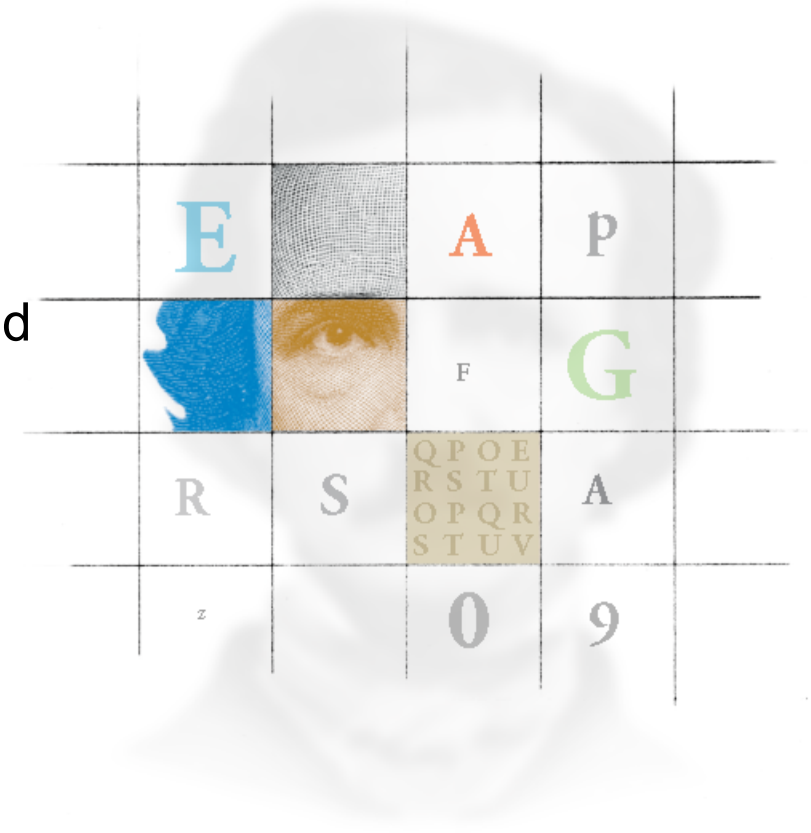
RSACONFERENCE2009

Short Redactable Signatures for Strings using Random Trees

Ee-Chien Chang, Chee-Liang Lim and Jia Xu

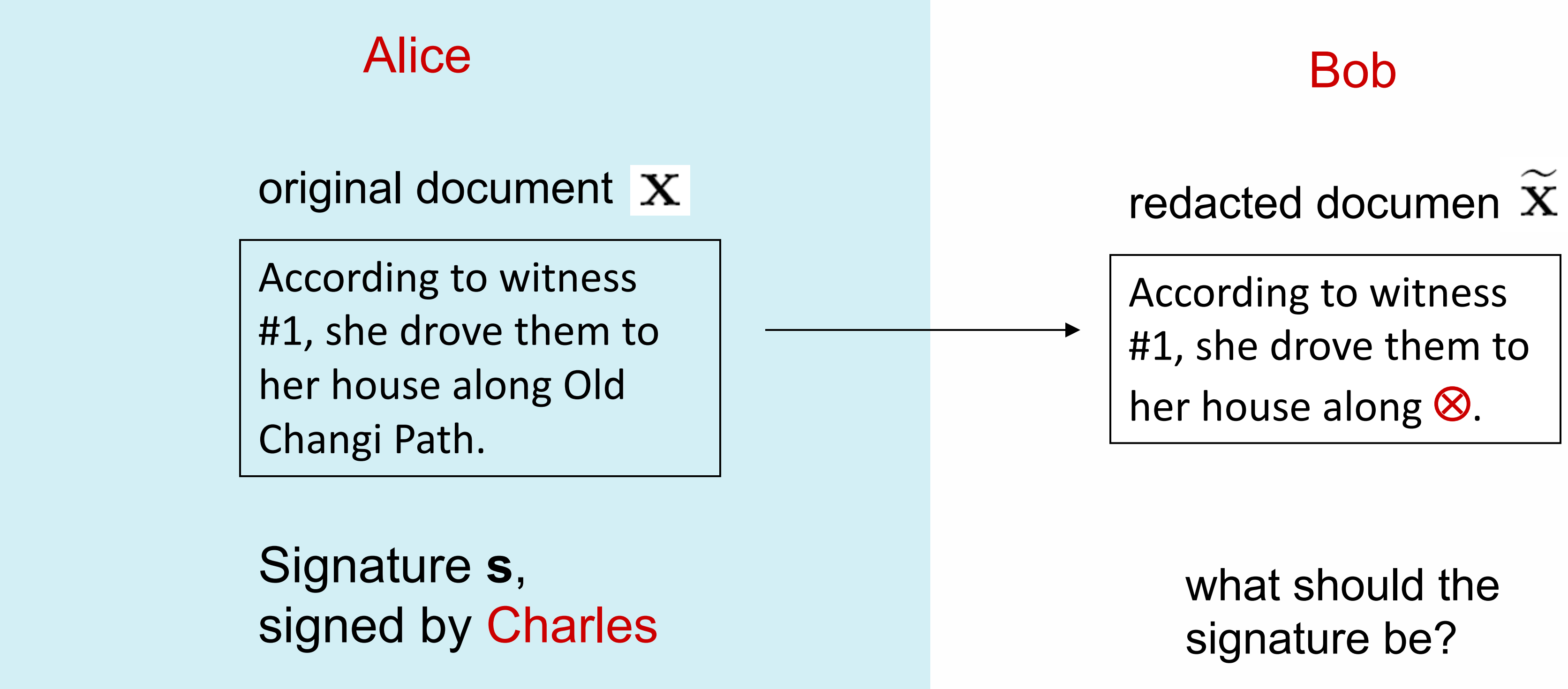
School of Computing
National University of Singapore

