On the Foundations of Modern Cryptography

Oded Goldreich
Weizmann Institute

IT IS POSSIBLE
TO BUILD A CABIN
WITH NO FOUNDATIONS,
BUT NOT A LASTING BUILDING.

ENG. I. GOLDREICH
(1906-1995)

THE NATURE OF CRYPTOGRAPHY

~ MAINTAINING DESIRED FUNCTIONALITY IN FACE OF ADVERSERIAL BEHAVIOR (TRANSENDING DESIGNER'S IMAGINATION).

Ad-hoc approaches & Heuristics are hardly justified when designer has a good idea about expected behavior.

THE NATURE OF CRYPTOGRAPHY

~ MAINTAINING DESIRED FUNCTIONALITY IN FACE OF ADVERSERIAL BEHAVIOR (TRANSENDING DESIGNER'S IMAGINATION).

Ad-hoc approaches & Heuristics are hardly justified when designer has a good idea about expected behavior.

NEED FIRM FOUNDATIONS!

PROVIDING FIRM FOUNDATIONS FOR CRYPTO'

- DEFINITIONAL ACTIVITY

  IDENTIFY, CONCEPTUALIZE, & DEFINE

  CRYPTOGRAPHIC TASKS

  CAPTURING NATURAL SECURITY CONCERNS.

- CONSTRUCTIVE ACTIVITY

  STUDY & DESIGN CRYPTO' SCHEMES

  SATISFYING THE ABOVE DEF'S.

- OTHER ACTIVITIES

  E.G., EXPLORATIVE { - PROPOSE DIRECTIONS
  - MARK LIMITATIONS.

DEFINITIONAL ACT' – EXAMPLE: <u>SECURE</u> ENC.

- What is there to define ?

[GM]
↓
- IS IT OK FOR A "SECURE ENCRYPTION" TO LEAK THE 1^{ST} BIT OF PLAINTEXT ?

⇒ REJECT THE NAIVE FORMULATION

SECURE ⇔ INFEASIBLE TO OBTAIN PLAINTEXT FROM CIPHERTEXT.

BTW, NAIVE FORM' REFERS TO...

... UNIFORMLY DISTR. PLAINTEXT

AND THUS, "DOUBLLY INADEQUATE"...

[illegible]

SEMANTIC SECURITY

overlap { – example
– rephrasing def.

SECURE ENCRYPTION – DEFINITION [GM]

COMPUTAT' ANALOG' OF SHANNON'S "PERFECT SECRECY"

IT IS INFEASIBLE TO OBTAIN (FROM CIPHERTEXT) ANY "NON-OBVIOUS" INFORMATION REGARD' PLAINTEXT, where "OBVIOUS" IS WHATEVER CAN BE EFFICIENTLY COMPUT' A-PRIORI.

COMMENT: NO DETERMINSTIC ENCRYPTION CAN SATISFY THIS DEFINITION.

by Deterministic Encryption
I mean Deter. Encryption algorithm
... not the key-gen ...

SEMANTIC SECURITY

overlap { - example
- negligible def.

SECURE ENCRYPTION – DEFINITION [GM]

COMPUTAT' ANALOG' OF SHANNON'S "PERFECT SECRECY"

IT IS INFEASIBLE TO OBTAIN (FROM CIPHERTEXT) ANY "NON-OBVIOUS" INFORMATION REGARD' PLAINTEXT, where "OBVIOUS" IS WHATEVER CAN BE EFFICIENTLY COMPUT' A-PRIORI.

$\Rightarrow$

EVERY FUNCTION OF PLAINTEXT WHICH CAN BE EFF' GUESSED FROM CIPHER' CAN BE EFF' GUESS' AS WELL FROM NOTHING.

COMMENT: NO DETERMINSTIC ENCRYPTION CAN SATISFY THIS DEFINITION.

by Deterministic Encryption
I mean Deter. Encryption algorithm
... not the key-gen....

SEMANTIC SECURITY

overlap { – example
– rephrasing def.

SECURE ENCRYPTION – DEFINITION [GM]

COMPUTAT' ANALOG' OF SHANNON'S "PERFECT SECRECY"

IT IS INFEASIBLE TO OBTAIN (FROM CIPHERTEXT) ANY "NON-OBVIOUS" INFORMATION REGARD' PLAINTEXT, where "OBVIOUS" IS WHATEVER CAN BE EFFICIENTLY COMPUT' A-PRIORI.

e.g.,

SUPPOSE $\Pr[\text{1ST BIT OF PLAINTEXT} = 0] = 1/3$

THEN, GIVEN CIPHERTEXT, YOU CAN GUESS 1ST BIT OF PLAINTEXT W.P. 2/3, BUT NOT BETTER.

Example

COMMENT: NO DETERMINISTIC ENCRYPTION CAN SATISFY THIS DEFINITION.

by Deterministic Encryption
I mean Deter. Encryption algorithm

INDIST OF ENCRYPT

Overlap { - example for DET failing
- did we ask too much?

SECURE ENC' – AN EQUIV. DEF. [GM]

IT IS INFEASIBLE TO DISTINGUISH ENCRYPTIONS OF ANY TWO MESSAGES. (EVEN WHEN MESSAGES ARE KNOWN!)

- EQUIVALENT TO PREVIOUS DEFINITION.
- NO (PUBLIC-KEY) ENCRYPTION SCHEME WITH DETERMINISTIC ENCRYPT' ALGORITHM CAN SATISFY THESE DEFINITIONS.

E.G., GIVEN ENCRYPTION-KEY (e), IT IS EASY TO DISTINGUISH $E_e(0)$ FROM $E_e(1)$.

