Verifiable Member and Order Queries on a List in Zero Knowledge

Esha Ghosh

Brown University

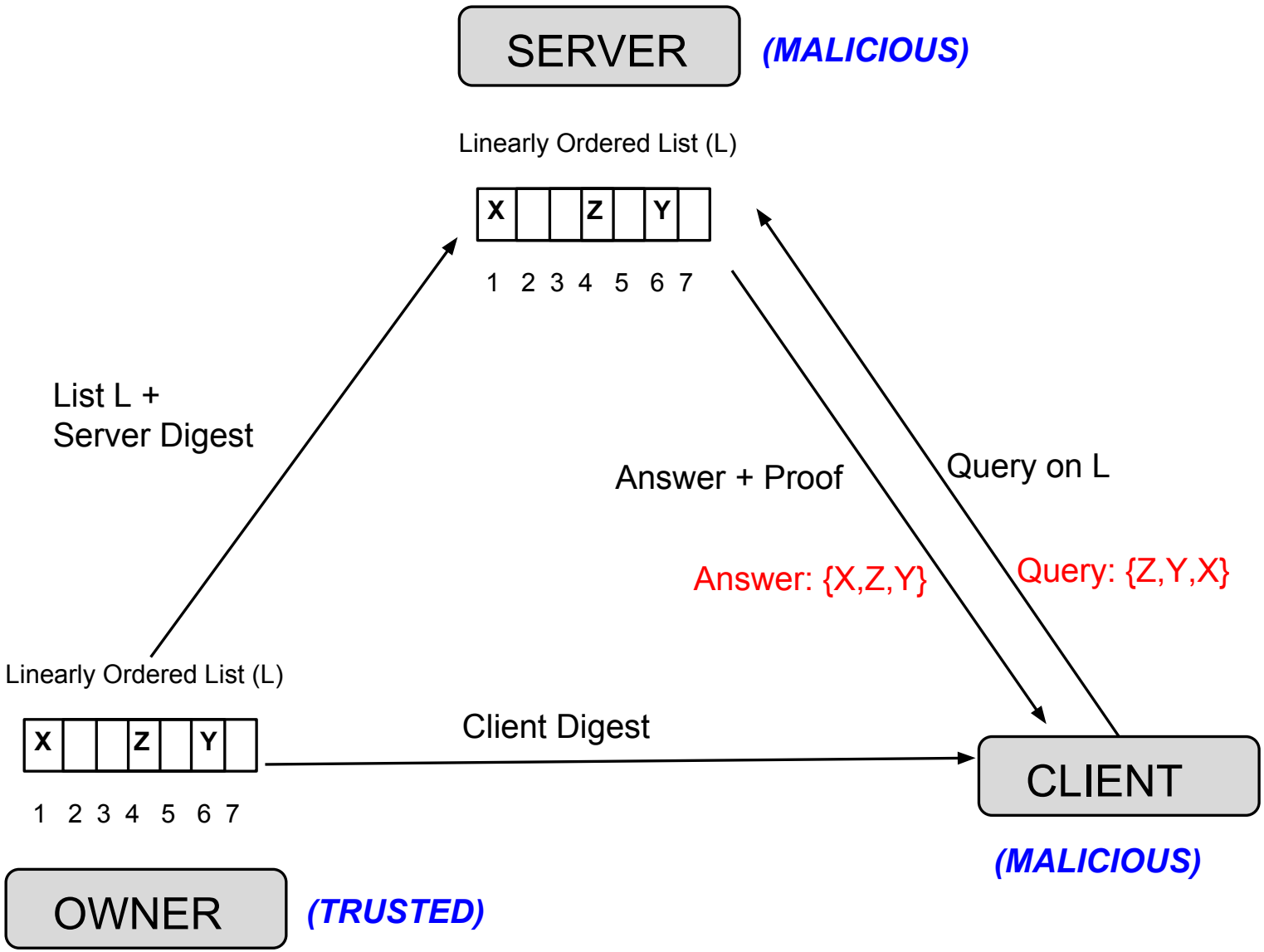
Joint work with:
Olga Ohrimenko, Microsoft Research
Roberto Tamassia, Brown University

August 19, 2014

Selectively revealing health record [BB12]

Vaccine	Date given (mm/dd/yyyy)	Administered by
Hepatitis B		
Diptheria, Tetanus		
Haemophilus influenzae type b		
Polio		
Rotavirus		
Measles, Mumps and Rubella		
Varicella		
Hepatitis A		
Meningococcal		
Human papillomavirus		

