The Title of Your Paper

Clever Student
1234567a

Abstract

Anonymous broadcast functionality $\mathcal{F}_R^K$

Initialise:

(1) a list of pending messages $L_{pend} \leftarrow []$
(2) $status_P \in \{0,1\} \leftarrow 0$ for party P indicating whether P has sent a message in the current round

■ Upon receiving (**sid**, **WRITE**, M) from honest party P or (**sid**, **WRITE**, M, P) from S on behalf of corrupted party P:
If $status_P = 0$, then

(1) set $status_P \leftarrow 1$
(2) append M to L_{pend}
(3) if $|L_{pend}| = K$, then
   (a) order the messages lexicographically as $< M_1, ..., M_K >$
   (b) set $Lpend \leftarrow []$
   (c) set $status_P \leftarrow 0$ for every P
   (d) send (**sid**, **BROADCAST**, $< M_1, ...M_K >$ to all parties and (**sid**, **BROADCAST**, $< M_1, ...M_K >, P$) to S
(4) else, send (**sid**, **WRITE**, $|M|$, P) to S

Figure 1: Anonymous broadcast ideal functionality.

Riposte UC Protocol

Variables:

- R - number of rows in each database table
- C - length of messages
- e_l - R x C x 2 bitstring containing 0 everywhere except in row l which contains $(M, M^2) \in \mathbb{F}^k$, where M is the message to be sent
- K - message limit in a round

Initialise:

(1) $status_P \in \{0,1\} \leftarrow 0$ for party P indicating whether P has sent a message in the current round
(2) $count \in \mathbb{N} \leftarrow 0$ indicating the number of valid write requests received this round

■ Upon receiving (**sid**, **WRITE**, M) from P
If $status_P = 0$, then

(1) set $status_P \leftarrow 1$
(2) P chooses index $l \xleftarrow{\$} \{x|x \in \mathbb{N}, 0 \leq x < R\}$ and generates bitstring e_l
(3) generate random R x C x 2 bitstring r
(4) send (**prove**, P, e_l) to $\mathcal{F}_{ZK}^{R,R'}$
(5)
(6) send $r \oplus e_l$ to Server B using $\mathcal{F}_{\mathcal{AEC}}(\{A, B\})$
(7) send e_l to Server A using $\mathcal{F}_{\mathcal{AEC}}(\{A, B\})$
(8) $count$ += 1
(9) if $count = K$, then
   (a) set $status_p \leftarrow 0$
   (b) set $count \leftarrow 0$

■ Upon receiving (**sid**, **BROADCAST**, M_A) from Server A and (**sid**, **BROADCAST**, M_B) from Server B

(1) Verify that $M_A = M_B$
(2) If $M_A = M_B$, forward to $\mathcal{Z}$

■ Upon receiving (**sid**, **SEND**, $r \oplus e_l$) from P, if P has not executed a write request in this phase, then
Server B executes the following: DOES THE SERVER NEED TO WAIT FOR VERIFICATION FROM ZK HERE?

(1) XOR $r \oplus e_l$ into its database
(2) if $count = K$, then
   (a) combine database with Server A's database
   (b) check for collisions
   (c) resolve collisions
   (d) order messages lexicographically as $M_B =< M_1, ..., M_K >$
   (e) broadcast messages to all parties

■ Upon receiving (**sid**, **SEND**, e_l) from P, if P has not executed a write request in this phase, then
Server A executes the following:

(1) XOR e_l into its database
(2) if $count = K$, then
   (a) combine database with Server B's database
   (b) check for collisions
   (c) resolve collisions
   (d) order messages lexicographically as $M_A =< M_1, ..., M_K >$
   (e) broadcast messages to all parties

Figure 2: Anonymous broadcast protocol.

