一种简单的加密通信方案

史鹏程 伍孝飞 杜扬帆

(东北大学 计算机科学与工程学院，沈阳 110169)

摘 要 信息安全一直是关乎民生和国家的头等大事，为了保证通信时的信息安全，多种加密方法已被广泛运用。本文中将给出一种方法，在存在可信第三方的前提下，结合 ElGamal 算法和 Diffie-Hellman 密钥交换算法，实现通信双方在不确定彼此成绩且不被外界确定的情况下，能够确定彼此成绩是否相同。具体将给出第三方知道双方成绩、知道其中一方成绩、不知道成绩信息的三种情况相应的算法设计和关于正确性、隐私性、安全性、公平性等方面的证明，最后说明了各个情况下的时间和空间复杂度。

关键词 加密；密码学；ElGamal 算法；Diffie-Hellman 密钥交换算法；通信方案；

中图法分类号 ****

A Simple Encryption Communication Protocol

SHI Peng-Cheng WU Xiao-Fei DU Yang-Fan

(School of Computer Science and Engineering, Northeastern University, Shenyang 110169, China)

Abstract Information security has always been the top priority for people's livelihood and the country. In order to ensure the information security in communication, a variety of encryption methods have been widely used. In this paper, we will present a method, which combines ElGamal algorithm and Diffie-Hellman Key Exchange algorithm under the premise of the existence of a trusted third party, so that both parties can determine whether their grades is the same under the condition that their grades are not determined by each other and the outside world. Specifically, we will give the corresponding algorithm design and proof of correctness, privacy, security, fairness and other aspects in three cases where the third party knows the score of both parties, knows the score of one party, and does not know the score information. Finally, it will explain the time and space complexity in each case.

Key words Encryption; Cryptography; ElGamal Cryptosystem; Diffie–Hellman Key Exchange; Communication Protocol

1 引言

1.1 问题引出

Alice 和 Bob 刚刚得知一门考试的成绩，他们都想知道两个人的成绩是否相同。但是，谁也不愿意暴露自己的成绩。假设成绩采用优、良、中、差四个等级。设计一种安全的游戏方案，使 Alice 和 Bob 在游戏中执行相应的算法，在不暴露自己成绩的前提下判定二人成绩是否相同。

为了得到正确的判定结果，假设 Alice 和 Bob 不会篡改自己的成绩，但为了保证游戏的公平性，应保证 Alice 和 Bob 均能验证结果的正确性。

1.2 问题分析

由于问题中强调了不暴露 Alice 和 Bob 二人成绩这一条件，我们意识到这是一个密码学相关的问题，也就是说我们需要一种方案来保证 Alice、Bob 以及 TTP 在交流过程中的安全性，从而让任何人都无法通过获取到的信息反推出二人的成绩信息。我们经过分析研究，针对不同场景，提出了相应的解

收稿日期：年-月-日；最终修改稿收到日期：年-月-日 *投稿时不填写此项*. 本课题得到…… 基金中文完整名称(No.项目号)、…… 基金中文完整名称(No.项目号)、…… 基金中文完整名称(No.项目号)资助.作者名1史鹏程，男，2000年生，学士，学生，不是计算机学会(CCF)会员，无主要研究领域、E-mail: 1551600819@qq.com. 作者名2伍孝飞，男，2001年生，学士，学生，不是计算机学会(CCF)会员，无主要研究领域、E-mail: 1337675840@qq.com. 作者名3杜扬帆，男，2000年生，学士，学生，不是计算机学会(CCF)会员，无主要研究领域、E-mail: 835842148@qq.com

决方案，简单易用，同时时间和空间复杂度都控制在了较低水平。本文还针对通信双方出现说谎和作弊的情况进行了讨论。

1.3 相关概念及工作

1.3.1 ElGamal 公钥体制：

它是基于 1985 年塔希尔·盖莫尔（Gamal T E）提出的公钥密码体制和椭圆曲线加密体系。既能用于数据加密也能用于数字签名，其安全性依赖于计算有限域上离散对数这一难题。是一种国际公认的较理想公钥密码体制，是网络上进行保密通信和数字签名的较有效的安全算法。

