CRYPTO = SECURE COMMUNICATION / COMPUTATION IN INSECURE ENVIRONMENTS

TASK: DESIGN ALGORITHMS AND PROTOCOLS

RESOURCES: ADVERSARY IS MORE POWERFUL THAN LEGITIMATE USERS.

MUST HANDLE ALL SORTS OF ADVERSARIES

DO NOT WANT TO ASSUME HOW ADVERSARY OPERATES.

LECTURES

BASIC ELEMENTS - DEFINITIONS

BASIC TASKS:

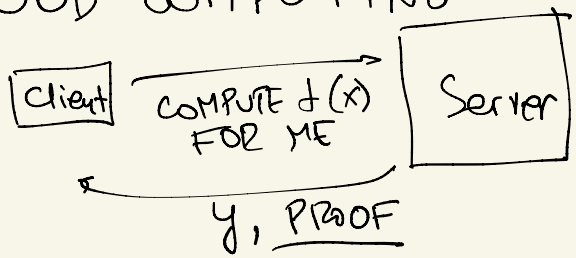
ENCRYPTION
IDENTIFICATION
AUTHENTICATION
} 1970s

SECURE MULTIPARTY COMPUTATION
ZERO-KNOWLEDGE PROOFS
} 1980s

WHAT CRYPTO CANNOT DO:

COPY PROTECTION
OBFUSCATION
} 2000s

CLOUD COMPUTING

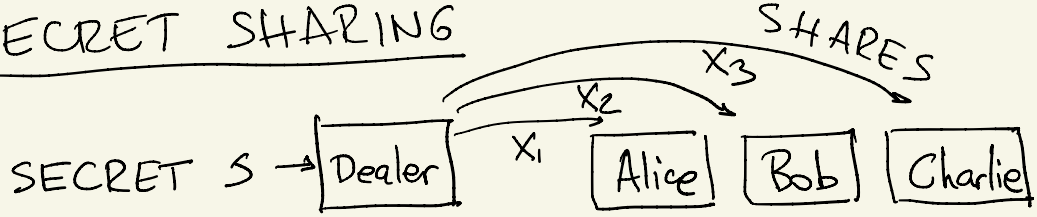


LEARNING: BREAKING CRYPTO IS LEARNING

CONSENSUS / BLOCKCHAINS: CRYPTO + INCENTIVES

QUANTUM COMPUTERS: DANGERS AND OPPORTUNITIES

SECRET SHARING



- Alice, Bob, & Charlie CAN RECOVER s
- NO SUBSET FINDS OUT ANYTHING ABOUT s.

EXAMPLE $s \in \{0,1\}$

- DEALER SAMPLES SHARES X_1, X_2, X_3 IN PRIVATE

$s=0$		$s=1$	
0 0 0	1/4	1 1 1	1/4
0 1 1	1/4	1 0 0	1/4
1 0 1	1/4	0 1 0	1/4
1 1 0	1/4	0 0 1	1/4

SECURITY: NO ONE OR TWO PARTIES CAN GET INFORMATION ABOUT s.

→ ANY 2 PARTIES OBSERVE TWO UNIFORM RANDOM BITS BOTH WHEN $s=0$ AND WHEN $s=1$.

DEALER USES RANDOMNESS TO HIDE INFORMATION.

ASSUMPTIONS

① RANDOMNESS IS PERFECT.

② ALL LOCAL COMPUTATIONS ARE PRIVATE.

THERE ARE PARTS OF CRYPTO THAT STUDY WHAT HAPPENS WHEN ① OR ② IS VIOLATED. WE WON'T WORRY ABOUT IT.

DEFINITIONS

FUNCTIONALITY. A SECRET SHARING SCHEME IS A PAIR OF ALGORITHMS (Share, Rec) WHERE Share IS A RANDOMIZED ALGORITHM THAT TAKES INPUT s AND PRODUCES SHARES $x_1, \ldots, x_n$ S.T.

FOR ALL s, $Rec(Share(s)) = s$ WITH PROBABILITY 1.

