

RESPONSE-HIDING ENCRYPTED RANGES



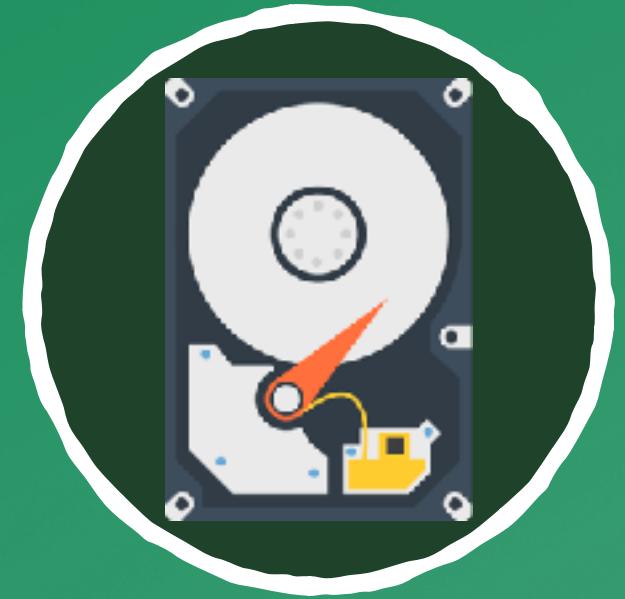
Revisiting Security via
Parametrized Leakage-Abuse Attacks

Evgenios Kornaropoulos
UC Berkeley

Charalampos Papamanthou
University of Maryland

Roberto Tamassia
Brown University

ENCRYPTED DATA



At Rest



In Transit



In Use

ENCRYPTED DATA



At Rest



In Transit



In Use

Queries on **ENCRYPTED DATA**

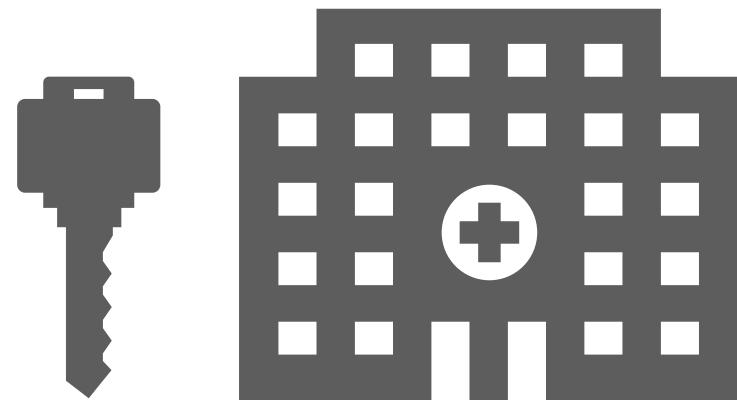




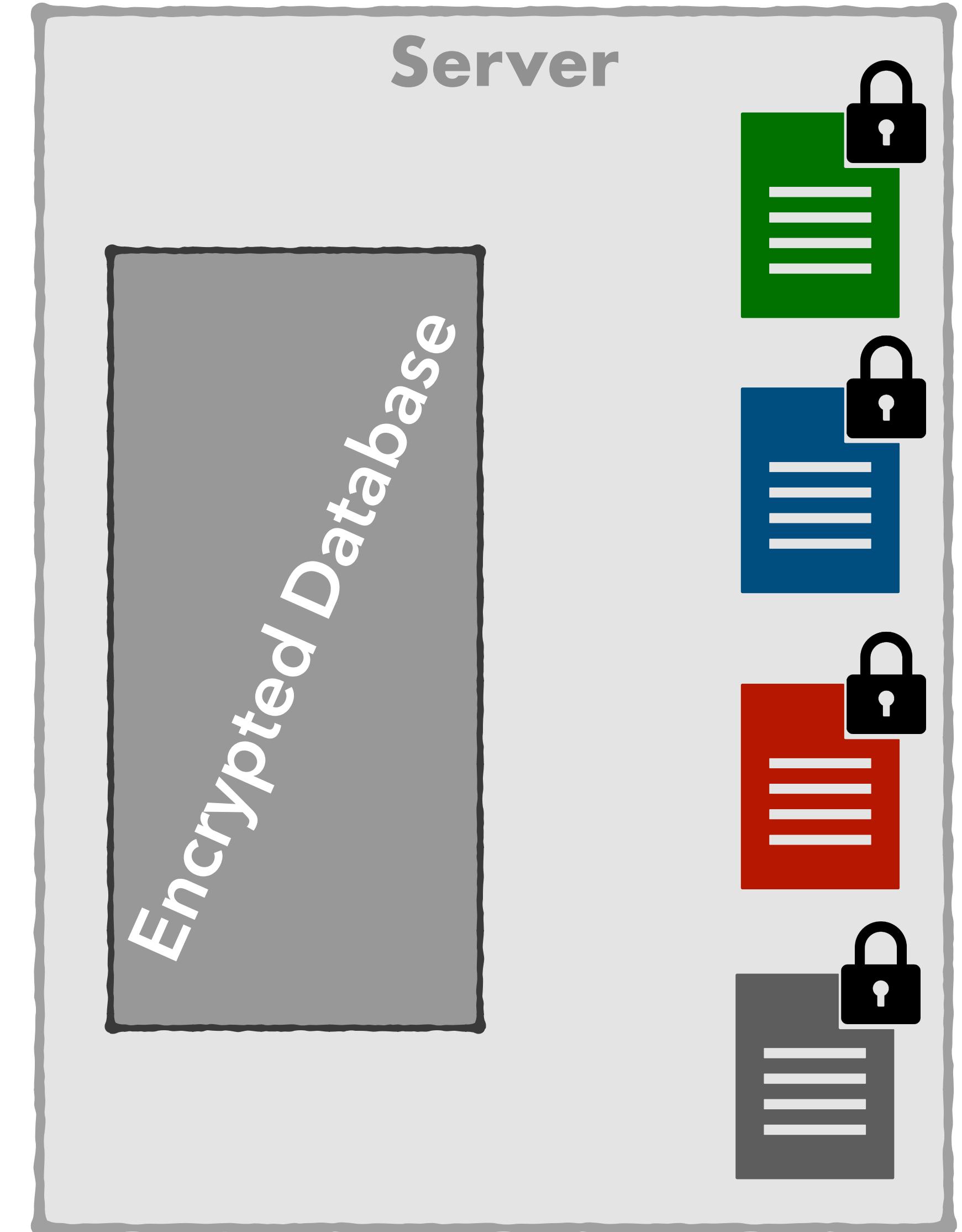
ATTACKING RESPONSE-HIDING DESIGNS

NO ACCESS-PATTERN LEAKAGE

Client



Server

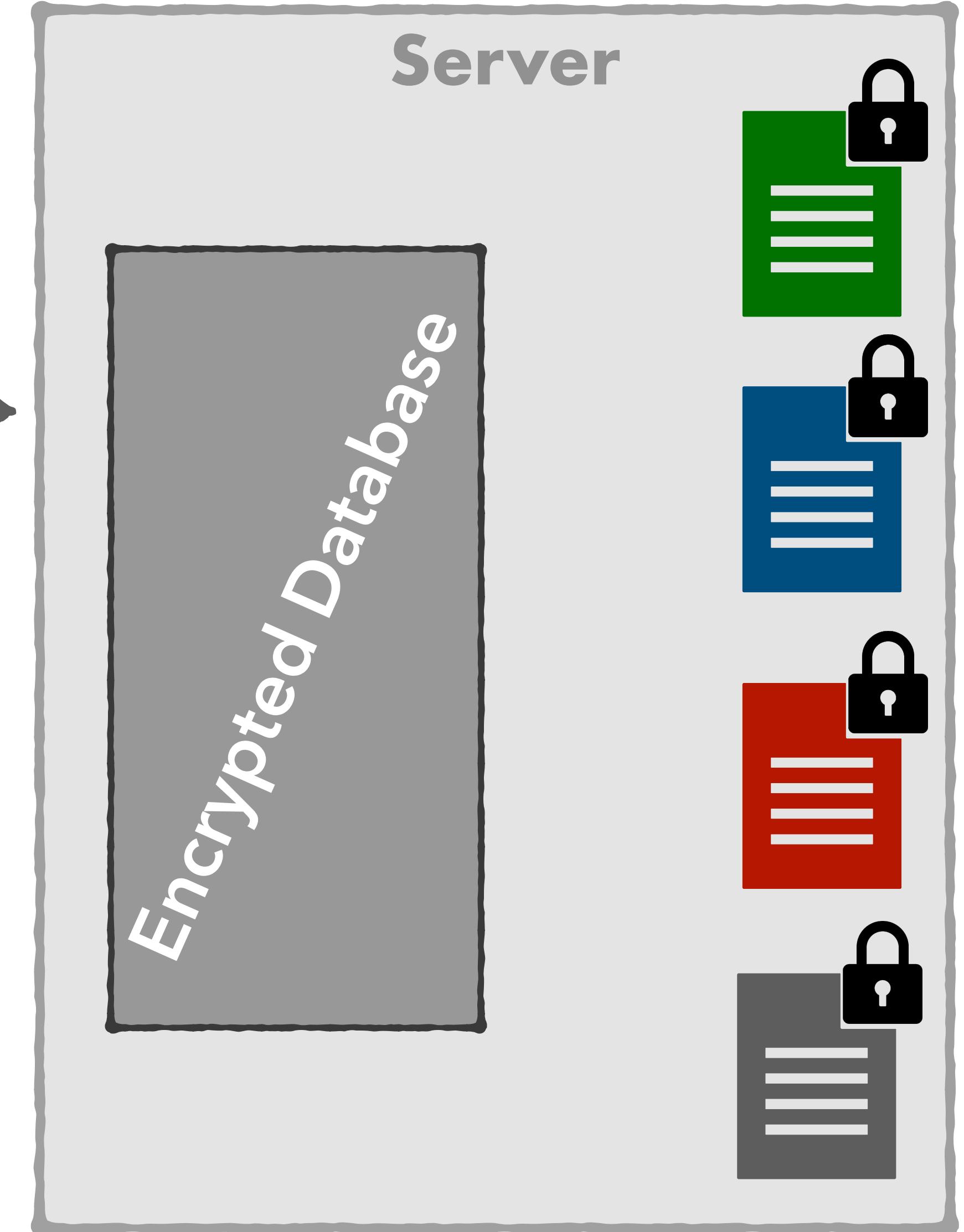
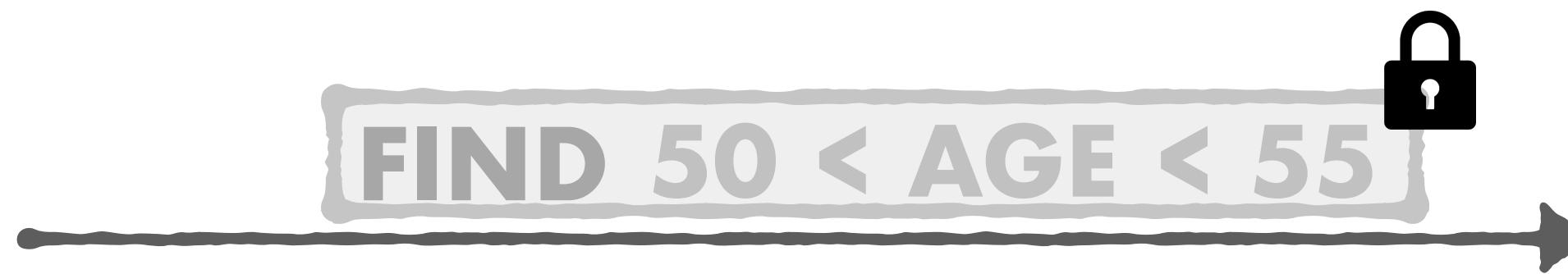
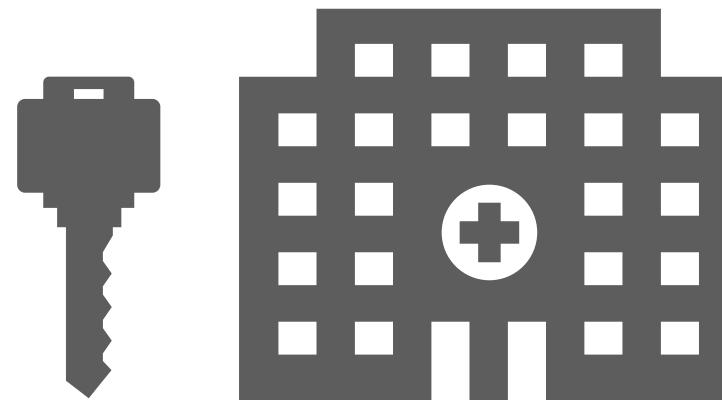




ATTACKING RESPONSE-HIDING DESIGNS

NO ACCESS-PATTERN LEAKAGE

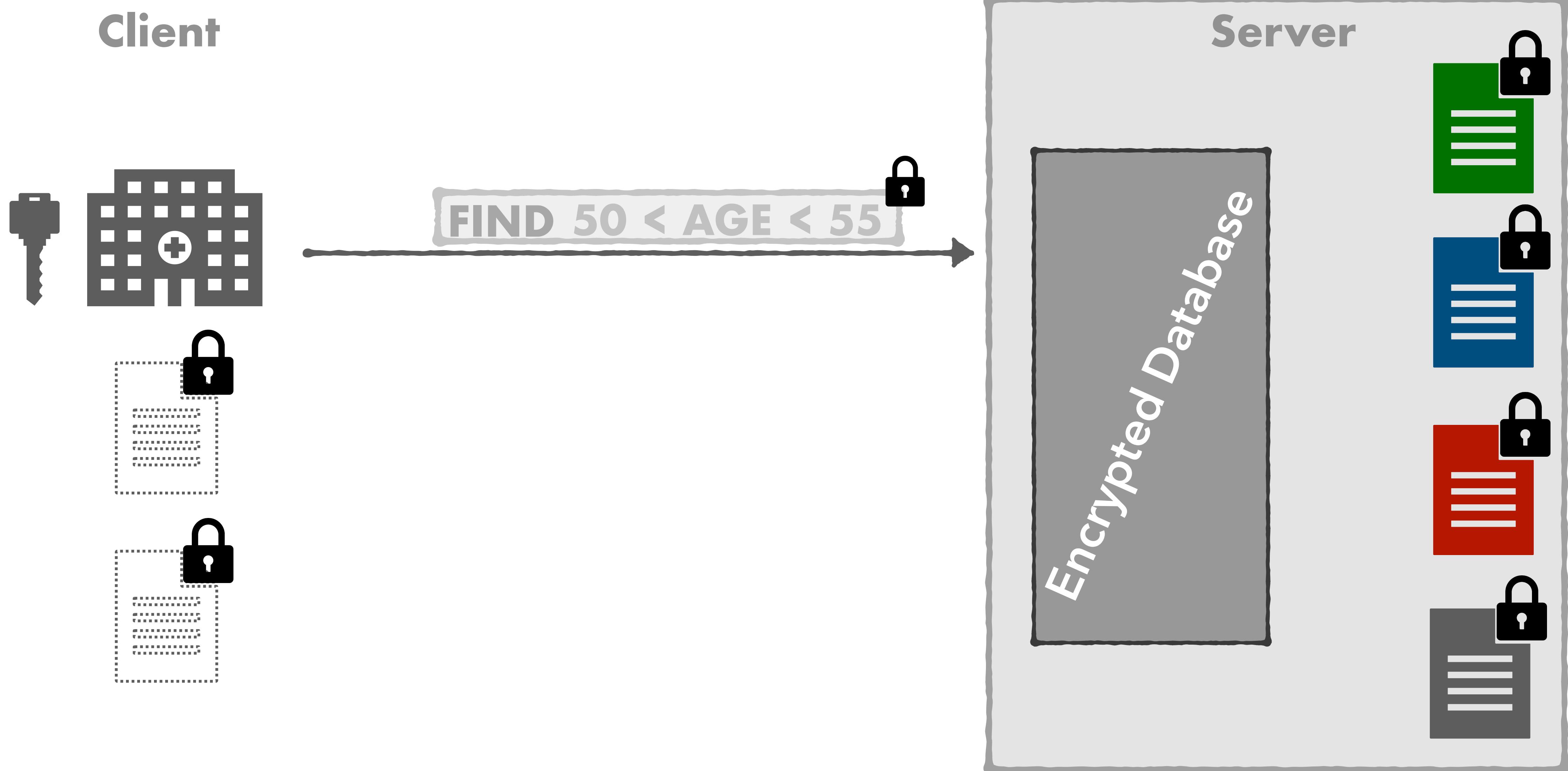
Client





ATTACKING RESPONSE-HIDING DESIGNS

NO ACCESS-PATTERN LEAKAGE



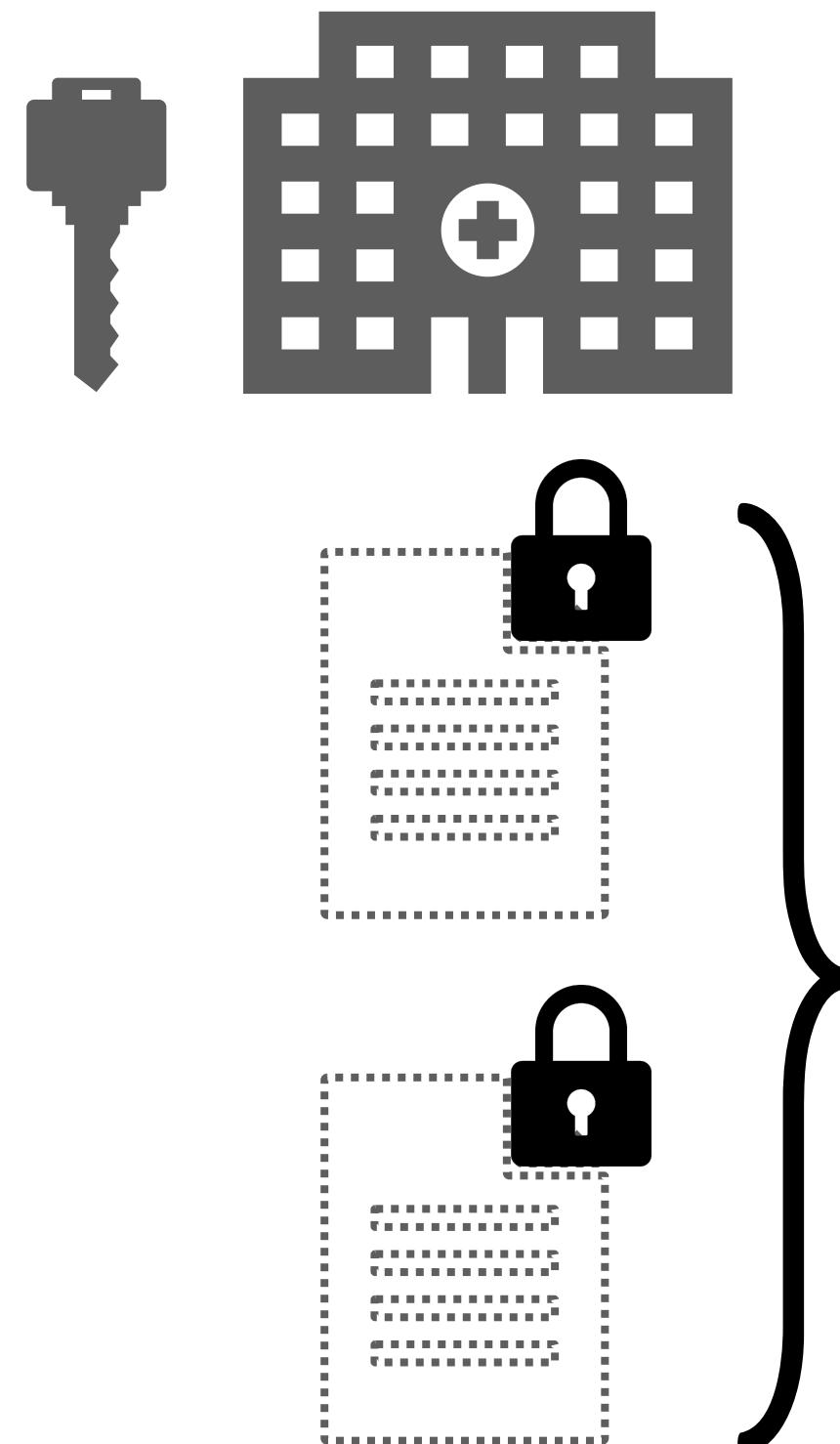


ATTACKING RESPONSE-HIDING DESIGNS

NO ACCESS-PATTERN LEAKAGE

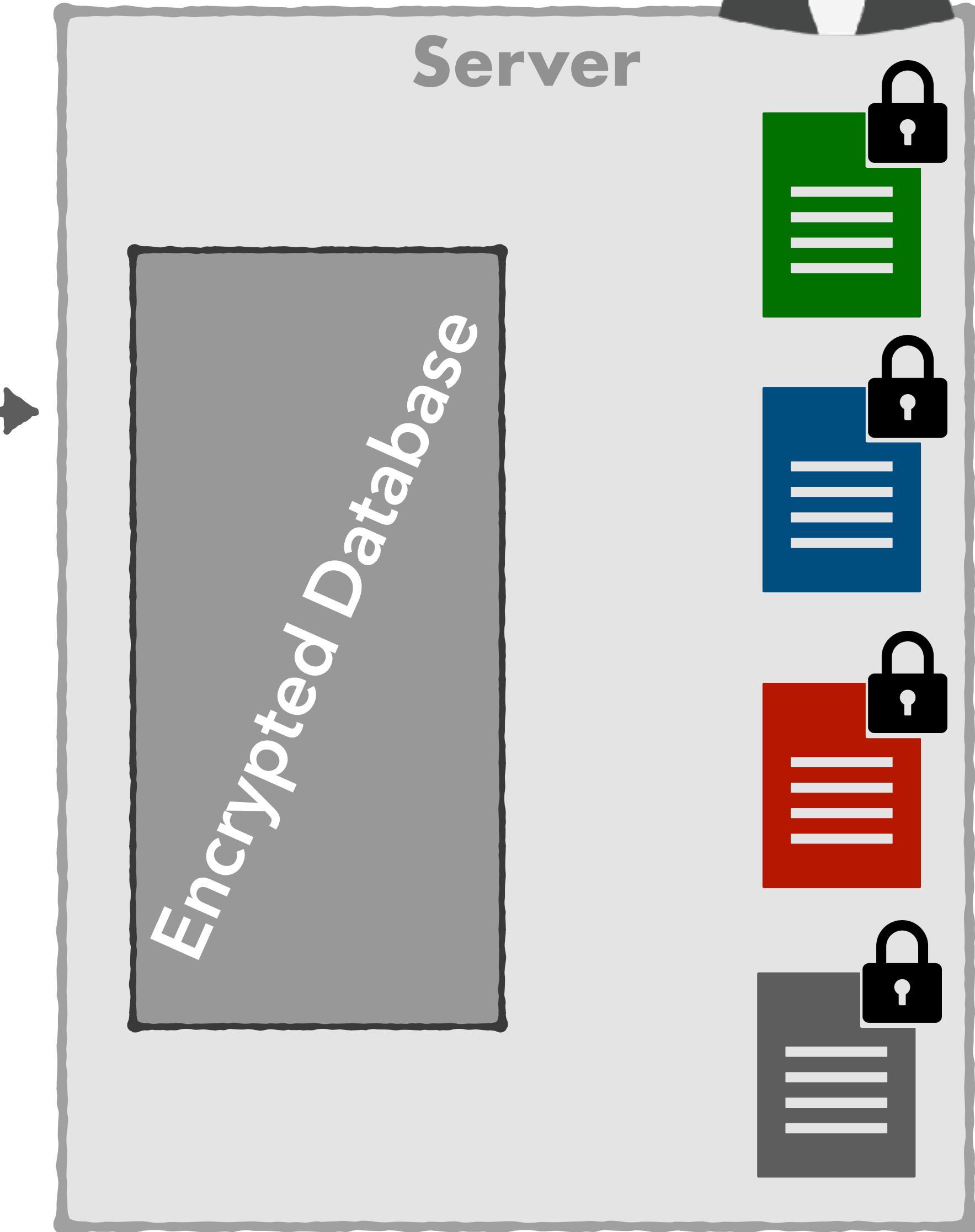


Client



Search-Pattern Leakage

FIND 50 < AGE < 55



Volume Leakage

IS THIS
LEAKAGE
ENOUGH TO MOUNT A
REALISTIC ATTACK?



CRYPTANALYSIS ON HARDENED RANGES RESPONSE-HIDING CONSTRUCTIONS ARE VULNERABLE TOO

Response-Hiding Encrypted Ranges: Revisiting Security via Parametrized Leakage-Abuse Attacks

Eugenios M. Kornaropoulos
UC Berkeley
eugenios@berkeley.edu

Charalampos Papamanthou
University of Maryland
csp@umd.edu

Roberto Tamassia
Brown University
rt@cs.brown.edu

Abstract—Despite a growing body of work on leakage-abuse attacks for encrypted databases, attacks on practical response-hiding constructions are yet to appear. Response-hiding constructions are superior in that they *nullify access-pattern based attacks* by returning only the search token and the result size of each query. Response-hiding schemes are vulnerable to existing volume attacks, which are, however, based on strong assumptions such as the uniformity query assumption or the dense database assumption. More crucially, these attacks only apply to schemes that cannot be deployed in practice (due to quadratic storage and increased leakage) when practical response-hiding schemes (Demertzis et al. [SIGMOD'16] and Falsi et al. [ESORICS'15]) have linear storage and less leakage. Due to these shortcomings, the value of existing volume attacks on response-hiding schemes is unclear.

In this work, we close the aforementioned gap by introducing a parametrized leakage-abuse attack that applies to *practical response-hiding structured encryption schemes*. The use of non-parametric estimation techniques makes our attack agnostic to both the data and the query distribution. At the very core of our technique lies the newly defined concept of a *counting function with respect to a range scheme*. We propose a two-phase framework to approximate the counting function for any range scheme. By simply switching our counting function for another, i.e., the smaller “parameter” of our modular attack, an adversary can attack different encrypted range schemes. We propose a constrained optimization formulation for the attack algorithm that is based on the counting functions. We demonstrate the effectiveness of our leakage-abuse attack on synthetic and real-world data under various scenarios.

INTRODUCTION

The notion of *searchable encryption*, introduced by Song-Wagner-Panigrahi in [37], proposes cryptographic schemes in which a client encrypts a privacy-sensitive data collection and outsources this resulting encrypted database to a server that efficiently answers search queries without ever decrypting the database. Since then, there has been a surge of research on this subject addressing issues such as improved definitions [9], dynamic constructions [23], [34], forward and backward privacy [4], [5], [7], [10], and locality of encrypted records [3], [11], [14]. For an overview of the area, see the survey by Fuller et al. [17]. In this work, we are interested in the general definitional framework called *Structured Encryption* (STE) introduced by Chase and Katzmaier [8] and, more specifically, schemes that support encrypted range queries [6], [13], [15].

To balance efficiency and privacy, STE schemes reveal some information about the query and its corresponding response. This information is called *leakage profile*. These schemes cryptographically guarantee that nothing more is revealed beyond what the designer allowed via the leakage profile.

