Name: Yitian Shan

Student Number: 202118022

UOW Number: 7377587

Date: 2021/11/20

1.



2．

因为 P 下標 r 左中括號 m 等於 m 下標 i 的 星號乘 次方 結束下標 右中括號 等於 分數 Q 下標 r o 結束下標 分之 1
s o 逗號 A D V 下標 c o 減 C D H 結束下標 大于或等于 （ 倾斜 ） 分數 Q 下標 r o 結束下標 分之 1 乘 A D V 下標 S I G 結束下標
向右箭头 A D V 下標 S I G 結束下標 小于或等于 （ 倾斜 ） Q 下標 r o 結束下標 乘 A D V 下標 c o 減 C D H 結束下標

因为 P 下標 r 左中括號 m 等於 m 下標 i 的 星號乘 次方 結束下標 右中括號 等於 分數 Q 下標 r o 結束下標 分之 1
s o 逗號 A D V 下標 c o 減 C D H 結束下標 大于或等于 （ 倾斜 ） 分數 Q 下標 r o 結束下標 分之 1 乘 A D V 下標 S I G 結束下標
向右箭头 A D V 下標 S I G 結束下標 小于或等于 （ 倾斜 ） Q 下標 r o 結束下標 乘 A D V 下標 c o 減 C D H 結束下標因为 P 下標 r 左中括號 m 等於 m 下標 i 的 星號乘 次方 結束下標 右中括號 等於 分數 Q 下標 r o 結束下標 分之 1
s o 逗號 A D V 下標 c o 減 C D H 結束下標 大于或等于 （ 倾斜 ） 分數 Q 下標 r o 結束下標 分之 1 乘 A D V 下標 S I G 結束下標
向右箭头 A D V 下標 S I G 結束下標 小于或等于 （ 倾斜 ） Q 下標 r o 結束下標 乘 A D V 下標 c o 減 C D H 結束下標

So BLS signature scheme is secure assuming coCDH assumption holds in pairing and is model as a random oracle.