INDIST OF ENCRYPT

Overlaps { - example for DET failing
- did we ask too much?

SECURE ENC' – AN EQUIV. DEF. [GM]

IT IS INFEASIBLE TO DISTINGUISH ENCRYPTIONS OF ANY TWO MESSAGES. (EVEN WHEN MESSAGES ARE KNOWN!)

- EQUIVALENT TO PREVIOUS DEFINITION.
- NO (PUBLIC-KEY) ENCRYPTION SCHEME WITH DETERMINISTIC ENCRYPT' ALGORITHM CAN SATISFY THESE DEFINITIONS.

- DID "WE" ASK FOR TOO MUCH ?
- PROBABILISTIC ENCRYPTION CAN/DOES SATISFY THE DEFINITIONS.

SECURE ENCRYPTION – DEF'S (TECHNICAL)

(G,E,D) = A PUB-KEY ENCRYPTION SCHEME.

$\forall$ EFFICIENT A $\exists$ EFF' A'

$\forall f: \{0,1\}^* \to \{0,1\}^*$ $\forall$ PROB' ENS' $\{X_n\}$

$$Pr[A(e, E_e(X_n)) = f(x_n)]$$

$$< Pr[A'(e, |X_n|) = f(x_n)] + \underline{neg}(n)$$

WHERE $e = G(1^n)$.

OR $A'(1^n)$

$\forall$ EFF' A $\forall$ $\{(a_n, b_n)\}$

$$\left| Pr[A(e, E_e(a_n)) = 1] - Pr[A(e, E_e(b_n)) = 1] \right|$$

$$< \underline{neg}(n)$$

CONSTRUCTIVE ACTIVITY – EXAMPLE:

SECURE ENCRYPTION

- GIVEN ANY TRAPDOOR PERMUTATION, CAN CONSTRUCT SECURE PUBLIC-KEY ENCRYPTION. [GM] [Y]

- IN PARTICULAR, ASSUMING FACTORING HARD, ∃ SECURE PUBLIC-KEY ENCRYPTION (ESSENTIALLY) AS EFFICIENT AS RSA. [BG]

  – "PLAIN RSA" IS NOT SECURE.

  – "RANDOMIZED RSA" MAY BE SECURE.

  – RSA CAN BE TRANSFORMED INTO A SECURE ENCRYPTION.

ON RSA – CLARIFICATIONS

- **THE ONE-WAY ASSUMPTION (OWA)**

  RSA IS HARD TO INVERT (UNDER UNIFORM DISTRIBUTION). ✓

- **PLAIN RSA IS NOT SECURE**

  E.G. $JS(RSA(m)) = JS(m)$ ✗

- **RANDOMIZED RSA** $n = |N|$

  TO ENCRYPT $m \in \{0,1\}^{n/2}$,

  SELECT $r \in_R \{0,1\}^{n/2}$ & OUTPUT $RSA_{e,N}(r \circ m)$

CONJ: OWA $\Rightarrow$ RANDRSA IS SECURE.

KNOWN TO HOLD IF ENCRYPT $m \in \{0,1\}^{\log n}$

BY $r \in_R \{0,1\}^{n - \log n}$ & OUTPUT $RSA_{e,N}(r \circ m)$

[ACGS]

THE BLUM-GOLDWASSER ENCRYPT' SCHEME

- FACTORING HARD $\Rightarrow$ SECURITY
- EFFICIENCY $\approx$ AS RSA.

PRIVATE KEY PRIMES p, q S.T. $p \equiv q \equiv 3 \pmod 4$

PUBLIC KEY THE PRODUCT $N = p \cdot q$. ($n = |N|$)

ENCRYPTION OF MESSAGE $x \in \{0,1\}^n$

- $s_0 \in_R Z_N$
- FOR $i = 1, \ldots, n$

  $\sigma_i \leftarrow LSB(s_{i-1})$ & $s_i \leftarrow (s_{i-1}^2 \bmod N)$
- OUTPUT CIPHERTEXT $(\sigma_1 \cdots \sigma_n \oplus x, s_n)$.

DECRYPTION OF CIPHERTEXT (y, s_n)

- $s_0 \leftarrow (s_n^d \bmod N)$, WHERE $d \leftarrow 2^{-n} \bmod \phi(N)$.
- RECOVER σ_i'S AND MESSAGE.

PAUSE

QUESTIONS ?

DEFINITIONAL ACTIVITY
– PSEUDO RANDOM GENERATORS

REPLACING ad-hoc NOTIONS SUCH AS

- PASSING TESTS LISTED IN KNUTH VOL. 2
- HAVING HIGH LINEAR (F.S.R) COMPLEXITY

BY THE ROBUST NOTION OF

> BEING COMPUTATIONALLY INDISTINGUISH' FROM THE UNIFORM DISTRIBUTION.

$\Leftrightarrow$ [BM, Y]

> INFEASIBLE TO PREDICT THE NEXT BIT (WITH SUCCESS PROB' $> \frac{1}{2}$)

"stream cipher"

PRG - DEFINITION (TECHNICAL)

- $G: \{0,1\}^n \to \{0,1\}^{2n}$ EFFICIENTLY COMPUT'

$\forall$ EFFICIENT A

$$\left| Pr[A(G(U_n)) = 1] - Pr[A(U_{2n}) = 1] \right| < neg(n)$$

$U_\ell \equiv$ UNIFORM OVER $\{0,1\}^\ell$.

CONSTRUCTIVE ACTIVITY – PRG

- GIVEN ANY ONE-WAY PERMUTATION, CAN CONSTRUCT A PRG. [BM, GL]

  EFFICIENCY VARIES –
  ONE→MANY PR-BITS PER OW-COMPUTATION.

