

doi: 10.11830/ISSN.1000-5013.201702014



群签名与广播加密的对偶性及应用

程小刚¹, 郭韧², 陈永红¹

(1. 华侨大学 计算机科学与技术学院, 福建 厦门 361021;
2. 华侨大学 工商管理学院, 福建 泉州 362021)

摘要: 提出群签名(GS)与广播加密(BE)是一对关系密切的对偶密码系统,类似公开加密与普通签名的对偶关系,即基于 GS 方案可以构建 BE 方案.而基于 BE 方案也可以构建 GS 方案.文中给出实现这种对偶关系的具体构建方法与步骤,即基于 NP(non-deterministic polynomial)证据加密(WE)可把一个可撤销群签名方案转换为一个可撤销广播加密方案,而基于非交互式零知识(NIZK)证明可把一个撤销广播加密方案转换为一个可撤销群签名方案.最后,指出基于广播加密的高效可撤销群签名方案可以纳入文中所提出的框架中.

关键词: 群签名; 广播加密; 对偶性; NP 证据加密; 成员撤销

中图分类号: TP 309 **文献标志码:** A **文章编号:** 1000-5013(2017)02-0207-05

Duality Between Group Signature and Broadcast Encryption and Its Applications

CHENG Xiaogang¹, GUO Ren², CHEN Yonghong¹

(1. College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China;
2. College of Business Administration, Huaqiao University, Quanzhou 362021, China)

Abstract: Group signature (GS) and broadcast encryption (BE) are shown to be dual with each other, similar with the duality between public key encryption (PKE) and digital signature. Namely, BE can be transformed to a GS scheme and vice versa. Concrete construction methods and procedures are given i. e., a revocable GS scheme can be transformed to a BE scheme based on NP (non-deterministic polynomial) witness encryption (WE) and a revocable BE can be transformed to a GS based on non-interactive zero knowledge (NIZK) proof. Finally, it point out that an efficient revocable GS scheme based on BE is also shown to be one incarnation of our framework.

Keywords: group signature; broadcast encryption; duality; NP witness encryption; membership revocation

群签名(group signature,GS)是 1991 年由 Chaum 和 Heyst 在 Crypto 密码学会议上提出^[1]. 由于结合了匿名与可追踪的良好特性,群签名迅速成为一种具有中心地位的密码系统,到今天群签名方案的构建在安全性、效率等方面有了很大的提高^[2],并在电子投票^[3]、电子货币^[4]、可信计算^[5]、网络追踪^[6]与隐藏机构内部结构等方面有广泛的应用^[2]. 广播加密(broadcast encryption,BE)^[7]典型的应用是付费电视的应用中,电视台对视频节目进行加密后广播出去,任何人可收到加密后的视频,但只有付过费的合法用户(拥有相关密钥)才能解密而正常收看电视节目. GS 与 BE 都是群组密码系统,即是面向多人、多参与方,而不象普通的签名或加密,通常是一个签名方(发送方),一个验证方(接收方). 对于此类

收稿日期: 2016-05-22

通信作者: 程小刚(1973-),男,讲师,博士,主要从事信息安全、密码学的研究. E-mail:cxg@hqu.edu.cn.

基金项目: 国家自然科学基金资助项目(61370007);福建省自然科学基金资助项目(2016J01336);福建省社会科学规划项目(FJ2016B090);华侨大学高层次人才科研启动项目(16BS309)

密码系统,研究的目的是发现他们之间非平凡的联系(正如普通的签名与公开加密之间的对偶关系),从而彼此相互借鉴、利用各自领域中的技术互相促进,构建出更好、更高效、更灵活、更通用的群组密码系统. Kiayias 等^[8]指出 GS 与叛逆者追踪 (traitor tracing, TT) 之间有密切的对偶关系^[9],而相对 GS 与 TT,GS 与 BE 之间相似度更大,关系更密切. 如 GS 与 BE 同时都有成员撤销问题^[10-11]. 本文提出 GS 与 BE 是一对关系密切的对偶密码系统,并给出了具体的相互构建方法与步骤.

1 初步知识

定义 1 群签名一般由下面 6 个随机多项式时间算法组成.

1) 设置(Setup). 给定一安全参数 K ,群管理员(GM)生成一个群公钥(GPK)可用于群签名的验证,和一群私钥(GSK)可用于生成成员证书及签名打开;安全性更好的是,负责纳入成员的 GM 及负责打开签名的 GM 角色是分开的(通过持有不同的密钥).

