Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products

Jonathan Katz (UMD), Amit Sahai (UCLA), Brent Waters (SRI)

Presented by Omkant Pandey (UCLA)

Standard public-key encryption

PK

C

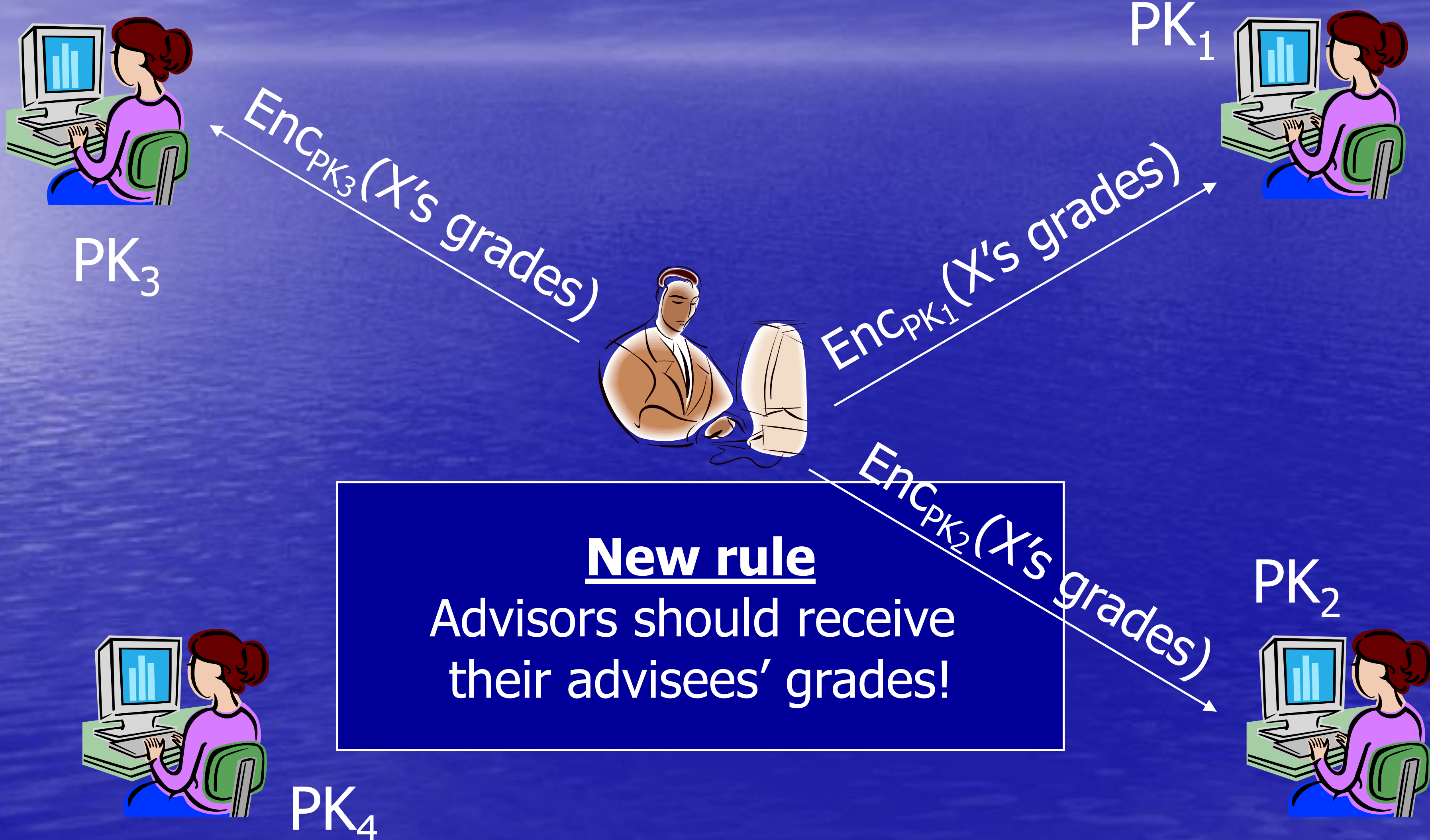
$C \leftarrow \mathrm{Enc}_{PK}(M)$

$(PK, SK) \leftarrow \mathrm{Gen}$

$M = \mathrm{Dec}_{SK}(C)$

No one other than the designated recipient can get any information about the message

Usage in complex environments?



New rule

Advisors should receive their advisees' grades!