- MORE EFFICIENT CONSTRUCTIONS BASED ON SPECIFIC HARD PROBLEMS. [IN]

- $\exists$ OW FUNCTIONS $\Rightarrow$ $\exists$ PRG. [HILL]
  ("plausibility result")

- PRG $\Rightarrow$ OW FUNCTIONS. [L]

PSEUDORANDOM FUNCTIONS [GGM]

$F_n = \{ f_s : \{0,1\}^n \to \{0,1\}^n \}_{s \in \{0,1\}^n}$ EFFICIENT EVAL$(s,x) = f_s(x)$.

- $\{F_n\}$ IS PSEUDORANDOM IF

> IT IS INFEASIBLE TO DISTINGUISH REPLIES BY $f_s \in_R F_n$ FROM REPLIES BY RANDOM $f : \{0,1\}^n \to \{0,1\}^n$.

- PRG $\Rightarrow$ PRF. (ALTERNATIVES BY [NR])
- PRF IS A POWERFUL TOOL.

  E.G. PRIVATE-KEY ENCRYPTION

  KEY = SEED/DESCRIPTION OF $f \in F_n$ (PRF)

  ENCRYPT MESSAGE $x \in \{0,1\}^n$

  - $r \in_R \{0,1\}^n$
  - OUTPUT CIPHERTEXT $(r, f(r) \oplus x)$.

DEFINITIONAL ACTIVITY – SIGNATURES

- CHOSEN MESSAGE ATTACK. ✓

WHAT DOES IT MEAN "TO FORGE"?

EXISTENTIAL FORGERY [GMR:]

> PRODUCE A SIGNATURE TO ANY NEW MESSAGE.

DEFINITIONAL ACTIVITY – SIGNATURES

– CHOSEN MESSAGE ATTACK. ✓

WHAT DOES IT MEAN "TO FORGE"?

EXISTENTIAL FORGERY [GMR:]

> PRODUCE A SIGNATURE TO ANY NEW MESSAGE.

IS IT "TOO CAUTIOUS"?

- WE WANT AN APPLICATION-INDEPENDENT NOTION OF SECURITY.
- EVEN IN A SPECIFIC APPLICATION, IT IS "IMPPOSIBLE" TO IDENTIFY "THE IMPORTANT MESSAGES".
- IN SOME APPLICATIONS (e.g. SIGNING SERIAL #S) EXIST-FORGERY DOES CAUSE DAMAGE.

CONSTRUCTIVE ACTIVITY – SIGNATURES

- SECURE SIGNATURES CONSTRUCTED UNDER FACTORING/RSA ASSUMPTION. [GMR:] [DN, CD]
  EFFICIENCY – VARYING ("5 TIMES SLOWER" THAN RSA)

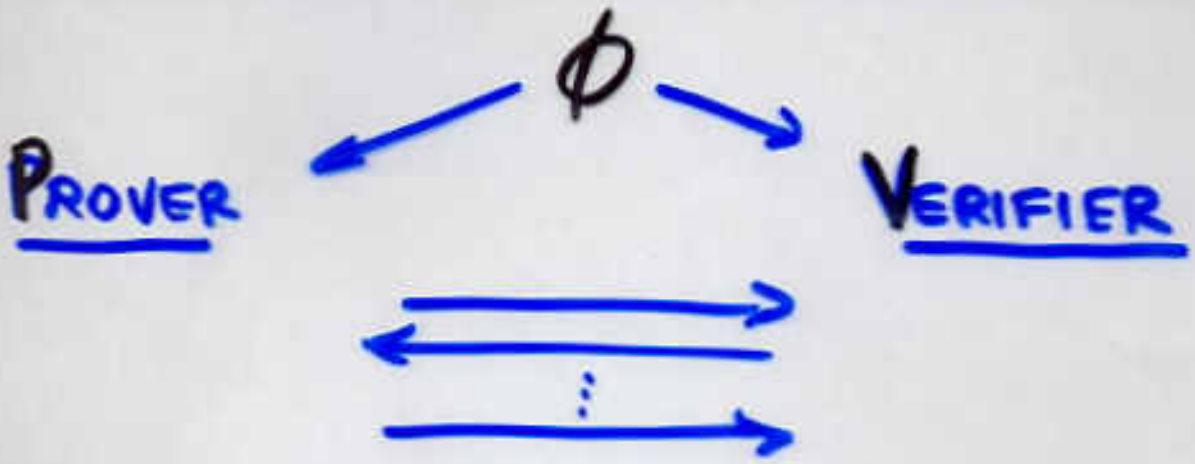
- $\exists$ OW FUNCTIONS $\Rightarrow$ $\exists$ SIGNATURES. [R]

- USEFUL PARADIGMS
  - REFRESHING OF KEYS. ("RANDOMIZATION
  - TREE AUTHENTICATION
  - HASHING (UOWHF [NY])

PAUSE
(#2)

FOR ME...

ZERO KNOWLEDGE [GMRa]



- INTERACTIVE PROOF SYSTEM

ϕ VALID $\Rightarrow$ $Pr[V \text{ ACCEPTS}] > 1 - neg.$

ϕ $\neg$VALID $\Rightarrow$ $Pr[V \text{ ACCEPTS}] < neg.$

- ZERO-KNOWLEDGE

WHATEVER CAN BE EFFICIENTLY COMPUTED AFTER INTERACT' WITH P ON ϕ

CAN BE EFFICIENTLY COMPUT' FROM ϕ ITSELF.

