Key-policy Attribute-based Encryption for Boolean Circuits from Bilinear Maps

Ferucio Laurenţiu Ţiplea and Constantin Cătălin Drăgan

Department of Computer Science
Alexandru Ioan Cuza University of Iaşi
Iaşi, Romania

BalkanCryptSec, Oct 16-17, 2014
Istanbul, Turkey

Outline

Key-policy Attribute-based Encryption (KP-ABE)

Setup(λ): PPT alg.: outputs public parameters *PP* and master key *MSK*;

Enc(m, A, PP): PPT alg.: encrypts message m with attributes $A \subseteq \mathcal{U}$;

KeyGen($\mathcal{C}, MSK$): PPT alg.: outputs decryption key for access structure $\mathcal{C}$;

Dec(E, D): DPT alg.: decrypts E with D and outputs a message or the special symbol $\perp$.

Correctness property:

$$E \leftarrow Enc(m, A, PP),\ \mathcal{C}(A) = 1,\ D \leftarrow KeyGen(\mathcal{C}, MSK) \Rightarrow m = Dec(E, D)$$

Secret Sharing and KP-ABE

V. Goyal et al.: *Attribute-based Encryption for Fine-grained Access Control of Encrypted Data*, CCS 2006

For n attributes $1, \ldots, n$:

Setup(λ): $y, t_1, \ldots, t_n \leftarrow \mathbb{Z}_p$, $MSK = (y, t_1, \ldots, t_n)$

$PP = (p, G_1, G_2, g, e, n, Y = e(g,g)^y, (T_i = g^{t_i} | i \in \mathcal{U}))$

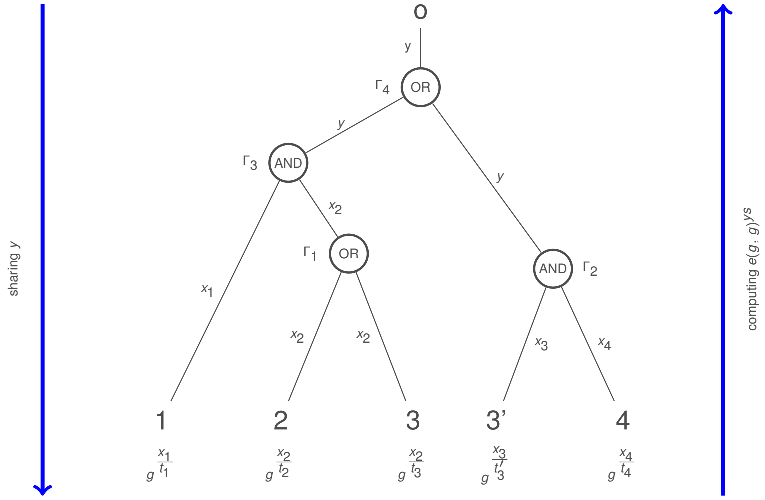
Enc(m, A, PP): $s \leftarrow \mathbb{Z}_p$, $E = (A, E' = mY^s, (E_i = T_i^s = g^{t_i s} | i \in A), g^s)$

KeyGen($\mathcal{C}, MSK$): $y \xrightarrow{Shamir} y_1, \ldots, y_n$, $D = (D_i = g^{y_i/t_i} | i \in \mathcal{U})$

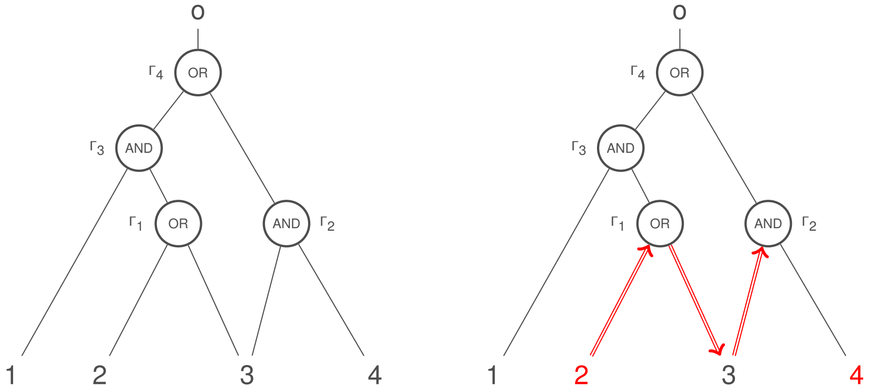
Dec(E, D): compute $Y^s = e(g,g)^{ys}$ (y is a linear combination of shares)

Works only for Boolean formulas !

