Efficient ABE in the Generic Group, Random Oracle Model.

Romain Gay

November 2017

1 Preliminaries

1.1 Access Structure

We recall the definition of (monotone) access structures using the language of (monotone) span programs [KW93], which capture boolean formulas.

Definition 1 (access structure [Bei96,KW93]). *A* (monotone) access structure *for attribute universe* $\mathcal{U}$ *is a pair* $(\mathbf{M}, \rho)$ *where* $\mathbf{M} \in \mathbb{Z}_p^{\ell \times \ell'}$ *and* $\rho : [\ell] \to \mathcal{U}$*. Given* $\mathcal{S} \subseteq \mathcal{U}$*, we say that*

$$\mathcal{S} \text{ satisfies } (\mathbf{M}, \rho) \text{ iff } \mathbf{1}^\top \in \mathsf{Span}(\mathbf{M}_\mathcal{S}),$$

Here, $\mathbf{1} := (1, 0, \ldots, 0) \in \mathbb{Z}^{\ell'}$ *is a row vector;* $\mathbf{M}_S$ *denotes the collection of vectors* $\{\mathbf{M}_j : \rho(j) \in \mathcal{S}\}$ *where* $\mathbf{M}_i$ *denotes the* i*'th row of* $\mathbf{M}$*; and* Span *refers to linear span of collection of (row) vectors over* $\mathbb{Z}_p$*.*

That is, $\mathcal{S}$ satisfies $(\mathbf{M}, \rho)$ iff there exists constants $\omega_1, \ldots, \omega_\ell \in \mathbb{Z}_p$ such that

$$\sum_{\rho(j) \in S} \omega_j \mathbf{M}_j = \mathbf{1}^\top \tag{1}$$

Observe that the constants $\{\omega_i\}$ can be computed in time polynomial in the size of the matrix $\mathbf{M}$ via Gaussian elimination.

$\underline{\mathsf{GenShare}(\mathbf{M} \in \mathbb{Z}_p^{\ell \times m}, \alpha \in \mathbb{Z}_p)\text{:}}$
$\boldsymbol{u} \leftarrow_R \mathbb{Z}_p^{m-1}$, for all $i \in [\ell]$, $\alpha_i := \mathbf{M}_i \binom{\alpha}{\boldsymbol{u}} \in \mathbb{Z}_p$
Return $\{\alpha_i\}_{i \in [\ell]}$.

Fig. 1. Share generation algorithm. Here, $\mathbf{M}_i$ denotes the i'th row of $\mathbf{M}$.

1.2 Pairing Groups

Let GGen be a PPT algorithm that on input 1^λ returns a description $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, p, P_1, P_2)$ of a type 3 pairing groups where $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ are cyclic groups of order p for a 2λ-bit prime p, P_1 and P_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficiently computable (non-degenerate) bilinear map. Define $P_T := e(P_1, P_2)$, which is a generator of $\mathbb{G}_T$. We use implicit representation of group elements. Namely, for $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_p$, define $[a]_s = aP_s \in \mathbb{G}_s$ as the implicit representation of a in $\mathbb{G}_s$. Note that from $[a]_s \in \mathbb{G}_s$ it is generally hard to compute the value a (discrete logarithm problem in $\mathbb{G}_s$). Further, from $[b]_T \in \mathbb{G}_T$, it is hard to compute

the value $[b]_1 \in \mathbb{G}_1$ and $[b]_2 \in \mathbb{G}_2$ (pairing inversion problem). Obviously, given $[a]_s \in \mathbb{G}_s$ and a scalar $x \in \mathbb{Z}_p$, one can efficiently compute $[a \cdot x]_s \in \mathbb{G}_s$. Further, given $[a]_1$, $[a]_2$, one can efficiently compute $[a \cdot b]_T$ using the pairing e. For any $a, b \in \mathbb{Z}_p$, define $[a]_1 \bullet [b]_2 := [a \cdot b]_T \in \mathbb{G}_T$, which can be computed using the pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.

2 Efficient ABE in the Generic Group, Random Oracle Model

$\underline{\mathsf{Setup}(1^\lambda):}$

$\mathcal{PG} \leftarrow_R \mathsf{GGen}(1^\lambda)$, $\alpha \leftarrow_R \mathbb{Z}_p$, $\mathsf{msk} := \alpha$, $\mathsf{pk} := [\alpha]_T$

Return $(\mathsf{pk}, \mathsf{msk})$.