1.3.2 DH 密钥交换：

是由 Whitfield Diffie 和 Martin Hellman 在 1976 年公布的一种密钥一致性算法。这种密钥交换技术的目的在于使得两个用户安全地交换一个秘密密钥，可用于加密、进一步的密钥管理或任何其它的加密方式，以便用于以后的报文加密. Diffie-Hellman 密钥交换算法的有效性依赖于计算离散对数的难度。

2 场景一算法设计

2.1 问题形式化定义

输入：A_{grade}, B_{grade}（代表 A 的成绩和 B 的成绩，只有优良中差四种情况。）

输出：ANS (代表最终的比较结果，只有相同不相同两种情况。)

问题：Alice 和 Bob 已知自己的成绩，存在可信第三方，第三方知道二人的成绩，请设计一种方法在不向任何人泄漏 Alice 和 Bob 成绩的情况下，并且第三方无法得知双方成绩是否相同，让二人知道两人的成绩是否相同。

2.2 参数说明

具体参数说明可见表 2.1

表 2.1 参数表

参数符号	参数说明
S_a	成绩为优
S_b	成绩为良
S_c	成绩为中
S_d	成绩为差
pk_a	Alice 成绩对应的公钥
pk_b	Bob 成绩对应的公钥
sk_a	Alice 成绩对应的私钥
sk_b	Bob 成绩对应的私钥

2.3 程序交互过程图

程序交互过程图如图 2.1 所示

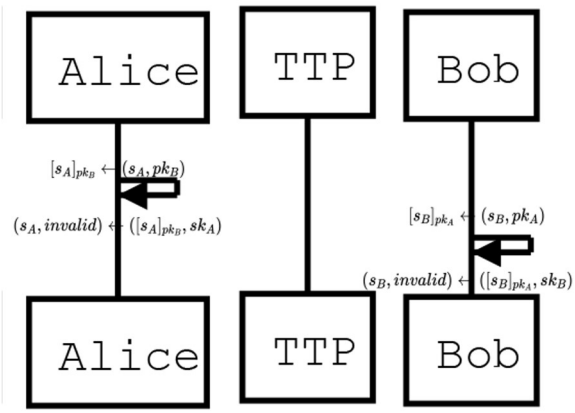

图 2.1 场景一程序交互过程图

2.4 伪代码

初始化：

①TTP：

使用 ELGamal 算法生成 A、B 成绩的公私钥对:

$$\mathrm{Generate}(\mathrm{pk_a}, \mathrm{pk_b}, \mathrm{sk_a}, \mathrm{sk_b})$$

将 Bob 成绩对应的公钥和 Alice 成绩的私钥发给 Alice

$$\mathrm{Alice} \leftarrow \mathrm{pk_b}, \mathrm{sk_a}$$

将 Alice 成绩对应的公钥和 Bob 成绩的私钥发给 Alice

$$\mathrm{Alice} \leftarrow \mathrm{pk_b}, \mathrm{sk_a}$$

游戏开始：

②Alice:

将 Alice 的成绩用 Bob 成绩的公钥加密

$$[A_{grade}]_{\mathrm{pk_b}} \leftarrow (A_{grade}, \mathrm{pk_b})$$

将密文用私钥解开

$$A_{grade} \leftarrow \left([A_{grade}]_{\mathrm{pk_b}}, \mathrm{sk_a}\right)$$

乱码则成绩不相同，否则成绩相同

③Bob:

将 Bob 的成绩用 Alice 成绩的公钥加密

$$[B_{grade}]_{\mathrm{pk_a}} \leftarrow (B_{grade}, \mathrm{pk_a})$$

将密文用私钥解开

$$B_{grade} \leftarrow \left([B_{grade}]_{\mathrm{pk_a}}, \mathrm{sk_b}\right)$$

乱码则成绩不相同，否则成绩相同

2.5 安全性证明

2.5.1 性质 1：假设 Alice 和 Bob 不会篡改自己的成绩，那么他们在游戏中一定能够得到正确的判定结果，并且无法确定对方的成绩。

证明：通过上述的算法可知，相同的成绩对应相同的私钥，如果两个成绩相同，则私钥一定可以解开加密后的密文。若成绩不相同，则会得到一个大整数，则代表成绩不相同。

此时，假设能通过此算法得到对方的成绩，那么一定得到了跟对方成绩相关的信息。两个只能得到一个公钥和一个私钥，无法得到与对方成绩相关的信息。导出矛盾，即原假设错误，两人无法通过此算法得到对方成绩。