AE channel functionality $\mathcal{F}_{\mathcal{AEC}}(\{A, B\})$

Initialise a list $PendingMsg \leftarrow \emptyset$.
■ Upon receiving (**sid**, **SEND**, M) from P, if P is honest, then:

(1) If $\{A, B\} \backslash \{P\}$ is corrupted, then send (**sid**, **SEND**, M, P) to $\mathcal{S}$.
(2) If $\{A, B\} \setminus \{P\}$ is honest, then
   - Choose a random tag $\xleftarrow{\$} \{0, 1\}^{\lambda}$.
   - Add (**tag**, M, P) to *PendingMsg*
   - Send (**sid**, **SEND**, **tag**, $|M|$, P, {A,B} \ {P}) to $\mathcal{S}$.
(3) Upon receiving (**sid**, **ALLOW**, **tag**) from $\mathcal{S}$, if there is a (**tag**, M, P) in *PendingMsg*, then remove (**tag**, M, P) from *PendingMsg* and send (**sid**,**SEND**,M) to {A,B}\{P}

Figure 3: Anonymous broadcast ideal functionality.

Zero-knowledge functionality $\mathcal{F}_{ZK}^{R,R'}$

(1) Wait for an input (**prove,** y, w) from P such that $(y, w) \in R$ if P is honest, or $y, w \in R'$ if P is corrupt. Send (**prove**, l(y)) to $\mathcal{A}$. Further, wait for a message **ready** from V, and send **ready** to $\mathcal{A}$.
(2) Wait for message **lock** from $\mathcal{A}$.
(3) Upon receiving a message **done** from $\mathcal{A}$, send **done** to P. Further, wait for an input **proof** from $\mathcal{A}$ and send (**proof**, y) to V.

Corruption rules:

- If P gets corrupted after sending (**prove**, y, w) and before Step 2, $\mathcal{A}$ is given (y, w) and is allowed to change this value to any value $(y', w') \in R'$ at any time before Step 2.

Figure 4: Zero-knowledge functionality $\mathcal{F}_{ZK}^{R,R'}$

1 Introduction

This document is the LaTeXtemplate for submitting your final MSci project paper, at the School of Computing Science of the University of Glasgow. This is an updated version, starting for the academic year 2024/25. Please make sure to update your personal details, including title, name, and matriculation number, within the `%% STUDENT INFORMATION %%` section of the attached LaTeXsource file `main.tex`.

This template is directly derived from ACM's `acmart` package; make sure to consult the corresponding documentation if you face any technical issues, or if you want to explore the full range of features offered.

Unless you are already an experienced LaTeXuser, perhaps the most straightforward way to typeset your paper is to work directly on Overleaf; this is a cloud service (so no need for a local installation) which you can easily sign up for using your `@glasgow.ac.uk` email. Here is also a very useful LaTeX tutorial.

2 Background

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Perhaps you want to cite the seminal paper of Turing [3], or prior [2] and concurrent [1] work.

3 My Amazing System

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

4 Evaluation

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

4.1 Experimental Setup

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

4.2 Experimental Analysis

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

	machine A	machine B
CPU	Intel Core i7-9700 CPU	2x Intel Xeon E5-2630 v3
CPU Frequency	3.00GHz	2.40GHz
RAM	16GB DDR4	128GB
OS	Ubuntu 20.04 LTS	Ubuntu 16.04 LTS
Compiler	GCC 9.3	GCC 7.3
libm	v2.31	v2.23
libomp	v4.5	v4.5

Table 1: This is the table caption.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Our results are summarized in Table 1, and a visual representation of our analysis can be seen in **??**.

5 Conclusions

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Acknowledgments

I would like to thank …

References

[1] Alonzo Church. 1936. An Unsolvable Problem of Elementary Number Theory. *American Journal of Mathematics* 58, 2 (1936), 345–363. http://www.jstor.org/stable/2371045

[2] Kurt Gödel. 1931. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik* 38–38, 1 (Dec. 1931), 173—-198. doi:10.1007/bf01700692

[3] Alan M. Turing. 1937. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society* s2-42, 1 (1937), 230–265. doi:10.1112/plms/s2-42.1.230