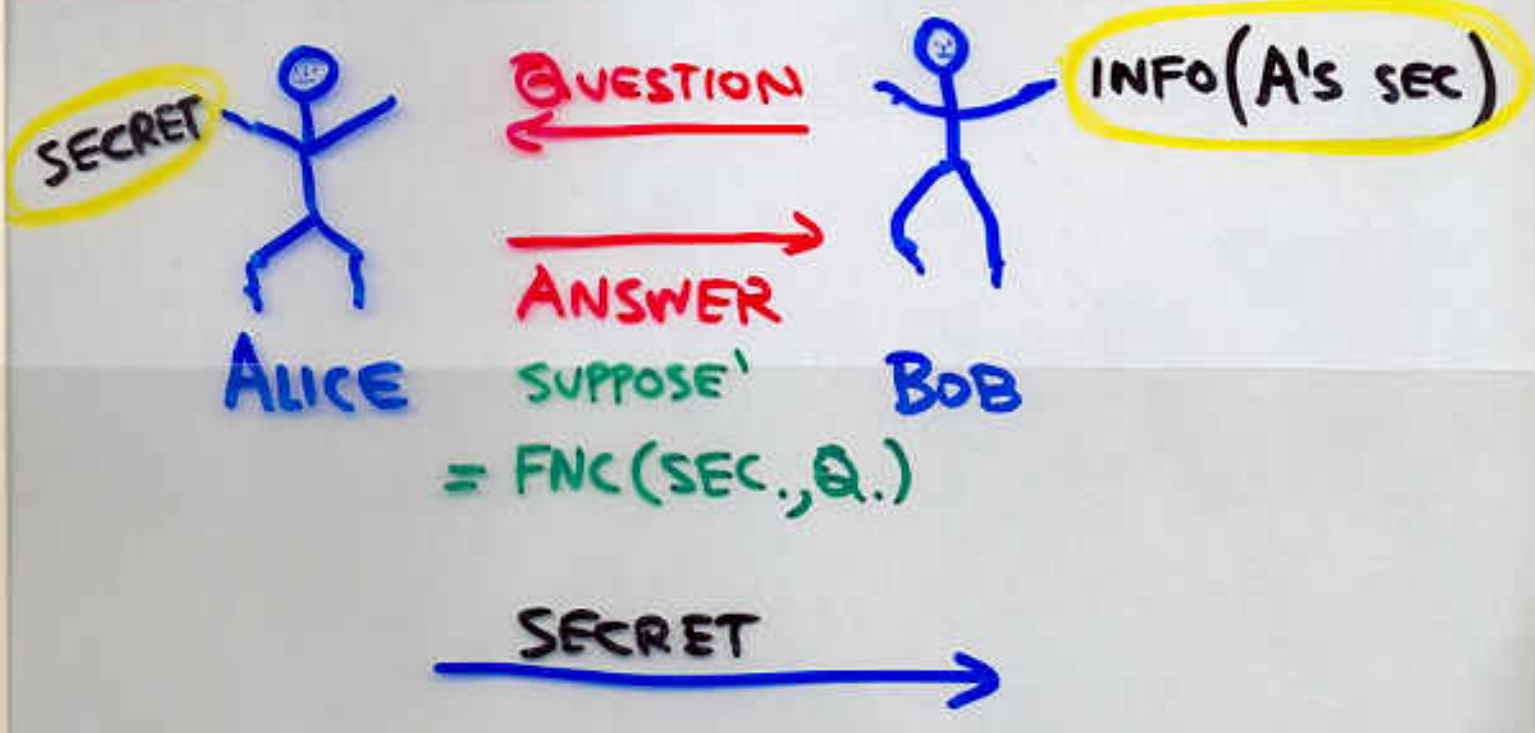
paradox? → only gain confidence!

plausibility res

ZK - A GENERAL PLAUSIBILTY RESULT

∃ OW FUNCTIONS $\overset{[HILL]}{\Rightarrow}$ ∃ PRG $\overset{[N]}{\Rightarrow}$ COMMITMENT SCHEMES

$\overset{[GMW]}{\Rightarrow}$ EVERY NP-ASSERTION CAN BE EFFICIENT' PROVEN IN Z.K.



SUPPOSE' = FNC(SEC., Q.)

SECRET →

BOB CAN CHECK

(1) MATCHES INFO

(2) ANS = F(SEC., Q.)

BOB IS OK. ✓

BUT, DOES NOT PROTECT A's INTERESTS...

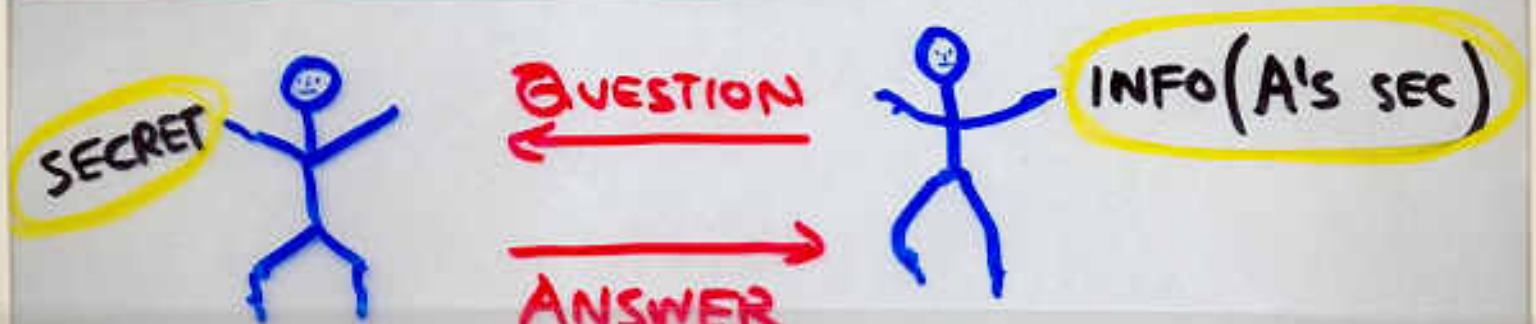
— NP-assertion
— plausibility

plausibility ??

