Predicate Encryptions: Equivalence of Abstract Encodings and Generic CCA-security

Sayantan Mukherjee, Tapas Pandit and Sanjit Chatterjee

Department of Computer Science and Automation, IISc, Bangalore

sayantan.mukherjee@csa.iisc.ernet.in

Abstract

A *predicate encryption* (PE) can be thought of as emulation of predicate function $R : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ in the encrypted domain. In case of a predicate encryption, given a key K_x ($x \in \mathcal{X}$) one can decrypt the ciphertext C_y ($y \in \mathcal{Y}$) if $R(x, y) = 1$. We studied predicate encryptions from different aspects.

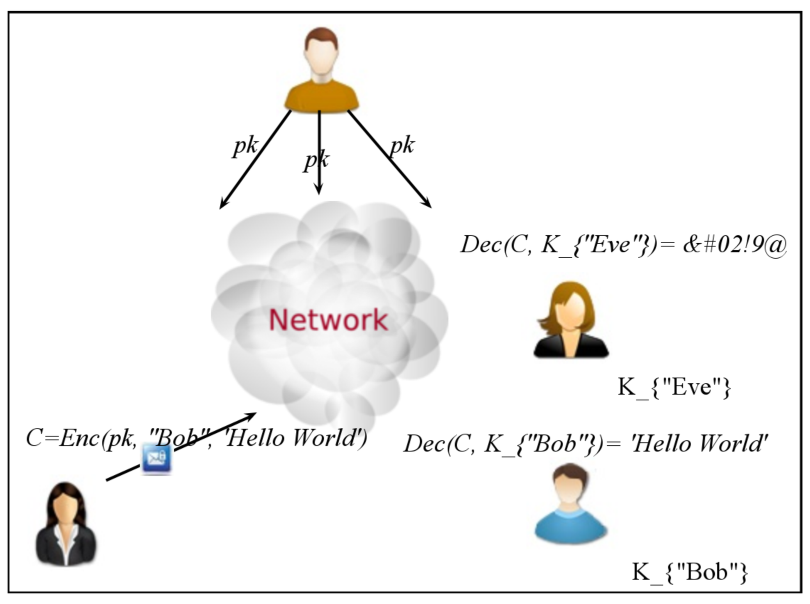
1. Available encodings
   (a) Pair Encoding due to Attrapadung.
   (b) Predicate Encoding due to Wee.
   (c) The encodings focus on the *exponent polynomials* of the available schemes.
   (d) We observed certain equivalence relation between the encodings.
2. Integrating pair encoding with dual system group.
3. CCA-secure predicate encryption
   (a) Schemes in both Attrapadung and Wee are only CPA-secure.
   (b) Delegation and verifiability based CPA-to-CCA generic conversion is inefficient.
   (c) We propose direct efficient conversion.

Introduction

For a Predicate Encryption (PE) for predicate function R,

- If ciphertext is C_y^M (M and y being the message and ciphertext-attribute)
- If key is K_x (x being key-attribute)
- Can decrypt if $R(x, y) = 1$

IBE is earliest PE with equality predicate function.



Examples

1. **Access Control Mechanism**:
   - A mail is encrypted for PhD students or Professors.
   - No ME/MSc student should be able to decrypt it.
   - Predicate function is *access control matrix*.
2. **Searchable Encryption**:
   - Office database is encrypted in cloud.
   - To search who gets salary more than $30,000$.
   - Predicate function is $\geq$.

[1, 4] simplified the construction and the proof of CPA-secure predicate encryption by defining *pair encoding* and *predicate encoding* respectively. [3] defined *dual system group* (DSG) to *codify* the *proof technique* also. Available conversion techniques to construct a CCA-secure predicate encryption from CPA-secure predicate encryption is not efficient.

Main Objectives

1. Finding relation between both the encodings is of theoretical interest.
2. Integrating pair encoding to dual system group allows one to design black-box security proof.
3. Available conversion mechanisms for CPA-secure PE to CCA-secure PE generically, is inefficient due to requirement of excess pairing evaluation (which is considered to be the costliest operation).

Mathematical Tool

For prime order (p) group $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$, $e : G_1 \times G_2 \to G_T$ is bilinear, non-degenerate and efficiently computable map.

Predicate Encryption

A predicate encryption scheme for predicate function R is defined by following probabilistic polynomial time algorithms,

- Setup: Generates pk and msk. Publishes pk.
- $\mathsf{Keygen}(msk, x)$: On input key-attribute x, generates secret key K_x.
- $\mathsf{Enc}(pk, M, y)$: Given ciphertext-attribute y, outputs ciphertext C_y^M as encryption of M.
- $\mathsf{Dec}(K_x, C_y^M)$: Outputs M if $R(x, y) = 1$.

