Key-policy Attribute-based Encryption for General Boolean Circuits from Secret Sharing and Multi-linear Maps

Constantin Cătălin Drăgan and Ferucio Laurenţiu Ţiplea

LORIA, Nancy, France

UAIC, Iaşi, Romania

BalkanCryptSec, Sept 3-4, 2015
Koper, Slovenia

Outline

Attribute-based Encryption (ABE)

- Introduced by Sahai and Waters in 2005 as a generalization of IBE;
- Two forms of ABE:
  - Key-policy ABE (KP-ABE);
  - Ciphertext-policy ABE (CP-ABE);
- Known constructions:
  - based on secret sharing and just one bilinear map;
  - based on leveled multi-linear maps;
  - based on lattices and the LWE problem.

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

A KP-ABE scheme consists of four algorithms:

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

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

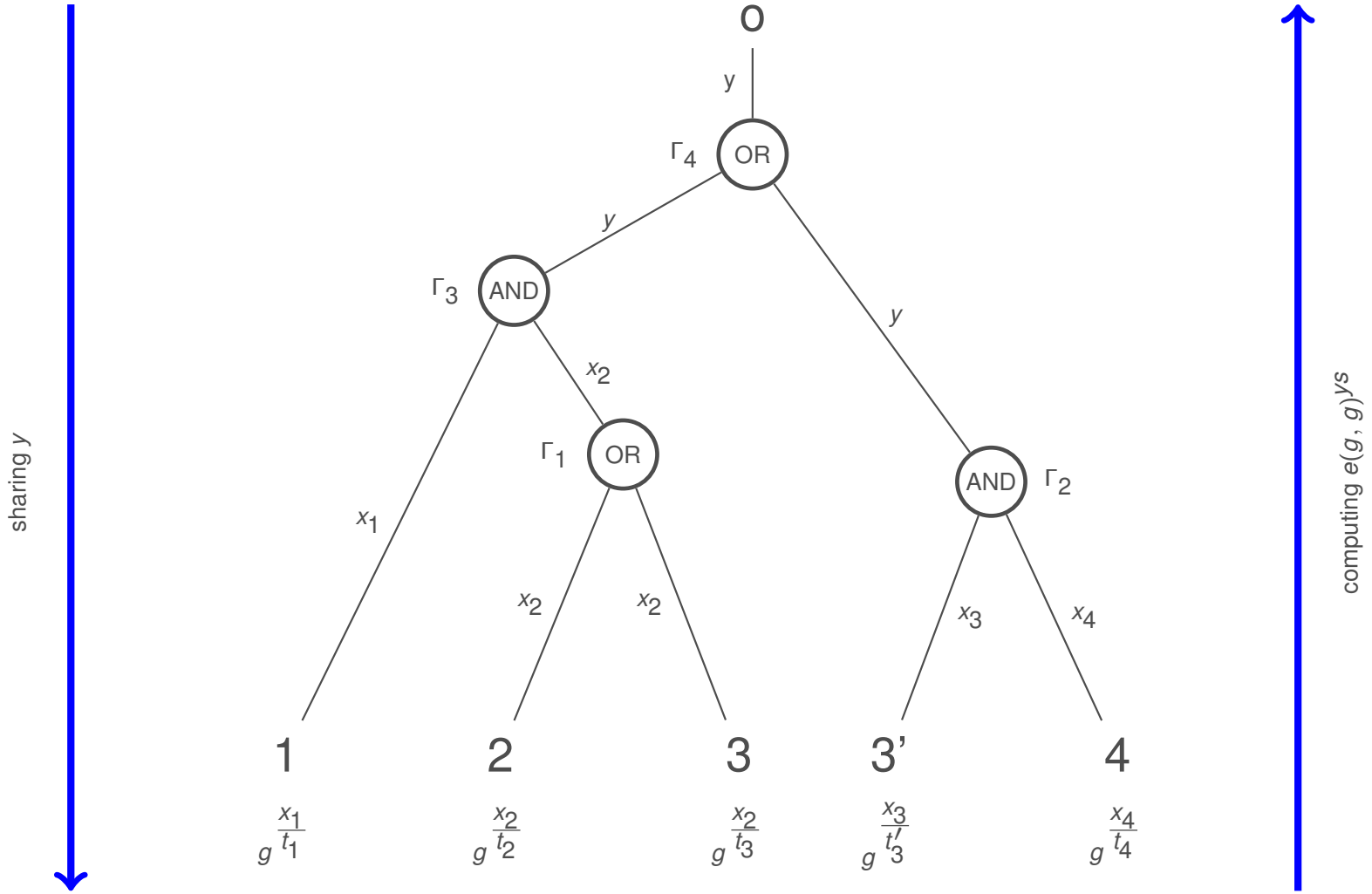
Enc(m, A, PP): $s \leftarrow \mathbb{Z}_p$, $E = (A, E' = mY^s, (E_i = T_i^s = g^{t_i s} | i \in A), g^s)$