2) 加入(Join). 对于动态的群签名,这是用户和 GM 之间执行的一个交互协议,完成后用户入群并获得成员证书及一个私钥,可用于群签名的生成,GM 获得相关的追踪信息,可用来打开此用户的群签名;而静态的群签名由 GM 直接生成成员的证书并秘密传给成员,就没有此交互过程. 缺点是 GM 可冒充成员进行签名.

3) 签名(Sign). 群成员可利用自己的成员证书和私钥生成任一消息的群签名.

4) 验证(Verify). 任何人获得 GPK 和一个消息/签名对,可验证此群签名是否合法,但对合法的群签名他不能找出实际的签名者,而且同一成员作的群签名之间也是不可链接的.

5) 打开与证明(Open and Prove). 对于合法的群签名,GM 能打开并找出实际的签名者;最好 GM 也能给出证据,说明一群签名的确是某成员签的,同时,不会破坏此成员未来的签名能力.

6) 撤销(Revoke). GM 可撤销某成员的签名权利,之后此用户就再也不能生成合法的群签名了.

群签名的安全模型主要有如下两个性质.

1) 匿名性. 给定一个合法的群签名,只有 GM 才能识别出真正的签名者,其他任何人都不能打开签名找出签名者.

2) 可追踪性. 一群合谋者将他们的私钥放在一起也不能生成一个合法的群签名,使其打开至其他群成员. 前述是成立的,即使合谋者知道 GM 打开签名的私钥.

定义 2 广播加密由如下 7 个多项式算法构成.

1) 设置(Setup). 生成系统的主公/私钥对 MPK/MSK,并初始将撤销列表(revocation list, RL)设置为空.

2) 加入(Join). 标识为 ID 的用户向系统申请加入,系统管理员审核后由 (MSK, ID) 生成用户私钥 SKID 并颁发给用户.

3) 加密(ENC(MPK, m , RL)). 用系统公钥 MPK 及 RL 对消息 m 进行加密,得到密文 CT.

4) 解密(DEC(CT, SKID)). 任何合法的用户(具有合法的私钥 SKID,并且其 ID 不在 RL 中),可对密文 CT 进行解密得到消息 m .

5) 撤销(Revoke). 系统管理员将欲撤销的用户标识 ID 放入 RL 中,标识其以后不再能收到消息.

6) 重新加入(Re-Join). 系统管理员将用户 ID 从 RL 中删除,此后该用户就能正常接收广播消息.

BE 的 IND_CPA(indistinguishable chosen plaintext attack)安全模型定义如下:

1) Challenger 生成 BE 方案的 MPK/MSK,并把 MPK 发送给敌手 ADV;

2) ADV 能自适应地向 Challenger 查询任一标识为 ID 的用户的私钥,Challenger 利用其掌握的 MSK 生成私钥,发送给 ADV,并将所有 ADV 查询过的 ID 加入集合 Q 中;

3) ADV 生成任意两个长度相同,但内容不同的消息 m_0, m_1 ,并发给 Challenger;

4) Challenger 首先将集合 Q 中的所有用户放入 RL 中去,再随机选择 $b=0$ 或 1 ,用 MPK 和 RL 对 m, b 进行加密,得到密文 CT,将密文发给 ADV;

5) ADV 收到 CT 后,要猜测 $b=0$ 还是 1 ,BE 是 IND_CPA 安全的,如果 ADV 的成功概率同 $1/2$ 的差是可忽略的,即

$$|\Pr[\text{ADV}(\text{CT}) \rightarrow b' : b' = b] - 1/2| < \text{negligible}(\lambda).$$

2 对偶关系的构建与步骤

2.1 基于GS及WE的BE方案构建

2.1.1 NP证据加密 该系统是Garg等^[12]提出的一种新的没有密钥生成过程的加密系统,它以一个NP(non-deterministic polynomial)语言 L 的实例 x 做为公钥,对消息 m 进行加密,如果 $x \in L$ 且解密者有相关的NP证据 w ,则可以对密文解密,得到消息 m ;而如果 $x \notin L$,则加密是语义安全的.文献[8]也给出了证据加密(witness encryption, WE)的多种应用,如公钥加密方案和IBE, ABE等.

文中给出WE的另一个应用,即用于构建可撤销的BE方案^[10,13],所构建的可撤销BE方案具有简单的成员重加入功能,很适合付费电视等的应用,如欠费的用户被停机,而当用户缴清欠费后又恢复其成员资格.