2.5.1 性质 2:在场景 1 中，除了 Alice 和 Bob 之外，存在一个第三方且知道二人的成绩。那么，在满足性质 1 的同时，除了 Alice、Bob 和这个第三方之外的其他人不会在游戏中得到与成绩相关的任何信息。

证明：Alice 和 Bob 在得到公钥和私钥后，都是独自进行游戏的，且没有在信道上传输任何信息。不存在由于在不安全信道传输信息导致的信息泄露，此外，由于 Alice 和 Bob 都不会主动泄露自己的成绩，所有不存在成绩泄露的情况。

2.6 隐私性证明

TTP 是否能够确定两者成绩异同，为什么？

可以，在初始情况下 TTP 就知道两者成绩

TTP 是否能够确定 Alice 或 Bob 的成绩，为什么？

可以，在初始情况下 TTP 就知道两者成绩

2.7 公平性证明

在进行游戏阶段，只有两个人独自进行游戏，如果有一方作弊，只会导致作弊方无法得到正确结果。并且，可以保证两者都能够得到正确的结果，从而保证了游戏的公平性。

2.8 性能分析

①时间复杂度：

Alice：

一次加密：一次随机数生成，两次模幂

一次解密：一次模幂，一次乘法逆元，一次乘法。

Bob：

一次加密：一次随机数生成，两次模幂

一次解密：一次模幂，一次乘法逆元，一次乘法。

②空间复杂度：

Alice:

一个公钥一个私钥各 1024 位，成绩 2 位，结果 1 位

Bob：

一个公钥一个私钥各 1024 位，成绩 2 位，结果 1 位

TTP：

两对公私钥，两个成绩

共计：

6154 位

3 场景二算法设计

3.1 问题形式化定义

输入：A_{grade}、B_{grade}分别表示 Alice 和 Bob 的成绩

输出：A_{result}、B_{result}分别表示 Alice 和 Bob 获得的关于两人成绩是否相同的结果

问题：Alice 和 Bob 已知自己的成绩，存在可信第三方，第三方知道 Alice 的成绩，请设计一种方法在不向任何人泄漏 Alice 和 Bob 成绩的情况下，并且第三方无法得知双方成绩是否相同，让二人知道两人的成绩是否相同。

3.2 参数说明

具体参数说明可见表 3.1

表 3.1 参数表

参数符号	参数说明
S_a	成绩为优
S_b	成绩为良
S_c	成绩为中

S_d	成绩为差
pk_{ab}	Alice 与 Bob 的 EL 公钥
pk_{ac}	Alice 与第三方的 EL 公钥
pk_{bc}	Bob 与第三方的 EL 公钥
h^{ac}	Alice 和第三方的 DH 密钥
h^{ab}	Alice 和 Bob 的 DH 密钥
h^{bc}	Bob 和第三方的 DH 密钥
sk_{ab}	Alice 和 Bob 的 EL 私钥
sk_{ac}	Alice 和第三方的 EL 私钥
sk_{bc}	Bob 和第三方的 EL 私钥