IN EXAMPLE: $Rec(x_1, x_2, x_3) = x_1 + x_2 + x_3 \mod 2$.

SECURITY.

ATTEMPT. NO TWO PARTIES CAN RECOVER s.... MAYBE CAN DEDUCE $s=0$ W/P 60%, 1 W/P 40%.

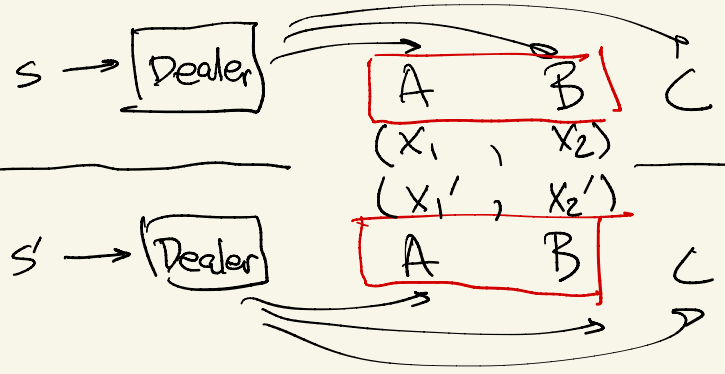
1 TIME OK... BUT INSECURITIES ACCUMULATE

MUCH BETTER IF: NO TWO PARTIES CAN GET ANY INFORMATION ABOUT THE SECRET.

CAN DEFINE "NO INFORMATION" WITHOUT DEFINING "INFORMATION."

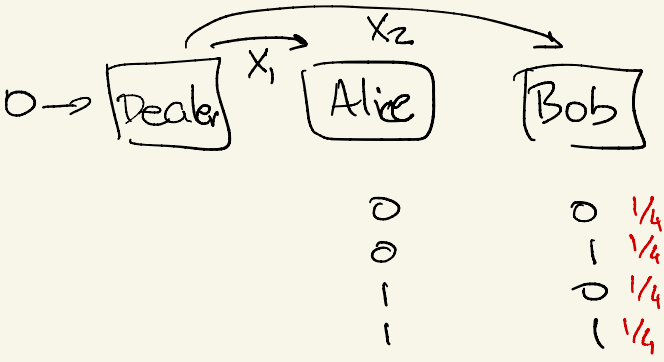
TWO PARADIGMS: INDISTINGUISHABILITY, SIMULATABILITY.

IND-SECURITY FOR SEC SHARING

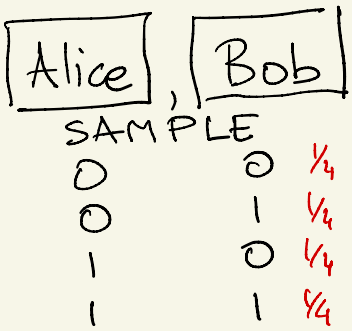


(Share, Rec) IS IND-SECURE IF FOR EVERY PROPER SUBSET S OF THE PARTIES AND EVERY TWO SECRETS s, s', THE R.V.S $(X_i)_{i \in S}$ AND $(X_i')_{i \in S}$ ARE IDENTICALLY DISTRIBUTED WHERE $X_1, \ldots, X_n$ ARE Share(s) AND $X_1', \ldots, X_n'$ ARE Share(s').

REAL EXECUTION



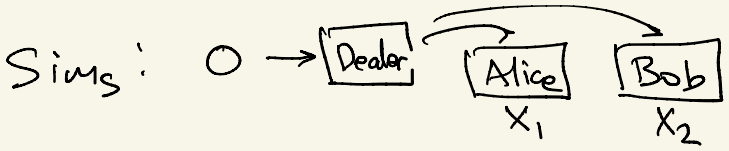
SIMULATION



(Share, Rec) IS SIM-SECURE IF $\forall$ PROPER S, $\exists$ RANDOMIZED ALGORITHM Sim_S (THE SIMULATOR) S.T. $\forall$ SECRETS s, THE OUTPUT OF Sim_S IS IDENTICALLY DISTRIBUTED TO $(X_i)_{i \in S}$ WHERE $(X_1, \ldots, X_n) = Share(s)$.