Drawbacks to standard PKE

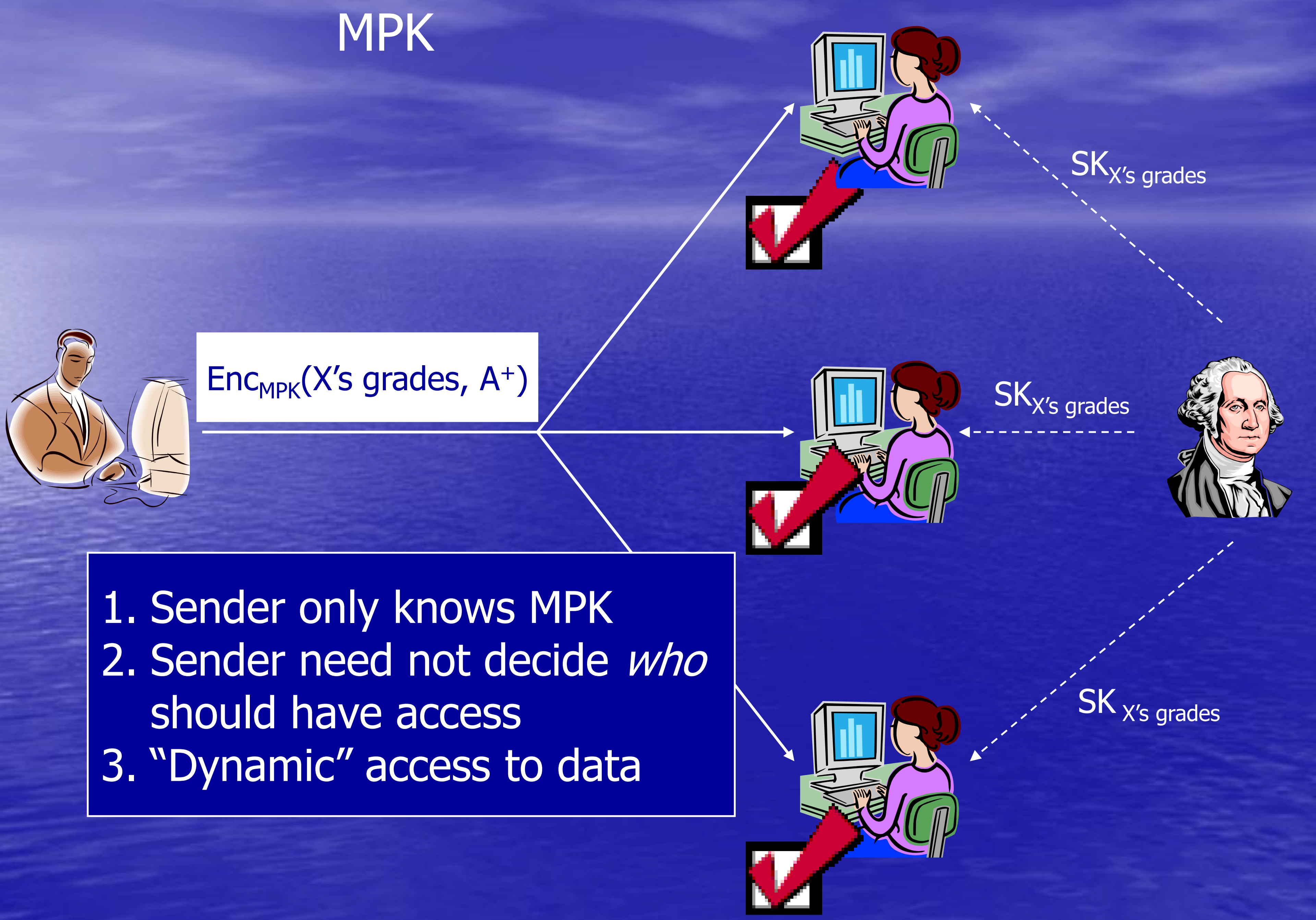
- Senders still have to obtain/store/manage *many users'* public keys
- Sender needs to be *actively involved* in deciding to whom to encrypt
  - Ease of use?
  - Greater potential for security breach
- "*Static*" set of parties who can decrypt
  - Must be provisioned *in advance*

A new approach

- Functional Encryption
- High-level idea:
  - Secret keys associated with “functions”/”capabilities”
  - Ciphertexts associated with “attributes”
  - A secret key decrypts a ciphertext iff function evaluates to 1 on the attribute (i.e., the capability gives the explicit right to decrypt)
- This idea unifies and generalizes line of work initiated by Attribute-Based Encryption [Sahai-Waters 05]