Secret Sharing and KP-ABE



Extension to Boolean Circuits. The Backtracking Attack



Solutions to the Backtraking Attack

1. based on multilinear maps
   1. Garg et al.: *Attribute-based Encryption for Circuits from Multiminear Maps*, CRYPTO 2013
2. based on integer lattices
   1. Gorbunov et al.: *Attribute-based Encryption for Circuits*, STOCS 2013
   2. Boneh et al.: *Attribute-based Encryption for Arithmetic Circuits*, Cryptology ePrint Archive 2013: 669
   3. Boneh et al.: *Fully Key-homomorphic Encryption, Arithmetic Circuit ABE, and Compact Garbled Circuits*, EUROCRYPT 2014

Can it be done using only bilinear maps ? Garg et al. conjectured “No”

Quick Review of Garg et al.'s Solution

1. uses leveled multilinear maps, which consists of:
   1. k groups $G_1, \ldots, G_k$ of prime order p, where $k-1$ is the circuit depth;
   2. k generators $g_1, \ldots, g_k$ of these groups
   3. set $\{e_{i,j} : G_i \times G_j \to G_{i+j} | i, j \geq 1,\ i+j \leq k\}$ of bilinear maps satisfying

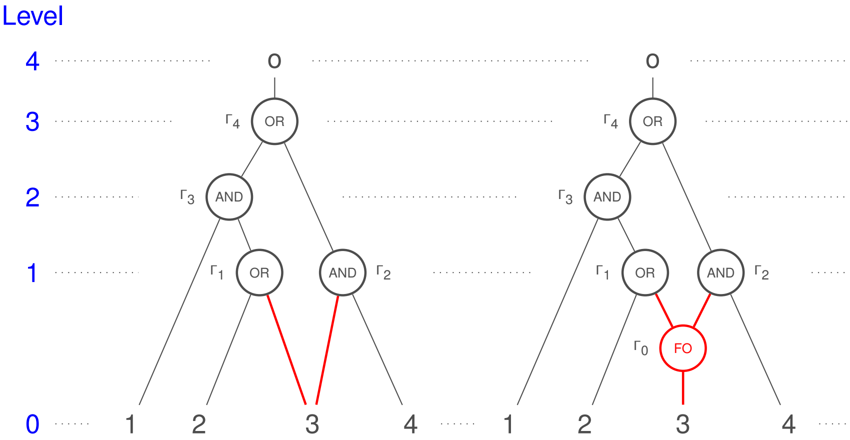
$$e_{i,j}(g_i^a, g_j^b) = g_{i+j}^{ab}$$

2. three or four keys are associated to each circuit gate
3. the circuit is evaluated bottom-up and the values associated to output wires of gates on level j are powers of g_{j+1}
4. $e_{i,j}$ work only in the "forward" direction

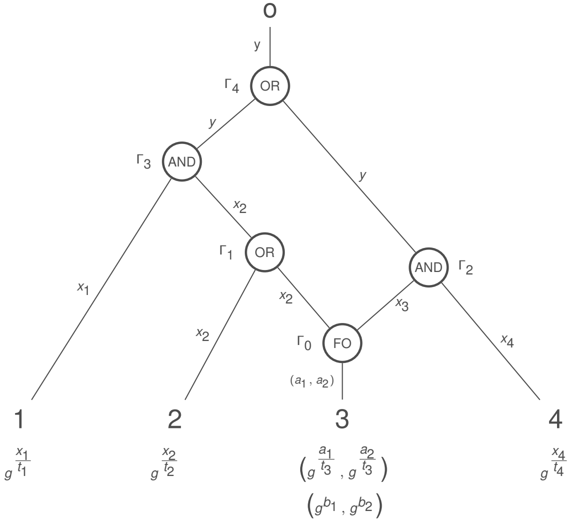
Outline

1. Introduction to ABE
2. Our Construction
   - Secret Sharing
   - Security Issues
   - Complexity
3. Application
4. Conclusions

FANOUT-gates



Secret Sharing

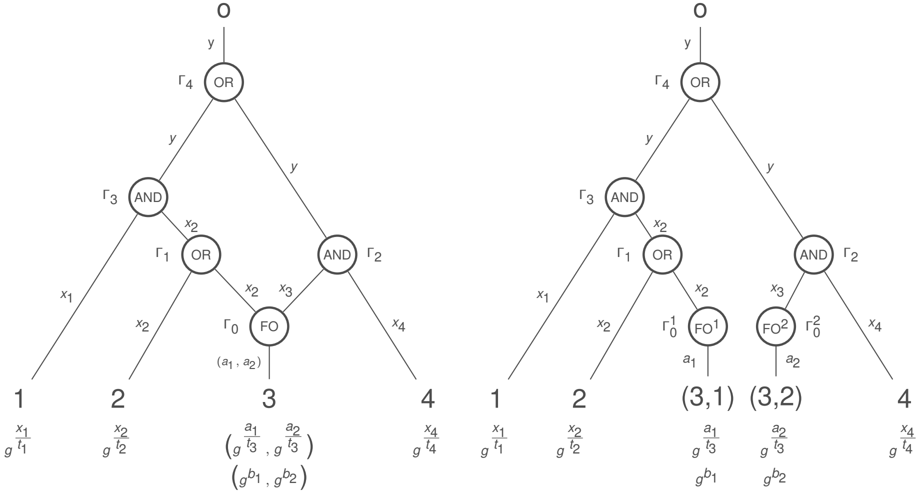


$$\Gamma_3: \quad x_1 \leftarrow \mathbb{Z}_p,\ x_2 = y - x_1$$

$$\Gamma_0: \quad a_1 \leftarrow \mathbb{Z}_p,\ b_1 = x_2 - a_1$$
$$a_2 \leftarrow \mathbb{Z}_p,\ b_2 = x_3 - a_2$$

