Identity-based Cryptography

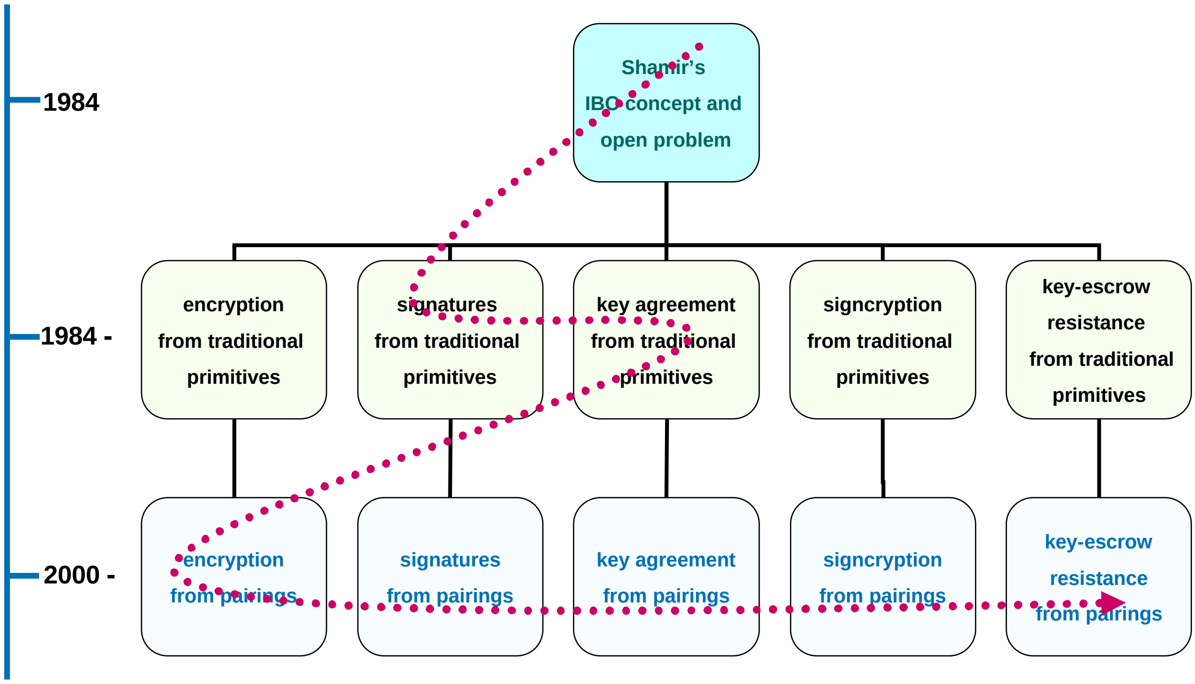
Liqun Chen
Hewlett-Packard Laboratories

liqun.chen@hp.com

What will be covered in this lecture

- Basic concept of identity-based cryptography (IBC)
- Examples of IBC mechanisms (not a complete list)
  - Identity-based encryption
  - Identity-based signatures
  - Identity-based combined encryption/signing
  - Identity-based key-agreement
  - Key-escrow resistance
- Brief introduction of security proofs
- International standards on IBC