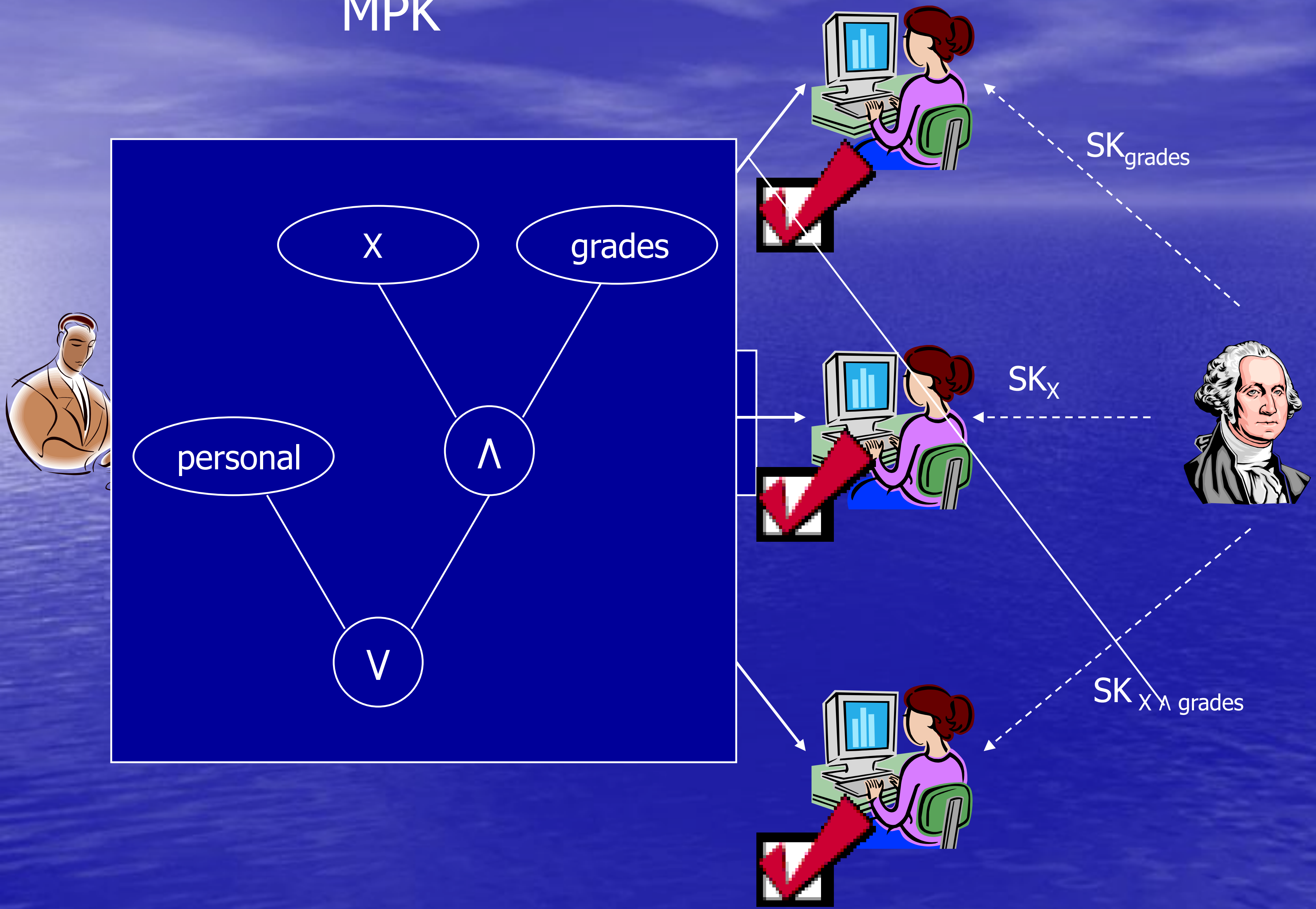
Our Syntax

- Class of functions F; set of attributes Σ
- Algorithms (Gen, Derive, Enc, Dec)
  - $\text{Gen}(1^n)$ outputs MPK, MSK
  - $\text{Derive}_{MSK}(f)$ returns SK_f (where $f \in F$)
  - $\text{Enc}_{MPK}(I, M)$ returns C (where $I \in \Sigma$)
  - $\text{Dec}_{SK_f}(\text{Enc}_{MPK}(I, M))$ returns:
    - M if $f(I) = 1$
    - $\perp$ if $f(I) = 0$



1. Sender only knows MPK
2. Sender need not decide *who* should have access
3. "Dynamic" access to data

MPK



Security – Warm Up (Payload Hiding)

Hide the **message** as long as none of the adversary's capabilities give it the **explicit** right to decrypt

Actual Security: Attr + Payload Hiding

Hide the **message** as long as none of the adversary's capabilities give it the explicit right to decrypt

<u>and</u>

Hide the **attribute** as long as none of the adversary's capabilities give it the explicit ability to distinguish