Model - Privacy Preserving Authenticated List (PPAL)



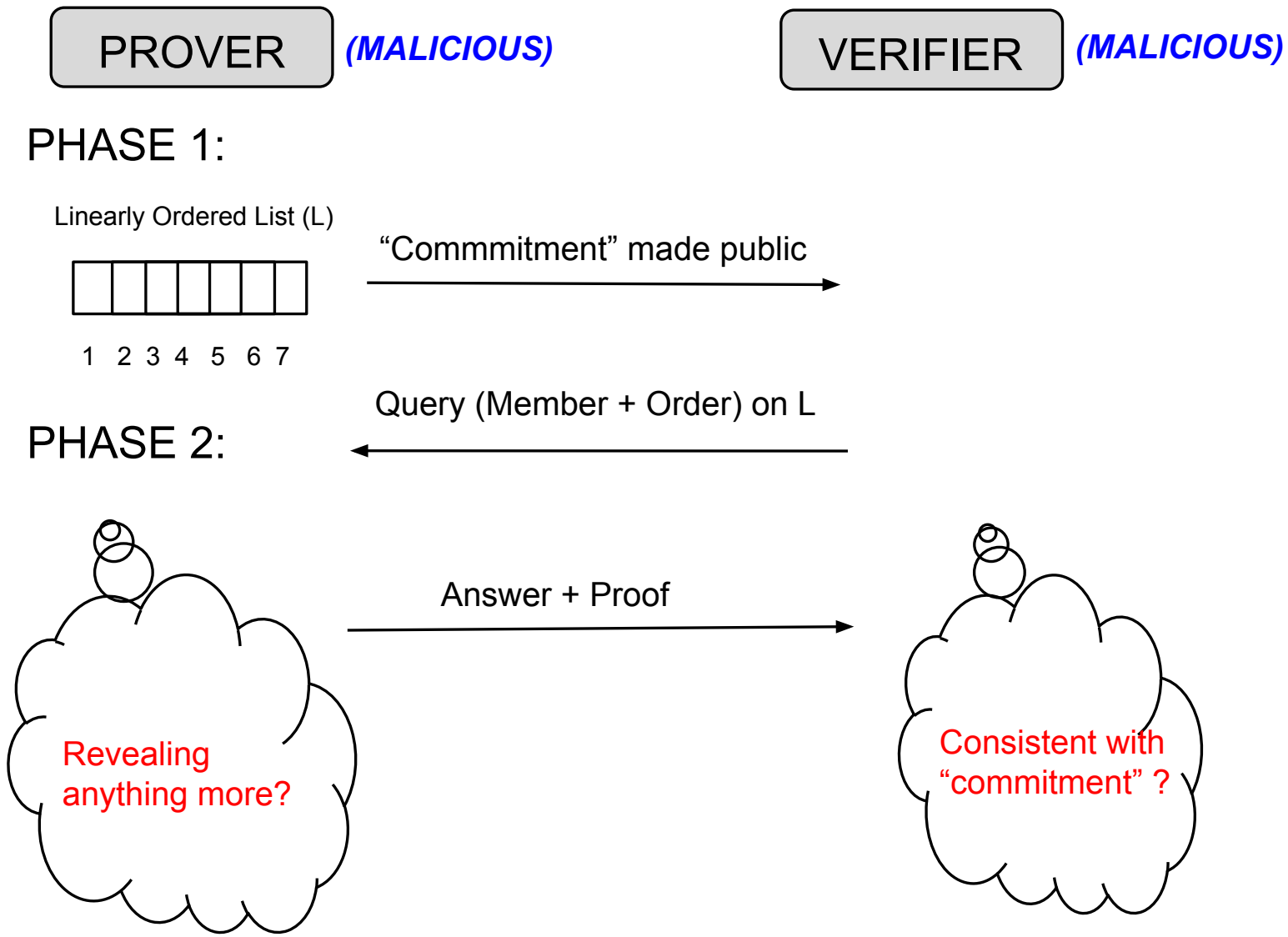
Security Properties - PPAL

Completeness: Honestly generated proofs are always accepted by the client.

