Intelligent Information Management, 2009, 6-14
doi:10.4236/iim.2009.11002 Published Online July 2009 (http://www.scirp.org/journal/iim)

Investigations on Simultaneously Secure IBE Scheme and Security Proofs under RO and Non-RO Model

Zhengtao JIANG [1], Yongbin WANG [1], Yong WANG [2], Yumin WANG [3]
[1] *School of Computer Science, Communication University of China, Beijing* 100024*, China*
[2] *School of Computer Science, Beijing University of Technology, Beijing* 100022*, China*
[3] *National Key Lab. of Integrated Service Networks, Xidian University, Xi'an* 710071*, China*

Abstract: Investigations on the proof theory and methods of simultaneously provable security under multi-model helps to construct formally secure cryptographic scheme under multi-environments. Further research is provided on the construction of efficient IBE scheme and provable security under CCA model. Elementary investigations on pairing-based CCA secure IBE scheme which is provably secure based on RO and non-RO model were provided. It avoided the induction inefficiency in the previous proofs. Based on the standard DBDH problem, its provable security under both models is argued. The proposed scheme has low parameter and ciphertext size, which were composed of four group element respectively. The induction of security proof is more concise and tight.

Keywords: IBE, bilinear pairing, DBDH, multi-model security, IND-CCA secure, IND-sID secure

RO 和無 RO 模型下同時安全 IBE 體制及安全證明的研究

姜正濤 [1]，王永濱 [1]，王勇 [2]，王育民 [3]

[1] 中國傳媒大學 計算機學院，北京 10024；[2] 北京工業大學 計算機學院，北京 100022
[3] 西安電子科技大學 綜合業務網國家重點實驗室，陝西 西安 710071

摘　要：探討多模型下同時安全的體制構造、證明理論與方法有助於構造多環境下形式化安全的密碼體制，本文進一步研究了高效的 IBE 體制構造和 CCA 模式下的可證明安全，基於所構造的體制探討了 RO 和無 RO 模型下的安全證明，並避免了本文指出的以往證明中在規約效率方面的不足，基於標準 DBDH 問題在兩種模型下證明體制的可證明安全性，另外該體制的特點是參數規模和密文長度更小，分別為 4 個群元素，安全證明規約更簡化和緊致。

關鍵詞: IBE，雙線性對，DBDH，多模型安全，IND-CCA 安全，IND-sID 安全
中圖分類號: TP309

1. 引 言

基於身份的加密體制(IBE)以主體身份 ID 作為主體的公鑰，如 Email、電話號碼等，這一方法避免了 PKI 環境下 CA 證書傳輸、驗證以及證書管理的複雜維護等問題[1][2]，基於 RSA 假設，A. Shamir 在 1984

基金專案：國家"211 工程"資助專案、國家自然科學基金資助項目(90412011).

年提出了基於身份公鑰密碼系統的概念[3]，自然地解決公鑰和實體身份的綁定問題，簡化公鑰證書的管理。IBE 通常分為 4 個步驟：(1) Setup，生成系統公開參數和主密鑰 MK；(2) Extract，運用 MK 為主體生成私鑰；(3) 加密；(4) 解密。與 PKI 不同的是，只要在階段(1)建立的公開參數後，即使主體還未建立自己的私鑰，成員也可以使用主體的身份對消息加密。隨後研究者對 IBE 及其簽名應用等領域進行了廣泛深入的研究[4-8]。

2001 年 D. Boneh 等利用雙線性線對構造了第一個安全有效的 IBE 體制，並定義了 IBE 體制的選擇明文(IND-ID-CPA)和選擇密文安全性(IND-ID-CCA)，目前 IND-ID-CCA 逐漸成為被普遍接受的安全定義，其中的攻擊者可以適應性選擇成員身份（公鑰）和密文分別進行私鑰提取和解密詢問，基於判斷雙線性對 Diffie-Hellman (DBDH)問題，在隨機預言(RO)模型下證明瞭體制的 IND-ID-CPA 安全性，並進一步把體制改進成具有 IND-ID-CCA 安全性，其語義安全等價於 DBCH 問題[9]。

R. Canetti 等運用雙線性對基於他們所提出的選擇身份(sID)安全定義[10][11]，在無 RO 模型下構造了一個可證明安全的層次 IBE 體制，在安全證明中，攻擊者可以適應性地選擇身份和密文進行解密預言詢問，但是其中的攻擊者需要在系統生成公開參數之前承諾(commit)攻擊目標的身份，另外私鑰詢問階段所選擇的身份既不能是攻擊目標身份也不能是該身份的任何首碼，D, Boneh 等稱其為 IND-sID-CCA 安全[12]。這是一種基於相對弱的安全模型的證明方法，在體制的解密過程中，對應於身份串的每一比特均要執行一次對運算，實現效率比較低。

D. Boneh 和 X. Boyen[12][13]對 R. Canetti 等[10]的 IND-sID-CCA 安全模式作了進一步限制，給出選擇選擇身份、選擇明文的安全性(IND-sID-CPA)定義，在 IND-sID-CPA 安全模式中，攻擊者不能進行解密預言詢問。基於 IND-sID-CPA 攻擊模式，D. Boneh 等在無 RO 模型下對兩個 IBE 體制及安全證明進行了研究，第一個為層次身份加密(HIBE)體制，證明瞭其 IND-sID-CPA 安全性基於 DBDH 問題，但其主體私鑰、公鑰以及密文規模比較大，加解密效率比較低。第二個體制在 D. Boneh 等定義的一個非標準的問題假設下(判斷雙線性 DH 逆問題 q-DBDHI)證明瞭體制的 IND-sID-CPA 安全性[12]。