History and categories



1984

Shamir's IBC concept and open problem

1984 -

encryption from traditional primitives

signatures from traditional primitives

key agreement from traditional primitives

signcryption from traditional primitives

key-escrow resistance from traditional primitives

2000 -

encryption from pairings

signatures from pairings

key agreement from pairings

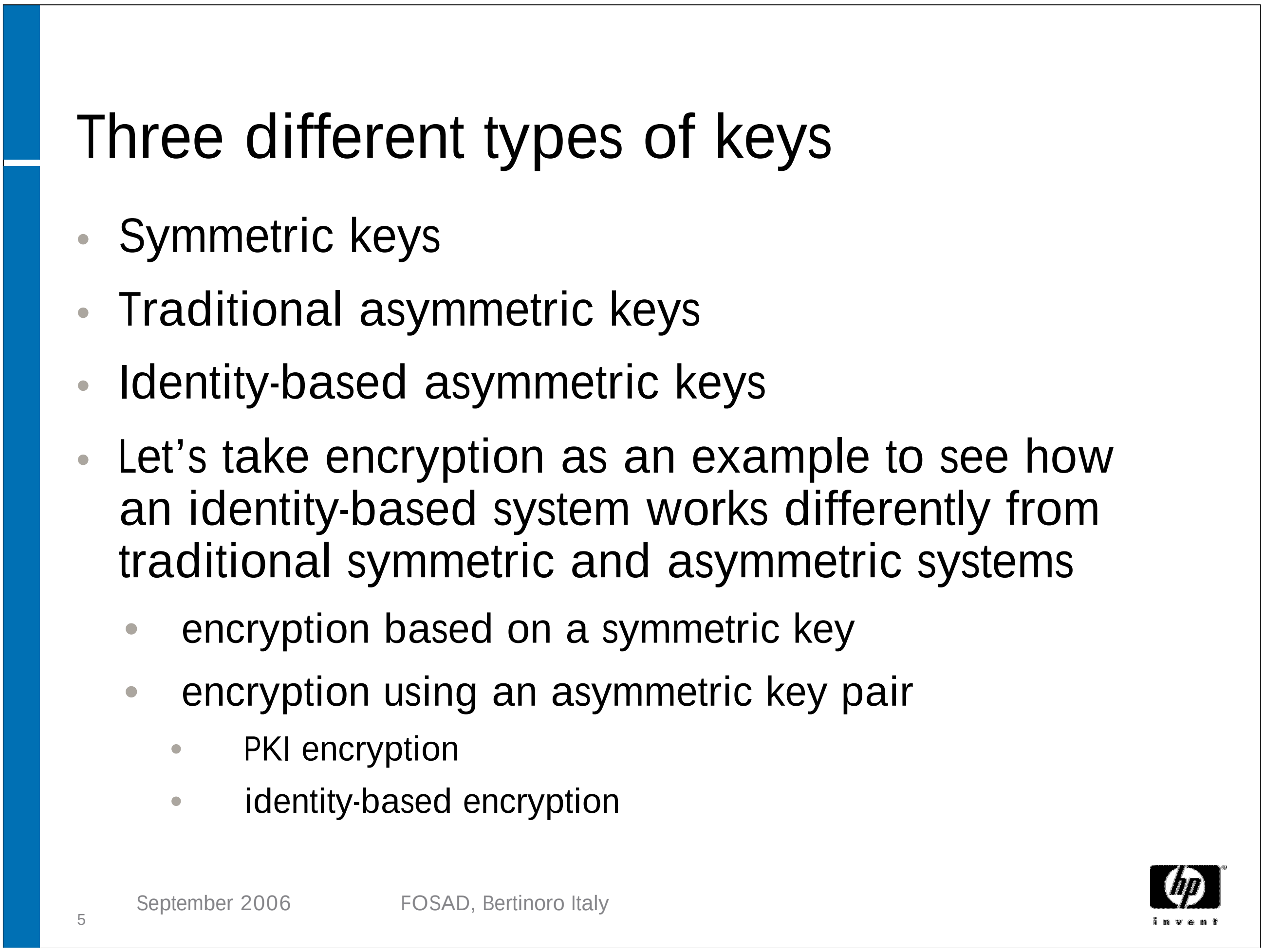
signcryption from pairings

key-escrow resistance from pairings

“identity-based …” – all about keys

The only difference between “an identity-based system” and “a traditional system” is –

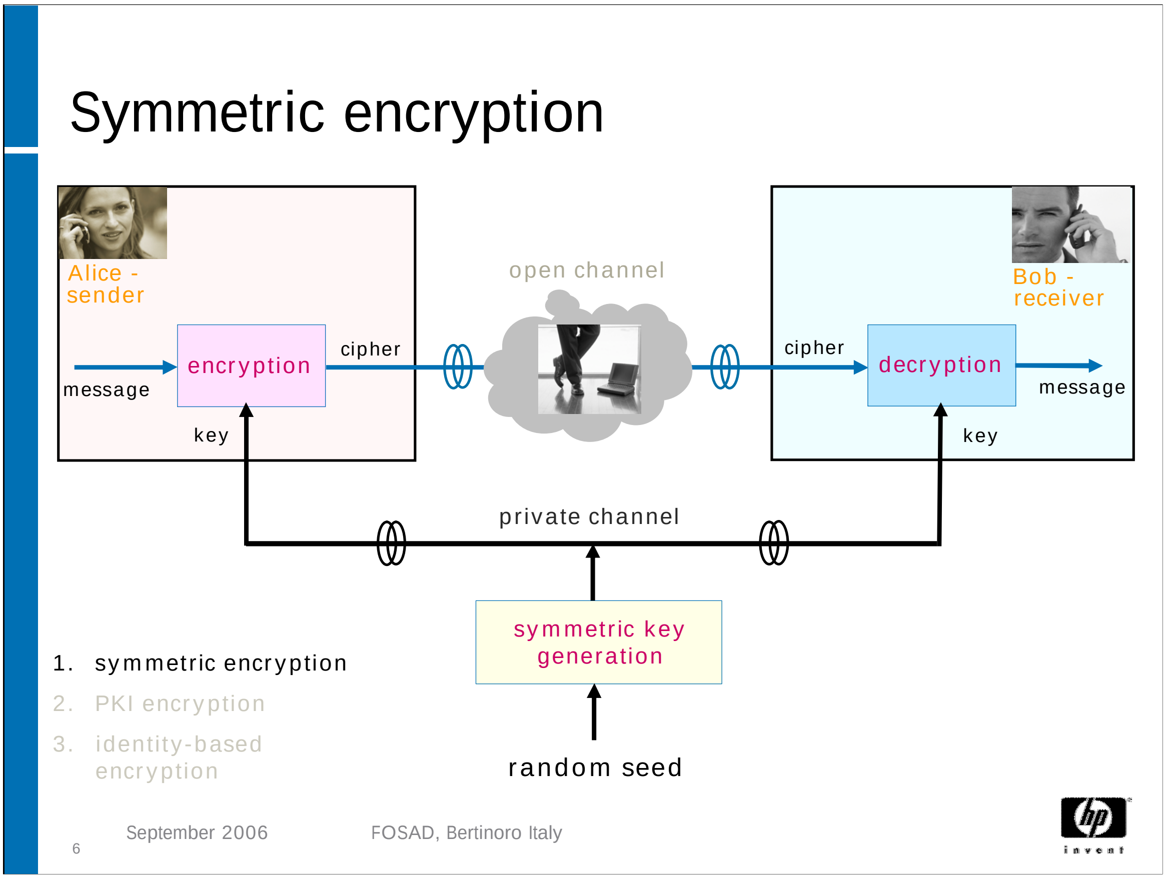
- How to construct a key
- How to authenticate the key
- How to distribute the key
- How to use the key