Prop. (Share, Rec) IS IND-SECURE IF AND ONLY IF IT IS SIM-SECURE.

Proof Sketch. IND $\longrightarrow$ SIM: RUN DEALER USING $s=0$ AS SECRET AND OUTPUT $(X_i)_{i\in S}$.



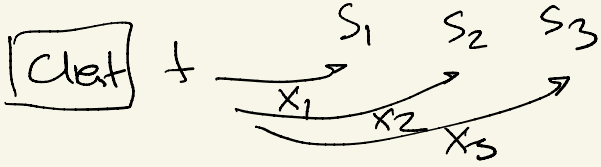
SIM $\longrightarrow$ IND: Sim$_S$ IS IDENTICALLY DISTRIBUTED TO BOTH $(X_1, X_2) \leftarrow$ Share(s) AND $(X_1', X_2') \leftarrow$ Share(s'), SO (X_1, X_2) AND (X_1', X_2') ARE IDENTICALLY DISTRIBUTED TO EACH OTHER.

SECRET SHARING

SPLIT s AMONG n PARTIES

Share(s) : SAMPLE $X_1, \ldots, X_n \sim \{0,1\}$
CONDITIONED ON $X_1 + \cdots + X_n = s$

Rec$(x_1, \ldots, x_n) = x_1 + \cdots + x_n \pmod 2$



EXTEND SEC SHARING TO ALLOW RECONSTRUCTION BY A SUBSET.

- ALLOW SOME PARTIES TO "FORGET" SHARES.

GAME : n PARTIES, "BUDGET" $n-r$

Adv → Protocol: s

Protocol RUNS Share(s)

Protocol → Adv: $X_1, \ldots, X_n$ (1)

Adv: (2) REPLACE $n-r$ X_i BY $\perp$

Adv → Protocol: $\hat{X}_1, \ldots, \hat{X}_n$

Protocol: Rec$(\hat{X}_1, \ldots, \hat{X}_n)$

↓

GUESS $\tilde{s}$ FOR s.

(Share, Rec) IS AN r-THRESHOLD SCHEME IF FOR EVERY ADVERSARY, $\tilde{S}=S$ WITH PROBABILITY 1.

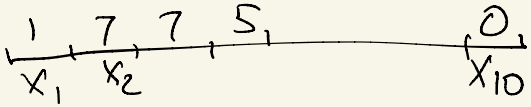
$Share(s) = (X_1=s, X_2=s, \ldots, X_n=s)$

IS A $(n-1)$-THRESHOLD SCHEME... NOT SECURE

(Share, Rec) IS t-SECURE IF IND/SIM-SECURITY HOLDS AGAINST SETS OF SIZE t OR LESS.

Thm. THERE IS AN r-THRESHOLD, $(r-1)$-SECURE SCHEME FOR EVERY $1 \le r \le n$.
SECRET & SHARES TAKE VALUES IN SOME ALPHABET OF SIZE $> n$ THAT IS A POWER OF A PRIME.

Ex. $n=10$, $r=7$, $t=6$ → CAN CHOOSE TO WORK OVER ALPHABET $\{0, \ldots, 10\}$ (SIZE 11).

$s \in \{0, \ldots, 10\}$ $\xrightarrow{\text{share}}$ 

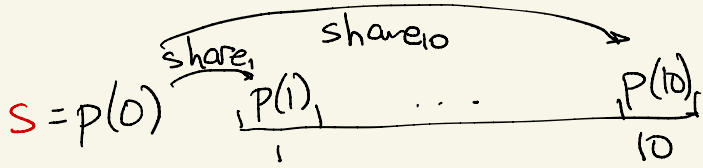
CONSTRUCTION: $\{0, \dots, 10\} = \mathbb{F}_{11}$ $(+, \times, \div \bmod 11)$.