B. Waters 對文[12]中的 IBE 體製作了進一步研究[14]，根據主體身份逐比特在橢圓曲線群中執行群運算，縮短了密文長度，提高了效率，在標準模型下把適應性選擇身份-選擇明文(IND-ID-CPA)安全性規約到 DBDH 問題，攻擊者在攻擊之前不需要承諾攻擊目標的身份，是在比較弱的非 CCA 攻擊模式下證明的，另外系統參數規模仍然比較大，安全證明規約不夠緊致，每次模擬只能以比較低的概率成功，安全證明中也存在不足。針對 IBE 參數規模和安全證明規約存在的上述問題，B. Waters 在文[14]最後提出了兩個進一步研究的問題：降低 IBE 體制的公開參數規模以及在無 RO 模型下更緊致的安全證明。目前對密碼體制的可證明安全研究，大都基於單一的安全模型，探討多模型下可證明安全的理論與方法可以為密碼體制的安全性提供更多的安全論證，是可證明安全領域有意義的研究內容[15][14][9]。

針對上述幾方面問題，本文進一步研究了雙線性對上構造公開參數規模小的選擇密文(CCA)可證安全的 IBE 體制，以及探討在 RO 和無 RO 兩種模型下可證明安全的體制的構造和證明方法，基於 DBDH 問題假設，嘗試分別在 RO 模型和無 RO 模型下證明體制的安全性，避免以往證明中的一個不足，系統參數規模小，公開參數與密文長度分別為 4 個群元素，證明規約更簡化和緊致，多模型下同時安全的體制構造和證明的理論與方法還處於研究初步階段，還沒有完善的證明，這一問題的研究有助於構造多攻擊環境下形式化安全的密碼體制，是可證明安全領域的一項有意義的研究內容。

2. 雙線性對與安全性定義

設 G_1 為 q 階加群，G_2 為 q 階乘群，其中 q 為素數，P 為 G_1 的生成元，定義在 $G_1 \times G_1$ 上的對是一個映射 $e: G_1 \times G_1 \to G_2$，滿足以下條件[16-18]：

1. 雙線性：對任意的 $Q, R, W \in G_1$，有
$$e(P, Q+R) = e(P, Q) \cdot e(P, R),$$
$$e(P+Q, R) = e(P, R) \cdot e(Q, R)。$$

2. 非退化：$e(P, P) \neq 1$。

3. e 可有效計算：對任意的 $Q,R \in G_1$，$e(Q,R)$ 可有效計算。

e 可以通過有限域上超奇異橢圓曲線中的 Weil 對 Tate 對來實現。

定義 1 雙線性參數生成器 Param-*Gen* 一個雙線性參數生成器 Param-*Gen* 為一個概率多項式時間演算法，輸入安全參數 k，輸出一個雙線性五元組 (q,G_1,G_2,e,P) 作為雙線性參數，其中 q 為大素數滿足 $q \geq 2^k$，G_1 為 q 階加群，G_2 為 q 階乘群，P 為 G_1 的生成元，$e: G_1 \times G_1 \to G_2$ 是一個雙線性對。

定義 2 計算雙線性 Diffie-Hellman (CBDH) 問題 給定 $P,aP,bP,cP \in G_1$，對於隨機的 $a,b,c \in Z_q^*$，計算 $e(P,P)^{abc} \in G_2$。

演算法 A 成功計算 CBDH 問題的概率記為：

$$Succ_{Gen,\mathcal{A}}^{CBDH} = \Pr[e(P,P)^{abc} \leftarrow A(P,aP,bP,cP)]$$

這裏 a,b,c 是 Z_q^* 中的亂數。

CBDH 問題假設：對於隨機選取的 $a,b,c \in Z_q^*$，不存在有效的多項式時間演算法 A，使得對於某個不可忽略的 ε，滿足 $Succ_{Gen,\mathcal{A}}^{CBDH} \geq \varepsilon$。

定義 3 判斷雙線性 Diffie-Hellman (DBDH)問題實例生成器 DBDH-*Gen* 一個判斷雙線性 Diffie-Hellman 問題實例生成器 DBDH-*Gen* 為一個概率多項式時間演算法，輸入一個雙線性五元組 (q,G_1,G_2,e,P)，輸出判斷雙線性五元組 $(P,a_iP,b_iP,c_iP,T_i) \in G_1^4 \times G_2$，這裏 $a_i,b_i,c_i (i=1,2...,n)$ 是 Z_q^* 中的亂數，T 為 G_2 中的亂數。

定義 4 判斷雙線性 Diffie-Hellman (DBDH)問題 輸入一個判斷雙線性五元組 $(P,a_iP,b_iP,c_iP,T_i) \in G_1^4 \times G_2$，判斷 $T_i = e(P,P)^{a_ib_ic_i}$ 是否成立。

演算法 A 成功判斷 DBDH 問題的概率記為：

$$Succ_{Gen,\mathcal{A}}^{DBDH} = \Pr[1 \leftarrow A(P,aP,bP,cP,e(P,P)^{abc})]$$

這裏的 $a_i,b_i,c_i (i=1,2...,n)$ 是 Z_q^* 中的亂數，T 為 G_2 中的亂數。

定義 5 DBDH 問題假設 對於隨機選取的 $a,b,c \in Z_q^*$ 和 $T \in G_2$，不存在演算法 B 可以在 t 時間內以不小於 ε 的優勢解決 DBDH 問題，即不存在演算法 B 使得 $Succ_{Gen,\mathcal{A}}^{DBDH} \geq \varepsilon + \frac{1}{2}$，此時稱 (t,ε) -DBDH 假設成立。

