On Anonymity of Group Signatures

Zhou Sujing and Lin Dongdai

SKLOIS Lab,Institute of Software, Chinese Academy of Sciences,
4# South Fourth Street, Zhong Guan Cun, Beijing 100080, P.R. China
zhousujing@is.iscas.ac.cn, ddlin@is.iscas.ac.cn

Abstract. A secure group signature is required to be anonymous, that is, given two group signatures generated by two different members on the same message or two group signatures generated by the same member on two different messages, they are indistinguishable except for the group manager. In this paper we prove the equivalence of a group signature's anonymity and its indistinguishability against chosen ciphertext attacks if we view a group signature as an encryption of member identity. Particularly, we prove ACJT's group signature is IND-CCA2 secure, so ACJT's scheme is anonymous in the strong sense. The result is an answer to an open question in literature.

1 Introduction

Group Signatures. A group signature, which includes at least algorithms of Setup, Join, Sign, Verify, Open and Judge (defined in Section 2), is motivated by enabling members of a group to sign on behalf of the group without leaking their own identities; but the signer's identity could be opened by the group manager, i.e., GM, on disputes.

Models of Group Signatures. In formally, a secure group signature scheme satisfies traceability, unforgeabilty, coalition resistance, exculpability, anonymity and unlinkability [1]. Formal models [2–5] of secure group signatures compressed the above requirements into redefined *anonymity*, *traceability*, *non-frameability.*

Anonymity. In [1], anonymity means similarly to IND-CPA (indistinguishable against chosen plaintext attacks, [6]), but in [2–5], it means similar to IND-CCA2 (indistinguishable against chosen ciphertext attacks, Section 2). We mean anonymity in the later strong sense hereafter.

An anonymous generic group signature is constructed based on any IND-CCA2 public encryption scheme [3]. The question is whether an IND-CCA2 public encryption is the minimum requirement to construct an anonymous group signature.

Some group signatures adopting ElGamal encryption are considered not anonymous and it is pointed out that after replacing the ElGamal encryption with a double ElGamal encryption scheme, an IND-CCA2 public encryption scheme, the group signatures will become anonymous (e.g. [4, 7]). In [8], it is further presented as an open question that whether ACJT's scheme [1] utilizing a single ElGamal encryption scheme provides anonymity. We explore this problem in this paper and answer the open question positively.

We point out that the problem lies in the behavior,specifically Open, of GM or OA (decryption oracle in the case of public encryption scheme).

Take an ordinary ElGamal encryption [9] as an example, let $(T_1 = m_i y^r, T_2 = g^r)$ be a challenge, an adversary can easily change it into a new ciphertext (my^sT_1, g^sT_2) and feed it to the decryption oracle, who definitely would reply with my^sm_i since the query is valid and different from challenge, then the adversary can resolve the challenge problem. In other word, ElGamal encryption is IND-CPA[6].

It is well known that an IND-CCA2 encryption scheme is available by double encrypting the same message under an IND-CPA encryption scheme [10]. The resulting IND-CCA2 ElGamal ciphertext consists of two independent ElGamal encryptions and a proof that the same plaintext is encrypted. The strong security of double-encryption transformed IND-CCA2 schemes comes from the difficulty of composing a valid ciphertext relating to the challenge by an computation bounded adversary, while a uncorrupted decryption oracle only decrypts queried valid ciphertexts.

Nevertheless a half corrupted decryption oracle might just ignore the invalidity of a ciphertext, decrypt any one of the two ciphertext pieces and reply to adversaries. It is possible in reality, for instance, a not well designed decryption software might misuse its decryption key by decrypting whatever it has got before checking the validity of the ciphertext, throw away decryption outputs inadvertently when they are found meaningless.

When ElGamal encryption is embedded in a group signature, e.g., ACJT scheme [1], the intuition is that it is difficult for an adversary to forge a new valid group signature from a challenge group signature, and the open oracle would firstly check the validity of a query before replying with the decrypted content.

In anonymous group signature schemes adopting double ElGamal encryption [4, 7, 8], if GM(OA) is half corrupted, i.e., it would directly open any queried group signature no matter whether the proof included in the ciphertext is correct or not, or the whole group signature is valid or not, anonymity of the group signature scheme is hard to guarantee.