3.3 程序交互过程图

程序交互过程图如图 3.1 所示

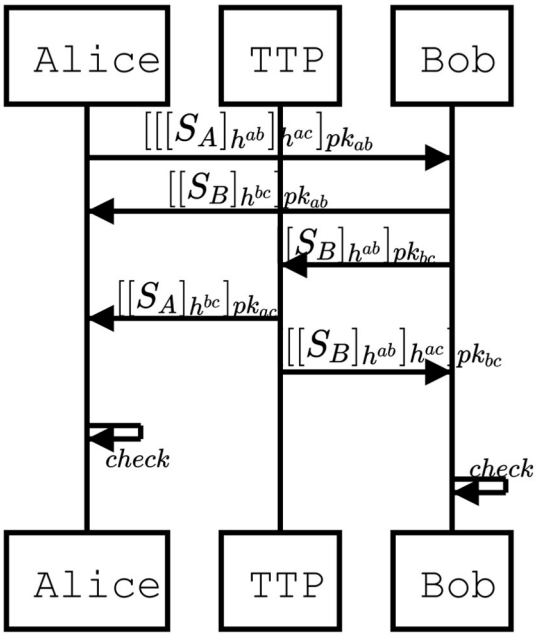

图 3.1 场景三程序交互过程图

3.4 伪代码

初始化：

Alice、Bob、TTP 三者之间两两协商一对 DH 密钥，以及一对 ELGamal 密钥

游戏开始：

（下面用s_A、s_B分别代表A_{grade}、B_{grade}）

（序号为整体的操作顺序）

Alice：

先进行加密操作

1) $[\mathrm{s_A}]_{h^{ab}} \leftarrow (\mathrm{s_A}, h^{ab})$

2) $\left[[\mathrm{s_A}]_{h^{ab}}\right]_{h^{ac}} \leftarrow \left([\mathrm{s_A}]_{h^{ab}}, h^{ac}\right)$

3) $\left[\left[[\mathrm{s_A}]_{h^{ab}}\right]_{h^{ac}}\right]_{pk_{ab}} \leftarrow \left(\left[[\mathrm{s_A}]_{h^{ab}}\right]_{h^{ac}}, pk_{ab}\right)$

4) 向 Bob 发送$\left[\left[[\mathrm{s_A}]_{h^{ab}}\right]_{h^{ac}}\right]_{pk_{ab}}$，收到 6）结果后解密

7) $[\mathrm{s_A}]_{h^{bc}} \leftarrow \left([\mathrm{s_A}]_{h^{bc}}]_{\mathrm{pk_{ac}}}, \mathrm{sk_{ac}}\right)$

7) $[\mathrm{s_B}]_{h^{bc}} \leftarrow \left([\mathrm{s_B}]_{h^{bc}}]_{\mathrm{pk_{ab}}}, \mathrm{sk_{ab}}\right)$

8) check$([\mathrm{s_A}]_{h^{bc}}, [\mathrm{s_B}]_{h^{bc}})$

Bob：

先进行加密操作

1) $[\mathrm{s_B}]_{h^{bc}} \leftarrow (\mathrm{s}_B, h^{bc})$

2) $\left[[\mathrm{s_B}]_{h^{bc}}\right]_{pk_{ab}} \leftarrow \left([\mathrm{s_B}]_{h^{bc}}, pk_{ab}\right)$

3) $[\mathrm{s_B}]_{h^{ab}} \leftarrow (\mathrm{s}_B, h^{ab})$

4) $\left[[\mathrm{s_B}]_{h^{ab}}\right]_{pk_{bc}} \leftarrow \left([\mathrm{s_B}]_{h^{ab}}, pk_{bc}\right)$

5) 向 Alice 发送$\left[[\mathrm{s_B}]_{h^{bc}}\right]_{pk_{ab}}$，向 TTP 发送$\left[[\mathrm{s_B}]_{h^{ab}}\right]_{pk_{bc}}$收到 6）结果后解密

7) $\left[[\mathrm{s_B}]_{h^{ab}}\right]_{h^{ac}} \leftarrow \left(\left[\left[[\mathrm{s_B}]_{h^{ab}}\right]_{h^{ac}}\right]_{pk_{bc}}, sk_{bc}\right)$

7) $\left[[\mathrm{s_A}]_{h^{ab}}\right]_{h^{ac}} \leftarrow \left(\left[\left[[\mathrm{s_A}]_{h^{ab}}\right]_{h^{ac}}\right]_{pk_{ab}}, sk_{ab}\right)$

8) check$(\left[[\mathrm{s_B}]_{h^{ab}}\right]_{h^{ac}}, \left[[\mathrm{s_A}]_{h^{ab}}\right]_{h^{ac}})$

TTP:

收到 5）结果后进行

5) $[\mathrm{s_A}]_{h^{bc}} \leftarrow (\mathrm{s}_A, h^{bc})$

5) $\left[[\mathrm{s_A}]_{h^{bc}}\right]_{pk_{ac}} \leftarrow \left([\mathrm{s_A}]_{h^{bc}}, pk_{ac}\right)$

5) $[\mathrm{s_B}]_{h^{ab}} \leftarrow \left([\mathrm{s_B}]_{h^{ab}}]_{\mathrm{pk_{bc}}}, \mathrm{sk_{bc}}\right)$

5) $\left[[\mathrm{s_B}]_{h^{ab}}\right]_{h^{ac}} \leftarrow \left([\mathrm{s_B}]_{h^{ab}}, h^{ac}\right)$

5) $\left[\left[[\mathrm{s_B}]_{h^{ab}}\right]_{h^{ac}}\right]_{pk_{bc}} \leftarrow \left(\left[[\mathrm{s_B}]_{h^{ab}}\right]_{h^{ac}}, pk_{bc}\right)$

6) 向 Alice 发送$\left[[\mathrm{s_A}]_{h^{bc}}\right]_{\mathrm{pk_{ac}}}$，向 Bob 发送$\left[\left[[\mathrm{s_B}]_{h^{ab}}\right]_{h^{ac}}\right]_{pk_{bc}}$

3.5 安全性证明

3.5.1 性质 1：假设 Alice 和 Bob 不会篡改自己的成绩，那么他们在游戏中一定能够得到正确的判定结果，并且无法确定对方的成绩。

证明：满足。第三方是可信的，所以在不篡改成绩的情况下两人一定能得到正确结果。Alice 和 Bob 在传递给他人的信息中，都保留不可被破解的哈希加密方法。由于外层有 ELGamal 算法加密，监听者也无法得知成绩是否相同。最后通过 hash 加密，比较结果就能得知是否相同。

3.5.2 性质 3：在场景 2 中，存在知道 Alice 成绩。但是不知道 Bob 成绩的第三方。那么，在满足性质 1 的同时，除了 Alice 和 Bob 之外的其他人不会在游戏中确定任意一个人的成绩。

证明：满足。对于第三方来说，第三方获得的是 Bob 加密后的数据，不可破解，就无法确定 Bob 的成绩。

3.6 隐私性证明

3.6.1 TTP 是否能够确定二者成绩异同，为什么？

证明：不可以，因为过程中的成绩比较环节由 Alice 和 Bob 完成，所以 TTP 不知道二人成绩是否相同。

3.6.2 TTP 是否能够确定 Alice 或 Bob 的成绩，为什么？

TTP 知道 Alice 的成绩，题目要求。不知道 Bob 的成绩，见 3.5.1.

3.7 公平性证明

（这一小节用 A、B、C 分别代表 Alice、Bob、TTP）

3.7.1 Alice 作弊处理：

证明：

f_{ab}, f_{ac} 为 AB，AC 的 DH 密钥

初始化：

由于 B 知道 $f_{ab}(x)$（指使用 f_{ab} 进行加密），B 得到四种结果 f_{ab} (优)， f_{ab} (良)， f_{ab} (中)，f_{ab}(差)，再由 B 发给 C 四种结果，C 知道 $f_{ac}(x)$，再对于四种结果进行二次加密，得到 4 * 4 = 16 种结果集合 G，再发送给 B。此时可以证明，A 发给 B 的数字，一定是 16 种结果之一。 若 A 作弊，那么 A 发送的信息一定不在 G 中。

判断流程：

初始化，B 发送四种结果给 C，C 再二次加密发给 B，B 获得一个包含 16 个元素的集合。游戏开始：A 发送信息给 B，若在此集合中，则没作弊。反之，作弊，游戏终止。

3.7.2 Bob 作弊处理：

证明：

f_{bc} 为 BC 的 DH 密钥

初始化：

C 将四种成绩的集合 G 加密发给 A

判断流程：

B 加密发送给 A，若信息在 G 中，那么没作弊，反之作弊，游戏终止。

3.8 性能分析

初始化：

3 次 DH 密钥交换，输出结果约定发送（不计算复杂度）

时间复杂度：

Alice:

一次 ElGamal 加密；一次乘法逆元解密

Bob：

两次 ElGamal 加密；一次乘法逆元解密

TTP：

两次 ElGamal 加密

注：每次 ElGamal 算法，是两次模幂运算。

空间复杂度：

Alice：

2 个 DH 密钥各 1024 位（bit）；B,C 发送 ElGamal 加密 a,b 两次各 1024 位，共 4096 位；A 成绩 2 位；

Bob：

2 个 DH 密钥各 1024 位（bit）；B,C 发送 ElGamal 加密 a,b 两次各 1024 位，共 4096 位；B 成绩 2 位；

TTP：

2 个 DH 密钥各 1024 位（bit）；B 发送的 ElGamal 加密 a , b 各 1024 位，共 2048 位，A 反馈结果 1 位。

共计：

10245bit

4 场景三算法设计

4.1 问题形式化定义

输入：A_{grade}、B_{grade}分别表示 Alice 和 Bob 的成绩
输出：A_{result}、B_{result}分别表示 Alice 和 Bob 获得的关于两人成绩是否相同的结果
问题：Alice 和 Bob 已知自己的成绩，存在可信第三方，请设计一种方法在不向任何人泄漏 Alice 和 Bob 成绩的情况下，让二人知道两人的成绩是否相同。

4.2 参数说明

具体参数说明可见表 4.1

表 4.1 参数表

参数符号	参数说明
S_a	成绩为优
S_b	成绩为良
S_c	成绩为中
S_d	成绩为差
pk_{ab}	Alice 和 Bob 的 DH 密钥
pk_{ac}	Alice 和第三方的 DH 密钥
pk_{bc}	Bob 和第三方的 DH 密钥

且有A_{grade}, $B_{grade} \in \{S_a, S_b, S_c, S_d\}$

4.3 程序交互过程图

程序交互过程图如图 4.1 所示

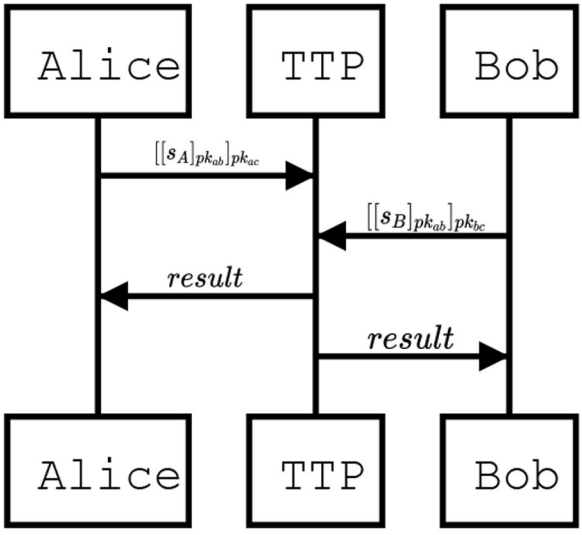

图 4.1 场景三程序交互过程图

4.4 伪代码

初始化：

Alice、Bob、TTP 三者之间两两协商一对 DH 密钥，
分别记为pk_{ab}，pk_{ac}，pk_{bc}。
游戏开始：
（下面用s_A、s_B分别代表A_{grade}、B_{grade}）

Alice 使用进行pk_{ab}进行一次哈希加密 ：

$$[\mathrm{s_A}]_{\mathrm{pk_{ab}}} \leftarrow (\mathrm{s_A}, \mathrm{pk_{ab}})$$

再使用pk_{ac}进行一次简单的对称加密

$$\left[[\mathrm{s_A}]_{\mathrm{pk_{ab}}}\right]_{\mathrm{pk_{ac}}} \leftarrow \left([\mathrm{s_A}]_{\mathrm{pk_{ab}}}, \mathrm{pk_{ac}}\right)$$

Bob 进行类似的过程得：

$$\left[[\mathrm{s_B}]_{\mathrm{pk_{ab}}}\right]_{\mathrm{pk_{bc}}} \leftarrow \left((\mathrm{s_A}, \mathrm{pk_{ab}}), \mathrm{pk_{bc}}\right)$$

