Key Escrow free Identity-based Cryptosystem

Manik Lal Das

DA-IICT, Gandhinagar, India

About DA-IICT and Our Group

DA-IICT is a private university, located in capital of Gujarat state in India. DA-IICT offers undergraduate and postgraduate programs in Information and Communication Technology.

About DA-IICT and Our Group

Cyber Security Research Group in DA-IICT:
http://security.daiict.ac.in

Outline

Authentication

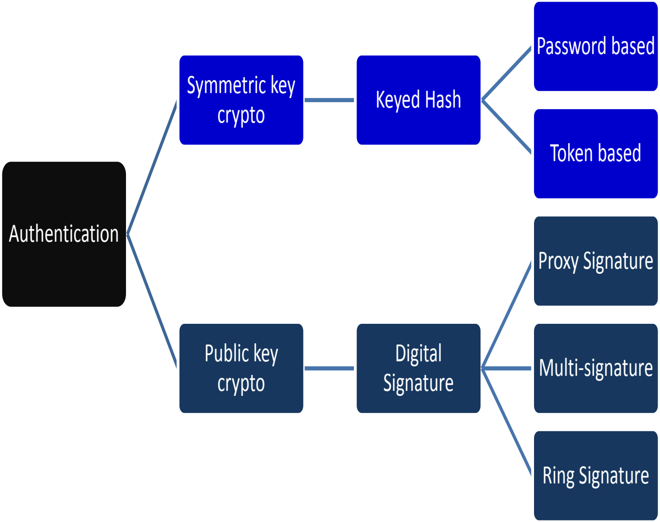
What is Authentication?

Authentication is a process of confirming the

(i) identity of an entity (entity authentication); and/or

(ii) legitimacy of a document (data origin authentication).

Authentication Techniques



Cryptosystem

A Cryptosystem is a 3-tuple (Key Generation, Encryption, Decryption) algorithm defined as:

Cryptosystem

A Cryptosystem is a 3-tuple (Key Generation, Encryption, Decryption) algorithm defined as:

Key Generation

INPUT: a security parameter.
OUTPUT: key(s) and public parameters.

Cryptosystem

A Cryptosystem is a 3-tuple (Key Generation, Encryption, Decryption) algorithm defined as:

Key Generation

INPUT: a security parameter.
OUTPUT: key(s) and public parameters.

Encryption

INPUT: key, message, public parameters.
OUTPUT: ciphertext.

Cryptosystem

A Cryptosystem is a 3-tuple (Key Generation, Encryption, Decryption) algorithm defined as:

Key Generation

INPUT: a security parameter.
OUTPUT: key(s) and public parameters.

Encryption

INPUT: key, message, public parameters.
OUTPUT: ciphertext.

Decryption

INPUT: key, ciphertext, public parameters.
OUTPUT: message.

Cryptosystem

A Cryptosystem is a 3-tuple (Key Generation, Encryption, Decryption) algorithm defined as:

Key Generation

INPUT: a security parameter.
OUTPUT: key(s) and public parameters.

Encryption

INPUT: key, message, public parameters.
OUTPUT: ciphertext.

Decryption

INPUT: key, ciphertext, public parameters.
OUTPUT: message.

Domain: Key space; Message space; Ciphertext space

Cryptosystem (contd.)

Symmetric key cryptosystem: One key is used for encryption and decryption.

Limitation: Secret key distribution.

Asymmetric key cryptosystem: Two keys are used for encryption (public key) and decryption (private key)

Limitation: Public key management.

Identity-based Cryptosystem

Public key is the user's identity or derived from the user's identity (e.g. email).

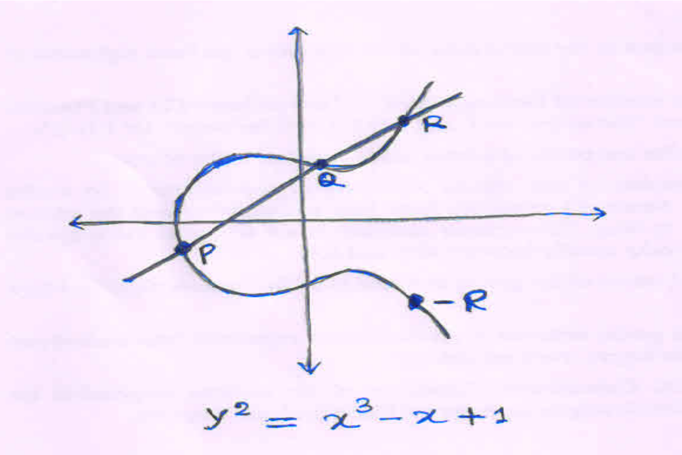
- User identity acts as the public key.
- Aim is to eliminate infrastructure for public key certification.

