# Privacy-preserving greater-than integer comparison without binary decomposition

Sigurd Eskeland

Norwegian Computing Center
Postboks 114 Blindern
0314 Oslo, Norway
sigurd.eskeland@nr.no

**Abstract.** Common for the overwhelming majority of privacy-preserving *greater-than* integer comparison schemes is that cryptographic computations are conducted in a bitwise manner. To ensure the secrecy, each bit must be encoded in such a way that nothing is revealed to the opposite party. The most noted disadvantage is that the computational and communication cost of the bitwise encoding is as best linear to the number of bits. Also, many proposed schemes have complex designs that may be difficult to implement and are not intuitive.
Carlton et al. [2] proposed in 2018 an interesting scheme that avoids bitwise decomposition and works on whole integers. A variant was proposed by Bourse et al. [1] in 2019. In this paper, we show that in particular the Bourse scheme does not provide the claimed security. Inspired by the two mentioned papers, we propose a comparison scheme with a somewhat simpler construction and with clear security reductions.

## 1 Introduction

The idea of the Millionaire's Problem [5] is to facilitate two millionaires, not trusting each other and who do not want to reveal their worth to each other, to find out who is the richest. Although such tasks could trivially be solved by a trusted third party who decides which party has the greatest value, the goal is to replace the trusted party with a privacy-preserving protocol. In other words, it is the ability to privately performing *greater-than* integer comparisons without a trusted third party. We refer to this concept as privacy-preserving integer comparison (PPC).

PPC may be typically used as a sub-protocol for conducting privacy-preserving computations on encrypted data sets. Practical applications are auctions with private biddings, voting systems, privacy-preserving database retrieval and data-mining, privacy-preserving statistical analysis, genetic matching, face recognition, private set intersection, where two parties holding separate data sets want to find common data points without disclosing the data sets to each other, etc.

Privacy-preserving integer comparison is an active research field, where contributions are based based on techniques such as homomorphic encryption, garbled circuits, oblivious transfer, and secret sharing. Authors generally tend to claim some improvement over some other scheme in particular with regard to efficiency, but the actual efficiency may not be readily comparable (for example due to that the methods are very different) nor available in many cases. Common for overwhelming majority of privacy-preserving *greater-than* integer comparison schemes is that cryptographic computations are conducted in a bitwise manner. To ensure the secrecy, each bit of the private inputs must be encoded in such a way that nothing is revealed to the opposite party. Bitwise cryptographic processing results in high computational and communication costs that is proportional to the data input sizes. Also, many proposed schemes have complex designs that may be difficult to implement and are not intuitive.

Carlton et al. [2] proposed in 2018 a PPC scheme that works on whole numbers and does not require bitwise coding or encryption. Inspired by [3, 4], it makes use of a special composite RSA modulus, whose two prime integers are selected with regard to the integers to be compared. Blinding is conducted to protect the input values. At the end of the protocol, a plaintext equality test (PET) subprotocol is ran to determine the outcome of the comparison. This subprotocol provides an additional performance cost. Bourse et al. [1] proposed a slightly modified two-pass PPC protocol that avoids using a PET protocol, and whose function is replaced simply by a control value that is sent to party A in the last pass. By means of this value, party A determines the outcome of the comparison.

Both the Carlton and Bourse schemes claim that the security is based on the *small RSA subgroup decision assumption*, cf. Definition 1. This assumption holds if integers from the group $\mathbb{Z}_n^*$ and the subgroup $\mathbb{H} \subset \mathbb{Z}_n^*$ are indistinguishable. However, this computational problem applies only to the first pass, while there is no clear security reduction in the second pass. After the second pass, party A performs a "decryption" that reduces the subgroup order to the subgroup $\mathbb{G}$, which are considerable smaller than $\mathbb{H}$, and is outside the scope of the claimed small RSA subgroup decision assumption. The group order of $\mathbb{G}$ is of a power order $p_0^d$, where $p_0$ is a small prime. Input values are represented internally in the Carlton and Bourse schemes as exponents to $p_0$, as $p_0^{d+m_A-m_B}$. This results in a reduced subgroup $\mathbb{G}' \subseteq \mathbb{G}$ of variable order that is a function of the input integers.

