Research on the security Oblivious Transfer protocol based on ECDDH

Xiaotian Wang\textsuperscript{a}, zichen Li\textsuperscript{b}

Beijing Institute of Graphic Communication School of Information Engineering
Beijing, China

\textsuperscript{a}972741827@qq.com, \textsuperscript{b}lizc2020@163.com

Abstract. A new type of Oblivious Transfer protocol is designed under the assumption of ECDDH. The protocol can be safely implemented under a malicious model, 1 of which are selected in N input values. The RAND function is defined under this assumption, and the security definition is given. Then, the security interaction mode of the sender and receiver is constructed. Finally, the correctness of the Protocol is analyzed and the security proof is given. The protocol has the interaction complexity of the constant number level, and the computational and communication complexity is only related to n linearity.

1. Introduction

With the rapid development of network technology, the massive collection of network information has caused people to pay attention to information security and privacy protection. Therefore, many cryptographic researchers have proposed a series of cryptographic schemes to avoid information leakage. Among them, one of the most concerned programs is secure multi-party computation, and many safe and feasible cryptographic protocols are designed. In these protocols, Oblivious Transfer as an essential tool plays an indispensable role in the protocol construction process.

Imagine a personal application scenario: the user needs to find the data he needs on the Internet, he must enter his or her needs into the search engine in clear text. When it comes to its own privacy, the user does not want to reveal his or her own search content, but also wants to get the desired data. In this way, the Oblivious Transfer can be well adapted to the needs of users.

The concept of dazed transmission was first proposed by Rabin in 1981, and has become an important basic primitive in the field of cryptography, and is widely used in the construction of other cryptography protocols. An extension given by Even \cite{2,3} et al. in 1985, An extended form, 1-out-of-2 OT(OT\textsuperscript{1} 2). The scenario mainly contains 2 parties, i.e. sender S and receiver R, where S has 2 input values, R wants to get one of them, but does not disclose their choice. In other words, a secure OT protocol must meet 2 security characteristics: 1) the sender does not know the receiver's choice information; Receivers cannot obtain any information about other data other than the data of their choice. In 1986, Brassard \cite{4} et al. for the first time expanded OT\textsuperscript{1} to OT\textsuperscript{1} and gave a basic construction pattern.

The main advantage of elliptic curve encryption is that it can use smaller keys under the same security compared to other encryption algorithms. The dazed transmission protocol designed in this paper is based on the assumption of the difficulty of determining discrete elliptic curves (ECDDH).
The main idea of the protocol is that the receiver R constructs 1 ECDDH. Groups and \( n-1 \) non-
ECDDH groups, a total of \( n \). In order to prevent the receiver R from constructing more than one
ECDDH group to obtain more information on sender S, zero knowledge proof technology is used to
ensure that R can honestly execute the protocol. Based on a single ECDH tuple zero knowledge proof
protocol, this paper gives batch ECDH Zero knowledge proof protocol of metagroups. After the
construction of the protocol is completed, the correctness of the protocol is proved, and the security of
the protocol is also given: under the malicious model, the receiver R and sender S are corrupted, the
protocol can also be safely executed. Finally, the efficiency of the protocol is analyzed. The results
show that the efficiency of the protocol is higher.

2. Basic theory

2.1. Assumption of ECDDH

Determining the assumption of ECDDH is similar to the assumption of DDH and is also a basic
assumption on number theory, and many cryptography schemes and protocols are established on that
assumption. So that G is a circular Abel group consisting of base point P on the standard elliptic curve,
generating elements as g, and orders of q. Given \( ag, bg, cg \), where, It is difficult to judge the
\( ab \equiv c (mod q) \), in other words, the assumption of ECDDH indicates that the following two distributions
are computationally indistinguishable:

\[
(1) x = (g, [a]g, [b]g, [ab]g), \text{where } a, b \in \mathbb{Z}^*
\]

\[
(2) x = (g, [a]g, [b]g, [c]g), \text{where } a, b, c \in \mathbb{Z}^* \text{ and } c \neq ab
\]

It can be seen that \( x_1 \) is an ECDH group and \( x_2 \) is a non-ECDH group, so the the assumption of
ECDDH can be expressed as it is difficult to determine whether a quaternions is an ECDH group or a
non-ECDH group.