ZK – A GENERAL PLAUSIBILTY RESULT

∃ OW FUNCTIONS $\overset{[HILL]}{\Rightarrow}$ ∃ PRG $\overset{[N]}{\Rightarrow}$ COMMITMENT SCHEMES

$\overset{[GMW]}{\Rightarrow}$ EVERY NP-ASSERTION CAN BE EFFICIENT' PROVEN IN Z.K.



SUPPOSE' = FNC(SEC., Q.)

ZK PROOF THAT

∃ SEC. S.T.

(1) MATCHES INFO

(2) ANS = F(SEC, Q.)

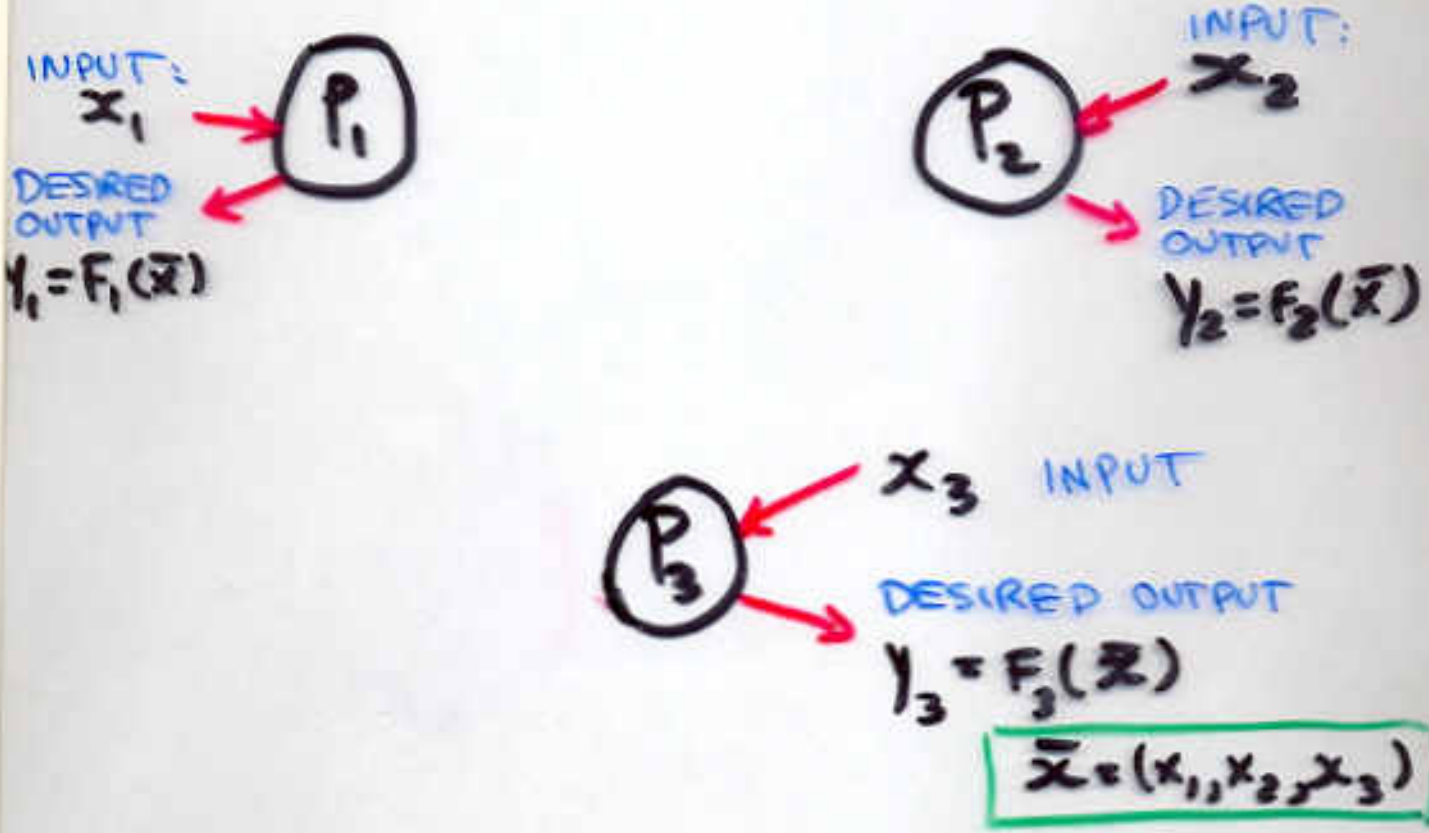
✓ ALICE MAINTAINS HER SECRET.