定義 6 RO 模型下 $(t,q_{ID},q_E,q_D,\varepsilon)$ -IND-ID -CCA 安全稱一個 IBE 體制是 $(t,q_{ID},q_E,q_D,\varepsilon)$ -IND-ID-CCA 安全的，如果不存在在適用性選擇密文攻擊者可以在 t 時間內、經過 q_{ID} 次身份預言詢問、q_E 次私鑰提取預言詢問和 q_D 次解密預言詢問，以不小於 ε 的優勢成功攻擊體制的語義安全性。

3. RO 和無 RO 模型下的安全 IBE

Setup: 密鑰生成中心 KGC 輸入安全參數 k，由雙線性參數生成器 Param-*Gen* 輸出一個雙線性五元組 (q,G_1,G_2,e,P)，這裏 G_1 為 q 階加群，G_2 為 q 階乘群，其中 q 為素數，P 為 G_1 的生成元，$e: G_1 \times G_1 \to G_2$ 是一個雙線性對。

$H: \{0,1\}^* \to G_1^*$ 為把一 bit 串映射到 G_1 中元素，滿足當 $x \neq y$ 時，有 $H(x) \neq H(y)$。

隨機選取 $\alpha \in Z_q$，計算 $P_1 = \alpha P$，隨機選取 $P_2, P_3 \in G_1$，生成主密鑰 $MK: \alpha P_2$，公開參數 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$。

KeyGen: 設主體的身份為 ID，向 KGC 申請私鑰；KGC 計算 $Q_{ID} = H(ID)$，隨機選取 $r \in Z_q$，計算主體 ID 的私鑰

$$d_{ID} = < \alpha P_2 + rP_2 + rQ_{ID} + rP_3, rP >,$$

並安全發送給主體 ID。

Encryption: 待加密的消息為 M，加密者隨機選取 $t \in Z_q$，計算密文

$$C = < e(P_1,P_2)^t M, tP, tP_2 + tQ_{ID} + tP_3 >$$

Decryption: 解密者收到 $C = < C_1, C_2, C_3 >$，根據自己的私鑰 $d_{ID} = < d_1, d_2 >$，計算得到明文

$$M = C_1 \frac{e(d_2, C_3)}{e(d_1, C_2)}$$

4. 可行性分析與安全證明

4.1 可行性分析

4.1.1 私鑰生成有效性

主體 ID 收到私鑰

$d_{ID}=(d_1,d_2)=<\alpha P_2+rP_2+rQ_{ID}+rP_3,rP>$，通過以下計算驗證私鑰 d_{ID} 是否的確是由 KGC 為自己生成的有效私鑰：

$$\frac{e(d_1,P)}{e(d_2,Q_{ID})e(d_2,P_3)}\stackrel{?}{=}e(d_2,P_2)e(P_2,P_1)$$

事實上，

$$\frac{e(d_1,P)}{e(d_2,Q_{ID})e(d_2,P_3)}=\frac{e(\alpha P_2+rP_2+rQ_{ID}+rP_3,P)}{e(rP,Q_{ID})e(rP,P_3)}$$
$$=e(d_2,P_2)e(P_2,P_1)\text{。}$$

4.1.2 解密可行性

解密者通過計算 $C_1\frac{e(d_2,C_3)}{e(d_1,C_2)}$ 可以得到相應的明文。

事實上，

$$C_1\frac{e(d_2,C_3)}{e(d_1,C_2)}$$
$$=e(P_1,P_2)^tM\frac{e(rP,tP+tQ_{ID}+tP_3)}{e(\alpha P_2+rP_2+rQ_{ID}+rP_3,tP)}$$
$$=M\text{。}$$

4.1.3 效率分析

加密需要一個對運算（可預計算），二個橢圓曲線上標量乘法運算，一個有限域上乘法運算，一個有限域上指數計算。

解密需要兩個對運算，一個有限域上乘法運算，一個有限域上除法運算。

4.2 RO 模型下的安全性證明

定理 1 在 RO 模型下，如果 $(t+O(q_{ID}+q_E+q_D),\varepsilon)$-DBDH 假設成立，則該 IBE 體制是 $(t,q_{ID},q_E,q_D,\varepsilon)$-IND-CCA 安全的，這裏攻擊者 A 進行 q_{ID} 次身份 Oracle 詢問，q_E 次私鑰提取 Oracle 詢問、q_D 次解密 Oracle 詢問。

證明 由判斷雙線性 DH 問題實例生成器 DBDH-*Gen* 隨機生成一個判斷雙線性五元組 (P,aP,bP,cP,T)，A 為 $(t,q_{ID},q_E,q_D,\varepsilon)$-IND-CCA 攻擊者，在 RO 模型下攻擊者 A 隨機選擇身份與模擬者 B 進行私鑰提取和解密詢問攻擊遊戲，模擬者 B 返回相應的私鑰作為對 A 私鑰詢問的應答，並對提交的密文進行解密應答，充分利用了 A 的攻擊能力，經過 q_{ID} 次身份 Oracle 詢問，q_E 次私鑰提取詢問、q_D 次解密詢問和一次挑戰，最後 A 以不可忽略的概率成功攻擊 IBE 體制的 IND-CCA 安全性，那麼存在一個演算法運用 A 的攻擊能力，可以不可忽略的概率成功解決 DBDH 問題，從而證明體制的安全性。