2.2. 1-out-of-n Oblivious Transfer

1-out-of-n Oblivious Transfer have a protocol function \( F_{\text{ot}} \), as described below

Input: S input n values \((x_1, x_2, \ldots, x_n) \in \{0,1\}^n \), R input a value \( \sigma \in \{1, \ldots, n\} \)

Output: R output \( x_\sigma \)

Protocols designed for this function \( F_{\text{ot}} \) must satisfy R only get \( x_\sigma \) and do not disclose its message.

2.3. RAND function

The RAND function is a mapping relationship defined on group G. Defining a group G with a
order of \( q \) (\( q \) as a prime number) and generating a meta to g. The input of the RAND function is a
quaternions \((a, b, x, y)\) on group G, and the output is a number pair \((u, v)\) on group G that can be
expressed as \( RAND(a,b,x,y) = (u, v) \), where \( u = a \cdot s + x \cdot t \) and \( v = b \cdot s + y \cdot t \), where \( s, t \in \mathbb{Z}^+ \). and the
function has the following properties

(1) If the quaternions \((a, b, x, y)\) is an ECDH group, there is evidence that \( k \) satisfies \( b = ka \) and \( y = kx \),
then the output of the RAND function \( v = ku \)

(2) If the quaternions \((a, b, x, y)\) is a non-ECDH group, then the output of the RAND function \((u, v)\)
is two random elements in group G. That is, the following two distributions \((a, b, x, y, RAND(a,b,x,y))\)
and \((a,b,x,y, [\alpha]g, [\beta]g)\) are computationally indistinguishable, where \( \alpha, \beta \in \mathbb{Z}^+ \)

The above attributes of RAND function are mainly based on the hypothesis of ECDDH difficulty
and play a vital role in constructing the Oblivious Transfer protocol.

2.4. Security definition

(1) The indistinguishability of the calculation. If there are two distributions:
\[
X = \{X(a,n), a \in \{0,1\}^*; n \in N\} \text{ and } Y = \{Y(a,n), a \in \{0,1\}^*; n \in N\}
\]
is computationally indistinguishable, expressed as $X=Y$, needs to be satisfied when there is a negligible function $\mu(\cdot)$ for each non-uniform polynomial time algorithm $D$, and there is $|\Pr[D(X(a,n)=1)]-\Pr[D(Y(a,n)=1)]|\leq \mu(\cdot)$, for each $a$ and $n$.

(2) Fully simulated security definition. make $f : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ is a two-party functional function, $\pi$ is a real two-party protocol. $\pi$ can safely calculate $f$ under a malicious model, it must meet the need for each non-uniform probability polynomial time adversary $A$ for the realistic model, there is always an ideal model of the non-uniform probability polynomial time adversary $S$.

With each: $i \in \{1,2\}$, $\text{IDEAL}_{i,\pi_{(x,y,z,n,s)}}(x,y,z,n,s) = \text{REAL}_{i,\pi_{(x,y,z,n,s)}}(x,y,z,n,s)$, where $x,y,z \in \{0,1\}^*$ meets $|x|=|y|$, and $n,s \in N$.

3. 1out of n Oblivious Transfer

3.1. 1out of n Oblivious Transfer construction

In this section, we present a fully simulated 1out of n Oblivious Transfer protocol under the malicious enemy model. The main idea of the protocol is to create $n$-quads, and only one quad to meet the ECDH attributes.

**Input**: Sender S enters $n$ values $(x_1, x_2, ..., x_n) \in \{0,1\}^*$, receiver R input a value $\sigma \in \{0,1, ..., n-1\}$.