A framework for existing results

- Framework captures:
  - Identity-based encryption (IBE) [S 84, BF 01, C 01]
  - Forward-secure encryption [CHK 03]
  - Attribute-based encryption [SW 05, GPSW 06, BSW 07]
  - Hidden-vector encryption [BW 07]
  - ..more

E.g., Identity-based encryption

- $\Sigma = \{0,1\}^*$
- $F = \{f_{ID} \mid ID \in \{0,1\}^*\}$, where
  $f_{ID}(ID') = 1$ iff $ID = ID'$
  - I.e., *equality tests*
- Payload hiding = standard IBE
- Attribute hiding = anonymous IBE

This work

- The functional encryption framework
- Attribute-hiding functional enc. for *disjunctions*
  - Previous work handles *conjunctions* only
  - Previous work mainly considers *payload hiding*
- Applications
  - Anonymous IBE; disjunctions of identities
- Generalizations
  - New functional enc. schemes for inner products, poly. evaluation, DNF/CNF formulae; and threshold IBE

Rest of the talk

- Goal: attribute-hiding identity-based encryption with disjunctions

- Generalization: functional encryption supporting “inner product” computations
  - A construction handling “inner product” functions
  - Applications to our goal, and more…

IBE with disjunctions

- $\Sigma = \{0,1\}^*$
- $F = \{f_{I_1, \ldots, I_n} \mid I_1, \ldots, I_n \in \Sigma\}$
- $f_{I_1, \ldots, I_n}(x) = 1$ iff $(x = I_1) \vee \cdots \vee (x = I_n)$

- Alternatively, $\Sigma = (\{0,1\}^*)^n$ and $f_{I_1, \ldots, I_n}(x_1, \ldots, x_n) = 1$ iff

$$(x_1 = I_1) \vee \cdots \vee (x_n = I_n)$$

Why isn't it trivial (given anon IBE)?

- Idea(?): use IBE + (trivial) secret sharing

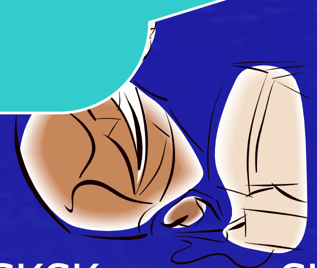
Me
At

Msg: M
Id: BadEval

Msg: M
Id: NewEmp

Can tell whether you were fired for being a "New Employee" or being "Late for Work"

Should only learn that at least one of the two attributes were present in the message.



WANT: $SK_{NewEmp \vee LateForWork}$

NOT ATTRIBUTE HIDING!

Inner product computations

- Let $\Sigma = Z_N^n$
- Let $F = \{f_v \mid v \in Z_N^n\}$, where
  $f_v(x) = 1$ iff $\langle v, x \rangle = 0 \bmod N$

- Why this function…?
  - Extend current state-of-the-art for Functional Encryption
  - Applications…

Polynomial evaluation

The approach also extends to *multivariate* polynomials (complexity grows as $O(d^t)$ for t-variate polynomials of degree at most d in each variable)

Disjunctions

Identity: I
Message: M

Encrypt using the attribute I

$SK_{I_1 \vee I_2}$

SK_p

where $p(x) = (x - I_1)(x - I_2)$

$$p(I) = 0 \Leftrightarrow I \in \{I_1, I_2\}$$

Conjunctions

Extending these ideas, can handle more complex CNF/DNF formulae

Other applications, too (see paper)

Our Construction (for Inner Products)

Background

- Bilinear groups of composite order [BGN]
  - $N=pqr$, product of *three* primes
  - Use multiplicative notation for all groups…
  - $e: G \times G \to G_T$ s.t. $e(P^a, Q^b) = e(P,Q)^{ab}$
- A nice feature here is "cancellation" across subgroups:
  - Let $G = G_p \times G_q \times G_r$
  - if $g_p \in G_p$ and $g_q \in G_q$, then $e(g_p, g_q) = 1$

Hardness assumptions

- New, somewhat complicated…
- …but fixed-size and non-interactive
- Hold in the generic group model (assuming hardness of factoring N)
- Intuitively, elements in different subgroups of G are indistinguishable (similar intuitively to the Subgroup Hiding Assumption of [BGN])

Intuition for the construction

- Computation of $<v, x>$ done in G_q (in the

Details omitted!
(See paper)

attribute hiding

Open questions

- Current situation seems analogous to the dawn of secure multi-party computation…
- We have examples of functional encryption schemes for various classes of functionalities – what else can we do?
  - Ultimate goal: any poly-time functionality!
  - No inherent reason why this should not be possible, but would require solving long-standing crypto problems (e.g. reusable garbled circuits)

Thank you!