Briefly summarized, the mentioned comparison schemes have the following issues:

1. The subgroup order of $\mathbb{G}$ is not fixed, but variable as a function of the input values.
2. No clear security assumption w.r.t. party A.

In this paper, we describe in particular the Bourse scheme and show that it vulnerable to attacks. We also propose a PPC scheme that mitigates the mentioned security issues. Our scheme has a simpler composite modulus $n$ than that of the

Carlton and Bourse schemes, and there is no long-term private key associated with a user.

## 2 The Bourse comparison scheme

In this section, we describe the Bourse scheme and show that it works in a smaller subgroup than claimed and that it is of variable order, and that this in conjunction with the mentioned control value (that replaces the PET subprotocol of the Carlton scheme) makes it vulnerable to attacks.

### 2.1 Preliminaries

The Carlton and Bourse schemes make use of the following parameters:

- $p_s$, $p_t$, $q_s$ and $q_t$ are large distinct primes.
- $p_0$ is a small prime, preferably an odd prime, for instance 3.
- $a$ and $d$, where $0 < a \leq d$ and $d/a$ is an upper bound on $m_A, m_B \leq d/a$.[1]
- A composite integer $n = pq$, where $p = 2p_0^d p_s p_t + 1$ and $q = 2p_0^d q_s q_t + 1$ are primes.
- A generator $g$ of order $p_0^d$ modulo $n$.[2]
- $\bar{b}$ is an upper bound of the secret $p_s q_s$.
- $c$ is a long-term private key that is used by party A, where

$$c = p_s q_s \left( \frac{1}{p_s q_s} \bmod p_0^d \right)$$

Public parameters are $\{n, a, d, p_0, g, h, \bar{b}\}$. Private parameters known by party A are $\{p, q, c\}$.

The scheme works in the cyclic subgroups $\mathbb{G} \subset \mathbb{Z}_n^*$ of order (number of elements) $p_0^d$ generated by $g$, and $\mathbb{H} \subset \mathbb{Z}_n^*$ of order $p_s q_s$ generated by $h$, and whose elements are coprime with $p_0$. The core idea in the Carlton scheme [2] is that the element

$$g^{p_0^{d+m_A-m_B}} \bmod n \tag{1}$$

can be used to compare two integers $m_A$ and $m_B$. Evidently, if multiples of $p_0$ exceed $p_0^d$ in the exponent in Eq. 1, this results in

$$g^{p_0^{d+m_A-m_B}} = g^{p_0^{d+x}} = (g^{p_0^d})^{p_0^x} = 1^{p_0^x} = 1 \quad \text{if} \quad m_A \geq m_B \quad \text{i.e.,} \quad x \geq 0$$

This construction is almost identical in the Bourse scheme [1], which has an additional public parameter[3] $a$, where integer comparison is conducted according to

$$g^{p_0^{d+a\cdot(m_A-m_B)}} = g^{p_0^{d+a\cdot x}}$$

[1] The parameter $a$ does not exist in the Carlton scheme, where simply $d$ is the upper bound $m_A, m_B \leq d$.

[2] Given the composition of $p$ and $q$, if $g$ generates a subgroup of order $p_0^d$ modulo $p$ and $q$, then it also generates the same modulo $n$.

[3] The purpose of this parameter is not clear, and the authors do not explain in what sense that $a$ contributes to security.

which entails that if $m_A < m_B$, then $x$ becomes negative.

An observation is that for a negative $x$, $0 > x \geq -\frac{d}{a}$, the element $g^{p_0^{d+a\cdot x}}$ generates variable subgroups $\mathbb{G}' \subset \mathbb{G}$, whose order is $p_0^{d+a\cdot x}$. This means that the maximum subgroup $\mathbb{G}$ is only present if $x = -\frac{d}{a}$. As elaborated in Section 2.5, this makes the Bourse scheme susceptible to attacks.

