A Hybrid KP-ABE Scheme for Universal Circuits, Based on Monotone Span Programs

Master's Thesis in Computer Science

Iulian Oleniuc

July, 2025

Table of Contents

Introduction

Overview of Our Work

Introduction

- **Semester 1:** Studying the theoretical foundations of (pairing-based) attribute-based encryption (ABE), monotone access structures (MASes), and monotone span program (MSP) constructions.
- **Semester 2:** Studying KP-ABE schemes for monotone Boolean circuits (MBCs) and MSP lower bounds; optimizing the MSP construction from MBCs with backtracking. $\Rightarrow$ *Paper rejected at Secrypt.*
- **Semester 3:** Studying graph access structures (GASes) and ABE libraries; introducing `U`-gates; proving a new lower bound. $\Rightarrow$ *Paper accepted at CSJM!*
- **Semester 4:** Designing a hybrid KP-ABE scheme for universal circuits. $\Rightarrow$ *Paper rejected at SAC, submitted at WISA.*

Motivation (1 / 3)

Introduction

- Cloud computing has become the backbone of modern enterprise software.
- **Privacy Concerns:** In typical cloud setups, service providers may have unrestricted access to sensitive data.
- **Solution:** Key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE).
- In KP-ABE, files are encrypted based on their attributes, such that only those users whose access policies are satisfied by these attributes can decrypt them.

Motivation (2 / 3)

Introduction

- There is a need for KP-ABE schemes running on more and more expressive access policies.
- More compact policies $\Rightarrow$ Shorter decryption keys.
- Trees $\rightarrow$ Circuits.
- `AND`/`OR`-gates [1] $\rightarrow$ (t/n)-threshold gates [2] $\rightarrow$ "CAS-nodes" [3] $\rightarrow$?

Motivation (3 / 3)

Introduction

- All state-of-the-art schemes [1, 4] for monotone Boolean circuits (MBCs) yield exponentially large keys, in order not to sacrifice the scheme security.
- Most existing results regarding ABE, linear secret sharing schemes (LSSSes), and monotone span programs (MSPs) are not clearly correlated in the literature.

Table of Contents

Preliminaries

Secret Sharing

Preliminaries

- A secret is distributed among a group of participants.
- Only specific subsets of participants can reconstruct the secret.

Monotone Access Structures

Preliminaries

- Let $\mathcal{P}$ be the set of participants.
- $\mathbb{A} \subseteq 2^{\mathcal{P}}$.
- **Monotonicity:** $\mathcal{X} \in \mathbb{A} \wedge \mathcal{X} \subseteq \mathcal{Y} \rightarrow \mathcal{Y} \in \mathbb{A}$.

Monotone Access Structures — Example

- $\mathbb{A} \equiv ((A \vee B) \wedge (B \vee C))$.
- $\mathbb{A} = \{\{B\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}$.

Monotone Span Programs

Preliminaries

- $\hat{M} = (M, \rho)$:
  - M is an $m \times d$ matrix.
  - $\rho : \{1, \ldots, m\} \to \mathcal{P}$ is a labeling function.
- $\hat{M}$ **computes** $\mathbb{A}$ if $\vec{1} \in \text{span}(M_{\mathcal{X}}) \leftrightarrow \mathcal{X} \in \mathbb{A}$.
- The **size** of $\hat{M}$ is m.
- **Theorem:** $\hat{M}$ never needs more than m columns to compute $\mathbb{A}$ [5].

Monotone Span Programs — Example

Preliminaries

- $\mathbb{A} \equiv ((A \wedge B) \vee (B \wedge C))$.
- $\vec{1} = (1, 0)$.
- $\hat{M} = \left[\begin{array}{c|cc} A & 0 & -1 \\ B & 1 & 1 \\ C & 0 & -1 \end{array}\right]$.

