OBLIVIUS TRANSFER

UNTERZEICHNEN VON VERTRÄGEN

Marcel Berg

Verfahren der modernen Kryptographie

31.01.2002

GLIEDERUNG

Einleitung:

I. Oblivius Transfer OT

A. mechanisches Modell

B. Implementation

II. Variante des Oblivius Transfer OT½

A. mechanisches Modell

B. Implementation

III. Äquvalents von OT und OT1/2

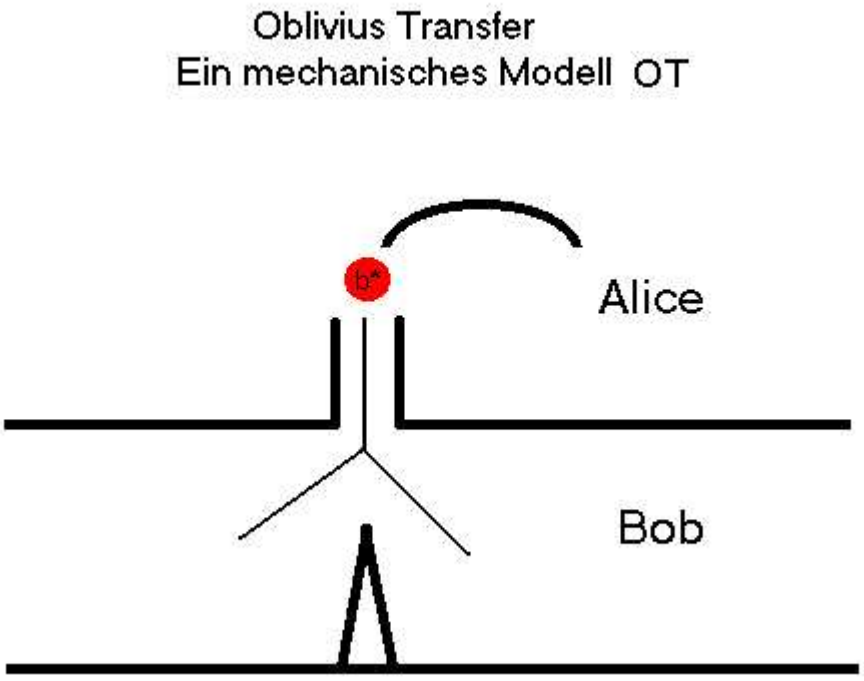
IV. Unterzeichnen von Verträgen

Oblivius Transfer

Einleitung:

Oblivius Transfer heißt soviel wie „Übertragung ohne Gedächtnis“ und ist eine Art kontrolliertes Zufallsexperiment.
Neuste Forschungen haben gezeigt, daß man die gesamte Kryptographie auf diesem Protokoll aufbauen kann.
Aber alle bekannten Implementierungen sind noch zu langsam, so daß ein praktischer Einsatz dieses Protokolls heute noch nicht möglich ist.

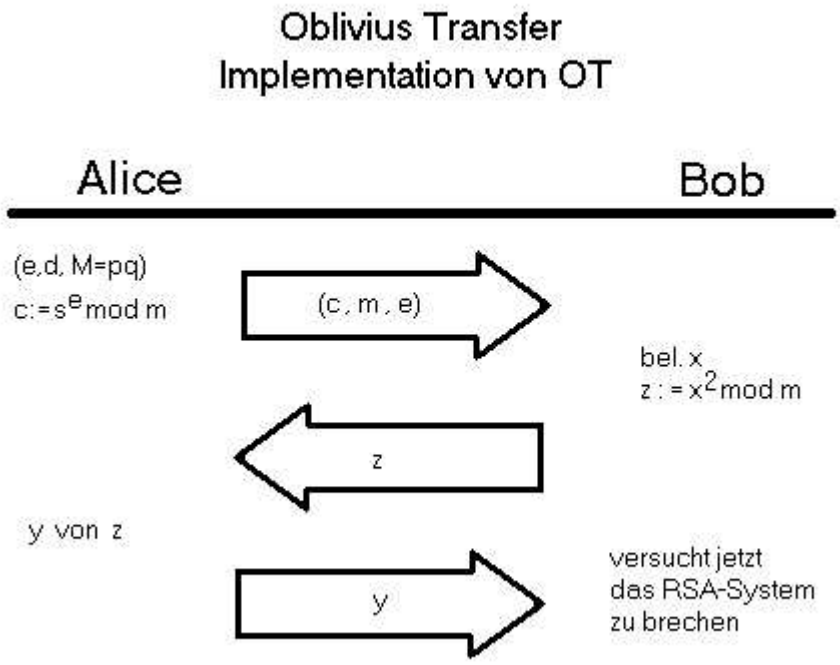
Oblivius Transfer OT



Dabei stellen Alice und Bob folgende Forderungen.