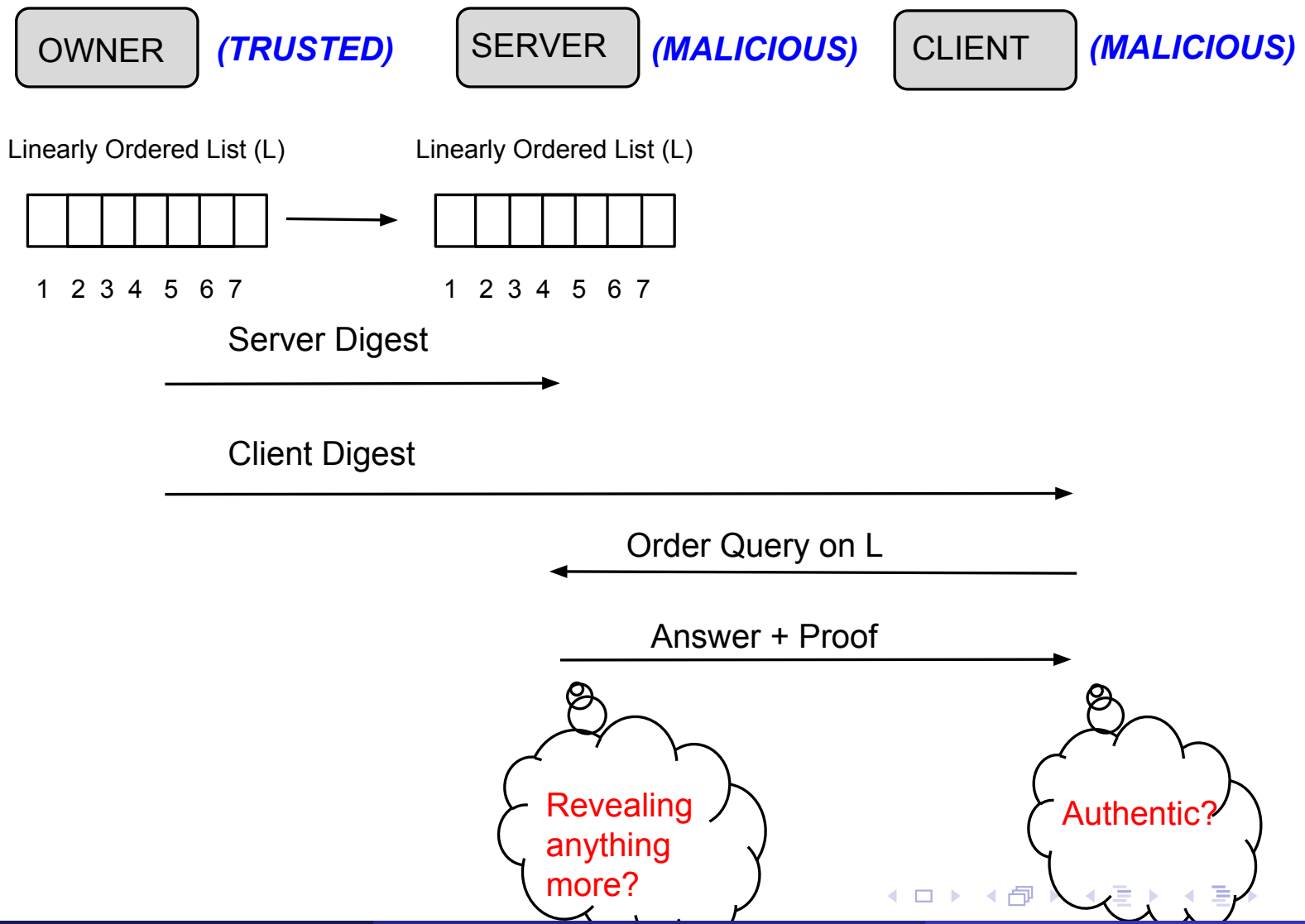
Soundness: Proofs forged by the server for incorrect answers to queries do not pass the verification.

Zero-Knowledge: Proofs do not reveal anything beyond the answers, i.e., the proofs are simulatable.