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

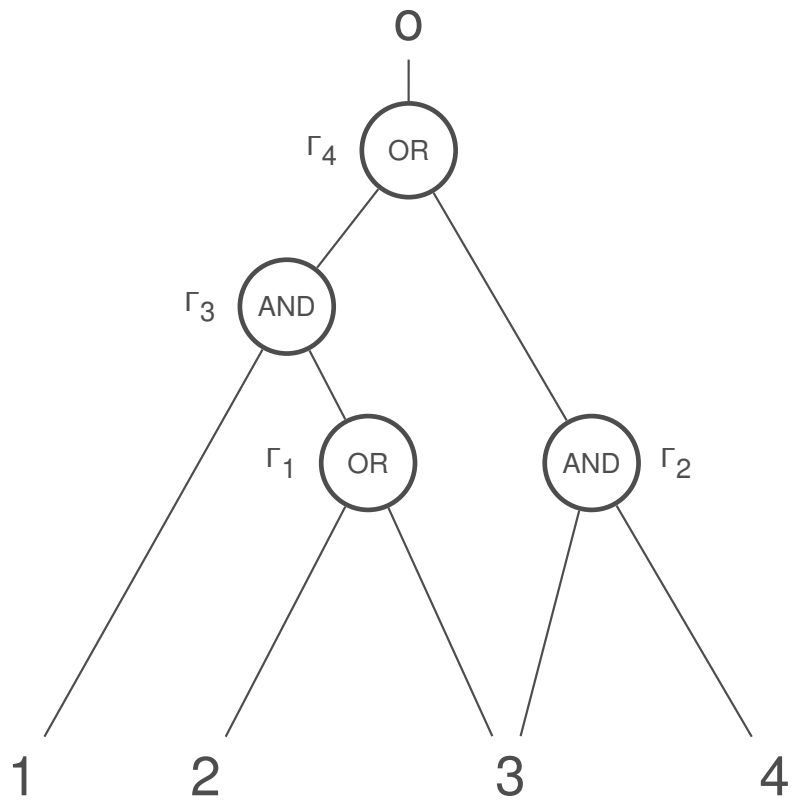
Dec(E, D): compute $Y^s = e(g,g)^{ys}$ (y is a linear combination of shares)

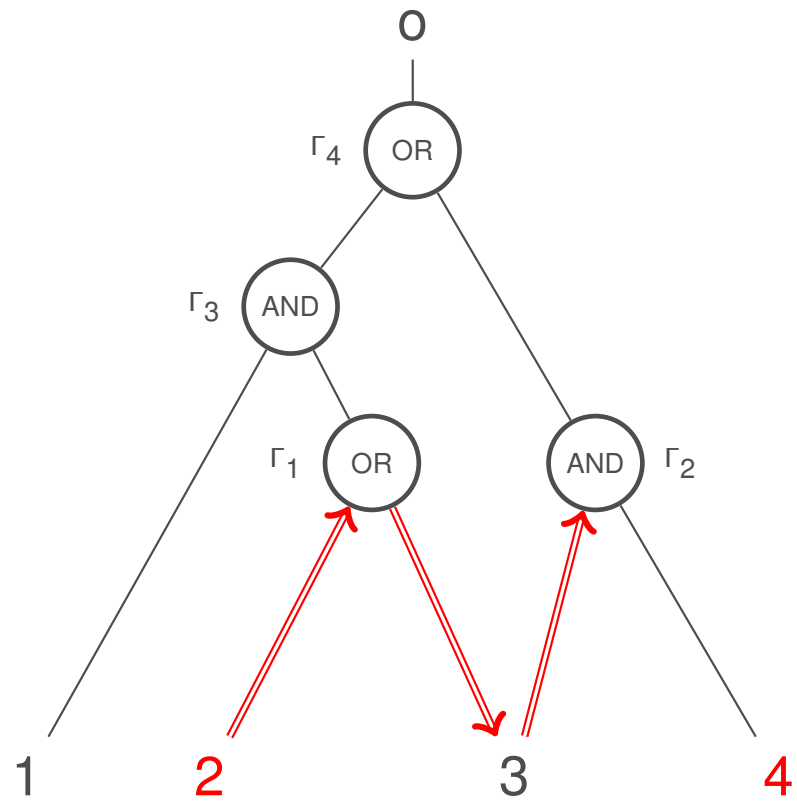
Works only for Boolean formulas !

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”

Progress: “F.L. Ţiplea, C.C. Drăgan: Key-policy ABE for Boolean Circuits from Bilinear Maps, BCS 2014”

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. A 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. Two keys are associated to each input wire
3. Three keys are associated to each AND-gate
4. Four keys are associated to each OR-gate
5. The circuit is evaluated bottom-up and the values associated to output wires of gates on level j are powers of g_{j+1}
6. $e_{i,j}$ works only in the "forward" direction