**Auxiliary input**: safety parameter $n$, and a $q$-order group $G$ on an elliptic curve, which generates a meta $g_0$.

**Output**: R output $x_\sigma$.

What the agreement is:

**Step 1**: R randomly selects $y_1, y_2, ..., y_n, k \in Z_q$ and calculates:

$$(g_i = [y_i]g, g_2 = [y_2]g, ..., g_n = [y_n]g)$$

and

$$(h = [k]g, h = [k+1]g, ..., h = [k+n-1]g)$$

Then sent $(h, (g_0, h_1, ..., g_n))$ to S.

**Step 2**: R Uses zero knowledge proof system to prove to S that there is a value $k$, satisfied:

$$h = [k]g, h = [k+1]g, ..., h = [k+n-1]g$$

That is, it is proved that the following n-1 quaternions: $(g_0, h_0, g_1, h_1, ..., g_n, h_n)$ are all ECDH groups and have the same multiple $k$. If S rejects, output $\bot$ and terminate the protocol. The following zero proof process for a given batch ECDH group:

1. R randomly selects the value $a \in Z_q$ and calculates $\alpha = ag_0$, then sends $\alpha$ to S.
2. S randomly selects the values $s, t, a_1, a_2, ..., a_s \in Z_q$ and calculates:

$$c = [s]g + [t]\alpha, g' = [a_1]g + [a_2]g + ... + [a_s]g$$

Then sends $c$ and $g'$ to R (this is a perfect hidden commitment to $c$, and $a_1, a_2, ..., a_s$ is a coefficient of random linear combinations)

3. R randomly selects the value $d \in Z_q$ and calculates

$$A = [d]g, B = [d]g',$$

and then sends $(A, B)$ to S.
4. S sends $s, t$ to R.
5. R first verify that if $c = s, g + t, \alpha$ is true or not, if not, terminate the agreement; Otherwise, R calculates $z = sk + r$, and then sends $z$ and $a$ to S.
(6) S verify that the following is true or not
1) \[ \alpha = [a]g \]
2) \[ A = [z]g_s - [s]h \]
3) \[ B = [z]g^* - [s]h^* \]

\[ h^* = [a_i](h - g_i) + [a_j](h_i - [2]g_s) + ... + [a_{n-1}](h_{n-1} - [n-1]g_s) \]

The above zero knowledge proof process requires 5 rounds of interaction, in which the participants exchange 9 group elements (of which R sends 5 and S sends 4), in addition to the participants calculating a total of \(2n+11\) times on the elliptical curve of the point multiplier operation (of which R calculates 6, S calculates \(2(n-1)+7\)).

Step 3: Receiver R randomly selects the value \( r \in Z^*_e \), and calculates \( g = rg_s, h = rh \), and then sends \((g, h)\) to R.

Step 4: S does as follows
1) Define the function \( \text{RAND}(w, x, y, e) = (u, v) \), where \( u = sw + ty, v = sx + te \), and \( s, t \in Z^*_e \).
2) For any \( i = 0, 1, ..., n-1 \), sender S first calculates \((u, v) = \text{RAND}(g_i, g, h, h)\), then calculates \( w_i = v_i + x_i \), and send \((u_i, w_i)\) to R.

Step 5: Receiver R output: \( x_s = w_s - [r]u_s \)

3.2. Proof of Agreement Correctness

If both parties are honest with the agreement, you can guarantee that R will only get \( x_s \), and we will analyze it according to \( i = \sigma \) and \( i \neq \sigma \).

