NEW PROVABLY SECURE BLIND SIGNATURE SCHEME WITH WEIL PAIRING

Neetu Sharma
School of Studies in Mathematics,
Pt. RavishankarShukla University
Raipur (C.G.) 492010 India
Email: nitusharma013@gmail.com

Birendra Kumar Sharma
School of Studies in Mathematics,
Pt. RavishankarShukla University
Raipur (C.G.) 492010 India
Email: sharmabk07@gmail.com

ABSTRACT

Blind signature scheme provide the feature that a user is able to get a signature without giving the actual message to the signer. Many Blind signature schemes have been proposed in which security are based on intractability of factoring or DLP (Discrete Logarithm Problem). In 2010, Fan et al.[11] gave a provably secure randomized blind signature whose security was based on solving ECDLP(Elliptic Curve Discrete Logarithm Problem). The security of this scheme is improved in order to propose a more secure and efficient scheme. The security of proposed scheme is based on expressing the torsion point of curve into linear combination of its basis points. This is more complicated than solving ECDLP (Elliptic Curve Discrete Logarithm Problem). Also, the simulation results from AVISPA tools confirm the security analysis of proposed protocol.

Keywords –Cryptography, Blind signature scheme, Elliptic curve cryptosystem, Chosen message attack, AVISPA.

I. INTRODUCTION

Blind signature is a type of digital signature, in this signature the content of a message is blinded before it is delivered, hence the name blind signature. Blind signature can be used in many applications, where authentication, integrity, non - repudiation, sender privacy etc. are necessary like e-mails, e-cash systems, software distributions, documents verification etc. Blind signatures have the additional properties like untraceability, can be used in applications where anonymity of the sender is required like electronic voting etc.

Dr. D. Chaum was the first scholar to propose the concept of the Blind signature scheme in 1982 [1]. This concept is widely used in electronic voting systems and electronic payment systems. In 1994, J. L. Camenisch, J. M. Priveteau and M. A. Stalder [2] first proposed the Blind signature based on discrete logarithm problems. Later, in 1995, Harn [3] claimed that the blind signature in [2] is traceable by the signer. However, in 1995, Horster et al. [4] illustrated that the signer cannot trace back to the owner of the signature. In 2001, H. Y. Chien, J. K. Jan and Y. M. Tseng [5] proposed the blind signature based on RSA algorithm. In 2003, M. S. Hwang, C. C. Lee and Y. C. Lai [6] proposed an untraceable Blind signature scheme based on RSA and Extended Euclidean algorithm [7]. Inspired by cryptanalysis techniques in [3], in 2005, Lee et al. [8] illustrated that the Camenisch et al.'s scheme does not satisfy the untraceability. To overcome this weakness, they proposed a new blind signature scheme based on the DLP.

In 2007, Jena et al. [9] presented a novel blind signature scheme (BSS) based on Nyberg – Rueppel Signature Scheme (NRSS) using Elliptic Curve Discrete Logarithm Problem (ECDLP). This algorithm is employed in off line digital cash payments which can be easily extended to E – voting application.

In 1994, Ferguson [10] suggested that the signer had better inject one or more randomization factors into the message to prevent attackers from predicting the exact content of the message the signer signs. In 2000, Fan, Chen, Yeh [11] proposed a randomization enhanced Blind signature scheme. They took a different approach to make the D. Chaum's blind signature scheme immune to the chosen plaintext attack. In 2001, Chien, Jan, and Tseng [5] also proposed a RSA based randomization enhanced partially Blind Signature Scheme.

In the last couple of years, the bilinear pairing has become flourishing area in cryptography, namely Weil pairing and Tate pairing are important tools for construction of ID-based cryptographic scheme. In 2010, Fan et al.[11] proposed provably secure randomized blind signature scheme based on bilinear pairing whose security was based on solving ECDLP. The security of [14] is modified in proposed paper to gain more security and enhanced efficiency.

This paper is organized into five sections. The next section briefly introduces some mathematical backgrounds. In section 3, a new blind signature scheme with weil pairing is proposed. In section 4 and 5, the security and efficiency of the new scheme is analyzed. Last section is conclusion.