04/21/09 | Session ID:CRYP108



Introduction

Redactable Signature Scheme



Alice

original document $\mathbf{x}$

According to witness #1, she drove them to her house along Old Changi Path.

Signature **s**, signed by Charles

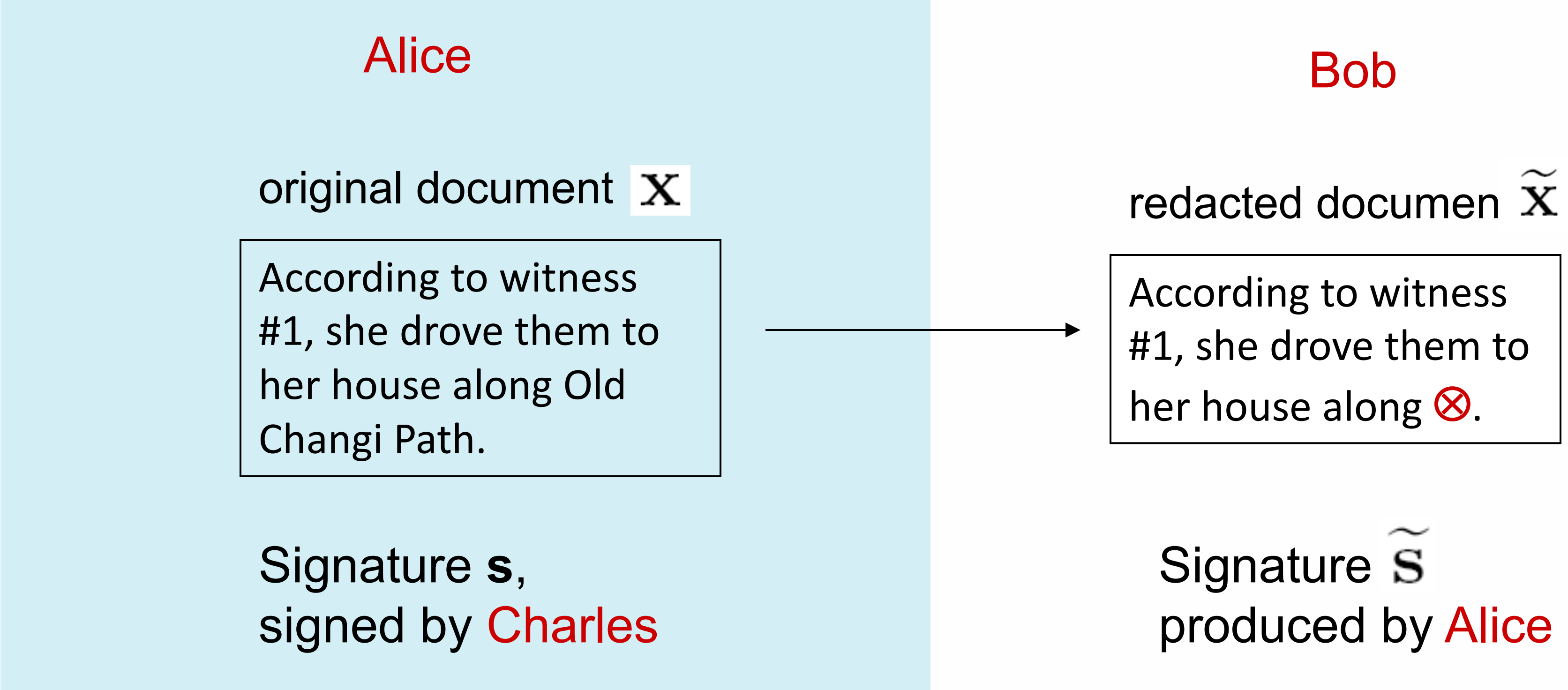
Bob

redacted documen $\tilde{\mathbf{x}}$

According to witness #1, she drove them to her house along ⊗.

what should the signature be?

Redactable Signature Scheme



Alice

original document $\mathbf{x}$

According to witness #1, she drove them to her house along Old Changi Path.

Signature **s**,
signed by Charles

Bob

redacted documen $\tilde{\mathbf{x}}$

According to witness #1, she drove them to her house along $\otimes$.

Signature $\tilde{\mathbf{s}}$
produced by Alice

1) (Authenticity) Bob can verify that $\tilde{\mathbf{x}}$ is indeed a document signed by Charles and properly redacted by Alice.