So in case of half corrupted GM(OA), not all IND-CCA2 encryption will ensure anonymity of the group signatures; but for uncorrupted GM(OA) an IND-CPA secure encryption might be enough to ensure anonymity. The point is that GM(OA), i.e., the open oracle should check the validity before applying its private key instead of misusing it.

Our Contribution: We prove the equivalence between anonymity of a group signatures and IND-CCA2 of it, if we view the group signature as a public key encryption of group member identities. Particularly, we prove the ACJT's group signature is IND-CCA2 secure under the DDH assumption, so ACJT's scheme is anonymous in the strong sense of [3]. The result is an answer to an open question proposed in [8].

2 Formal Definitions

Group Signature [3]. Group manager GM is separated into issuer authority IA and opener authority OA. A group signature $\mathcal{GS}$ is composed of the following algorithms:

Setup. It includes a group key generation algorithm Gkg, and a user key generation algorithm Ukg.

- Gkg: a probabilistic polynomial-time algorithm for generating the group public key gpk and IA's secret key ik, as well as OA's secret key ok, given security parameter 1^{k_g};
- Ukg: a probabilistic polynomial-time run by a group member candidate to obtain a personal public and private key pair (upk_i, usk_i), given security parameter 1^k.

Join. A probabilistic polynomial-time interactive protocol between IA and a member candidate with user public key upk_i that results in the user becoming a new group member in possession of secret signing key gsk_i, i.e., a certificate signed by group issuer. They follow a specified relation R: $R(ID_i,upk_i,usk_i,gsk_i) = 1$. Set $Grp = Grp \cup \{ID_i\}$, where Grp denotes the set of valid group members, with initial value $NULL$.

Sign. A probabilistic polynomial-time algorithm which, on input a message M, gsk_i,upk_i,usk_i,$ID_i \in Grp$, and gpk, returns a group signature σ on M. (m, σ) can also be written as (m, ρ, π), where ρ is a blinding of member identity, π is a proof of correctness of ρ.

Verify. A deterministic polynomial-time algorithm which, on input a message-signature pair (M, σ), and gpk, returns 1 (*accept*) or 0 (*reject*); a group signature (M, σ) is valid if and only if Verify$(M, \sigma) = 1$.

Open. A deterministic polynomial-time algorithm that on input a message-signature pair (M, σ), OA's secret key ok, returns an ID, and a proof π showing its correctness in decryption.

Judge. A deterministic polynomial-time algorithm that takes (M, σ, ID, π) as input, returns 1 (*accept*) or 0 (*reject*) indicating a judgement on output from Open.

Anonymity [3]. A group signature scheme is anonymous if for any polynomial-time adversary $\mathcal{A}$, large enough security parameter k, $Adv_{\mathcal{A}}^{anon}$ is negligible: $Adv_{\mathcal{A}}^{anon} = P[Exp_{\mathcal{A}}^{anon-1}(k) = 1] - P[Exp_{\mathcal{A}}^{anon-0}(k) = 1]$, where experiments Exp^{anon-b}, $b = \{0, 1\}$ are defined as in Table 1. Oracles Ch, $Open$, $SndToU$, $WReg$, USK, $CrptU$ are defined as:

Ch: It randomly chooses $b \in \{0, 1\}$ and generates a valid group signature σ on a given m under keys $(ID_u, upk_b, usk_b, gsk_b)$, where $b \in_R \{0, 1\}$.

$Open$: If input (σ, m) is not valid, it returns $reject$; else it open σ, outputs (ID, π). We emphasize that $Open$ oracle is fully reliable, i.e, decrypts a group signature if and only if it is valid, in analyzing anonymity through this paper.

$SndToU$ plays as IA in Join, i.e., generating valid certificates (secret signing keys) gsk_u on queries. $WReg$ resets any entry in registration table (storing Join transcripts) to specified value. USK returns usk_i, gsk_i of specified member i. $CrptU$ sets a corrupted member's upk_i to specified value.