Three different types of keys

- Symmetric keys
- Traditional asymmetric keys
- Identity-based asymmetric keys
- Let’s take encryption as an example to see how an identity-based system works differently from traditional symmetric and asymmetric systems
  - encryption based on a symmetric key
  - encryption using an asymmetric key pair
    - PKI encryption
    - identity-based encryption

- The differentiation related to how to construct an asymmetric key pair can also be found in other cryptographic mechanisms, such as signatures, signcryption, key agreement and so on.



Symmetric encryption

Alice - sender

message → encryption → cipher

key

open channel

Bob - receiver

cipher → decryption → message

key

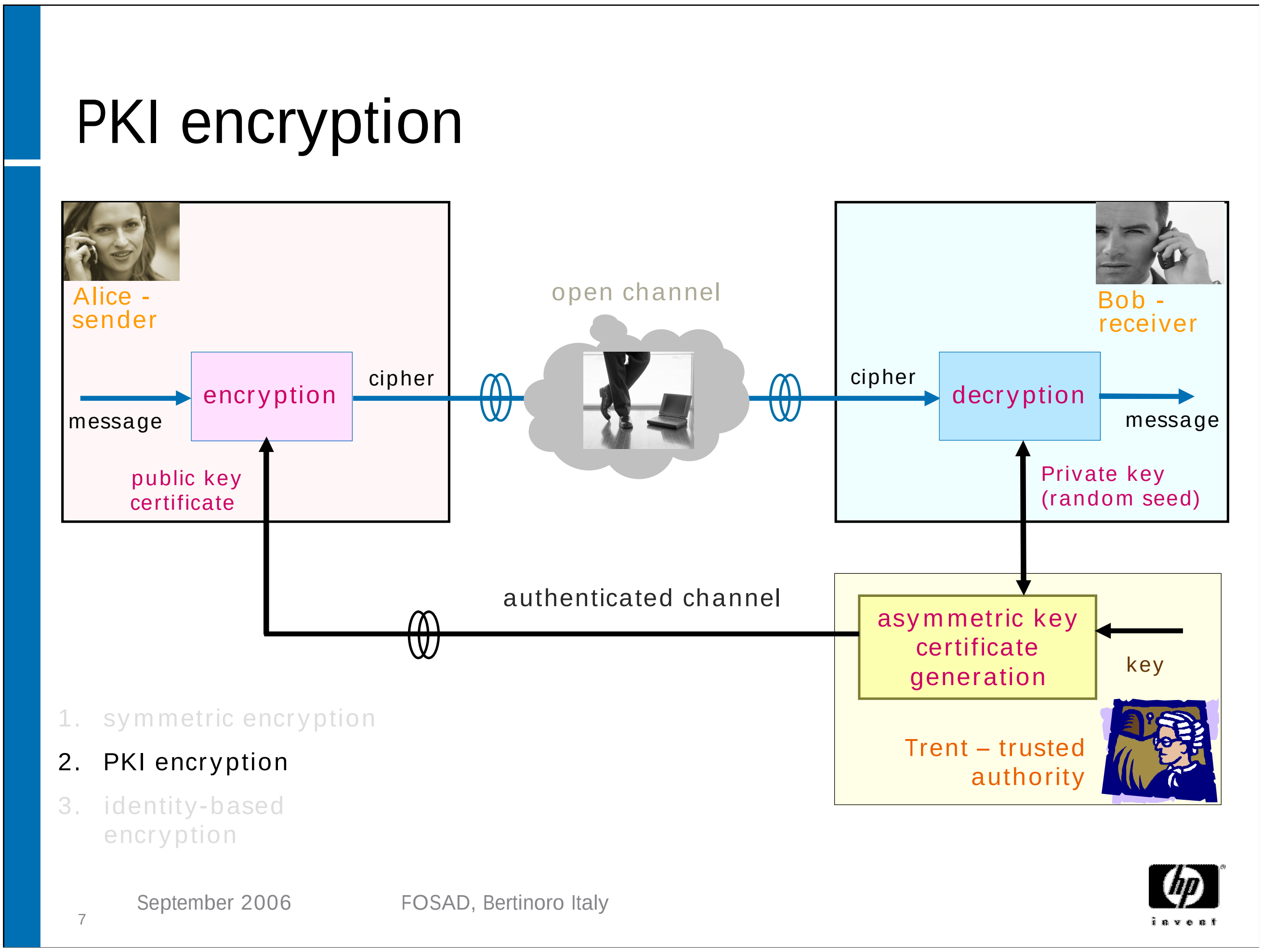
private channel

symmetric key generation

random seed

1. symmetric encryption
2. PKI encryption
3. identity-based encryption

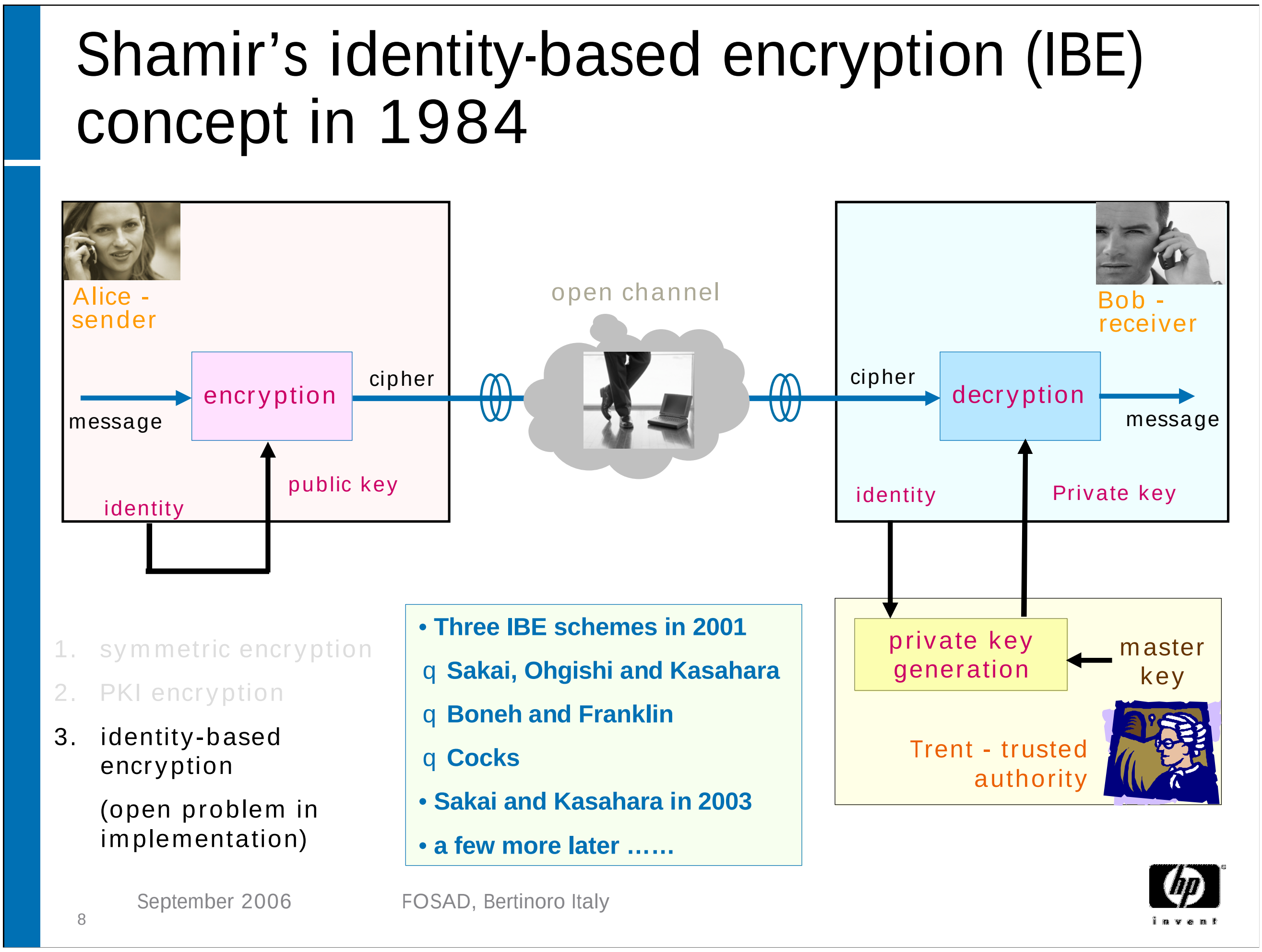
- In a symmetric encryption mechanism, Alice and Bob share the same key.



PKI encryption

1. symmetric encryption
2. PKI encryption
3. identity-based encryption

- PKI - Public Key Infrastructure.
- In the PKI applications, Trent plays the role of a Certificate Authority (CA).
- Alice has to obtain Bob’s public key and certificate before sending him an encrypted message.



Shamir’s identity-based encryption (IBE) concept in 1984

Alice - sender

message

encryption

cipher

public key

identity

open channel

cipher

decryption

message

Bob - receiver

identity

Private key

private key generation

master key

Trent - trusted authority

1. symmetric encryption
2. PKI encryption
3. identity-based encryption

   (open problem in implementation)

- Three IBE schemes in 2001
  - Sakai, Ohgishi and Kasahara
  - Boneh and Franklin
  - Cocks
- Sakai and Kasahara in 2003
- a few more later ……

- With identity-based encryption, Alice can create/choose a public key for Bob. Bob doesn’t have to make his decryption key ready before Alice can send him an encrypted message.