BOB IS CONVINCED ✓

– NP-assertion
– plausibility

SECURE MULTI-PARTY PROTOCOLS FOR ANY FUNCTIONALITY [GMW2]

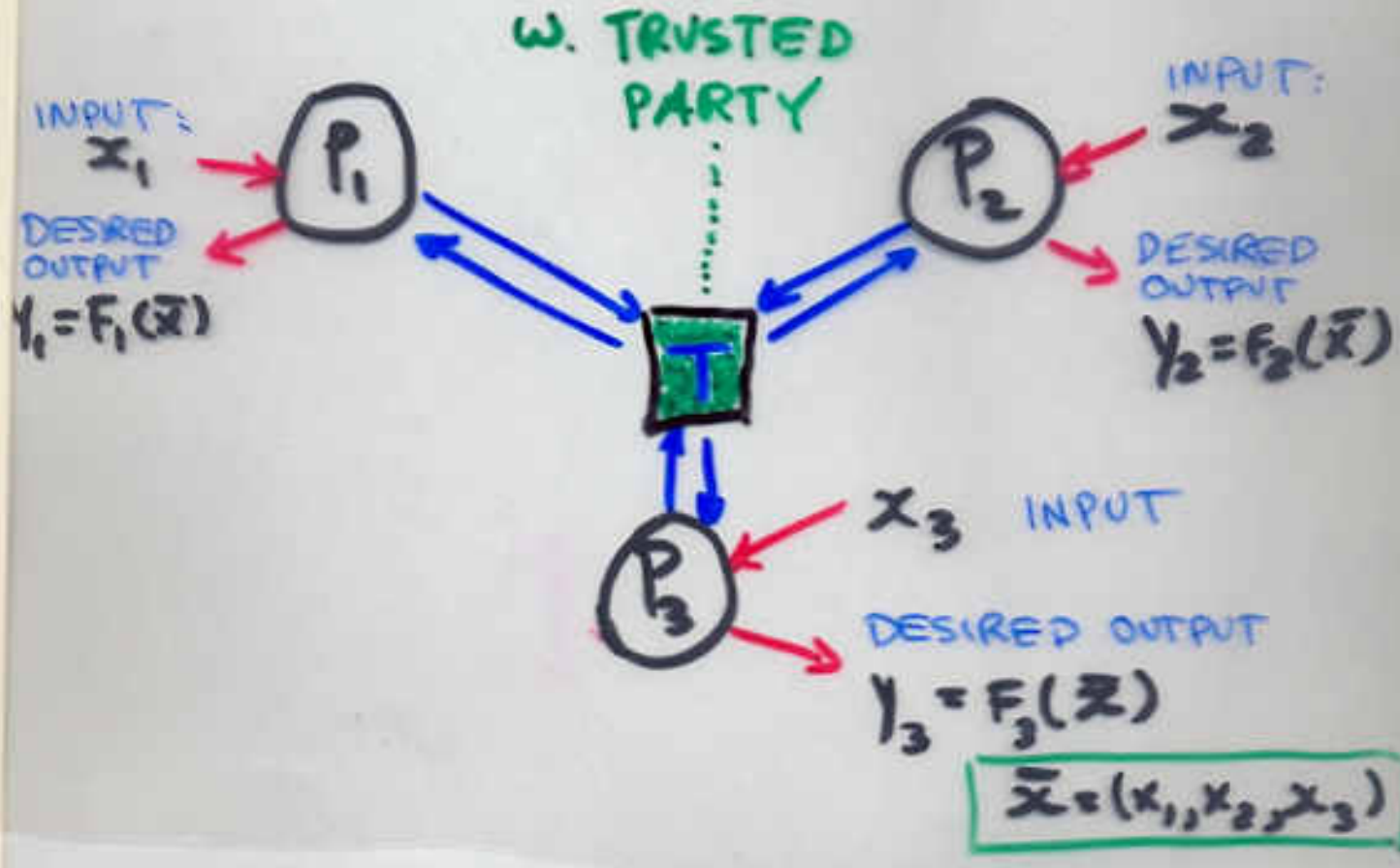
- $\{F_i\}_{i=1}^{3}$ = DESIRED FUNCTIONALITY.



- F_i's MAY BE PROBABILISTIC
- CAN BE EXTENDED TO ITERACTIVE TASKS

SECURE MULTI-PARTY PROTOCOLS FOR ANY FUNCTIONALITY [GMW2]