RESPONSE-HIDING ENCRYPTED RANGES: REVISITING SECURITY VIA PARAMETRIZED LEAKAGE-ABUSE ATTACKS

KORNAROPOULOS, PAPAMANTHOU, TAMASSIA

Proc. IEEE SECURITY & PRIVACY , 2021

● RESTRICTED LEAKAGE: ONLY SEARCH-PATTERN & VOLUME

● NEW METHODOLOGY TO ATTACK PRACTICAL CONSTRUCTIONS

● AGNOSTIC TO QUERY DISTRIBUTION



STATE-OF-THE-ART CRYPTANALYSIS FOR RANGE CONSTRUCTIONS

Value Reconstruction Attack Algorithms	Applies to Response-Hiding Range Schemes	Applies to non-Quadratic Range Schemes	Assumptions			Exploited Leakage		
			Query Distribution	Dense Database	Known Data Distribution	Volume Leakage	Access-Pattern Leakage	Search-Pattern Leakage
KKNO [26] ACCESSPATTERNBASED	-	-	Uniform	-	-	-	●	-
LMP [30] FULLRECONSTRUCTION	-	-	Agnostic	●	-	-	●	-
GLMP [18] GENERALIZEDKKNO	-	-	Uniform	-	-	-	●	-
GLMP [18] AOR to ADR	-	-	Known	-	●	-	●	-
KPT [29] AGNOSTICRECONSTRUCTION	-	-	Agnostic	-	-	-	●	●
KKNO [26] VOLUMEBASED	●	-	Uniform	-	-	●	-	-
GLMP [20] GETELEMVOLUMES	●	-	Agnostic	●	-	●	-	-
GJW [21] EXTENDLEFTRIGHT	●	-	Agnostic	●	-	●	-	-
This Work	●	●	Agnostic	-	-	●	-	●



STATE-OF-THE-ART CRYPTANALYSIS FOR RANGE CONSTRUCTIONS

Value Reconstruction Attack Algorithms	Applies to Response-Hiding Range Schemes	Applies to non-Quadratic Range Schemes	Assumptions			Exploited Leakage		
			Query Distribution	Dense Database	Known Data Distribution	Volume Leakage	Access-Pattern Leakage	Search-Pattern Leakage
KKNO [26] ACCESSPATTERNBASED	-	-	Uniform	-	-	-	●	-
LMP [30] FULLRECONSTRUCTION	-	-	Agnostic	●	-	-	●	-
GLMP [18] GENERALIZEDKKNO	-	-	Uniform	-	-	-	●	-
GLMP [18] AOR to ADR	-	-	Known	-	●	-	●	-
KPT [29] AGNOSTICRECONSTRUCTION	-	-	Agnostic	-	-	-	●	●
KKNO [26] VOLUMEBASED	●	-	Uniform	-	-	●	-	-
GLMP [20] GETELEMVOLUMES	●	-	Agnostic	●	-	●	-	-
GJW [21] EXTENDLEFTRIGHT	●	-	Agnostic	●	-	●	-	-
This Work	●	●	Agnostic	-	-	●	-	●



STATE-OF-THE-ART CRYPTANALYSIS FOR RANGE CONSTRUCTIONS

Value Reconstruction Attack Algorithms	Applies to Response-Hiding Range Schemes	Applies to non-Quadratic Range Schemes	Assumptions			Exploited Leakage		
			Query Distribution	Dense Database	Known Data Distribution	Volume Leakage	Access-Pattern Leakage	Search-Pattern Leakage
KKNO [26] ACCESSPATTERNBASED	-	-	Uniform	-	-	-	●	-
LMP [30] FULLRECONSTRUCTION	-	-	Agnostic	●	-	-	●	-
GLMP [18] GENERALIZEDKKNO	-	-	Uniform	-	-	-	●	-
GLMP [18] AOR to ADR	-	-	Known	-	●	-	●	-
KPT [29] AGNOSTICRECONSTRUCTION	-	-	Agnostic	-	-	-	●	●
KKNO [26] VOLUMEBASED	●	-	Uniform	-	-	●	-	-
GLMP [20] GETELEMVOLUMES	●	-	Agnostic	●	-	●	-	-
GJW [21] EXTENDLEFTRIGHT	●	-	Agnostic	●	-	●	-	-
This Work	●	●	Agnostic	-	-	●	-	●



STATE-OF-THE-ART CRYPTANALYSIS FOR RANGE CONSTRUCTIONS

Value Reconstruction Attack Algorithms	Applies to Response-Hiding Range Schemes	Applies to non-Quadratic Range Schemes	Assumptions			Exploited Leakage		
			Query Distribution	Dense Database	Known Data Distribution	Volume Leakage	Access-Pattern Leakage	Search-Pattern Leakage
KKNO [26] ACCESSPATTERNBASED	-	-	Uniform	-	-	-	●	-
LMP [30] FULLRECONSTRUCTION	-	-	Agnostic	●	-	-	●	-
GLMP [18] GENERALIZEDKKNO	-	-	Uniform	-	-	-	●	-
GLMP [18] AOR to ADR	-	-	Known	-	●	-	●	-
KPT [29] AGNOSTICRECONSTRUCTION	-	-	Agnostic	-	-	-	●	●
KKNO [26] VOLUMEBASED	●	-	Uniform	-	-	●	-	-
GLMP [20] GETELEMVOLUMES	●	-	Agnostic	●	-	●	-	-
GJW [21] EXTENDLEFTRIGHT	●	-	Agnostic	●	-	●	-	-
This Work	●	●	Agnostic	-	-	●	-	●



IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

Range: [1,8]





IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

Range: [1,8]





IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

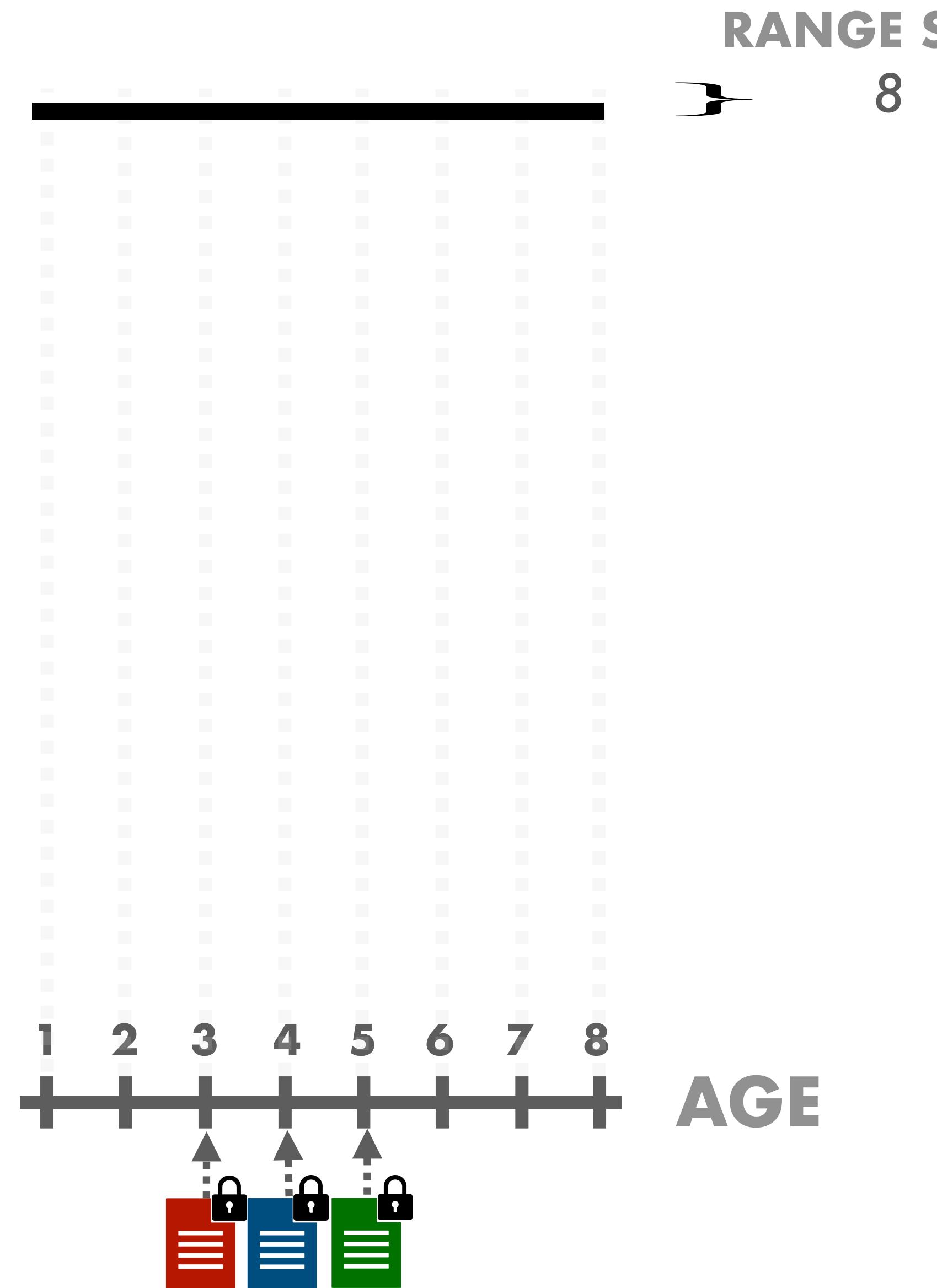
RANGE SPAN





IS THIS LEAKAGE ENOUGH TO ATTACK?

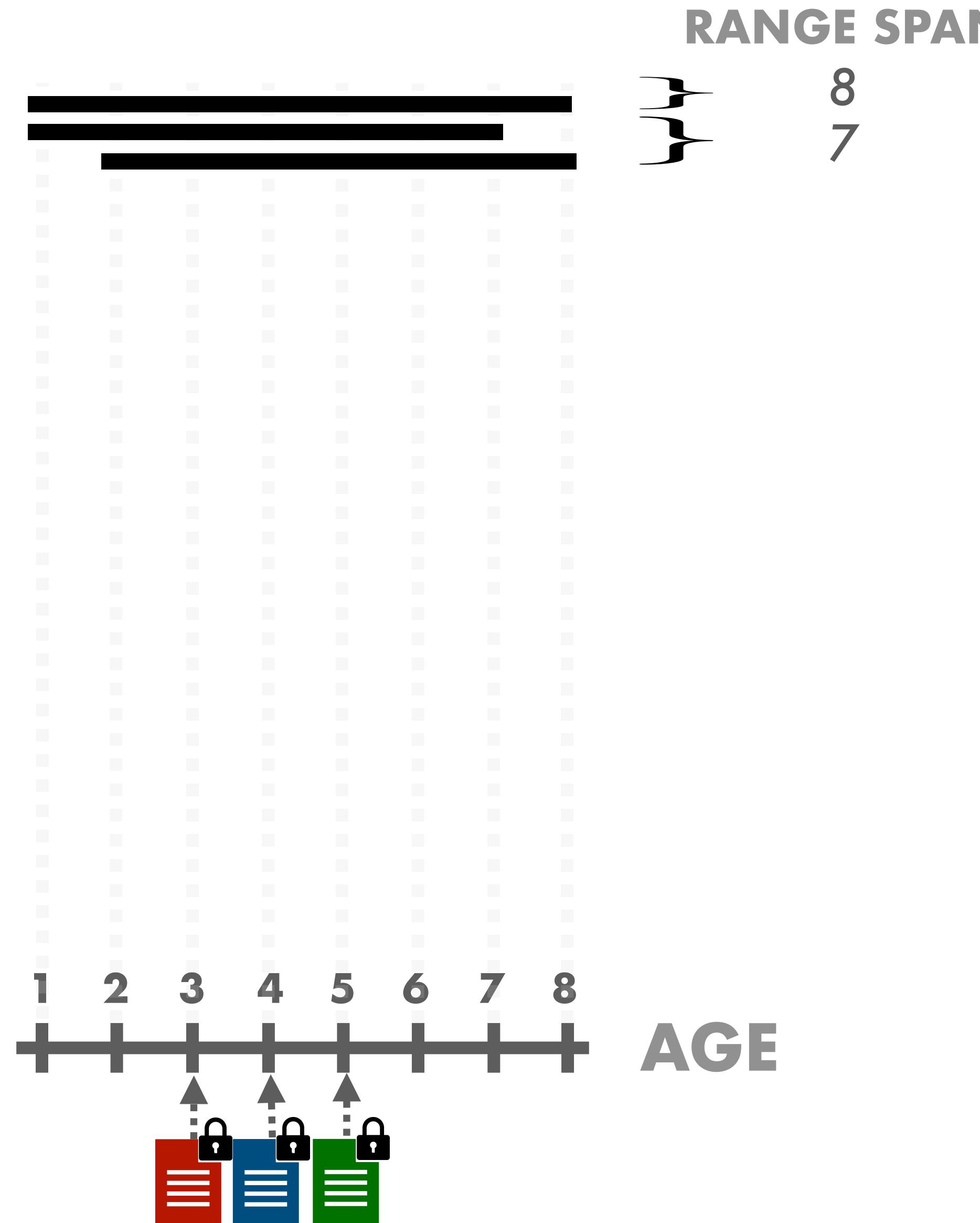
ANSWER: VOLUMES REVEAL GEOMETRY





IS THIS LEAKAGE ENOUGH TO ATTACK?

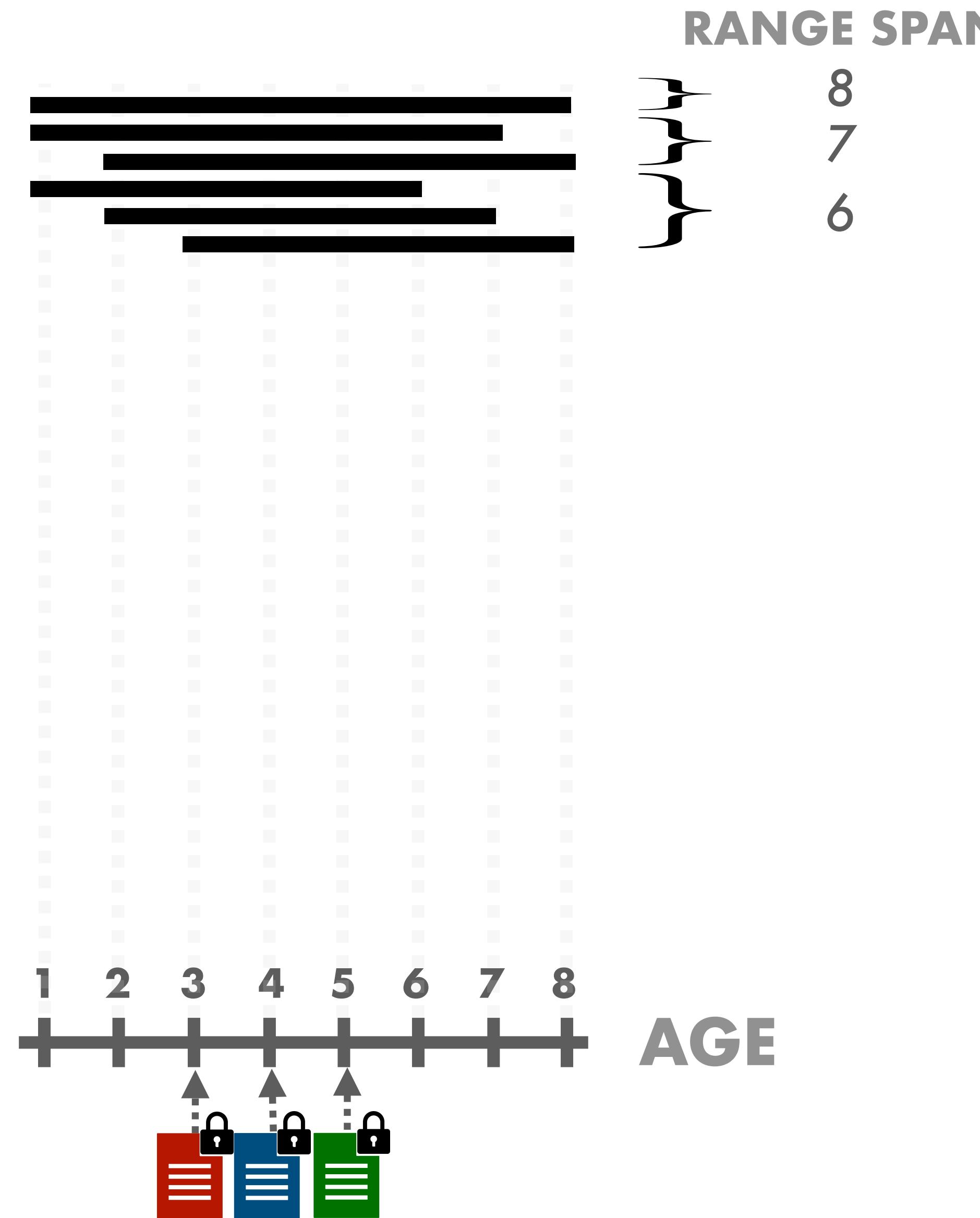
ANSWER: VOLUMES REVEAL GEOMETRY





IS THIS LEAKAGE ENOUGH TO ATTACK?

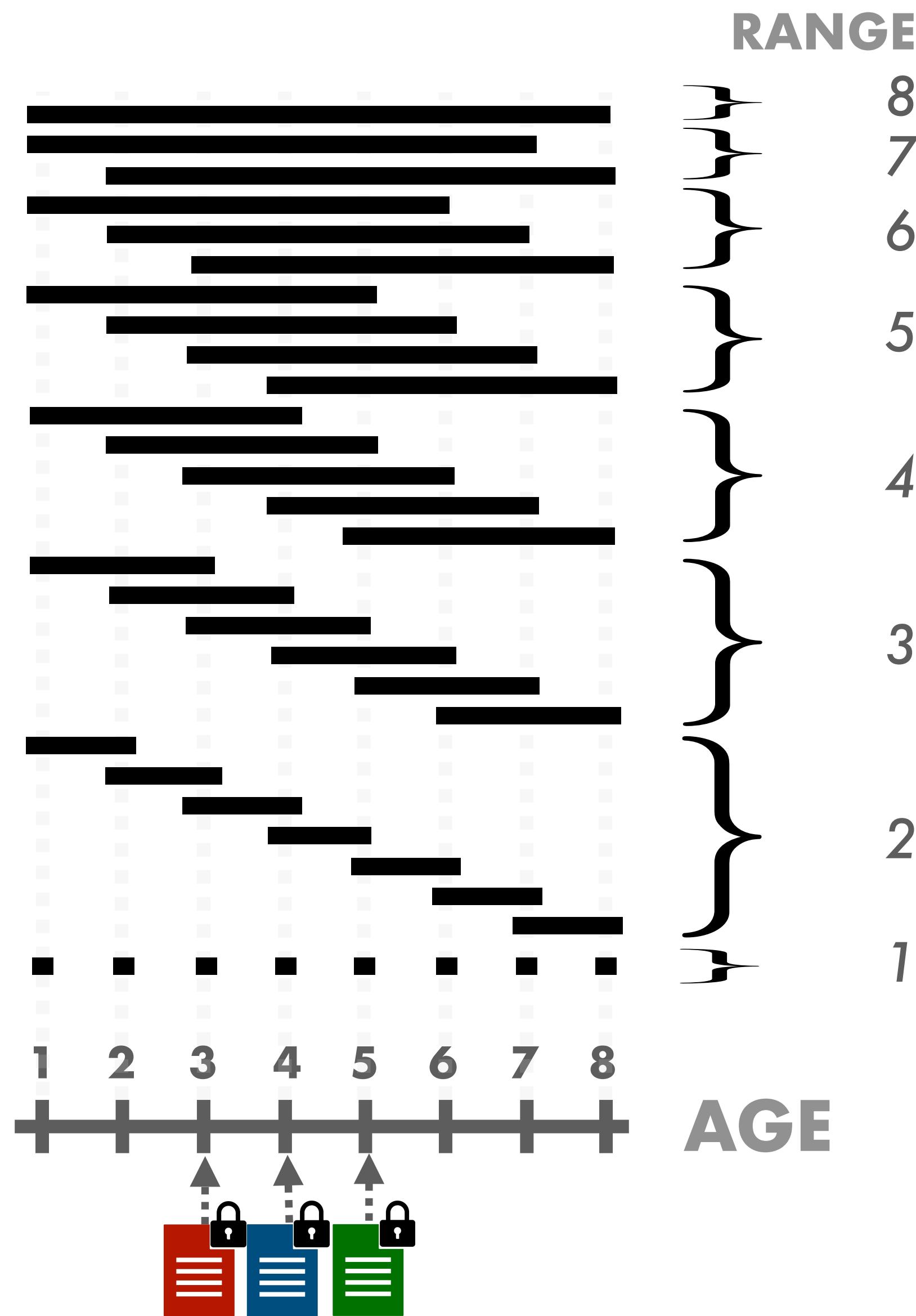
ANSWER: VOLUMES REVEAL GEOMETRY





IS THIS LEAKAGE ENOUGH TO ATTACK?

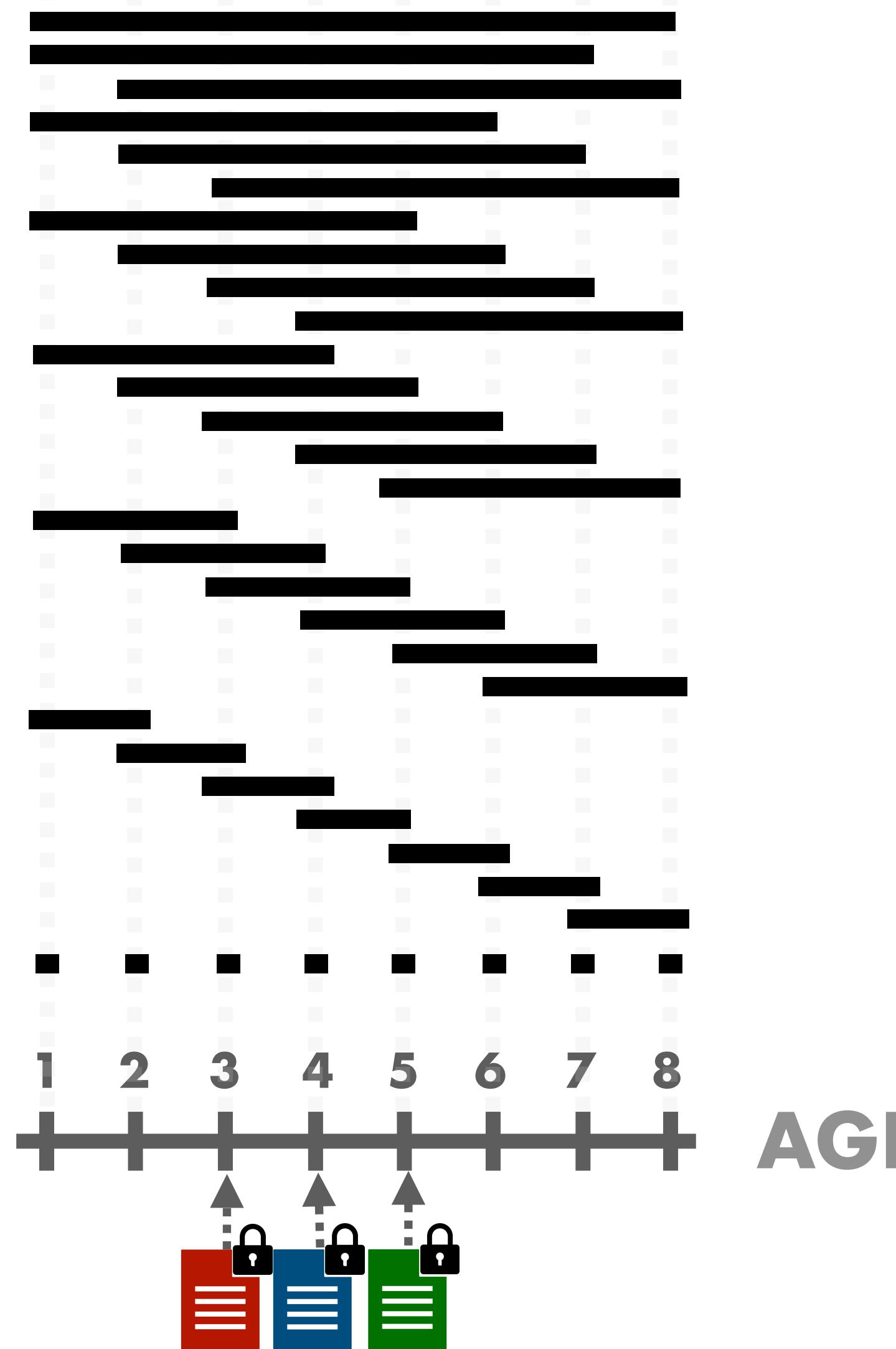
ANSWER: VOLUMES REVEAL GEOMETRY



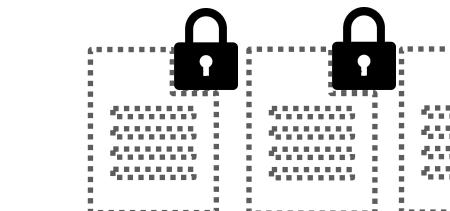


IS THIS LEAKAGE ENOUGH TO ATTACK?

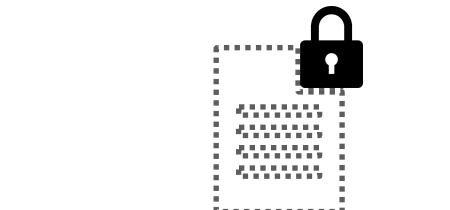
ANSWER: VOLUMES REVEAL GEOMETRY



VOLUME



COUNTER

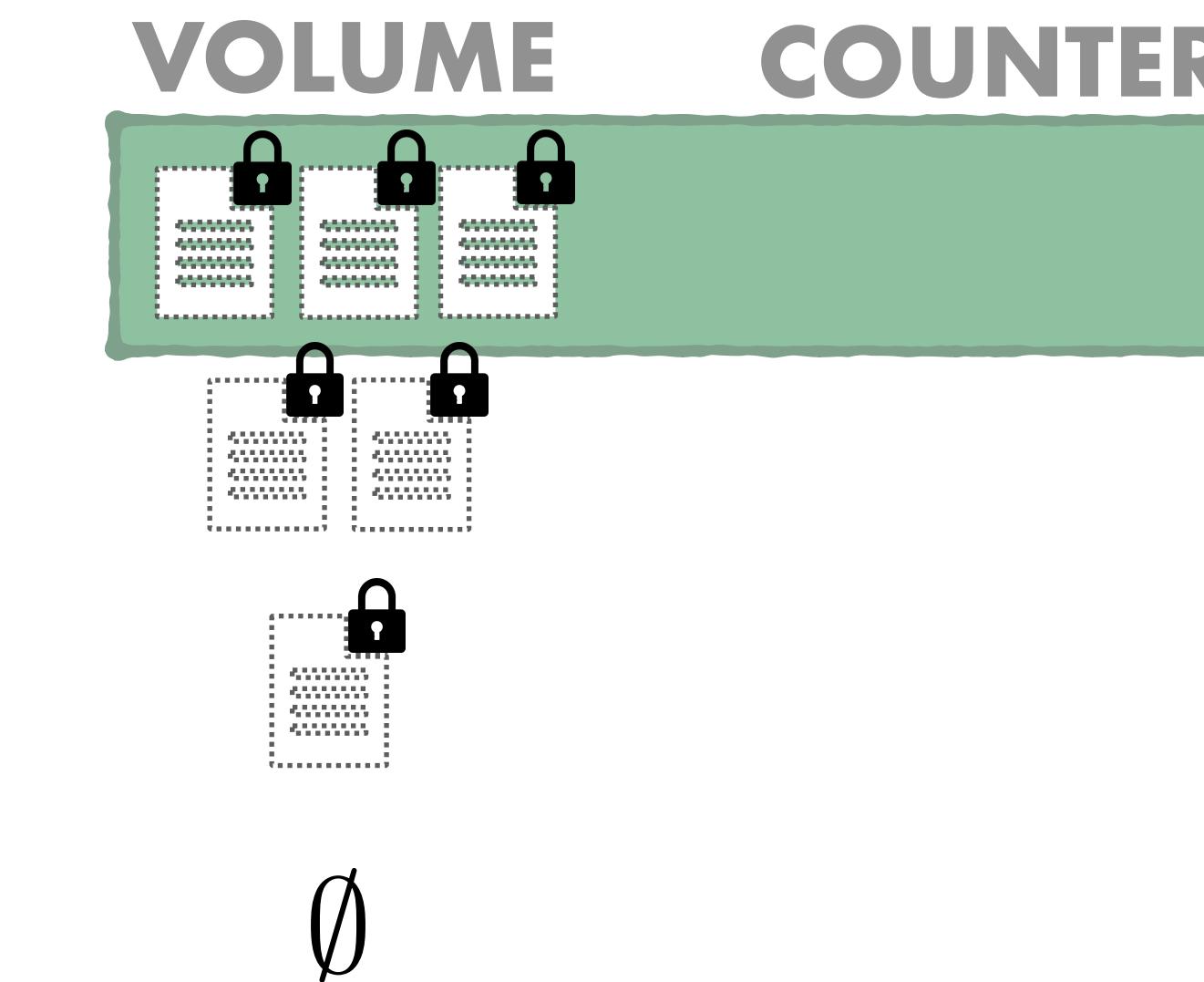
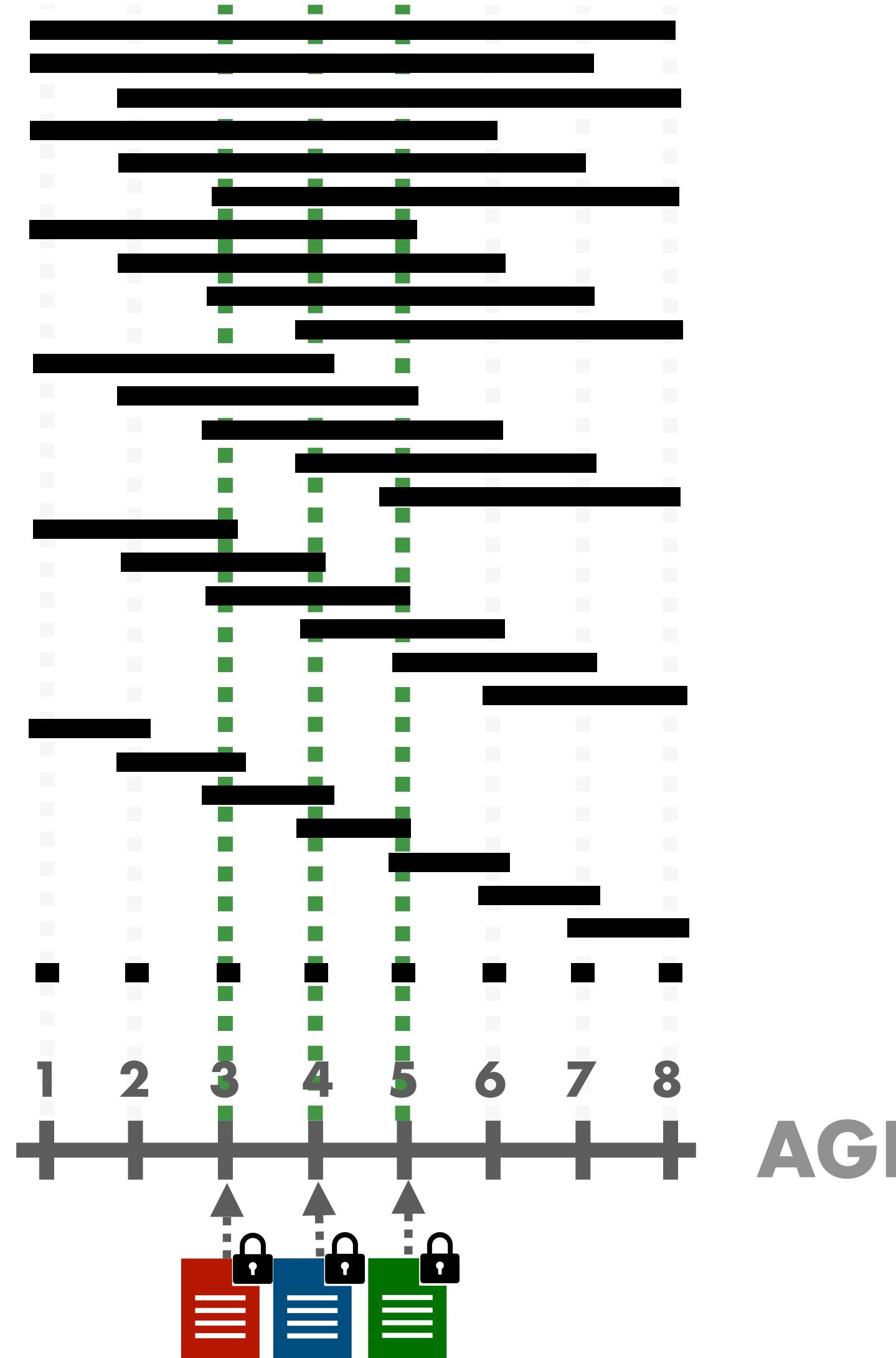


∅



IS THIS LEAKAGE ENOUGH TO ATTACK?