### 2.2 The Bourse scheme

The Bourse et al. scheme [1] is summarized in Figure 1. In the first pass, Alice blinds her plaintext $m_A$ by computing

$$C = g^{p_0^{a\cdot m_A}} h^{r_1} \bmod n \tag{2}$$

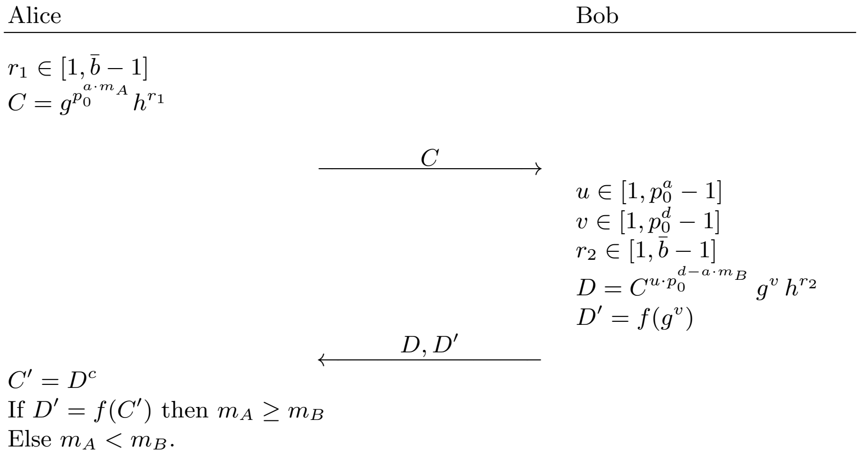
Subsequently in the second pass, Bob computes a blinded computation that contains $m_B$:

$$D = C^{u\cdot p_0^{d-a\cdot m_B}} g^v h^{r_2} \bmod n \tag{3}$$

and the control value $D' = f(g^v)$. Finally, Alice computes

$$\begin{aligned} C' = D^c &= (C^{u\cdot p_0^{d-a\cdot m_B}} g^v h^{r_2})^c \\ &= (g^{p_0^{a\cdot m_A}\cdot u\cdot p_0^{d-a\cdot m_B}} h^{r_1} g^v h^{r_2})^c \\ &= g^{u\cdot p_0^{d+a\cdot(m_A-m_B)}} g^v \end{aligned} \tag{4}$$

Note that by application of $c$ the factors containing the base $h$ are eliminated.



Alice

Bob

$r_1 \in [1, \bar{b}-1]$
$C = g^{p_0^{a\cdot m_A}} h^{r_1}$

$\xrightarrow{C}$

$u \in [1, p_0^a - 1]$
$v \in [1, p_0^d - 1]$
$r_2 \in [1, \bar{b}-1]$
$D = C^{u\cdot p_0^{d-a\cdot m_B}} g^v\, h^{r_2}$
$D' = f(g^v)$

$\xleftarrow{D, D'}$

$C' = D^c$
If $D' = f(C')$ then $m_A \geq m_B$
Else $m_A < m_B$.

**Fig. 1.** The Bourse et al. comparison scheme

### 2.3 Claimed security assumption

Carlton et al. and Bourse et al. [2, 1] state that the security of their schemes is based on the small RSA subgroup decision assumption. The following definition is from [1]:

**Definition 1 (The small RSA subgroup decision assumption)** *This assumption holds if given an RSA quintuple $(u, p_0, d, n, g)$, the distributions $x$ and $x^{p_0^d p_1 q_1}$ are computationally indistinguishable for a uniformly random quadratic residue $x = r^2 \bmod n$.*

This assumption states that it is hard to distinguish elements in $\mathbb{H} \subset \mathbb{Z}_n^*$ of order $p_s q_s$ (generated by $h$) from a random quadratic residue in $Z_n^*$. In other words, it holds if it is not possible to determine if an integer belongs to $\mathbb{H}$ or not.

### 2.4 Actual security viewed by computational complexity

In the Bourse scheme, Party B generates three secret random secret integers $(r_2, u, v)$:

- $r_2$ is exponent of the factor $h^{r_2}$ of $D$, cf. Eq. 3. Since $h^{r_2}$ is eliminated by party A, cf. Eq. 4, it does not provide any security w.r.t. party A.
- $u$ is an exponent in $D$.
- $v$ is exponent of the factor $g^v$ of $D$ and the control value $D' = f(g^v)$.

Brute-forcing is conducted w.r.t. $u$ and the low-entropy $m_B$ in conjunction with the control value $D'$, by checking $f(g^{-u' \cdot p_0^{d-a \cdot m'_B}} C') \overset{?}{=} D'$. The actual security of the scheme w.r.t party A is determined by the secret random integer $u$ only.