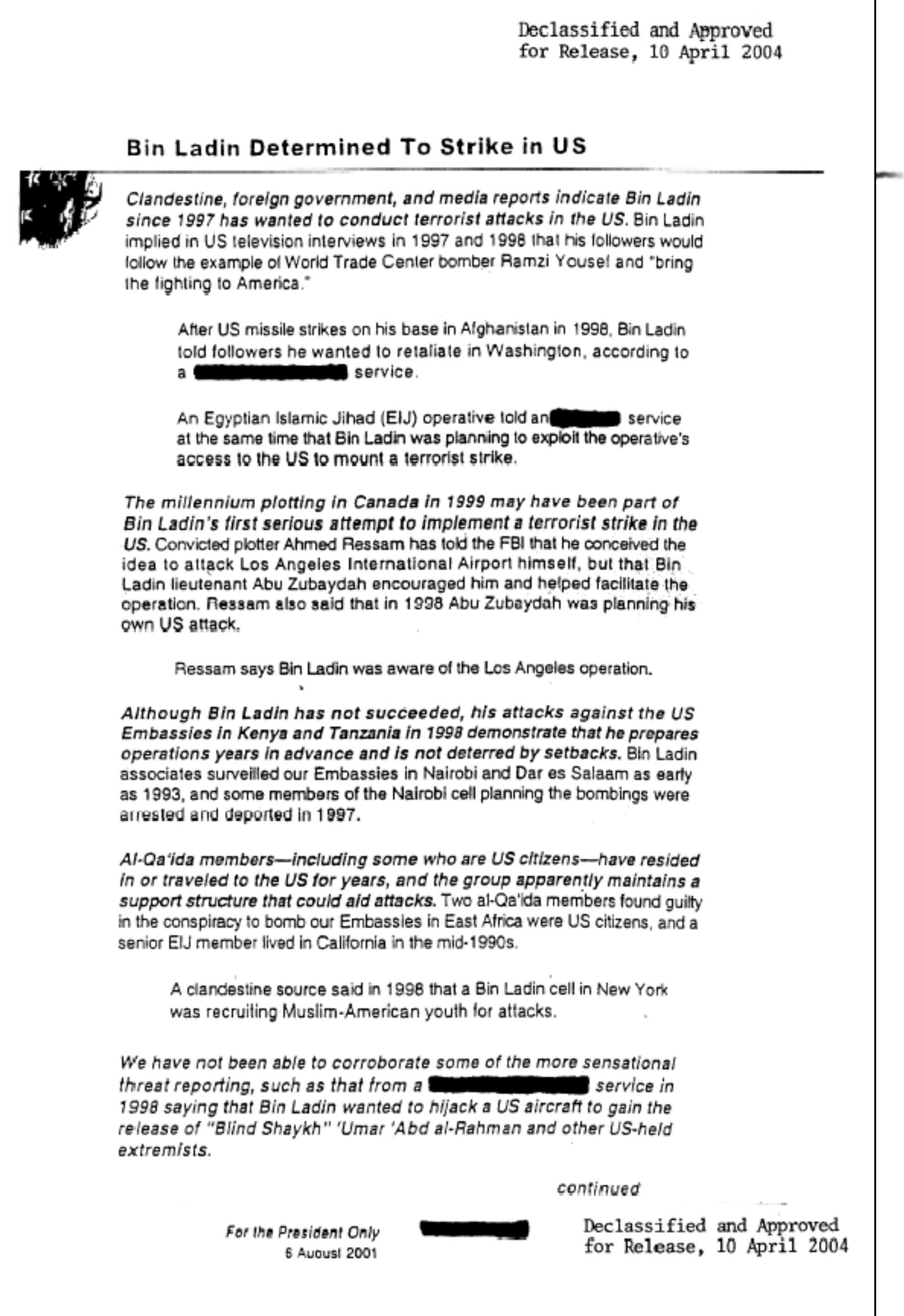
2) **(Privacy)** Bob is unable to obtain any information of the removed string.

- Existing schemes leak an important piece of information: the length of the removed substrings.

- The "length" can reveal crucial information, especially when the entropy of the removed string is low.

- Example: "Approved" vs "Not Approved"

A well known example.



Declassified and Approved
for Release, 10 April 2004

Bin Ladin Determined To Strike in US

Clandestine, foreign government, and media reports indicate Bin Ladin since 1997 has wanted to conduct terrorist attacks in the US. Bin Ladin implied in US television interviews in 1997 and 1998 that his followers would follow the example of World Trade Center bomber Ramzi Yousef and "bring the fighting to America."

> After US missile strikes on his base in Afghanistan in 1998, Bin Ladin told followers he wanted to retaliate in Washington, according to a [redacted] service.
>
> An Egyptian Islamic Jihad (EIJ) operative told an [redacted] service at the same time that Bin Ladin was planning to exploit the operative's access to the US to mount a terrorist strike.

The millennium plotting in Canada in 1999 may have been part of Bin Ladin's first serious attempt to implement a terrorist strike in the US. Convicted plotter Ahmed Ressam has told the FBI that he conceived the idea to attack Los Angeles International Airport himself, but that Bin Ladin lieutenant Abu Zubaydah encouraged him and helped facilitate the operation. Ressam also said that in 1998 Abu Zubaydah was planning his own US attack.

> Ressam says Bin Ladin was aware of the Los Angeles operation.