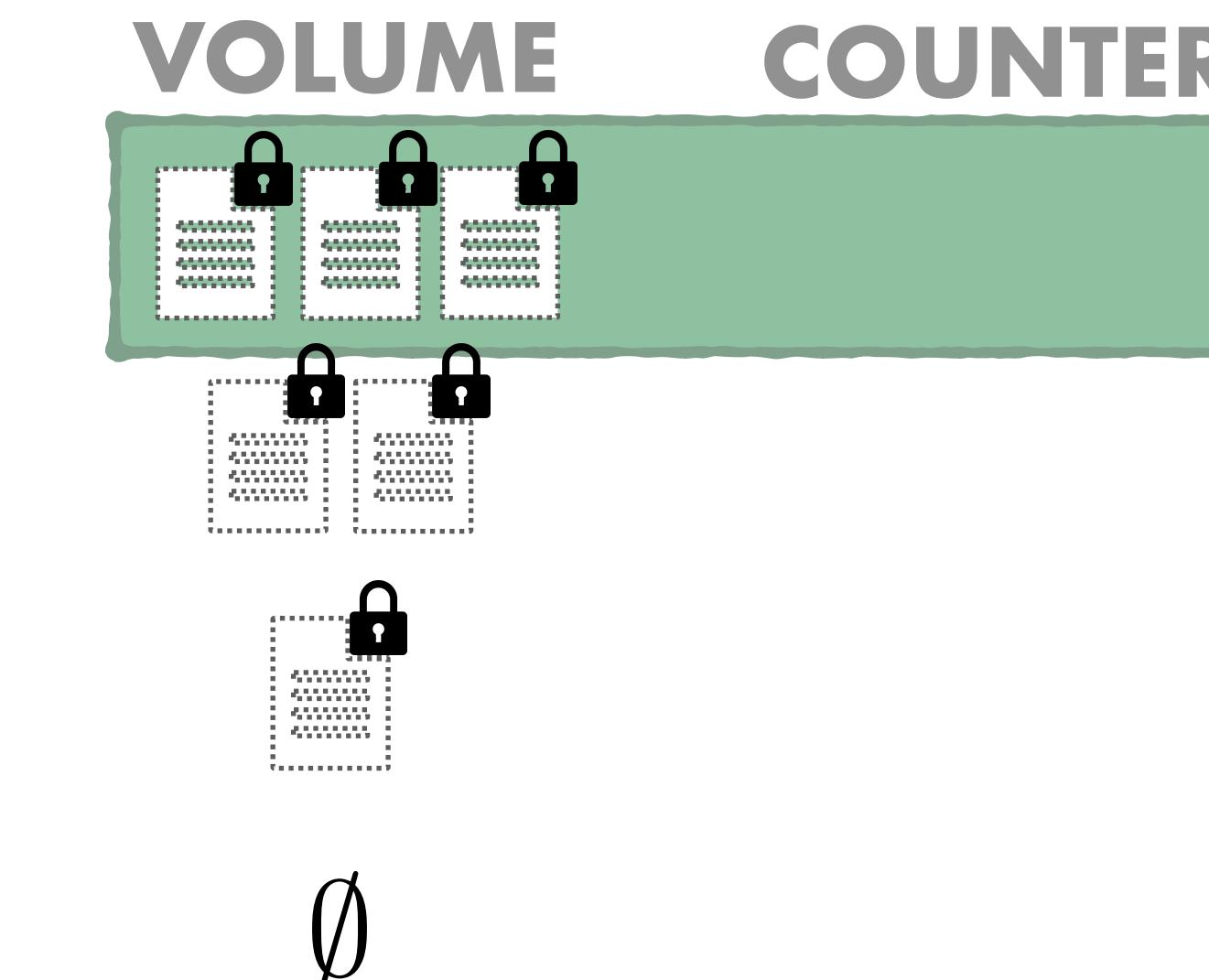
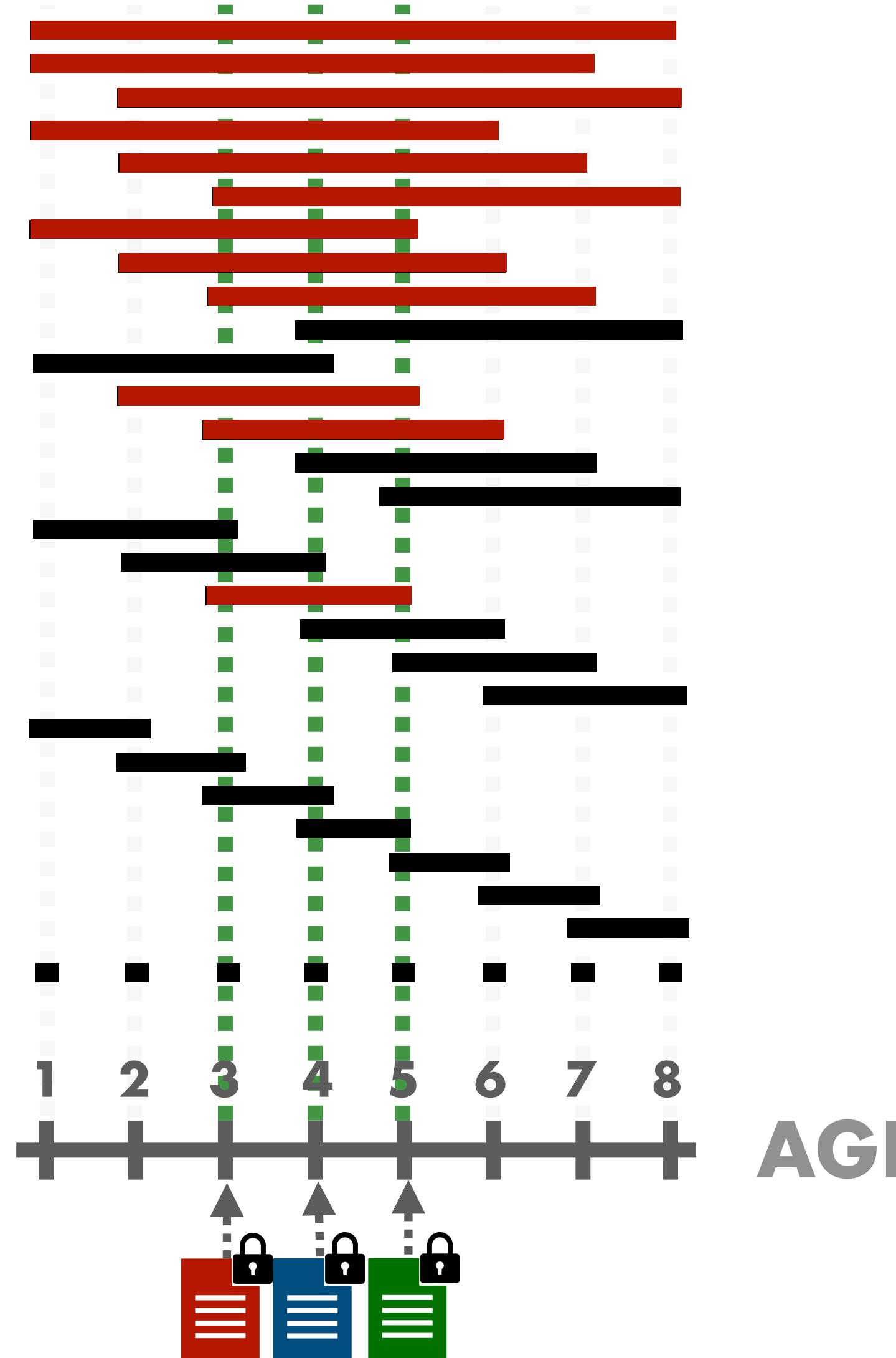
ANSWER: VOLUMES REVEAL GEOMETRY





IS THIS LEAKAGE ENOUGH TO ATTACK?

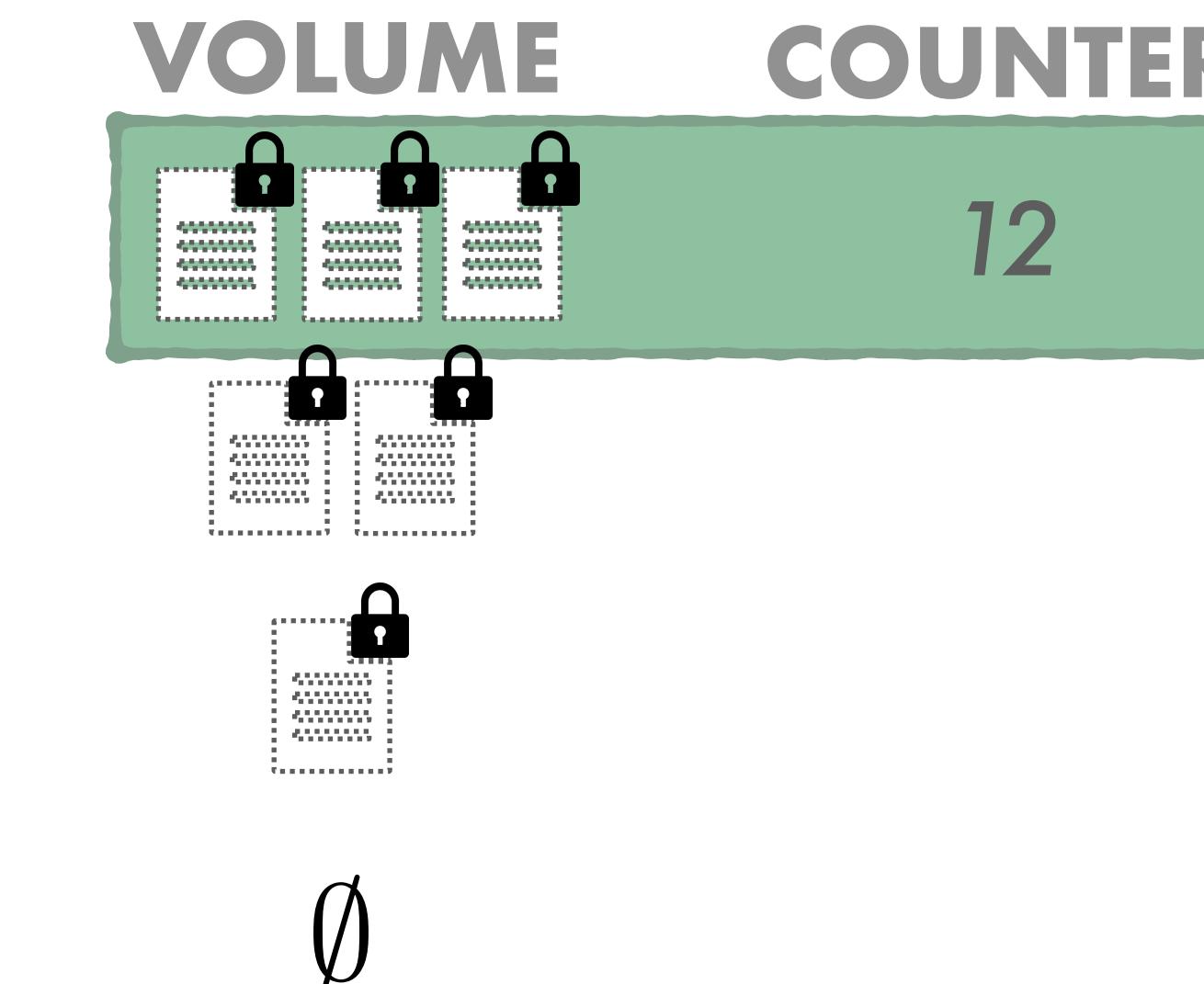
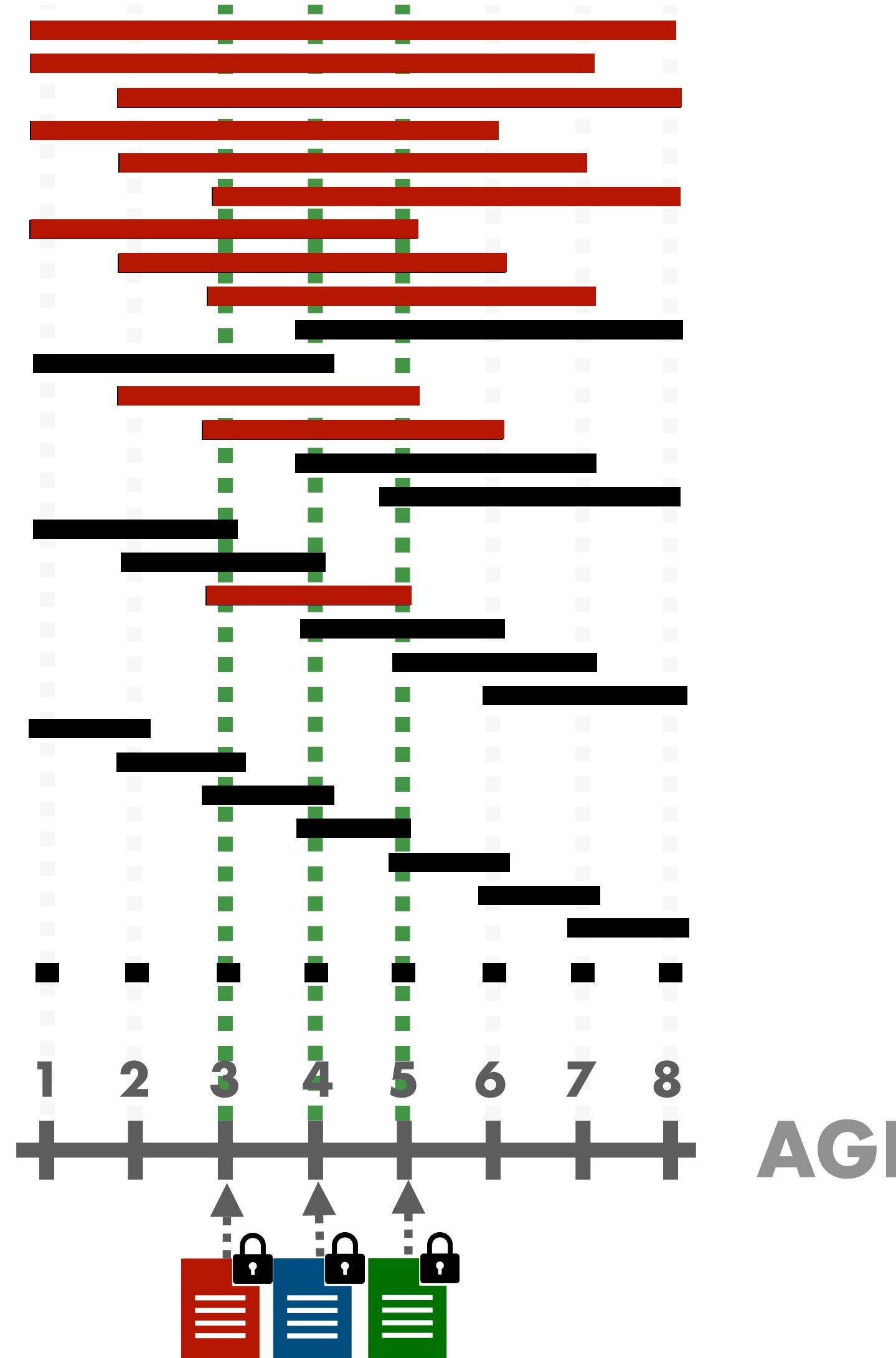
ANSWER: VOLUMES REVEAL GEOMETRY





IS THIS LEAKAGE ENOUGH TO ATTACK?

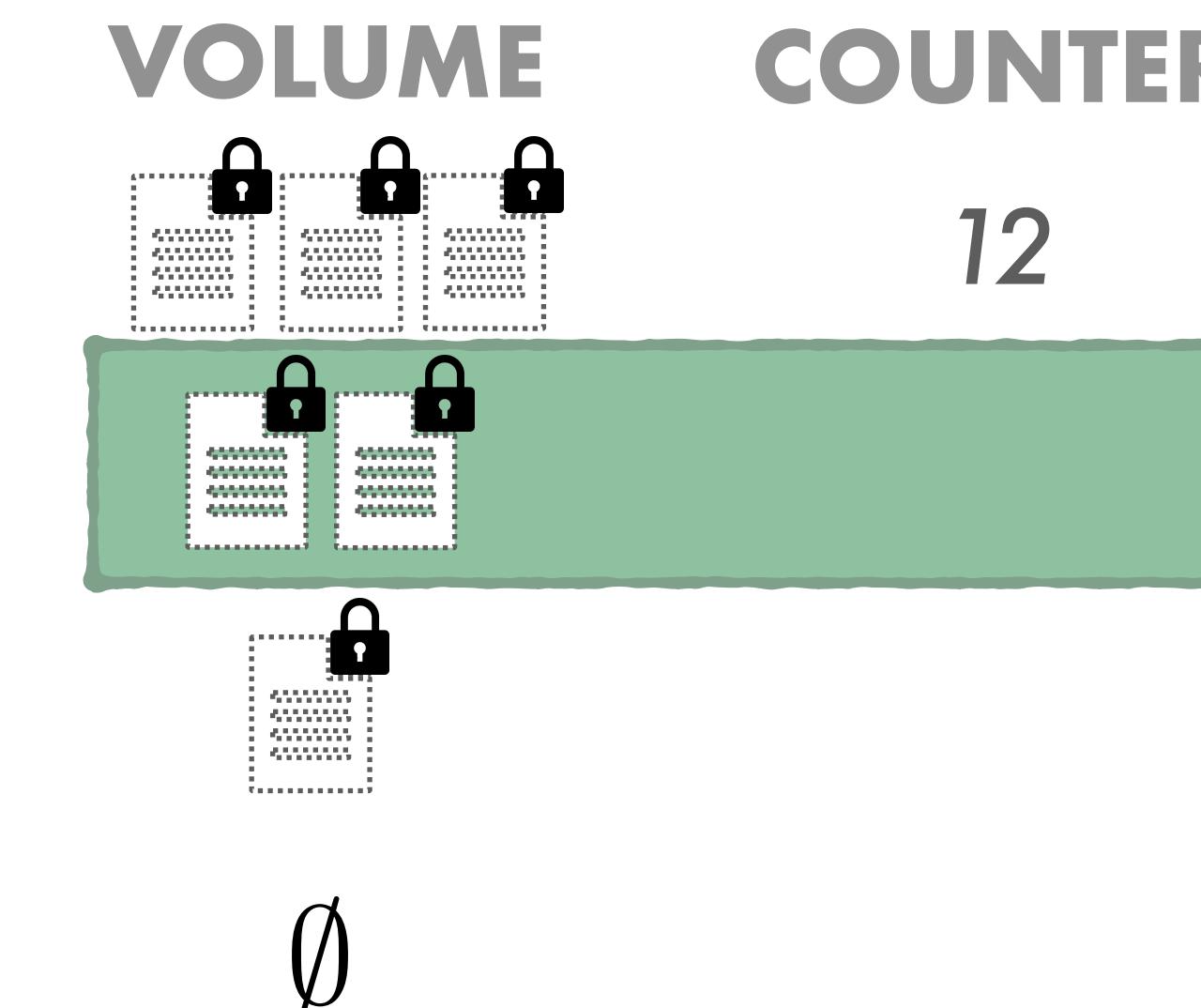
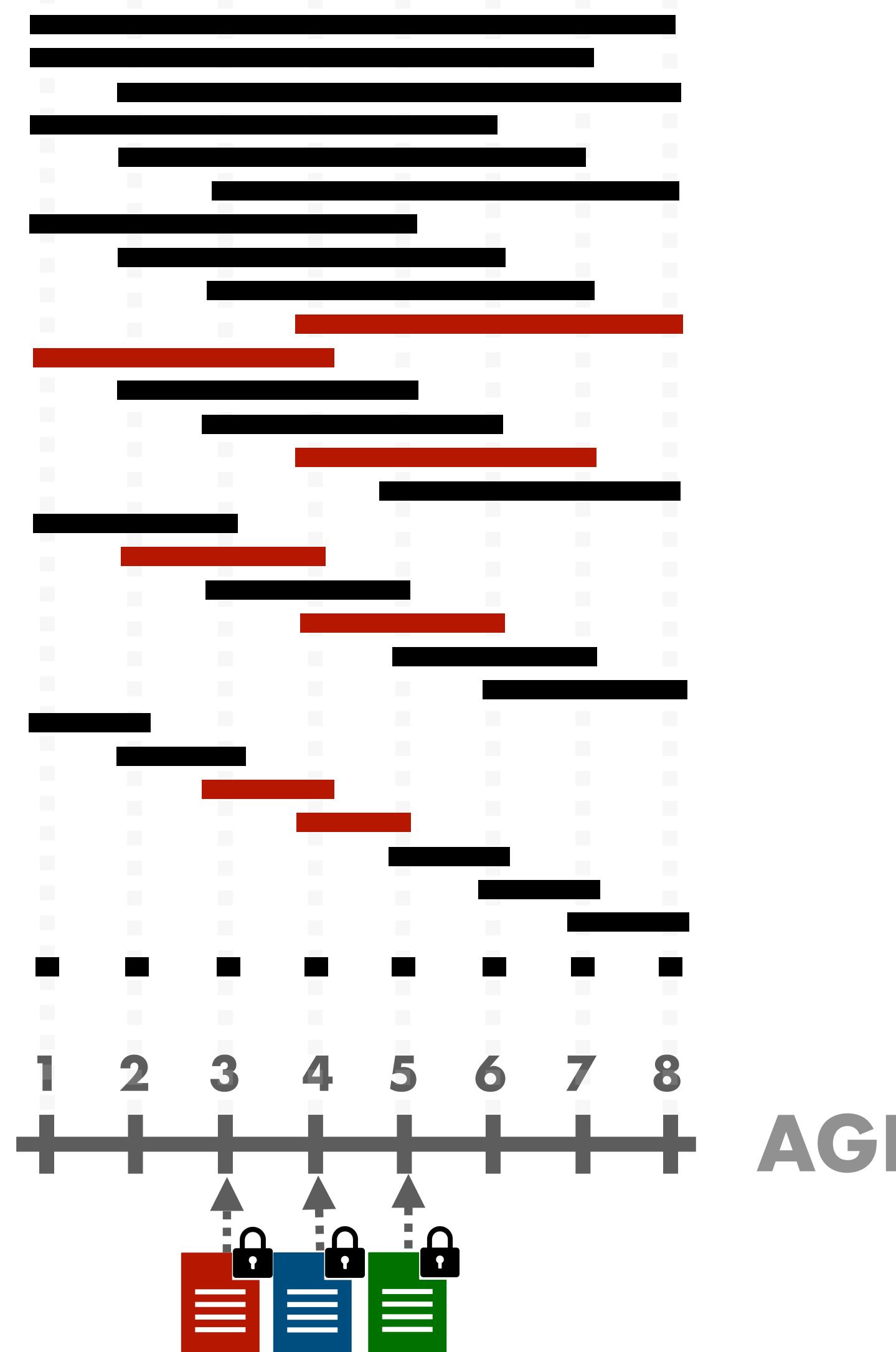
ANSWER: VOLUMES REVEAL GEOMETRY





IS THIS LEAKAGE ENOUGH TO ATTACK?

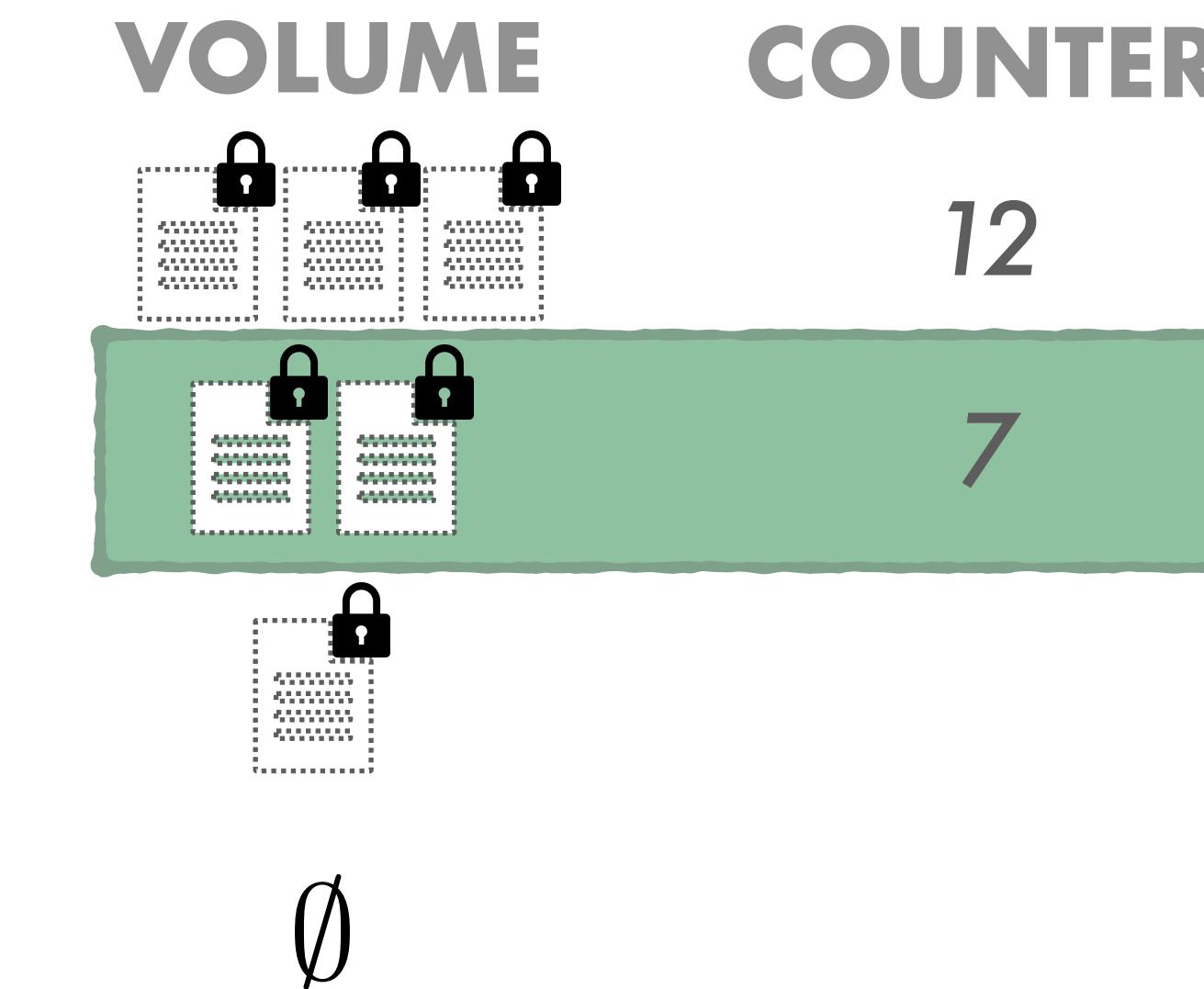
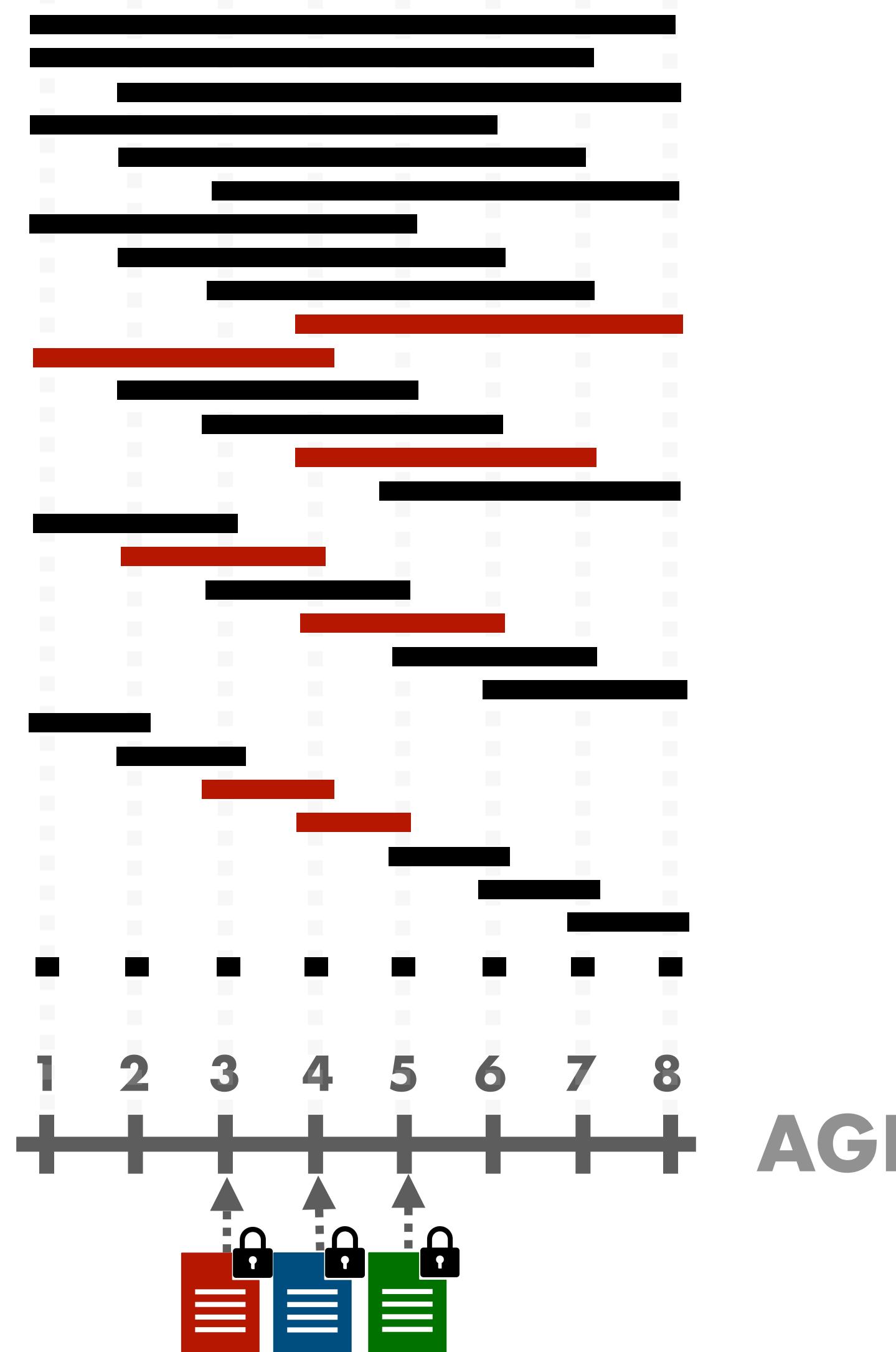
ANSWER: VOLUMES REVEAL GEOMETRY