Pair Encoding

A Pair Encoding P for a predicate function R consists of four deterministic algorithms,

- $\mathsf{Param}(\kappa) \to n$ which is number of *common variables* $\mathbf{h} = (h_1, \dots, h_n)$ in EncK and EncC.
- $\mathsf{EncK}(\mathbf{x}, N) \to$ $(\mathbf{k_x} = (k_1, \dots, k_{m_1}); m_2)$ where each k_i is a polynomial of m_2 own variables $(r_1, \dots, r_{m_2})$, n common variables and msk α.
$$k_i(\alpha, (r_1, \dots, r_{m_2}), (h_1, \dots, h_n)) = b_i\alpha + \sum_{j \in [1,m_2]} b_{ij} r_j + \sum_{\substack{j \in [1,m_2] \\ k \in [1,n]}} b_{ijk} r_j h_k$$
- $\mathsf{EncC}(\mathbf{y}, N) \to$ $(\mathbf{c_y} = (c_1, \dots, c_{w_1}); w_2)$ where each c_i is a polynomial of $(1 + w_2)$ own variables $(s_0, \dots, s_{w_2})$ and n common variables.
$$c_i(\alpha, (s_0, \dots, s_{w_2}), (h_1, \dots, h_n)) = \sum_{j \in [0,w_2]} a_{ij} s_j + \sum_{\substack{j \in [0,w_2] \\ k \in [1,n]}} a_{ijk} s_j h_k$$
- $\mathsf{Pair}(\mathbf{x}, \mathbf{y}) \to \mathbf{E} \in \mathbb{Z}_p^{m_1 \times w_1}$ such that $\mathbf{k_x} \mathbf{E} \mathbf{c_y}^\top = \alpha s_0$.

Predicate Encoding

A predicate encoding $\mathcal{P}$ for a predicate function R consists of five [2] deterministic algorithms $(\mathsf{sE}, \mathsf{rE}, \mathsf{kE}, \mathsf{sD}, \mathsf{rD})$ satisfying following properties:

- **linearity**: $\forall (x, y) \in \mathcal{X} \times \mathcal{Y}$, $\mathsf{sE}(y, \cdot), \mathsf{rE}(x, \cdot), \mathsf{kE}(x, \cdot), \mathsf{sD}(x, y, \cdot), \mathsf{rD}(x, y, \cdot)$ are $\mathbb{Z}_p$-linear.
- **restricted** α**-reconstruction**: $\forall (x, y) \in \mathcal{X} \times \mathcal{Y}$ such that $R(x, y) = 1$ and $\forall \mathbf{w} \in \mathcal{W}$, $\mathsf{sD}(x, y, \mathsf{sE}(y, \mathbf{w})) = \mathsf{rD}(x, y, \mathsf{rE}(x, \mathbf{w}))$ and $\mathsf{rD}(x, y, \mathsf{kE}(x, \alpha)) = \alpha$.

Dual System Group

Dual system group consists of three abelian groups $(\mathbb{G}, \mathbb{H}, \mathbb{G}_T)$, an admissible bilinear map $\hat{e} : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$ and six [3] randomized algorithms:

- $\mathsf{SampP}(1^\kappa, 1^n)$: outputs public parameter pp and secret parameter sp. pp contains common variables and a linear map μ on $\mathbb{H}$ and sp contains a special element $\tilde{h} \in \mathbb{H}$ such that $\mu(\tilde{h}) = 1$.
- SampGT: $Im(\mu) \to \mathbb{G}_T$.
- $\mathsf{SampG}(pp)$: Output $\mathbf{g} \in \mathbb{G}^{n+1}$.
- $\mathsf{SampH}(pp)$: Output $\mathbf{h} \in \mathbb{H}^{n+1}$.
- $\widehat{\mathsf{SampG}}(pp, sp)$: Output $\hat{\mathbf{g}} \in \mathbb{G}^{n+1}$.
- $\widehat{\mathsf{SampH}}(pp, sp)$: Output $\hat{\mathbf{h}} \in \mathbb{H}^{n+1}$.

with following properties:

- **projective**: $\forall h \in \mathbb{H}, s \xleftarrow{U} \mathbb{Z}_p$, $\mathsf{SampGT}(\mu(h); s) = \hat{e}(\mathsf{SampG}_0(pp; s), h) = \hat{e}(g_0, h)$
- **associative**: $\forall \mathbf{g} = (g_0, \dots, g_n)$ and $\forall \mathbf{h} = (h_0, \dots, h_n)$ and $\forall i \in [1, n]$, $\hat{e}(g_0, h_i) = \hat{e}(g_i, h_0)$.