Although Bin Ladin has not succeeded, his attacks against the US Embassies in Kenya and Tanzania in 1998 demonstrate that he prepares operations years in advance and is not deterred by setbacks. Bin Ladin associates surveilled our Embassies in Nairobi and Dar es Salaam as early as 1993, and some members of the Nairobi cell planning the bombings were arrested and deported in 1997.

Al-Qa'ida members—including some who are US citizens—have resided in or traveled to the US for years, and the group apparently maintains a support structure that could aid attacks. Two al-Qa'ida members found guilty in the conspiracy to bomb our Embassies in East Africa were US citizens, and a senior EIJ member lived in California in the mid-1990s.

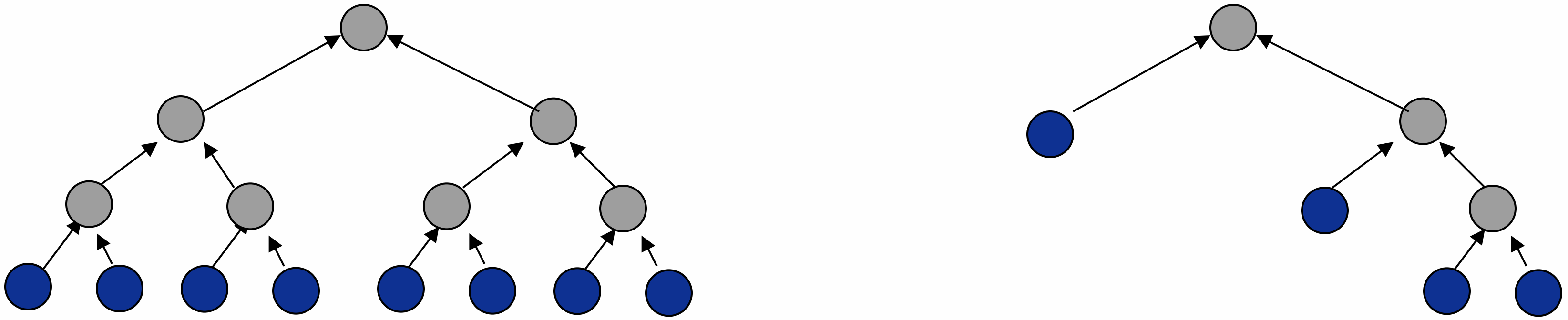
> A clandestine source said in 1998 that a Bin Ladin cell in New York was recruiting Muslim-American youth for attacks.

We have not been able to corroborate some of the more sensational threat reporting, such as that from a [redacted] service in 1998 saying that Bin Ladin wanted to hijack a US aircraft to gain the release of "Blind Shaykh" 'Umar 'Abd al-Rahman and other US-held extremists.

continued

Existing Scheme

- Based on Merkle Tree & GGM. (*Johnson et al.*)



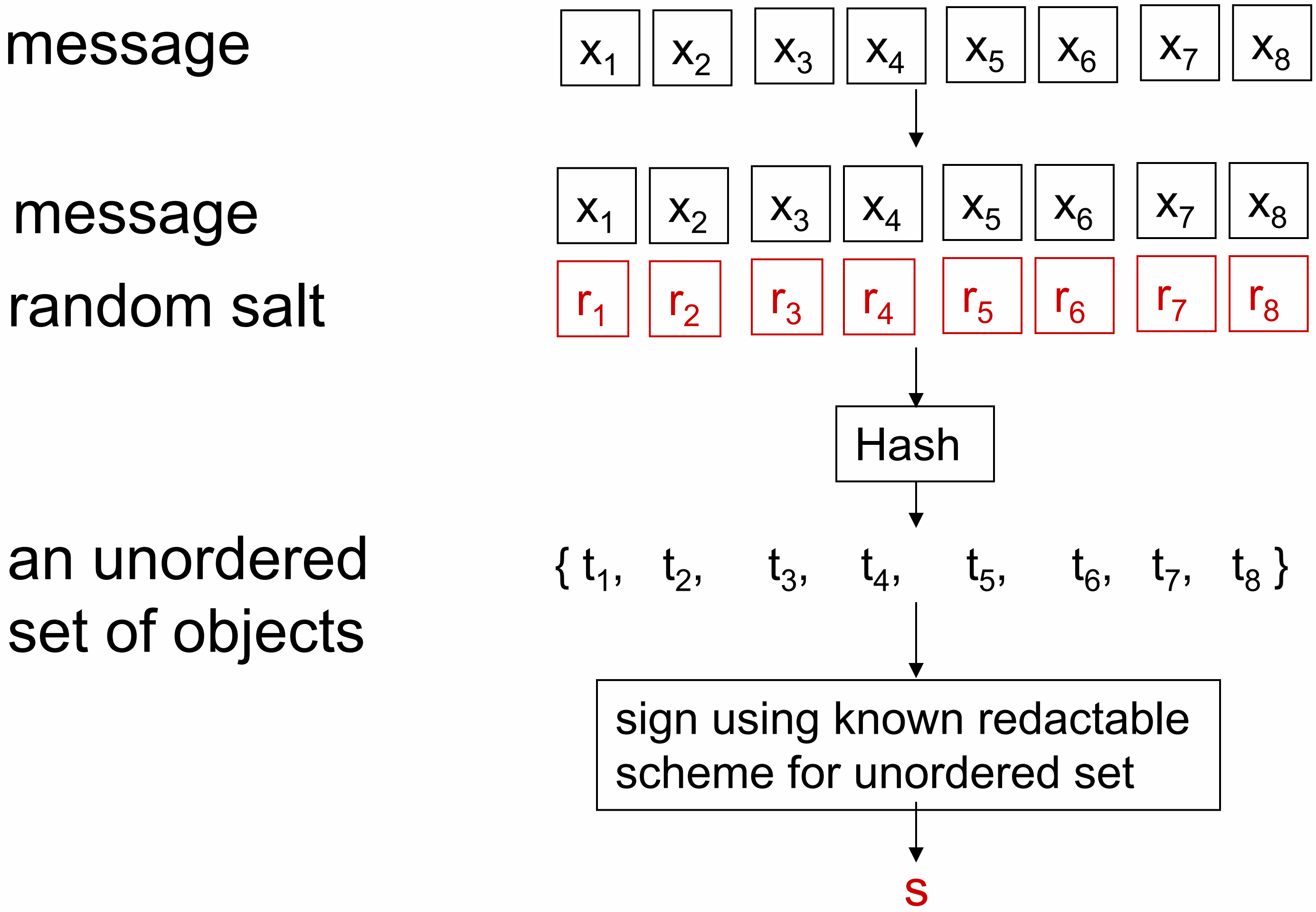
- Designed for unordered set (*Miyazaki et al & Johnson et al*.)