Solution 1: Zero-Knowledge List (ZKL)



Solution 2: Direct Privacy-Preserving Authenticated List (PPAL) Construction



Efficiency Comparison:

Notations:

n = List size

m = Query size

k = Security parameter

	Time Complexity		Space Complexity	
	via ZKL	PPAL	via ZKL	PPAL
Owner (Setup)	$O(kn)$	$O(n)$	$O(kn)$	$O(n)$
Server (Query)	$O(km)$	$O(min\{m \log n, n\})$[1]	$O(kn)$	$O(n)$
Client (Verify)	$O(km)$	$O(m)$	$O(km)$	$O(m)$

[1] With preprocessing time $O(n)$

How we compare

	[SBZ01]	[JMSW02]	[CLX09]	[BBD+10]	[SPB+12]	[PSPDM12]	[KAB12]	This Work
Zero-Knowledge				✓	✓	✓		✓
Setup time	$n \log n$	n	n	n^2	n^2	n	n	n
Space	n	n	n	n^2	n^2	n	n^2	n
Query time	m	$n \log n$	n	mn	m	n	n	$\min(m \log n, n)$
Verification time	$m \log n \log m$	$m \log n$	n^2	m^2	m^2	m	m	m
Proof size	m	$m \log n$	n	m^2	m^2	m	n	m
Assumption	RSA	RSA	SRSA, Division	EUCMA	ROH, nEAE	AnAHF	ROH, RSA	ROH,nBDHI

Table: Comparison of our construction of a privacy-preserving authenticated list with previous work. All the time and space complexities are asymptotic. Notation: n is the number of elements of the list, m is the number of elements in the query. Acronyms for the assumptions: Associative non-abelian hash function (AnAHF); Bilinear Diffie Hellman Inversion Assumption (BDHI) n-Bilinear Diffie Hellman Inversion Assumption and n-weak Bilinear Diffie Hellman Inversion Assumption (Decisional) (nBDHI); n-Element Aggregate Extraction Assumption (nEAE); Existential Unforgeability under Chosen Message Attack (EUCMA) of the underlying signature scheme; Random Oracle Hypothesis (ROH); Strong RSA Assumption (SRSA);

References

Jordan Brown and Douglas M. Blough.
Verifiable and redactable medical documents.
AMIA Annu Symp Proc, pages 1148 – 1157, 2012.

Ron Steinfeld, Laurence Bull, and Yuliang Zheng.
Content extraction signatures.
In *Int. Conf. on Information Security and Cryptology (ICISC)*, volume 2288 of *LNCS*, pages 285–304. Springer, 2001.

Robert Johnson, David Molnar, Dawn Xiaodong Song, and David Wagner.
Homomorphic signature schemes.
In *Proc. RSA Conf. — Cryptographer's Track (CT-RSA)*, LNCS, pages 244–262, London, UK, UK, 2002. Springer.

Ee-Chien Chang, Chee Liang Lim, and Jia Xu.
Short redactable signatures using random trees.
In *Proc. RSA Conf. — Cryptographer's Track (CT-RSA)*, LNCS, pages 133–147, Berlin, Heidelberg, 2009. Springer.

Christina Brzuska, Heike Busch, Ozgur Dagdelen, Marc Fischlin, Martin Franz, Stefan Katzenbeisser, Mark Manulis, Cristina Onete, Andreas Peter, Bertram Poettering, and Dominique Schröder.
Redactable signatures for tree-structured data: Definitions and constructions.
In *ACNS*, pages 87–104, 2010.

Kai Samelin, Henrich C. Poehls, Arne Bilzhause, Joachim Posegga, and Hermann De Meer.
Redactable signatures for independent removal of structure and content.
In *Proc. Int. Conf. on Information Security Practice and Experience (ISPEC)*, volume 7232 of *LNCS*. Springer, 2012.

Henrich C. Poehls, Kai Samelin, Joachim Posegga, and Hermann De Meer.
Length-hiding redactable signatures from one-way accumulators in $O(n)$.
Technical Report MIP-1201, Faculty of Computer Science and Mathematics (FIM), University of Passau, 2012.

Ashish Kundu, Mikhail J. Atallah, and Elisa Bertino.
Leakage-free redactable signatures.
In *Proc. ACM Conf. on Data and Application Security and Privacy (CODASPY)*, pages 307–316, 2012.

Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham.
Aggregate and verifiably encrypted signatures from bilinear maps.
In *Advances in cryptology - EUROCRYPT 2003*, pages 416–432. Springer, 2003.

Dan Boneh and Xavier Boyen.
Efficient selective-id secure identity based encryption without random oracles.
In *Proceedings of Eurocrypt 2004, volume 3027 of LNCS*, pages 223–238. Springer-Verlag, 2004.

Dan Boneh, Xavier Boyen, and Eu-Jin Goh.
Hierarchical identity based encryption with constant size ciphertext.
In *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 440–456.
Berlin: Springer-Verlag, 2005.

Paper at: `http://arxiv.org/abs/1408.3843`

Thank you!