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

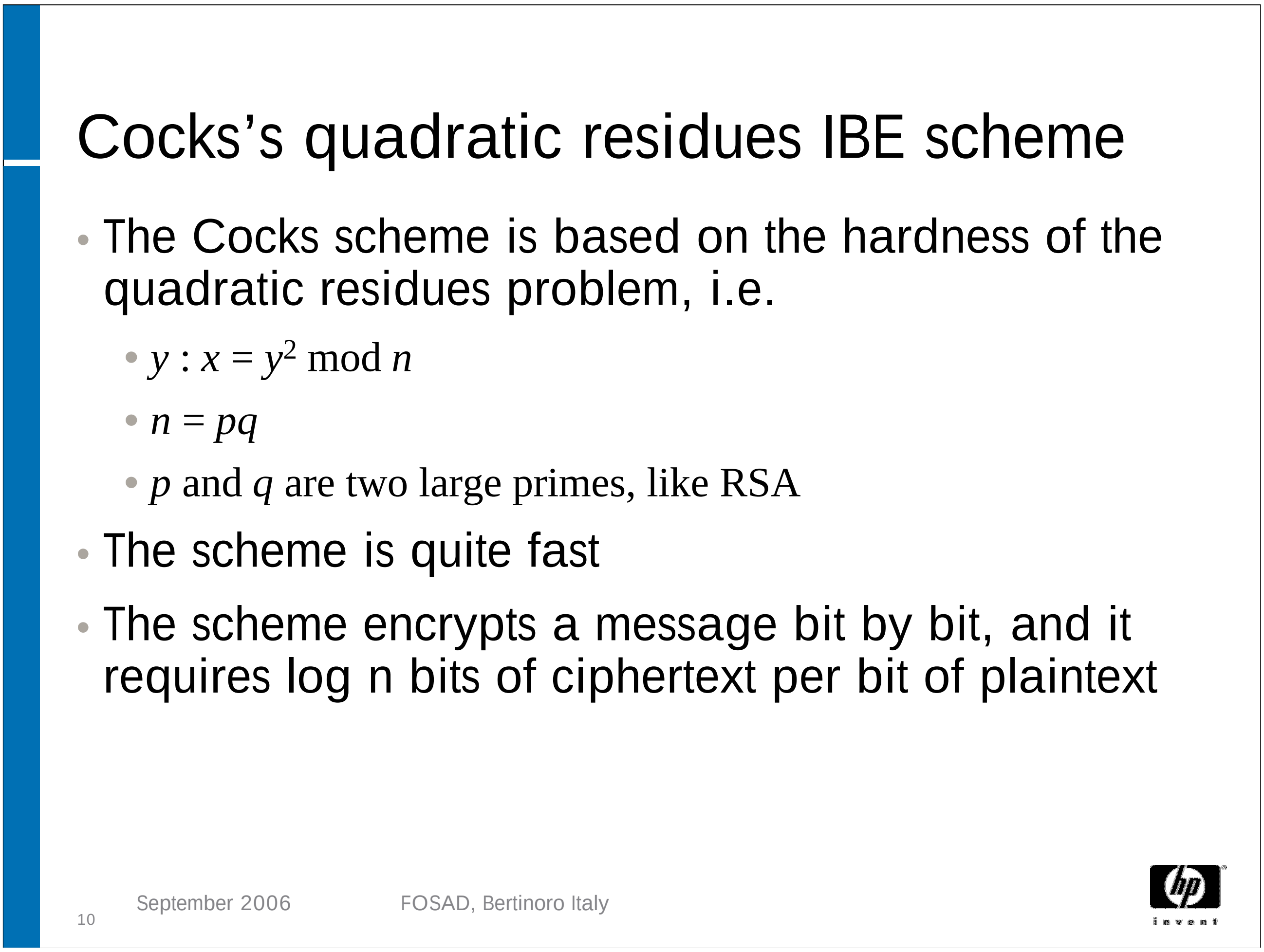
- Quoted from the Shamir paper:

  “At this stage we have concrete implementation proposals only for identity-based signature schemes, but we conjecture that identity-based cryptosystems exist as well and we encourage the reader to look for such systems.”

- It took many years to solve the Shamir option problem ……

What could be used as a public key?

- Any personal information, such as an email address, a photo, a phone number, a post address, etc
- Any terms and conditions, such as a policy, a time, a role, etc
- Any thing you can think about relative to a particular entity
- An application example is role-based access: we have designed a role-based email system for those clients with sensitive secure email requirements