定义3 WE(NP证据加密).针对一NP语言 L 的WE方案有如下的多项式时间算法.

- 1) $\text{ENC}(1^\lambda, x, M)$. 算法输入为安全参数 λ , 一个字符串 x 和待加密的消息 M , 输出为密文CT.
- 2) $\text{DEC}(\text{CT}, w)$. 算法输入为一密文CT, 一个字符串 w , 输出为一个消息 M 或一特殊符号 \perp .

这些算法满足下面2个主要性质.

- 1) 正确性. 如果 $x \in L$ 且 w 是相应的NP证据, 那么, 解密算法总能正确解密得到消息 M , 即

$$\Pr[\text{DEC}(\text{ENC}(1^\lambda, x, M), w) = M] = 1.$$

- 2) 公正性. 如果 $x \notin L$, 那么对于任何的多项式时间敌手 A 来说, 除了可忽略概率之外, 对两个不同消息加密的密文分布是相同的, 即

$$|\Pr[A(\text{ENC}(1^\lambda, x, m_0)) = 1] - \Pr[A(\text{ENC}(1^\lambda, x, m_1)) = 1]| < \text{Negligible}(\lambda).$$

2.1.2 BE方案构建 方案构建的思想是:成员加入所获得的证书私钥就是GM颁发的数字签名,之后BE时用WE来加密,GM的签名验证公钥是公开的,所用的NP关系是存在一个消息 m 及一个合法的签名(相对GM签名验证公钥),并且此消息 m 不在RL中.

基于GS和WE的BE方案构建如下:

BE. Setup, 就是GS. Setup;

BE. Join, 就是GS. Join, 完成后成员获得成员私钥(此私钥在GS中是用来生成群签名,而在BE中是用来进行广播消息的解密);

BE. Encrypt, 用如下的NP语言利用WE对消息 m 进行加密, 即

$$\text{NP} = \{\text{GS. GPK} \mid \exists \text{Usk 是合法的} \wedge \text{Usk 未被撤销}\}$$

BE. Decrypt, 显然拥有合法Usk的成员能利用其NP证据利用WE的Decrypt算法对广播消息进行解密;

BE. Revo, 就是GS. Revo, 撤销后成员的Usk就不再是合法的NP证据, 所以也就无法对之后的广播消息进行解密.

2.2 基于BE的GS方案构建

基于BE的GS方案构建的思想是:GS中成员的私钥就是BE中成员的解密私钥,签名时利用NIZK证明系统证明自己是合法的成员(即拥有合法的解密私钥).在此应指出Libert等^[14-15]的高效可撤销GS方案构建可看作是此思想的具体实现.

2.2.1 NNL广播撤销^[10] NNL广播方案中把所有用户对应到树的叶子节点,每个用户对应一个叶子节点,进行撤销时,把合法的广播接收成员划分成若干个子集.每个子集 S_{K_i, U_i} 的含义,如图1所示.

从图1可以看出: U_i 是 K_i 的子孙节点, S_{K_i, U_i} 表示合法的用户是 K_i 的后代叶子节点,而不是 U_i 的后代叶子节点.如图1中叶子节点1,2的用户为合法的接收者,而3,4不是.这被称为SD(subset sifference)方法,并证明了只要 $O(R)$ 个集合就可支持任意的撤销, R 为被撤销用户数量,且用户不用更新自己的私钥,因而效率较高.

2.2.2 基于广播加密的高效可撤销群签名方案 每个群成员对应一个叶子节点 i ,设从树根到此叶子

节点的路径为 I_1, I_2, \dots, I_l , 其中, l 为树的高度, 则群成员的证书为 $(ID(v), X, C_v, \delta_v)$, 其中, $ID(v)$ 是用户的叶子节点编号, $X = g^x$ 是群成员提供给 GM 的值 (x 的值只有群成员自己知道, 是其签名私钥), $C_v = g^{I_1}, \dots, g^{I_l}, g_1, \dots, g_l$ 等都是公开参数, δ_v 是 GM 对 (X, C_v) 的 SPS 签名.