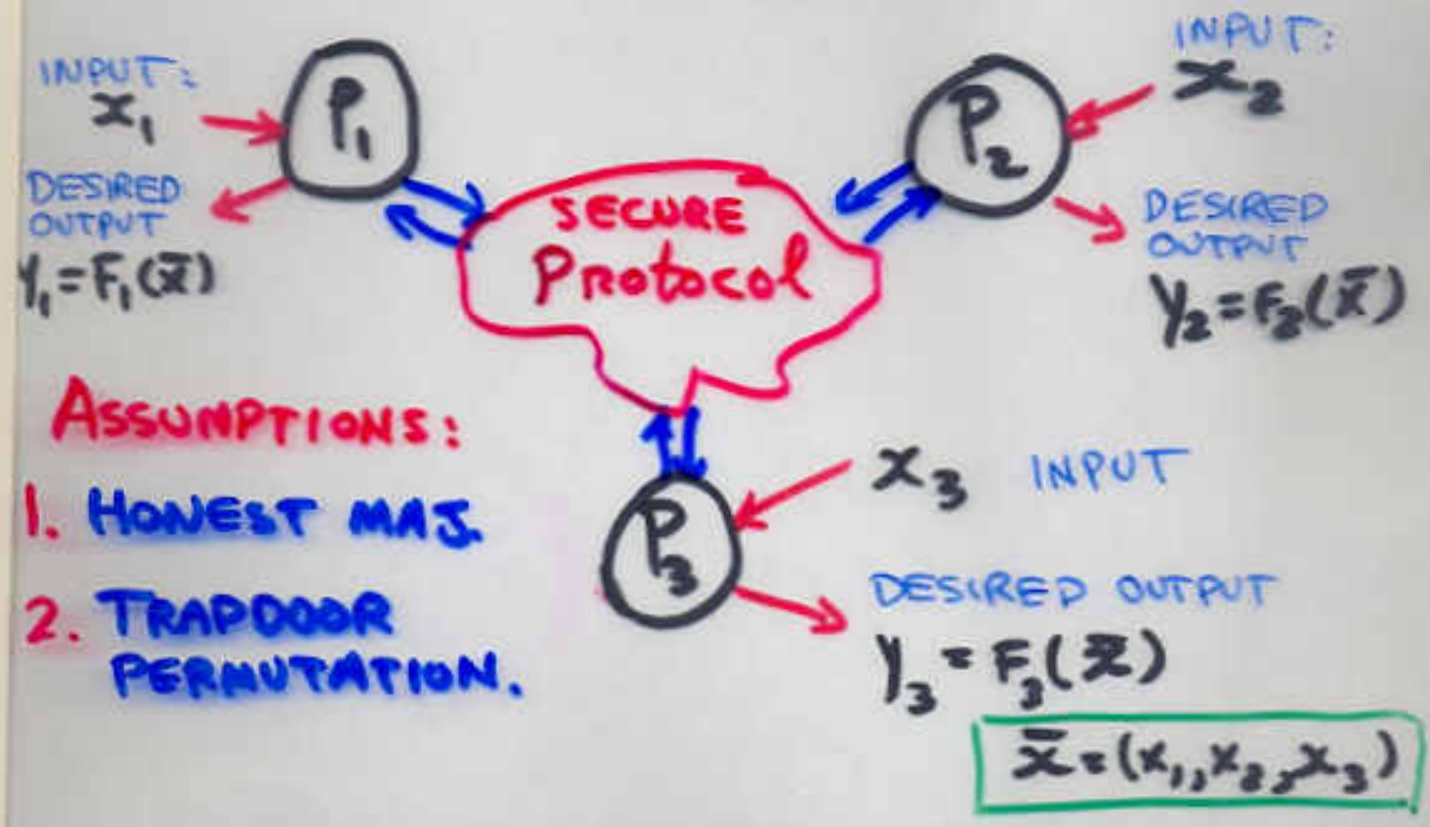
- $\{F_i\}_{i=1}^{3}$ = DESIRED FUNCTIONALITY.



- F_i's MAY BE PROBABILISTIC
- CAN BE EXTENDED TO ITERACTIVE TASKS.

SECURE MULTI-PARTY PROTOCOLS FOR ANY FUNCTIONALITY [GMW2]

- $\{F_i\}_{i=1}^{3}$ = DESIRED FUNCTIONALITY.



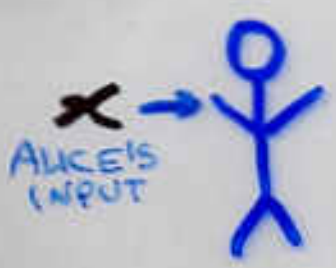
ASSUMPTIONS:

1. HONEST MAJ.
2. TRAPDOOR PERMUTATION.

- F_i's MAY BE PROBABILISTIC
- CAN BE EXTENDED TO ITERACTIVE TASKS

SECURE TWO-PARTY PROTOCOLS WITH EARLY STOPPING [Y2]

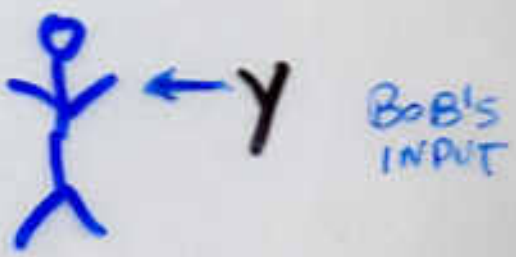
- **ANY** FUNCTIONALITY $F, G : (\{0,1\}^*)^2 \to \{0,1\}^*$.
- OUTPUT "SIMULTANEOUSLY" – IMPOSSIBLE [C].



ALICE

DESIRED OUTPUT

$F(x,y)$



BOB

DESIRED OUTPUT

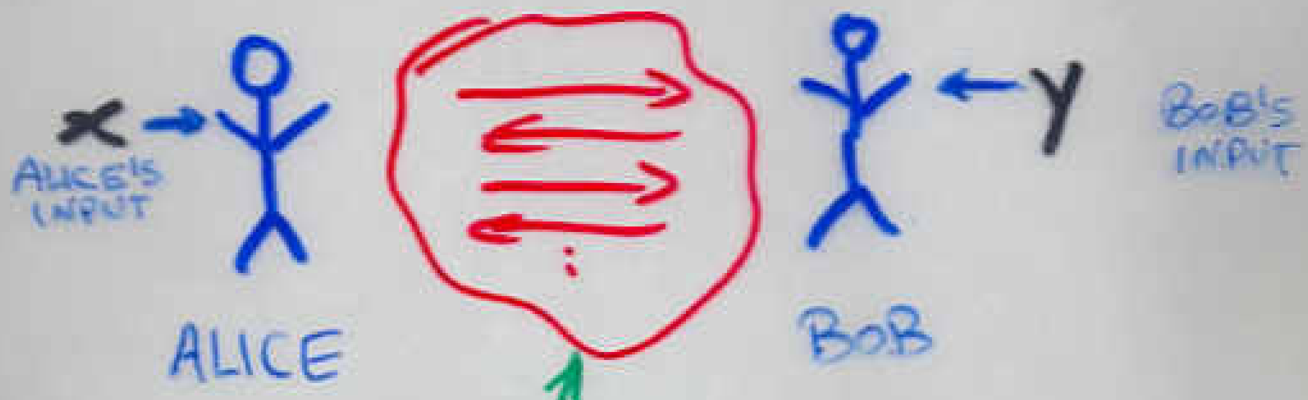
$G(x,y)$

OR $\perp \triangleq$ "ALICE HAS ABORTED."