(1) When: \( i = \sigma \)

The quaternions \((g_s, g, h, h) = (g_s, [r]g_s, h, [r]h)\) are the ECDH group.

\[ w_s - [r]u_s = [s]g + [t]h + x_s - [r]([s]g + [t]h) \]

\[ = [r]([s]g + [t]h) + x_s - [r]([s]g + [t]h) = x_s \]

(2) When: \( i \neq \sigma \)

The quaternions \((g_s, g, h, h) = (g_s, [r]g_s, h, [r]h)\) are not the ECDH group

\[ w_s - [r]u_s = [s]g + [t]h + x_s - [r]([s]g + [t]h) \]

\[ = [r]([s]g + [t]h) + x_s - [r]([s]g + [t]h) \neq x_s \]

3.3. Protocol security analysis

Receiver R to S proves that the four-piece structuring system is required by a zero-knowledge proof system, So R can only get a specific value sent by S. In addition to it, receiver R is still ignorant of the other input. Considering the privacy of R, because the ECDDH problem on the group is difficult, S can not distinguish which is the ECDH group, so it also does not know the choice of R. There are two types of processes:

(1) R is corrupted

To make T a real-life adversary, it can control R's behavior. We make up a simulator \( S' \) to call the enemy T input and do the following:

Step 1: Simulator \( S' \) receives the value \((h_s, h, g_s, h_s, h_s, h_s, h_s, h, h)\) from T and verifies zero proof of knowledge to the honest sender S.

1) If validation fails, \( S' \) sends \( \perp \) to a trusted third party to calculate the Oblivious Transfer function and aborts the protocol.
2) Otherwise, \( S' \) runs a zero knowledge proof system, obtains evidence \( k \), and then calculates the \([k+i]g\) and compares with \( h \) for \( i=0,1,2,...,n-1 \), and will make the two sides equal i-value note, set to the enemy T input \( \sigma \).

Step 2: \( S' \) sends the enemy real input \( \sigma \) to a trusted third party of the Oblivious Transfer function, getting the value \( x_\sigma \).

Step 3: \( S' \) will calculate \((u_\sigma, w_\sigma)\) according to the protocol, for the i value of \( i \neq \sigma \), \( S' \) randomly selects the elements in the group \( G \) and sends the value

\((u_\sigma, w_\sigma), (u_\sigma, w_\sigma), ..., (u_\sigma, w_\sigma)\) to the enemy T and outputs, and then aborts the protocol.

The above is the specific process of R corruption. Since S does not output during the implementation of the protocol, it is only necessary to prove that the output distribution of the adversary T and the simulator \( S' \) in the ideal world is indistinguishable from the output distribution of the real-world adversary T and the honest sender S. \( S' \) does not receive enough input \( x_\sigma \), so the resulting \((u_\sigma, w_\sigma)\) is only a randomly selected element on the group. But in the case of

\( i \neq \sigma \), the quaternions \((g_s, g_h, h)\) is not an ECDH group, further by RAND The nature of the function is known: the output of the quaternions s two elements of random independence on the group. Thus proves that the ideal simulation and the reality protocol are indistinguishable and secure.

(2) \( S \) is corrupted

Make T a real-life adversary, he can control the behavior of S. Fictitious a simulator ss ss calls the enemy T input and does the following:

Step 1: \( S' \) randomly selects \( y_1, y_2, ..., y_{n+1}, k \in Z_q \) and calculates \( g_1 = [y_1]g, g_2 = [y_2]g, ..., g_{n+1} = [y_{n+1}]g \), then sets \( h = [k]g, h = [k]g, ..., h = [k]g \), which is different from honest receiver R. Then \( S' \) sends

\((h_1, (g, h), ..., (g, h))\) to T.

Step 2: \( S' \) simulates the knowledge of the zero knowledge proof system and delivers step 1 to the adversary T, which means that R has completed the zero knowledge proof process and passed the verification.

Step 3: \( S' \) randomly selects a value \( r \in Z_q \) and calculates \( g = [r]g, h = [r]h \), and then sends \( (g, h) \) to T.

Step 4: \( S' \) receives the \((u_\sigma, v)\) value sent by T, \( S' \) calculates \((x_\sigma, x, ..., x_{n+1})\) after the honest R, then sends these values to the functional function of the calculation of the dazed transmission protocol, and then outputs the output of T and aborts the protocol.