2. PRELIMINARIES

Definition 2.1.Elliptic Curve

Let $K = F_q$ be a finite field, where q is a power of some prime number. The Weierstrass equation of an elliptic curve over K can be written in the following form:-

$$y^2 + cxy + dy = x^3 + ax + b$$
$$where\ a, b, c, d \in K$$

If $q > 3$ then by a linear change of variables above equation can be reduced in simpler form

$$y^2 = x^3 + ax + b\ with\ a, b \in GF\ (q)\ and$$
$$4a^3 + 27b^2 \neq 0,$$

An elliptic curve over K is the set of solutions of the Weierstrass equation with a point O, called point at infinity. An adding operation can be defined over the elliptic curve, which turns the set of the points of the curve into a group. The adding operation between two points is defined as follows.

In affine coordinates let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the elliptic curve, neither being the point at infinity over $GF\ (q)$. The inverse of a point P_1 is $-P_1 = (x_1, \ -y_1)$.

If $P_1 \neq P_2$ then $P_1 + P_2 = P_3 = (x_3, y_3)$ with

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

where

$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, if $P_1 \neq P_2$

$= \frac{3x_1^2 + a}{3y_1}$, if $P_1 = P_2$ (doubling)

Definition 2.2.Torsion Points and Basis Points

Let $m \geq 1$ be an integer. A point $P \epsilon E$ satisfying $mP = O$(point at infinity) is called point of order m in the group E. The set of points of order m is denoted by

$$E[m] = \{P \in E;\ mP = O\}$$

Such points are called points of finite order or torsion points. If P and Q are in $E[m]$ then $P + Q$ and $-P$ are also in$E[m]$, so $E[m]$ is subgroup of E.

Proposition 2.1. Let $m \geq 1$ be an integer

(1) Let E be an elliptic curve over Ror C. Then

$$E(K)[m] \cong \frac{Z}{mZ} \times \frac{Z}{mZ}$$

(2) Let E be an elliptic curve over F_q and assume that p does not divide m then there exists a value k such that

$$E\left(F_{p^{jk}}\right)[m] \cong \frac{Z}{mZ} \times \frac{Z}{mZ} \ \ for\ all\ j \geq 1$$

Proof. For the proof of proposition refer [15], Corollary III 6.4.

According to proposition, if we allow points with coordinates in a sufficiently large field, then $E[m]$looks like a 2-dimensional vector space over the field Z/mZ. Let'schoose basis P_1, P_2 in $E[m]$. Then any element $P \in E[m]$ can be expressed in terms of the basis elements as $P = aP_1 + bP_2$ for unique a, b in Z/mZ. Expressing a point in terms of the basis points P_1, P_2 is more complicated than solving ECDLP [16].

Definition2.3.Weil pairing [15]:- Weil pairing $e_m : E[m] \times E[m] \rightarrow G$, where G is a multiplicative group of m^{th}roots of unity. Weil pairing is denoted by e_m, takes as input a pair of points $P, Q \in E[m]$ and gives as output an m^{th} root of unity $e_m(P, Q)$. The bilinearity of the Weil pairing is expressed by the equations

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$$
$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$$

The weil pairing has many useful properties:-

a) The values of the Weil pairing satisfy $e_m(P, Q)^m = 1$ for all $P, Q \in E[m]$.
b) The Weil pairing is alternative, which means that $e_m(P, P) = 1$ for all $P \in E[m]$.
c) The Weil pairing is non-degenerate, which means that if $e_m(P, Q) = 1$ for all $Q \in E[m]$ then $P = O$.

3. A NEW RANDOMIZED BLIND SIGNATURE SCHEME

The implementation of the proposed new blind signature scheme involves the initialization phase, blinding phase, Signing Phase, Unblinding phase, Verification phase as below :-

3.1. System initialization Phase :- In the system initialization phase, the commonly required parameters are generated to initialize the scheme :-

a) A field size q, which is selected such that, q = p if p is an odd prime, otherwise, $q = 2^n$, as q is a prime power.
b) Two parameters $a, b \in F_q$ that define the equation of elliptic curve E over F_q $(y^2 = x^3 + ax + b(modq)$ in the case $q > 3$, where $4a^3 +$

$27b^2 \neq 0(modq))$.

c) A large prime number m, and basis points P_1 and P_2 of $E[m]$.

d) Weil pairing $e_m : E[m] \times E[m] \to G$, where G is a multiplicative group of m^{th} roots of unity.

e) $H(,)$ a secure hash function.

f) A positive integer t, which is the secure parameter, say $t \geq 72$ [7].