1. Bob soll die Nachricht mit einer Wahrscheinlichkeit von ½ erhalten.
2. Alice darf nicht wissen, welcher der beiden Möglichen Fälle eingetreten ist.

Wir stellen uns vor das Alice einen Ball mit der Nachricht b* durch ein Rohr in das untere Stockwerk wirft.
Der Ball fällt auf eine Mauer, die dieses Stockwerk in zwei Räume Teilt.
Er prallt von ihr ab und fällt mit einer Wahrscheinlichkeit von ½ in den linken oder in den rechten Raum.
Die Forderung für Bob ist also erfüllt.
Die Forderung für Alice ist erfüllt, wenn sie durch das Rohr nicht sehen kann in welchen Raum der Ball gefallen ist.



Alice wählt die zu einem RSA Protokoll nötigen Schlüssel (e, d) und die Zahl m = p*q.
Im ersten Schritt verschlüsselt Alice die Nachricht s mit dem RSA Verfahren und erhält die Verschlüsselung c.
Sie sendet Bob den Wert c und macht den Schlüssel e und die Zahl m bekannt (im Internet).
Im zweiten Schritt berechnet Bob einen quadratischen Rest (QR) von einer Zahl x, die er sich wählt und sendet den Wert z Alice.
Im dritten Schritt berechnet Alice eine Zahl y für die der QR z ist und sendet Bob den Wert y)
Im letzten Schritt versucht Bob das RSA Verfahren zu brechen.

Matematische Grundlagen:

Gilt für z: ggT(z, n) = 1

FALL 1: n = p Primzahl und für 3 = p mod 4

Dann gilt: $x = z^{(p+1)/4} \bmod p$ sind die einzigen Quadratwürzeln des QR z im mod p.

$(z = x^2 \bmod p)$

FALL 2: n = p * q mit p, q Primzahlen, ggT(z, p) = ggT(z, q) = 1

Dann berechnet man y1 mit FALL 1 und n = p
und y2 mit FALL 1 und n = q.

Nach dem Chinesischen Restsatz erhält man dann die 4 Quadratwurzeln x_i, so dass $z = x_i^2 \bmod p * q$.

Chinesischer Restsatz:

Das System simultaner Kongruenzen

$x \equiv a_1 \pmod p$
$x \equiv a_2 \pmod q$

besitzt genau eine Lösung x in Z_M mit M = p * q

Lösung:

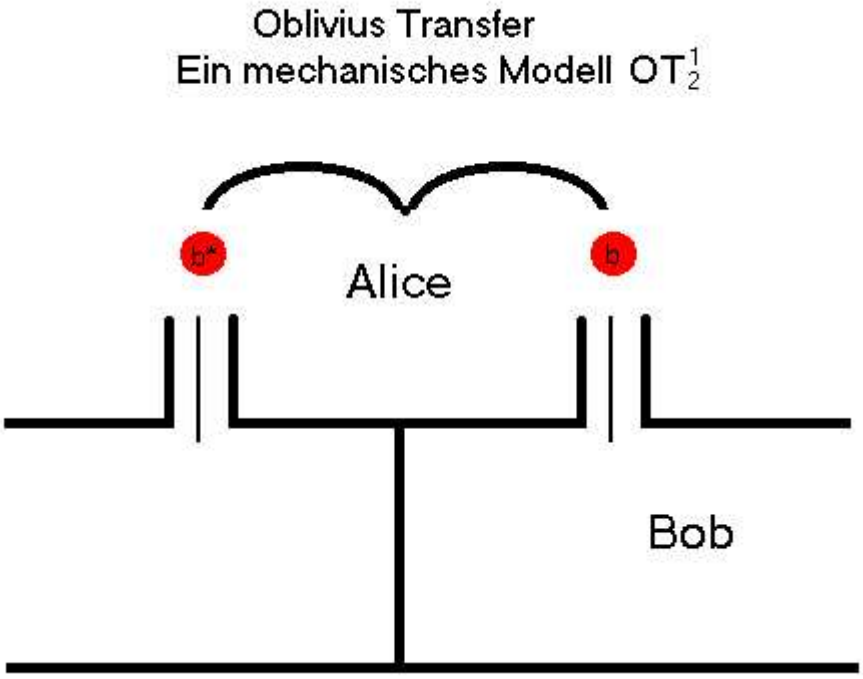
$M_1 = M/p = q \implies ggT(p, M_1) = 1$
$M_2 = M/q = p \implies ggT(q, M_1) = 1$