Share(s): DEALER CHOOSES RANDOM VALUES $s_1, \dots, s_6 \sim \mathbb{F}_{11}$ AND CREATES THE POLYNOMIAL

$$p(x) = s + s_1 x + s_2 x^2 + \dots + s_6 x^6.$$

SECRET — RANDOMNESS

HE SETS $\text{share}_i = p(i)$.



RECONSTRUCTION: Adv ELIMINATED 3 SHARES

TASK: RECONSTRUCT s FROM $p(x_1), \dots, p(x_7)$

Claim. GIVEN ANY DISTINCT $x_1, \dots, x_7 \in \mathbb{F}_{11}$ AND ANY $\text{share}_1, \dots, \text{share}_7 \in \mathbb{F}_{11}$ THERE IS A UNIQUE p OF DEGREE 6 S.T. $p(x_i) = \text{share}_i$.

UNIQUENESS PROOF. IF $p(x_i) = p'(x_i) = \text{share}(x_i)$ FOR 7 x_i THEN $p - p'$ IS A DEGREE-6 POLYNOMIAL WITH 7 ROOTS, SO IT MUST BE 0, I.E., $p = p'$

FOR EXISTENCE, THERE ARE 11^7 POLYNOMIALS OF DEGREE 6 AND 11^7 POSSIBLE VALUES FOR $(p(x_1), \dots, p(x_7))$ SO THERE MUST BE ONE FOR EVERY 7-TUPLE OF VALUES.

TO RECONSTRUCT, FIND (UNIQUE) p THEN DERIVE $s = p(0)$.

SECURITY. WE ARGUE $p(x_1), \ldots, p(x_6)$ CAN BE SIMULATED WITHOUT KNOWING s.

INTUITION FOR 1-SECURITY: $p(1) = s + s_1 + \ldots + s_6$ IS UNIFORMLY RANDOM mod 11 (FOR ALL s)
$p(2) = s + 2s_1 + \ldots + 2^6 s_6$ IS ALSO UNIFORMLY RANDOM; EVEN FOR FIXED $s, s_2, \ldots, s_6$, $2s_1$ "COVERS" ALL OF $\mathbb{F}_{11}$.

r-SECURITY $\forall$ share$(x_1), \ldots,$ share(x_6) THERE IS A UNIQUE p CONSISTENT WITH $p(x_1) =$ share(x_1), $\ldots, p(x_{r-1}) =$ share(x_6) AND $p(0) = s$

SO A RANDOM p CONDITIONED ON $p(0) = s$ IS EQUALLY LIKELY TO GIVE ALL POSSIBLE 6-TUPLES OF SHARES (share$(x_1), \ldots,$ share(x_6)).

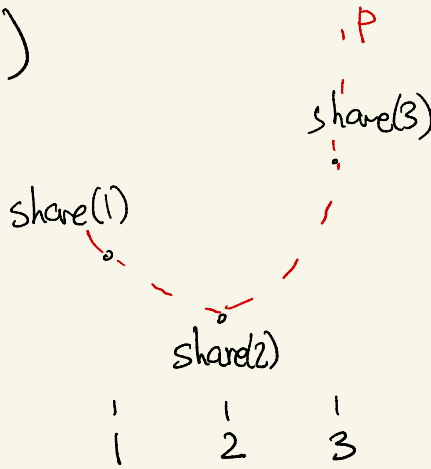
TO SIMULATE (WITHOUT KNOWING s), SAMPLE UNIFORM, INDEPENDENT VALUES FOR THE 6 SHARES.

Ex. $n=10$, $r=3$ $\pmod{11}$

$p(1) = s + s_1 + s_2$

$p(2) = s + 2s_1 + 4s_2$

$p(3) = s + 3s_1 + 9s_2$



TO RECONSTRUCT, SOLVE FOR s, s_1, s_2 GIVEN $p(1), p(2), p(3)$ (IN mod 11 ARITHMETIC) → INTERPOLATION PROBLEM

SECRECY FOR PARTIES 1&3 HOLDS BECAUSE FOR ANY s, EACH PAIR OF VALUES FOR $(p(1), p(3))$ ARISES FROM EXACTLY ONE CHOICE OF (s_1, s_2)