Public Key Encryption [6]. Specify key space $\mathcal{K}$, message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$, a public key encryption scheme based on them consists of the following algorithms:

–Gen: a probabilistic polynomial-time algorithm that on input 1^k outputs a public/secret key pair $(pk, sk) \in \mathcal{K}$;

–Enc: a probabilistic polynomial-time algorithm that on input 1^k, a message $m \in \mathcal{M}$, pk, returns a ciphertext $c \in \mathcal{C}$;

–Dec: a deterministic polynomial-time algorithm that on input 1^k, a ciphertext $c \in \mathcal{C}$, sk, returns a message $m' \in \mathcal{M}$ or a special symbol *reject*.

IND-CCA2 [6]. A public key encryption is indistinguishable against chosen ciphertext attacks if for any polynomial time adversary $\mathcal{A}$, large enough security parameter k, $Adv_{\mathcal{A}}^{IND-CCA2}$ is negligible: $Adv_{\mathcal{A}}^{IND-CCA2} = P[Exp_{\mathcal{A}}^{IND-CCA2-1}$ $(k) = 1] - P[Exp_{\mathcal{A}}^{IND-CCA2-0}(k) = 1]$, where experiments $Exp_{\mathcal{A}}^{IND-CCA2-b}$, $b = \{0, 1\}$ are defined as in Table 1. Oracles $Ch, Open, Enc$ are defined as:

Ch: It randomly chooses $b \in \{0, 1\}$ and generates a valid encryption c of m_b on input (m_0, m_1).

Dec: On a query ciphertext c, it firstly checks its validity and returns decrypted plaintext if valid, else returns *reject*.

Enc: It generates a ciphertext c of queried m.

$Exp_{\mathcal{A}}^{anon-b}(k)$: $(gpk, ik, ok) \leftarrow GKg(1^k)$, $d \leftarrow \mathcal{A}(gpk, ik, Ch, Open, SndToU,$ $WReg, USK, CrptU)$, return d.	$Exp_{\mathcal{A}}^{IND-CCA2-b}(k)$: $(pk, sk) \leftarrow Gk(1^k)$, $d \leftarrow \mathcal{A}(pk, Ch, Dec, Enc)$, return d.

Table 1. Definitions of Experiments.

3 Equivalence of Anonymity and IND-CCA2

Abdalla et al. constructed a public key encryption scheme from any group signature [11], and proved that if the adopted group signature is secure, i.e., fully anonymous (same as anonymous in [3]) and fully traceable [2] , their construction is an IND-CPA secure public key encryption, furthermore it is IND-CCA2 if the message space is restricted to $\{0, 1\}$, but they did not investigate the inverse direction.

It is evident that an IND-CCA2 secure public key encryption alone is impossible to produce a secure group signature because of lack of non-traceability and non-frameability. Nevertheless we show the existence of an equivalence between anonymity of group signatures and IND-CCA2 of corresponding public key encryptions.

An Encryption Scheme of Member Identity. Suppose there exists a group signature $\mathcal{GS}$ as defined in Section 2, let $\mathcal{K} = \{gpk, ik, ok : (gpk, ik, ok) \leftarrow \mathrm{Gpk}(1^{\mathrm{k_g}})\}$, $\mathcal{M} = \{ID : R(ID, upk_u, usk_u, gsk_u) = 1 : \exists upk_u \leftarrow Ukg(1^k)$, $gsk_u \leftarrow$ Join $(upk_u$, ik, $gpk)\}$ and $\mathcal{C}$, the following algorithms compose a public key encryption scheme $\mathcal{EI}$:

–Gen: i.e., Gkg, outputs $pk = (gpk, ik)$, $sk = ok$;

–Enc: to encrypt an ID, firstly generate upk_u, usk_u, gsk_u such that $R(ID, upk_u, usk_u, gsk_u) = 1$, select a random $r \in_R \{0,1\}^*$, then run Sign on r, return (σ, r);

–Dec: given a ciphertext (σ, r), run Open, and return an ID and a proof π.

Theorem 1. *If $\mathcal{GS}$ is anonymous, then $\mathcal{EI}$ is IND-CCA2 secure.*

Proof. Suppose $\mathcal{A}$ is an IND-CCA2 adversary of $\mathcal{EI}$, we construct $\mathcal{B}$ to break anonymity of $\mathcal{GS}$.

