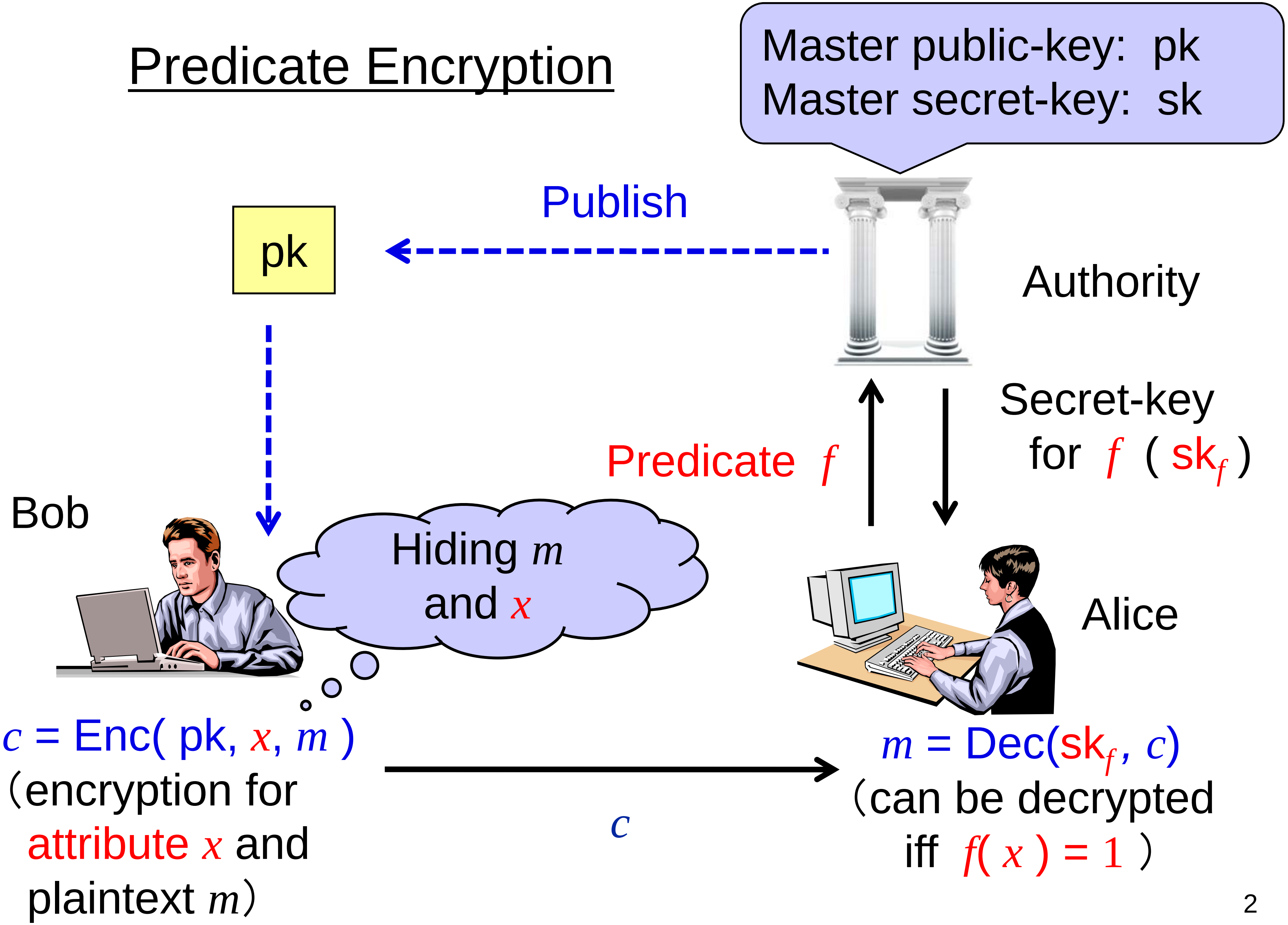
Efficient (Hierarchical) Inner Product Encryption Tightly Reduced from the Decisional Linear Assumption

2012 / 8 / 21

Tatsuaki Okamoto (NTT),
Katsuyuki Takashima (Mitsubishi Electric).

To appear in IEICE Trans. Fundamentals

Predicate Encryption



Inner Product Encryption (IPE) [KSW08]

- $f_{\vec{v}}(\vec{x}) = 1$ iff $\vec{x} \cdot \vec{v} = 0$

  $f_{\vec{v}}$: predicate with $\vec{v} \in \mathbb{F}_q^n$, $\vec{x} \in \mathbb{F}_q^n$: attribute

- Setup: pk: (master) public key, sk: (master) secret key
- $\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$: $\mathsf{sk}_{\vec{v}}$: secret key for $\vec{v}$
- $\mathsf{Enc}(\mathsf{pk}, \vec{x}, m)$: $c_{\vec{x}}$: ciphertext for $\vec{x}$
- $\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, c)$: plaintext m or $\perp$

  m can be decrypted iff $f_{\vec{v}}(\vec{x}) = 1$, i.e., $\vec{x} \cdot \vec{v} = 0$