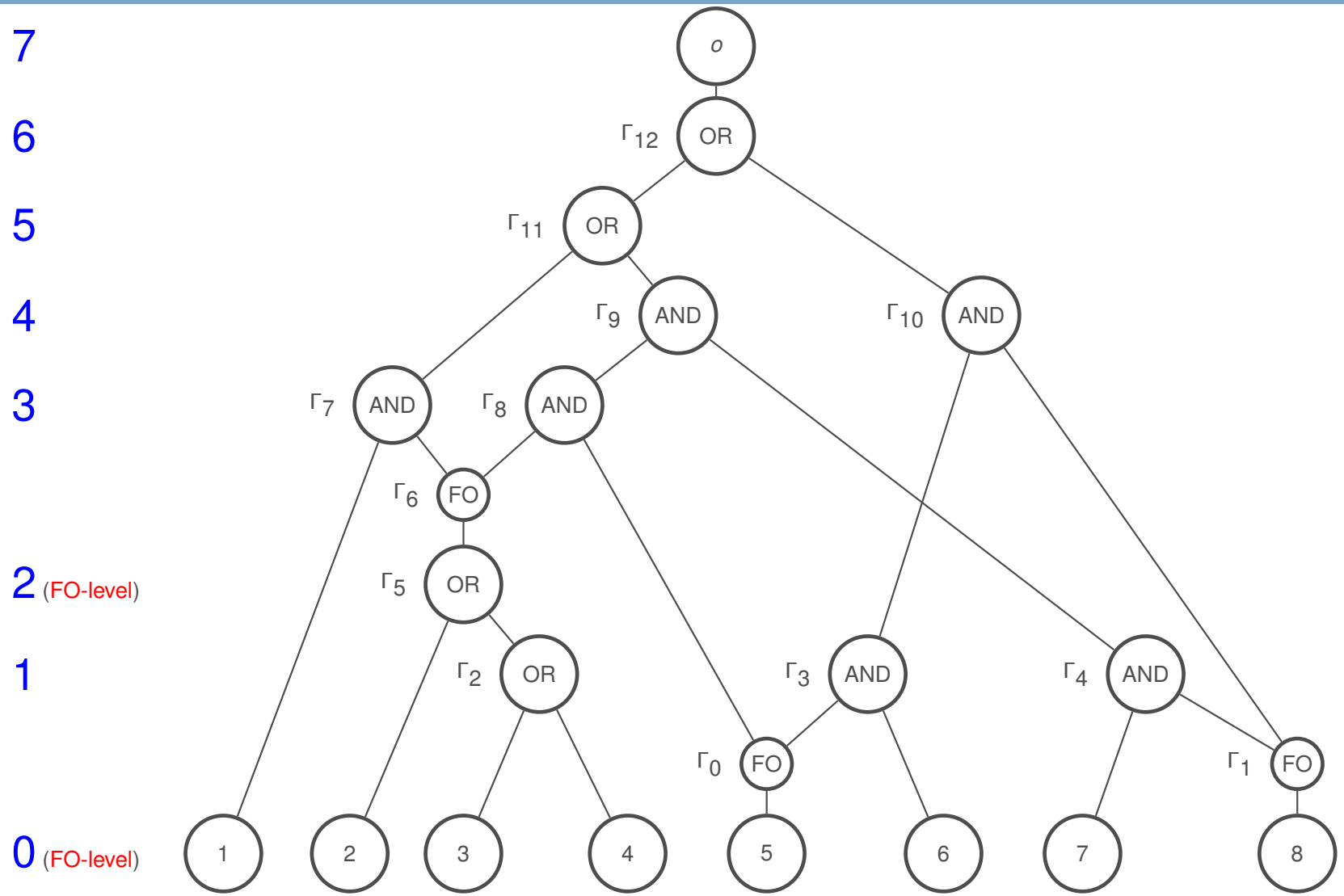
Our Construction

Basic elements of our construction:

1. Gates of fan-out greater than 1 are split into two gates;
2. Different secret sharing procedure;
3. Reconstruction based on chained multi-linear maps.