### 2.5 Security issues

We will now discuss the alluded security issues of the Bourse scheme.

**The stated security assumption is not applicable** After the second pass, Alice uses her long-term private key $c$ and computes $C' = D^c$, cf. Eq. 4. Since $C'$ is an element in $\mathbb{G}$, this crucial final computation is outside the scope of the stated *small RSA subgroup decision assumption*, which pertains to the much larger subgroup $\mathbb{H}$. This means that the stated security assumption is not applicable. This also means that this "decryption" operation provides no added protection for neither party, which makes the use of a long-term private key unclear.

The consequence of the "decryption" is that the resulting value $C'$ is in the small subgroup $\mathbb{G}$, which is considerable smaller than $\mathbb{H}$. However, next we will see that $C'$ is element of a smaller subgroup $\mathbb{G}' \subset \mathbb{G}$. This means a lower computational complexity and security than claimed, which is discussed next.

A note on semantic security. This is equivalent to so-called ciphertext indistinguishability under chosen-plaintext attack. Bourse et al. formulated the *small*

*RSA subgroup decisional problem* in order to show semantic security. However, the small RSA subgroup decision assumption implies indistinguishability and semantic security, but since this is assumption not applicable to their construction, the scheme cannot be said to uphold semantic security.

**Variable subgroup order** In the Bourse paper, the computation $C'$ (Eq. 4) is claimed to be element in $\mathbb{G}$, whose order is $p_0^d$. But the input values $(m_A, m_B)$ figure as exponents to $p_0$ as $p_0^{d+a\cdot(m_A-m_B)}$, cf. Eq. 4. This means that $C'$ is an element of a smaller subgroup $\mathbb{G}' \subseteq \mathbb{G}$, whose order is variable and is a function of the input plaintext values. Hence, $\mathbb{G}' = \mathbb{G}$ if $m_A = 0$ and $m_B = d$, otherwise $\mathbb{G}' \subset \mathbb{G}$.

The reduced subgroup order of $\mathbb{G}'$ makes the Bourse scheme more suspectable to attacks, w.r.t. to the security of party B, where party A represents the adversarial party. For this purpose, party A sets $m_A = 0$. As noted, the security of the scheme depends on the secrecy of the random integer $u$, which protects the privacy-sensitive factor $g^{u\cdot p_0^{d-a\cdot m_B}}$ of $C'$.

The reduced subgroup order means that the integer range to brute-force w.r.t. $u$ is reduced as a function of $m_B$ to the range $[0, p_0^{d-a\cdot m_B}]$, which reflects the variable subgroup order of $\mathbb{G}'$, due to the congruence relation

$$u\ p_0^{d-a\cdot m_B} \equiv u'\ p_0^{d-a\cdot m_B} \pmod{p_0^d}$$

where $u' < u$.

## 3 Privacy-preserving integer comparison

Inspired by [2, 1], our scheme uses a cyclic subgroup of a power order $p_0^d$ that is reflected in the composition of a RSA modulus $n$. Similar to [2], the idea is that Eq. 1 can be used to compare two integers $m_1$ and $m_2$ in a privacy-preserving manner. Unlike the mentioned papers, whose schemes partially rely on the small RSA subgroup decision problem, the security of our scheme partially assumes the following computational problem:

**Definition 2 (Small RSA subgroup computational problem)** *Given $(\alpha, g, n)$ and a random integer $R \in \mathbb{Z}_n^*$, it is computationally intractable to find $R^{p_1 q_1}$, which is an element in the subgroup $\mathbb{G}$.*

Our privacy-preserving *greater-than* integer comparison protocol is presented next.

**Construction** Let $n = pq$ denote a modulus, where

- $p_0$ is a small odd prime.
- $p = 2p_0^d p_1 + 1$, $q = 2p_0^d q_1 + 1$, $p_1$ and $q_1$ are large distinct primes.
- $d$ is an upper bound for $0 \leq m_A, m_B < d$.