Cocks's quadratic residues IBE scheme

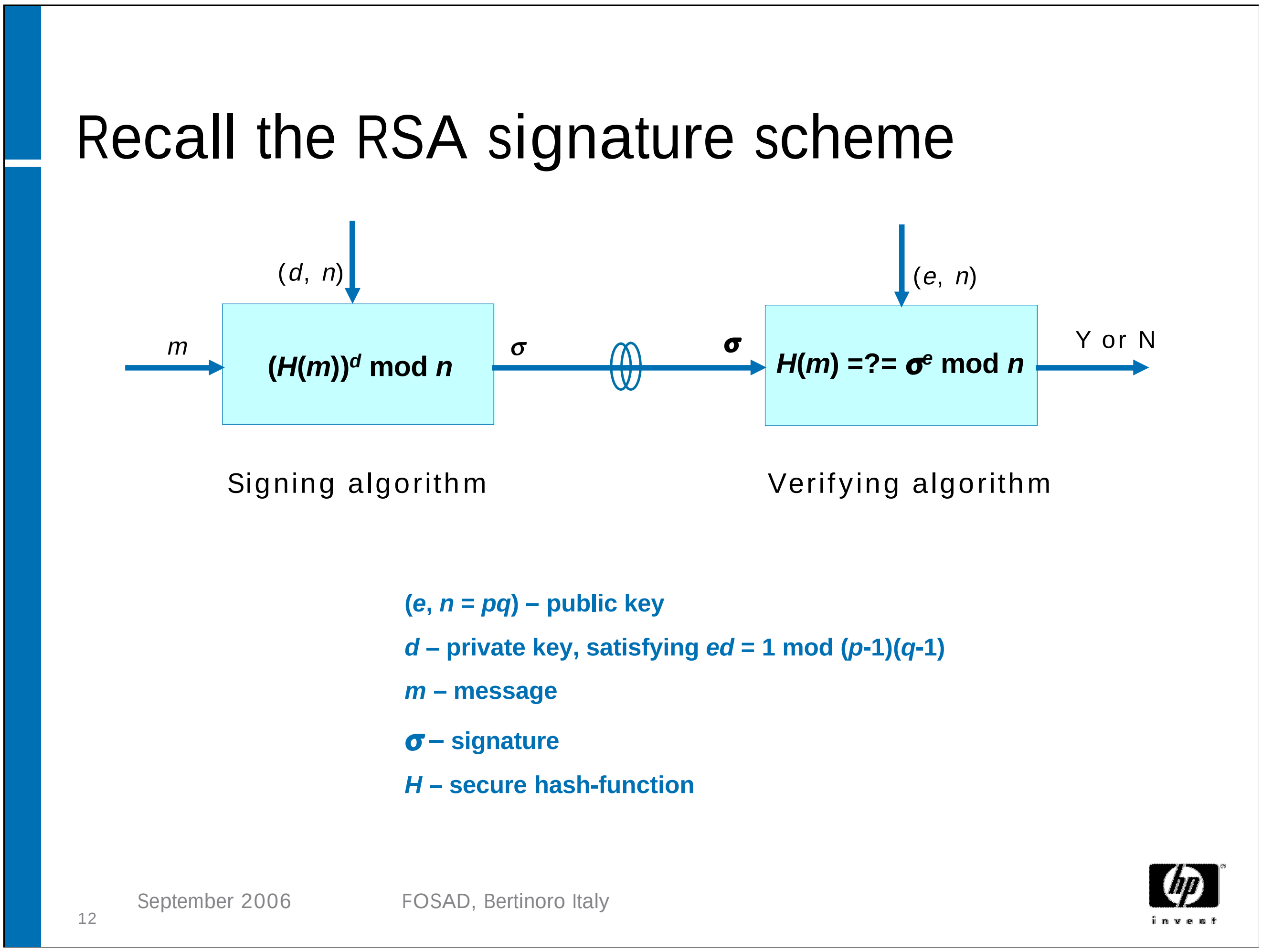
- The Cocks scheme is based on the hardness of the quadratic residues problem, i.e.
  - $y : x = y^2 \bmod n$
  - $n = pq$
  - p and q are two large primes, like RSA
- The scheme is quite fast
- The scheme encrypts a message bit by bit, and it requires log n bits of ciphertext per bit of plaintext

In the following paper, Cocks proposed an identity-based encryption scheme based on quadratic residues. This is the only IBE scheme, which does not use pairings.

- C. Cocks. An identity-based encryption scheme based on quadratic residues. In Proceedings of Cryptography and Coding, LNCS 2260, pp. 360-363, Springer-Verlag, 2001.

We will talk more about the IBE schemes from pairings later.