$\mathcal{B}$ has inputs gpk, ik and accesses of oracles Ch, $Open$, $SndToU$, $WReg$, USK, $CrptU$. It publishes $\mathcal{M}$ and corresponding $(upk_u$, usk_u, $gsk_u)$, for $ID_u \in \mathcal{M}$. It simulates oracles of $\mathcal{EI}$ as follows:

Decryption Oracle $\mathcal{EI}.Dec$: after getting query ciphertext (m, ρ, π), transfers to $Open$ oracle. If it is valid, $Open$ would return corresponding plaintext, i.e., member's identity ID. $\mathcal{B}$ transfers the reply to $\mathcal{A}$.

Challenge Oracle $\mathcal{EI}.Ch$: after getting query $ID_0, ID_1 \in \mathcal{M}$, selects $m \in_R \{0,1\}^*$ and sends (ID_0, ID_1, m) to its oracle Ch. Ch would choose $b \in_R \{0,1\}$ and generate a group signature of m by (upk_b, usk_b, gsk_b): (m, ρ_b, π_b).

$\mathcal{B}$ may continue to answer queries to $\mathcal{EI}.Open$ except (m, ρ_b, π_b).

$\mathcal{B}$ transfers (m, ρ_b, π_b) to $\mathcal{A}$ who is able to figure out b with probability more than 1/2. $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs. □

Theorem 2. *If $\mathcal{EI}$ is IND-CCA2 secure, then the underlying $\mathcal{GS}$ is anonymous.*

Proof. Suppose $\mathcal{A}$ is a adversary against anonymity of $\mathcal{GS}$, we construct $\mathcal{B}$ to break IND-CCA2 security of $\mathcal{EI}$.

$\mathcal{B}$ has access to oracles Ch, Dec. It simulates $\mathcal{GS}$'s oracles $\mathcal{GS}.Ch$, $\mathcal{GS}.Open$, $\mathcal{GS}.\{SndToU, WReg, USK, CrptU\}$ as follows:

Open Oracle $\mathcal{GS}.Open$: after getting query (m, ρ, π), transfers to its decryption oracle Dec. If it is a valid ciphertext, Dec would return the corresponding plaintext, i.e., member's identity ID and π. $\mathcal{B}$ transfers the reply to $\mathcal{A}$.

Oracles of $\mathcal{GS}.\{SndToU, WReg, USK, CrptU\}$: since $\mathcal{B}$ has the private keys of issue authority, it can simulate these oracles easily.

Challenge Oracle $\mathcal{GS}.Ch$: after getting challenge query $(ID_0, upk_0, usk_0, gsk_0)$, $(ID_1, upk_1, usk_1, gsk_1)$ and m, $\mathcal{B}$ transfers them to its challenge oracle Ch, who chooses $b \in_R \{0,1\}$ and generates a valid encryption of ID_b using random m: (m, ρ_b, π_b), i.e., a valid signature of m under $(ID_b, upk_b, usk_b, gsk_b)$. Subsequent proof is the same as in Theorem 1. □

4 Anonymity of ACJT's Group Signature

ACJT's scheme [1] dose not conform to the model of [3] (Section 2) completely, but such aspects are beyond our consideration of anonymity here. The following is a rough description of ACJT's scheme:

–**Setup**. IA randomly chooses a safe RSA modulus n and a, a_0, g, h, specifies two integer intervals Δ, Γ. OA chooses x, sets $y = g^x$. $gpk = \{n, a, a_0, y, g, h\}$, ik is factors of n, $ok = x$.

–**Join**. User selects $usk_i = x_i$,$upk_i = a^{x_i}$, where $x_i \in_R \Delta$, gets $gsk_i = (A_i, e_i), e_i \in_R \Gamma$ from IA. A relation is defined $R : A_i = (a^{x_i} a_0)^{1/e_i} \bmod n$.

–**Sign**. A group signature $(T_1, T_2, T_3, s_1, s_2, s_3, s_4, c)$ is a zero-knowledge proof of knowledge of A_i, x_i, e_i, and T_1, T_2 is a correct encryption of A_i.