Select an element $\alpha$ that is a generator (a.k.a. a primitive root) for $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Then $g = \alpha^{2p_1q_1} \bmod n$ is a generator that generates the subgroup $\mathbb{G}$ of order $p_0^d$ modulo $n$.

| Alice | | Bob |
|---|---|---|
| $r_1, r_2 \in Z_{\bar{b}}$ | | $r_3 \in \mathbb{Z}^*_{p_0^d}$<br>$r_4, r_5 \in \mathbb{Z}_{\bar{b}}$ |
| $x = g^{p_0^{m_A}} \alpha^{r_1}$ | | |
| | $\xrightarrow{x}$ | |
| | | $y = \alpha^{r_3 p_0^{d-m_B}}$<br>$c = \alpha^{r_4}$<br>$z = x^{r_3 p_0^{d-m_B}} c$<br>$\beta = c^{r_5}$ |
| | $\xleftarrow{y, z, \beta}$ | |
| $c' = zy^{-r_1}$<br>$\gamma = (c')^{r_2}$<br>$\delta = \beta^{r_2}$ | | |
| | $\xrightarrow{\gamma, \delta}$ | |
| | | If $\delta = \gamma^{r_5}$<br>then $m_A \geq m_B$<br>Else $m_A < m_B$. |

**Fig. 2.** Protocol for secure comparison

### 3.1 Correctness

Next is a detailed exposition of the proposed scheme that is summarized in Figure 2. Let $\mathbb{Z}^*_{p_0^d}$ denote the integers less than $p_0^d$ that are coprime with $p_0$, and $\mathbb{Z}_{\bar{b}} = \{x \in \{1, \ldots, \bar{b}\} \mid \gcd(x, p_0){=}1\}$ denote the integers less than $\bar{b}$ that are coprime with $p_0$, where $\bar{b} < p_1, q_1$ is an upper boundary.

Alice randomly generates the secret ephemeral integers $r_1, r_2 \in \mathbb{Z}_{\bar{b}}$ and Bob generates $r_3 \in \mathbb{Z}^*_{p_0^d}$, $r_4, r_5 \in \mathbb{Z}_{\bar{b}}$. In Round 1 Alice shares the blinded

$$x = g^{p_0^{m_A}} \alpha^{r_1}$$

with Bob. In Round 2, Bob computes and sends to Alice:

- $y = \alpha^{r_3 p_0^{d-m_B}}$
- $z = x^{r_3 p_0^{d-m_B}} c = (g^{p_0^{m_A}} \alpha^{r_1})^{r_3 p_0^{d-m_B}} c = g^{r_3 p_0^{d+m_A-m_B}} \alpha^{r_1 r_3 p_0^{d-m_B}} \alpha^{r_4}$, where $c = \alpha^{r_4}$ is a control value for the subsequent comparison.
- $\beta = c^{r_5}$

In Round 3, a privacy-preserving equality comparison of $c$ is performed. Alice computes

$$\begin{aligned} c' &= zy^{-r_1} \\ &= (g^{r_3 p_0^{d+m_A-m_B}} \alpha^{r_1 r_3 p_0^{d-m_B}} \alpha^{r_4})(\alpha^{r_3 p_0^{d-m_B}})^{-r_1} \\ &= g^{r_3 p_0^{d+m_A-m_B}} c \end{aligned} \tag{5}$$

Note that Eq. 5 has two outcomes. If $m_A \geq m_B$, then $g^{r_3 p_0^{d+m_A-m_B}}$=1 and $c' = c$. Otherwise, $c' \neq c$.

Next, Alice computes and sends

$$\gamma = (c')^{r_2} \quad \text{and} \quad \delta = \beta^{r_2}$$

to Bob, who checks

$$\delta \overset{?}{=} \gamma^{r_5}$$

If $m_A \geq m_B$ then $\delta = \beta^{r_2} = c^{r_2 r_5}$. Otherwise, if $m_A < m_B$ then $\delta \neq \gamma^{r_5}$ with an overwhelming probability.

### 3.2 Security of the proposed protocol

In this section, we prove that the proposed protocol preserve the confidentiality of private inputs against honest-but-curious adversaries in the standard model.

**Theorem 1 (Privacy of A).** *The secrecy of $m_A$ is preserved.*

*Proof.* Round 1. Let $\alpha^{r_1} \in \mathbb{Z}_n^*$ and $g^{p_0^{m_A}} \in \mathbb{G}$ be factors of $x$. Since the group size of $Z_n^*$ is larger than $\mathbb{G}$, and $\alpha^{r_1}$ is uniformly random and unique for every instance of $x$, then $x$ is not distinguishable from some uniform random integer $\alpha^r$. Thus, $x$ does not leak any information about $m_A$.