Setup: 密鑰生成中心 KGC 輸入安全參數 k，由雙線性參數生成器 Param-*Gen*，輸出一個雙線性五元組 (q,G_1,G_2,e,P)。

由判斷雙線性 DH 問題實例生成器 DBDH-*Genn* 生成一個判斷雙線性五元組實例 $(P,A,B,C,T)=(P,aP,bP,cP,T)$。

B 構造 IBE 體制，令 $P_1=A=aP$，$P_2=B=bP$，隨機選取 $P_3\in G_1$，相應的公開參數為 Params=$<q,G_1,G_2,e,P,P_1,P_2,P_3>$。

Phase 1: 攻擊者 A 與模擬者 B 執行 l $(<q_{ID})$ 次身份 Oracle 詢問-應答、n $(<q_E)$ 次私鑰 Oracle 詢問-應答和 u $(<q_D)$ 次解密 Oracle 詢問-應答。

B 構造一個身份 Oracle 應答列表 T_{ID-H}，初始為空。

1) 攻擊者 A 提交一個身份 ID_i 進行身份 Oracle 詢問：

如果 ID_i 已被 A 詢問過，B 從列表 T_{ID-H} 中直接讀取；

否則，B 隨機選取 $m_i\in Z_q$，令 $H(ID_i)=Q_i=m_iP-P_3$ 發給 A，並把身份詢問-應答 $<ID_i,Q_i>$ 添加到 T_{ID-H} 中。

由於 $m_i\in Z_q$ 是由 B 隨機選取的，Q_i 與 G_1 中隨機元素不可區分。

如果攻擊者 A 需要對主體 ID_i 進行私鑰 Oracle 詢問，執行下麵的 2）。

2) 攻擊者 A 提交一個身份 ID_i 進行私鑰 Oracle 詢問：

如果身份 ID_i 在 1)中被詢問過, 則 B 直接從 T_{ID-H} 讀取 $H(ID_i)$，否則隨機生成新的 $H(ID_i)=Q_i=m_iP-P_3$ 發送給 A，並把新的身份詢問-應答對 $<ID_i,Q_i>$ 添加到 T_{ID-H} 中。

B 隨機選取 $r_i\in Z_q$，輸出二元組 $d_i=(d_{i,0},d_{i,1})$ $=(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,r_iP-P_1)$。

事實上，

$$d_{i,0}=-m_iP_1+r_iP_2+r_iQ_i+r_iP_3$$

$$=aP_2+(-a)P_2+-m_iP_1+r_iP_2+r_iQ_i+r_iP_3$$

$$=aP_2+(r_i-a)(P_2+Q_i+P_3)$$

$$d_{i,1}=r_iP-P_1=(r_i-a)P$$

令 $r_i'=r_i-a$，則 $d_i=(d_{i,0},d_{i,1})$ $=(aP_2+r_i'P_2+r_i'Q_i+r_i'P_3,r_i'P)$。

攻擊者 A 可以通過以下等式驗證私鑰應答的正確性：

$$\frac{e(d_{i,1},P)}{e(d_{i,2},Q_i)e(d_2,P_3)}=\frac{e(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,P)}{e(r_iP-P_1,Q_i)e(r_iP-P_1,P_3)}$$

$$=e(d_{i,2},P_2)e(P_2,P_1)$$

所以，

$d_i=(d_{i,0},d_{i,1})=(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,r_iP-P_1)$ 是身份 $Q_i=H(ID_i)$ 對應的有效私鑰。

如果攻擊者 A 需要對主體 ID_i 進行解密 Oracle 詢問，執行下麵的 3)。

3) 攻擊者 A 選擇一條明文 M, 構造合法的密文, 進行解密 Oracle 詢問：

攻擊者 A 選擇一個身份 ID_i，如果身份 ID_i 在 1), 2) 中被詢問過, 則 A 直接生成合法密文, 否則把身份 ID_i 提交給 B，B 隨機選取 $m_i\in Z_q$ 並生成新的 $H(ID_i)=Q_i=m_iP-P_3$ 發送給 A, 並把新的 $<ID_i,Q_i>$ 添加到 T_{ID-H} 中。

A 隨機選取 $t\in Z_q$，生成合法密文 $C=<C_1,C_2>=<e(P_1,P_2)^tM,tP,tP_2+tQ_i+tP_3>$ 發送給模擬者 B。

模擬者 B 收到密文 C 後，如果 A 在 2)對身份 ID_i 進行過私鑰 Oracle 詢問，則直接使用已生成的私鑰進行解密，否則針對身份 ID_i，B 隨機選取 $r_i\in Z_q$ 生成新的 $d_i=(d_{i,0},d_{i,1})$ $=(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,r_iP-P_1)$ 進行解密：

B 計算

$$C_1\frac{e(d_{i,2},C_3)}{e(d_{i,1},C_2)}$$

$$=e(P_1,P_2)^tM\frac{e(r_iP-P_1,tP_2+tQ_i+tP_3)}{e(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,tP)}$$

=M

並把 M 發送給 A。

由於 1),2),3)中對於新的身份 ID_i 和新的私鑰詢問，$m_i,r_i\in Z_q$ 是由 B 隨機生成的，攻擊者 A 能夠得到滿意的身份、私鑰和解密 Oracle 應答，模擬者 B 成功模擬攻擊者 A 在 Phase1 階段的詢問。

A 分別重複 1), 2),3) l $(<q_{ID})$ 次、n $(<q_E)$ 次和 u $(<q_D)$ 次，完成 Phase1。

Challenge: 類比者 B 對 DBDH 問題實例 $(P,A,B,C,T)=(P,aP,bP,cP,T)$ 的判斷沒有任何優勢，B 所能做的是構造適於 A 展開攻擊的場景，充分利用 A 的 IND-CCA 能力。