A. Shamir. Identity-based cryptosystems and signature schemes.In Proc. of Advances in Cryptology-CRYPTO'84, LNCS 196, Springer-Verlag, pp. 47-53, 1984.

IEEE Standard for identity-based cryptographic techniques using pairings - 1363.3 (2013).

Interesting Properties of Elliptic Curve

Let $y^2 = x^3 + ax + b$ be an elliptic curve that forms an elliptic curve group, where $a, b \in F_q$ for a large prime q.



Bilinear Pairing

Let G_1 be an additive group of order a prime q, P be a generator of G_1, and G_2 be a multiplicative group of order prime q.

A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$ that satisfies the following properties.

Properties of Bilinear Pairing

1) $e(aP, bQ) = e(P, Q)^{ab}$, for all $P, Q \in G_1$ and $a, b \in Z_q^*$.

2) There exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.

3) There exists an efficient algorithm to compute $e(P, Q)$.

Computational Hardness Assumptions

Elliptic curve discrete logarithm problem
Given $P, Q(= xP)$, finding x is computationally infeasible.

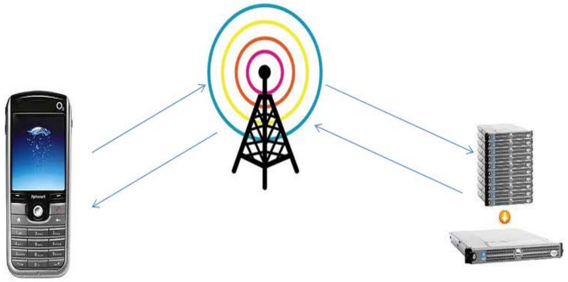
Computational Diffie-Hellman problem
Given P, aP, bP, finding abP is computationally infeasible.

There are many other variants...

Pairing-based Authenticated Key Exchange+

Contents
Background
Identity-based Cryptosystem
Identity-based Signature
Conclusion

Scenario: Mobile communications



Signature by scalar multiplication

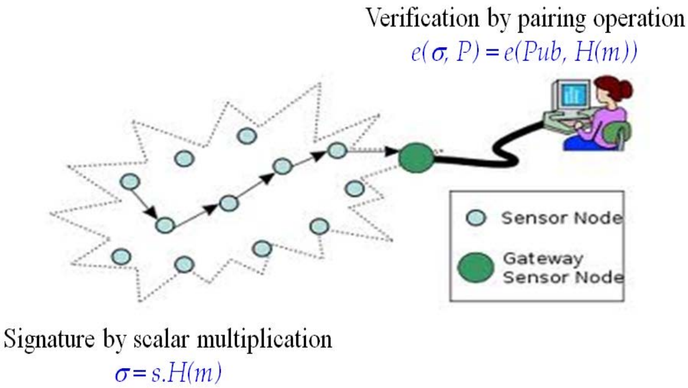
$\sigma = s.H(m)$

Verification by pairing operation

$e(\sigma, P) = e(Pub, H(m))$

Pairing-based Authenticated Key Exchange+

Scenario: Wireless Sensor Networks



Identity-based Signature(IDS) Scheme

IDS is defined by the 4-tuple (Setup, KeyGen, Sign, Verify)

Identity-based Signature(IDS) Scheme

IDS is defined by the 4-tuple (Setup, KeyGen, Sign, Verify)

System keys $\leftarrow$ Setup(1^k)

Inputs a security parameter k; Outputs system secret and public keys.

Identity-based Signature(IDS) Scheme

IDS is defined by the 4-tuple (Setup, KeyGen, Sign, Verify)

System keys $\leftarrow$ Setup(1^k)

Inputs a security parameter k; Outputs system secret and public keys.

User private key $\leftarrow$ KeyGen(user ID, system keys)

Inputs user ID; Outputs user private key.

Identity-based Signature(IDS) Scheme

IDS is defined by the 4-tuple (Setup, KeyGen, Sign, Verify)

System keys $\leftarrow$ Setup(1^k)

Inputs a security parameter k; Outputs system secret and public keys.

User private key $\leftarrow$ KeyGen(user ID, system keys)

Inputs user ID; Outputs user private key.

$\sigma \leftarrow$ Sign(m, user private key, public parameter)

Inputs message m and user private key; Outputs signature σ.

Identity-based Signature(IDS) Scheme

IDS is defined by the 4-tuple (Setup, KeyGen, Sign, Verify)

System keys $\leftarrow$ Setup(1^k)

Inputs a security parameter k; Outputs system secret and public keys.