In Round 3, Bob knows $(r_3, r_4, r_5, c, \beta, \gamma, \delta)$. Let $m_B = d$ to ensure that

$$g^{r_3 p_0^{d+m_A-m_B}} = g^{r_3 p_0^{m_A}} \begin{cases} \neq 1 & \text{if} \quad 0 \leq m_A < d \\ = 1 & \text{if} \quad m_A = d \end{cases} \tag{6}$$

There two options w.r.t. disclosing $m_A$:

1. Solve the equation $\beta^{r_2} = \delta$. Then insert $r_2$ into Eq. 7 and solve it w.r.t. $m_A$.
2. Solve the equation
$$\left(g^{r_3 p_0^{m_A}} c\right)^{r_2} = \gamma \tag{7}$$
w.r.t. $(r_2, m_A)$.

Either case requires solving discrete logarithms. But the Discrete Logarithm Problem has no known feasible solution, which means that the secrecy of $m_A$ is preserved. □

**Theorem 2 (Privacy of B).** *The secrecy of $m_B$ is preserved provided that the small RSA subgroup computational problem holds.*

*Proof.* In Round 2, Alice receives $(y, z, \beta)$. After Round 2, Alice knows $(r_1, r_2, x, y, z, \beta)$. We consider $y$ and $z, \beta$ as two cases:

1. By transforming $y$ into $y^{p_1 q_1}$ enables deduction of $m_B$ by simple trial-and-error w.r.t $m_B$. Transforming $y$ into $y^{p_1 q_1}$ requires to solve the small RSA subgroup computational problem. Assuming that this assumption holds, the confidentiality of $m_B$ is protected w.r.t. $y$.
2. Solving the equation

$$\left(\frac{z}{x^{r_3 p_0^{d-m_B}}}\right)^{r_5} = \left(\frac{x^{r_3 p_0^{d-m_B}} \alpha^{r_4}}{x^{r_3 p_0^{d-m_B}}}\right)^{r_5} = \beta \tag{8}$$

   w.r.t. $(r_3, r_5, m_B)$. However, since there are three unknowns, Eq. 8 is underdefined and has more than one solution. In addition, the ranges of $r_3, r_5$ are too large for brute-force attacks.

Given the hardness of both cases, the secrecy of $m_B$ is therefore preserved. □

## 4 Conclusion

Common for the overwhelming majority of privacy-preserving *greater-than* integer comparison schemes is that cryptographic computations are conducted in a bitwise manner. Recently, Carlton et al. [2] and Bourse et al. [1] proposed privacy-preserving integer comparison schemes that work on whole integers in contrast to bitwise decomposition and encoding of the private inputs. In this paper, we have presented and analysed the Bourse scheme and shown that its security does not reduce to the small RSA subgroup decisional problem as claimed and that it is vulnerable to attacks. Inspired by the two mentioned papers, our other contribution is a comparison scheme that has a somewhat simpler construction and with clear security reductions.

## References

1. Florian Bourse, Olivier Sanders, and Jacques Traoré. Improved secure integer comparison via homomorphic encryption. Cryptology ePrint Archive, Report 2019/427, 2019. `https://eprint.iacr.org/2019/427`.
2. Rhys Carlton, Aleksander Essex, and Krzysztof Kapulkin. Threshold properties of prime power subgroups with application to secure integer comparisons. Cryptology ePrint Archive, Report 2018/224, 2018. `https://eprint.iacr.org/2018/224`.
3. Ivan Bjerre Damgård, Martin Geisler, and Mikkel Krøigaard. Homomorphic encryption and secure comparison. *International Journal of Applied Cryptography*, (1):22–31, 02 2008.
4. Ivan Damgård, Martin Geisler, and Mikkel Krøigaard. A correction to "efficient and secure comparison for on-line auctions". *IACR Cryptology ePrint Archive*, 2008:321, 01 2008.
5. Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82, pages 160–164, Washington, DC, USA, 1982. IEEE Computer Society.