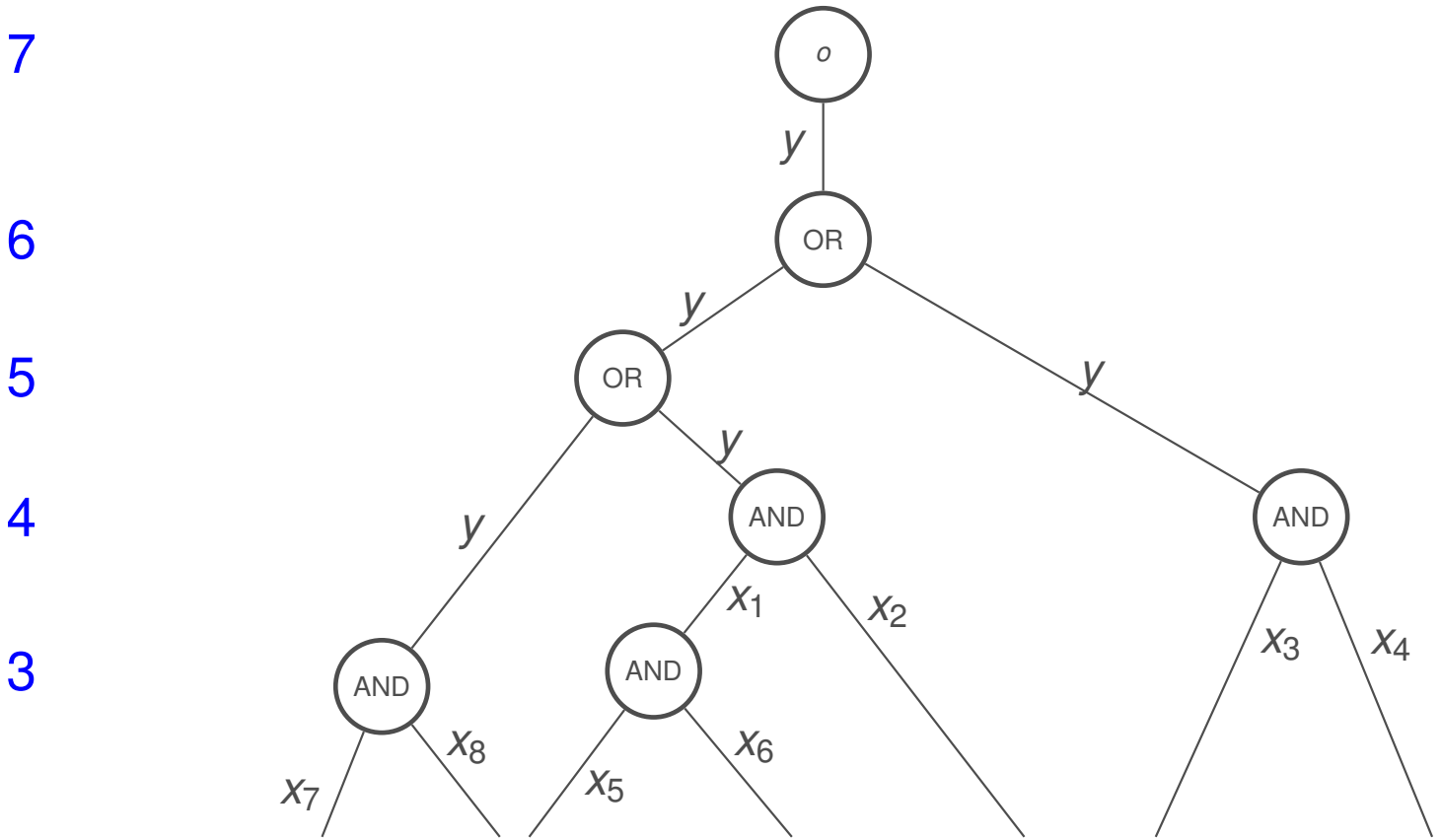
Outline

FO-gates and FO-levels

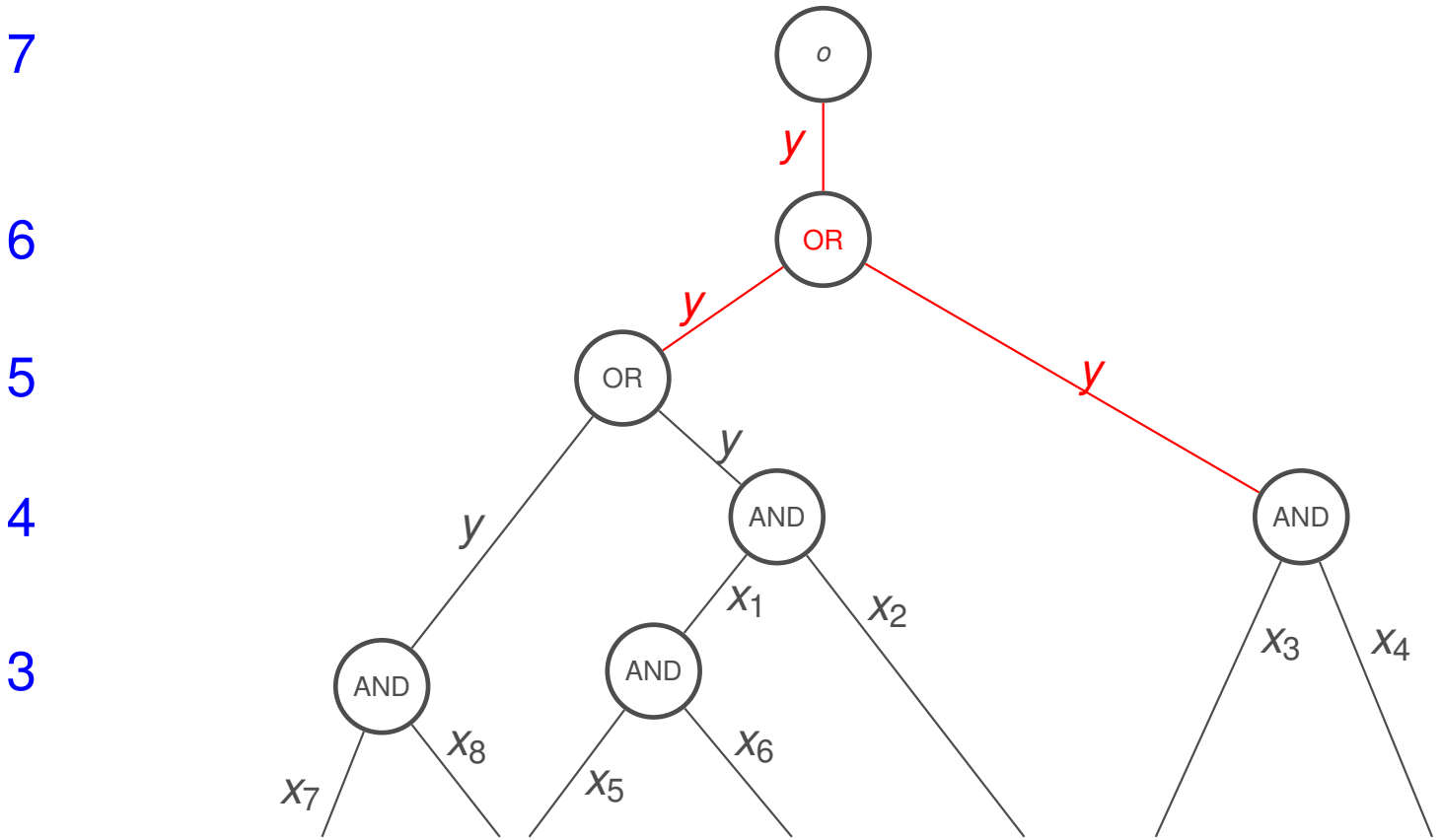