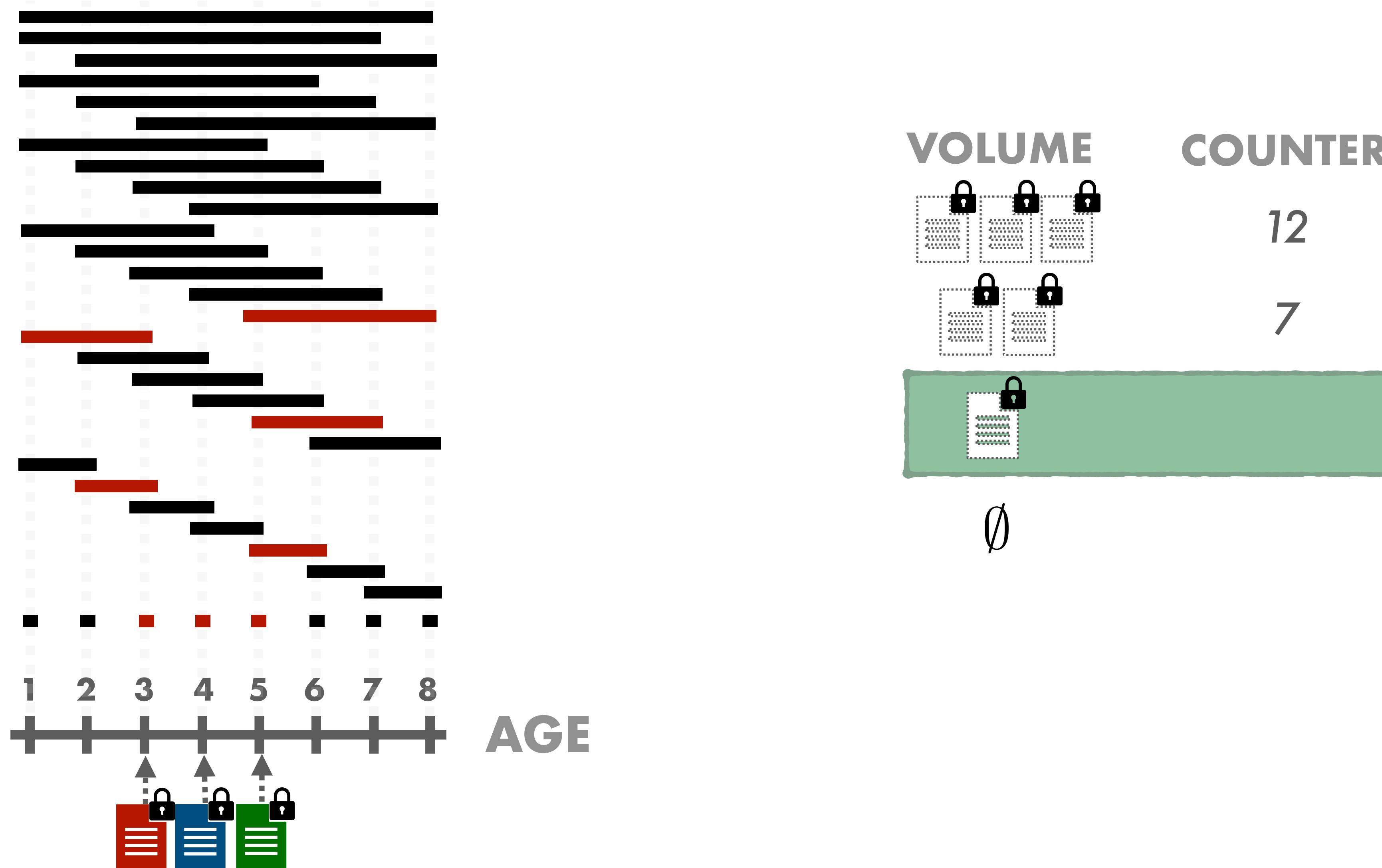
IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY





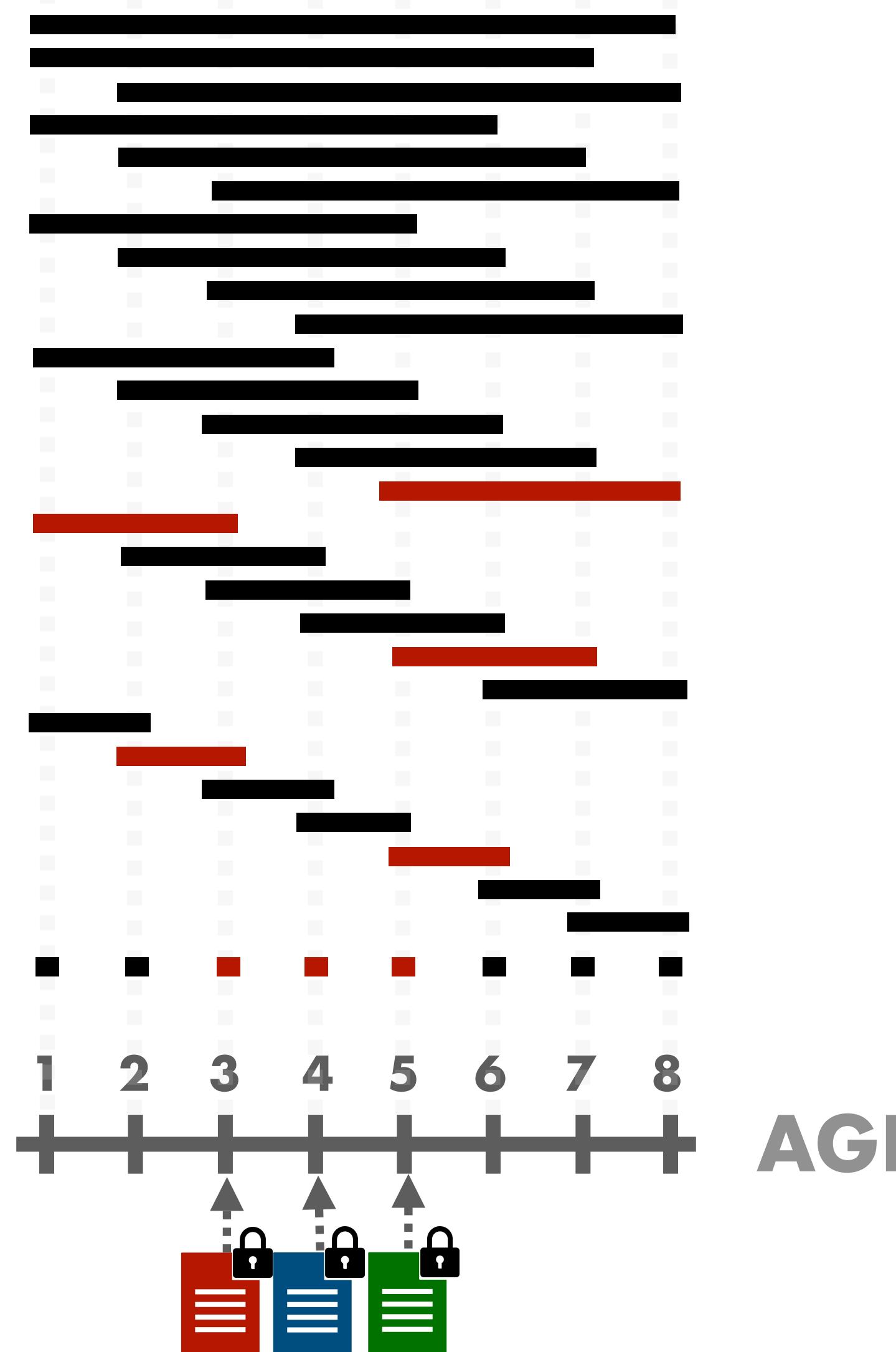
IS THIS LEAKAGE ENOUGH TO ATTACK? ANSWER: VOLUMES REVEAL GEOMETRY





IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY



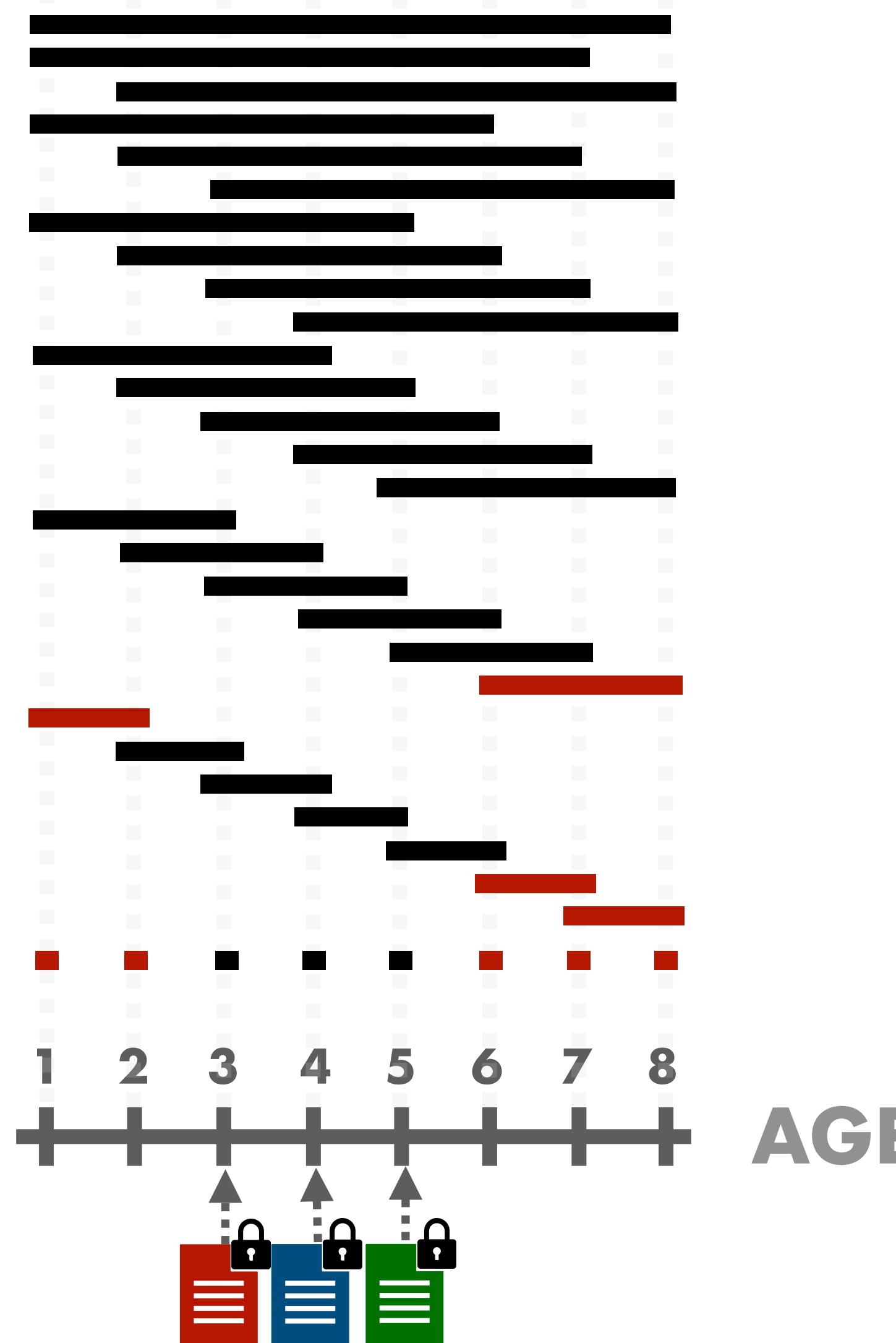
VOLUME	COUNTER
	12
	7
	8

∅



IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

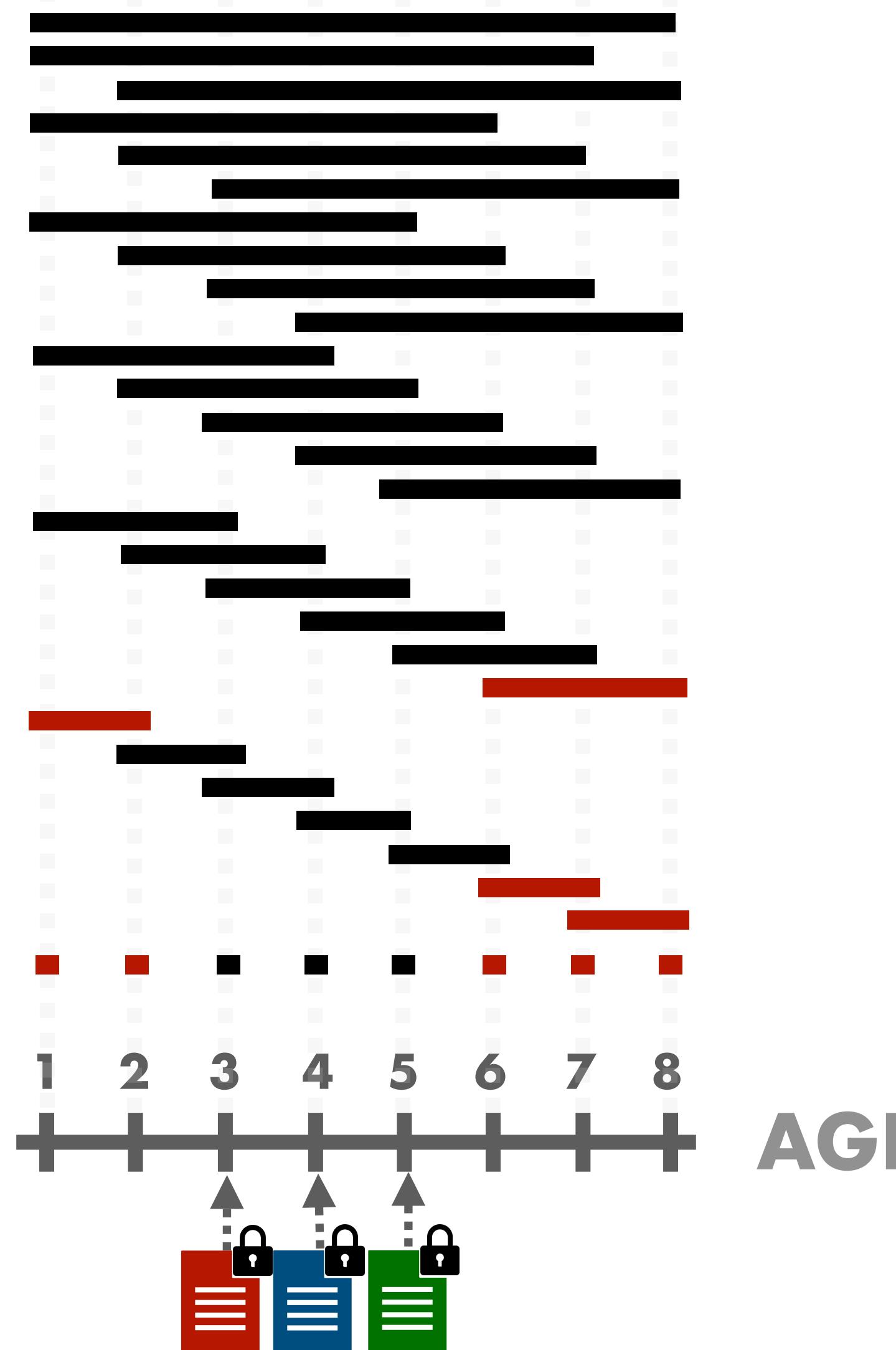


VOLUME	COUNTER
	12
	7
	8



IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

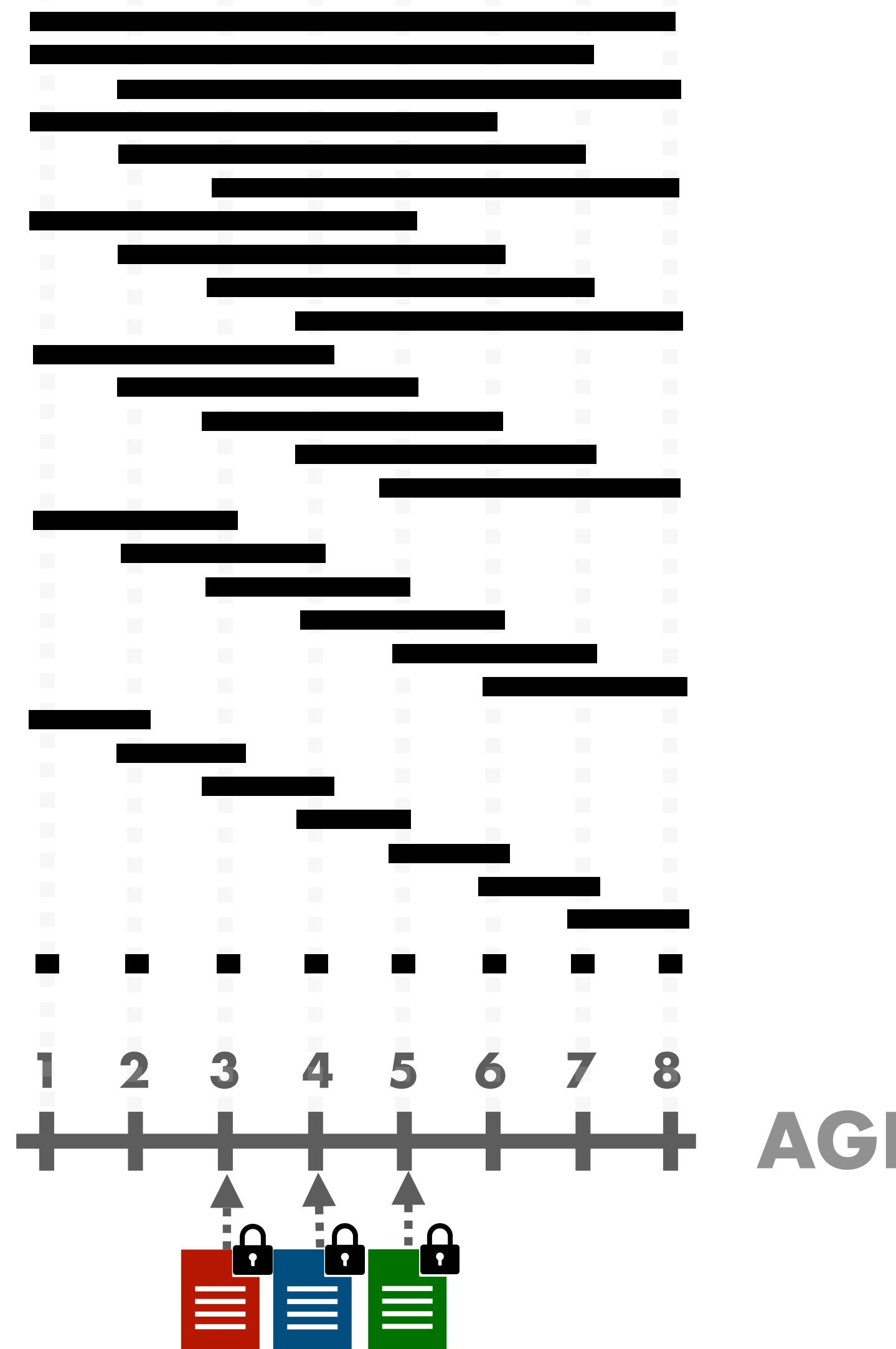


VOLUME	COUNTER
	12
	7
	8
	9

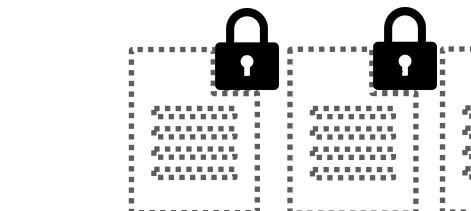


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY



VOLUME



COUNTER

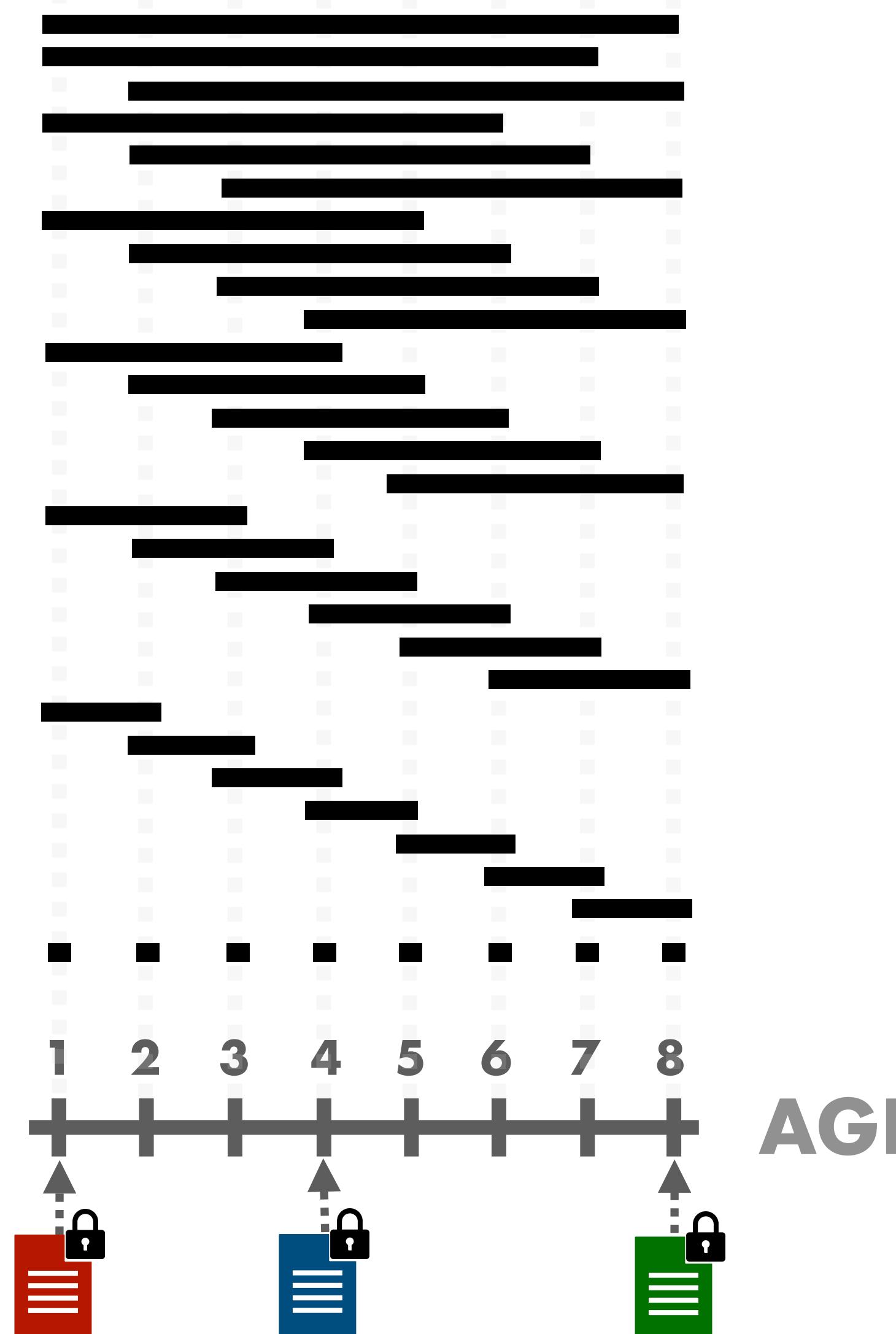
∅



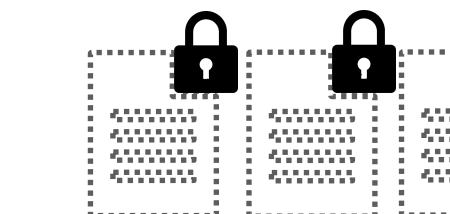


IS THIS LEAKAGE ENOUGH TO ATTACK?

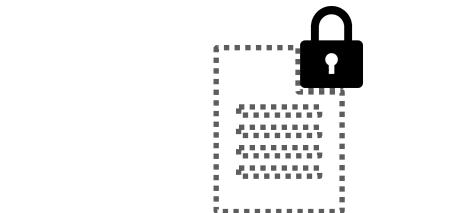
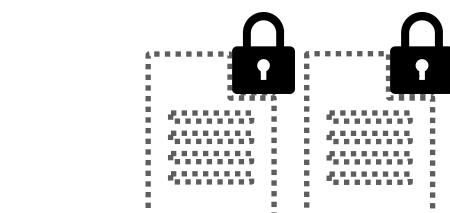
ANSWER: VOLUMES REVEAL GEOMETRY



VOLUME



COUNTER



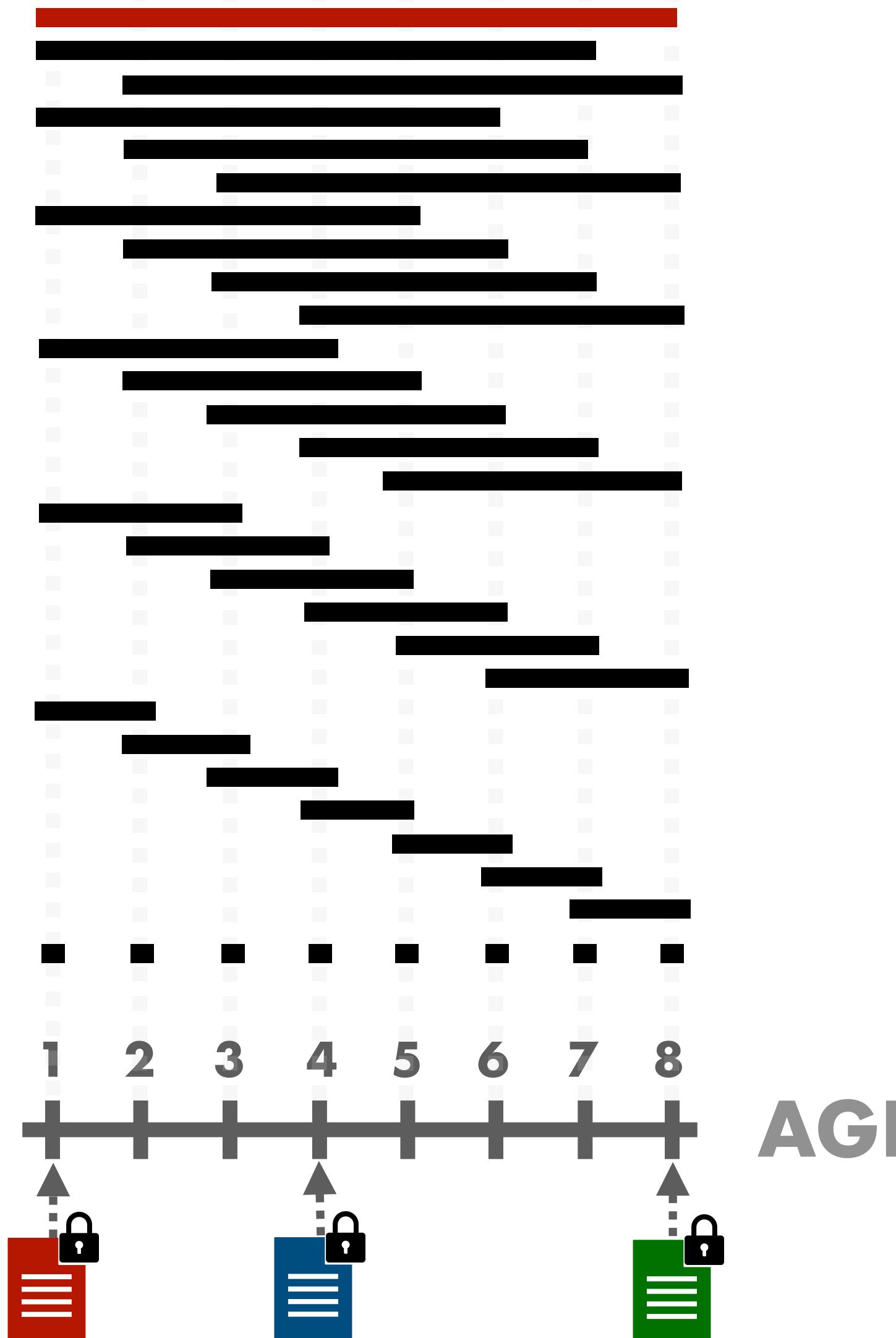
∅



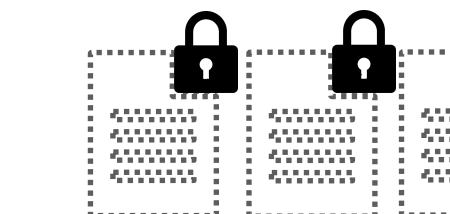


IS THIS LEAKAGE ENOUGH TO ATTACK?