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathcal{S}):}$

$s \leftarrow_R \mathbb{Z}_p$, for all $\mathsf{att} \in \mathcal{S}$, $[c_{\mathsf{att}}]_1 := H(\mathsf{att}) \cdot s$

Return $\mathsf{ct} := ([s]_2, \{[c_{\mathsf{att}}]_1\}_{\mathsf{att}\in\mathcal{S}})$, $k := s \cdot [\alpha]_T$

$\underline{\mathsf{KeyGen}\Big(\mathsf{msk}, (\mathbf{M} \in \mathbb{Z}_p^{\ell\times m}, \rho : [\ell] \to \{0,1\}^*)\Big):}$

$\{\alpha_i\}_{i\in[\ell} \leftarrow \mathsf{GenShare}(\mathbf{M}, \alpha)$, $r \leftarrow_R \mathbb{Z}_p$, for all $i \in [\ell]$: $[d_i]_1 := [\alpha_i]_1 + H\big(\rho(i)\big) \cdot r$

Return $\mathsf{sk} := \big([r]_2, \{[d_i]_1\}_{i\in[\ell]}\big)$

$\underline{\mathsf{Dec}\left(\mathsf{pk}, \mathsf{ct} := ([s]_2, \{[c_{\mathsf{att}}]_1\}_{\mathsf{att}\in\mathcal{S}}), \mathsf{sk} := \big([r]_2, \{[d_i]_1\}_{i\in[\ell]}\big)\right):}$

Return $\left[\sum_{i\in[\ell],\rho(i)\in\mathcal{S}} \omega_i \cdot d_i\right]_1 \bullet [s]_2 - \left[\sum_{i\in[\ell],\rho(i)\in\mathcal{S}} \omega_i \cdot c_{\rho(i)}\right]_1 \bullet [r]_2$

Fig. 2. KP-ABE. Here, $H : \{0,1\}^* \to \mathbb{G}_1$ is a RO.

$\underline{\mathsf{Setup}(1^\lambda):}$

$\mathcal{PG} \leftarrow_R \mathsf{GGen}(1^\lambda)$, $\alpha \leftarrow_R \mathbb{Z}_p$, $w \leftarrow_R \mathbb{Z}_p^*$, $\mathsf{msk} := (\alpha, w)$, $\mathsf{pk} := ([w]_1, [\alpha]_T)$

Return $(\mathsf{pk}, \mathsf{msk})$.

$\underline{\mathsf{Enc}\Big(\mathsf{pk}, (\mathbf{M} \in \mathbb{Z}_p^{\ell \times m}, \rho : [\ell] \to \{0,1\}^*)\Big):}$

$s \leftarrow_R \mathbb{Z}_p$, $\{s_i\}_{i \in [\ell} \leftarrow \mathsf{GenShare}(\mathbf{M}, s)$, $u \leftarrow_R \mathbb{Z}_p$, for all $i \in [\ell]$, $[c_i]_1 := [s_i]_1 + H(\rho(i)) \cdot u$

Return $\mathsf{ct} := \big([u]_2, [s \cdot w]_1, \{[c_i]_1\}_{i \in [\ell]}\big)$, $k := s \cdot [\alpha]_T$

$\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathcal{S}):}$

$r \leftarrow_R \mathbb{Z}_p$, for all $\mathsf{att} \in \mathcal{S}$, $[d_{\mathsf{att}}]_1 := H(\mathsf{att}) \cdot r$

Return $\mathsf{sk} := \big([r]_2, [w^{-1} \cdot (\alpha - r)]_2, \{[d_{\mathsf{att}}]_1\}_{\mathsf{att} \in \mathcal{S}}\big)$

$\underline{\mathsf{Dec}\left(\mathsf{pk}, \mathsf{ct} := \big([u]_2, [s \cdot w]_1, \{[c_i]_1\}_{i \in [\ell]}\big), \mathsf{sk} := \big([r]_2, [w^{-1} \cdot (\alpha - r)]_2, \{[d_{\mathsf{att}}]_1\}_{\mathsf{att} \in \mathcal{S}}\big)\right):}$

Return $\Big[\sum_{i \in [\ell], \rho(i) \in \mathcal{S}} \omega_i \cdot c_i\Big]_1 \bullet [r]_2 - \Big[\sum_{i \in [\ell], \rho(i) \in \mathcal{S}} \omega_i \cdot d_{\rho(i)}\Big]_1 \bullet [u]_2 + [s \cdot w]_1 \bullet [w^{-1} \cdot (\alpha - r)]_2$

Fig. 3. CP-ABE. Here, $H : \{0,1\}^* \to \mathbb{G}_1$ is a RO.

References

Bei96. Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. Ph.D., Technion - Israel Institute of Technology, 1996. 1

KW93. M. Karchmer and A. Wigderson. On span programs. In *Structure in Complexity Theory Conference, 1993., Proceedings of the Eighth Annual*, pages 102–111, May 1993. 1

Acknowledgements.
We thank Miguel Ambrona, Michele Orrù and Hoeteck Wee for insightful discussions