–**Open**. OA decrypts $A := T_1/T_2^x$, and a proof of knowledge of decryption key x.

–**Verify**&**JUDGE**. Verification of corresponding zero-knowledge proof.

Theorem 3. *ACJT's scheme is IND-CCA2 secure encryption of* $\mathcal{M} = \{A \in QR_n | \exists e \in \Gamma, \overline{x} \in \Delta, A^e = a^{\overline{x}} a_0\}$*, under DDH assumption in random oracle model.*

The proof is standard as in [6], and provided in Appendix. It follows that:

Theorem 4. *ACJT's group signature is anonymous under DDH assumption in random oracle model.*

References

1. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in *Crypto'00*, LNCS 1880, pp. 255–270, Springer-Verlag, 2000.
2. M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," in *Eurocrypt'03*, LNCS 2656, pp. 614–629, Springer-Verlag, 2003.
3. M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," in *CT-RSA'05*, LNCS 3376, pp. 136–153, Springer-Verlag, 2005.
4. A. Kiayias and M. Yung, "Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders," in *http://eprint.iacr.org/2004/076/*.
5. A. Kiayias and M. Yung, "Group signatures with efficient concurrent join," in *Eurocrypt'05*, LNCS 3494, pp. 198–214, Springer-Verlag, 2005.
6. R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," *SIAM J. Comput.*, vol. 33, no. 1, pp. 167–226, 2004.
7. A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable signatures," in *Eurocrypt'04*, LNCS 3027, pp. 571–589, Springer, 2004.
8. L. Nguyen and R. Safavi-Naini, "Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings," in *Asiacrypt'04*, LNCS 3329, pp. 372–386, Springer-Verlag, 2004.
9. T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Crypto'84*, LNCS 196, pp. 10–18, Springer, 1985.
10. M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *22nd Annual ACM Symposium on the Theory of Computing*, pp. 427–437, ACM Press, 1990.
11. M. Abdalla and B. Warinschi, "On the minimal assumptions of group signature schemes," in *Information and Communications Security (ICICS 2004)*, LNCS 3269, pp. 1–13, Springer-Verlag, 2004.

A Proof of Anonymity

Theorem 5. *If we view ACJT's group signature [1] as an encryption scheme of message space* $\mathcal{M} = \{A \in QR_n | \exists e \in \mathit{\Gamma}, \overline{x} \in \mathit{\Delta}, A^e = a^{\overline{x}} a_0 \bmod n\}$*, then it is IND-CCA2 secure under the assumption that DDH is hard when factorization of* n *is known (in random oracle model).*

Proof. Choose $y = g^x \bmod n$, $x \in_R [1, (p-1)(q-1)/4]$.

Game G_0:

$(A_0, x_0, e_0, A_1, x_1, e_1) \leftarrow \mathcal{A}^{Enc,Dec,Random}(p, q, n, y, g)$,

$(m, \rho_b, \pi_b) \leftarrow Ch(A_0, x_0, e_0, A_1, x_1, e_1)$,

$b^* \leftarrow \mathcal{A}^{Enc,Dec,Random}(m, \rho_b, \pi_b)$,

If $b^* = b$ return 1, else return 0.

Sub-protocol **Ch**$(A_0, x_0, e_0, A_1, x_1, e_1)$:
$b \in_R \{0, 1\}$,
return $Enc(A_b, x_b, e_b)$.

Sub-protocol **Enc**(A, x, e):
$r \in_R [1, (p-1)(q-1)/4]$, $m \in_R \{0, 1\}^*$,
$\rho =_{def} (T_1, T_2, T_3) = (Ay^r, g^r, g^e h^r)$,
$\pi = PK\{(\alpha, \beta, \gamma, \delta) : a_0 = T_1^{\alpha}/a^{\beta} y^{\gamma}, T_2 = g^{\delta}, 1 = T_2^{\alpha}/g^{\gamma},\ T_3 = g^{\alpha} h^{\delta}, \alpha \in \mathit{\Gamma}, \beta \in \mathit{\Delta}\}\{m\}$
$=(c, s_1, s_2, s_3, s_4)$,
$c \leftarrow \mathcal{H}(g, h, y, a_0, a, T_1, T_2, T_3, a_0^c T_1^{s_1 - c2^{\gamma_1}}/(a^{s_2 - c2^{\lambda_1}} y^{s_3}),$
$T_2^{s_1 - c2^{\gamma_1}}/g^{s_3},\ T_2^c g^{s_4}, T_3^c g^{s_1 - c2^{\gamma_1}} h^{s_4}, m)$.
return (m, ρ, π).