In the above process, unlike the original protocol, the \( S' \) error construction \( h = [k]g, h = [k]g \) in step 1 makes all quaternions \((g_s, g_h, h), (g_s, g, h), ..., (g_s, g, h)\) be ECDH groups, which can be understood by the ECDDH hypothesis on the group: the ECDH group and the non-ECDH group are computationally indistinguishable and still meet the confidentiality of the input of R in the agreement.

3.4. Efficiency analysis of the protocol

The efficiency of the agreement consists of three main aspects:

(1) Number of interactive rounds. The above protocol requires a total of 6 rounds of interaction, including zero knowledge proof 5 rounds of interaction

(2) Point multiplier calculation. S and R are calculated as \( 4n \) and \( 2n+2 \) times times, respectively. Plus zero knowledge proof protocol \( 2(n-1) + 13 \) times, the total calculation of the protocol is \( 8n+13 \)

(3) Bandwidth. In the OT phase, R sends a total of \( 2n-1 \) group elements to S, S sends a total of \( 2n \) elements to R. Plus 9 group elements of the zero-knowledge proof protocol, and the agreement participants exchange a total of \( 4n-10 \) group elements.

4. Conclusion

The Oblivious Transfer protocol is of great significance in the data stealth transmission. This paper constructs the advantages of the ellipse curve inherited by the dazed transport protocol based on the
ECDDH hypothesis: (1) under the same security, it requires a smaller number of keys and a higher efficiency (2) the more secure ellipse curve. The problem of attacking discrete xrexis can be used by exponential integral, but the discrete xeral problem on the elliptic curve is not valid. The literature shows that the computational complexity of calculating elliptic curves is higher than that of discrete pairs.

References

[1] Yao, Andrew Chi-Chih. How to generate and exchange secrets [P]. Foundations of Computer Science, 1986., 27th Annual Symposium on, 1986.

[2] Even S, Goldreich O, Lempel A. A Randomized Protocol for Signing Contracts [J]. Acm Sigact News, 1983, 15 (1): 34-39.

[3] Goldreich O. A randomized protocol for signing contracts [J]. Information Theory IEEE Transactions on, 1985, 36 (1): 40-46

[4] Brassard G, Crepeau C, Robert J M. All-or-Nothing Disclosure of Secrets [C]// On Advances in Cryptology-crypto. 1987

[5] Yadong Qu,Zifeng Hou ,Wei Wei. A Protocol for Signing Contracts Based on Oblivious Transfer [J]. Journal of Computer Research and Development, 2003 (04): 615-619.

[6] Bing Zhang, Qiuliang Xu,Han Jang. New recombination of resistant adaptive enemy Oblivious Transfer protocols [C]// China Computer Networks and Information Security Conference. 2011.

[7] Hazay C, Lindell Y. Efficient Secure Two-Party Protocols: Techniques and Constructions[M]// Efficient secure two-party protocols. 2010.

[8] Lindell Y, Pinkas B. An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2007.

[9] Xiaochao Wei,Han Jang,Chuan Zhao. An efficient and fully simulated 1-out-of-n Oblivious Transfer protocol [J]. Journal of Computer Research and Development, 2016, 53 (11): 2475-2481.

[10] Xiaochao Wei. The basic theory of high-efficiency and safety safety computing and the research on key technologies [D]. Shandong University,2017.

[11] Chuan Zhao,Han Jang,Xiaochao Wei ,Qiuliang Xu.Cut-and-Choose Oblivious Transfer [J]. Journal of Software, 2017, 28 (02): 352-360.

[12] Chunming Tang,Zhengan Yao,Dongqin Xie. Verifiable oblivious transfer protocol [J]. Journal of Guangzhou University(Natural Science Edition), 2010, 9(02): 20-24.

[13] Parakh, A.. Communication Efficient Oblivious Transfer Using Elliptic Curves [P]. High-Assurance Systems Engineering (HASE), 2012 IEEE 14th International Symposium on,2012.

[14] Dowsley, R.,Lacerda, F.,Nascimento, A.C.A.. Oblivious transfer in the bounded storage model with errors[P]. Information Theory (ISIT), 2014 IEEE International Symposium on,2014