CCA-secure predicate encryption from pair encoding

- $\mathsf{Setup}(1^\kappa)$: Outputs $PK = \begin{pmatrix} \mathcal{H}, g_T^{\boldsymbol{\alpha}^\top \mathbf{B}\binom{\mathbf{I_d}}{0}}, & g_1^{\mathbf{B}\binom{\mathbf{I_d}}{0}}, & g_1^{\mathbf{H}_1\mathbf{B}\binom{\mathbf{I_d}}{0}}, & \dots, & g_1^{\mathbf{H}_n\mathbf{B}\binom{\mathbf{I_d}}{0}}, & g_1^{\mathbf{H}_{n+1}\mathbf{B}\binom{\mathbf{I_d}}{0}}, & g_1^{\mathbf{H}_{n+2}\mathbf{B}\binom{\mathbf{I_d}}{0}} \\ & g_2^{\mathbf{Z}\binom{\mathbf{I_d}}{0}}, & g_2^{\mathbf{H}_1^\top\mathbf{Z}\binom{\mathbf{I_d}}{0}}, & \dots, & g_2^{\mathbf{H}_n^\top\mathbf{Z}\binom{\mathbf{I_d}}{0}}, & g_2^{\mathbf{H}_{n+1}^\top\mathbf{Z}\binom{\mathbf{I_d}}{0}}, & g_2^{\mathbf{H}_{n+2}^\top\mathbf{Z}\binom{\mathbf{I_d}}{0}} \end{pmatrix}$
  where $\mathbf{H}_i \xleftarrow{U} \mathbb{Z}_p^{(d+1)\times(d+1)}$, $i \in [1, n+2]$, $\mathbf{B}, \tilde{\mathbf{D}}, \boldsymbol{\alpha} \xleftarrow{U} \mathbb{GL}_{d+1}(\mathbb{Z}_p) \times \mathbb{GL}_d(\mathbb{Z}_p) \times \mathbb{Z}_p^{(d+1)\times 1}$, $\mathbf{D} = \begin{pmatrix} \tilde{\mathbf{D}} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$, $\mathbf{Z} = \mathbf{B}^{-\top}\mathbf{D}$, random $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p$ and $g_1, g_2 \xleftarrow{U} \mathbb{G}_1 \times \mathbb{G}_2$, $g_T = e(g_1, g_2)$, $n \leftarrow \mathsf{Param}(\kappa)$
- $\mathsf{Keygen}(\mathbf{x}, MSK)$: Outputs secret key $\mathbf{K_x} = \{g_2^{k_i(\boldsymbol{\alpha}, \mathbf{R}, \mathbf{H}|_n)}\}_i \in \left(\mathbb{G}_2^{(d+1)\times 1}\right)^{m_1}$ where $(\mathbf{k_x}; m_2) \leftarrow \mathsf{EncK}(\mathbf{x}, N)$ for $k_i := b_i\boldsymbol{\alpha} + \sum_{j \in [1,m_2]} b_{ij}\mathbf{Z}\binom{\mathbf{r}_j}{0} + \sum_{\substack{j \in [1,m_2] \\ k \in [1,n]}} b_{ijk}\mathbf{H}_k^\top \mathbf{Z}\binom{\mathbf{r}_j}{0}$ for $i \in [1, m_1]$ and $\mathbf{R} = \left(\binom{\mathbf{r}_1}{0}, \dots, \binom{\mathbf{r}_{m_2}}{0}\right) \xleftarrow{U} \mathbf{Z}_p^{(d+1)\times m_2}$
- $\mathsf{Enc}(y, M, PK)$: Outputs ciphertext $\mathbf{C_y} = (C_0', \mathbf{C_y^{cpa}})$ where $C_0' = g_1^{(\eta\mathbf{H}_{n+1} + \mathbf{H}_{n+2})\mathbf{B}\binom{\mathbf{s}_0}{0}}$, $\mathbf{C_y^{cpa}} = (\{g_1^{c_i(\mathbf{S}, \mathbf{H}|_n)}\}_i \in \left(\mathbb{G}_1^{(d+1)\times 1}\right)^{w_1}, M.g_T^{\alpha^\top \mathbf{B}\binom{\mathbf{s}_0}{0}})$ for $c_i := \sum_{j \in [0,w_2]} a_{ij}\mathbf{B}\binom{\mathbf{s}_j}{0} + \sum_{\substack{j \in [0,w_2] \\ k \in [1,n]}} a_{ijk}\mathbf{H}_k\mathbf{B}\binom{\mathbf{s}_j}{0}$ for $i \in [1, w_1]$, $\eta = \mathcal{H}(\mathbf{C_y^{cpa}})$ and $(\mathbf{c_y}; w_2) \leftarrow \mathsf{EncC}(\mathbf{y}, N)$
- $\mathsf{Dec}(\mathbf{C_y}, \mathbf{K_x})$: It first defines *modified secret key* $\hat{\mathbf{K}}_\mathbf{x} = (K_0, \Phi \cdot \tilde{K}_\mathbf{x}[1], \tilde{K}_\mathbf{x}[2], \dots, \tilde{K}_\mathbf{x}[w_1])$ where $K_0 = g_2^{-\mathbf{Z}\binom{\mathbf{t}}{0}}$, $\Phi = g_2^{(\eta\mathbf{H}_{n+1}^\top + \mathbf{H}_{n+2}^\top)\mathbf{Z}\binom{\mathbf{t}}{0}}$ and $\tilde{K}_\mathbf{x}[i'] = \prod_{i \in [m_1]} (\mathbf{K_x}[i])^{E_{ii'}}$ for $\eta = \mathcal{H}(\mathbf{C_y^{cpa}})$, $\mathbf{t} \xleftarrow{U} \mathbb{Z}_p^d$ and $\mathbf{E} \leftarrow \mathsf{Pair}(\mathbf{x}, \mathbf{y}, N)$. Then it computes $e(g_1, g_2)^{\alpha^\top \mathbf{B}\binom{\mathbf{s}_0}{0}} = e(C_0', \hat{\mathbf{K}}_\mathbf{x}[0]) \prod_{i \in [1,w_1]} e(\mathbf{C_y^{cpa}}[i], \hat{\mathbf{K}}_\mathbf{x}[i])$

Results

Pair Encoding and Predicate Encoding

- Equivalent if we restrict $m_2 = 1$ and $w_2 = 1$ in pair encoding.
- Decryption matrix $\mathbf{E}$ in pair encoding = $\begin{pmatrix} \mathsf{rD}(x,y,\cdot) & \mathbf{0} \\ 0 & \mathsf{sD}(x,y,\cdot)^\top \end{pmatrix}$.

Pair Encoding and Dual System Group

- Black-box integration needs SampG and SampH is run $(1 + w_2)$ and m_2 times respectively.
- We present correctness based on *fundamental theorem of finite abelian group* and proof based on extended assumptions.