$\{x_1, x_2, x_3, x_4, x_5\} \longrightarrow \delta$

$\{x_1, x_2,$ [redacted] $x_5\} \longrightarrow \tilde{\delta}$

Our approach

Our approach



message

x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8

message

x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8

random salt

r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8

Hash

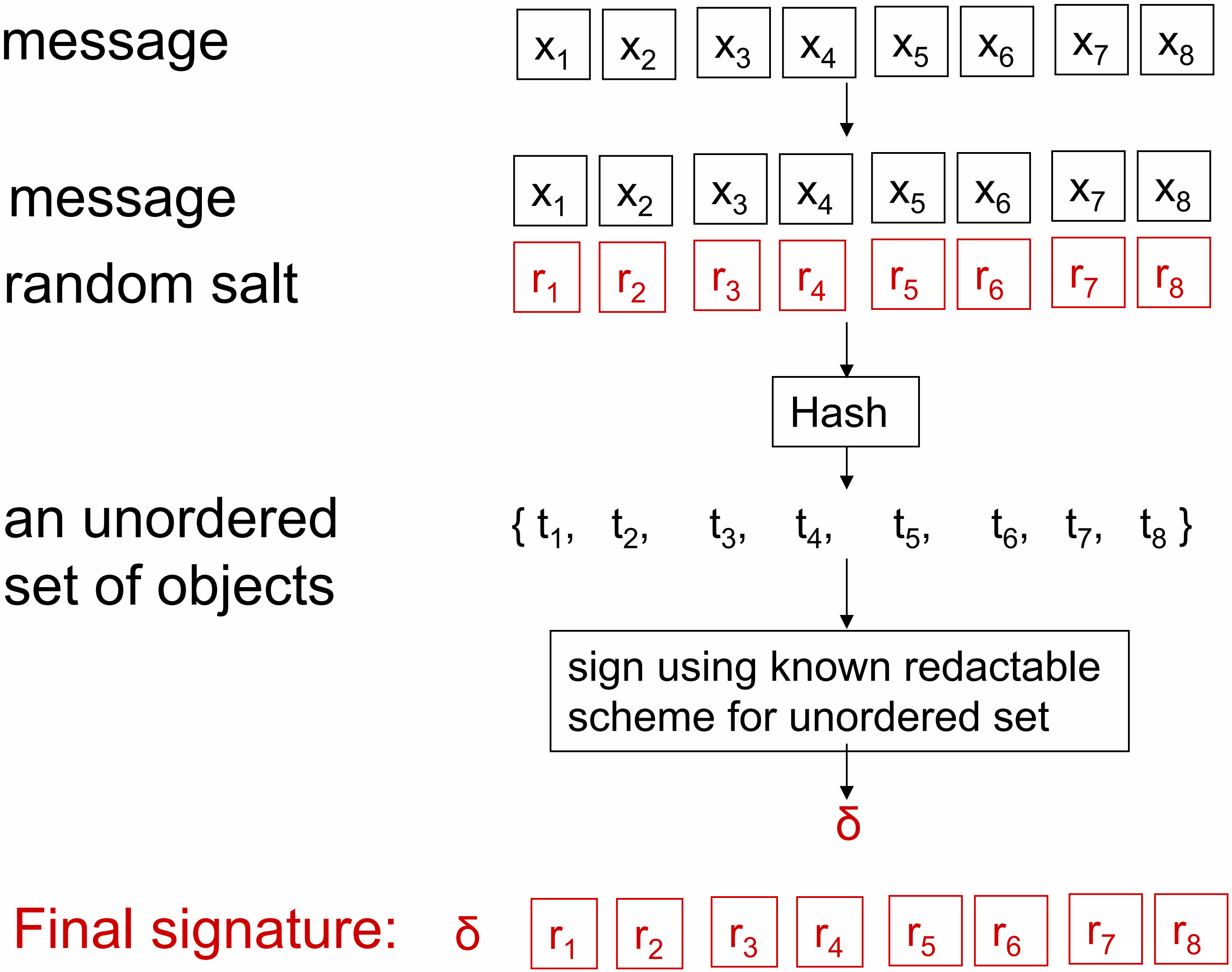
an unordered set of objects

