Identity based signature schemes by using pairings

Parshuram Budhathoki
Department of Mathematical Science
FAU
02/21/2013
Goal:

1. Alice wants to send a message to Bob.
2. She wants to make sure that Bob could verify it, and no one can change the message during the process.
3. So, she signs her message by using her identity.

Possible Identity:
- email id: alice@fau.edu
- phone: 561297alice
- Address: 777 Glades Road

Now after getting message, Bob uses Alice’s identity to verify either its from Alice or someone else. And he could verify that it is written by Alice.

ID based signature scheme
Outline:

- Signature Scheme in ID Based Cryptography
- Pairings
- Hash Functions
- Attack Model
- Secure Scheme
- Diffie-Hellman Problem
- Hess’s Scheme
Signature Scheme in ID Based Cryptography:

1. Setup
2. Extract
3. Sign
4. Verify
Signature Scheme in ID Based Cryptography:

1. Setup
2. Extract
3. Sign
4. Verify

Trust Authority (TA)
- Secret Key
- Public Parameter
- Private Key for Alice

Verifier

ID:= alice@fau.edu

Signature:=Sign( Message, Private Key )

Verify ( Signature, ID )
Pairing

Domain $G_1$ $G$

Range $V$

$e(P, Q)$

e

$G$

Domain

$Q$
Pairing

Let \((G,+), (V, \cdot)\) denote cyclic groups of prime order \(q\), \(P \in G\), a generator of \(G\) and a pairing

\[ e: G \times G \rightarrow V \]

is a map which satisfies the following properties:

1) **Bilinearity** : \(\forall\ P, Q, R \in G\) we have

\[ e(P+R, Q) = e(P,Q) e(R,Q) \]

and

\[ e(P, R+Q) = e(P,R) e(P,Q) \]

2) **Non-degeneracy** : There exists \(P, Q \in G\) such that

\[ e(P,Q) \neq 1. \]

3) \(e\) is efficiently computable.
Hash Functions:

- **Domain**: Any size
- **Range**: Fixed size
- **No Inverse**
- **H(x)**
Hash Function:

• One way transformation

• Input := Random size, Output:= Fixed size

• $H(x_1) = H(x_2)$ for $x_1 \neq x_2$ , Not possible
Attack Model: GAME

Setup
- Give me a hash value for this and that...
- Give me a private key for ID
- Give me a signature for ID₂ and message M

Challenger
- Public Parameters
- Here is the hash value of this & that...
- Private key for ID₂ and message M

Adversary
**Attack Model:** GAME

Adversary outputs $(ID, M, \text{Signature})$, such that ID and $(ID, M)$ are not equal to the inputs of any query.

And, Adversary wins the game if Signature is a valid signature for ID and M.
We say ID based signature scheme is secure against existential forgery on adaptively chosen message and ID attacks if no polynomial time adversary has a non-negligible probability of success against a challenger in previous Game.
Diffie-Hellman Problem:

Let $G$ be a cyclic group of order $q$ with generator $P$. The Diffie-Hellman Problem (DHP) in $G$ is to find, on input $(aP, bP, P)$, with uniformly and independently chosen $a, b$ from $\{1, ..., q\}$, the value $abP$. 
Hess Scheme

Let \((G, +)\) and \((V, \cdot)\) denote cyclic groups of prime order \(q\) such that \(G = \langle P \rangle\), and let \(e: G \times G \rightarrow V\) be a pairing.

The hash functions:
- \(h: \{0,1\}^* \times V \rightarrow \mathbb{Z}_q^*\)
- \(H: \{0,1\}^* \rightarrow G^*\)

Where \(G^* := G \setminus \{0\}\)

Assumption: \textbf{DHP} in \(G\) is hard.
Hess Scheme:

2. Extract
1. Setup
3. Sign
4. Verify

ID:= alice@fau.edu

1. Compute $r = e(U, P) e(H(ID), -Q)^V$
2. Accept the signature if $V = h(M, r)$

Sign Algorithm:
Alice picks random $k$ from $Z_q^*$
1. $r = e(S_{ID}, P)^k$
2. $V = h(M, r)$
3. $U = (V + k) S_{ID}$
Signature := $(U, V)$

TA

Setup Algorithm:
- Chooses $s$ from $Z_q^*$
- Master Key := $s$
- Public key $Q:= sP$
Public Key $Q= sP$

Verify

Extract Algorithm:
$S_{ID} := s H(ID)$

Verifier

02/21/2013
Cyber Security Seminar, FAU
Correctness of Verification:

1. \( e(\{ U, P \} \cdot e(H(ID), -Q)^V = e((V + k) \cdot sH(ID), P) \cdot e(H(ID), -sP)^V \) \\
   = \( e(H(ID), P)^{s(V + k)} \cdot e(H(ID), P)^{-sV} \) \\
   = \( e(H(ID), P)^{sk} \) \\
   = \( e(sH(ID), P)^k \) \\
   = r \\

2. Accepts if \( V = h(M, r) \)
Summary

• Did we achieve our goal?

• Do we know any Id based signature scheme?

• We have proposed an Id based signature scheme 😊 !!!
Questions?

Thank You 😊