CCA-secure Predicate Encryption

- Exploits the *regular encoding* property of pair encoding.
- We reuse randomness $g_1^{\mathbf{B}\binom{\mathbf{s}_0}{0}}$ to compute $C_0' = g_1^{(\eta\mathbf{H}_{n+1} + \mathbf{H}_{n+2})\mathbf{B}\binom{\mathbf{s}_0}{0}}$.
- During decryption η is recomputed to compute $g_2^{\left(-\mathbf{Z}\binom{\mathbf{t}}{0}, (\eta\mathbf{H}_{n+1}^\top + \mathbf{H}_{n+2}^\top)\mathbf{Z}\binom{\mathbf{t}}{0}, \mathbf{0}, \dots, \mathbf{0}\right)}$ for $\mathbf{t} \xleftarrow{U} \mathbb{Z}_p^d$ and $\mathbf{B}, \mathbf{Z} \in \mathbb{Z}_p^{(d+1)\times(d+1)}$ are somewhat orthogonal.
- Decryption now needs only 1 unit extra pairing to check validity of ciphertext.

Forthcoming Research

- Instantiate (weakly) attribute hiding predicate encryption using pair encoding and DSG as black-box.

References

[1] Nuttapong Attrapadung. *Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More*, pages 557–577. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[2] Jie Chen, Romain Gay, and Hoeteck Wee. *Improved Dual System ABE in Prime-Order Groups via Predicate Encodings*, pages 595–624. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[3] Jie Chen and Hoeteck Wee. *Dual System Groups and its Applications-Compact HIBE and More*. *IACR Cryptology ePrint Archive*, 2014:265, 2014.

[4] Hoeteck Wee. *Dual System Encryption via Predicate Encodings*, pages 616–637. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

CCA-Secure Predicate Encryption Based on Pair Encoding in Prime-Order Groups

Sayantan Mukherjee

Indian Institute of Science, Bangalore

April 8th, EECS SYMPOSIUM 2017, Bangalore

joint work with *Sanjit Chatterjee* and *Tapas Pandit*

Introduction

- Predicate Encryption (PE) emulates of predicate function ($R : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$) in encrypted domain.
- One can decrypt ciphertext $C_{\mathbf{y}}$ if the key $K_{\mathbf{x}}$ satisfies the predicate function (i.e. $R(\mathbf{x}, \mathbf{y}) = 1$).
- Different predicate encryptions for different predicate functions.
  - Equality predicate : Identity-Based Encryption.
  - Inner Product predicate : Inner Product Encryption.
  - Access Control predicate : Attribute-Based Encryption.
- Applications: encrypted database search, controlling access to an encrypted document etc.
- Ciphertext and keys are usually elements of certain groups.
- Available abstract encodings (pair and predicate encoding)
  - Focus on processing of exponents of those group elements.
  - Are abstract forms to achieve PE.

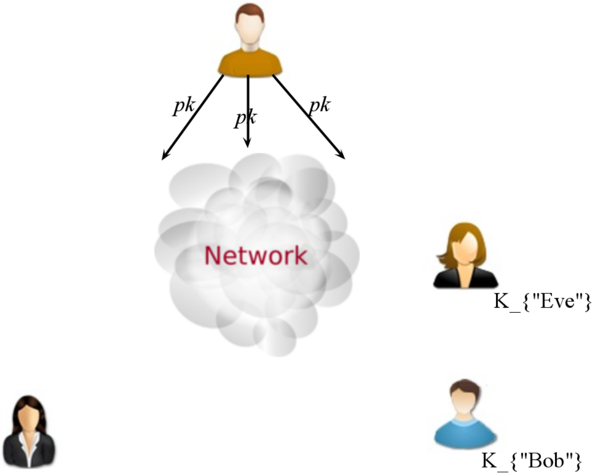
Introduction

- Predicate Encryption (PE) emulates of predicate function ($R : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$) in encrypted domain.
- One can decrypt ciphertext $C_{\mathbf{y}}$ if the key $K_{\mathbf{x}}$ satisfies the predicate function (i.e. $R(\mathbf{x}, \mathbf{y}) = 1$).
- Different predicate encryptions for different predicate functions.
  - Equality predicate : Identity-Based Encryption.
  - Inner Product predicate : Inner Product Encryption.
  - Access Control predicate : Attribute-Based Encryption.
- Applications: encrypted database search, controlling access to an encrypted document etc.
- Ciphertext and keys are usually elements of certain groups.
- Available abstract encodings (pair and predicate encoding)
  - Focus on processing of exponents of those group elements.
  - Are abstract forms to achieve PE.

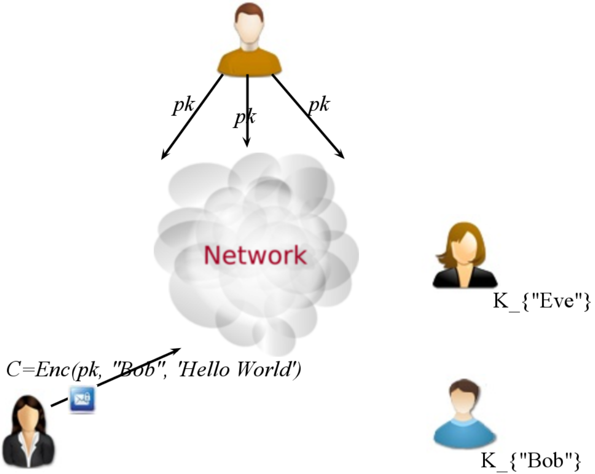
Our Achievements

- Certain equivalence relation between pair and predicate encoding.
- Generic integration of *pair encoding* with *dual system group*.
- Efficient and generic conversion of CPA-secure PE to CCA-secure PE in prime order groups.

