enc(PK,M_2'))$ D

UNLIKE IN SK CASE

SKE ⟶ PKE



OBFUSCATION



C' COMPUTES SAME THING AS C,
BUT DOESN'T REVEAL HOW C WORKS.

FUNCTIONALITY: $\forall C$, $C' = Obf(C)$ AND C COMPUTE SAME FUNCTION.

SECURITY: Eve CANNOT LEARN ANYTHING BY LOOKING AT C'.
NOT TRUE B/C CAN LEARN $C'(7) = C(7)$.

VBB (VIRTUAL BLACK BOX): ONLY INFO CAN BE GAINED BY EVALUATING C'
(EVERYTHING ELSE CAN BE SIMULATED.)

$\forall$ CKT L OF SIZE s $\exists$ Sim OF SIZE t S.T. $L(Obf(C))$ AND Sim^C ARE $(\varepsilon, \varepsilon)$- INDISTINGUISHABLE.

$C =$ "$M \longrightarrow Enc(k, M)$" $\quad PK = Obf(C)$

Sim^C = CPA FUNCTIONALITY

PROBLEM: VBB OBFUSCATION DOES NOT EXIST.

INDISTINGUISHABILITY Obf: $Obf(C), Obf(C')$ ARE $(\varepsilon, \varepsilon)$-IND. WHENEVER C, C' COMPUTE SAME FUNCTION.

VBB OBF $\rightarrow$ IND OBF

MAY BE POSSIBLE AND IS SUFFICIENT FOR PUBLIC-KEY ENCRYPTION.

THESE ARE ENCRYPTION SCHEMES OF THE FUTURE. FOR THE PRESENT, WE'LL LOOK AT NUTS & BOLTS OF PSEUDORANDOM GENERATORS.

MODULAR EXPONENTIATION

$\mathbb{Z}_p$ = INTEGERS MODULO p $+, -, \times, \div$ ← IF p PRIME

$g \neq 0$ $\quad g^x = \underbrace{g \cdot \ldots \cdot g}_{x \text{ TIMES}}$ $\quad x$ INTEGER

TAKES $x-1$ MULTIPLICATIONS. CAN CALCULATE IN $O(\log x)$ OPERATIONS:

$$g^{2^{100}} = \underbrace{\left(\left(\left(g^2\right)^2\right)^{2 \cdots}\right)}_{100 \text{ TIMES}}$$

$$g^x = \begin{cases} \text{EVEN} & \left(g^{x/2}\right)^2 \\ \text{ODD} & \left(g^{(x-1)/2}\right)^2 \cdot g \end{cases}$$

$O(\log x)$ TIME

DISCRETE LOG $\quad g, h$: FIND x S.T. $g^x = h$

$g^{p-1} = 1 \qquad g, g^2, g^3, \ldots, g^{p-1} = 1, g^p = g, \ldots$

TRY OUT ALL $x \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ $\quad O(p)$ INEFFICIENT

IN GENERAL : BEST KNOWN ALG TAKE TIME

EXP. IN q = LARGEST PRIME FACTOR OF $p-1$

IDEALLY $p, p-1$ PRIME ✗

NEXT BEST $p, \frac{p-1}{2}$ PRIME SAFE PRIMES

ASSUME p IS A SUFFICIENTLY LARGE SAFE PRIME. $\longrightarrow$ DISCRETE LOG mod p CONJECTURED TO BE HARD. (EXP. IN p).

DECISIONAL DIFFIE-HELLMAN (IN BASE g)

(g^X, g^Y, g^{XY}) (s,ε)-IND (g^X, g^Y, g^Z)

DETERM. INDEP.

X, Y, Z RANDOM IN $\mathbb{Z}_p^*$.

PRG: $g^X\ g^Y\ g^{XY}$ DH $X\ Y$ $\approx 3\log p$ BITS $\approx 2\log p$ BITS

THERE EXIST g S.T. DDH BASE g IS FALSE.

$p = 11$. $\frac{p-1}{2} = 5$. $g=2$ $g^2=4$ $g^3=8, \dots$

$\{g, g^2, \dots, g^{10}=1\} = \{1, \dots, 10\} = \mathbb{Z}_{11}^*$

X EVEN $g^X \in \{g^2, g^4, g^6, g^8, g^{10}\} = EP$ (EVEN POWERS)

$P(Z \text{ EVEN}) = \frac{1}{2}$ $P(XY \text{ EVEN}) = \frac{3}{4}$

$P(g^Z \in EP) = \frac{1}{2}$ $P(g^{XY} \in EP) = \frac{3}{4}$

TEST IF h IS EVEN POWER OF g EFFICIENTLY

$g^2\ g^4\ g^6\ g^8\ g^{10}=1$ / $g^1\ g^3\ g^5\ g^7\ g^9$ — $\boxed{h^5 = g^{x \cdot 5}}$ — $h=1$ / $h \neq 1$