3.2.**Blinding Phase:-**The signer U compute secret and public key pair using two basis point $P_1, P_2 \in E[m]$.

a) Randomly select integers $r_{a_1}, r_{a_2} \in_R Z_q^*$ from the interval $[1, 2, \ldots, n-1]$ as the secret key.

b) Compute the corresponding public key as $P_a = r_{a_1}P_1 + r_{a_2}P_2$, where $P_1, P_2 \in E[m]$ be two basis point, and send P_a to user.

c) After receiving it, the user prepares a plaintext message M, and selects $r_{b_1}, r_{b_2} \in_R Z_q^*$ and compute
$$P_b = r_{b_1}P_1 + r_{b_2}P_2$$

And compute the blinded message,
$$K_1 = r_{b_2}P_1$$
and
$$K_2 = r_{b_2}P_2 + H(M||P_b)$$

The user then transmits (K_1, K_2) to the signer.

3.3. Signing Phase :- The signer signs on (K_1, K_2) by producing

$$T = r_{a_1}K_1 + r_{a_2}K_2$$

3.4. Unblinding phase :- After obtaining the blind signature T, the user extracts the signature

$$S = T - r_{b_2}P_a$$

The signature – message triple is (S, M, P_b).

3.4.Verification phase :- The validity of the signature – message triple (S, M, P_b) can be verified by the formula –
$$e_m(P_1, SP_2) = e_m(P_1, P_a)^{H(M||P_b)}$$

3.5. Correctness of scheme:-

Theorem3.1. The equation $e_m(P_1, SP_2) = e_m(P_1, P_a)^{H(M||P_b)}$ is correct.
Proof :-

$$\begin{aligned}
e_m(P_1, SP_2) &= e_m(P_1, (T - r_{b_2}P_a)\,P_2) \\
&= e_m(P_1, (r_{a_1}K_1 + r_{a_2}K_2 - r_{b_2}P_a)\,P_2) \\
&= e_m(P_1, (r_{a_1}(r_{b_2}P_1) + r_{a_2}\,(r_{b_2}P_2 + H(M||P_b)) \\
&\qquad - r_{b_2}P_a)\,P_2) \\
&= e_m(P_1, (r_{a_1}r_{b_2}P_1 + r_{a_2}\,r_{b_2}P_2 + r_{a_2}\,H(M||P_b) \\
&\qquad - r_{b_2}P_a)\,P_2) \\
&= e_m(P_1, (r_{b_2}(r_{a_1}P_1 + r_{a_2}P_2) + r_{a_2}\,H(M||P_b) \\
&\qquad - r_{b_2}P_a)\,P_2) \\
&= e_m(P_1, (r_{b_2}P_a + r_{a_2}\,H(M||P_b) - r_{b_2}P_a)\,P_2) \\
&= e_m(P_1, r_{a_2}\,H(M||P_b)P_2) \\
&= e_m(P_1, r_{a_2}P_2)^{H(M||P_b)} \\
&= e_m(P_1, r_{a_1}P_1 + r_{a_2}P_2)^{H(M||P_b)} \\
&= e_m(P_1, P_a)^{H(M||P_b)}
\end{aligned}$$

4. SECURITY ANALYSIS:-

We use the following lemma and other security properties to discuss the security of our scheme and also we use AVISPA tool for security analysis.

Lemma 4.1. If one can express a point of elliptic curve into linear combination of basis points then he can easily solve ECDLP.
Proof. Solving the ECDLP for P means that if Q is a multiple of P, then find m so that $Q = mP$. If Q is any point of elliptic curve then expressing Q in terms of the basis means finding m_1 and m_2, so that $Q = m_1P_1 + m_2P_2$. If we can solve the former, then given P and Q, write $P = n_1P_1 + n_2P_2$ and $Q = m_1P_1 + m_2P_2$. Since P_1 and P_2 are independent, if $Q = kP$, then

$$m_1 = k * n_1 \ mod(orderP_1)$$
$$m_2 = k * n_2 \ mod(orderP_2)$$

From this one can solve for k modulo the order of P.