Outline

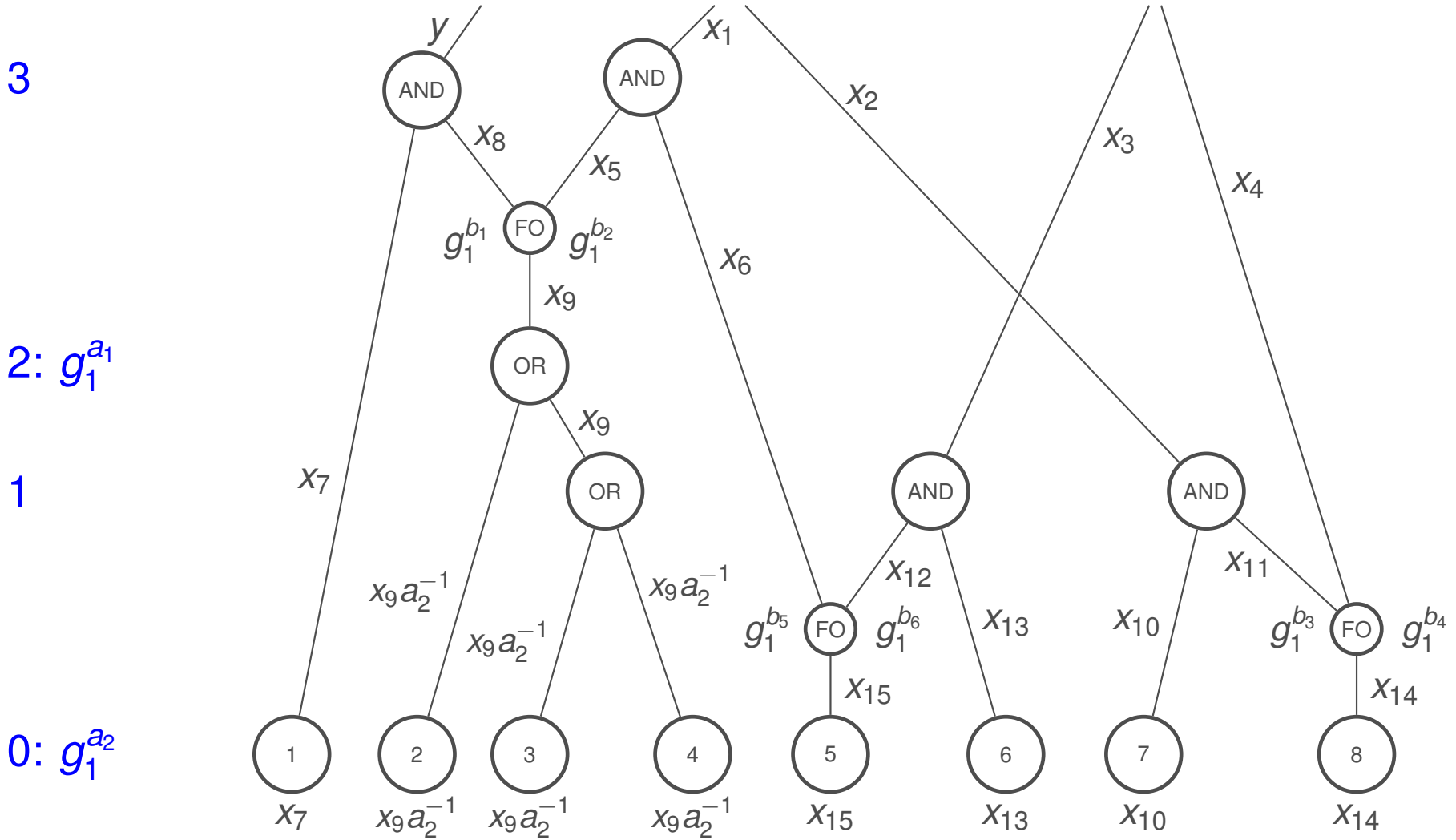
Secret Sharing (Part 1): Gates not Crossing FO-levels