Outline

Resistance to the Backtracking Attack



Selective Security for KP-ABE

The adversary's advantage in the following game is negligible:

Init: adversary announces the set A of attributes

Setup: adversary receives PP

Phase 1: oracle access to the decryption key generation oracle (for Boolean circuits $\mathcal{C}$ with $\mathcal{C}(A) = 0$)

Challenge: adversary submits two equally length messages m_0 and m_1 and receives the ciphertext associated to A and one of the two messages, say m_b

Phase 2: oracle access to the decryption key generation oracle (with the same constraint as above)

Guess: adversary outputs a guess $b' \leftarrow \{0, 1\}$

Security in the Selective Model

Decisional BDH problem in (G_1, G_2, e):

Instance: (g, g^a, g^b, g^c, z), where $\langle g \rangle = G_1$ and $a, b, c, z \leftarrow \mathbb{Z}_p$

Question: distinguish between $e(g, g)^{abc}$ and $e(g, g)^z$

Decisional BDH assumption: no PPT algorithm can solve the DBDH problem with more than a negligible advantage

Theorem 1

The KP-ABE_Scheme is secure in the selective model under the decisional bilinear Diffie-Hellman assumption.

Outline

Complexity

Parameters: n input wires, r FANOUT-gates of maximum fanout j

1. Case 1: no paths between FANOUT-gates

   key components: $\leq n + r(j-1)$

2. Case 2: there are paths between FANOUT-gates

   key components: exponential in the number of FANOUT levels

Our scheme is efficient if the FANOUT-gates are not connected and/or are on the lowest levels (the next slide illustrates this)

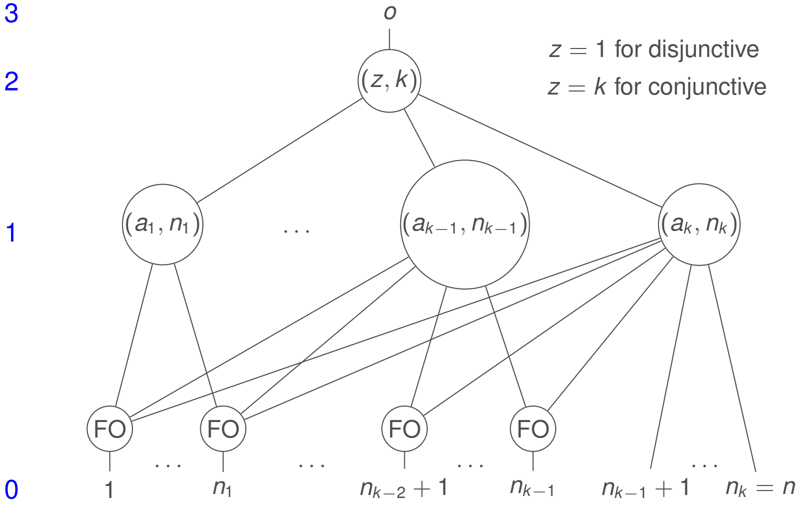
Multivelel Access Structure

$(\overline{a}, \overline{\mathcal{U}}, \mathcal{S})$, where

1. $\overline{a} = (a_1, \ldots, a_k)$ is a vector of positive integers with $0 < a_1 < \cdots < a_k$
2. $\overline{\mathcal{U}} = (\mathcal{U}_1, \ldots, \mathcal{U}_k)$ is a partition of $\mathcal{U}$
3. Disjunctive: $\mathcal{S} = \{A \subseteq \mathcal{U} | (\exists 1 \leq i \leq k)(|A \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq a_i)\}$
4. Conjunctive: $\mathcal{S} = \{A \subseteq \mathcal{U} | (\forall 1 \leq i \leq k)(|A \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq a_i)\}$

Multilevel access structures cannot be represented by Boolean formulas !

Boolean Circuit for Multilevel Access Structures



Comparissons

Scheme	Average no. of keys	multilinear/bilinear
Garg et al.'s multi-linear map approach	Case 1: $a_i = n_i$ for all i $n^{\frac{k+5}{2}} + 3k + 1 - z$ Case 2: $a_i < n_i$ for all i $\geq \left(2 + \frac{(k+1)(k+5)}{3}\right) n + 2k + 1 - z$	multilinear map with 3 components
Our scheme	$n^{\frac{k+1}{2}}$	one bilinear map

Conclusions

1. We have proposed an ABE scheme for Boolean circuits, based on secret sharing and just one bilinear map;
2. The scheme is efficient only for some distributions of the FANOUT-gates in the circuit
3. It is more efficient for multilevel access structures than the scheme(s) based on multilinear maps

Finding an ABE scheme with just one bilinear map and efficient for all Boolean circuits still remains an open problem (might not be possible !)