Blindness :- Blindness is the first important property in a blind signature scheme. In our scheme, the signature – requester (user) has to submit the blinded data K_1, K_2 to the signer, and then the signer computes $T = r_{a_1}K_1 + r_{a_2}K_2$ and sends to the signature – requester. The signer does not know the content of the message.

Randomization :- In the proposed scheme, the signer randomizes the blinded data using the random $r_{a_1}, r_{a_2} \in_R Z_q^*$, in the blinding phase the signer select integers $r_{a_1}, r_{a_2} \in_R Z_q^*$and sends $P_a = r_{a_1}P_1 + r_{a_2}P_2$ to the user. Then the user sends K_1, K_2 to the signer.

The signer returns $T = r_{a_1}K_1 + r_{a_2}K_2$

to the signature requester. If the user tries to remove r_{a_1}, r_{a_2} from T, then he has to solve $P_a = r_{a_1}P_1 + r_{a_2}P_2$ which is clearly infeasible.

Unforgeability :-

Attack I. Suppose eavesdropper is able to solve ECDLP. Since P_1 and P_2 are independent. So P can not be expressed as scalar multiple of P_1 and P_2. Hence Adv cannot use ECDLP to find the values of r_{a_1} and r_{a_2} from $P_a = r_{a_1}P_1 + r_{a_2}P_2$.

Attack II. Adv wishes to obtain blinded message (K_1, K_2) using all information that available from the system. Adv needs to obtain secret key of user r_{b_1}, r_{b_2} for which Adv needs to solve $P_b = r_{b_1}P_1 + r_{b_2}P_2$ which is clearly infeasible because the difficulty is based on expressing the torsion point of curve into linear combination of its basis points, it is more complicated than solving ECDLP.

Untraceability :- Untraceability is also an important requirement in the Blind signature scheme. The signer is unable to link the signature with the message when publishing the message – signature pair (S, M, P_b). In the proposed blind signature scheme, if the signer wants to track the Blind signature, when the requester publishes the message–signature pair (S, M, P_b) in public, the signer cannot get any information from the set of values that he/she keeps. Because the signer does not know the values including $r_{b_1}, r_{b_2} \in_R Z_q^*$ he/she cannot trace the relationship between the message–signature pair and the Blind signature.

Simulation Result :-

In the last decade, we have witnessed the development of a large number of new techniques for the formal analysis of security protocols. One of the analysis tools that has the widest use in the cryptography is the AVISPA. AVISPA is a push-button tool for the automated validation of the Internet security-sensitive protocols and applications. It provides a modular and expressive formal language for specifying protocols and their security properties, and integrates different back-ends that implement a variety of state-of-the-art automatic analysis techniques[17].

The AVISPA tool has four different back-ends: On-the-fly Model-Checker(OFMC), CL-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC) and Tree-Automata-based Protocol Analyzer (TA4SP). These back-ends perform the analysis and output the results in precisely defined output format stating whether there are problems in the protocol or not.

In order to evaluate the security of the proposed protocol by the AVISPA tools, the protocol is first coded in HLPSL. The HLPSL code of the protocol is included in Appendix A. After execution of the code in AVISPA tool, OFMC, CL–AtSe, SATMC back-ends outputs were generated. According to the summary results of the outputs shown in Figure , the proposed protocol is safe and there are no major attacks to the proposed protocol[18].

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/web-interface-
computation/./tempdir/workfileSU4bKU.if
GOAL
as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.05s
visitedNodes: 13 nodes
   depth: 4 plies
```

```
  SUMMARY
    SAFE
  DETAILS
    BOUNDED_NUMBER_OF_SESSIONS
    TYPED_MODEL
  PROTOCOL
    /home/avispa/web-interface-
  computation/./tempdir/workfileSU4bKU.if
  GOAL
    As Specified
  BACKEND
    CL-AtSe
  STATISTICS
  Analysed   : 0 states
    Reachable  : 0 states
    Translation: 0.01 seconds
Computation: 0.00 seconds
```