Identity-based signatures from RSA



Recall the RSA signature scheme

Signing algorithm

Verifying algorithm

(e, $n = pq$) – public key

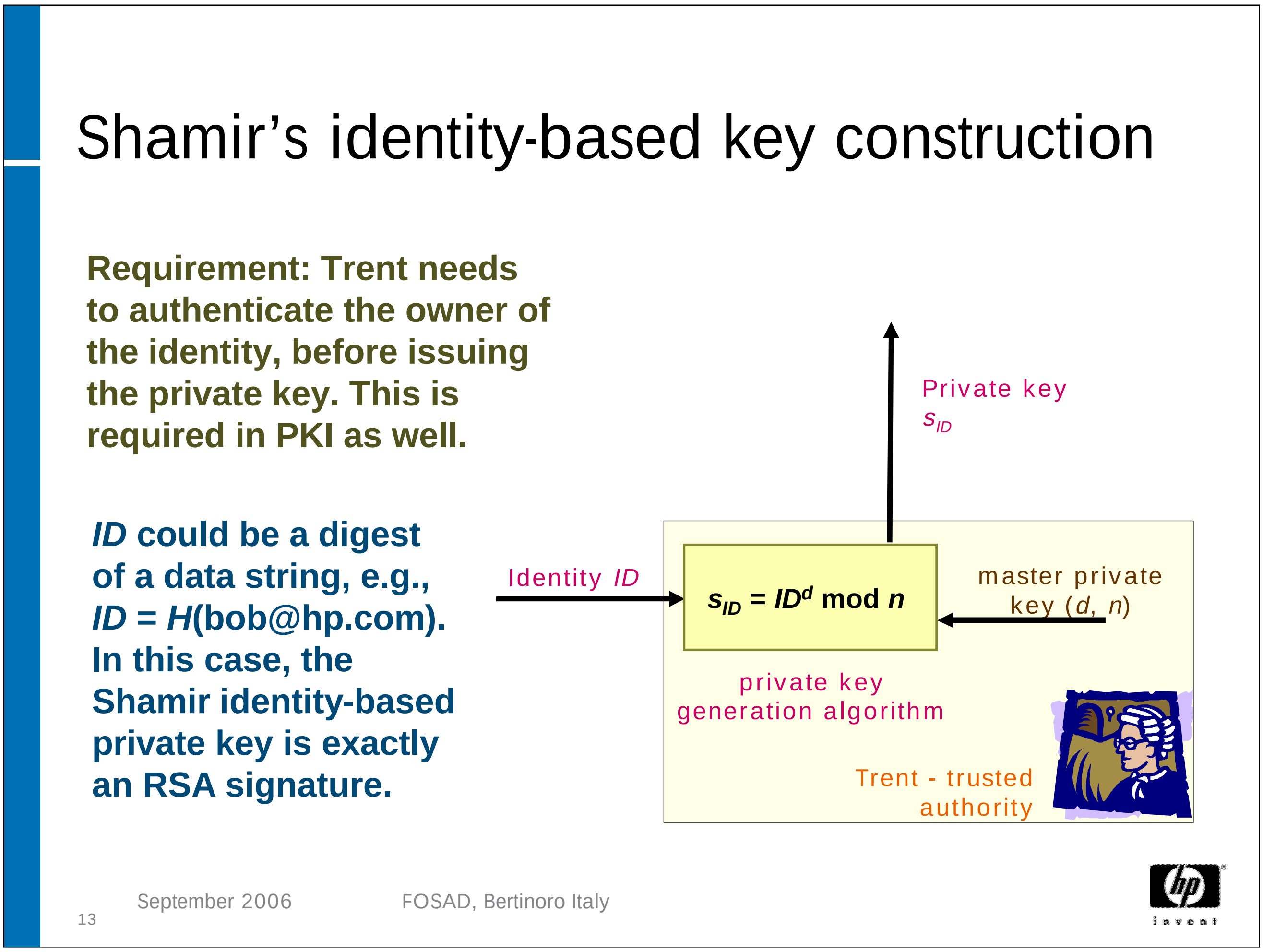
d – private key, satisfying ed = 1 mod (p-1)(q-1)

m – message

σ – signature

H – secure hash-function

- RSA public key (e, n)
  - n = pq, which is called an RSA modulus
  - p and q are two large primes
  - e is a prime and does not divide (p -1)(q -1)
- RSA private key d
  - d = 1/e mod (p -1)(q -1)
- Create a signature σ on a message m
  - Compute $\sigma = (H(m))^d$ mod n
  - H is a secure hash-function
- Verify the signature
  - Check H(m) =?= σ^e mod n
  - If the above equation holds, output “accept”; otherwise output “reject”



Shamir’s identity-based key construction

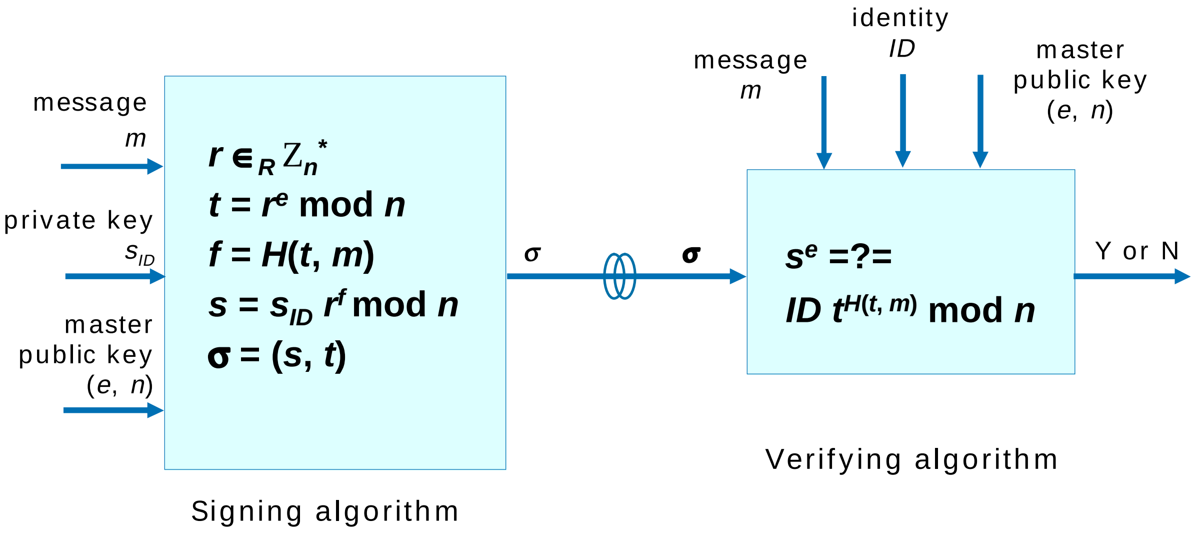
Requirement: Trent needs to authenticate the owner of the identity, before issuing the private key. This is required in PKI as well.