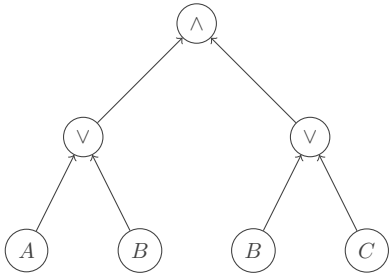
Linear Secret Sharing Schemes

Preliminaries

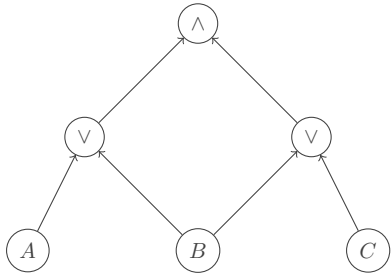
- Each share is given in the form of one or multiple vectors.
- The reconstruction of the secret involves only linear operations over them.
- The **size** of an LSSS is the number of shared vectors.
- An LSSS is **ideal** if each share consists of exactly one vector.
- **Theorem:** LSSSes and MSPs are equivalent [6].

Computational Models

Preliminaries



(a) An MBT computing $\mathbb{A}$.



(b) An MBC computing $\mathbb{A}$.

Figure: An MBT and, respectively, an equivalent MBC, both of them computing the same MAS $\mathbb{A} = \{\{B\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}$.

Table of Contents

Monotone Span Program Limitations

Operations, Constructions, Lower Bounds

Monotone Span Program Limitations

- There are known operations that combine MSPs [7].
- There are known constructions for MSPs from MBTs of in-degree 2 [8] and from threshold trees [9].
- There are known MSP lower bounds [10, 11, 12].

Theoretical Lower Bounds

Monotone Span Program Limitations

- **Theorem:** A lower bound for the size of an MSP computing a particular **monotone access structure** (in *the number of participants*) is $2^{\Omega(n)}$ [13].
- **Problem:** Lack of practical character, since the size of the input to the LSSS is not actually n.

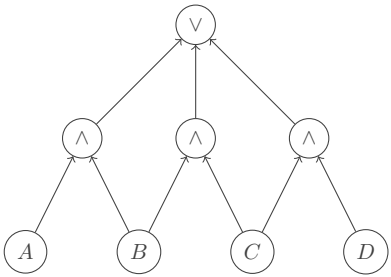
Practical Lower Bounds

Monotone Span Program Limitations

- **Question:** What about a lower bound for the size of an MSP computing a particular **monotone Boolean circuit** (in *its size*)?
- **Proved Claim:** Some polynomial-size monotone Boolean circuits require exponential-size MSPs.

U-Gates

Monotone Span Program Limitations



- $\mathbb{A} \equiv ((A \wedge B) \vee (B \wedge C) \vee (C \wedge D))$.
- Does not admit an MSP of size 4 (proved).
- Can be computed by an MSP of size 5.
- $\vec{1} = (1, 0, 0)$.
- $\hat{M} = \left[\begin{array}{c|ccc} A & 0 & -1 & 0 \\ B & 1 & 1 & 0 \\ C & 0 & -1 & 0 \\ C & 1 & 0 & 1 \\ D & 0 & 0 & -1 \end{array}\right]$.

Graph Access Structures

Monotone Span Program Limitations

- Let $\mathcal{P}$ be the set of participants.
- Let $\mathbb{A}^+$ be the set of minterms in $\mathbb{A}$.
- $\mathbb{A}^+ \subseteq \{\{U, V\} \mid U, V \in \mathcal{P}, U \neq V\}$.

Criterion for Graphs to Admit Ideal LSSSes

Monotone Span Program Limitations

- They should not contain `U`-gates as subgraphs.
- Equivalently, they should be multipartite.
- It is also a sufficient condition [14].

Table of Contents

From Monotone Boolean Circuits to KP-ABE Schemes

Construction Approaches

From Monotone Boolean Circuits to KP-ABE Schemes

1. Circuit $\xrightarrow{[4]}$ LSSS.
2. Circuit $\xrightarrow{\text{NIM optimization [15]}}$ Circuit $\xrightarrow{[4]}$ LSSS.
3. Circuit $\rightarrow$ Tree $\rightarrow$ 2-Tree $\xrightarrow{[8]}$ MSP $\xrightarrow{[2]}$ LSSS.
4. Circuit $\rightarrow$ Tree $\rightarrow$ DNF-Tree $\equiv$ Access Structure $\xrightarrow{\text{backtracking}}$ MSP $\xrightarrow{[2]}$ LSSS.