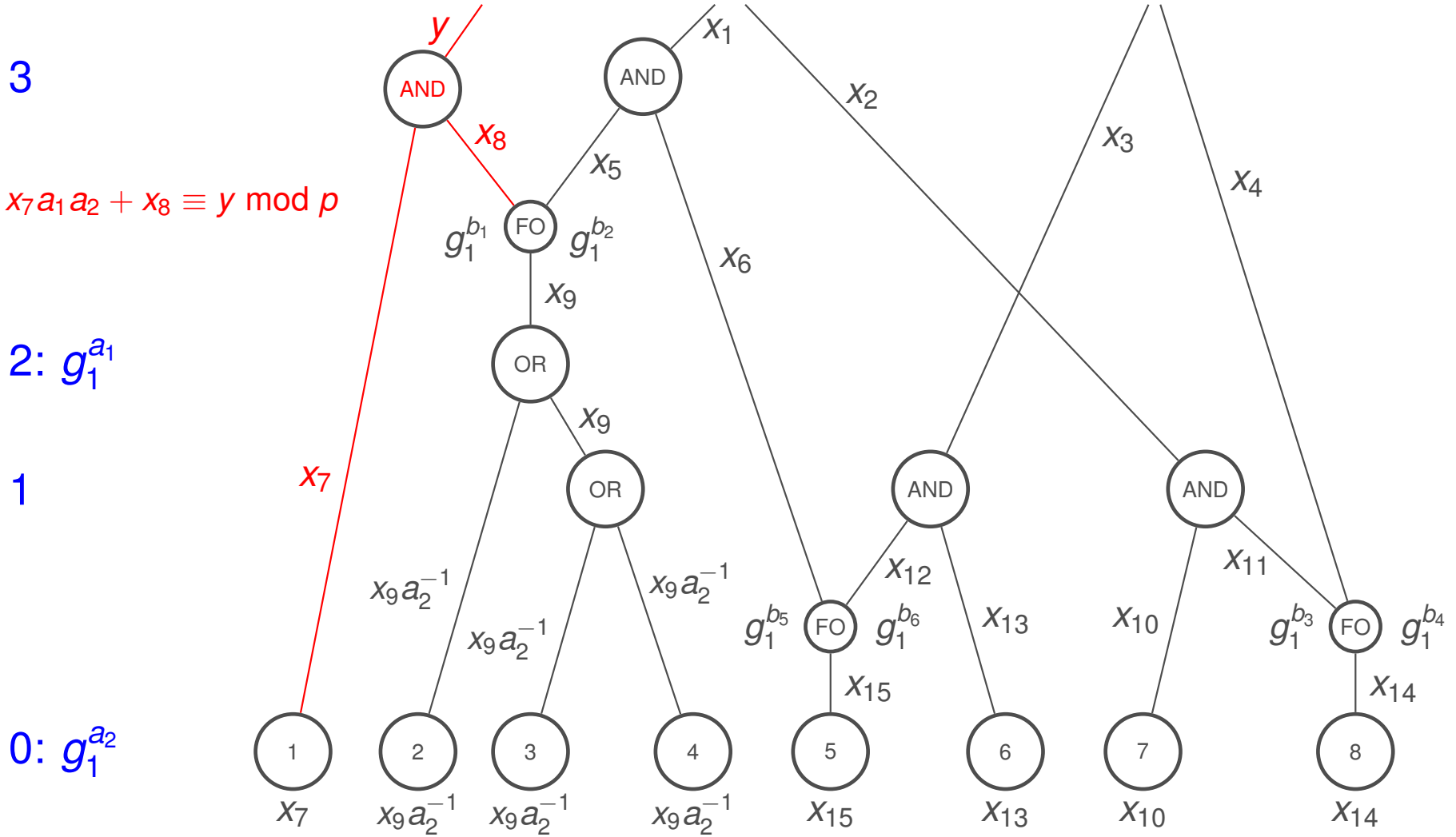
Secret Sharing (Part 1): OR-gate



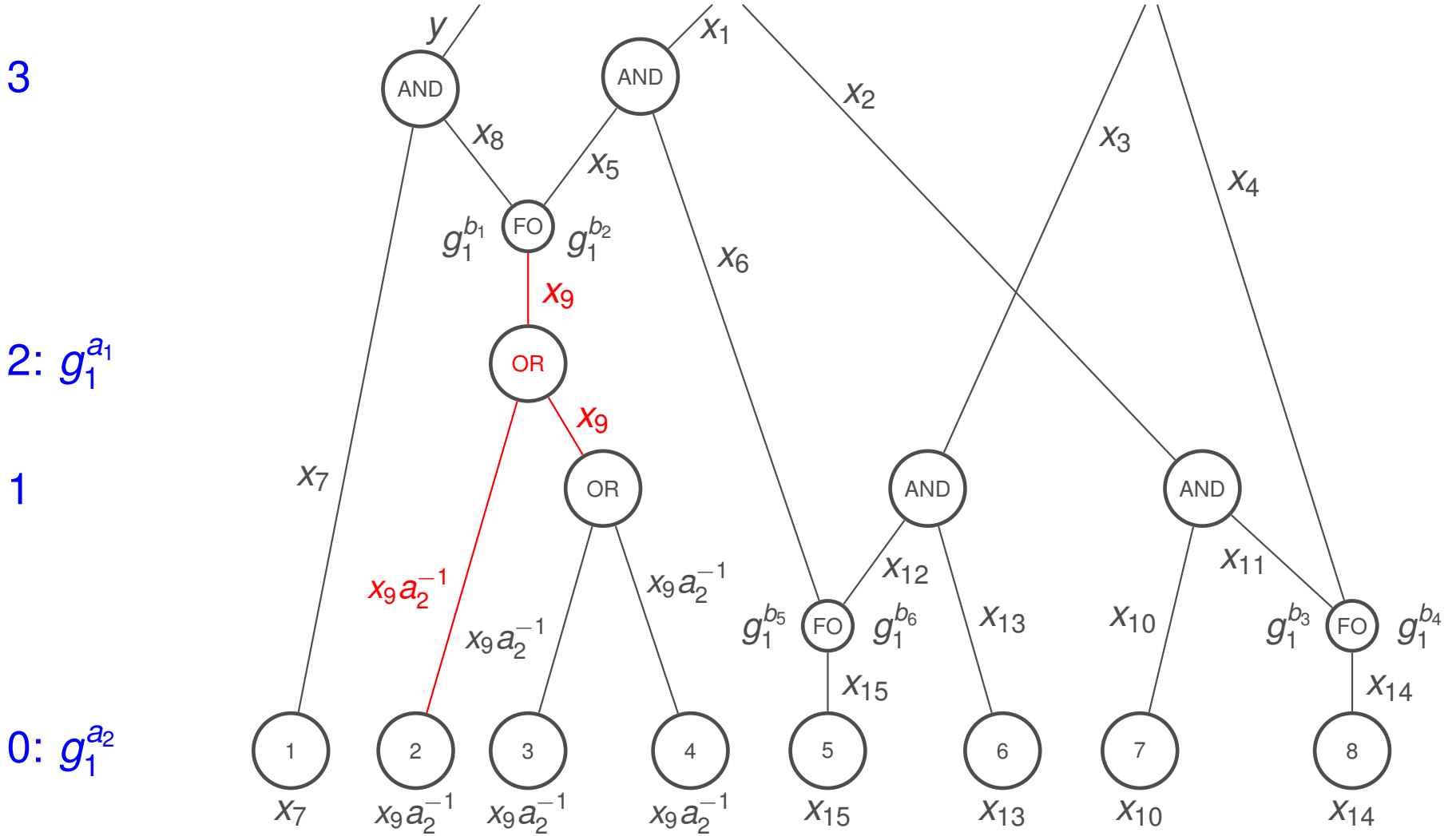
Secret Sharing (Part 2): Gates Crossing FO-levels