TEST: $h^5 \stackrel{?}{=} 1$

IN GENERAL $h^{\frac{p-1}{2}} = 1 \longleftrightarrow h$ IS EVEN POWER OF g

$g = 2$ X

IF I CHOSE $g' = g^2 = 4$, g'^x COVERS EVEN POWERS OF g

$g', g'^2, g'^3, g'^4, g'^5 = 1$

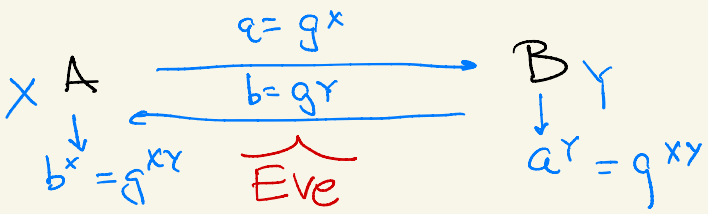
EXPONENTS BASE g' HAVE PRIME ORDER $\frac{p-1}{2}$

→ g'^{xy}, g'^z BOTH UNIFORM AMONG EVEN POWERS OF g (A.K.A. QUADRATIC RESIDUES)

DDH BASE g' PLAUSIBLE FOR $g' =$ QUADRATIC RESIDUE (SQUARE OF SOMETHING.

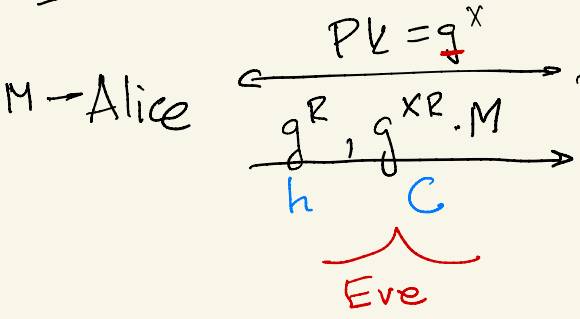
$$(g^x, g^y, g^{xy}) \approx (g^x, g^y, g^z)$$

DIFFIE-HELLMAN KEY EXCHANGE



Eve OBSERVES g^x, g^y. RELATIVE TO THIS, THE KEY g^{xy} IS INDISTINGUISHABLE FROM THE INDEPENDENT NUMBER g^z, WHICH SHE CAN SIMULATE ON HER OWN

EL GAMAL ENCRYPTION



$Dec(h, C) = h^{-x} \cdot C$

$Dec(g^R, g^{xR} \cdot M) = M$

SECURITY: Eve's VIEW $(PK, h, C) = (g^x, g^R, g^{xR} \cdot M)$

IF $\exists$ D THAT ε-DIST

$(g^x, g^R, g^{xR} \cdot M)$ FROM (g^x, g^R, g^z)

TAKE $D'(h, i, j) = D(h, i, j \cdot M^{-1})$

D' BREAKS DDH

EFFICIENT CONVERSION BETWEEN

G = EVEN POWERS $\longleftrightarrow$ $\{1,\dots,q\}$ $\quad q = \frac{p-1}{2}$

$h^2 \longleftarrow h \qquad -h$

$k \longrightarrow |k^{\frac{p-1}{2}}|$

$\mathbb{Z}_p^* = \{-q,\dots,-1,1,\dots,q\}$

WEAKNESS: INSECURE AGAINST QUANTUM COMP.

LEARNING WITH ERRORS OVER $\mathbb{Z}_q$ (mod q)

$q = 191$

n

$$\left.\begin{array}{l} 36x_1 + 17x_2 + 39x_3 \approx 113 \\ 7x_1 + 111x_2 + 9x_3 \approx 31 \\ 150x_1 + 37x_2 + 7x_3 \approx 3 \\ 11x_1 + 95x_2 + 77x_3 \approx 177 \end{array}\right\} m \quad \text{NOISE}$$

$$Ax \approx y \qquad (= Ax + e)$$

A: RANDOM PUBLIC

x: RANDOM SECRET

e: SMALL RANDOM $\sim \{-b,\dots,b\}$

ALGORITHMS

1. TRY ALL POSSIBLE x: q^n
2. TRY ALL POSSIBLE e: b^m
3. ROUGHLY TIME e^{b^2}. (A BIT MORE COMPLICATED)

SEARCH-LWE : THERE IS NO CKT OF SIZE s THAT GIVEN $A, Ax+e$ FINDS x WITH PROBABILITY $> \varepsilon$.

e IS DISCRETE GAUSSIAN IND. $p(j) \propto e^{-j^2/2\sigma^2}$

$\sigma \approx$ BOUND ON NOISE

SO MANY PARAMETERS!

(m, n, q, σ)-LWE IS HARD ← HARD TO APPROXIMATE SHORTEST VECTOR IN AN n-DIM LATTICE TO WITHIN $\approx \sqrt{n}\, q/\sigma$. ← ONE PARAMETER

BEST KNOWN EFFICIENT ALGORITHM $\approx 2^{n/\log n}$

Ex. $q = n^{10}$ OR EVEN $q = 2^{n/(\log n)^2}$, $\sigma = 2\sqrt{n}$ BELIEVED TO BE SECURE.