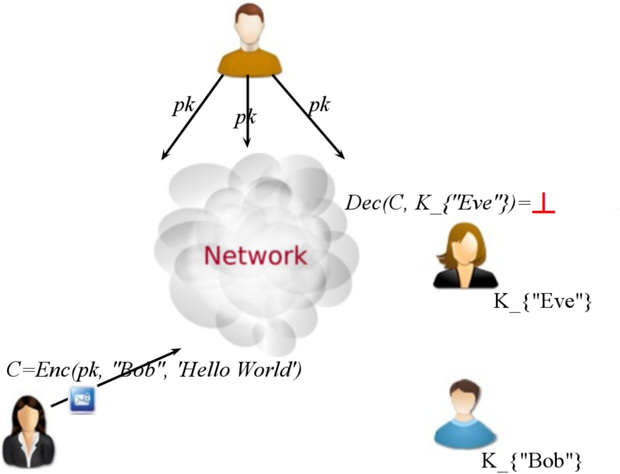
Equality Predicate: Identity-Based Encryption



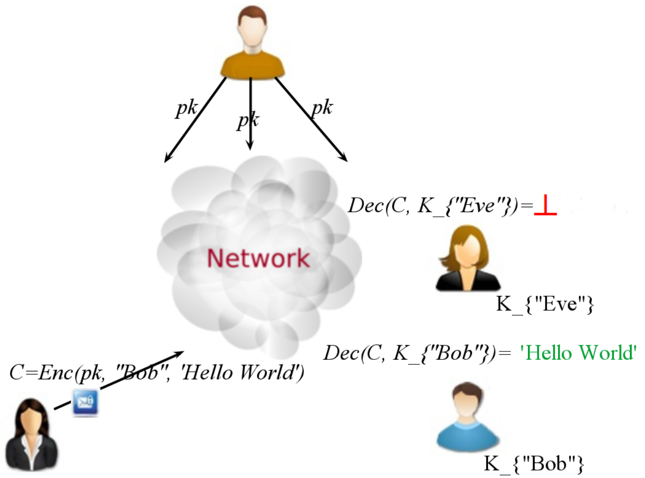
Equality Predicate: Identity-Based Encryption



Equality Predicate: Identity-Based Encryption



Equality Predicate: Identity-Based Encryption



Chosen Ciphertext Security

- Adversaries are usually active and can tamper with the ciphertext.
- In certain situation it can get decryption of certain messages of its choice.
- Chosen ciphertext security prevents such strong adversaries
  - Is therefore harder to achieve.
- Verifiability based generic CPA-to-CCA conversions are available.

Chosen Ciphertext Security

- Adversaries are usually active and can tamper with the ciphertext.
- In certain situation it can get decryption of certain messages of its choice.
- Chosen ciphertext security prevents such strong adversaries
  - Is therefore harder to achieve.
- Verifiability based generic CPA-to-CCA conversions are available.

Example Scenario

We concentrate on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) by Lewko.

- ABE emulates access control predicate function $R(\mathbf{x}, \mathbf{y})$
  - $\mathbf{x}$ is attribute set (e.g. Student, Professor, PhD, CSA etc)
  - $\mathbf{y}$ is access control matrix (A, ρ) where ρ defines authorized parties.
- Lewko's CP-ABE is secure against passive adversaries (i.e. CPA-secure).
- Verifiability based CPA-to-CCA conversion
  - Checks ciphertext validity.
  - Such checking needs $\mathcal{O}(|\mathbf{x}|)$ (extra) pairing which is the costliest operation.

Predicate Encryption from Pair Encoding

For a predicate family $R : \mathcal{X} \times \mathcal{Y} \rightarrow \{0,1\}$,

- **Setup**(1^κ): Generates public parameters PP and master secret msk using $\mathbf{h} = (h_1, \ldots, h_n) \leftarrow \mathrm{Param}(\kappa)$. PP is published and msk is kept secret.
- **Keygen**$(msk, \mathbf{x} \in \mathcal{X})$: Generates corresponding secret key $K_\mathbf{x}$ using $((k_1, \ldots, k_{m_1}); m_2) \leftarrow \mathrm{EncK}(\mathbf{x}, N)$ where each k_i is a polynomial of m_2 own variables $(r_1, \ldots, r_{m_2})$, n common variables and msk α.

$$k_i\Big(\alpha,(r_1,\ldots,r_{m_2}),(h_1,\ldots,h_n)\Big) = b_i\alpha + \sum_{j\in[1,m_2]} b_{ij} r_j + \sum_{\substack{j\in[1,m_2]\\ k\in[1,n]}} b_{ijk} r_j h_k \ .$$

- **Encrypt**$(PP, \mathbf{y} \in \mathcal{Y}, M)$: Generates $C_\mathbf{y}^M$ using $((c_1, \ldots, c_{w_1}); w_2) \leftarrow \mathrm{EncC}(\mathbf{y}, N)$ where each c_i is a polynomial of $(1 + w_2)$ own variables $(s_0, \ldots, s_{w_2})$ and n common variables.

$$c_i\Big((s_0,\ldots,s_{w_2}),(h_1,\ldots,h_n)\Big) = \sum_{j\in[0,w_2]} a_{ij} s_j + \sum_{\substack{j\in[0,w_2]\\ k\in[1,n]}} a_{ijk} s_j h_k$$

- **Decrypt**$(K_\mathbf{x}, C_\mathbf{y}^M)$: Outputs M by using $\mathbf{E} \in \mathbb{Z}_p^{m_1\times w_1} \leftarrow \mathrm{Pair}(\mathbf{x}, \mathbf{y})$ if $R(\mathbf{x}, \mathbf{y}) = 1$, else outputs $\perp$.