攻擊者 A 提交兩條明文 $M_0,M_1\in\{0,1\}^n$ 和一個身份 ID_{ch}，為充分運用 A 的攻擊能力，對 ID_{ch} 唯一的要求是沒有在 Phase1 進行過私鑰詢問。模擬者 B 收到 M_0,M_1 和 ID_{ch} 後, 根據 DBDH 問題實例 (P,A,B,C,T) 構造合法密文。

模擬者 B 隨機選取 $k\in Z_q$，計算 $Q_{ch}=kP-P_2-P_3$，令 $H(ID_{ch})=Q_{ch}$，把 $H(ID_{ch})=Q_{ch}$ 發送給 A，並在 T_{ID-H} 中添加 $<ID_{ch},Q_{ch}>$。

模擬者 B 構造合法密文：

B 擲幣隨機選取 $\gamma\in\{0,1\}$，構造密文 $Z=(T\cdot M_\gamma,C,kC)$，併發送給 A。

事實上，如果 $(P,A,B,C,T)=(P,aP,bP,cP,T)$ 是 DBDH 問題五元組，即 $T=e(P,P)^{abc}$，則有

$$Z=(T\cdot M_\gamma,C,kC)=(e(P_1,P_2)^cM_\gamma,cP,c\cdot kP)$$

$$=(e(P_1,P_2)^cM_\gamma,cP,c\cdot P_2+c\cdot Q_{ch}+c\cdot P_3)$$

是明文 M_γ 對應的有效密文。

另外，由於 $k \in Z_q$ 隨機選取，在攻擊者 A 看來，Q_{ch} 與從 G_1 中隨機選取的元素隨機性不可區分。

Phase 2: 類似 Phase1，攻擊者 A 與模擬者 B 分別重複執行 $q_E - l - 1$ 次身份 Oracle 詢問-應答、$q_E - n$ 私鑰 Oracle 詢問-應答和 $q_D - u$ 解密 Oracle 詢問-應答，唯一限制是 A 不能對主體身份 ID_{ch} 進行私鑰和解密 Oracle 詢問。

Quess: 最後，攻擊者 A 輸出對 γ 的猜測 γ'。

4.3 無 RO 模型下的安全性證明

下麵的證明擴展了 R. Canetti 等基於 DBDH 問題在無 RO 模型下構造的選擇身份（sID）安全證明，攻擊者除了擁有文[10]中描述的攻擊能力外，還可以選擇 DBDH 問題實例（也可固定），攻擊者完成第一階段的選擇身份、選擇 DBDH 問題實例的私鑰和解密預言詢問後，在 challenge 階段攻擊者選擇目標 DBDH 問題實例和身份進行挑戰，模擬者在對 DBDH 問題沒有任何優勢的情況下，基於問題參數生成合法密文，在攻擊遊戲結束後，模擬者利用攻擊者的選擇身份、選擇 DBDH 問題實例的 CCA（IND-sID||sIN-CCA）攻擊能力，回答 DBDH 問題。

定理 2 在無 RO 模型下，如果 $(t+O(q_{ID}+q_{IN}+q_E+q_D),\varepsilon)$ -DBDH 假設成立，則該 IBE 體制是 $(t,q_{ID},q_{IN},q_E,q_D,\varepsilon)$ -IND-sID||sIN-CCA 安全的，這裏攻擊者 A 進行 q_{ID} 次身份選擇、q_{IN} 次實例選擇、q_E 次私鑰提取 Oracle 詢問、q_D 次解密 Oracle 詢問。

證明 由判斷雙線性 DH 問題實例生成器 DBDH-*Gen* 隨機生成 n 個判斷雙線性五元組 (P,a_iP,b_iP,c_iP,T_i) , $i=1,2,...,n$，A 為攻擊者，類比者 B 根據 A 選擇攻擊實例和身份構造適合 A 展開攻擊的攻擊場景，以充分運用 A 具有的攻擊能力，攻擊者 A 隨機選擇身份和DBDH問題實例與類比者B進行私鑰提取詢問和解密詢問攻擊遊戲，模擬者 B 提交相應的私鑰和明文分別作為對 A 私鑰詢問和解密詢問的應答，充分利用了 A 的攻擊能力，在時間 t 內，進行 q_{ID} 次身份選擇、q_{IN} 次實例選擇、q_E 次私鑰提取 Oracle 詢問、q_D 次解密 Oracle 詢問和一次挑戰，最後 A 以不可忽略的概率成功攻擊 IBE 體制的語義安全性，B 把 A 的這一適應性攻擊能力規約到 DBDH 問題的解決，從而在無 RO 模型下證明體制安全性。

Setup: 密鑰生成中心 KGC 輸入安全參數 k，由雙線性參數生成器 Param-*Gen*，輸出一個雙線性五元組 (q,G_1,G_2,e,P)。

根據體制的建立階段，設元素變換函數 $H(\cdot)=h(\cdot)P \in G_1$ 為 $\{0,1\}^* \to G_1^*$ 的抗碰撞 Hash 函數，$h:\{0,1\}^* \to Z_q$ 為一密碼學 Hash 函數，如 SHA-1 等，實現把不同的身份 ID 映射為 G_1 中不同的群元素，記 $H(ID)=h(ID)P=h_{ID}P$。