```
    SUMMARY =  SAFE
    DETAILS      STRONGLY_TYPED_MODEL

    BOUNDED_NUMBER_OF_SESSIONS
                  BOUNDED_SEARCH_DEPTH
                 BOUNDED_MESSAGE_DEPTH
    PROTOCOL
      workfileSU4bKU.if
    GOAL    =   %% see the HLPSL specification..
    BACKEND
      SATMC
    COMMENTS
    STATISTICS
      Attack Found               false     boolean
      Upper Bound Reached          true      boolean
      Graph Leveled Off            2        steps
      Sat Solver                 zchaff    solver
      Max Steps Number             11       steps
      Steps Number               2        steps
      Atoms Number                0        atoms
      Clauses Number              0        clauses
      Encoding Time              0.02      seconds
      Solving  Time              0        seconds
      if2sateCompilationTime    0.11      seconds

ATTACK TRACE     :-    %% no attacks have been
found..
```

5. EFFICIENCY:-

Table 1 defines our notation. The time complexity of the proposed protocol and some other protocol in terms of modular multiplication operation, modular weil pairing operation, modular inverse operation, modular scalar multiple scalar multiplication and one way hash function is shown in table 1.Table 2 shows the efficiency comparison of our newly propose scheme with the scheme Fan et al.[11].

Table 1. Time complexity of various operations

Notation	Definition
T_{BP}	Time complexity for the execution of a bilinear pairing.
T_{EC-MUL}	Time complexity for the execution of an elliptic curve multiplication.
T_{SM}	Time complexity for the execution of a scalar multiple scalar multiplication.
T_{EXP}	Time complexity for the execution of a exponentiation.
T_{IN}	Time complexity for the execution of an inversion.
T_H	Time complexity for the execution of a hash function.
T_{MUL}	Time complexity for the execution of a modular multiplication.
T_{EC-ADD}	Time complexity for the execution of an elliptic curve addition.
T_{ADD}	Time complexity for the execution of an addition.

Table 2:- Comparison of efficiency

	Key generation	Signature generation	Signature verification
Fan et al.[11]	$2T_{EC-MUL}$	$7T_S$ + $1T_H$+$1T_{INV}$ + $1T_m$	$1T_M$+$3T_{BP}$ + $1T_H$
Our's scheme	-	$2T_{SM}$+$5T_S$ +$1T_H$	$2T_{BP}$ +$1T_H$

6. CONCLUSION

Security of our scheme is based on expressing the torsion point of the curve into linear combination of its basis points, it is more complicated than solving ECDLP. The simulation results from AVISPA tools confirm the security analysis of proposed protocol. So our scheme is more secure than all based on ECDLP and as compare to other existing schemes it is efficient also.

7. REFERENCES

[1] D. Chaum, Blind signatures for untraceable payments, Advances in cryptology-Crypto'82, pp. 199-203, 1982.

[2] Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler. Blind Signatures Based on the Discrete Logarithm Problem. In Advances in Cryptology|EUROCRYPT '94, volume 950 of Lecture Notes in Computer Science, pages 428-432, Perugia, Italy, 1994. Springer

[3] LeinHarn. Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem.Electronic Letters, 31(14):1136, 1995.

[4] Patrick Horster, Markus Michels, and HolgerPetersen. Comment: Cryptanalysis of the BlindSignatures Based on the Discrete Logarithm Problem. Electronic Letters, 31(21):1827, 1995.

[5] H. Y. Chien.J.K.Jan and Y.M.Tseng, RSA based partially blind signature with low computation, Proc. of the 8th IEEE International Conference on parallel and distributed Systems, pp. 385-389, 2001.

[6] M. S. Hwang, C. C. Lee, Y. C. Lai,"An untraceable blind signature scheme", IEICE Transactions on Foundations, vol. E86-A, no. 7, pp. 1902-1906, 2003.

[7] J.M Alfred, A.V. Scott, and C.V.O Paul, Handbook of Applied Cryptography, CRC Press,1996.

[8] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability. Applied Mathematics and Computation, 164(3): 837-841, 2005.

[9] N. Ferguson, Single term off-line coins, in: Advances in Cryptology-EUROCRYPT'93, in: LNCS, vol. 765, 1994, pp. 318-328.

[10] C.I. Fan, W.K. Chen, Y.S. Yeh, Randomization enhanced chaums blind signature scheme, Computer Communications 23, pp. 1677-1680, 2000.

[11] Chun-I Fan, Wei-Zhe Sun, Vincent Shi-Ming Huang, Provably secure randomized blind signature scheme based on bilinear pairing, Computers and Mathematics with Applications, 60, pp. 285- 293,2010.

[12] N. Koblizt, Elliptic curve cryptosystem, *Mathematics of Computation 48(177)*, 1987, pp. 203-209.

[13] V .S. Miller, Use of elliptic curves in cryptography, Advances in Cryptology-Proceedings of Crypto85, LNCS, vol. 218, Springer, 1986.

[14] J.H.Silverman.: *The arithmetic of elliptic curves*, volume 106 of graduate texts in mathematics, springer-verlag, Newyork 1986.

[15] J. Hoffstein, J. Pipher., and J. H. Silverman, *An introduction to mathematical cryptography*, springer.

[16] Y. Zhang, W. Liu, W. Lou, Y. Fang, Securing mobile ad hoc networks with certificateless public keys, IEEE Transactions on Dependable and Secure Computing vol. 3 (4), 386-399, 2006.

[17] Avispa - a tool for Automated Validation of Internet Security Protocols. http:\\ www.avispa project.org.

[18] D6.2: Specification of the Problems in the High-Level Specification Language. http:\\www.avispa-project.org.

APPENDIX A