Secret Sharing (Part 2): AND-gate



Secret Sharing (Part 2): OR-gate



Secret Sharing (Part 2): FO-gate

3

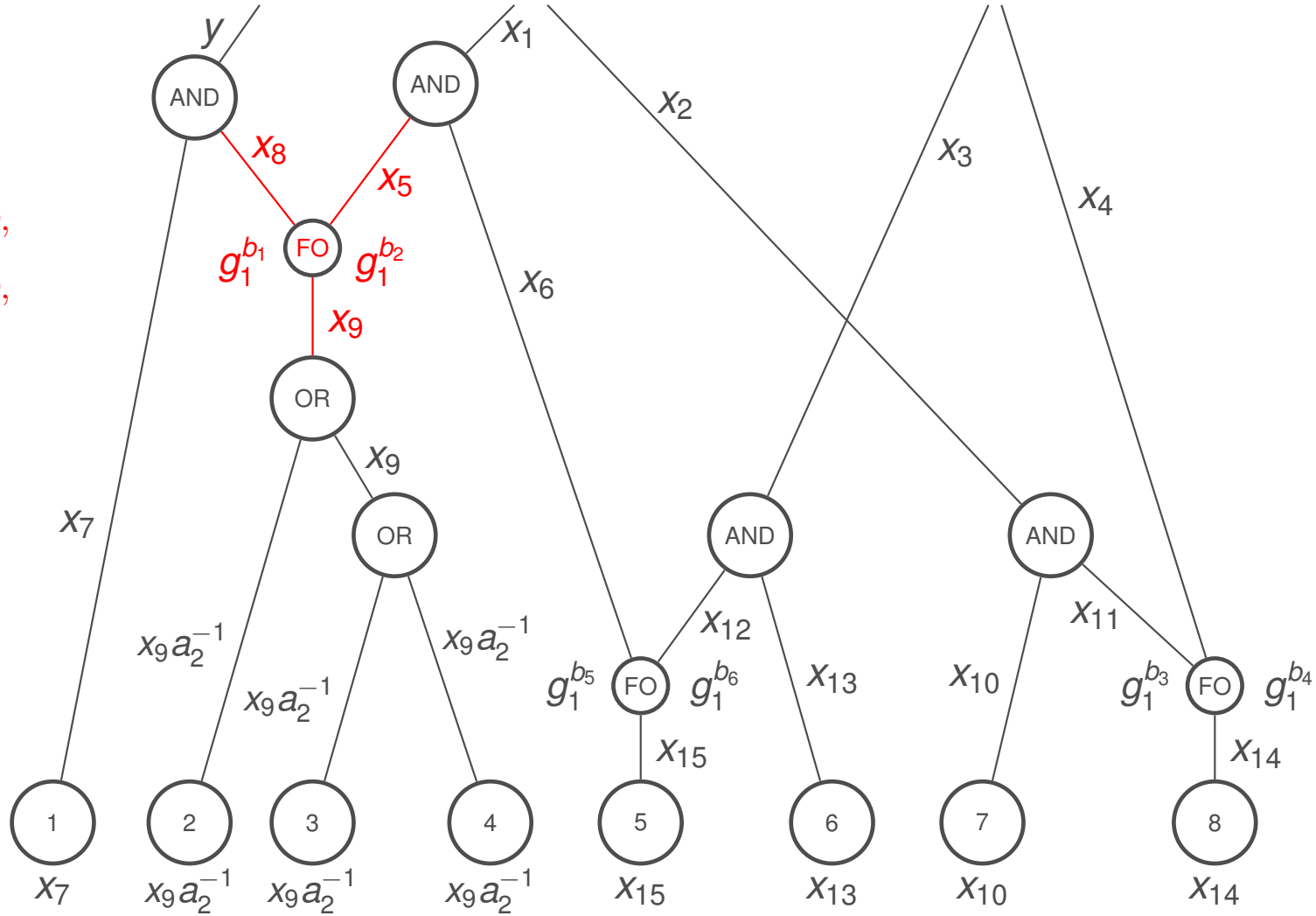
$x_8 \equiv x_9 b_1 \bmod p$,

$x_5 \equiv x_9 b_2 \bmod p$,

2: $g_1^{a_1}$

1

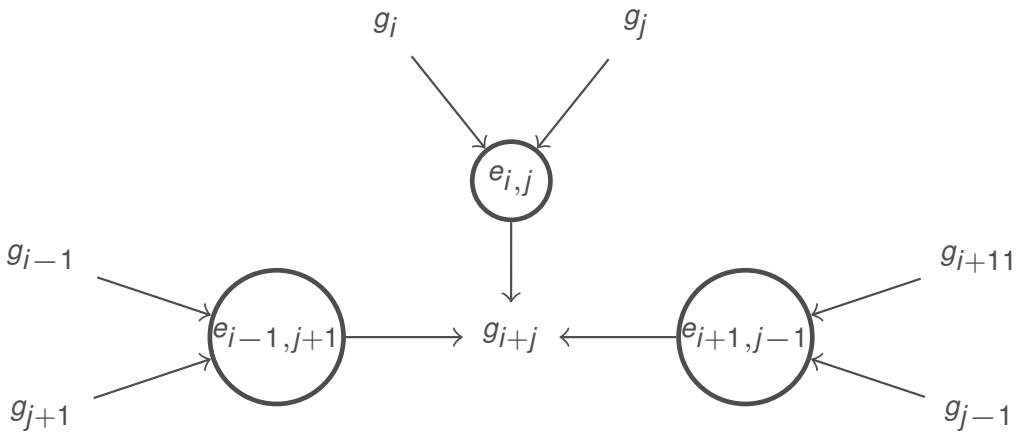
0: $g_1^{a_2}$



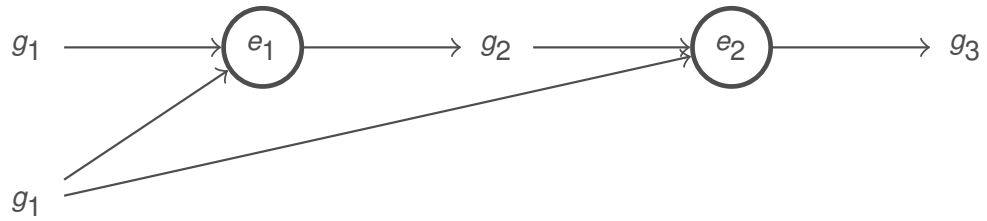
Outline

Reconstruction: Leveled vs. Chained Multi-linear Maps

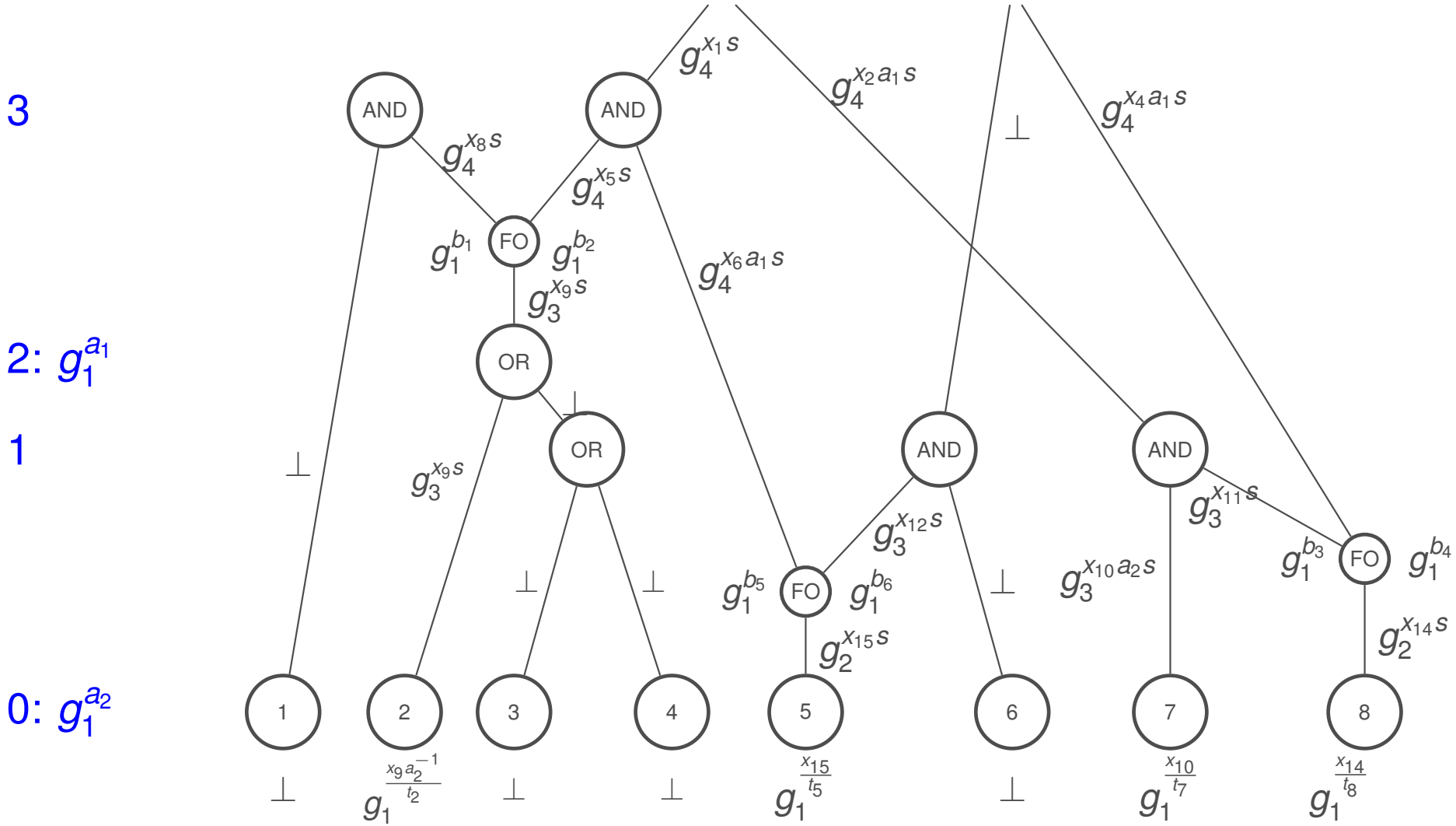
Leveled multi-linear map



Chained multi-linear map



Reconstruction by Chained Multi-linear Maps



Outline

Translation into Graded Encoding Systems (GES)

Direct translation into the CLT (Coron, Lepoint, Tibouchi) GES (CRYPTO 2015):

- For each integer associated to an input wire, the sampling procedure outputs a level-0 encoding;
- For each FO-level key or FO-gate public key, the sampling procedure outputs a level-1 encoding;

Outline

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 MDH problem in $\mathbf{e} = \{e_{i,j} : G_i \times G_j \to G_{i+j},\ i + j \leq k\}$:

Instance: $(g_1, g_1^s, g_1^{c_1}, \ldots, g_1^{c_k}, z)$, where $\langle g_1 \rangle = G_1$ and $s, c_1, \ldots, c_k, z \leftarrow \mathbb{Z}_p$