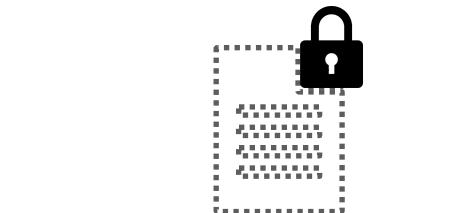
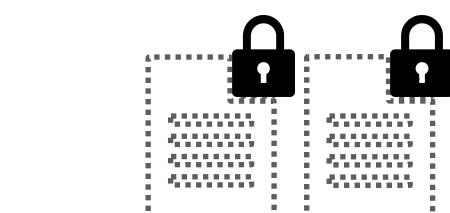
ANSWER: VOLUMES REVEAL GEOMETRY



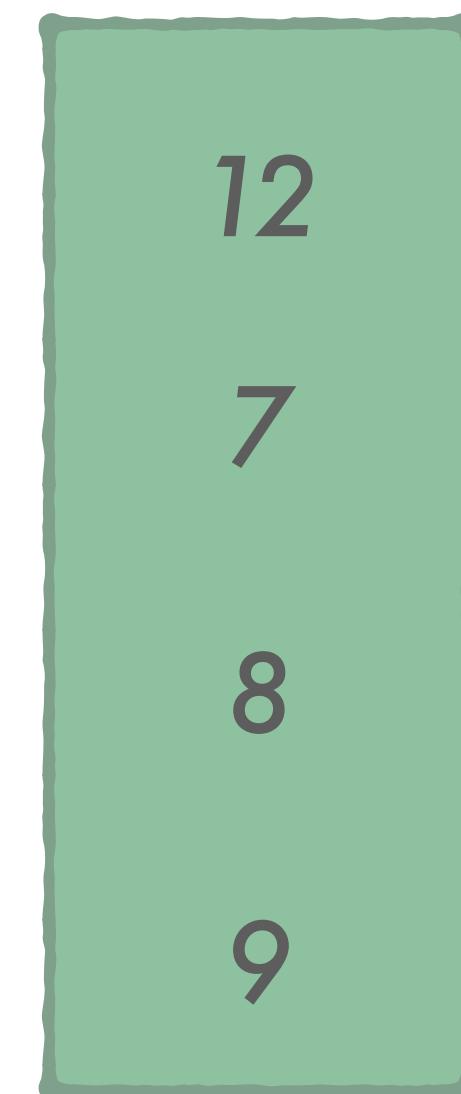
VOLUME



COUNTER



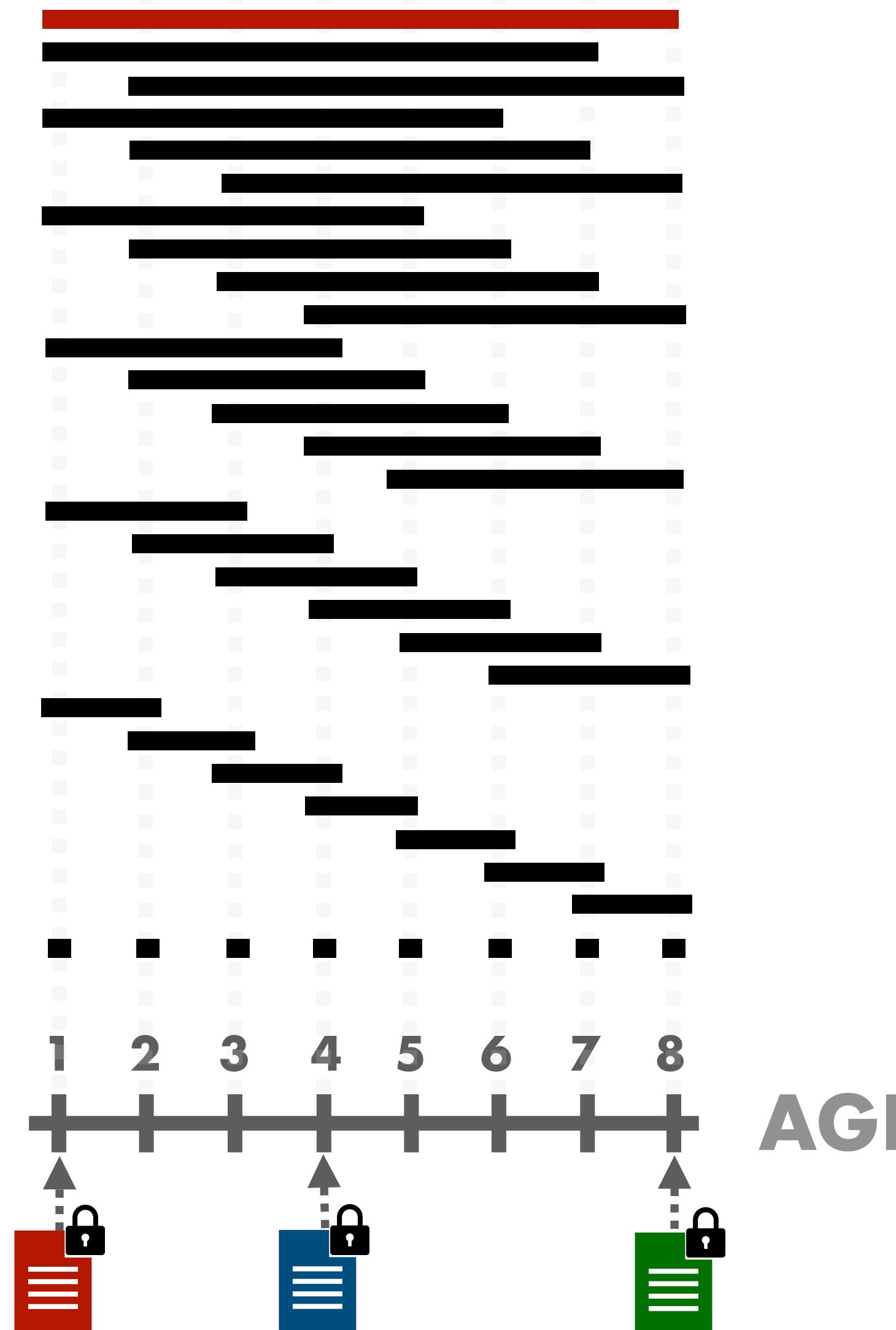
∅



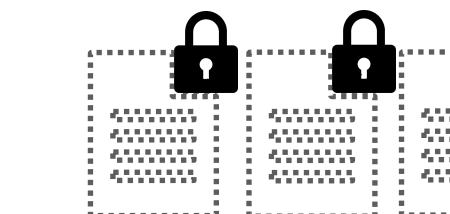


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

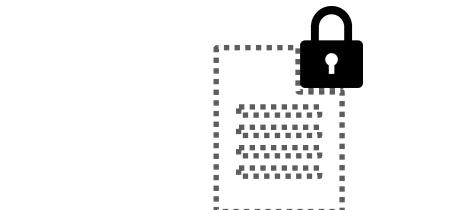
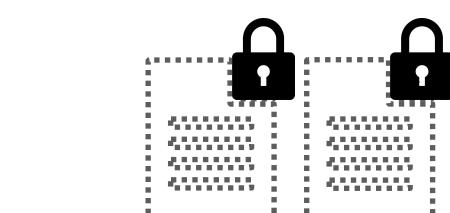