$N_1 M_1 \equiv 1 \pmod p$ und $N_2 M_2 \equiv 1 \pmod q$
erhält man die N_i.

Das führt zur Lösung

$$x \equiv a_1 * N_1 * M_1 + a_2 * N_2 * M_2 \pmod M$$

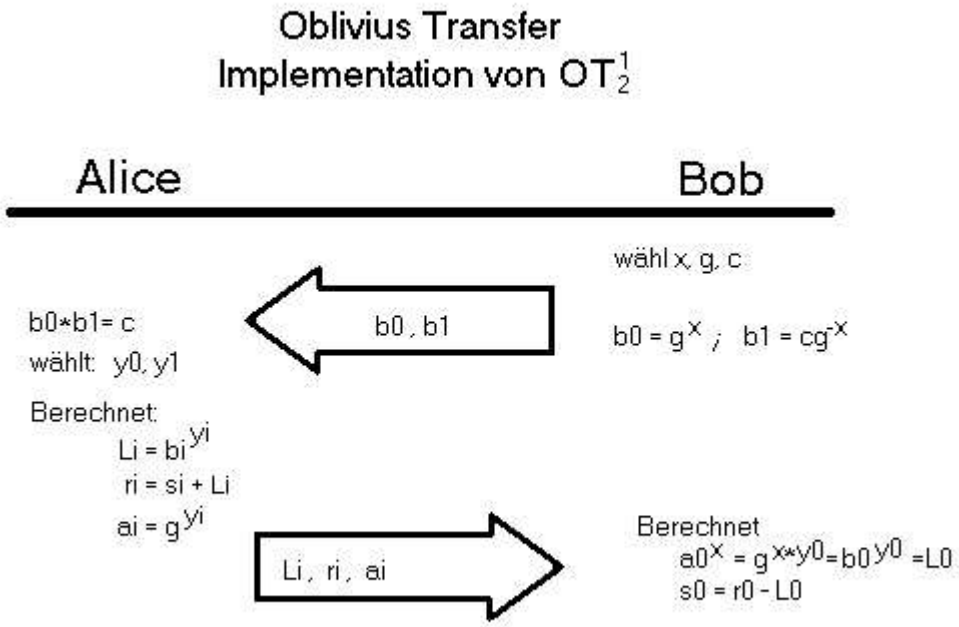
Man setzt die Kombinationen (y1, y2), (-y1, y2), (y1, -y2), (-y1, -y2) in den Chinesischen Restzatz als (a1, a2) ein und berechnet die 4 Quadratwurzeln.



Dabei stellen Alice und Bob folgende Forderungen.

1. Bob holt sich genau einer Nachricht, er kann dabei zwischen b und b* wählen.
2. Alice darf nicht wissen, welche Nachricht Bob erhält.

Wieder wirft Alice eine Nachricht in das untere Stockwerk, dass wieder in zwei Räume unterteilt ist.
Alice wirft die Nachricht b* in den linken und b in den rechten Raum.
Bob kann sich den Raum aussuchen und wählt sich damit die Nachricht aus (wenn er b haben möchte geht er in den rechten Raum).
Dabei hat Bob nur zu genau einen Raum zutritt.
Daraus folgt Bob erhält nur genau eine Nachricht und Alice weiß nicht welche, weil sie nicht sehen kann in welchen Raum Bob sich befindet.