Question: distinguish between $g_k^{sc_1 \cdots c_k}$ and g_k^z

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

Theorem 1

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

Outline

Complexity and Comparisons

Boolean circuits with – n_1 input gates of fan-out 1 – n_2 input gates of fan-out > 1 – q_1 logic gates of fan-out > 1 – q_2 logic gates of fan-out > 1 – r FO-levels and depth ℓ	No of keys	Multi-linear map (type, size, and mult. depth)
Garg et al.'s KP-ABE scheme	$2(n_1 + n_2) + 3(q_1 + q_2) \leq$ *no. keys* $\leq$ $2(n_1 + n_2) + 4(q_1 + q_2)$	• leveled • $\frac{\ell(\ell+1)}{2}$ • $\ell + 1$
Our KP-ABE scheme	$n_2 + q_1 + q_2 + 3 \leq$ *no. keys* $\leq$ $n_2 + q_1 + 2q_2 + 2$	• chained • $r + 1 < \ell$ • $r + 1$

Conclusions

1. We have proposed a KP-ABE scheme for general Boolean circuits, based on secret sharing and chained multi-linear maps;
2. Our scheme associates exactly one key to each input, each FO-level, and each FO-gate output;
3. The scheme is more efficient than Grag et al.'s scheme based on leveled multi-linear maps.

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