VOLUME

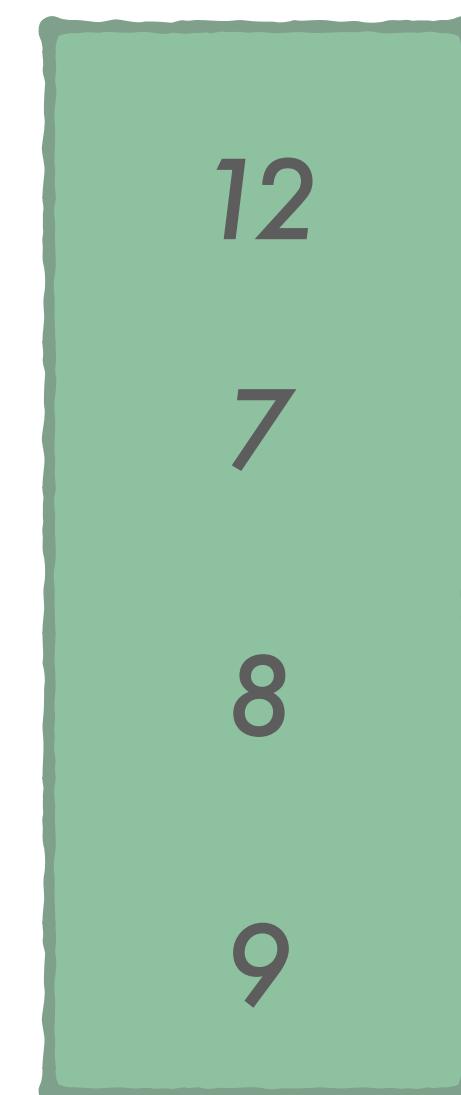


COUNTER

1



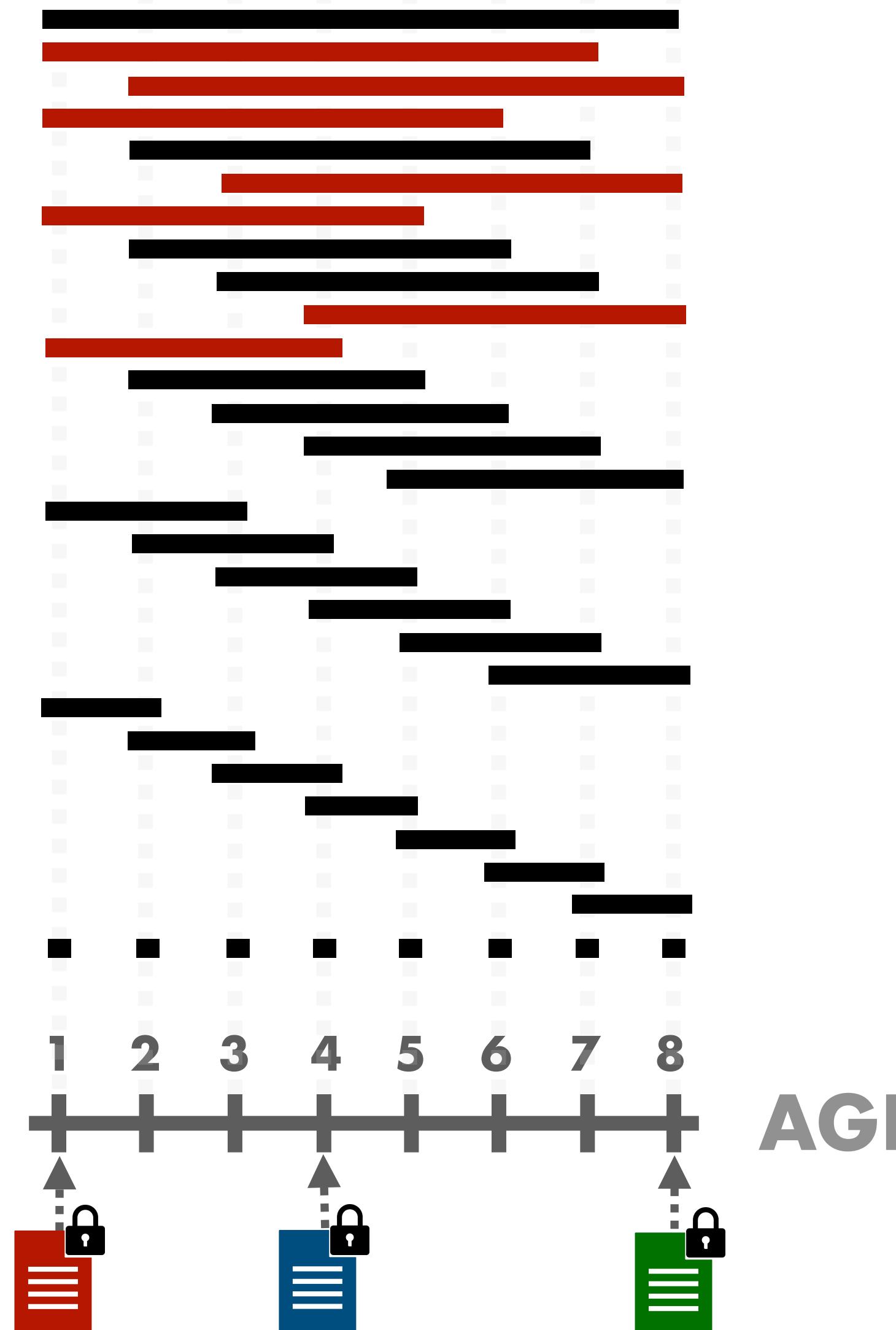
∅



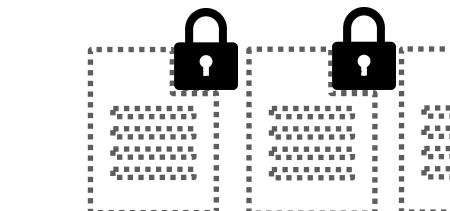


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

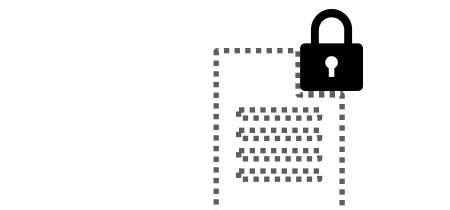


VOLUME

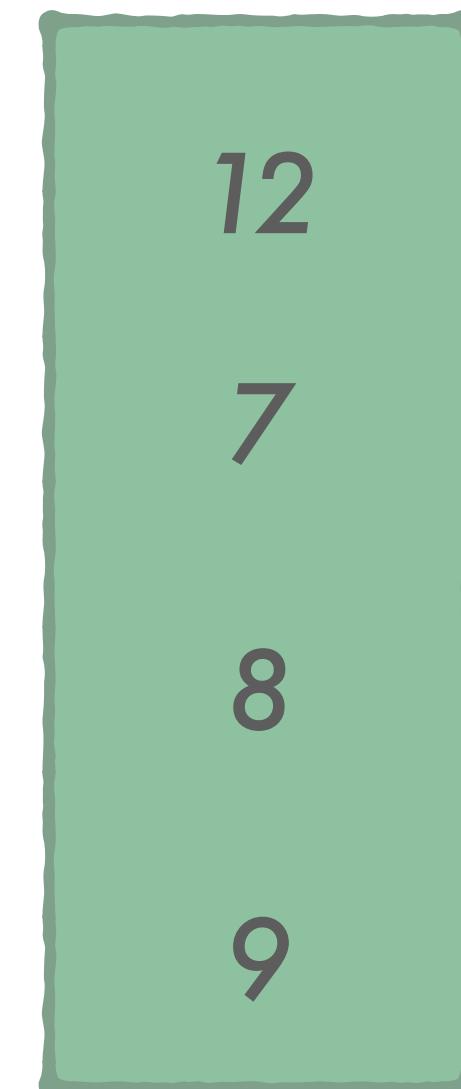


COUNTER

1



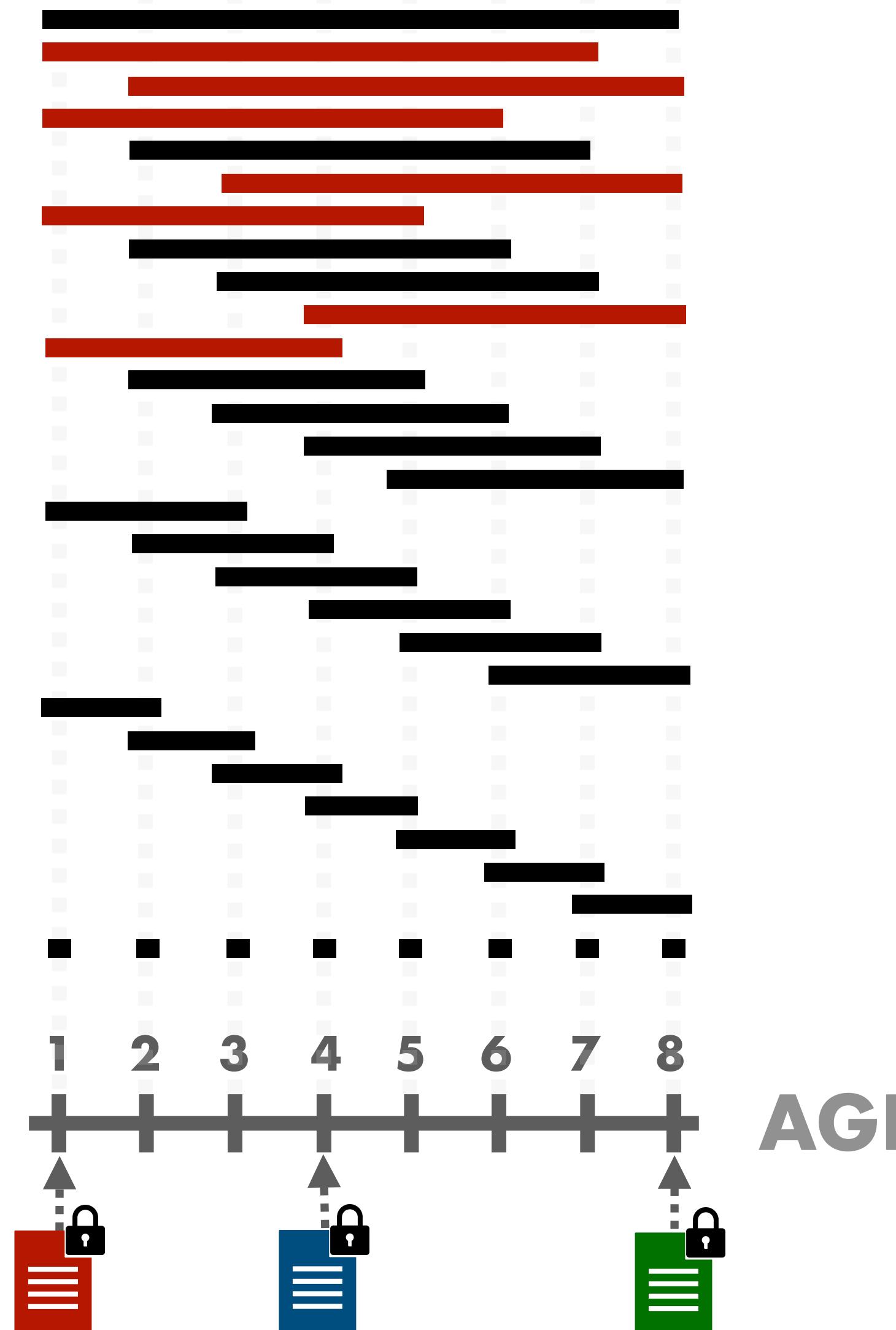
∅



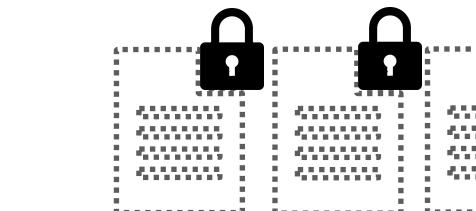


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY



VOLUME

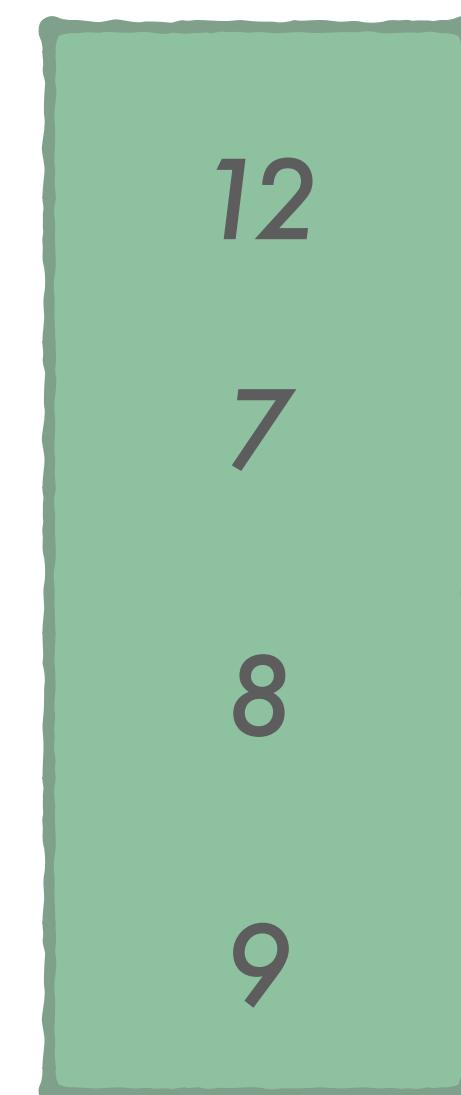


COUNTER

1

7

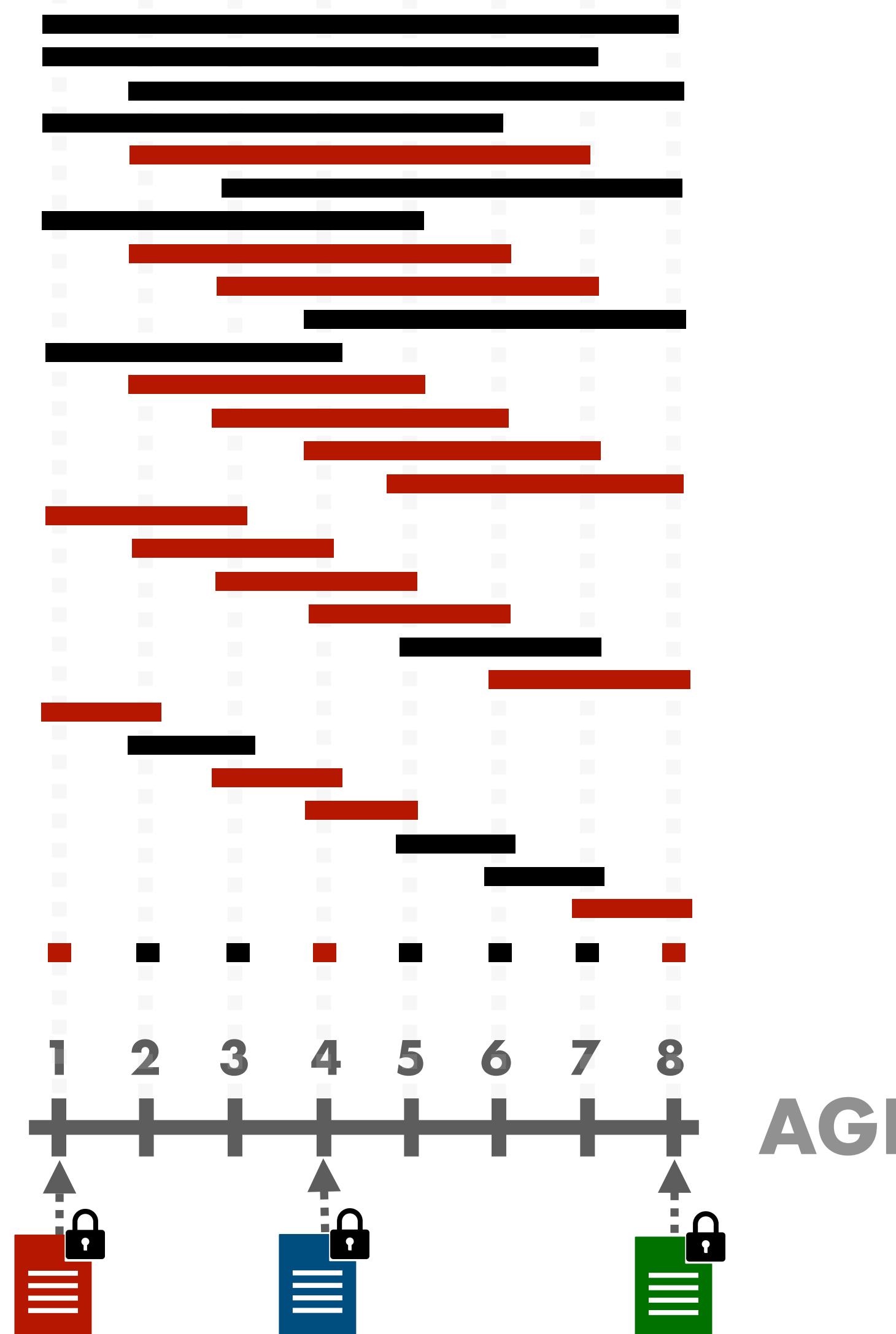
∅



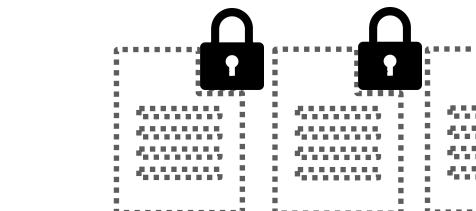


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY



VOLUME

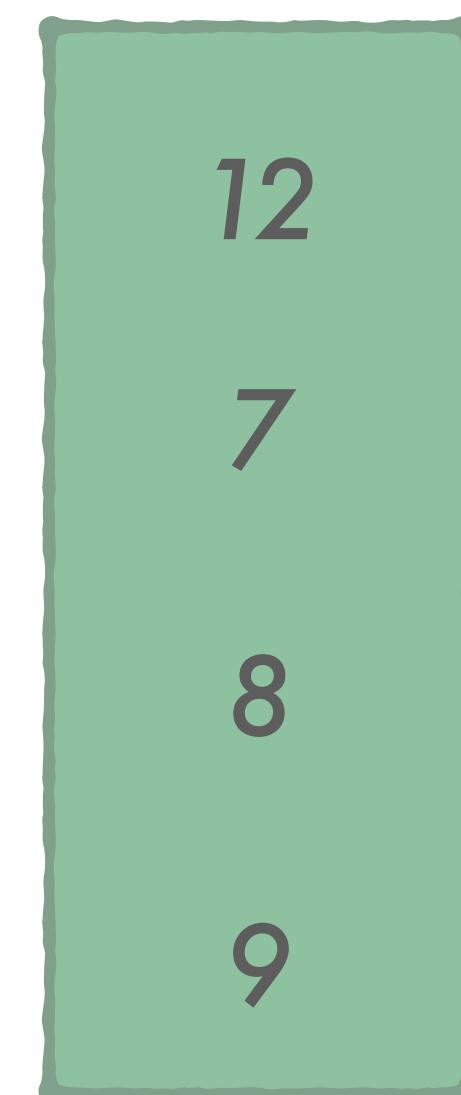


COUNTER

1

7

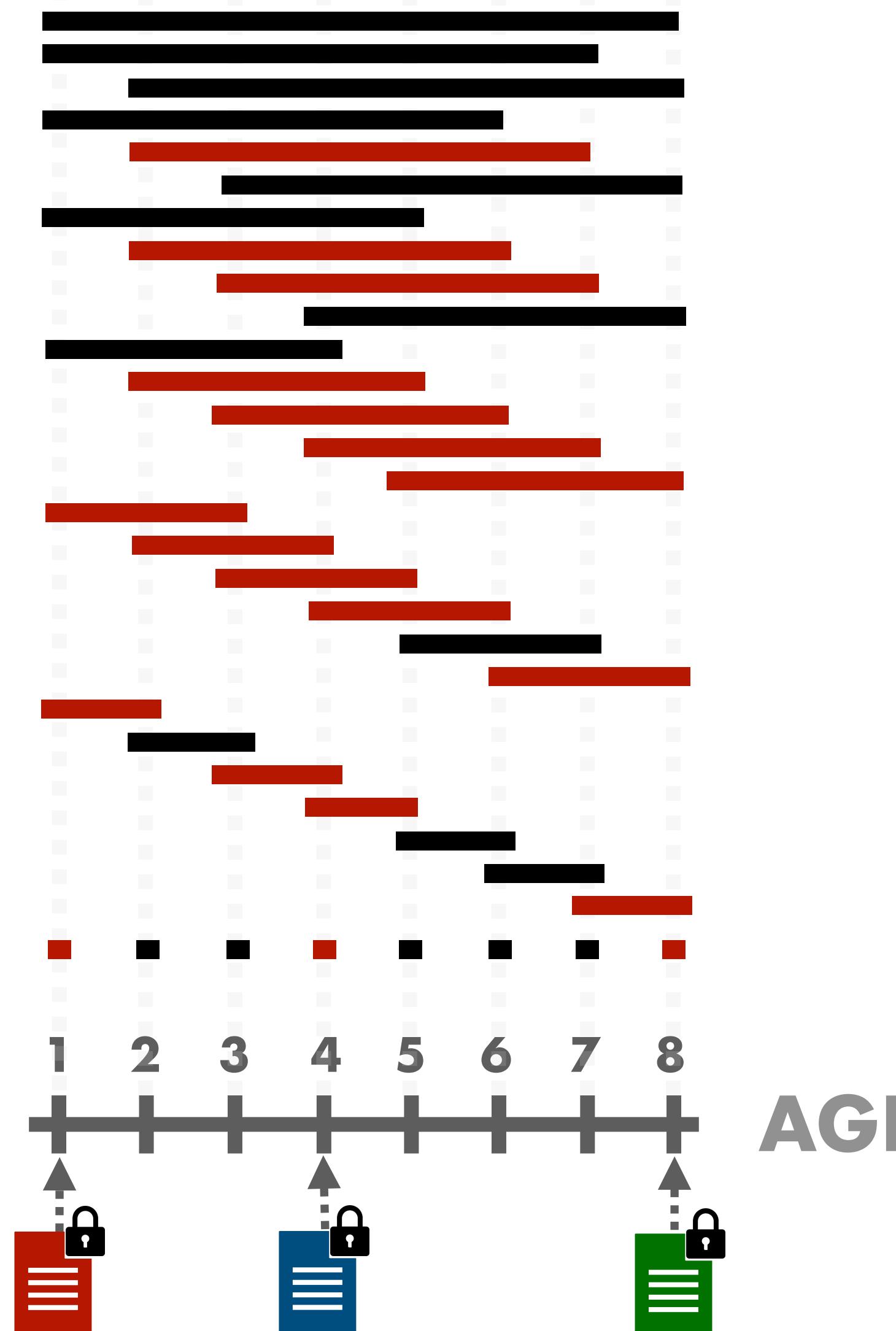
∅



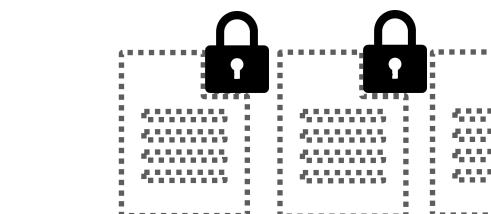


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY

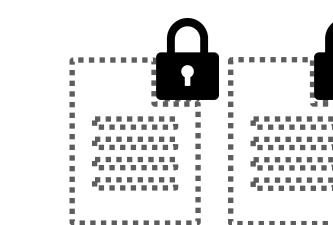


VOLUME

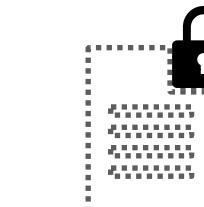


COUNTER

1



7



19

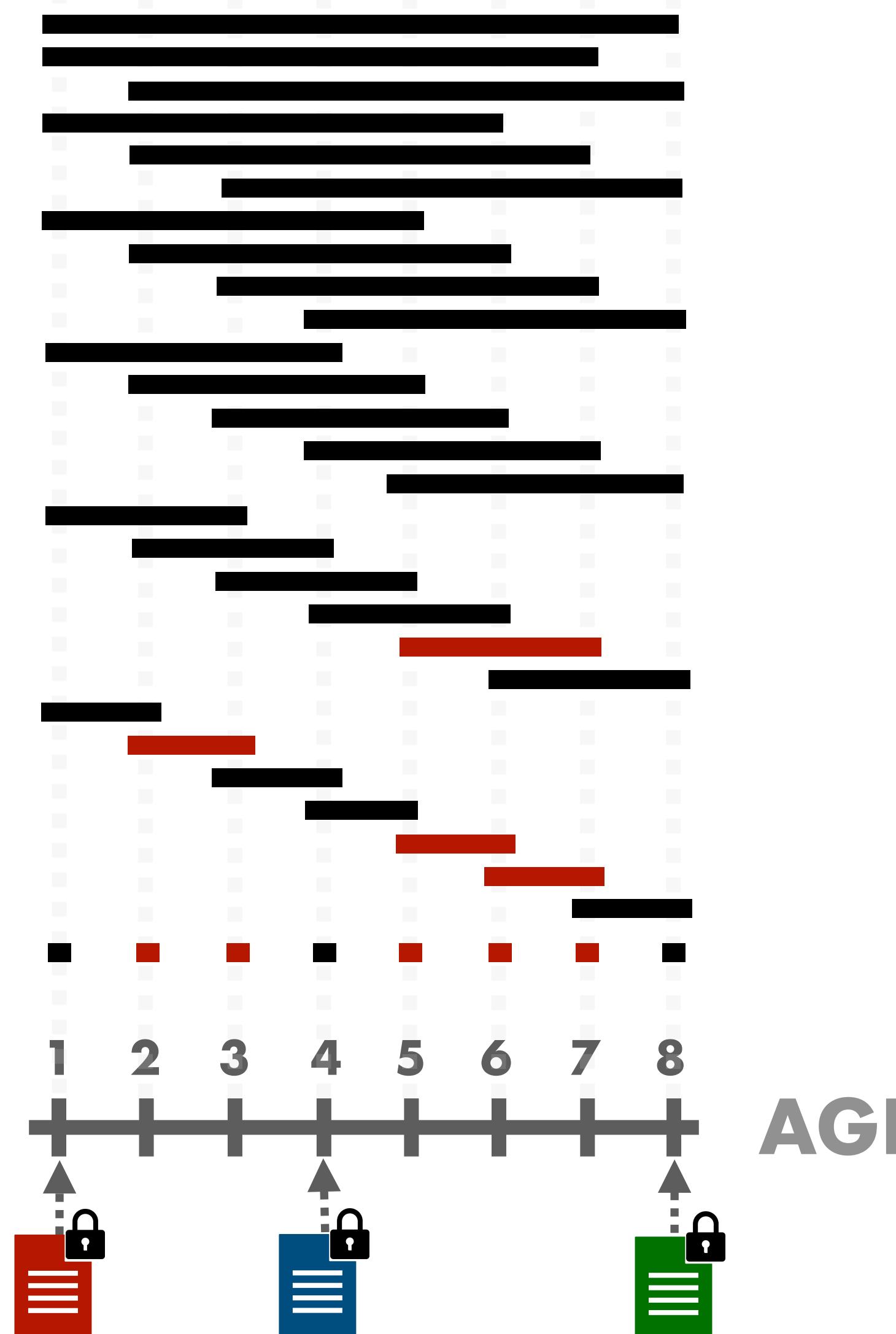
∅



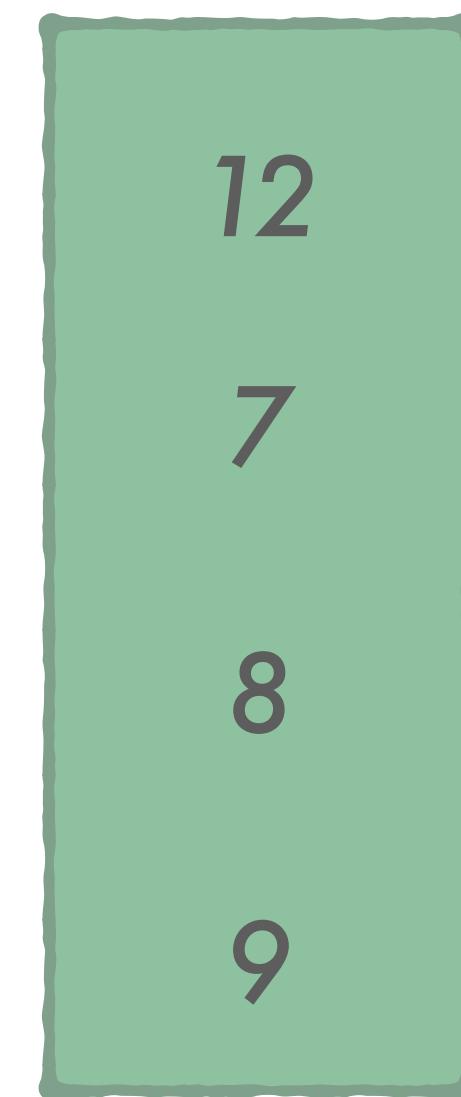


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY



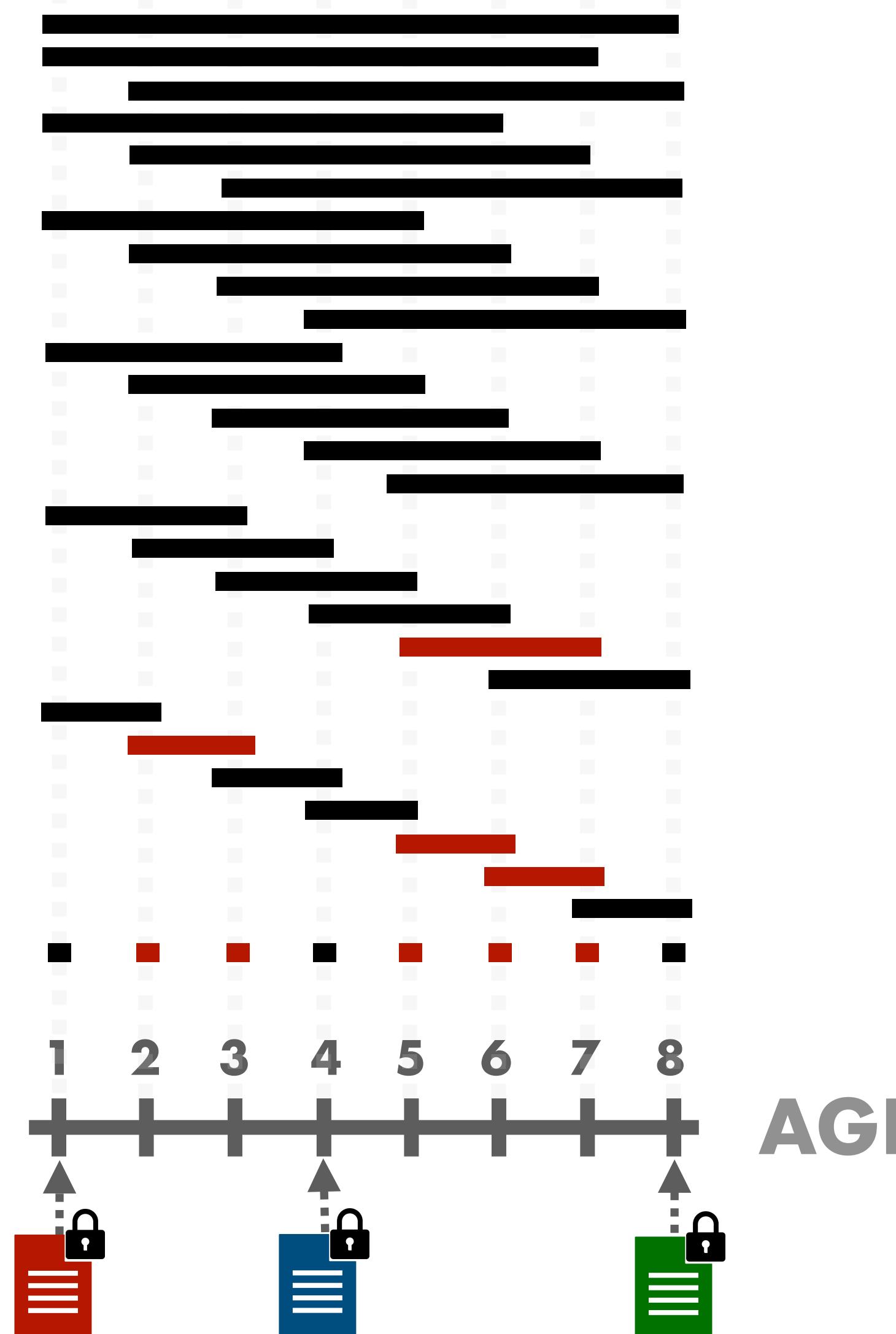
VOLUME	COUNTER
	1
	7
	19
	∅



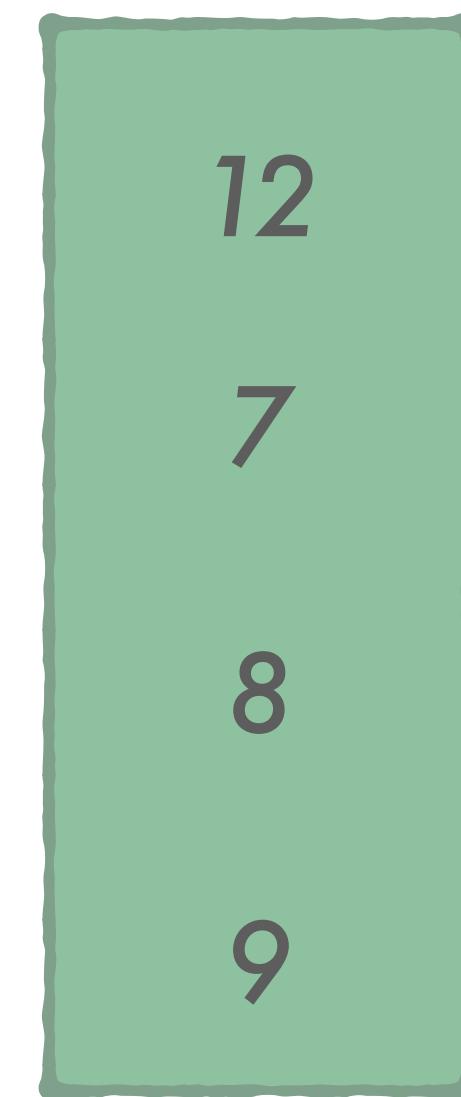


IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY



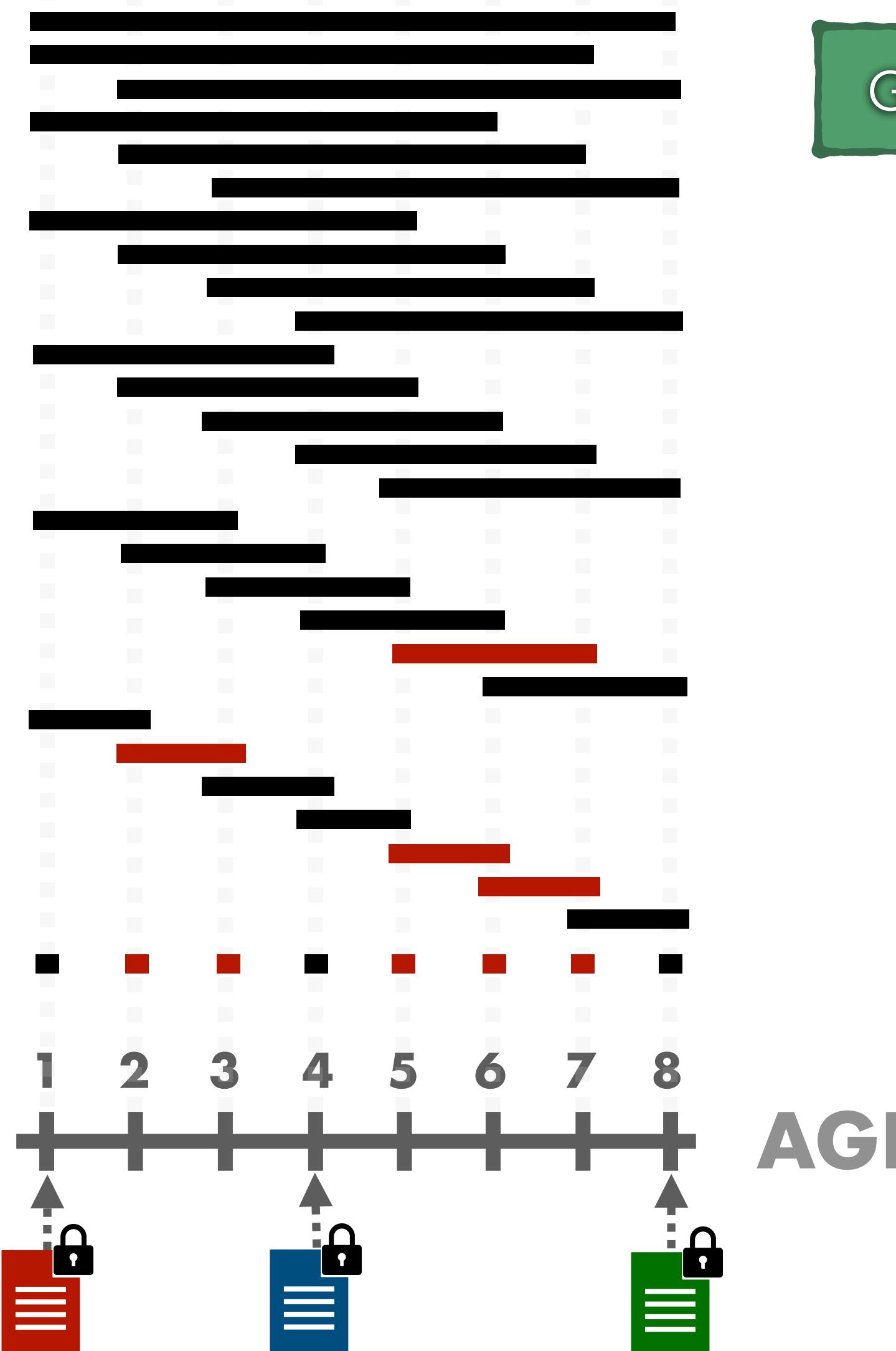
VOLUME	COUNTER
	1
	7
	19
	9





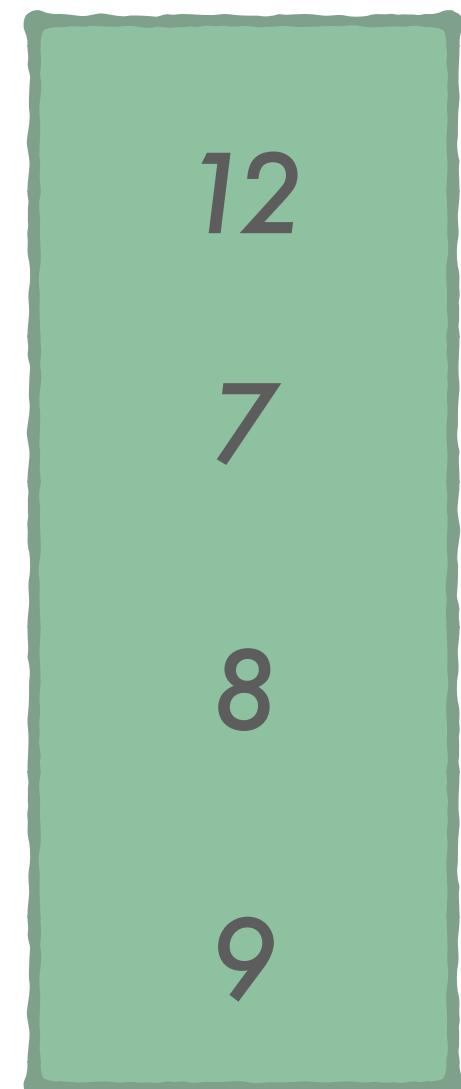
IS THIS LEAKAGE ENOUGH TO ATTACK?

ANSWER: VOLUMES REVEAL GEOMETRY



GEOMETRY IS REVEALED EVEN **WITHOUT ACCESS-PATTERN LEAKAGE**

VOLUME	COUNTER
	1
	7
	19
\emptyset	9





CRYPTANALYSIS ON HARDENED RANGES RESPONSE-HIDING CONSTRUCTIONS ARE VULNERABLE TOO

Response-Hiding Encrypted Ranges: Revisiting Security via Parametrized Leakage-Abuse Attacks

Eugenios M. Kornaropoulos
UC Berkeley
eugenios@berkeley.edu

Charalampos Papamanthou
University of Maryland
csp@umd.edu

Roberto Tamassia
Brown University
rt@cs.brown.edu

Abstract—Despite a growing body of work on leakage-abuse attacks for encrypted databases, attacks on practical response-hiding constructions are yet to appear. Response-hiding constructions are superior in that they *nullify access-pattern based attacks* by returning only the search token and the result size of each query. Response-hiding schemes are vulnerable to existing volume attacks, which are, however, based on strong assumptions such as the uniformity query assumption or the dense database assumption. More crucially, these attacks only apply to schemes that cannot be deployed in practice (and with quadratic storage and increased leakage) when practical response-hiding schemes (Demertzis et al. [SIGMOD’16] and Falsi et al. [ESORICS’15]) have linear storage and less leakage. Due to these shortcomings, the value of existing volume attacks on response-hiding schemes is unclear.

In this work, we close the aforementioned gap by introducing a parametrized leakage-abuse attack that applies to *practical response-hiding structured encryption schemes*. The use of non-parametric estimation techniques makes our attack agnostic to both the data and the query distribution. At the very core of our technique lies the newly defined concept of a *counting function with respect to a range scheme*. We propose a two-phase framework to approximate the counting function for any range scheme. By simply switching our counting function for another, i.e., the smaller “parameter” of our modular attack, an adversary can attack different encrypted range schemes. We propose a constrained optimization formulation for the attack algorithm that is based on the counting functions. We demonstrate the effectiveness of our leakage-abuse attack on synthetic and real-world data under various scenarios.

INTRODUCTION

The notion of *searchable encryption*, introduced by Song-Wagner-Panigrahi in [37], proposes cryptographic schemes in which a client encrypts a privacy-sensitive data collection and outsources this resulting encrypted database to a server that efficiently answers search queries without ever decrypting the database. Since then, there has been a surge of research on this subject addressing issues such as improved definitions [9], dynamic constructions [23], [34], forward and backward privacy [4], [5], [7], [10], and locality of encrypted records [3], [11], [14]. For an overview of the area, see the survey by Fuller et al. [17]. In this work, we are interested in the general definitional framework called *Structured Encryption* (STE) introduced by Chase and Kamara [8] and, more specifically, schemes that support encrypted range queries [6], [13], [15].

To balance efficiency and privacy, STE schemes reveal some information about the query and its corresponding response. This information is called *leakage profile*. These schemes cryptographically guarantee that nothing more is revealed beyond what the designer allowed via the leakage profile.

RESPONSE-HIDING ENCRYPTED RANGES: REVISITING SECURITY VIA PARAMETRIZED LEAKAGE-ABUSE ATTACKS

KORNAROPOULOS, PAPAMANTHOU, TAMASSIA

Proc. IEEE SECURITY & PRIVACY , 2021

● RESTRICTED LEAKAGE: ONLY SEARCH-PATTERN & VOLUME

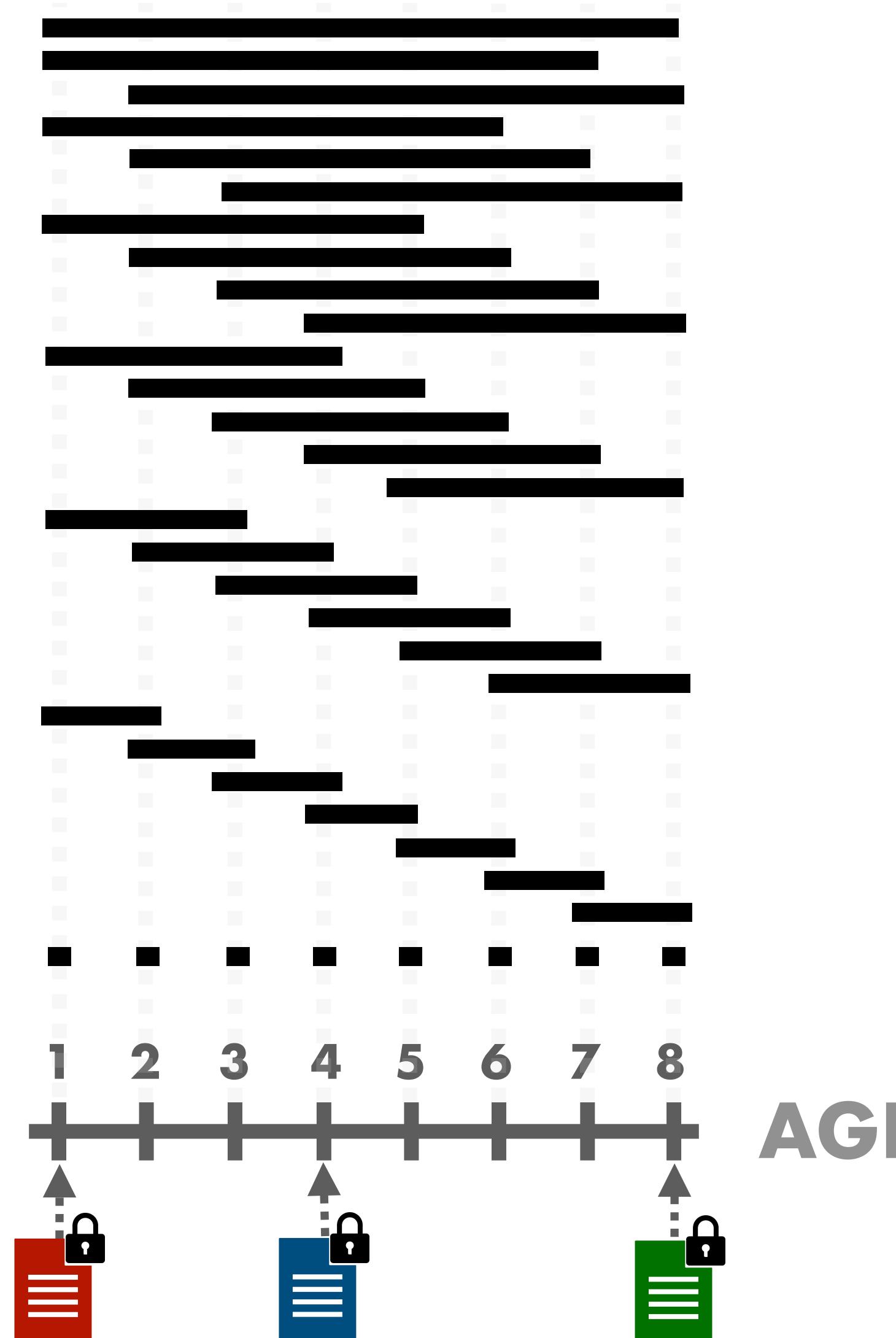
● NEW METHODOLOGY TO ATTACK PRACTICAL CONSTRUCTIONS

● AGNOSTIC TO QUERY DISTRIBUTION



ATTACKS ON PRACTICAL CONSTRUCTIONS ONLY A SUBSET OF RANGE QUERIES

QUADRATIC SCHEME

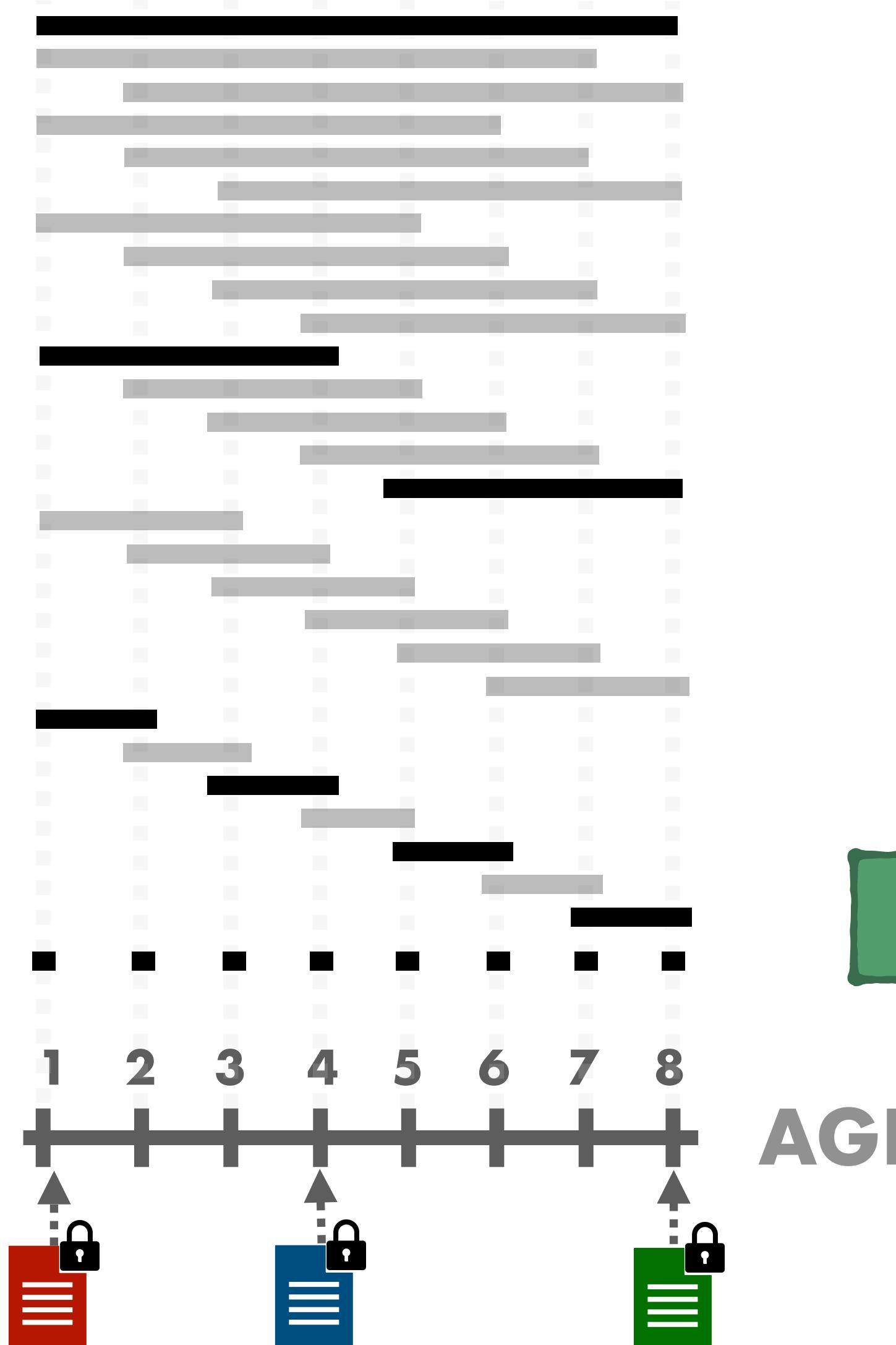


- ALL PREVIOUS ATTACKS FOCUS ON THE QUADRATIC SCHEME
- REVEALS $O(n^2)$ VOLUMES (MORE LEAKY)
- STORES $O(n^2)$ RESPONSES (MORE STORAGE)



ATTACKS ON PRACTICAL CONSTRUCTIONS ONLY A SUBSET OF RANGE QUERIES

BINARY SCHEME



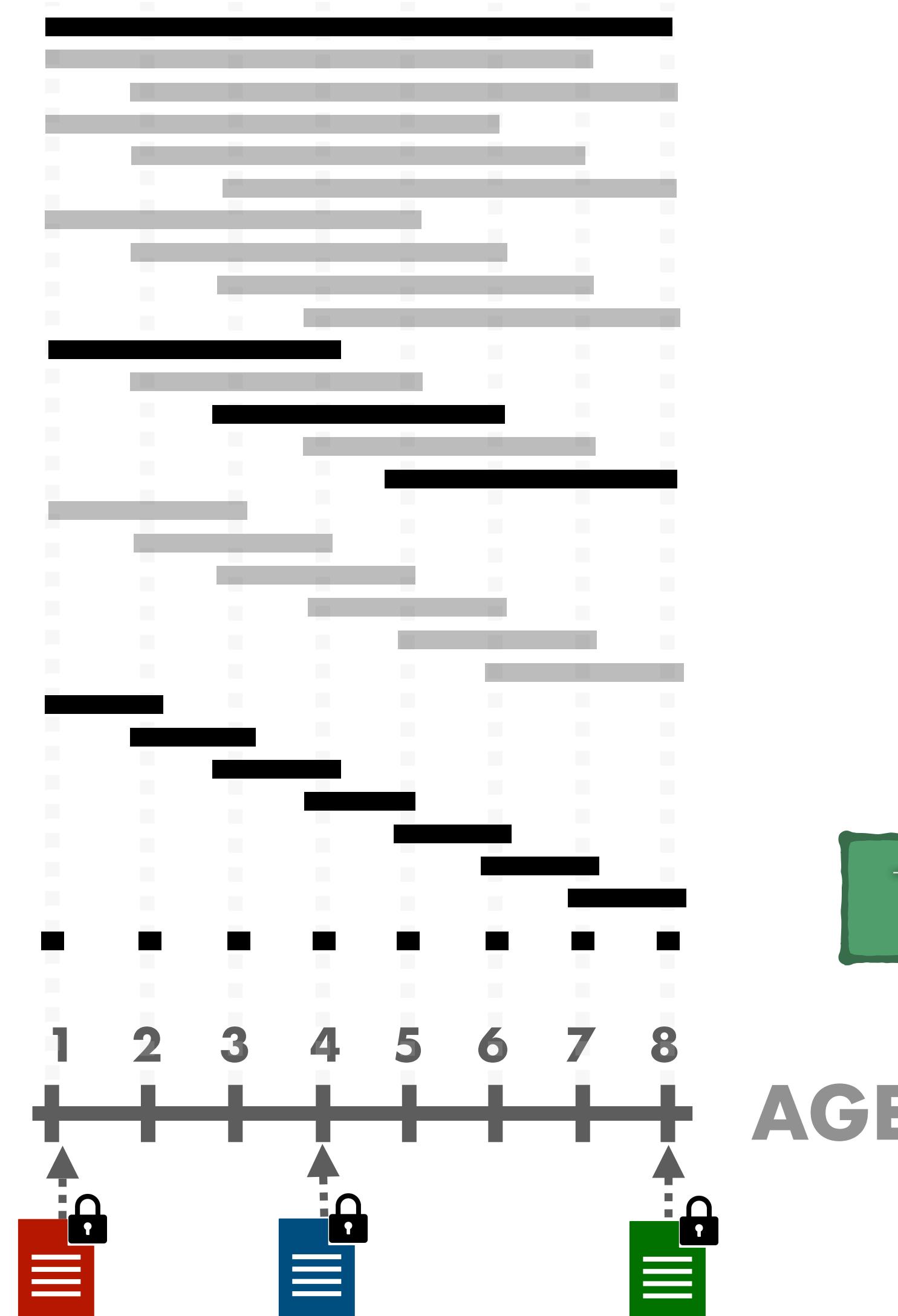
- INTRODUCED BY FABER ET AL. (ESORICS'15)
- REVEALS $O(n)$ VOLUMES (LESS LEAKY)
- STORES $O(n)$ RESPONSES (LESS STORAGE)