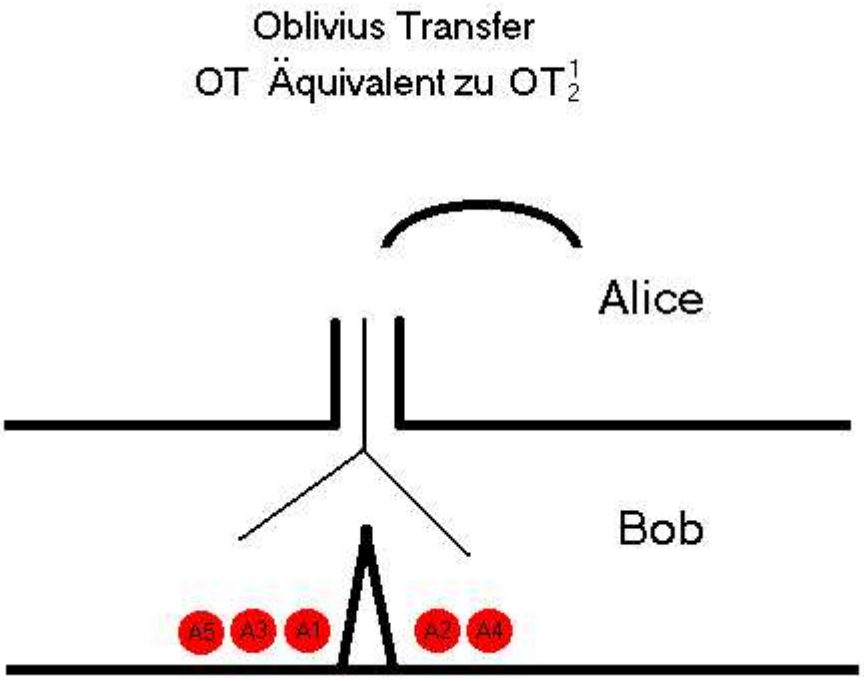
Bob und Alice wählen sich eine Basis g und eine Zahl c, deren diskreter Logarithmus unbekannt ist.
Im ersten Schritt wählt Bob sich eine Zahl x und berechnet b0 und b1 wie in der Abbildung, wenn er die Nachricht s0 haben will.
Dann sendet er b0 und b1 an Alice.
Im zweiten Schritt kontrolliert Alice ob b0 * b1 = c ist, wählt sich zwei Zahlen (y0, y1) und dann löst die Gleichungen $Li = bi^{yi}$ für i = 1,2 .
Jetzt verschlüsselt sie die Nachricht si mit der Gleichung ri = si + Li.
Zum Schluss berechnet sie noch zwei Schlüssel $ai = g^{yi}$.
Im letzten Schritt berechnet Bob $L0 = a0^x$ und s0 = r0 – L0 und hat nun die Nachricht s0 entschlüsselt.

Wenn er die Nachricht s1 haben will berechnet er b0 = b1 (b1 von der Abbildung) und b1= b0(b0 von der Abbildung) und berechnet zum Schluss nicht s0 sondern s1.

Äquivalentz von OT und OT½

Das man aus OT½ ein OT machen kann ist ganz leicht nachzuweisen.
Alice wirft nur eine Nachricht zu Bob, wobei sie eine Münze wirft um zu entscheiden in welches Rohr sie die Nachricht wirft.
Daraus folgt das Bob die Nachricht mit einer Wahrscheinlichkeit von ½ und Alice weiß nicht ob er sie erhalten hat.

Das man aus OT ein OT½ machen kann ist nicht so leicht zu zeigen.
Claude Crepeau hat dies mit folgendem Verfahren gezeigt.



Im ersten Schritt wirft Alice Balle(die Nachrichten enthalten), die von 1 bis n nummeriert sind, in das untere Stockwerk.
Dabei wird n so groß gewählt, dass mit einer sehr großen Wahrscheinlichkeit in einem Raum minimal n/3 und maximal 2*n/3 Bälle fallen.
Im zweiten Schritt schickt Bob zwei Listen zu Alice.
Die Liste 1 enthält die Nummern der Bälle deren Nachrichten Bob bekannt sind und die Liste 2 enthält die Nummern der Bälle deren Nachrichten Bob unbekannt sind.
Im dritten Schritt addierte Alice zu der Nachricht 1 die Summe der Nachrichten aus der 1. Liste, zu der Nachricht 2 die Summe der Nachrichten aus der 2.Liste und sendet Bob diese beiden Werte.
Im letzten Schritt braucht Bob nur von dem Wert 1 die die Summe der Nachrichten aus der 1. Liste abziehen und hat nun die Nachricht 1.