RL 就是上述 NNL 广播加密中的 $\{S_{K_1, U_1}, S_{K_2, U_2}, \dots, S_{K_m, U_m}\}$ 和 GM 对每个子集的 SPS 签名. 进行群签名是合法的群成员首先要 RL 中找到自己位于哪个子集 (注意被撤销的群成员是找不到这样的子集的, 所以他没有签名的权利) 中, 如 S_{K_i, U_i} ; 然后, 群成员要以匿名的方式证明自己的合法性 (因其证书是 SPS 签名, 而 RL 中的也是 SPS 签名, 所以可用 Groth-Sahai 证明系统来做), 即自己的群证书中的路径 I_1, I_2, \dots, I_l (保存在 C_v 中) 是符合子集 S_{K_i, U_i} 的. 即在 φ_i 层上 (K_i 所位于的层) C_v 中的节点编号是 K_i , 而在 ψ_i 层上 (U_i 所位于的层) C_v 中的节点编号 $\neq U_i$, 从而证明了自己是合法的群成员.

注意 C_v 采用的技术是简洁向量承诺 (concise vector commitment, CVC) 方案^[16], 即承诺方可对一个向量 (有多个坐标) 进行承诺, 在此就是从根到某个叶子节点的一条路径 (I_1, I_2, \dots, I_l) , 然后, 可对向量中的任一个坐标进行高效打开 (即证据的大小不依赖于向量大小). CVC 可与 NNL 广播加密方案很好地结合, 实现高效群成员合法性证明, 即成员在证明自己的合法性时, 只要先对从根到自己所在的叶子节点的一条路径进行承诺为 C_v , 然后, 证明承诺中的值第 φ_i 个坐标是等于 K_i 的, 而第 ψ_i 个坐标是不等于 U_i 的, 这样就证明了自己的合法性.

2.3 安全性与性能分析

在上述基于 GS 方案的 BE 方案构建中, 合法的群成员能提供出合法的未被撤销的签名私钥, 即下述 NP 语言的证据:

$$NP = \{GS, GPK \mid \exists Usk \text{ 是合法的} \wedge Usk \text{ 未被撤销} \}.$$

因而根据 WE 方案的定义, 此成员能够对 WE 密文进行解密, 从而得到加密的广播消息; 而不合法的成员 (如没有证书, 或其证书被撤销, 即在 RL 中) 由于没有 NP 证据就不能对密文进行解密, 得不到广播的消息.

上述基于 BE 的 GS 方案的安全性分析与证明可参见文献[15]. 其基本思想如下: 合法的成员用 NIZK 证明自己具有 BE 的解密私钥且未被撤销, 此 NIZK 可作为 GS 签名, 即自己是合法的群成员.

在性能方面, 文献[15]中的 GS 方案效率很高, 是迄今撤销效率最高的标准模型下可撤销群签名方案. 同以前的撤销方案相比, 其优势在于: 公钥大小为 $O(\log N)$, 签名和验证的复杂度都为 $O(1)$, 撤销成员时用户不需要更新自己的私钥, 此种撤销效率超越了以前的任何一种方案.

上述的基于 GS 和 WE 的 BE 方案构建, 效率不是很高, 是因为构建中要把用到的 NP 语言归约到 WE 方案中的 NP 完全问题 (如文献[12]中的构建用到的是精确覆盖问题), 而这种规约通常效率较低.

3 结 论

提出群签名与广播加密之间有密切的对偶关系, 并给出了如何具体实现这种对偶关系. 即基于 WE 可把一个可撤销群签名方案转换为一个可撤销广播加密方案, 而基于 NIZK 可把一个撤销广播加密方案转换为一个可撤销群签名方案. 同时, 指出基于广播加密的高效可撤销群签名方案可以纳入文中所提出来的框架中.

文中提出这种非平凡的对偶关系对各自方案的构建提供了新的思路与方法, 但基于 GS 和 WE 的 BE 方案仅仅是理论上的方案构建, 还不能够应用于实际, 其价值体现在理论上. 文中提出了 BE 的构建的另一种思想, 未来如果出现高效的直接的 WE 方案构建, 那么理论方案也就可应用于实际.

本研究工作应该说只是一个开始, 还有大量的研究工作有待进行. 即探索大量面向群组的密码系统

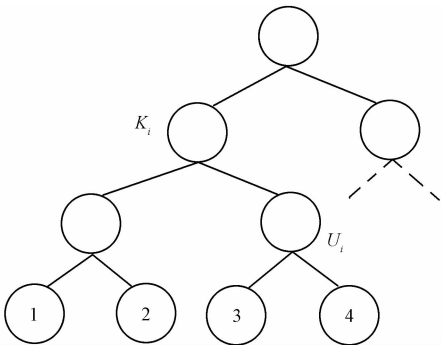


图 1 NNL 广播撤销示意图
Fig. 1 NNL broadcast revocation schematic

(如群签名、群加密^[17]、广播加密、叛逆者追踪、环签名^[18]、秘密分享和门限签名^[19]等)之间的非平凡关系,以及高效的相互转换的理论与方法.