WITH HIGH PROB EVEN AN EXPONENTIAL NUMBER OF NOISE SAMPLES WILL BE b-BOUNDED FOR $b = n$ EG

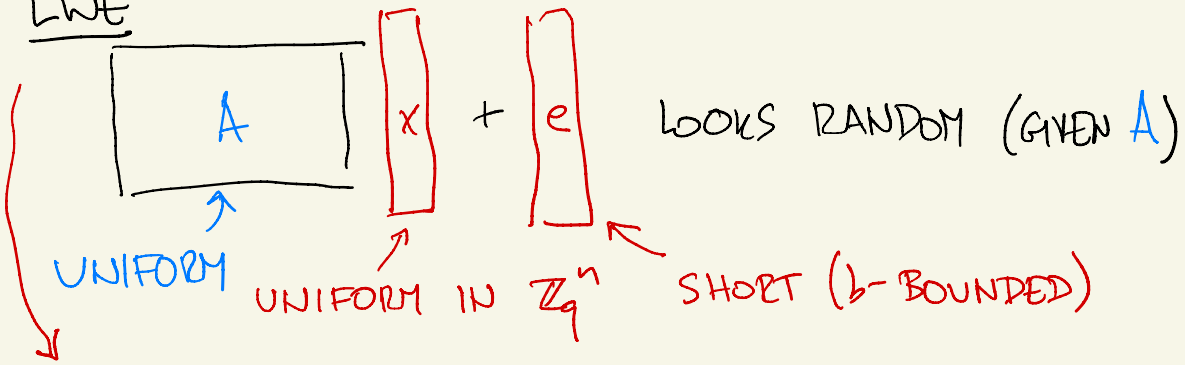
LWE ASSUMPTION: $(A, Ax+e)$ (s,ε)-INDISTINGUISHABLE FROM (A, r) r IND.

EQUIVALENTLY, $G(A, x, e) = (A, Ax+e)$ IS A PRG.

$n \log q$ $m \log b$ $m \log q$

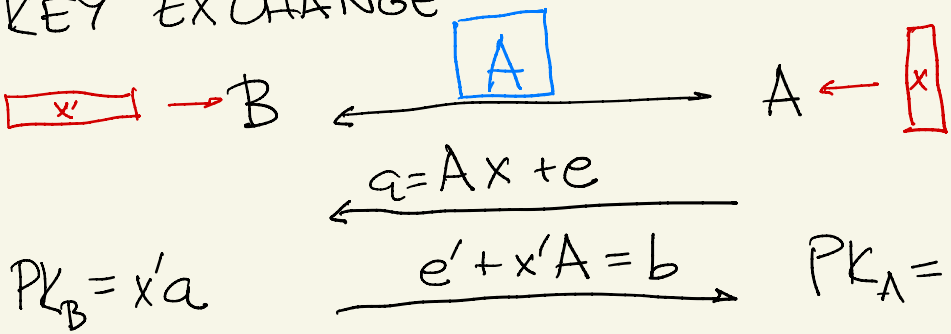
UNLIKE DDH AND DLOG, LWE AND searchLWE ARE EQUIVALENT.

LWE



short-LWE : x IS SHORT (SAME DISTRIBUTION AS e) SO IT IS b-BOUNDED.

KEY EXCHANGE



FUNCTIONALITY : $PK_A \stackrel{?}{=} PK_B$

$x'a = x'Ax + x'e$

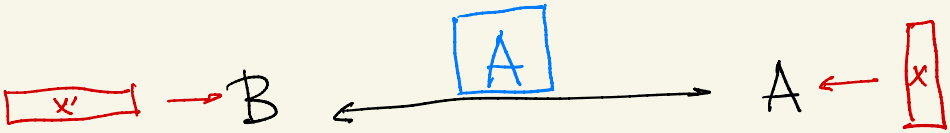
$bx = x'Ax + e'x$

$\mathbb{Z}_q$ $\quad q >> b^2n$

MAGNITUDE $\leq b^2n$

NOT IDENTICAL BUT GOOD ENOUGH FOR SKE.

SECURITY: (A, a, b, PK_A) CAN BE SIMULATED



$a = Ax + e$

$e' + x'A = b$

$PK_B = x'a$

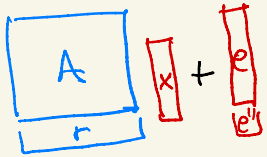
$PK_A = bx + e''$

Eve: SIMULATE $(A, Ax+e, b = e'+x'A, bx+e'')$

LWE: CAN REPLACE b BY r IND. OF x'

$(A, Ax+e, r, rx+e'')$

LOOKS LIKE



PSEUDORANDOM BY LWE AGAIN!