THIS WORK IS THE FIRST TO ATTACK THIS PRACTICAL SCHEME



ATTACKS ON PRACTICAL CONSTRUCTIONS ONLY A SUBSET OF RANGE QUERIES

AUGMENTED BINARY SCHEME



- INTRODUCED BY DEMERTZIS ET AL. (SIGMOD'16)
- REVEALS $O(n)$ VOLUMES (LESS LEAKY)
- STORES $O(n)$ RESPONSES (LESS STORAGE)

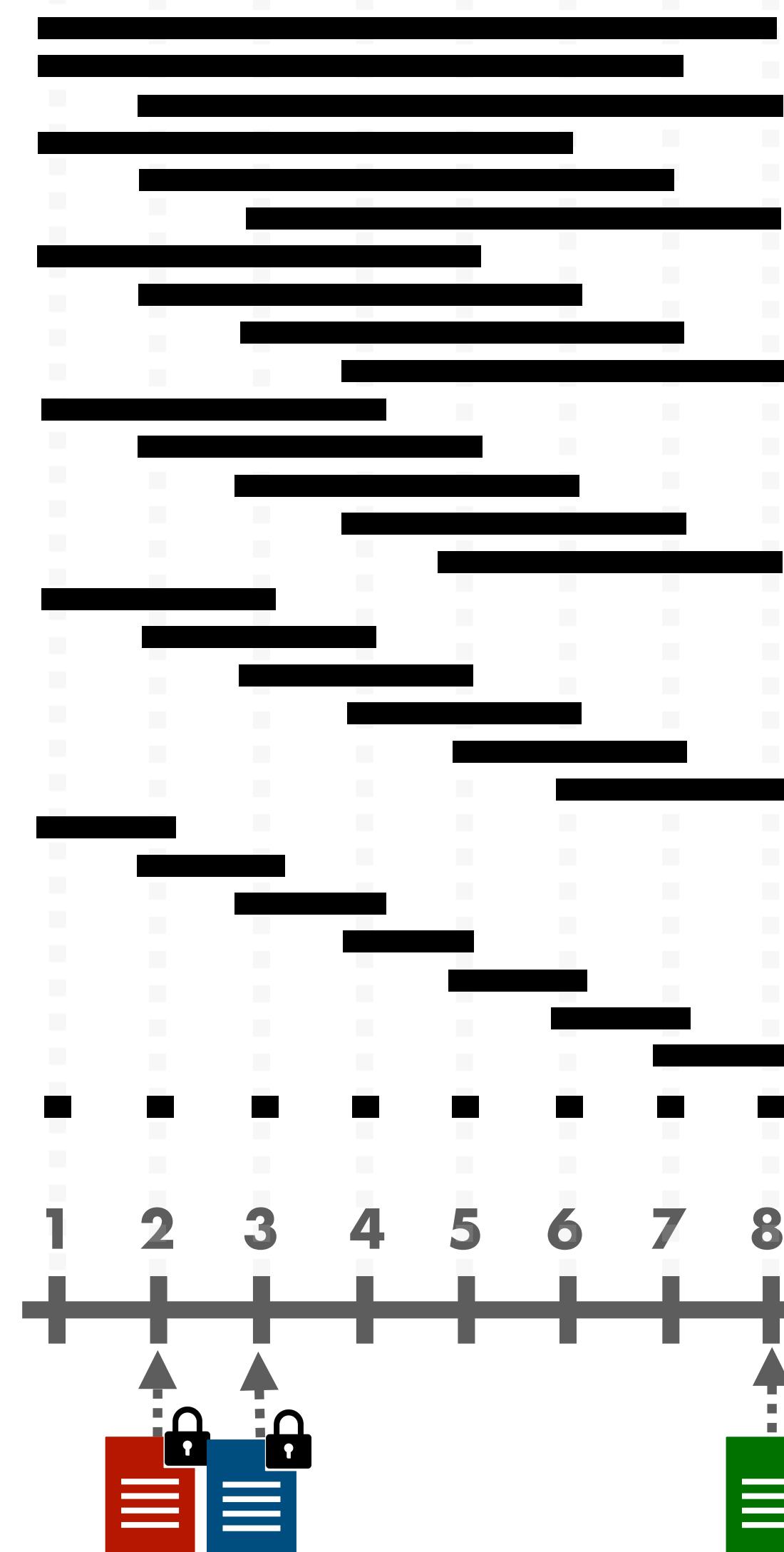
THIS WORK IS THE FIRST TO ATTACK THIS PRACTICAL SCHEME



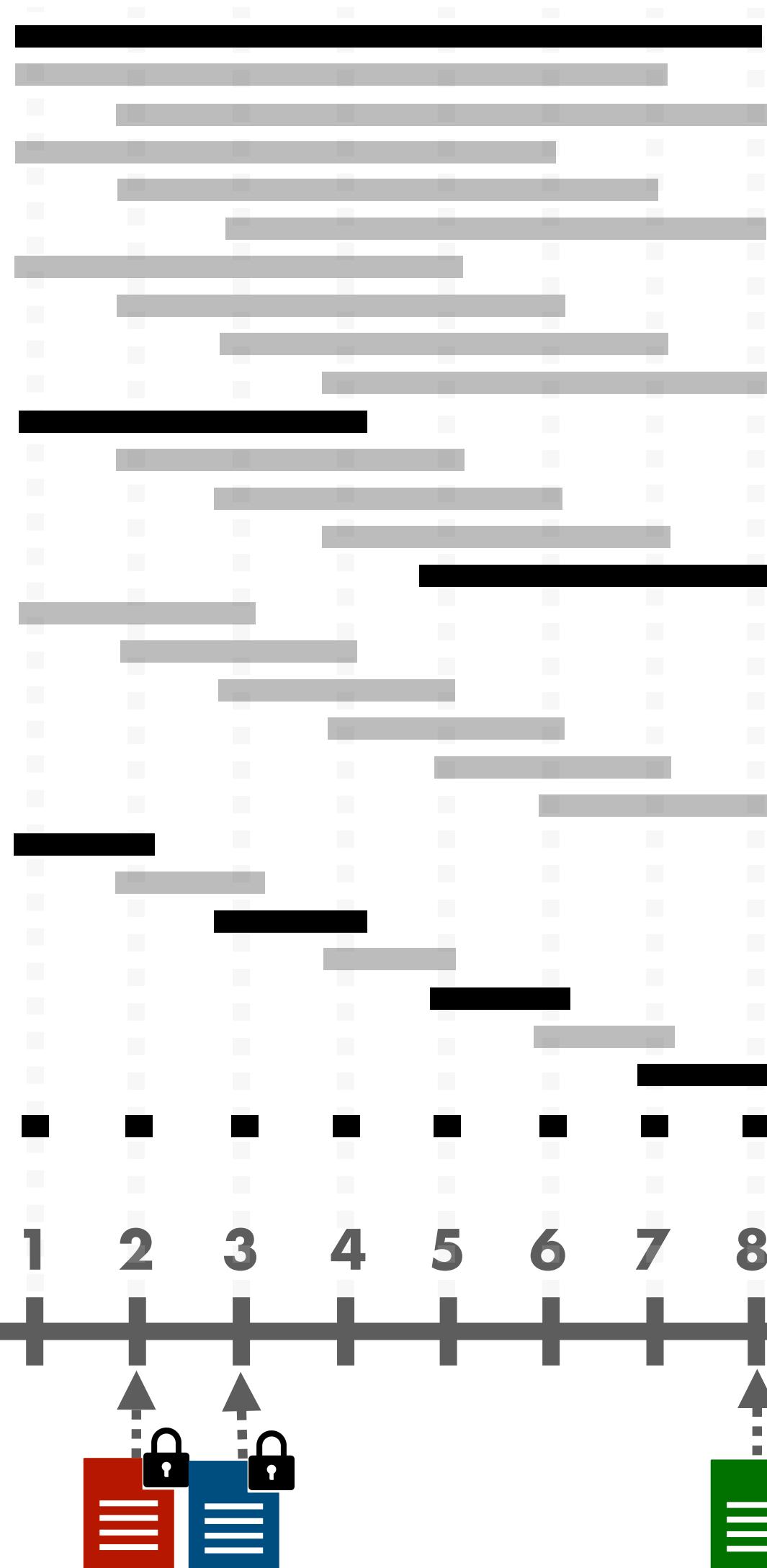
ATTACKS ON PRACTICAL CONSTRUCTIONS

ONLY A SUBSET OF RANGE QUERIES

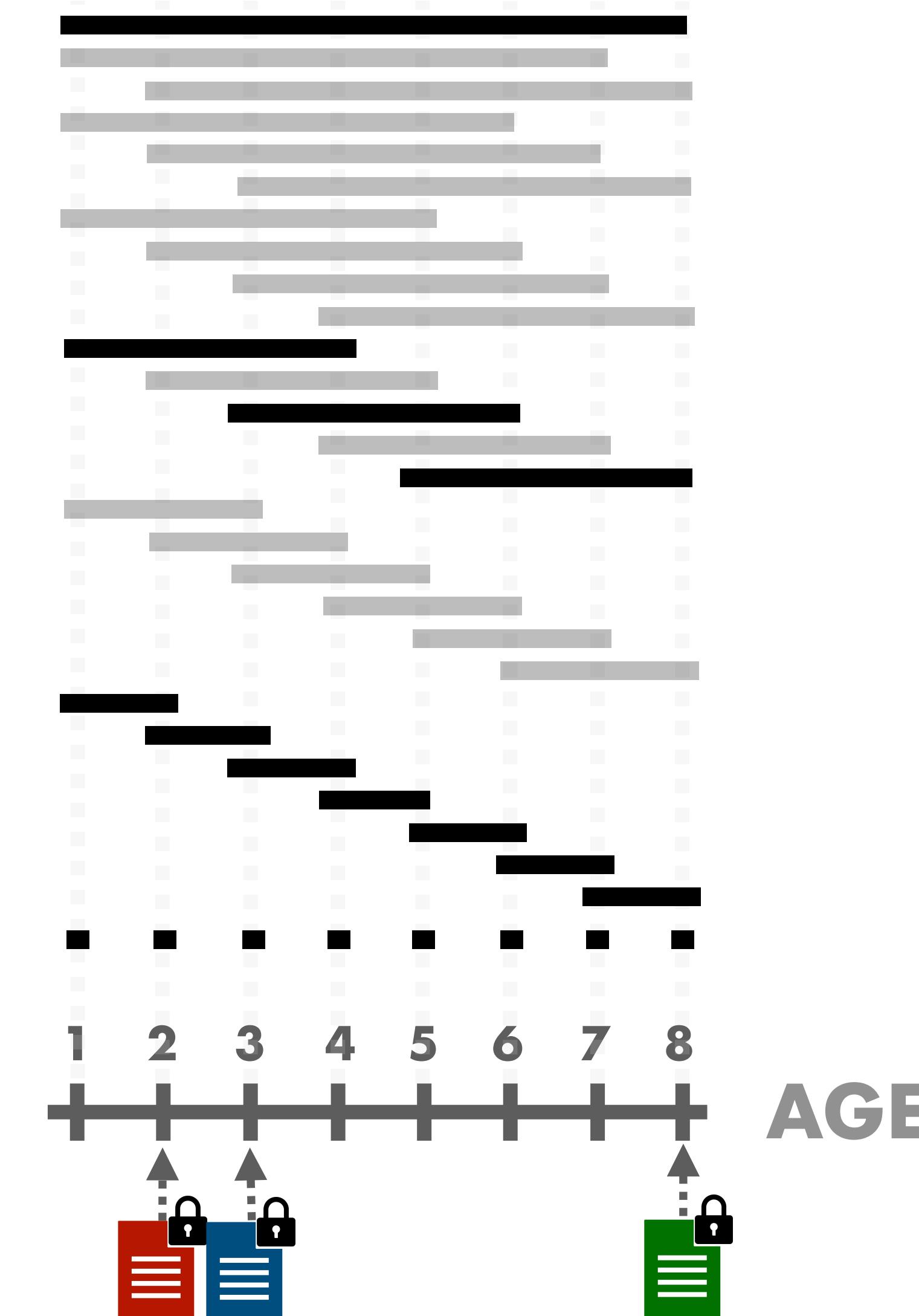
QUADRATIC SCHEME



BINARY SCHEME



AUGMENTED BINARY SCHEME

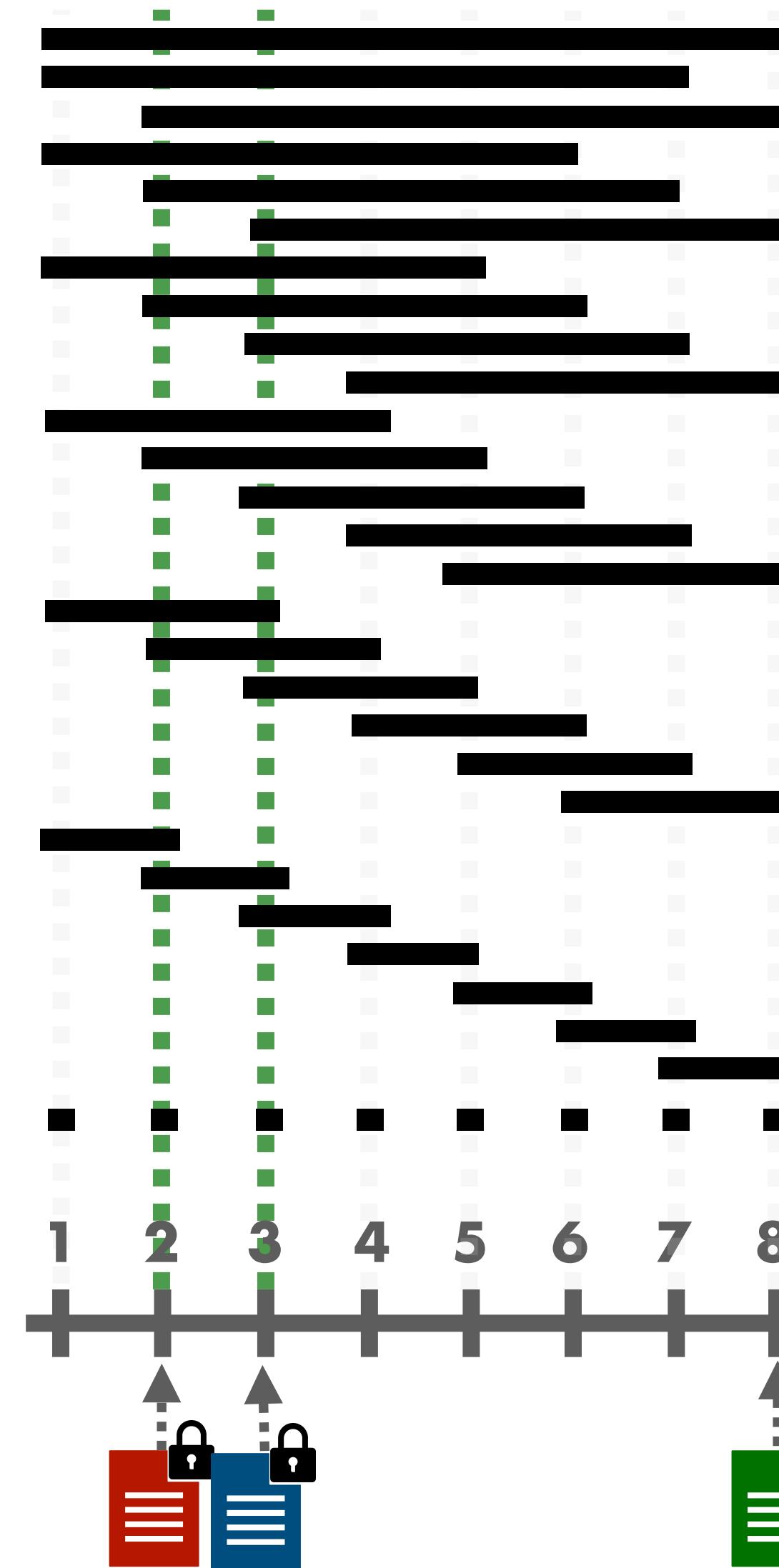




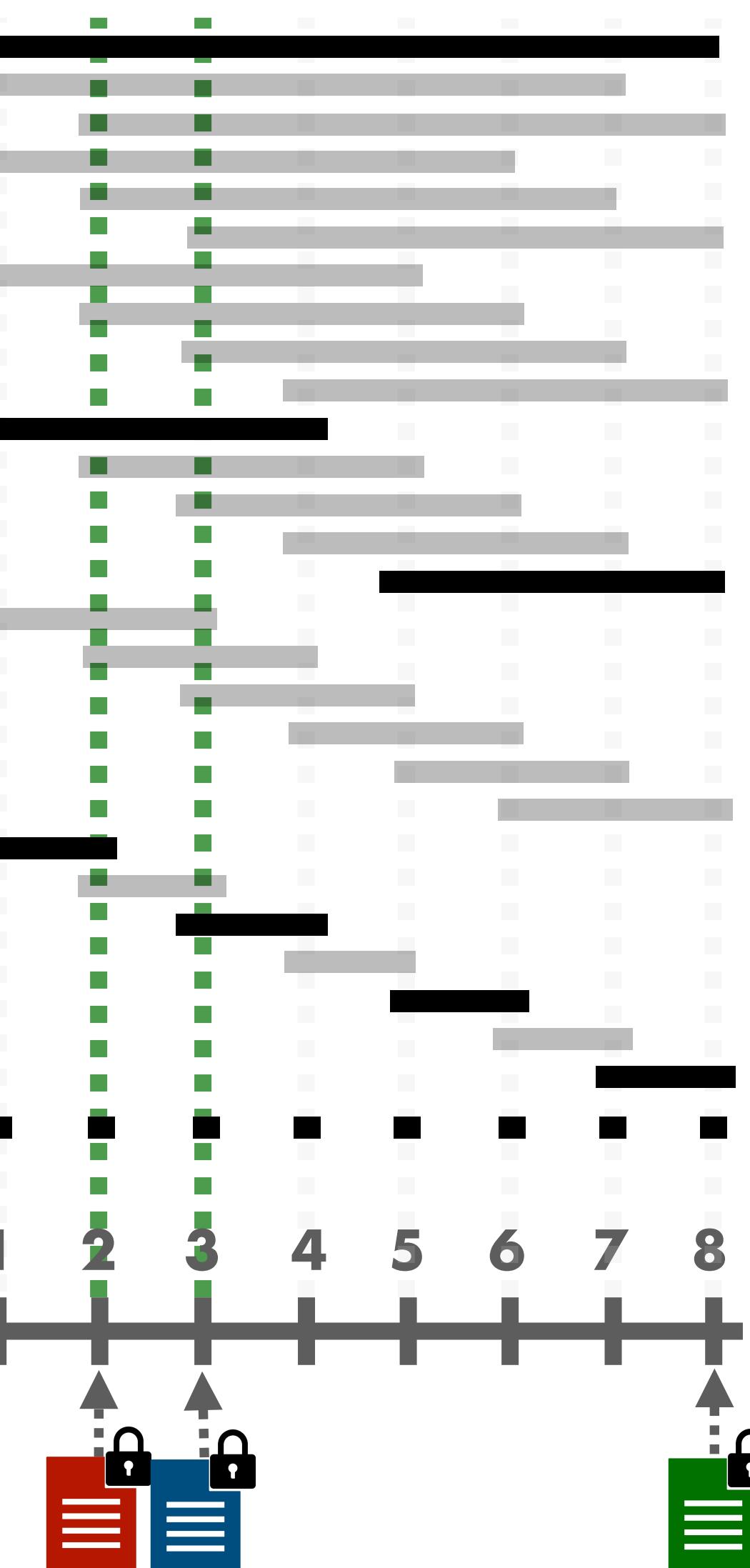
ATTACKS ON PRACTICAL CONSTRUCTIONS

ONLY A SUBSET OF RANGE QUERIES

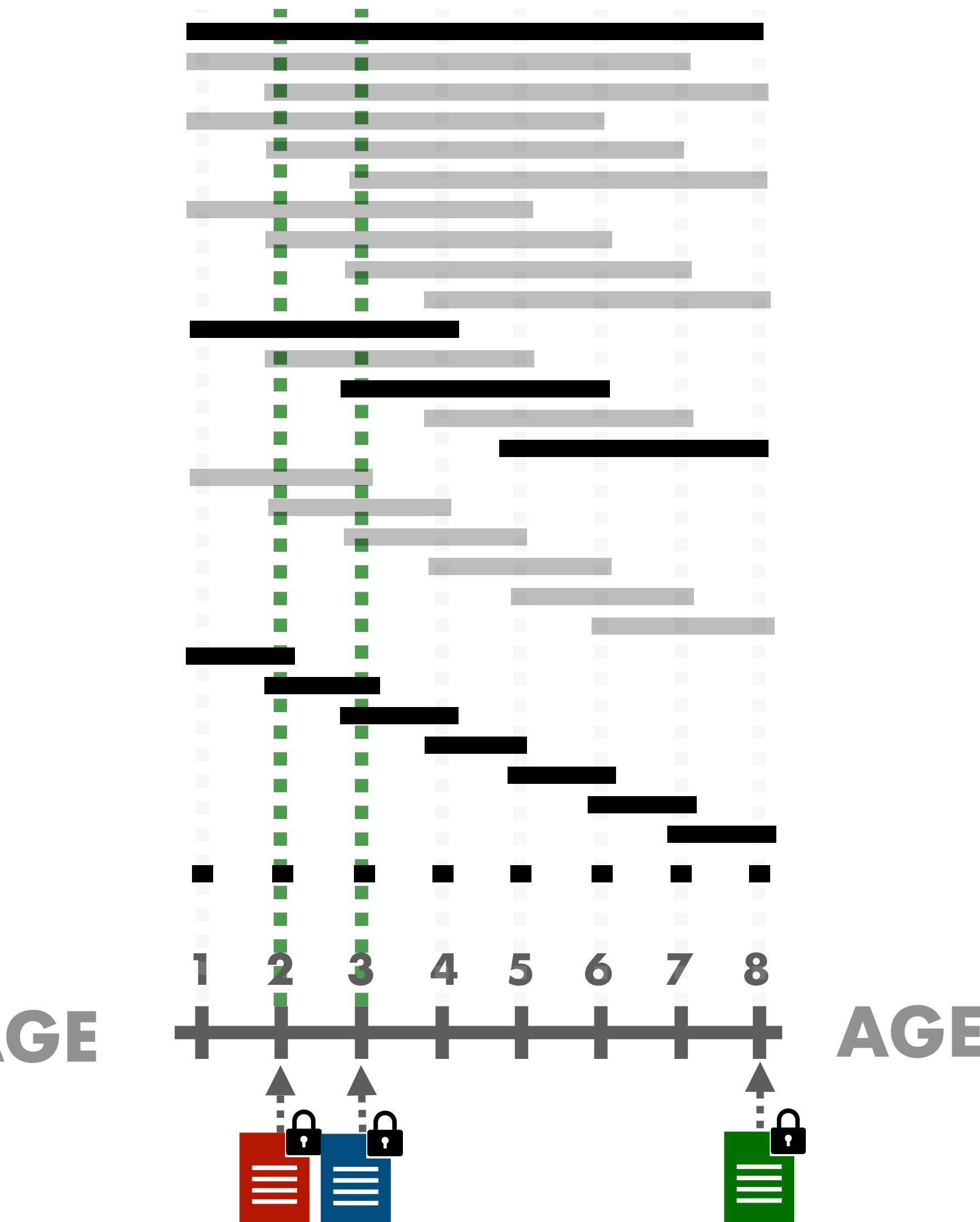
QUADRATIC SCHEME



BINARY SCHEME



AUGMENTED BINARY SCHEME

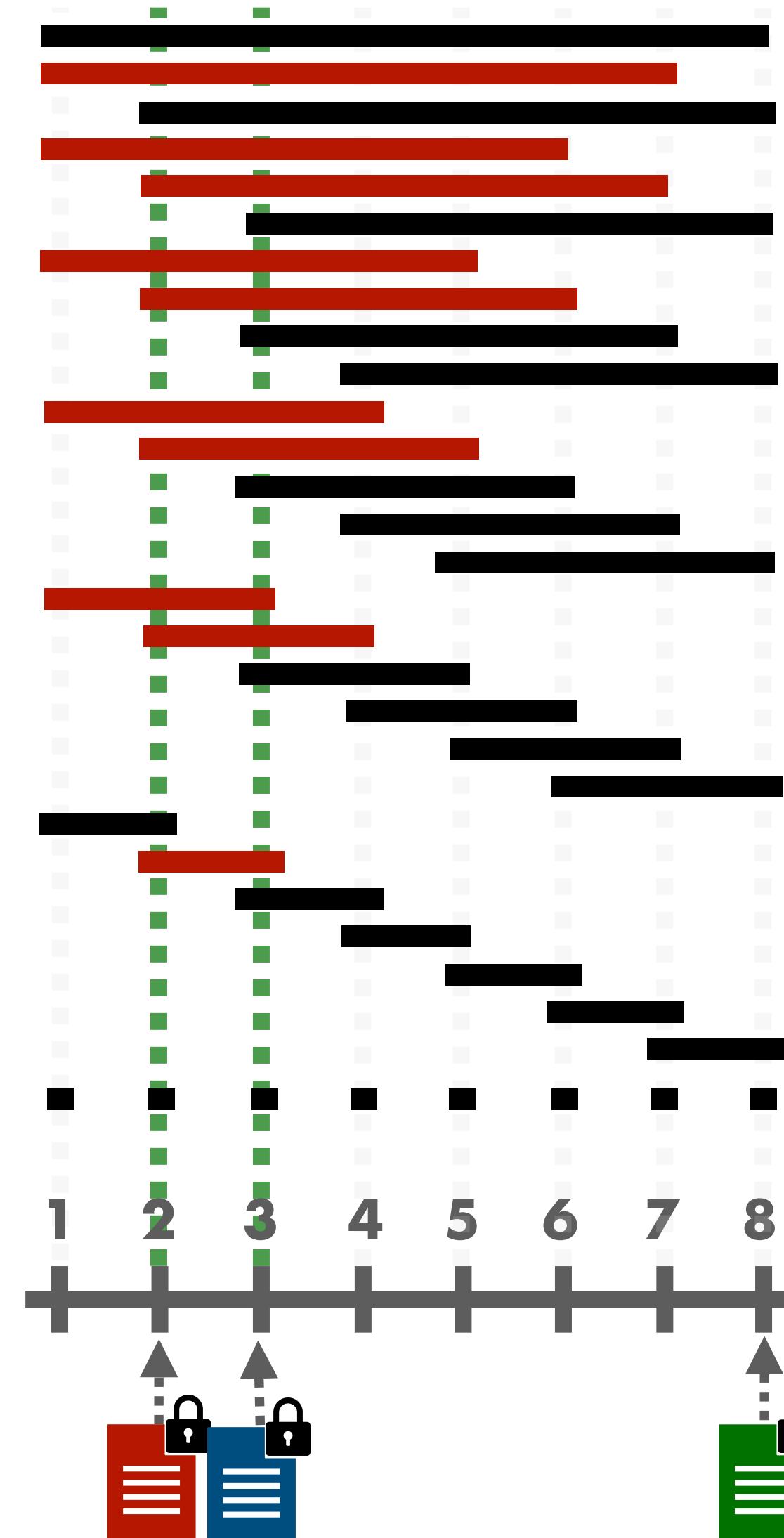




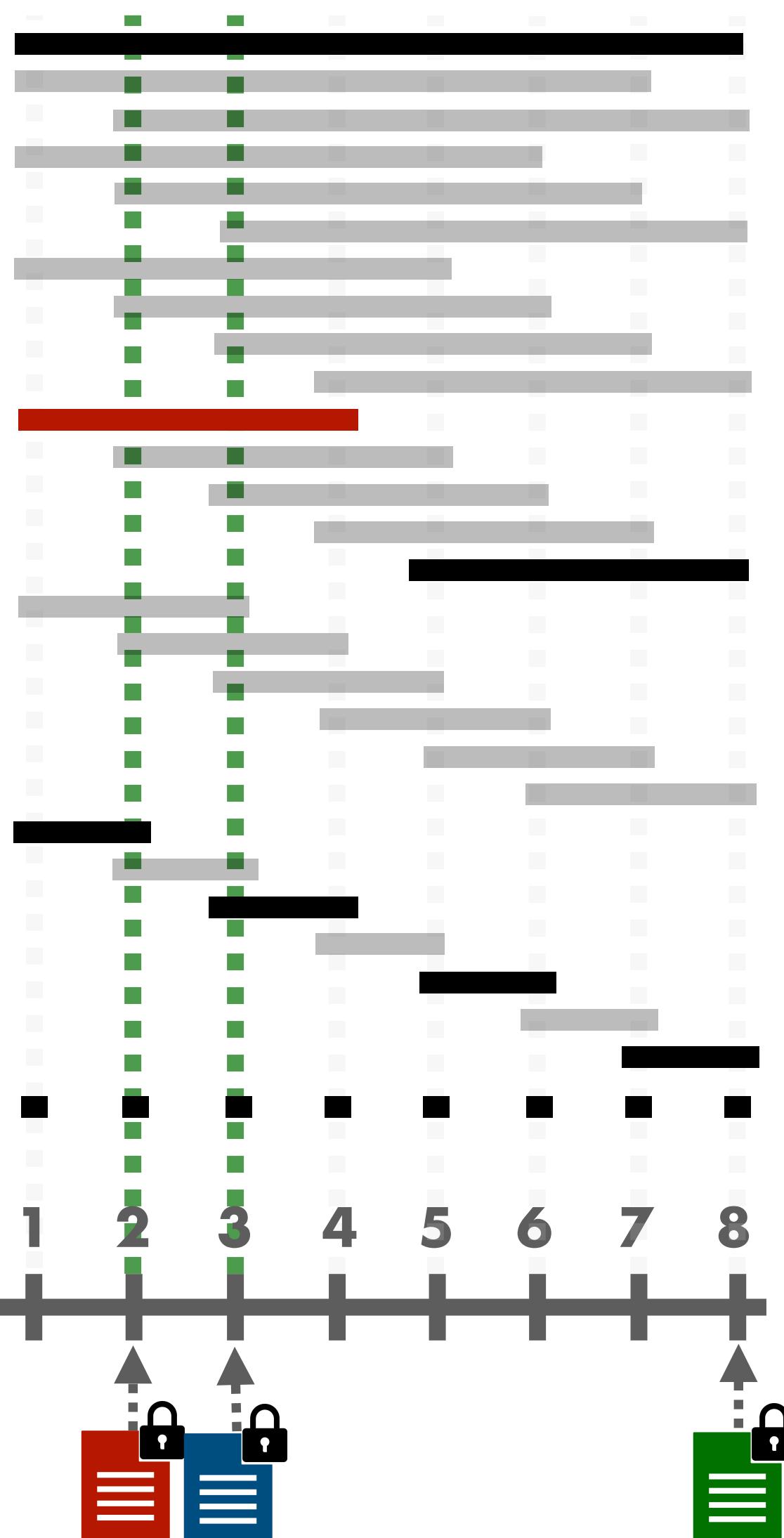
ATTACKS ON PRACTICAL CONSTRUCTIONS

ONLY A SUBSET OF RANGE QUERIES

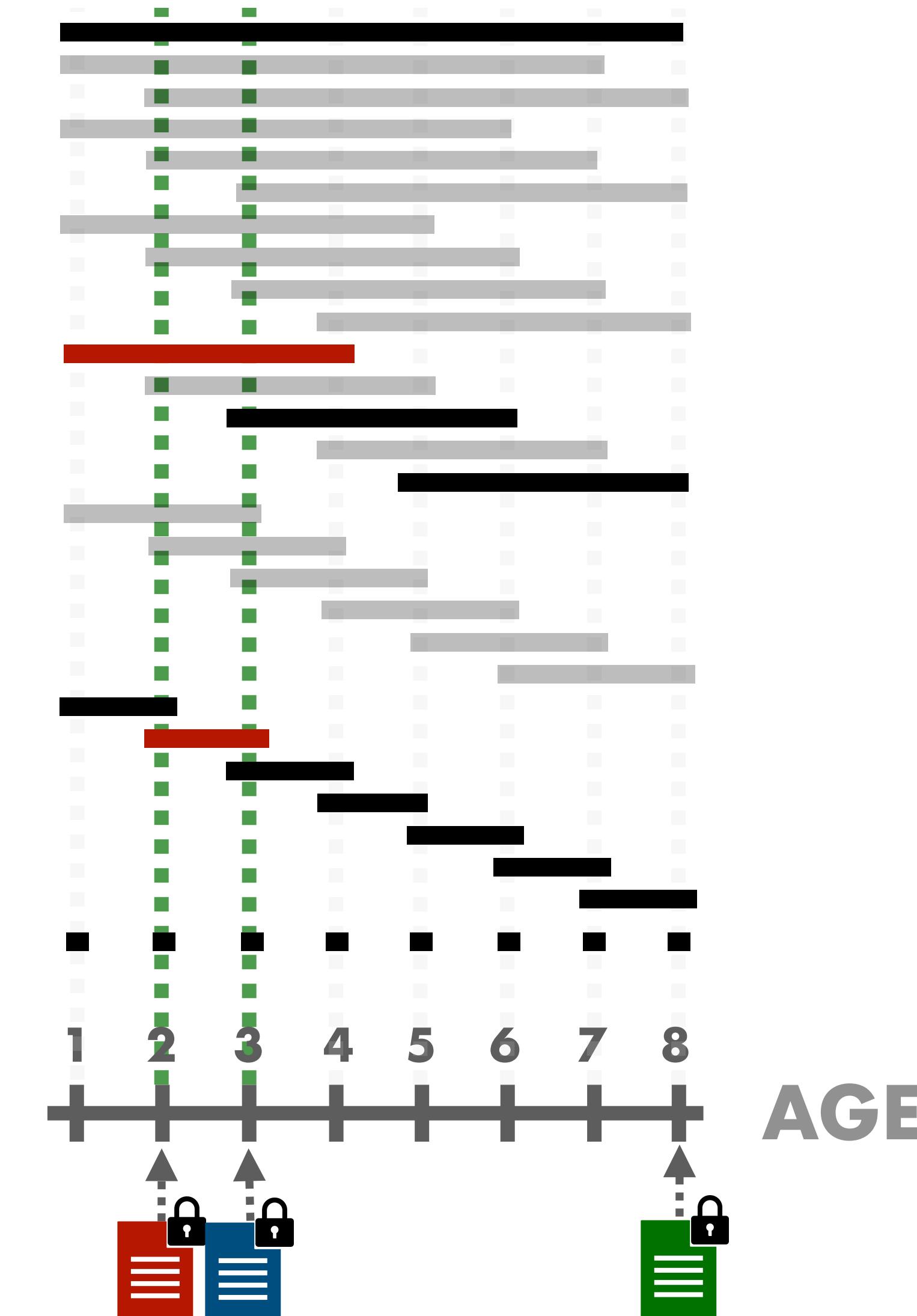
QUADRATIC SCHEME



BINARY SCHEME



AUGMENTED BINARY SCHEME





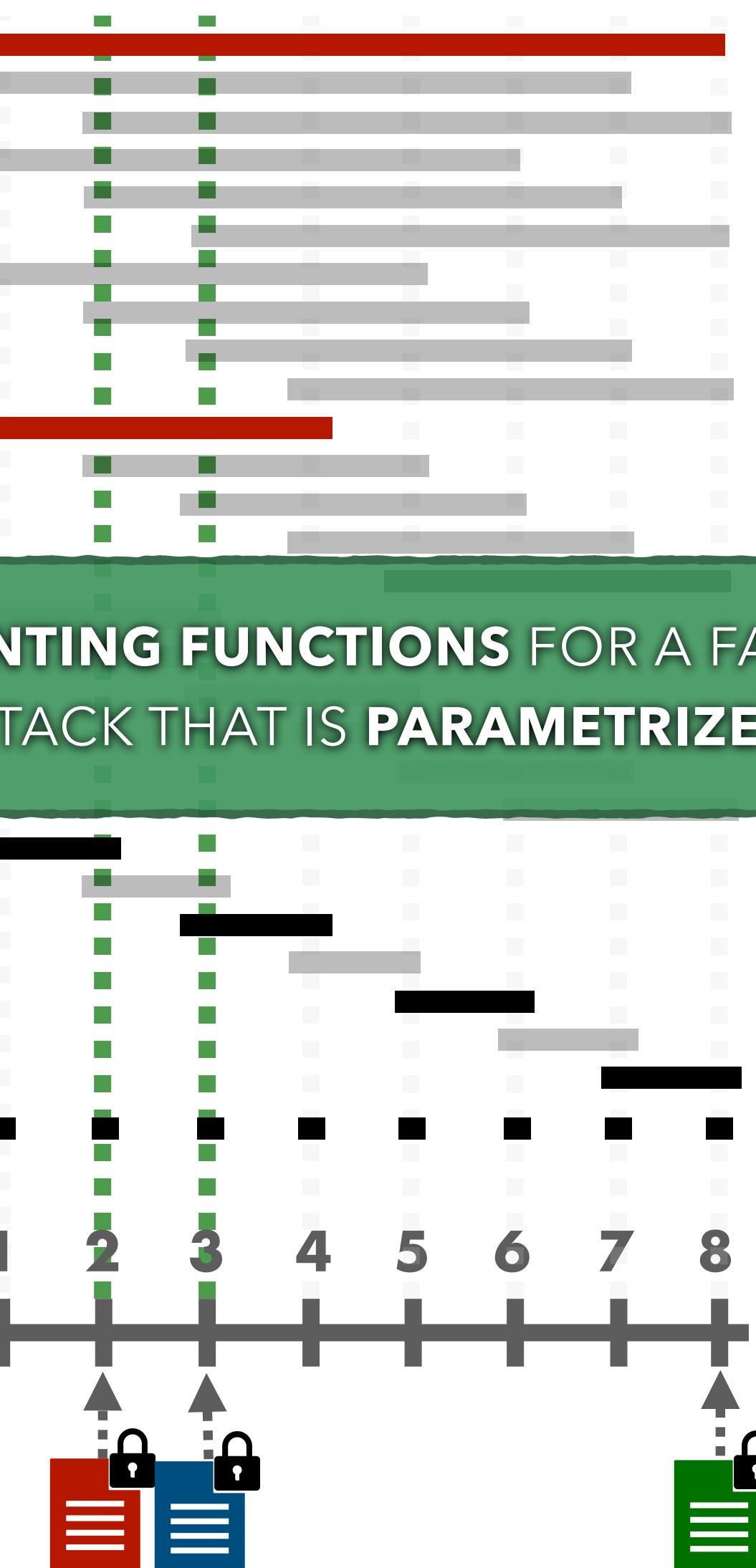
ATTACKS ON PRACTICAL CONSTRUCTIONS

ONLY A SUBSET OF RANGE QUERIES

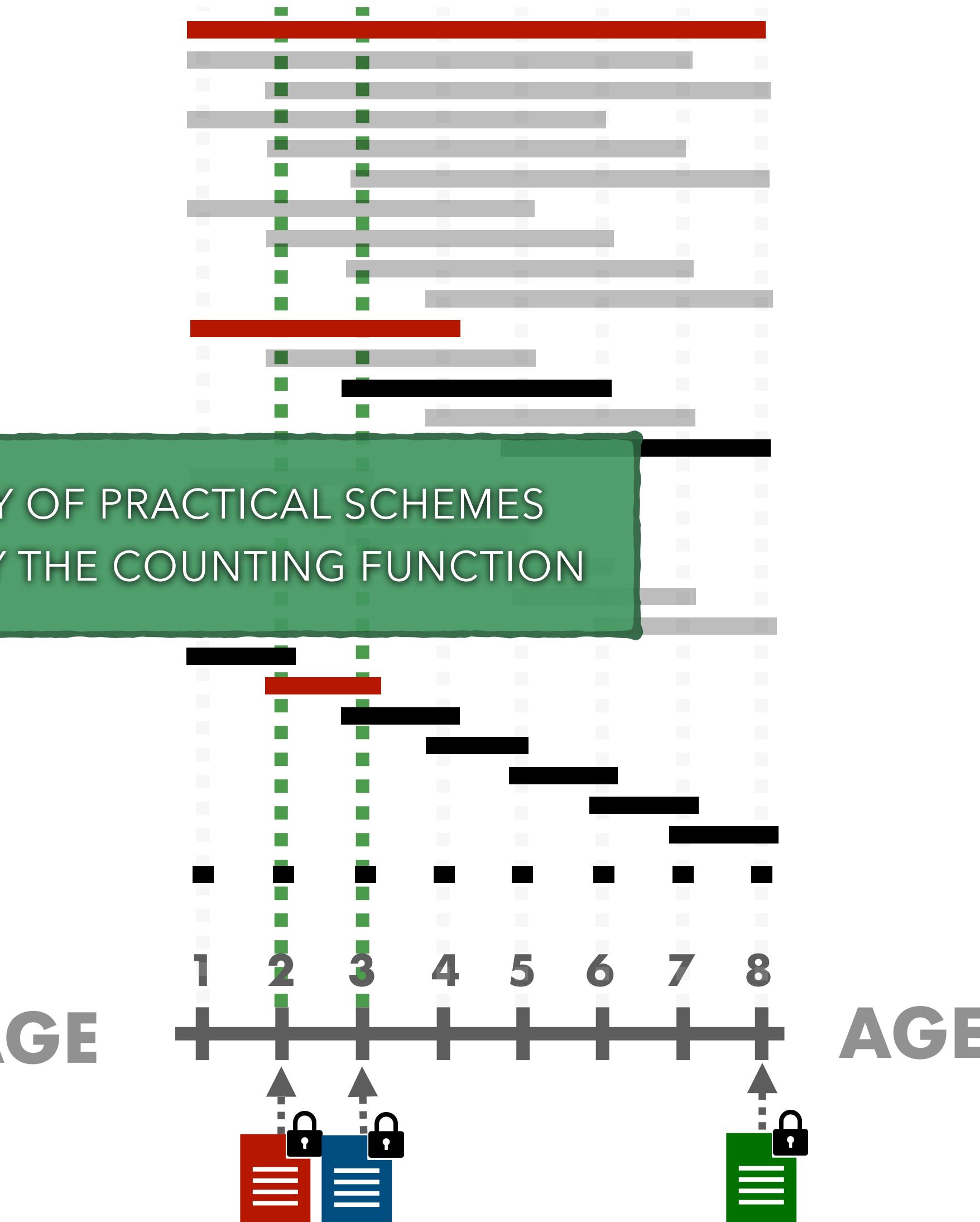
QUADRATIC SCHEME



BINARY SCHEME



AUGMENTED BINARY SCHEME



- WE PROPOSE **COUNTING FUNCTIONS** FOR A FAMILY OF PRACTICAL SCHEMES
- WE PRESENT AN ATTACK THAT IS **PARAMETRIZED** BY THE COUNTING FUNCTION



ATTACKS FORMULATION AN OPTIMIZATION APPROACH

$$\min_{DB} (\text{Count}_{\text{Vol}=1}(DB) - \text{Leakage}_{\text{Vol}=1})^2 + \dots + (\text{Count}_{\text{Vol}=n}(DB) - \text{Leakage}_{\text{Vol}=n})^2$$



ATTACKS FORMULATION AN OPTIMIZATION APPROACH

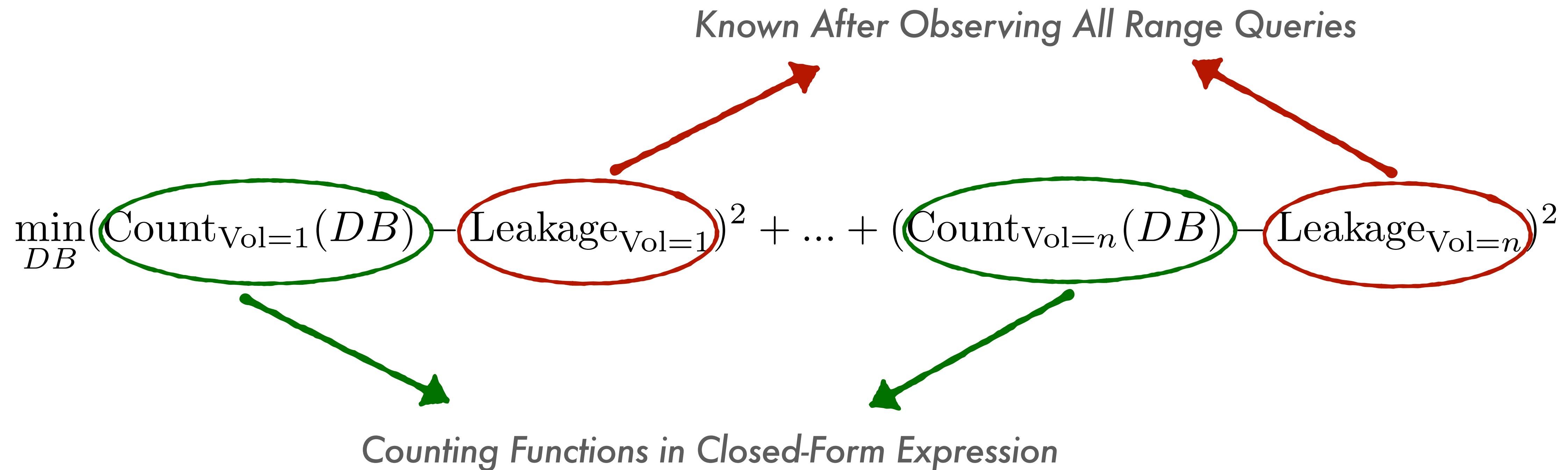
Known After Observing All Range Queries

$$\min_{DB} (\text{Count}_{\text{Vol}=1}(DB) - \text{Leakage}_{\text{Vol}=1})^2 + \dots + (\text{Count}_{\text{Vol}=n}(DB) - \text{Leakage}_{\text{Vol}=n})^2$$

The equation illustrates an optimization problem where the goal is to minimize the sum of squared differences between observed counts and leakage values across n different volume levels. The terms involving leakage are circled in red, and two red arrows point from the text 'Known After Observing All Range Queries' to these circled terms, indicating that the leakage values are known or can be derived from observing all range queries.



ATTACKS FORMULATION AN OPTIMIZATION APPROACH





CRYPTANALYSIS ON HARDENED RANGES RESPONSE-HIDING CONSTRUCTIONS ARE VULNERABLE TOO

Response-Hiding Encrypted Ranges: Revisiting Security via Parametrized Leakage-Abuse Attacks

Eugenios M. Kornaropoulos
UC Berkeley
eugenios@berkeley.edu

Charalampos Papamanthou
University of Maryland
csp@umd.edu

Roberto Tamassia
Brown University
rt@cs.brown.edu

Abstract—Despite a growing body of work on leakage-abuse attacks for encrypted databases, attacks on practical response-hiding constructions are yet to appear. Response hiding constructions are superior in that they *only* modify access-pattern based attacks by revealing only the search token and the result size of each query. Response-hiding schemes are vulnerable to existing volume attacks, which are, however, based on strong assumptions such as the uniformity query assumption or the dense database assumption. More crucially, these attacks only apply to schemes that cannot be deployed in practice (and with quadratic storage and increased leakage) when practical response-hiding schemes (Demertzis et al. [SIGMOD’16] and Falsi et al. [ESORICS’15]) have linear storage and less leakage. Due to these shortcomings, the value of existing volume attacks on response-hiding schemes is unclear.

In this work, we close the aforementioned gap by introducing a parametrized leakage-abuse attack that applies to *practical* response-hiding *structured encryption* schemes. The use of non-parametric estimation techniques makes our attack agnostic to both the data and the query distribution. At the very core of our technique lies the newly defined concept of a *counting function* with respect to a range scheme. We propose a two-phase framework to approximate the counting function for any range scheme. By simply switching our counting function for another, i.e., the smaller “parameter” of our modular attack, an adversary can attack different encrypted range schemes. We propose a constrained optimization formulation for the attack algorithm that is based on the counting functions. We demonstrate the effectiveness of our leakage-abuse attack on synthetic and real-world data under various scenarios.

INTRODUCTION

The notion of *searchable encryption*, introduced by Song-Wang-Panigrahi in [37], proposes cryptographic schemes in which a client encrypts a privacy-sensitive data collection and outsources this resulting encrypted database to a server that efficiently answers search queries without ever decrypting the database. Since then, there has been a surge of research on this subject addressing issues such as improved definitions [9], dynamic constructions [23], [34], forward and backward privacy [4], [5], [7], [10], and locality of encrypted records [3], [11], [14]. For an overview of the area, see the survey by Fuller et al. [17]. In this work, we are interested in the general definitional framework called *Structured Encryption* (STE) introduced by Chase and Kamara [8] and, more specifically, schemes that support encrypted range queries [6], [13], [15].