Our Conversion Technique

From Lewko's CPA-secure CP-ABE ($\mathbf{y} = (A \in \mathbb{Z}_p^{n \times k}, \rho : \{1, \ldots, n\} \to \mathcal{U})$, $\mathbf{x} = S$), we instantiate CCA-secure predicate encryption as follows,

- Setup(N, κ): $g_1, g_2 \xleftarrow{\$} \mathbb{G}_1 \times \mathbb{G}_2$, $g_T := e(g_1, g_2)$, $n \leftarrow \mathsf{Param}(\kappa)$

$$\mathbb{H} := (\mathbf{H}_0, \mathbf{H}_1, \ldots, \mathbf{H}_n) \text{ where } \mathbf{H}_i \xleftarrow{\$} \mathbb{Z}_p^{(d+1)\times(d+1)},\ i \in \{0, \ldots, n\}.$$

$$\mathbf{B}, \tilde{\mathbf{D}}, \boldsymbol{\alpha} \xleftarrow{\$} \mathbb{GL}_{d+1}(\mathbb{Z}_p) \times \mathbb{GL}_d(\mathbb{Z}_p) \times \mathbb{Z}_p^{(d+1)\times 1}$$

$$\mathbf{D} := \begin{pmatrix} \tilde{\mathbf{D}} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}, \mathbf{Z} := \mathbf{B}^{-\top}\mathbf{D}\ .$$

$$PK = \left(g_T^{\boldsymbol{\alpha}^\top \mathbf{B} \begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}}, \begin{matrix} g_1^{\mathbf{B}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}}, & g_1^{\mathbf{H}_0\mathbf{B}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}}, & g_1^{\mathbf{H}_1\mathbf{B}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}}, & \cdots, & g_1^{\mathbf{H}_n\mathbf{B}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}} \\ g_2^{\mathbf{Z}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}}, & g_2^{\mathbf{H}_0^\top\mathbf{Z}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}}, & g_2^{\mathbf{H}_1^\top\mathbf{Z}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}}, & \cdots, & g_2^{\mathbf{H}_n^\top\mathbf{Z}\begin{pmatrix} \mathbf{I_d} \\ 0 \end{pmatrix}} \end{matrix} \right)$$

$$MSK = g_2^{\boldsymbol{\alpha}}$$

Our Conversion Technique

From Lewko's CPA-secure CP-ABE ($\mathbf{y} = (A \in \mathbb{Z}_p^{n\times k}, \rho : \{1, \ldots, n\} \to \mathcal{U})$, $\mathbf{x} = S$), we instantiate CCA-secure predicate encryption as follows,

- Setup(N, κ): $g_1, g_2 \xleftarrow{\$} \mathbb{G}_1 \times \mathbb{G}_2$, $g_T := e(g_1, g_2)$, $n \leftarrow \mathrm{Param}(\kappa)$

  $\mathbb{H} := (\mathbf{H}_0, \mathbf{H}_1, \ldots, \mathbf{H}_n, \mathbf{H}_{n+1}, \mathbf{H}_{n+2})$ where $\mathbf{H}_i \xleftarrow{\$} \mathbb{Z}_p^{(d+1)\times(d+1)}$, $i \in \{0, \ldots, n, n+1, n+2\}$.

  $\mathbf{B}, \tilde{\mathbf{D}}, \boldsymbol{\alpha} \xleftarrow{\$} \mathbb{GL}_{d+1}(\mathbb{Z}_p) \times \mathbb{GL}_d(\mathbb{Z}_p) \times \mathbb{Z}_p^{(d+1)\times 1}$

  $\mathbf{D} := \begin{pmatrix} \tilde{\mathbf{D}} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$, $\mathbf{Z} := \mathbf{B}^{-\top}\mathbf{D}$ and chooses collision resistant hash $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p$.

  $PK =$

$$\left(\mathcal{H}, g_T^{\boldsymbol{\alpha}^\top \mathbf{B}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, \begin{matrix} g_1^{\mathbf{B}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_1^{\mathbf{H}_0\mathbf{B}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_1^{\mathbf{H}_1\mathbf{B}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & \ldots, & g_1^{\mathbf{H}_n\mathbf{B}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_1^{\mathbf{H}_{n+1}\mathbf{B}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_1^{\mathbf{H}_{n+2}\mathbf{B}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}} \\ g_2^{\mathbf{Z}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_2^{\mathbf{H}_0^\top\mathbf{Z}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_2^{\mathbf{H}_1^\top\mathbf{Z}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & \ldots, & g_2^{\mathbf{H}_n^\top\mathbf{Z}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_2^{\mathbf{H}_{n+1}^\top\mathbf{Z}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}}, & g_2^{\mathbf{H}_{n+2}^\top\mathbf{Z}\begin{pmatrix}\mathbf{I_d}\\0\end{pmatrix}} \end{matrix} \right)$$