User private key $\leftarrow$ KeyGen(user ID, system keys)

Inputs user ID; Outputs user private key.

$\sigma \leftarrow$ Sign(m, user private key, public parameter)

Inputs message m and user private key; Outputs signature σ.

Accept/Reject $\leftarrow$ Verify(user ID, m, σ, public parameter)

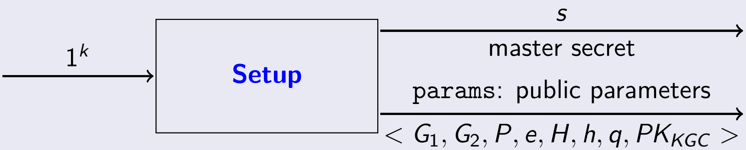
Inputs signature σ, message m, user ID, public parameters; Outputs Accept or Reject.

Identity-based Signature Scheme (Setup, KeyGen, Sign, Verify)

System keys $\leftarrow$ Setup(1^k)

G_1 is an additive group of order prime q;
G_2 is a multiplicative group of order prime q;
P is a generator of G_1 ;
$e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map;
H, h are cryptographic hash function.

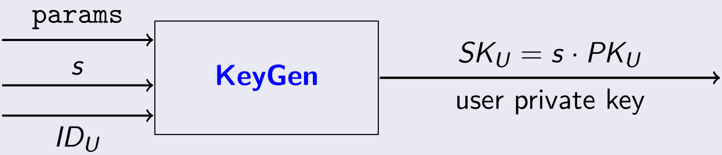
The system selects $s \in Z_q^*$ as the **master secret key** and computes its **public key** $PK_{KGC} = s \cdot P$. The KGC publishes the public parameters $\texttt{params} = < G_1, G_2, P, e, H, h, q, PK_{KGC} >$.



Identity-based Signature Scheme (Setup, KeyGen, Sign, Verify)

$SK_U \leftarrow$ **KeyGen**(params, s, ID_U)

KGC generates user private key $SK_U = s.PK_U$, where user public key $PK_U = H(ID_U)$.



KGC sends the private key SK_U to the user securely.

Problems in user private key generation

KGC generates user private key and sends it to the user securely.

(1) User's private key is known to the KGC
$\Rightarrow$ **Key-escrow problem**.

(2) Sending user private key requires **secure channel**.

Proposed Solution: Binding-Blinding Technique

- User chooses two secret blinding factors, calculates the binding parameters and sends the parameters to the KGC over a public channel for his partial key.
- KGC gets a confirmation from the user about his request for the partial key, and then KGC proceeds to the next step.
- After validating the user's binding parameters, the KGC computes user partial key and sends it to the user over a public channel.

Proposed Solution: Binding-Blinding Technique

- User chooses two secret blinding factors, calculates the binding parameters and sends the parameters to the KGC over a public channel for his partial key.
- KGC gets a confirmation from the user about his request for the partial key, and then KGC proceeds to the next step.
- After validating the user's binding parameters, the KGC computes user partial key and sends it to the user over a public channel.

No key escrow and no secure channel for user private key generation.

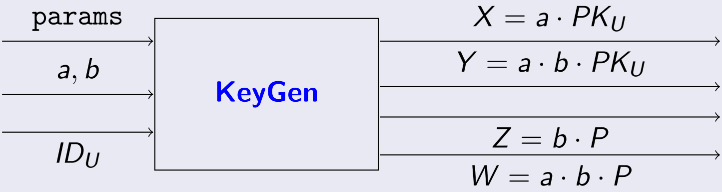
Identity-based Signature Scheme (Setup, KeyGen, Sign, Verify)

Binding parameters with user secret blinding factor.

Binding Parameters ← KeyGen(params, ID_U, a, b)

User selects secret blinding factors $a, b \in Z_q^*$ and computes $X = a \cdot PK_U$, $Y = a \cdot b \cdot PK_U$, $Z = b \cdot P$, $W = a \cdot b \cdot P$.

User sends the binding parameters (X, Y, Z, W, ID_U) to KGC over a public channel.



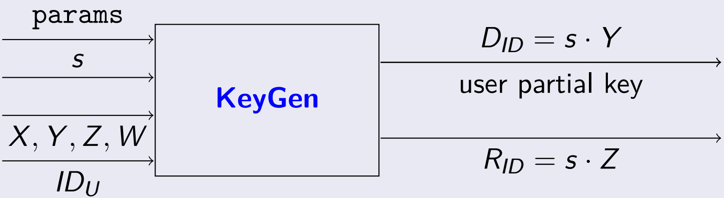
Identity-based Signature Scheme (Setup, KeyGen, Sign, Verify)

User Partial Key generation.