参考文献:

- [1] CHAUM D, HEYST E. Group signatures[C]// DAVIES D. Advances in Cryptology: EUROCRYPT'91. Heidelberg: Springer-Verlag, 1991: 257-265.
- [2] 程小刚, 王箭, 杜吉祥. 群签名综述[J]. 计算机应用研究, 2013, 30(10): 2881-2886.
- [3] 陈晓峰, 王育民. 基于匿名通讯信道的安全电子投票方案[J]. 电子学报, 2003, 31(3): 390-393.
- [4] 李梦东, 杨义先, 马春光, 等. 由群签名实现的可撤销匿名性的电子现金方案[J]. 北京邮电大学学报, 2005, 28(2): 30-33.
- [5] BRICKELL E, LI J. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(3): 345-360.
- [6] AFANASYEV M, KOHNO T, MA J, et al. Privacy-preserving network forensics[J]. Commun ACM, 2011, 54(5): 78-87.
- [7] FIAT A, NAOR M. Broadcast encryption[C]// STINSON D R. Advances in Cryptology: CRYPTO'93. Heidelberg: Springer-Verlag, 1994: 480-491.
- [8] CHOR B, FIAT A, NAOR M. Tracing traitors[C]// DESMEDT Y G. Advances in Cryptology: CRYPTO'94. Heidelberg: Springer-Verlag, 1994: 257-270.
- [9] KIAYIAS A, YUNG M. Extracting group signatures from traitor tracing schemes[C]// BJHAM E. Advances in Cryptology: EUROCRYPT 2003. Heidelberg: Springer-Verlag, 2003: 630-648.
- [10] NAOR D, NAOR M, LOTSPIECH J. Revocation and tracing schemes for stateless receivers[C]// KILIAN J. Advances in Cryptology: CRYPTO 2001. Heidelberg: Springer-Verlag, 2001: 41-62.
- [11] 张德栋, 马兆丰, 杨义先, 等. 群签名中成员撤销问题解决方案[J]. 通信学报, 2014, 35(3): 193-200.
- [12] GARG S, GENTRY C, SAHAI A, et al. Witness encryption and its applications[C]// Proceedings of the Annual Acm Symposium on Theory of Computing. New York: [s. n.], 2013: 467-476. doi:10.1145/2488608.2488667.
- [13] DODIS Y, FAZIO N. Public key broadcast encryption for stateless receivers[C]// Digital Rights Management. Heidelberg: Springer-Verlag, 2003: 61-80.
- [14] LIBERT B, PETERS T, YUNG M. Scalable group signatures with revocation[C]// POINTCHEVAL D, JOHANSSON T. Advances in Cryptology: EUROCRYPT 2012. Heidelberg: Springer-Verlag, 2012: 609-627.
- [15] LIBERT B, PETERS T, YUNG M. Group signatures with almost-for-free revocation[C]// SAFAVI-NAINI R, CANETTI R. Advances in Cryptology: CRYPTO 2012. Heidelberg: Springer-Verlag, 2012: 571-589.
- [16] LIBERT B, YUNG M. Concise mercurial vector commitments and independent zero-knowledge sets with short proofs[C]// International Conference on Theory of Cryptography. Heidelberg: Springer-Verlag, 2010: 499-517.
- [17] CATHALO J, LIBERT B, YUNG M. Group encryption: Non-interactive realization in the standard model[C]// MATSUI M. Advances in Cryptology: ASIACRYPT 2009. Heidelberg: Springer-Verlag, 2009: 179-196.
- [18] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]// BOYD C. Advances in Cryptology: ASIACRYPT 2001. Heidelberg: Springer, 2001: 552-565.
- [19] 韩金广, 亢保元, 王庆菊. 面向群通信的门限签名方案的密码学分析[J]. 华侨大学学报(自然科学版), 2008, 29(2): 213-217. doi:10.11830/ISSN.1000-5013.2008.02.0213.

(责任编辑: 黄仲一 英文审校: 吴逢铁)