Wenn er die Nachricht 2 haben möchte braucht er nur die Listen zu vertauschen.

Unterzeichnen von Verträgen

Wenn man einen gültigen Vertrag haben möchte müssen beide Vertragspartner unterzeichnen.
Sollte sich diese Persönlich gegenüberstehen ist das keine Schwierigkeit.
Über das Internet könnte einer den Vertrag unterschreiben, dem anderen zuschicken und dieser Unterzeichnet auch, aber er schickt diesen nicht zurück.
Damit hat der zweite einen gültigen Vertrag und kann den anderen dazu bringen sich an den Vertrag zu halten.
Wärend der erste das nicht kann, er ist davon abhängig, dass der zweite den Vertrag einhalten möchte.

Nun versuchen wir dieses Problem zu lösen:

1) Mit einer vertrauensvollen dritten Partei (TTP)

   Die beiden Vertragspartner senden der TTP einen signierten und einen unsignierten Vertrag.
   Die TTP überprüft, ob die Signierung gültig ist und wenn ja signiert sie beide signierten Verträge.
   Die TTP sendet zum Schluss jedem Vertragspartner den signierten Vertrag des anderen zu.
   Nun kann jeder diesen Vertrag signieren und halten nun einen Vertrag in der Hand, der von beiden Vertragspartnern und dem Notar signiert worden ist.

2) nur mit den beiden Vertragspartnern

   Im ersten Schritt teilen beiden den Vertrag auf n verschiedene Weise in zwei Hälften.
   Diese werden nummeriert, wobei v(1) und v(n + 1) die beiden zueinander gehörenden Hälften darstellen.
   Nun signieren beide ihre v(i) und erhalten dann $D_A(i)$ und $D_B(i)$.
   Im zweiten Schritt gibt jeder dem anderen mit Hilfe des OT½ Verfahren die signierten Hälften v(i) und v(n + 1) an den anderen Weiter.
   Im dritten Schritt werden von jeden die 2n Hälften bitweise übertragen.
   Das erste Bit von $D_A(1)$, $D_A(2)$, ... , $D_A(2n)$, $D_B(1)$, $D_B(2)$, ... , $D_B(2n)$ und dann das zweite Bit usw. bis alle Bits übertragen wurden.

Jetzt muss man noch überprüfen, ob einer der Vertragspartner den anderen betrügen Kann.
Wenn einer im ersten Schritt betrügen möchte, könnte er die Hälften falsch signieren.
Dann würde dies im zweiten Schritt auffallen, denn der andere kann alle Hälften die er erhalten hat überprüfen.
Wenn einer im dritten Schritt betrügen möchte müsste er im ersten Schritt eine Hälfte des Vertrages falsch signieren und die andere Hälfte richtig signieren.

Die Wahrscheinlichkeit das er die Hälfte richtig signiert die der andere sich im zweiten Schritt aussucht liegt bei ½.
Er muss aber um betrügen zu können bei allen Vertragshalbierungen richtig raten und damit liegt die Wahrscheinlichkeit bei $(½)^n$.
Nun könnte er noch im dritten Schritt früher aufhören, da er zum Beispiel als letzter die letzten Bits sendet.
Das heißt er erhält alle Bits und hat damit mindesten einen gültigen Vertrag, während dem anderen das letzte Bit von jeder Hälfte fehlt.
Die eine Hälfte hat er im zweiten Schritt erhalten und die andere braucht er nur durch ausprobieren des fehlenden Bits ergänzen.
Sollte der erste Partner früher auf aufhören braucht der zweite gerade mal doppelt so lange wie der erste.
Damit haben wir gezeigt, dass man mit 2) eine schöne und sichere Möglichkeit hat einen Vertrag zu unterschreiben.