由判斷雙線性 DH 問題實例生成器 DBDH-*Genn* 生成 n 個判斷雙線性五元組實例 (P,a_iP,b_iP,c_iP,T_i) , $i=1,2,...,n$。

對於 A 提交一個 DBDH 問題實例 (P,a_iP,b_iP,c_iP,T_i)，相應的公開參數為 *Params*= $<q,G_1,G_2,e,P,P_1,P_2,P_3>$，其中 $P_1=a_iP, P_2=b_iP$，$P_3 \in G_1$ 為由 B 根據 DBDH 問題實例隨機選取的元素。

Phase 1: 攻擊者 A 隨機選取 l $(<q_{ID})$ 個身份、k $(<q_{IN})$ 個 DBDH 問題實例 (P,a_iP,b_iP,c_iP,T_i)、與模擬者 B 執行 n $(<q_E)$ 次私鑰 Oracle 詢問-應答和 u $(<q_D)$ 次解密 Oracle 詢問-應答。

1) 攻擊者 A 隨機選擇 DBDH 問題實例 (P,a_iP,b_iP,c_iP,T_i) 和身份 ID_j。

類比者 B 根據 A 選擇的參數構造合法的 IBE 實例 *Params*= $<q,G_1,G_2,e,P,P_1,P_2,P_3>$，其中 $P_1=A_i=a_iP, P_2=B_i=b_iP$，B 隨機選取 $m \in Z_q$，計算 $P_3=mP$*，由於 $m \in Z_q$ 是由 B 隨機選擇的，在 A 看來 P_3 與 G_1 中的隨機元素不可區分。

如果攻擊者 A 需要對主體 ID_j 進行私鑰 Oracle 詢問，執行下麵的 2）。

2) 攻擊者 A 提交一個身份 ID_j 進行私鑰 Oracle 詢問：

B 隨機選取 $r_j \in Z_q$，輸出二元組 $d_j=(d_{j,0},d_{j,1})$ $=(-mP_1-h_jP_1+r_jP_2+r_jQ_j+r_jP_3, r_jP-P_1)$。

事實上，

$$d_{j,0}=-mP_1-h_jP_1+r_jP_2+r_jQ_j+r_jP_3$$
$$=aP_2+(-a)(P_2+Q_j+P_3)+r_jP_2+r_jQ_i+r_jP_3$$

*這裏 $P_3=mP$ 也可以在 Phase1 階段之前由模擬者 B 隨機選定.

$= aP_2 + (r_j - a)(P_2 + Q_j + P_3)$

$d_{j,1} = r_j P - P_1 = (r_j - a)P$

令 $r'_j = r_j - a$，則 $d_j = (d_{j,0}, d_{j,1})$ $= (aP_2 + r'_j P_2 + r'_j Q_j + r'_j P_3, r'_j P)$ 是關於 IBE 實例 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$，身份 ID_j 對應的有效私鑰。

如果攻擊者 A 需要進一步對主體 ID_j 進行解密 Oracle 詢問，執行下麵的 3)。

3) 攻擊者 A 選擇一條明文 M, 構造合法的密文，進行解密 Oracle 詢問：

攻擊者 A 選擇一個身份 ID_j，隨機選取 $t \in Z_q$，生成密文

$C = < C_1, C_2 > = < e(P_1, P_2)^t M, tP, tP_2 + tQ_j + tP_3 >$ 發送給模擬者 B。

模擬者 B 收到密文 C 後，如果 A 在 2)中對身份 ID_j 進行過私鑰 Oracle 詢問，則直接使用已生成的私鑰進行解密，否則針對身份 ID_j，B 隨機選取 $r_j \in Z_q$ 生成新的私鑰 $d_j = (d_{j,0}, d_{j,1})$ $= (-mP_1 - h_j P_1 + r_j P_2 + r_j Q_j + r_j P_3, r_j P - P_1)$ 進行解密：

B 計算

$$C_1 \frac{e(d_{j,1}, C_3)}{e(d_{j,0}, C_2)}$$

$$= e(P_1, P_2)^t M \frac{e(r_j P - P_1, tP_2 + tQ_j + tP_3)}{e(-mP_1 - h_j P_1 + r_j P_2 + r_j Q_j + r_j P_3, tP)}$$

=M

並把 M 發送給 A。

關於 IBE 實例 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$，由於 1),2),3)中對於身份 ID_j 和私鑰詢問，$r_j \in Z_q$ 是由 B 隨機生成的，攻擊者 A 能夠得到滿意的私鑰和解密 Oracle 應答，模擬者 B 成功模擬攻擊者 A 在 Phase1 階段的私鑰和解密 Oracle 詢問。

A 分別重複 1),2),3)，隨機選取 l $(< q_{ID})$ 個身份、k $(< q_{IN})$ 個 DBDH 問題實例 $(P, a_i P, b_i P, c_i P, T_i)$、與模擬者 B 執行 n $(< q_E)$ 次私鑰 Oracle 詢問-應答和 u $(< q_D)$ 次解密 Oracle 詢問-應答，完成 Phase1。

Challenge: 攻擊者 A 提交兩條明文 $M_0, M_1 \in \{0,1\}^n$ 和一個主體身份 ID_{ch}，並從 DBDH 問題實例中隨機選取 $(P, A, B, C, T) = (P, a_i P, b_i P, c_i P, T_i)$，相應的公開參數為 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$，其中 $P_1 = a_i P, P_2 = b_i P$，$P_3 \in G_1$ 由 B 隨機選取, 這裏對 ID_{ch} 的唯一限制是在 Phase1 針對實例 $(P, a_i P, b_i P, c_i P, T_i)$ 沒有對 ID_{ch} 進行過私鑰詢問。