  $MSK = g_2^{\boldsymbol{\alpha}}$

Our Conversion Technique

- Keygen$(\mathbf{x} = (x_1, \ldots, x_n), MSK)$: $(\mathbf{k_x}; m_2 = 1) \leftarrow \mathsf{EncK}(\mathbf{x}, N)$

  $\mathbf{R} = \binom{\mathbf{r}}{0} \xleftarrow{\$} \mathbf{Z}_p^{(d+1)\times m_2}$ and outputs secret key $\mathbf{K_x} = g_2^{\mathbf{k_x}(\boldsymbol{\alpha}, \mathbf{R}, \mathbb{H})}$

  such that $K_1 = g_2^{\boldsymbol{\alpha} + \mathbf{H}_0^\top \mathbf{Z}\binom{\mathbf{r}}{0}}$, $K_2 := g_2^{\mathbf{Z}\binom{\mathbf{r}}{0}}$, and $K_{3,i} = g_2^{\mathbf{H}_i^\top \mathbf{Z}\binom{\mathbf{r}}{0}}$ for $i \in [n]$

- Enc$(\mathbf{y} = (A, \rho), M, PK)$: $(\mathbf{c_y}; w_2 = n + k - 1) \leftarrow \mathsf{EncC}(\mathbf{y}, N)$

  $\mathbf{S} = (\binom{\mathbf{s}}{0}, \binom{\mathbf{s}_1}{0}, \ldots, \binom{\mathbf{s}_n}{0}, \binom{\mathbf{v}_2}{0}, \ldots, \binom{\mathbf{v}_k}{0}) \xleftarrow{\$} \mathbf{Z}_p^{(d+1)\times(w_2+1)}$

  defines $\mathbf{C}_\mathbf{y}^{\mathrm{cpa}} = (C', g_1^{\mathbf{c_y}(\mathbf{S}, \mathbb{H}|_n)})$

  where $C_{1,\ell} = g_1^{\mathbf{H}_0\left(A_{\ell,1}\mathbf{B}\binom{\mathbf{s}}{0} + \sum_{j\in[2,k]} A_{\ell,j}\mathbf{B}\binom{\mathbf{v}_j}{0}\right) + \mathbf{H}_{\rho(\ell)}\mathbf{B}\binom{\mathbf{s}_\ell}{0}}$, $C_{2,\ell} = g_1^{\mathbf{B}\binom{\mathbf{s}_\ell}{0}}$ for $\ell \in [1, n]$

  and $C_0 = g_1^{\mathbf{B}\binom{\mathbf{s}}{0}}$, $C' = M.e(g_1, g_2)^{\boldsymbol{\alpha}^\top \mathbf{B}\binom{\mathbf{s}}{0}}$.

Our Conversion Technique

- Keygen($\mathbf{x} = (x_1, \ldots, x_n), MSK$): $(\mathbf{k_x}; m_2 = 1) \leftarrow \mathsf{EncK}(\mathbf{x}, N)$

  $\mathbf{R} = \binom{\mathbf{r}}{0} \xleftarrow{\$} \mathbf{Z}_p^{(d+1)\times m_2}$ and outputs secret key $\mathbf{K_x} = g_2^{\mathbf{k_x}(\boldsymbol{\alpha}, \mathbf{R}, \mathbb{H})}$

  such that $K_1 = g_2^{\boldsymbol{\alpha} + \mathbf{H}_0^\top \mathbf{Z}\binom{\mathbf{r}}{0}}$, $K_2 := g_2^{\mathbf{Z}\binom{\mathbf{r}}{0}}$, and $K_{3,i} = g_2^{\mathbf{H}_i^\top \mathbf{Z}\binom{\mathbf{r}}{0}}$ for $i \in [n]$

- Enc($\mathbf{y} = (A, \rho), M, PK$): $(\mathbf{c_y}; w_2 = n + k - 1) \leftarrow \mathsf{EncC}(\mathbf{y}, N)$

  $\mathbf{S} = \left(\binom{\mathbf{s}}{0}, \binom{\mathbf{s}_1}{0}, \ldots, \binom{\mathbf{s}_n}{0}, \binom{\mathbf{v}_2}{0}, \ldots, \binom{\mathbf{v}_k}{0}\right) \xleftarrow{\$} \mathbf{Z}_p^{(d+1)\times(w_2+1)}$

  defines $\mathbf{C}_\mathbf{y}^{\mathrm{cpa}} = (C', g_1^{\mathbf{c_y}(\mathbf{S}, \mathbb{H}|_n)})$

  where $C_{1,\ell} = g_1^{\mathbf{H}_0\left(A_{\ell,1}\mathbf{B}\binom{\mathbf{s}}{0} + \sum_{j\in[2,k]} A_{\ell,j}\mathbf{B}\binom{\mathbf{v}_j}{0}\right) + \mathbf{H}_{\rho(\ell)}\mathbf{B}\binom{\mathbf{s}_\ell}{0}}$, $C_{2,\ell} = g_1^{\mathbf{B}\binom{\mathbf{s}_\ell}{0}}$ for $\ell \in [1, n]$

  and $C_0 = g_1^{\mathbf{B}\binom{\mathbf{s}}{0}}$, $C' = M.e(g_1, g_2)^{\boldsymbol{\alpha}^\top \mathbf{B}\binom{\mathbf{s}}{0}}$.

