明治学院大学情報数理学部付属 情報数理科学研究所
Institute for Mathematical Informatics attached to Faculty of Mathematical Informatics, Meiji Gakuin University

穴田研究室の研究テーマ Research Themes in Anada Laboratory /* 共同研究を想定した紹介 */

“Group Signatures with Designated Traceability”

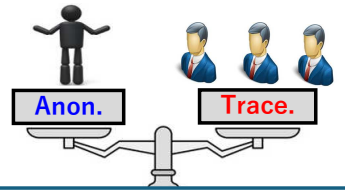
Background

A group signature [1] enables a signer to sign a message on behalf of a group to which he/she belongs.

- *Anonymous:* the signer is not identified in the group.
- *Traceable:* an authority called an opener can identify the signer by using an opening key.

Our result

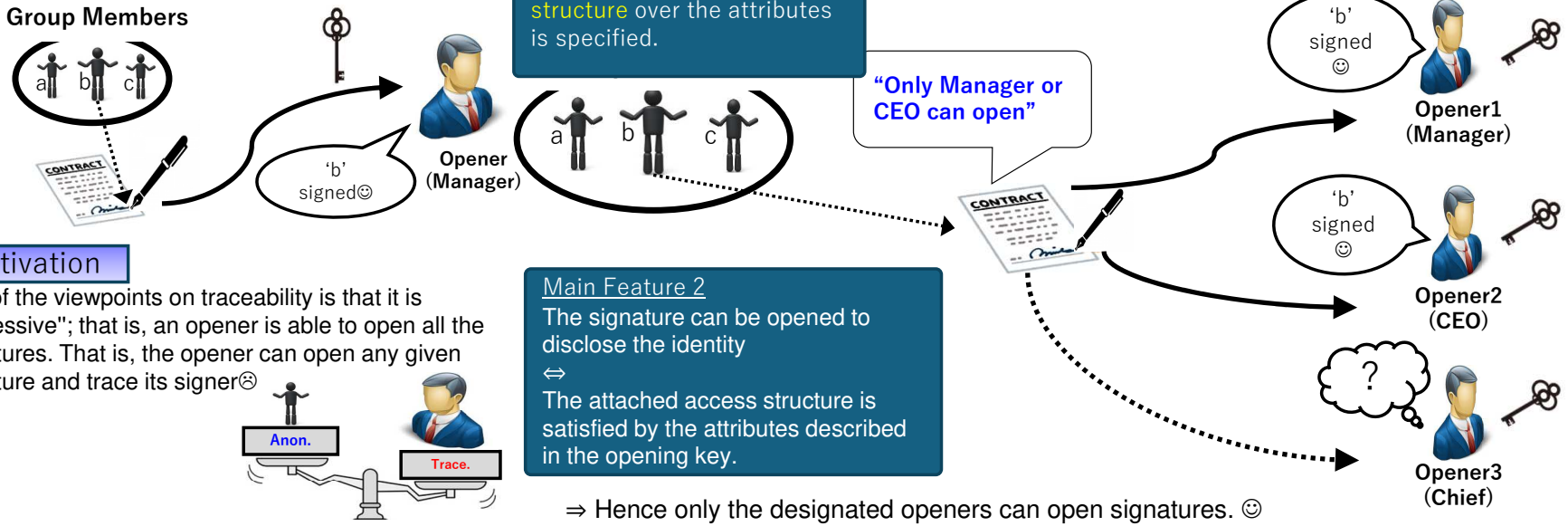
In this paper, we introduce a function of *designated traceability* in a group signature scheme, which concerns with users' right on the opening function.



Main Feature 1
A user can generate a signature in which an access structure over the attributes is specified.

Setting 1
Multiple Openers

Setting 2
Each of opener has an opener key which is related to his/her attributes



Motivation

One of the viewpoints on traceability is that it is ``excessive''; that is, an opener is able to open all the signatures. That is, the opener can open any given signature and trace its signer☹

Main Feature 2
The signature can be opened to disclose the identity
⇔
The attached access structure is satisfied by the attributes described in the opening key.

⇒ Hence only the designated openers can open signatures. ☺

[1] Chaum, van Heyst: “Group Signatures”, EUROCRYPT1991

明治学院大学情報数理学部付属 情報数理科学研究所
Institute for Mathematical Informatics attached to Faculty of Mathematical Informatics, Meiji Gakuin University

科学上の興味 Scientific Curiosity /* 研究に関する自由記述 */

Syntax around "opening key"

GSdT := (GKG, OKG, UKG, Join, Iss, GSign, GVrfy, Open, Judge)
group-signature σ consists of
$\sigma = (Y, \sigma_0)$
Y : Access-structure
σ_0 : Other part → Later, "ciphertext + ...of"
Opener's secret key $\boldsymbol{ok}[j]$ is issued by the group manager
$\boldsymbol{X}$: Opener's attributes
$\boldsymbol{ok}[j] \leftarrow \mathrm{OKG}(gpk, omk, j, X)$
$\boldsymbol{ok}[j] = (X, ok_0)$: ciphertext can be ope... $R(X,Y) = 1$

Security def. of anonymity

$\mathrm{Expr}^{\text{anon-}b}_{\mathrm{GSdT},\mathbf{A}}(1^\lambda)$ // $b \in \{0,1\}$

$(gpk, ik, omk) \leftarrow \mathrm{GKG}(1^\lambda)$

$\mathrm{CU} \leftarrow \emptyset, \mathrm{HU} \leftarrow \emptyset, \mathrm{MS} \leftarrow \emptyset, \mathrm{CO} \leftarrow \emptyset, \mathrm{OP} \leftarrow \emptyset$

$d \leftarrow \mathbf{A}(gpk, ik : \mathrm{ChaO}_b(\cdot,\cdot,\cdot,\cdot), \mathrm{AddOO}(\cdot,\cdot),$
$\mathrm{OpenO}(\cdot,\cdot,\cdot), \mathrm{StoUO}(\cdot,\cdot), \mathrm{WRegO}(\cdot,\cdot), \mathrm{USKO}(\cdot),$
$\mathrm{CrptOO}(\cdot), \mathrm{CrptUO}(\cdot,\cdot))$

Return d

Our stand point
Only already added openers are designated to open signatures
→ **"CPA-security" of ABE ☺**

Our generic construction

GS [2]
Sig + PKE + SS-NIZK
⇒
Our GSdT
Sig + CP-ABE + SS-NIZK

Components of a group sig.

$\sigma = (Y, \sigma_0) = (Y, (C_0, \pi_1))$

Y : **access structure**
C_0 : ABE ciphertext of **signer's certification** under Y
π_1 : a **proof** generated with SS-NIZK$_1$
under the statement $x := (\mathrm{pk}_{\mathrm{ABE}}, \mathrm{pk}_{\mathrm{Sig}}, m, C_0)$
& with witness $w := (i, \mathrm{pk}_i, cert_i, s, r)$

Security properties

Theorem 1 [Correctness]
Theorem 2 [Anonymity]
Theorem 3 [Traceability]
Theorem 4 [Non-frameability]

ABE: adaptive-IND-CPA,
SS-NIZK$_1$: sim-sound & comp. zk,
SS-NIZK$_2$: comp. zk,
⇒our GSdT: anonymous.

Future work

- Instantiation: (1) **Bilinear groups**; (2) **Lattice**
- **Further** study towards "**Mutual accountability**"

[2] Bellare, Shi, Zhang: "Foundations of Group Signatures: The Case of Dynamic Groups", CT-RSA 2005