為充分利用攻擊者 A 的攻擊能力, 模擬者 B 隨機選擇 $k \in Z_q$，計算 $P_3 = kP - P_2 - Q_j$，令 $C = c_i P$，B 擲幣隨機選取 $\gamma \in \{0,1\}$，構造密文 $Z = (T \cdot M_\gamma, C, kC)$。

事實上，如果 $(P, A, B, C, T) = (P, a_i P, b_i P, c_i P, T_i)$ 是 BDH 五元組，即 $T = e(P,P)^{abc}$，則有

$Z = (T \cdot M_\gamma, C, kC) = (e(P_1, P_2)^c M_\gamma, cP, c \cdot kP) = (e(P_1, P_2)^c M_\gamma, cP, c \cdot P_2 + c \cdot P_3 + c \cdot P_3)$

是明文 M_γ 對應的有效密文。

另外，由於 $k \in Z_q$ 隨機選取，在攻擊者 A 看來，P_3 與從 G_1 中隨機選取的元素 $P'_3 \in G_1$ 隨機性不可區分。

Phase 2: 類似 Phase1 重複進行 $q_{ID} - l - 1$ 個身份選取、$q_{IN} - k - 1$ 個 DBDH 問題實例選取、$q_E - n$ 次私鑰 Oracle 詢問-應答和 $q_D - u$ 次解密 Oracle 詢問-應答，唯一限制是 A 不能針對 DBDH 問題實例 $(P, a_i P, b_i P, c_i P, T_i)$ 對主體身份 ID_{ch} 進行私鑰詢問。

Quess: 最後，攻擊者 A 輸出對 γ 的猜測 γ'。

分析：

對任意的 DBDH 問題實例 $(P, a_i P, b_i P, c_i P, T_i)$, $i = 1,2,...,n$，類比者 B 在沒有判斷優勢的情況下，通過類比適於 A 展開攻擊的場景，充分利用 A 的攻擊能力，最終回答 DBDH 問題。

(1) 在 Phase2 階段，對攻擊者 A 的唯一限制是 A 不能對 Challenge 階段的 < 實例, 身份 > 對 $< (P, a_i P, b_i P, c_i P, T_i), ID_{ch} >$ 私鑰詢問，即只要 $< (P, A, B, C, T), ID_i > \neq < (P, a_i P, b_i P, c_i P, T_i), ID_{ch} >$，$< (P, A, B, C, T), ID_i >$都可以在 Phase1,2 階段執行私鑰 Oracle 詢問-應答和解密 Oracle 詢問-應答，這種情況包含了文[14][10]安全證明中的私鑰提取詢問過程。

(2) 在 Challenge 階段，對於 DBDH 問題實例

(P,a_jP,b_jP,c_jP,T_j)，模擬者 B 沒有任何優勢，對於 A 隨機選擇的兩條明文 $M_0,M_1\in\{0,1\}^n$，B 通過構造有效的密文，利用攻擊者 A 的攻擊能力，並把這一能力規約到解決 DBDH 問題：(P,A,B,C,T) 是 BDH 五元組，當且僅當 A 可以正確判斷 $\gamma\in\{0,1\}$。

注：本文初步探討了同時在 RO 和無 RO 模型下的安全體制構造與安全證明，目前對密碼體制的構造和安全性證明大都基於單一的安全模型，多模型下的體制構造、安全模型與證明方法的研究還不成熟，還需要進一步做大量的研究。定理 2 中無 RO 模型下的安全證明中，其安全模型可以看作是 sID-CCA 安全的一個擴展，進一步研究參數規模小、多模型下可證安全的體制構造與證明方法對於構造多攻擊環境下安全的高效密碼體制具有重要意義。

4.4 相關工作分析

本文主要在B. Waters等對的IBE體制研究的基礎上做進一步研究[14][10](本文 IBE 體制同樣也可進一步構造 RO 和無 RO 模型下可證安全的簽名體制)，主要包括：對公開參數規模簡化（ RO 模型下可以令 $P_3=O$，進一步簡化系統參數而不影響證明)；把 CPA 模式下的安全改進到 CCA 模式下的安全；在此基礎上，探討同時在 RO 和無 RO 模型下安全的 IBE 體制構造與規約緊致的安全證明，並避免了文[14]證明中的一個不足。

在 B. Waters 的安全證明中[14]，模擬者選取的公開參數 $u'=g_2^{p-km+x'}g^{y'}$, $u_i=g_2^{x_i}g^{y_i}$， $i=1,2,...,n$，其中 $x',x_i\in[0,m-1]$， $y',y_i\in Z_p$， $m=4q$， q 為攻擊者的私鑰詢問次數， m,n,k 均為多項式有界量，攻擊者可以以不可忽略的概率猜得所有的 x' 和 $x_i\ (i=1,2,...,n)$（攻擊者也可以在 Phase1,2 階段，通過 $K(v)$ 的值，構造 n+1 組 $x'+\sum_{i\in V^*}x_i=0(\mathrm{mod}\,m)$ 同餘線性方程組求得 x' 和 $x_i\ (i=1,2,...,n)$)。