Table of Contents

A Hybrid KP-ABE Scheme for Universal Circuits

Universal Circuits

A Hybrid KP-ABE Scheme for Universal Circuits

- A directed acyclic graph consisting of:
  1. *input* (i.e., of in-degree zero) nodes, which embed Boolean variables over the attribute set;
  2. *internal* (i.e., of in-degree non-zero) nodes, which embed MSPs computing specific local MASes;
  3. exactly one *output* (i.e., of out-degree zero) node, indicating whether the overall access policy is fulfilled.

Example — Universal Circuit

A Hybrid KP-ABE Scheme for Universal Circuits

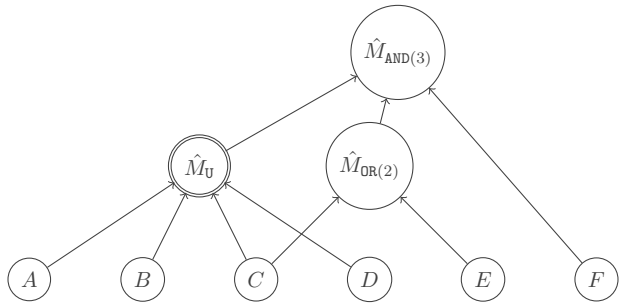


Figure: Example of a universal circuit $\tilde{\mathcal{C}}$ using `AND`, `OR`, and `U`-gates.

Example — Monotone Boolean Circuit

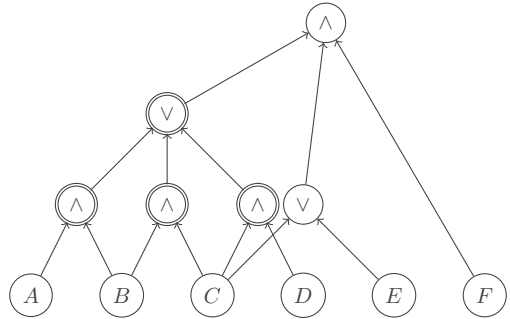


Figure: The circuit $\tilde{\mathcal{C}}$ rewritten as a monotone Boolean circuit $\tilde{\mathcal{C}}'$.

Implementation Detail

A Hybrid KP-ABE Scheme for Universal Circuits

- The implementation does not rely on the entire matrix of each MSP $\hat{M}$, but rather on two custom associated functions:
  1. one that computes the dot product between M and a given vector $\vec{r}$;
  2. one that finds solutions to the equation $\vec{\alpha} \cdot M_{\mathcal{X}} = \vec{1}$.
- We provide the optimized implementations for the `AND`, `OR`, and (t/n)-threshold gates.

Construction

A Hybrid KP-ABE Scheme for Universal Circuits

- Highly technical.
- Based on the constructions of the Hu–Gao scheme for Boolean circuits [1] and the Goyal et al. scheme for MSPs [2].
- Like Hu–Gao, we structure the decryption process over a circuit.
- Over the MSP of each gate, we apply the Goyal et al. scheme.

Security Proof

A Hybrid KP-ABE Scheme for Universal Circuits

- Highly technical.
- Reduction from the Decisional Bilinear Diffie–Hellman problem to the security game.
- Based on the proofs of the Goyal et al. scheme for threshold trees and of the Goyal et al. scheme for MSPs [2].

Efficiency

A Hybrid KP-ABE Scheme for Universal Circuits

- For Boolean circuits and threshold trees — as efficient as previous existing schemes.
- For strictly universal circuits — more efficient, since they can encode policies using way fewer gates, resulting in way lower decryption key sizes.
- Downside inherited from Hu–Gao — the decryption key size may be exponential in the size of the circuit, since the key size equals the number of leaves of the DFS-tree.

Example — Monotone Boolean Circuit

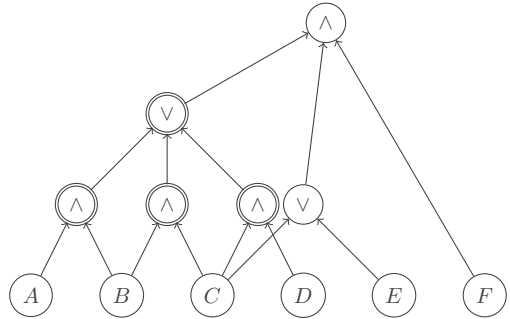


Figure: The circuit $\tilde{\mathcal{C}}$ rewritten as a monotone Boolean circuit $\tilde{\mathcal{C}}'$.