$D_{ID} \leftarrow$ KeyGen($\texttt{params}$, s, ID_U, Binding parameters)

KGC checks whether $e(Y, P) = e(X, Z) = e(PK_U, W)$.

If the above holds, KGC computes the user partial key $D_{ID} = s \cdot Y$ and creates a registration-token $R_{ID} = s \cdot Z$. Then, KGC publishes $< R_{ID}, ID_U >$ in a public directory and sends D_{ID} to the user over a public channel.



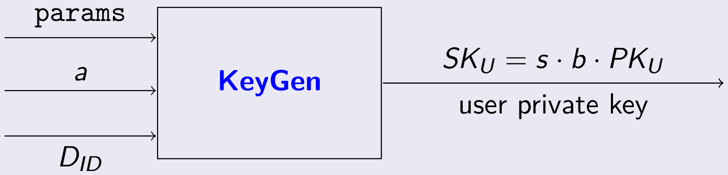
Identity-based Signature Scheme (Setup, KeyGen, Sign, Verify)

Unblinding Partial Key $\rightarrow$ User Private Key.

$SK_U \leftarrow$ KeyGen$(\texttt{params}, a, D_{ID})$

User checks whether $e(D_{ID}, P) = e(Y, PK_{KGC})$.

If it holds, user unblinds his partial key and generates his private key SK_U as $SK_U = a^{-1} \cdot D_{ID} = b \cdot s \cdot PK_U$.



Identity-based Signature Scheme (Setup, KeyGen, Sign, Verify)

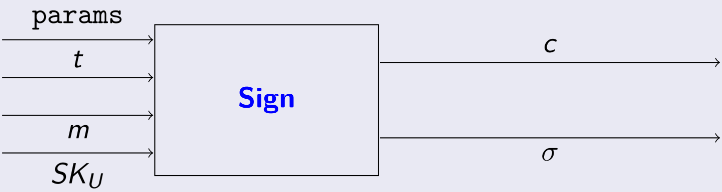
Signature Generation.

$(\sigma, c, m) \leftarrow$ Sign($\mathtt{params}, t, m, SK_U$)

To sign a message m, the signer does the following:

- Pick a random $t \in Z_q^*$
- Compute $r = e(P, P)^t$ and $c = h(m, r, R_{ID})$
- Compute $\sigma = c \cdot SK_U + t \cdot P$.

The signature on message m is (σ, c, m).

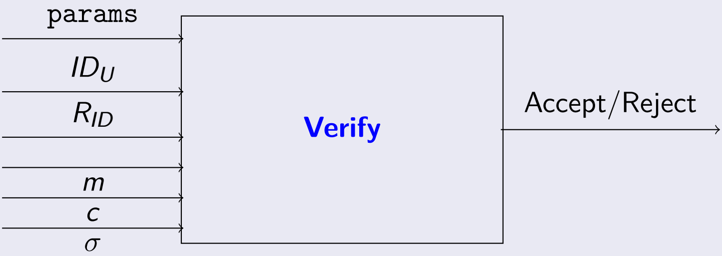


Identity-based Signature Scheme (Setup, KeyGen, Sign, Verify)

Signature Verification.

Accept/Reject ← Verify$(\texttt{params}, ID_U, R_{ID}, m, c, \sigma)$

- Compute $\hat{r} = e(\sigma, P) \cdot e(PK_U, -R_{ID})^c$
- Accept the signature if $c = h(m, \hat{r}, R_{ID})$.



Conclusion:

Merit and Limitation of the proposed solution

- The proposed technique provides solution to key escrow problem in ID-based construction.
- The proposed technique eiminates the use of secure channel in ID-based construction.
- User Registration identity needs to be managed, which is a bottleneck of the suggested solution.

Manik Lal Das. Key-escrow free multi-signature scheme using bilinear pairings. *Groups-Complexity-Cryptology*, 7(1):47-57, 2015.

Manik Lal Das. A key escrow-free identity-based signature scheme without using secure channel. *Cryptologia*, 35(1): 58-72, 2011.

Conclusion:
Merit and Limitation of the proposed solution

- The proposed technique provides solution to key escrow problem in ID-based construction.
- The proposed technique eiminates the use of secure channel in ID-based construction.
- User Registration identity needs to be managed, which is a bottleneck of the suggested solution.

Manik Lal Das. Key-escrow free multi-signature scheme using bilinear pairings. *Groups-Complexity-Cryptology*, 7(1):47-57, 2015.

Manik Lal Das. A key escrow-free identity-based signature scheme without using secure channel. *Cryptologia*, 35(1): 58-72, 2011.

Thanks!