两人将结果发给 TTP
TTP 接收结果后

$$[\mathrm{s_A}]_{\mathrm{pk_{ab}}} \leftarrow \left(\left[[\mathrm{s_A}]_{\mathrm{pk_{ab}}}\right]_{\mathrm{pk_{ac}}}, \mathrm{pk_{ac}}\right)$$

$$[\mathrm{s_B}]_{\mathrm{pk_{ab}}} \leftarrow \left(\left[[\mathrm{s_B}]_{\mathrm{pk_{ab}}}\right]_{\mathrm{pk_{bc}}}, \mathrm{pk_{bc}}\right)$$

TTP 比较$[s_A]_{pk_{ab}}$和$[s_B]_{pk_{ab}}$得到结果A_{result}和B_{result}，并发回
游戏结束

4.5 安全性证明

4.5.1 性质 1：假设 Alice 和 Bob 不会篡改自己的成绩，那么他们在游戏中一定能够得到正确的判定结果，并且无法确定对方的成绩。

证明：满足。第三方是可信的，所以在不篡改成绩的情况下两人一定能得到正确结果。Alice 和 Bob 都无法获得用于破解加密信息的手段，故即使监听到了通讯内容也无法得知对方的成绩。

4.5.2 性质 4：在场景 3 中，不存在任何知道 Alice 或 Bob 成绩的第三方。那么，在满足性质 1 的同时，除了 Alice 和 Bob 之外的其他人不会在游戏中确定任意一个人的成绩。

证明：满足。对于第三方来说，他最后获得的是 Alice 和 Bob 带有一层加密的成绩，且无法破解，故无法得知成绩。对于其他监听者，得到的是带有两层加密的成绩，更无法破解。

4.6 隐私性证明

4.6.1 TTP 是否能够确定二者成绩异同，为什么？

证明：可以，因为过程中的成绩比较环节由 TTP 完成，所有 TTP 能够知道二人成绩是否相同。

4.6.1 TTP 是否能够确定 Alice 或 Bob 的成绩，为什么？

证明：不能，见 4.5.2 节。

4.7 公平性证明

在初始化阶段，令 Alice 和 Bob 分别将四种成绩用要求的加密方式加密处理，并发送给第三方。在游戏阶段，第三方检查两人发送的内容是否在刚才的几种结果之中即可判断二人是否作弊。如果作弊，游戏终止，两人都无法获得正确结果。从而保证了 TTP 可以发现二人之中的作弊者，且发现后游戏终止，二人均无法得到正确结果。

4.8 性能分析

时间复杂度：

Alice：

一次哈希加密；一次简单的对称加密（字符串连接）

Bob：

一次哈希加密；一次简单的对称加密（字符串连接）

TTP：

两次简单的解密（字符串拆分）

空间复杂度：

Alice：

2 个 DH 密钥各 1024 位（bit）；两次加密后的结果（哈希长度 256 + 字符串拼接 1024 = 1280 位）；A 成绩 2 位；结果 1 位。

Bob：

2 个 DH 密钥各 1024 位（bit）；两次加密后的结果（哈希长度 256 + 字符串拼接 1024 = 1280 位）；B 成绩 2 位；结果 1 位。

TTP：

2 个 DH 密钥各 1024 位（bit），两个解密后的结果各 256 位。结果 1 位。

共计 $1024 * 6 + 1280 * 4 + 256 * 2 + 2 * 2 + 1 * 3 = 11783$位。

5 结论

我们的算法较为全面、完善地解决了 1.1 节提到的问题，能够在不篡改成绩的情况下保证算法的正确性，即 Alice 和 Bob 都能得到正确结果且不泄露成绩给其他人。也在三种场景中具备隐私性和安全性和公平性，保证了在 Alice 和 Bob 说谎和作弊情况下算法仍能正确工作。同时具有一定的泛用性，应用我们的方法，可传递的信息远不止成绩，可以使其他各种各样的信息，使得算法可以被广泛使用。而且算法具有较为良好的时间和空间复杂度，可以用来应对较为复杂的需求。除此之外，在研究过程中还意识到可信第三方对于我们算法的重要性，对此我们也在积极探索不需要第三方的加密通信算法，这也是现在我们的不足之处。