Fully Attribute-Hiding Security of IPE

Challenger

$(\mathsf{pk}, \mathsf{sk})$

$\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$

$b \xleftarrow{\mathsf{U}} \{0,1\}$

$c \xleftarrow{\mathsf{U}} \mathsf{Enc}(\mathsf{pk}, \vec{x}^{\,(b)}, m^{(b)})$

Adversary $\mathcal{A}$

pk

$\vec{v}$

$\mathsf{sk}_{\vec{v}}$

$\vec{x}^{\,(0)}, \vec{x}^{\,(1)} \quad m^{(0)}, m^{(1)}$

c

b'

1. $f_{\vec{v}}(\vec{x}^{\,(0)}) = f_{\vec{v}}(\vec{x}^{\,(1)})$ for all queried $\vec{v}$
2. If matching $\vec{v}$ is queried, then $m^{(0)} = m^{(1)}$

Adversary $\mathcal{A}$ wins if $b = b'$.

No additional information on $\vec{x}$ is revealed to anyone,
(even to any person with a matching key $\mathsf{sk}_{\vec{v}}$, i.e., $f_{\vec{v}}(\vec{x}) = 1$.)

Fully Attribute-Hiding Security of IPE

selective game

Challenger

$(\mathsf{pk}, \mathsf{sk})$

$\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$

$b \xleftarrow{\mathsf{U}} \{0,1\}$

$c \xleftarrow{\mathsf{U}} \mathsf{Enc}(\mathsf{pk}, \vec{x}^{\,(b)}, m^{(b)})$

Adversary $\mathcal{A}$

$\vec{x}^{\,(0)}, \vec{x}^{\,(1)}$

pk

$\vec{v}$

$\mathsf{sk}_{\vec{v}}$

$m^{(0)}, m^{(1)}$

c

b'

1. $f_{\vec{v}}(\vec{x}^{\,(0)}) = f_{\vec{v}}(\vec{x}^{\,(1)})$ for all queried $\vec{v}$
2. If matching $\vec{v}$ is queried, then $m^{(0)} = m^{(1)}$

Adversary $\mathcal{A}$ wins if $b = b'$.

No additional information on $\vec{x}$ is revealed to anyone,
(even to any person with a matching key $\mathsf{sk}_{\vec{v}}$, i.e., $f_{\vec{v}}(\vec{x}) = 1$.)

Previous Works (Pairing-Based IPE)

- [KSW08, LOS+10, OT09, OT10, P11] : Aim at better security,
  e.g., adaptive security, fully-attribute-hiding,
  weaker (standard) assumptions
- [OT12] : Adaptively secure and fully attribute-hiding IPE
  under the DLIN assumption

From a practical point, the performance is not so satisfactory,
e.g., ciphertext includes $4n+2$ elements of $\mathbb{G}$,
the security reduction is not tight.

Our Result

Proposed IPE

- Fully-attribute-hiding and selectively secure from DLIN,
- Almost the shortest ciphertext among existing attribute-hiding IPEs, i.e., $n+4$ elements of $\mathbb{G}$ and 1 element of $\mathbb{G}_T$,
- The security reduction is (almost) tight.

Comparison

highest security !

	KSW08	OT09	Park11	OT12 (basic)	OT12 (variant)	Proposed (basic)	Proposed (variant)
Security	selective & fully-AH	selective & weakly-AH	selective & weakly-AH	adaptive & fully-AH	adaptive & fully-AH	selective & fully-AH	selective & fully-AH
Order of $\mathbb{G}$	composite	prime	prime	prime	prime	prime	prime
Assump.	2 variants of GSD	2 variants of DSP	DLIN & DBDH	DLIN	DLIN	DLIN	DLIN
Reduction factor	6	2	6	$3\nu+2$	$3\nu+2$	2	2
PK size	$O(n)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n)\lvert\mathbb{G}\rvert$	$O(n^2)\lvert\mathbb{G}\rvert$	$O(n)\lvert\mathbb{G}\rvert$
SK size	$(2n+1)\lvert\mathbb{G}\rvert$	$(n+3)\lvert\mathbb{G}\rvert$	$(4n+2)\lvert\mathbb{G}\rvert$	$(4n+2)\lvert\mathbb{G}\rvert$	$11\lvert\mathbb{G}\rvert$	$(n+4)\lvert\mathbb{G}\rvert$	$6\lvert\mathbb{G}\rvert$
CT size	$(2n+1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(n+3)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(4n+2)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(4n+2)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(5n+1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(n+4)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(n+4)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$

n: dimension of attribute vector
ν: the maximum number of key-queries
$\lvert\mathbb{G}\rvert$, $\lvert\mathbb{G}_T\rvert$: size of an element of $\mathbb{G}$, $\mathbb{G}_T$
AH : attribute-hiding
PK, SK, CT : public key, secret key, ciphertext
GSD, DSP, DBDH : general subgroup decision, decisional subspace problem, decisional bilinear Diffie-Hellman

fully-AH
tight reduction from DLIN
shortest CT

Thank You !