(plausibility)

SECURE TWO-PARTY PROTOCOLS WITH EARLY STOPPING [Y2]

- **ANY** FUNCTIONALITY $F, G : (\{0,1\}^n)^2 \to \{0,1\}^n$.
- OUTPUT "SIMULTANEOUSLY" – IMPOSSIBLE [C].



DESIRED OUTPUT

$F(x,y)$

DESIRED OUTPUT

$G(x,y)$

OR $\perp$ ≙ "ALICE HAS ABORTED."

SECURE PROTOCOL

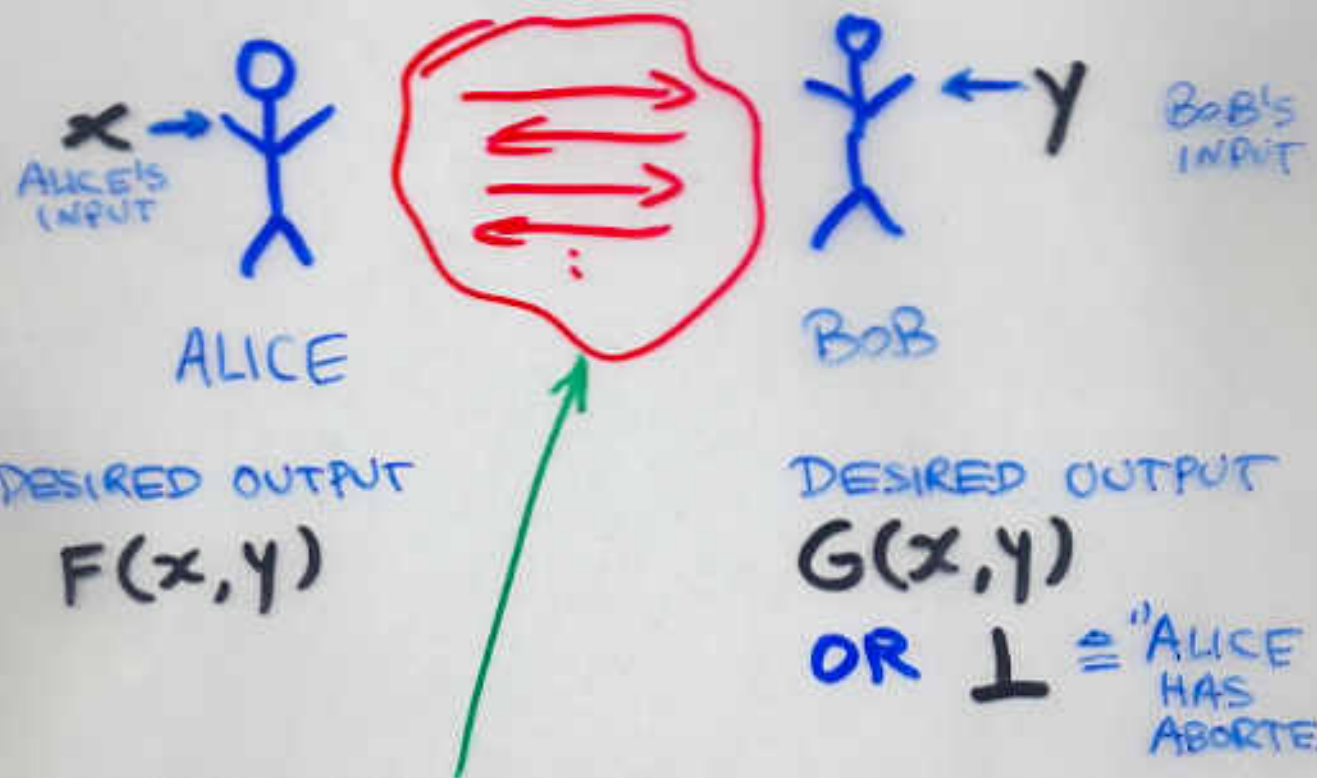
USING ANY TRAPDOOR PERMUTATION.

- ZERO-KNOWLEDGE PROOFS FOR NP AS SPECIAL CASE.

(plausibility)

SECURE TWO-PARTY PROTOCOLS WITH EARLY STOPPING [Y2]

- **ANY** FUNCTIONALITY $F, G : (\{0,1\}^*)^2 \to \{0,1\}^*$.
- OUTPUT "SIMULTANEOUSLY" – IMPOSSIBLE [C].



SECURE PROTOCOL
USING ANY TRAPDOOR PERMUTATION.

- ZERO-KNOWLEDGE PROOFS FOR NP AS SPECIAL CASE.

(plausibility) ...

SOME CONCLUDING REMARKS

- THEORY QUITE INDEPENDENT OF SPECIFIC NOTION OF EFFICIENCY (E.G., ASYMPTOTICS, PPT).
  - RELATIONS BETWEEN NOTIONS/TASKS ARE THE TRUE CONTENTS.
  - "SECURITY" AS QUANTITY.
  - CLASSIFICATION OF RESULTS.

- "TOO CAUTIOUS" DEFINITIONS ?
  - You can never be "too cautious"
  - APPLICATION INDEPENDENCE.
  - "IMPOSSIBILITY" OF DEFINING THE EXACT CONCERNS (EVEN IN SPECIFIC APPLIC.).