另外，在獲得 x' 和 $x_i\ (i=1,2,...,n)$後，公開參數指數部分包含 x' 和 x_i 成分起不到保密作用，而且額外增加計算量；另外在攻擊者 A 獲得 $x',x_i\ (i=1,2,...,n)$ 後，在 Challenge 階段，A 可以選擇身份 v^* 並計算 $F=x'+\sum_{i\in V^*}x_i$，如果 $F\neq km$，就把 v^* 提交給模擬者，這樣模擬者中斷模擬的概率為 1，而不是 $1-\frac{1}{8(n+1)q}$。類似地在 Phase1 或 Phase2 階段，利用已知的 $x',x_i\ (i=1,2,...,n)$，攻擊者可以選擇身份 v^* 並計算 $E=x'+\sum_{i\in V^*}x_i \bmod m$, 若 $E=0$, 提交身份 v^* 進行私鑰詢問，同樣模擬者會以概率 1 中斷模擬，而不是 $1-\frac{1}{8(n+1)q}$。出現這一情況的主要原因是安全規約的參數構造階段 $x',x_i\ (i=1,2,...,n)$的選擇範圍較小，不能很好隱藏冪指數，攻擊者 A 可以獲得 $x',x_i\ (i=1,2,...,n)$, 但是如果 $x',x_i\ (i=1,2,...,n)$的選擇範圍過大（ m 比較大），對於隨機選擇的身份 v^*，在 Challenge 階段攻擊遊戲中斷的概率同樣趨向於 1，對攻擊者來說參數和所選擇的身份不能看作是完全隨機的。

5. 結 論

本文基於 B. Waters 提出的兩個公開有待研究的問題和目前安全證明模型單一的問題，對雙線性對上構造 RO 與無 RO 模型下安全有效的 IBE 體制和安全證明做了進一步研究，用小規模的參數構造基於 RO 與無 RO 的 CCA 模式下可證安全 IBE 體制，避免以往證明中的一點不足，安全證明規約更簡化和緊致，基於 DBDH 假設，在 RO 和無 RO 模型下分別證明瞭體制的安全性，探討多安全模型下構造同時可證安全的密碼體制與證明方法是一個比較新穎和有意義的研究內容，有利於形式化保證密碼體制在多應用環境下的安全，其理論與方法還不成熟，還需要展開深入的研究。

REFERENCES

[1] Wang Yu-Min, Liu Jian-Wei. Communication network security-Theory and technique. Xidian University Press, 2002, 5 (王育民, 劉建偉. 通信網的安全—理論與技術. 西安電子科技大學出版社, 2002, 5).

[2] PKI. http://www.pki-page.org/

[3] Shamir A.. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto'84, LNCS 196, 1984, Berlin: Springer-Verlag, 47-53.

[4] Tanaka H.. A realization scheme for the identity-based cryptosystem. Advances in Cryptology-Crypto'87, LNCS 293, 1987, Berlin: Springer-Verlag, 341-349.

[5] Hühnlein D., Jacobson, M. Weber D.. Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders. Selected Areas in Cryptography, LNCS 2012, 2000, Berlin: Springer-Verlag, 275-287.

[6] Sakai R., Ohgishi K., Kasahara M.. Cryptosystems based on pairing. Symposium on Cryptography and Information Security-SCIS'00, 2000, Okinawa, Japan, 26-28.

[7] Ma Chun-Bo, Ao Jun, He Da-Ke. Multi-Signature and Group Signature Based on Bilinear Pairing. Chinese Journal of Computers, 2005, 28(9): 1558-1563 (in Chinese) (馬春波, 敖珺, 何大可. 基於雙線性映射的多重簽名與群簽名. 電腦學報, 2005, 28(9): 1558-1563).

[8] Boyen X., Waters B. Full-domain subgroup hiding and constant-size Group signatures. Advances in Cryptology-PKC'07, LNCS 4450, 2007, Berlin: Springer-Verlag, 1-15.

[9] Boneh D., Franklin M.. Identity-based encryption from the weil pairing. Advances in Cryptology-Crypto'01, LNCS 2139, 2001, Berlin: Springer-Verlag, 213-22.

[10] Canetti R., Halevi S., Katz J. A forward-secure public-key encryption scheme. Advances in Cryptology-EUROCRYPT'03, LNCS 2656, 2003, Berlin: Springer-Verlag, 255-271.

[11] Canetti R., Halevi S., Katz J. Chosen-ciphertext security from identity-based encryption. Advances in Cryptology-EUROC RYPT'04, LNCS 3027, 2004, Berlin: Springer-Verlag, 207-22.

[12] Boneh D., Boyen X. Efficient selective-ID secure identity based encryption without random oracles. Advances in Cryptology-EUROCRYPT'04, LNCS 3027, 2004, Berlin: Springer-Verlag, 223-238.

[13] Boneh D., Boyen X. Secure identity based encryption without random oracles. Advances in Cryptology-CRYPTO 2004, LNCS 3152, 2004, Berlin: Springer-Verlag, 443-59.

[14] Waters B. Efficient identity based encryption without random oracles. Advances in Cryptology-EUROCRYPT'05, LNCS 3494, 2005, Berlin: Springer-Verlag, 114-127.

[15] Goyal V. Reducing Trust in the PKG in Identity Based Cryptosystems. Advances in Cryptology – CRYPTO'07, NCS 4622, Berlin: Springer, 2007, 430-447.

[16] Washington L. C.. Elliptic Curve Number Theory and Cryptography. New York, CRC Press, 2003.

[17] Boneh D., Franklin M.. Identity-based encryption from the weil pairing. SIAM Journal of Computing, 2003, 32(3): 586-615.

[18] Ming Yang. Study and design of universal designated verifier signature schemes [Ph. D. dissertation]. Xi'an: Xidian University, 2007, 12 (in Chinese) ([明 07] 明洋. 廣義指定驗證者簽名體制的研究和設計[博士論文]. 西安電子科技大學, 2007, 12).