Sub-protocol **Dec**(m, ρ, π):
Check validity of π by executing $V(m, \rho, \pi)$.
If $V(m, \rho, \pi) = 1$, parse ρ into (T_1, T_2, T_3),
return $A = T_1/T_2^x$ and a proof $\pi_d = PK\{x : T_1/A = T_2^x, y = g^x\}$,
else return *reject*.

Random Oracle $\mathcal{H}(r)$:
If r exists in table H, return corresponding h;
Else select $h \in_R \{0, 1\}^k$, store (r, h) in H and return h.

```
Sub-protocol $\mathbf{V}(m,\rho,\pi)$
Parse $\rho$ into $T_1, T_2, T_3$ and $\pi$ into $c, s_1, s_2, s_3, s_4$,
Let $d'_1 := a_0^c T_1^{s_1-c2^{\gamma_1}} / (a^{s_2-c2^{\lambda_1}} y^{s_3}) \bmod n$,
$d'_2 := T_2^{s_1-c2^{\gamma_1}} / g^{s_3} \bmod n$,
$d'_3 := T_2^c g^{s_4} \bmod n$,
$d'_4 := T_3^c g^{s_1-c2^{\gamma_1}} h^{s_4} \bmod n$,
Check table $H$ for $r = (g, h, y, a_0, a, T_1, T_2, T_3, d'_1, d'_2, d'_3, d'_4, m)$ and $c$.
If $(r, c)$ does not exist in table $H$, return 0;
else if $s_1 \in \pm\{0,1\}^{\epsilon(\gamma_2+k)+1}$,$s_2 \in \pm\{0,1\}^{\epsilon(\lambda_2+k)+1}$,
$s_3 \in \pm\{0,1\}^{\epsilon(\gamma_1+2l_p+k+1)+1}$,
$s_4 \in \pm\{0,1\}^{\epsilon(2l_p+k)+1}$, return 1.
```

Game G_1:

Same as Game G_0 except sub-protocol Ch.

```
Sub-protocol $\mathbf{Ch}(A_0, x_0, e_0, A_1, x_1, e_1)$:
$b \in_R \{0,1\}$, $m \in_R \{0,1\}^*$,
$r, r' \in_R [1, (p-1)(q-1)/4]$,
$\rho_b =_{def} (T_1, T_2, T_3) = (A_b y^r, g^{r'}, g^{e_b} h^r)$,
Simulate a proof
$\pi_b = PK\{(\alpha,\beta,\gamma,\delta) : a_0 = T_1^\alpha / a^\beta y^\gamma, T_2 = g^\delta, 1 = T_2^\alpha / g^\gamma, T_3 = g^\alpha h^\delta, \alpha \in \mathit{\Gamma}, \beta \in \mathit{\Delta}\}\{m\}$
$= (c, s_1, s_2, s_3, s_4)$,
$c \leftarrow \mathcal{H}(g, h, y, a_0, a, T_1, T_2, T_3,$
$a_0^c T_1^{s_1-c2^{\gamma_1}} / (a^{s_2-c2^{\lambda_1}} y^{s_3})$, $T_2^{s_1-c2^{\gamma_1}} / g^{s_3}$, $T_2^c g^{s_4}$, $T_3^c g^{s_1-c2^{\gamma_1}} h^{s_4}, m)$.
return $(m, \rho_b, \pi_b)$.
```

The difference between G_0 and G_1 is that in G_0 $(g, y, T_2, T_1/A_b)$ is a DDH sample, while a random sample in G_1.