$\{ t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8 \}$

sign using known redactable scheme for unordered set

s

Signature generation



message x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8

message x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8

random salt r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8

Hash

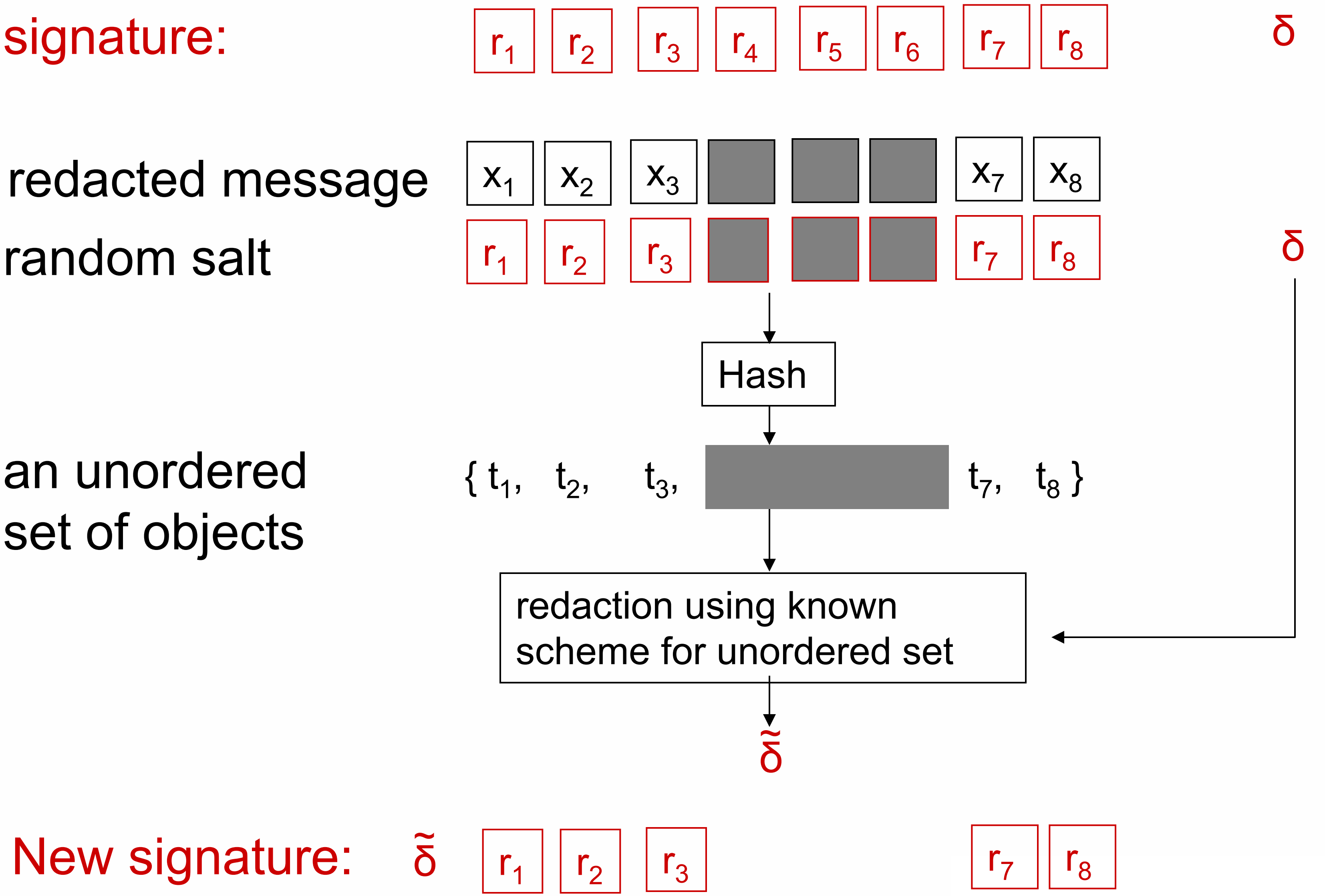
an unordered set of objects $\{ t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8 \}$