  then it computes $\eta = \mathcal{H}(\mathbf{C}_\mathbf{y}^{\mathrm{cpa}})$ and defines $\mathbf{C_y} = (C_0', \mathbf{C}_\mathbf{y}^{\mathrm{cpa}})$

  where $C_0' = g_1^{(\eta \mathbf{H}_{n+1} + \mathbf{H}_{n+2})\mathbf{B}\binom{\mathbf{s}}{0}}$

Our Conversion Technique

- Dec($\mathbf{C}_{\mathsf{y}}, \mathbf{K}_{\mathsf{x}}$): Computes $\tilde{K}_{\mathsf{x}}[i'] = \prod_{i \in [m_1]} (\mathbf{K}_{\mathsf{x}}[i])^{E_{ii'}}$ for $\mathbf{E} \leftarrow \mathrm{Pair}(\mathbf{x}, \mathbf{y}, N)$.

  defines $\hat{\mathbf{K}}_{\mathsf{x}} = (\tilde{K}_{\mathsf{x}}[1], \tilde{K}_{\mathsf{x}}[2], \ldots, \tilde{K}_{\mathsf{x}}[w_1])$.

  Then it computes $e(g_1, g_2)^{\boldsymbol{\alpha}^{\top} \mathbf{B} \binom{\mathbf{s}}{0}} = \prod_{i \in [1, w_1]} e(\mathbf{C}_{\mathbf{y}}^{\mathrm{cpa}}[i], \hat{\mathbf{K}}_{\mathsf{x}}[i])$ which is used to unblind C'.

Correctness: $\prod_{i \in [1, w_1]} e(\mathbf{C}_{\mathbf{y}}^{\mathrm{cpa}}[i], \hat{\mathbf{K}}_{\mathsf{x}}[i]) = e(g_1, g_2)^{\boldsymbol{\alpha}^{\top} \mathbf{B} \binom{\mathbf{s}}{0}}$

Therefore $\frac{C'}{\prod_{i \in [1, w_1]} e(\mathbf{C}_{\mathbf{y}}^{\mathrm{cpa}}[i], \hat{\mathbf{K}}_{\mathsf{x}}[i])} = M$

Our Conversion Technique

- Dec($\mathbf{C}_\mathbf{y}, \mathbf{K}_\mathbf{x}$): Computes $\tilde{K}_\mathbf{x}[i'] = \prod_{i\in[m_1]} (\mathbf{K}_\mathbf{x}[i])^{E_{ii'}}$ for $\mathbf{E} \leftarrow \mathsf{Pair}(\mathbf{x}, \mathbf{y}, N)$.

  defines $\hat{\mathbf{K}}_\mathbf{x} = (K_0, \Phi\cdot\tilde{K}_\mathbf{x}[1], \tilde{K}_\mathbf{x}[2], \ldots, \tilde{K}_\mathbf{x}[w_1])$ where $K_0 = g_2^{-\mathbf{Z}\binom{\mathbf{t}}{0}}$ and $\Phi = g_2^{(\eta\mathbf{H}_{n+1}^\top + \mathbf{H}_{n+2}^\top)\mathbf{Z}\binom{\mathbf{t}}{0}}$ for $\eta = \mathcal{H}(\mathbf{C}_\mathbf{y}^{\mathrm{cpa}})$ and $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_p^d$.

  Then it computes $e(g_1, g_2)^{\boldsymbol{\alpha}^\top\mathbf{B}\binom{\mathbf{s}}{0}} = e(C_0', \hat{\mathbf{K}}_\mathbf{x}[0]) \prod_{i\in[1,w_1]} e(\mathbf{C}_\mathbf{y}^{\mathrm{cpa}}[i], \hat{\mathbf{K}}_\mathbf{x}[i])$ which is used to unblind C'.

Correctness: $\prod_{i\in[1,w_1]} e(\mathbf{C}_\mathbf{y}^{\mathrm{cpa}}[i], \hat{\mathbf{K}}_\mathbf{x}[i]) = e(g_1, g_2)^{\boldsymbol{\alpha}^\top\mathbf{B}\binom{\mathbf{s}}{0} + (\mathbf{t}^\top 0)\mathbf{Z}^\top(\eta\mathbf{H}_{n+1} + \mathbf{H}_{n+2})\mathbf{B}\binom{\mathbf{s}}{0}}$

$e(C_0', \hat{\mathbf{K}}_\mathbf{x}[0]) = e(g_1, g_2)^{-(\mathbf{t}^\top 0)\mathbf{Z}^\top(\eta\mathbf{H}_{n+1} + \mathbf{H}_{n+2})\mathbf{B}\binom{\mathbf{s}}{0}}$

Therefore $\dfrac{C'}{e(C_0', \hat{\mathbf{K}}_\mathbf{x}[0]) \prod_{i\in[1,w_1]} e(\mathbf{C}_\mathbf{y}^{\mathrm{cpa}}[i], \hat{\mathbf{K}}_\mathbf{x}[i])} = M$

We see that number of extra pairing computation in this scheme is 1.

Conclusion

- Efficient and generic conversion of CPA-secure PE to CCA-secure PE in prime order groups.
- Pair and predicate encodings are equivalent in some restricted settings.
- Generic integration of *pair encoding* with *dual system group* results in a simpler proof.

Conclusion

- Efficient and generic conversion of CPA-secure PE to CCA-secure PE in prime order groups.
- Pair and predicate encodings are equivalent in some restricted settings.
- Generic integration of *pair encoding* with *dual system group* results in a simpler proof.

Thank You