

Predicate Encryption

J. Katz, A. Sahai, B. Waters

Georg Lippold

Information Security Institute
Queensland University of Technology

11 April 2007



Agenda

Predicate Encryption

Structure of the Paper

Open problems



Predicate Encryption

- ▶ Recently discovered by Katz, Sahai and Waters (2007).
- ▶ Abstraction from standard IBE, anonymous IBE, fuzzy threshold IBE and attribute based encryption.
- ▶ First scheme that allows also disjunctions in computations in the ciphertext
- ▶ Uses three primes, hardness assumption is factoring of large composite number, dBDH, and decisional discrete logarithm.
- ▶ Ciphertexts are twice as long as encrypted attributes.

Structure of the Paper I

1. Introduction, comparison to other papers and overview of results:
 - ▶ (anonymous) ID-based encryption (IBE), attribute-based encryption, other predicate encryption schemes (Boneh & Waters 07).
 - ▶ Features “matching” of attributes.
 - ▶ Examples for derived encryption schemes.
2. Definitions
 - ▶ Predicate encryption scheme: set of attributes Σ , \mathcal{F} set of predicates over Σ . A predicate is a function that takes an attribute and evaluates to 0 or 1:

$$\forall f \in \mathcal{F}, l \in \Sigma : f(l) = \begin{cases} 1 : l \text{ matches } f \\ 0 : \text{otherwise} \end{cases}$$

Structure of the Paper II

3. Complexity Assumptions:

- ▶ Factorizing of large composite numbers $N = p \cdot q \cdot r$.
- ▶ Distinguish between element of g^{pr} from g^{pqr} .
- ▶ Bilinear Diffie-Hellman.

See Appendix B for details.

4. Main Construction

- ▶ Predicate-only scheme, not with messages (Appendix D has full scheme).
- ▶ Idea for scheme:
 - ▶ Vector \vec{x} as attribute, vector \vec{y} as predicate.
 - ▶ Have three groups, $\mathbb{G}_p, \mathbb{G}_q, \mathbb{G}_r$ with generators g_p, g_q, g_r . \mathbb{G}_p encodes equation that evaluates to 0, \mathbb{G}_q encodes vectors in secret key & ciphertext, \mathbb{G}_r hides information.
- ▶ Proof Intuition: Double encryption and transitions between games
Proof for predicate-only scheme in Appendix C.

Structure of the Paper III

5. Applications:

- ▶ Anonymous ID-Based Encryption
- ▶ Hidden Vector Encryption
- ▶ Polynomial Evaluations
- ▶ Disjunctions, Conjunctions, CNF/DNF Formulas
- ▶ Exact Thresholds

Predicate Encryption

Definition 2.1, Page 3f.

- ▶ $N = p \cdot q \cdot r$ product of three primes.
- ▶ Set of possible attributes is $\Sigma = \mathbb{Z}_N^k$
- ▶ Predicates $\mathcal{F} = \{f_{\vec{x}} \mid \vec{x} \in \mathbb{Z}_N^k\}$, predicate $f_{\vec{x}}(\vec{y}) = 1$ if $\sum_{i=1}^k x_i y_i = 0$.
- ▶ A predicate encryption scheme consists of four PPT algorithms:
 - Setup** Input: security parameter 1^n . Output: master public key \mathcal{K}_{pub} , master secret key $\mathcal{K}_{\text{priv}}$.
 - GenKey** Input: master secret key $\mathcal{K}_{\text{priv}}$, predicate f . Output secret key $\mathcal{K}_{\text{priv}_f}$.
 - Enc** Input: master public key \mathcal{K}_{pub} , attribute $I \in \Sigma$, message M . Output: ciphertext C .
 - Dec** Input: secret key $\mathcal{K}_{\text{priv}_f}$, ciphertext C . Output: if $f(I) = 1 : M$ else \perp .



Example: ID-based encryption as subclass of predicate encryption

- ▶ Identities are mapped to \mathbb{Z}_N (e.g. by hash function).
- ▶ Identities then correspond to vectors of length 2. Predicate vector is $\vec{y} = \{1, -ID_i\}$, attribute (identity) used for encryption is $\vec{x} = \{ID_j, 1\}$. For $ID_i = ID_j = ID$ we have
$$f_{\vec{y}}(x) = \vec{x} \cdot \vec{y} = ID - ID = 0$$

Open Problems

- ▶ Full scheme (Appendix D) is only CPA secure: multiplication of the Message with a known value will go undetected
- ▶ Have to select sub-space for “valid” messages as decryption with wrong private key leads to arbitrary message.
- ▶ “Master Theorem” in Appendix B seems to be too general: The adversary seems to have no way to win the game with more than possibility $1/2$ as distinguishing feature for test is not defined. Fixed in “application” in Appendix B.2.
- ▶ Ciphertext is twice as long as encoded attributes
- ▶ Compared to previous schemes, generalization leads to further overhead (double length of attribute vectors for ID-based and hidden vector; length + 1 for exact thresholds)
- ▶ Fuzzy IBE’s not fully possible since “ \geq ”/“ \leq ” cannot be encoded in polynomial equations.