sign using known redactable scheme for unordered set

δ

Final signature: δ r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8

Redaction



signature: r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 δ

redacted message x_1 x_2 x_3 x_7 x_8

random salt r_1 r_2 r_3 r_7 r_8 δ

Hash

an unordered set of objects $\{ t_1, t_2, t_3, t_7, t_8 \}$

redaction using known scheme for unordered set

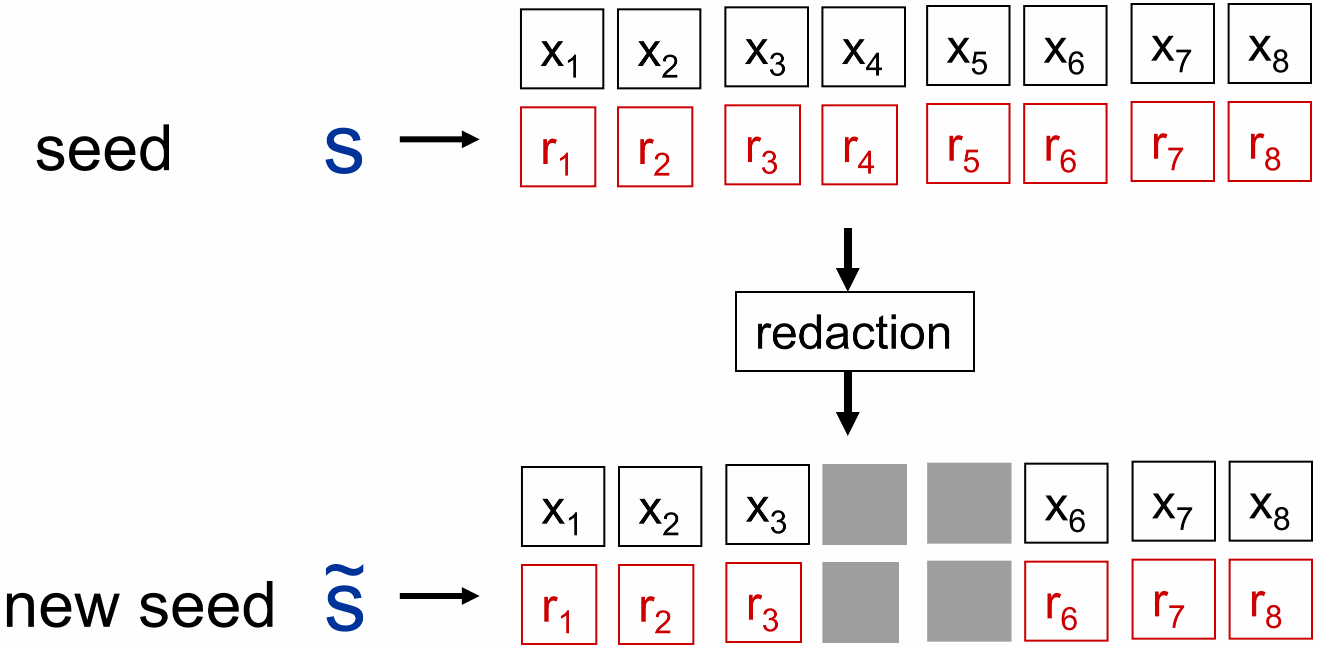
$\tilde{\delta}$

New signature: $\tilde{\delta}$ r_1 r_2 r_3 r_7 r_8

RSACONFERENCE2009

Signature size

- Size of signature too large.
- Need a method to generate the sequence of random number from a short seed, and yet able to hide the removed numbers.


x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8
seed
s
r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8
redaction
x_1 x_2 x_3 x_6 x_7 x_8
new seed
$\tilde{s}$
r_1 r_2 r_3 r_6 r_7 r_8

Problems to be solved

In order to implement the abovementioned approach, we require

- a "collision-resistant" hash that maps a string of objects to an unordered set of objects, and
- a method to generate a sequence of pseudo numbers s.t. a new seed for the redacted sequence can be efficiently computed.

Contributions (1)

- We give a redactable scheme that is able to hide the length of each redacted strings. The size of the signature is in

$$k + O(t \log n)$$

  where $t \geq 1$ is the number of substrings redacted, n is the size of the original document, and k the size of an underlying known redactable signature scheme for unordered set.

- The scheme consists of 2 components:

  - A "collision-resistant" function that maps an ordered sequence to an un-ordered set.

  - A random-tree based PRNG that achieves a hiding property.