Example — Monotone Boolean Tree

A Hybrid KP-ABE Scheme for Universal Circuits

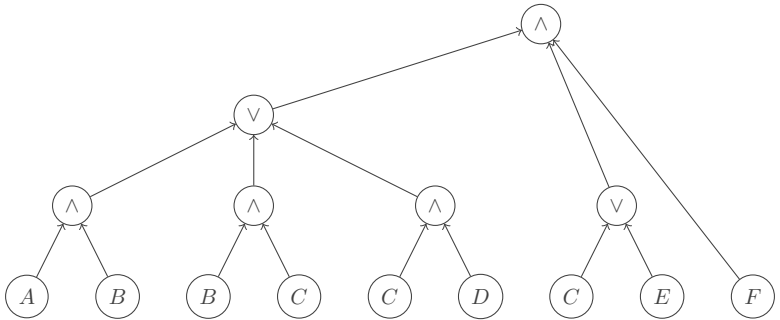


Figure: The monotone Boolean circuit $\tilde{\mathcal{C}}'$ rewritten as a monotone Boolean tree (its DFS-tree) $\tilde{\mathcal{T}}'$.

Implementation

A Hybrid KP-ABE Scheme for Universal Circuits

- Openly accessible on GitHub.
- Written in `C++` (for speed) and `Python` (for linear algebra).
- Using the `C++` wrapper of the `PBC` library for pairing operations.
- Using the `Galois` and `NumPy` libraries for computing $M_{\mathcal{X}'}^{-1}$.
- Developers can define fully-customizable MSP classes, just by writing custom `dot` and `solve` functions.
- The MSP implementations for the `AND`, `OR`, and (t/n)-threshold gates are already provided and highly optimized.

Table of Contents

Conclusion

Our Contribution

Conclusion

- Provided a novel way of proving the nonexistence of ideal LSSSes for certain MASes.
- Proved a new MSP lower bound.
- Introduced the concept of “universal circuits” — circuits at the highest degree of generalization.
- Developed a pairing-based KP-ABE scheme for them.
- Proved that it is more efficient than the Hu–Gao scheme for “general circuits” and the Goyal et al. scheme for “access trees.”
- Implemented it in `C++` (on GitHub).

Future Work

Conclusion

- The decryption key size may be exponential in the size of the circuit — room for improvement.
- More MSP-embedded gates are to be created and implemented (e.g., for "CAS-nodes" [3]).
- Improving the implementation by transpiling the `Python` code for inverting a `Galois` matrix into `C++`.

Bibliography

Conclusion

Peng Hu and Haiying Gao.
A key-policy attribute-based encryption scheme for general circuit from bilinear maps.

Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters.
Attribute-based encryption for fine-grained access control of encrypted data.

Alexandru Ionita.
Optimizing attribute-based encryption for circuits using compartmented access structures.

Ferucio Laurențiu Țiplea and Constantin Cătălin Drăgan.
Key-policy attribute-based encryption for boolean circuits from bilinear maps.

Anna Gál.
A characterization of span program size and improved lower bounds for monotone span programs.

Amos Beimel.
Secure schemes for secret sharing and key distribution.

Ventzislav Nikov and Svetla Nikova.
New monotone span programs from old.

Allison Lewko and Brent Waters.
Decentralizing attribute-based encryption.

Bibliography

Conclusion


Zhen Liu, Zhenfu Cao, and Duncan S Wong.
Efficient generation of linear secret sharing scheme matrices from threshold access trees.


Ingo Wegener.
The complexity of Boolean functions.


Amos Beimel, Anna Gál, and Mike Paterson.
Lower bounds for monotone span programs.


László Babai, Anna Gál, and Avi Wigderson.
Superpolynomial lower bounds for monotone span programs.


Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A Cook.
Exponential lower bounds for monotone span programs.


Ernest F Brickell and Daniel M Davenport.
On the classification of ideal secret sharing schemes.


Alexandru Ioniţă, Denis-Andrei Banu, and Iulian Oleniuc.
Heuristic optimizations of boolean circuits with application in attribute-based encryption.

Q & A

Thank you for your attention!