Game G_2:

Same as Game G_1 except sub-protocol Ch.

```
Sub-protocol $\mathbf{Ch}(A_0, x_0, e_0, A_1, x_1, e_1)$:
$b \in_R \{0,1\}$, $m \in_R \{0,1\}^*$,
$r, r', r'' \in_R [1, (p-1)(q-1)/4]$,
$\rho_b =_{def} (T_1, T_2, T_3) = (A_b y^r, g^{r'}, g^{e_b} h^{r''})$,
Simulate a proof
$\pi_b = PK\{(\alpha,\beta,\gamma,\delta) : a_0 = T_1^\alpha / a^\beta y^\gamma, T_2 = g^\delta, 1 = T_2^\alpha / g^\gamma, T_3 = g^\alpha h^\delta, \alpha \in \mathit{\Gamma}, \beta \in \mathit{\Delta}\}\{m\}$
$= (c, s_1, s_2, s_3, s_4)$,
$c \leftarrow \mathcal{H}(g, h, y, a_0, a, T_1, T_2, T_3,$
$a_0^c T_1^{s_1-c2^{\gamma_1}} / (a^{s_2-c2^{\lambda_1}} y^{s_3})$, $T_2^{s_1-c2^{\gamma_1}} / g^{s_3}$, $T_2^c g^{s_4}$, $T_3^c g^{s_1-c2^{\gamma_1}} h^{s_4}, m)$.
return $(m, \rho_b, \pi_b)$.
```

The difference between G_1 and G_2 is that in G_1 $(y, h, T_1/A_b, T_3/g^{e_b})$ is a DDH sample, while a random sample in G_2.

Denote $\mathcal{A}$'s output in Game G_i as $\mathcal{A}^{G_i}$, then suppose $\mathcal{A}$ is a successful adversary against IND-CCA2 attacks, that is $\exists \epsilon > 0$ which is non-negligible, so that

$$P[\mathcal{A}^{G_0} = 1|b = 1] - P[\mathcal{A}^{G_0} = 1|b = 0] \geq \epsilon.$$

Because

$$|P[\mathcal{A}^{G_0} = 1|b] - P[\mathcal{A}^{G_1} = 1|b]| \leq Adv_{\mathcal{A}}^{DDH}, \text{ for } b = 0 \text{ and } 1.$$

$$|P[\mathcal{A}^{G_1} = 1|b] - P[\mathcal{A}^{G_2} = 1|b]| \leq Adv_{\mathcal{A}}^{DDH}, \text{ for } b = 0 \text{ and } 1.$$

In Game G_2, every component of challenge is randomized independently, so there exists a negligible ϵ_1

$$P[\mathcal{A}^{G_2} = 1|b = 1] - P[\mathcal{A}^{G_2} = 1|b = 0] < \epsilon_1,$$

But

$$\begin{aligned}
\epsilon &\leq P[\mathcal{A}^{G_0} = 1|b = 1] - P[\mathcal{A}^{G_0} = 1|b = 0] \\
&= P[\mathcal{A}^{G_0} = 1|b = 1] - P[\mathcal{A}^{G_1} = 1|b = 1] \\
&\quad + P[\mathcal{A}^{G_1} = 1|b = 1] - P[\mathcal{A}^{G_0} = 1|b = 0] \\
&\quad + P[\mathcal{A}^{G_1} = 1|b = 0] - P[\mathcal{A}^{G_1} = 1|b = 0] \\
&\leq 2Adv_{\mathcal{A}}^{DDH} + P[\mathcal{A}^{G_1} = 1|b = 1] - P[\mathcal{A}^{G_2} = 1|b = 1] \\
&\quad + P[\mathcal{A}^{G_2} = 1|b = 1] - P[\mathcal{A}^{G_2} = 1|b = 0] \\
&\quad + P[\mathcal{A}^{G_2} = 1|b = 0] - P[\mathcal{A}^{G_1} = 1|b = 0] \\
&\leq 4Adv_{\mathcal{A}}^{DDH} + P[\mathcal{A}^{G_2} = 1|b = 1] - P[\mathcal{A}^{G_2} = 1|b = 0] \\
&< 4Adv_{\mathcal{A}}^{DDH} + \epsilon_1
\end{aligned}$$

Thus $Adv_{\mathcal{A}}^{DDH}$ is non-negligible. □