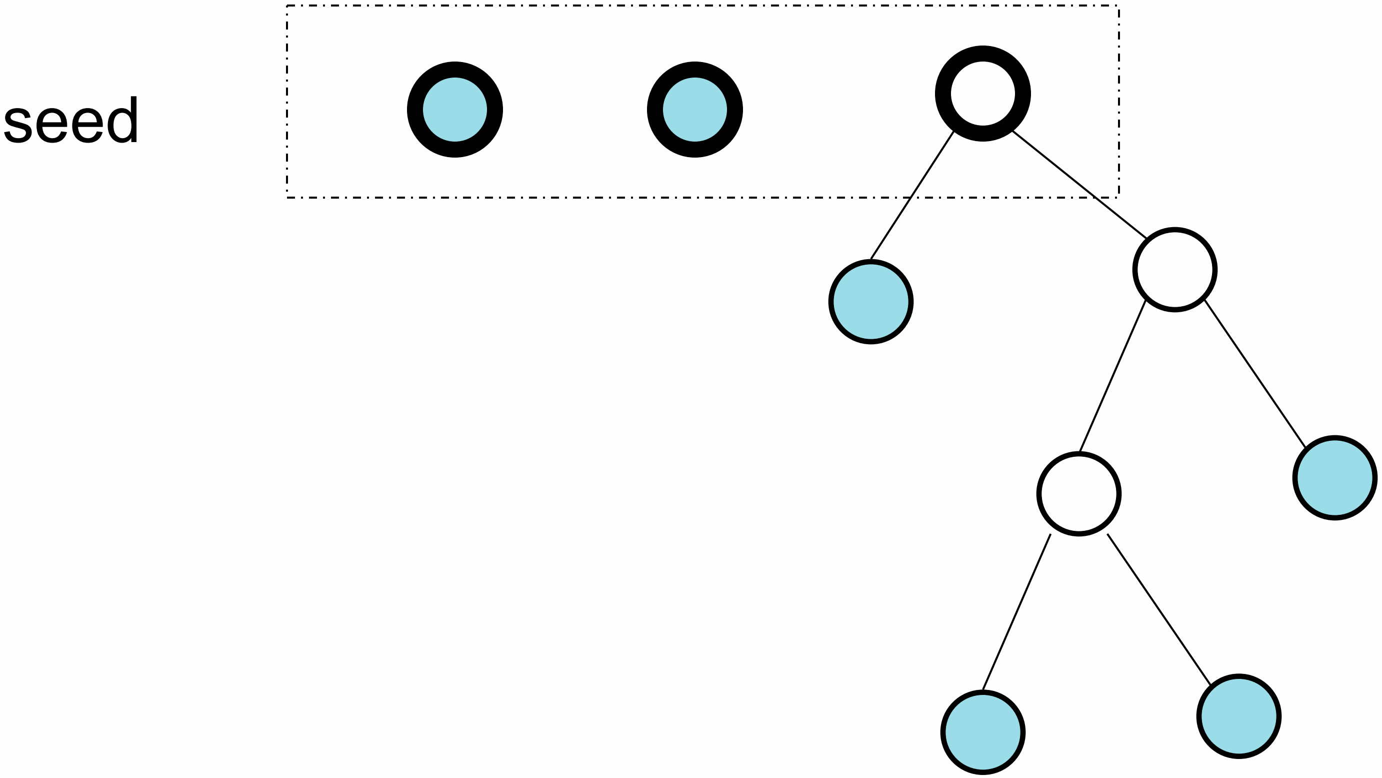
Contributions (2)

- We observe a hiding property of a random tree. Based on the observation, we propose RGGM, a pseudo random number generator that
  - If multiple substrings of pseudo random numbers are to be removed, we can efficiently find a new seed that generates the retained numbers, and
  - yet it is computationally difficult to derive the content or length of each removed substring from the new seed, except the locations of the removed substrings.

Random tree oblivious to deletion

Random GGM

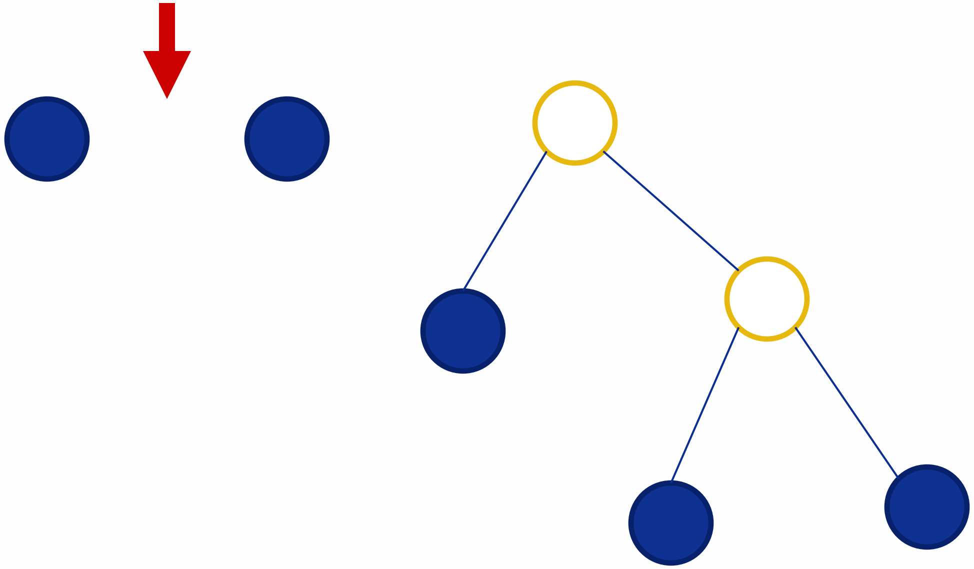
Generate a sequence of pseudo random numbers from seeds



Consider a game between Alice and Bob.

- Bob chooses a tree *T*, with either 6 or 100 leaves.
- Bob removes a sequence of consecutive leaves and their ancestors, such that the resulting forest *T′* has 5 leaves.
- Bob shows Alice the redacted *T′.*
- Alice wants to guess the initial number of leaves in *T.*

unknown number of leaves are removed here.



Given this forest,
Alice wants to guess the initial number of leaves.

We propose a way to generate the tree such that Alice is unable to succeed with probability better than ½.   Note that this is an information-theoretic result.

Conclusion

- We provide a redactable signature scheme that is able to hide the length of the redacted strings, and the signature size is small.
- The scheme consists of two components: (1) a hash that maps ordered sequence to unordered set, and (2) Randomized GGM tree.
- The randomized GGM tree exploits an intriguing statistical property of a random tree. The random tree is oblivious to previous deletion.

Apply Slide

- Ordering information in the string can be treated as "combinatorics structure".

- We applied combinatorics techniques to solve this problem in cryptography.