参 考 资 料

[1] https://cryptobook.nakov.com/key-exchange/diffie-hellman-key-exchange

[2] https://math.asu.edu/sites/default/files/elgamal.pdf

附 录

分工

成员	组长	组员	组员
学号	20191757	20194687	20194657
姓名	史鹏程	伍孝飞	杜扬帆
班级	计 1904	计 1904	计 1904
任务分工	参与设计各场景算法。场景三程序实现及相应报告。以及本组总体报告的整理工作	负责各个场景的核心算法设计任务。场景二程序实现及相应报告。	参与设计各个场景的算法设计任务。场景一程序实现及相应报告。
工作比例	33.3%	33.3%	33.3%

实验环境

硬件	CPU	Intel(R)Core(TM)i5-8265UCPU @1.60GHz1.80 GHz
	GPU	NVIDI MX250
	内存	64GB
软件	操作系统	Windows 10（1909）
	开发语言	Python 3.7.6
	开发用库	Sys、math、random
	开发工具	PyCharm 2019.2.3 Professional
		Jupyter notebook 6.2.0

心得体会

史鹏程：

本次算法课程设计涉及的是一个全新的学科——密码学。考虑到我之前对此知之甚少，在本次课设中也是从老师在任务书里给的资料开始从头一点点了解的，和队友一起学习进步，所幸需要用到的密码学知识并不是很多。现在回过来总结，也发现现在的自己真是比一开始有了不少的进步，对于高深莫测的密码学也有了一些初步的认识，算法设计能力也经历了实践的考验，心里也有了一些成就感。总的来说，这次课设的经历十分令人难忘。

这次课设再次让我认识到了团队合作的重要性，面对老师们对于任务提出的一个又一个要求和对于方案提出的一个又一个不足，这些问题的克服都是我们小组一起不断合作讨论的结果，乃至是后来的程序实现和完成报告阶段，我们在这个过程之间的互相帮助，互相安慰，互相加油都对我们最终取得胜利功不可没。我认为经过这次课设，我的团队协作能力又有了一些提高。

最后也感谢老师和助教学长在这段时间的辛勤付出，总能为我们答疑解惑，指出不足，谢谢老师和助教学长。

伍孝飞：

在课设过程中，对于课题的要求，一直采取精益求精的态度和严谨的证明去解决问题。中途想了非常多的半成熟的想法，虽然最后都被抛弃了，但是也有很大的启示作用。课设的三周时间中，就像爬山一样，要求一点一点严格，让整个方案越来越完善，直到解决问题，这一点是最重要的。在解决问题中，小组成员也通力合作，一起讨论，脑力风暴，对整个过程有极其重要的作用。

通过这一次课设，我融会贯通本课程所学专业理论知识，培养我独立分析问题、解决问题的能力，以及系统软件设计的能力，培养我的创新能力及团队协作精神。算法课的精髓，解决问题，问题建模，优化模型能力，最后也非常感谢老师，学长在自己闲暇时间对我们提出方案进行判断，以及提出不完善的点。

杜扬帆：

这次课设的选题很有趣，给我们很大的施展空间，语言没有作限制，让我们可以随心所欲用自己熟悉的语言和环境编程，为的就是开阔我们的思路，得到更优化的算法。

这次课设我负责算法的构思和情景一的编程与报告，课设刚开始的前五天，我思索出来了三四套解决方案，都被老师否决了。不安全、有尝试的可能性等等，虽然感到十分沮丧，但是我也大致明白了老师的要求是什么，为后续的算法设计做下了铺垫。

作为这一次课设的组员，我很感激我的队友们，他们本来就是我的好朋友，通过和另外两个同学沟通，我的三个场景的算法的解得以大幅度优化，当我的程序出现 bug 时，我会找他们絮絮叨叨，然后问题就迎刃而解。

这次课设是心情最快乐的一次，因为算法并不是那样难以理解，也不是建立一个庞大的工程，牵一发而动全身，debug 的压力很小。书写论文的过程也是整理思路，反思自己设计的算法的过程，严格的论文排版让我预先了解到了发论文的种种要求。感激老师的指导，老师非常友善，耐心的解决了很多问题。