To balance efficiency and privacy, STE schemes reveal some information about the query and its corresponding response. This information is called *leakage profile*. These schemes cryptographically guarantee that nothing more is revealed beyond what the designer allowed via the leakage profile.

RESPONSE-HIDING ENCRYPTED RANGES: REVISITING SECURITY VIA PARAMETRIZED LEAKAGE-ABUSE ATTACKS

KORNAROPOULOS, PAPAMANTHOU, TAMASSIA

Proc. IEEE SECURITY & PRIVACY , 2021

● RESTRICTED LEAKAGE: ONLY SEARCH-PATTERN & VOLUME

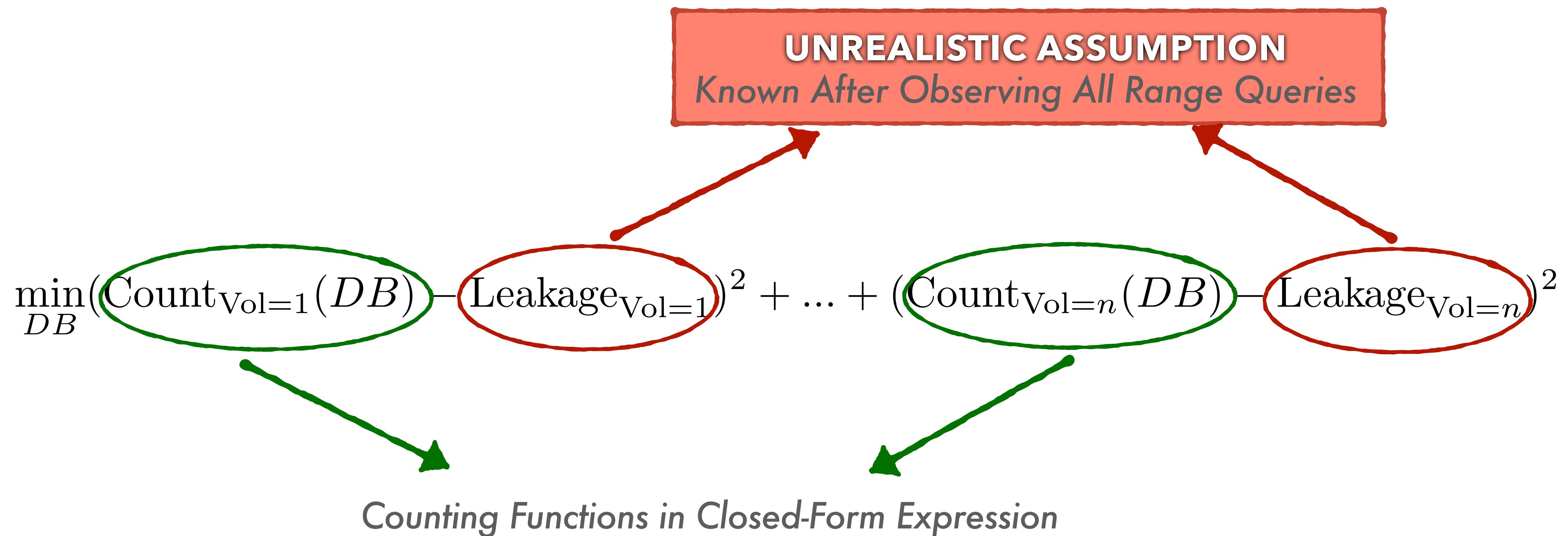
● NEW METHODOLOGY TO ATTACK PRACTICAL CONSTRUCTIONS

● AGNOSTIC TO QUERY DISTRIBUTION



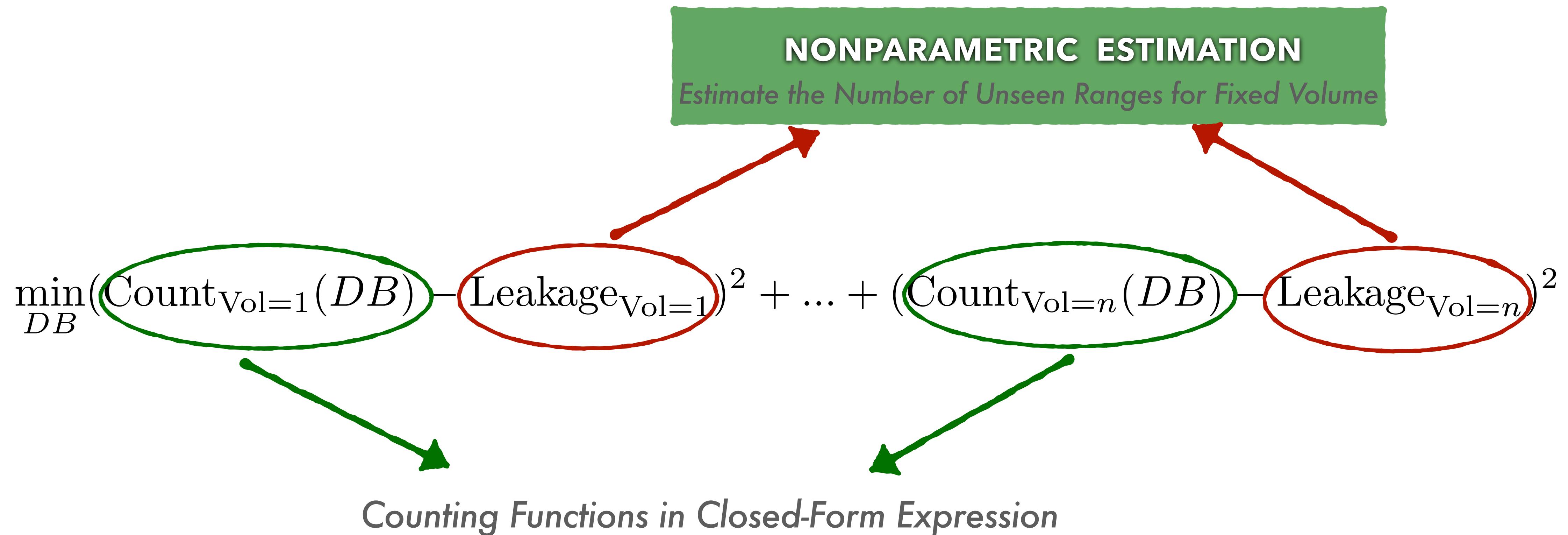
ATTACKS ON PRACTICAL CONSTRUCTIONS

ONLY A SUBSET OF RANGE QUERIES





ATTACKS ON PRACTICAL CONSTRUCTIONS ONLY A SUBSET OF RANGE QUERIES





EXPERIMENTS HOSPITAL DATABASE

Domain Density	Scheme	Attribute AGE		Attribute AGEDAY	
		Algo. 1 Attack	Oracle Attack	Algo. 1 Attack	Oracle Attack
5%	BASE	2.8	12.4	28.0	43.1
	ABT	2.1		28.5	
	BT	3.6		26.5	
10%	BASE	5.9	8.4	17.3	42.6
	ABT	6.0		17.9	
	BT	7.1		20.0	
25%	BASE	7.9	4.8	48.4	20.1
	ABT	8.0		49.2	
	BT	7.8		47.0	
50%	BASE	11.0	3.0	57.6	11.0
	ABT	11.1		42.0	
	BT	11.2		57.7	

TABLE III

PERFORMANCE OF OUR ATTACK FOR VARIOUS DATA DENSITIES ON ATTRIBUTES FROM HOSPITAL DATA OF HCUP [1]. THE QUALITY IS MEASURED AS THE MEAN ABSOLUTE ERROR (MAE PLAINTEXT).



CRYPTANALYSIS ON HARDENED RANGES RESPONSE-HIDING CONSTRUCTIONS ARE VULNERABLE TOO

Response-Hiding Encrypted Ranges: Revisiting Security via Parametrized Leakage-Abuse Attacks

Eugenios M. Kornaropoulos
UC Berkeley
eugenios@berkeley.edu

Charalampos Papamanthou
University of Maryland
csp@umd.edu

Roberto Tamassia
Brown University
rt@cs.brown.edu

Abstract—Despite a growing body of work on leakage-abuse attacks for encrypted databases, attacks on practical response-hiding constructions are yet to appear. Response-hiding constructions are superior in that they *nullify access-pattern based attacks* by returning only the search token and the result size of each query. Response-hiding schemes are vulnerable to existing volume attacks, which are, however, based on strong assumptions such as the uniformity query assumption or the dense database assumption. More crucially, these attacks only apply to schemes that cannot be deployed in practice (and over practical usage) and increased leakage when practical response-hiding schemes (Demertzis et al. [SIGMOD'16] and Falsi et al. [ESORICS'15]) have linear storage and less leakage. Due to these shortcomings, the value of existing volume attacks on response-hiding schemes is unclear.

In this work, we close the aforementioned gap by introducing a parametrized leakage-abuse attack that applies to *practical response-hiding structured encryption schemes*. The use of non-parametric estimation techniques makes our attack agnostic to both the data and the query distribution. At the very core of our technique lies the newly defined concept of a *counting function with respect to a range scheme*. We propose a two-phase framework to approximate the counting function for any range scheme. By simply switching our counting function for another, i.e., the smaller “parameter” of our modular attack, an adversary can attack different encrypted range schemes. We propose a constrained optimization formulation for the attack algorithm that is based on the counting functions. We demonstrate the effectiveness of our leakage-abuse attack on synthetic and real-world data under various scenarios.

INTRODUCTION

The notion of *searchable encryption*, introduced by Song-Wagner-Panigrahi in [37], proposes cryptographic schemes in which a client encrypts a privacy-sensitive data collection and outsources this resulting encrypted database to a server that efficiently answers search queries without ever decrypting the database. Since then, there has been a surge of research on this subject addressing issues such as improved definitions [9], dynamic constructions [23], [34], forward and backward privacy [4], [5], [7], [10], and locality of encrypted records [3], [11], [14]. For an overview of the area, see the survey by Fuller et al. [17]. In this work, we are interested in the general definitional framework called *Structured Encryption* (STE) introduced by Chase and Katzmaier [8] and, more specifically, schemes that support encrypted range queries [6], [13], [15].

To balance efficiency and privacy, STE schemes reveal some information about the query and its corresponding response. This information is called *leakage profile*. These schemes cryptographically guarantee that nothing more is revealed beyond what the designer allowed via the leakage profile.

RESPONSE-HIDING ENCRYPTED RANGES: REVISITING SECURITY VIA PARAMETRIZED LEAKAGE-ABUSE ATTACKS

KORNAROPOULOS, PAPAMANTHOU, TAMASSIA

Proc. IEEE SECURITY & PRIVACY , 2021

● RESTRICTED LEAKAGE: ONLY SEARCH-PATTERN & VOLUME

● NEW METHODOLOGY TO ATTACK PRACTICAL CONSTRUCTIONS

● AGNOSTIC TO QUERY DISTRIBUTION