```
%%PROTOCOL:Blind Signature protocol
%%ALICE BOB:
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%HLPSL:
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
rolealice(
A,B:agent,
Ra1,Ra2,Rb1,Rb2: symmetric_key,
H,Minus,Union,Pred,Conc,Expr,Ebilinear:hash_func,
SND,RCV : channel(dy))
played_by A def=
transition
1.State=0/\RCV(start)=|>State':=2
/\P1':=new()
/\P2':=new()
/\Pa':=Union(Pred(Ra1,P1),Pred(Ra2,P2))
/\SND(Pa)
2.State=2/\RCV(K1,K2)=|>
State':=4/\T':=Union(Pred(Ra1,K1),Pred(Ra2,K2))
/\SND(T)
/\secret(key1,key_id1,{a,b})
/\request(A,B,key1,key2)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role bob(
H,Minus,Union,Pred,Conc,Expr,Ebilinear:hash_func,
SND,RCV:channel(dy))
played_by B def=
init State:=1
transition
1.State=1/\RCV(Pa)=|>State':=3
/\P1':=new()
/\P2':=new()
/\Pb':=Union(Pred(Rb1,P1),Pred(Rb2,P2))
/\K1':=Union(H(Conc(M,Pa)),Pred(Rb2,P1))
/\K2':=Pred(Rb2,P2)
/\SND(K1,K2)
2.State=3/\RCV(T)=|>State':=5
/\S':=Minus(T,Pred(Rb2,Pb))
/\N':= Ebilinear(P1,Pred(S,P2))
/\N':=Ebilinear(P1,Pred(H(Conc(M,Pb)),P2))
/\secret(key2,key_id2,{b,a})
/\request(B,A,key2,key1)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role session(
A,B:agent,
H,Minus,Union,Pred,Conc,Expr,Ebilinear:hash_func)
def=
local
SendA,ReceiveA:channel(dy),
SendB,ReceiveB:channel(dy)
composition
```

```
alice(A,B,Ra1,Union,Pred,Conc,Expr,Ebilinear,SendA,ReceiveA)
/\bob(A,B,Union,Pred,Conc,Expr,Ebilinear,SendB,ReceiveB)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role environment()
composition
session(a,b,ra1,ra2,rb1,rb2,h,minus,union,pred,conc,expr,ebilinear)
/\session(a,i,ra1,ra1,ri1,ri2,h,minus,union,pred,conc,expr,ebilinear)
/\session (i,b,ri1,ri2,rb1,rb2,h,minus,union,pred,conc,expr,ebilinear)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
goal
secrecy_of key_id1,key_id2
end goal
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
environment()=
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```