***ID* could be a digest of a data string, e.g., *ID* = *H*(bob@hp.com). In this case, the Shamir identity-based private key is exactly an RSA signature.**

Private key s_{ID}
Identity *ID*
$s_{ID} = ID^d \bmod n$
master private key (*d*, *n*)
private key generation algorithm
Trent - trusted authority

- Master public key – an RSA public key
  - e , $n = pq$, where p and q are two large primes, and e is a prime and does not divide $(p\text{-}1)(q\text{-}1)$
- Master private key – an RSA private key
  - $d = 1/e \bmod (p\text{-}1)(q\text{-}1)$
- User’s public key - his identity
  - *ID*
  - *ID* could be a digest (using a secure hash-function) of a meaningful identifier, e.g., an email address
- User’s private key
  - $s_{ID} = ID^d \bmod n$

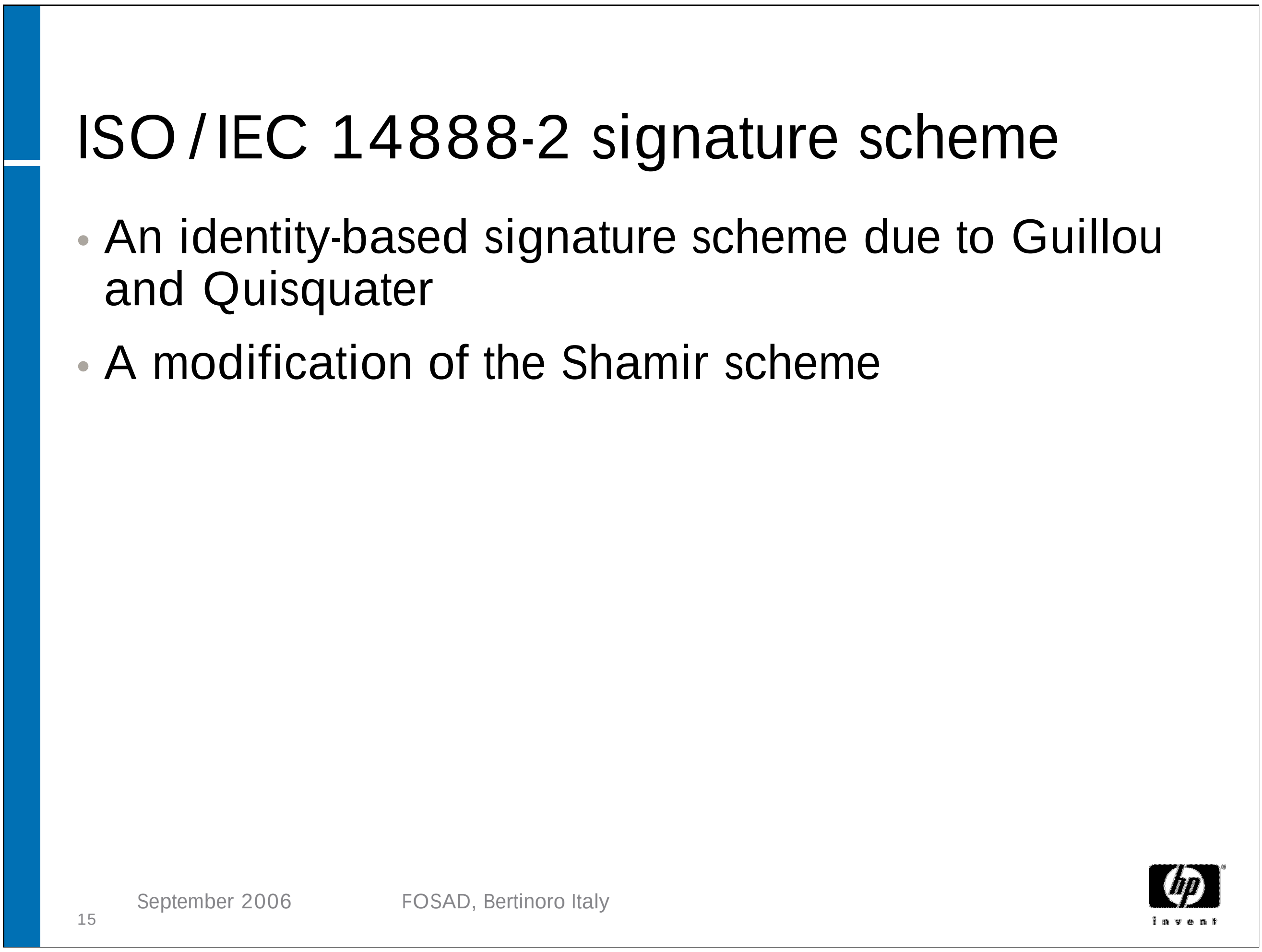
Shamir’s signature scheme



$r \in_R \mathbb{Z}_n^*$
$t = r^e \bmod n$
$f = H(t, m)$
$s = s_{ID}\, r^f \bmod n$
$\sigma = (s, t)$

s^e =?= $ID\; t^{H(t,\, m)} \bmod n$

- Signing a message $m \in \{0, 1\}^*$
  - Choose r at random
  - Compute $t = r^e \bmod n$
  - Compute $f = H(t, m)$, where H is one way function
  - Compute $s = s_{ID}\, r^f \bmod n$
  - Output signature $(s,\ t)$
- Verifying the signature
  - Check whether the equation holds
    s^e =?= $ID\; t^{H(t,\, m)} \bmod n$
  - If the equation holds, accept the signature; otherwise reject it

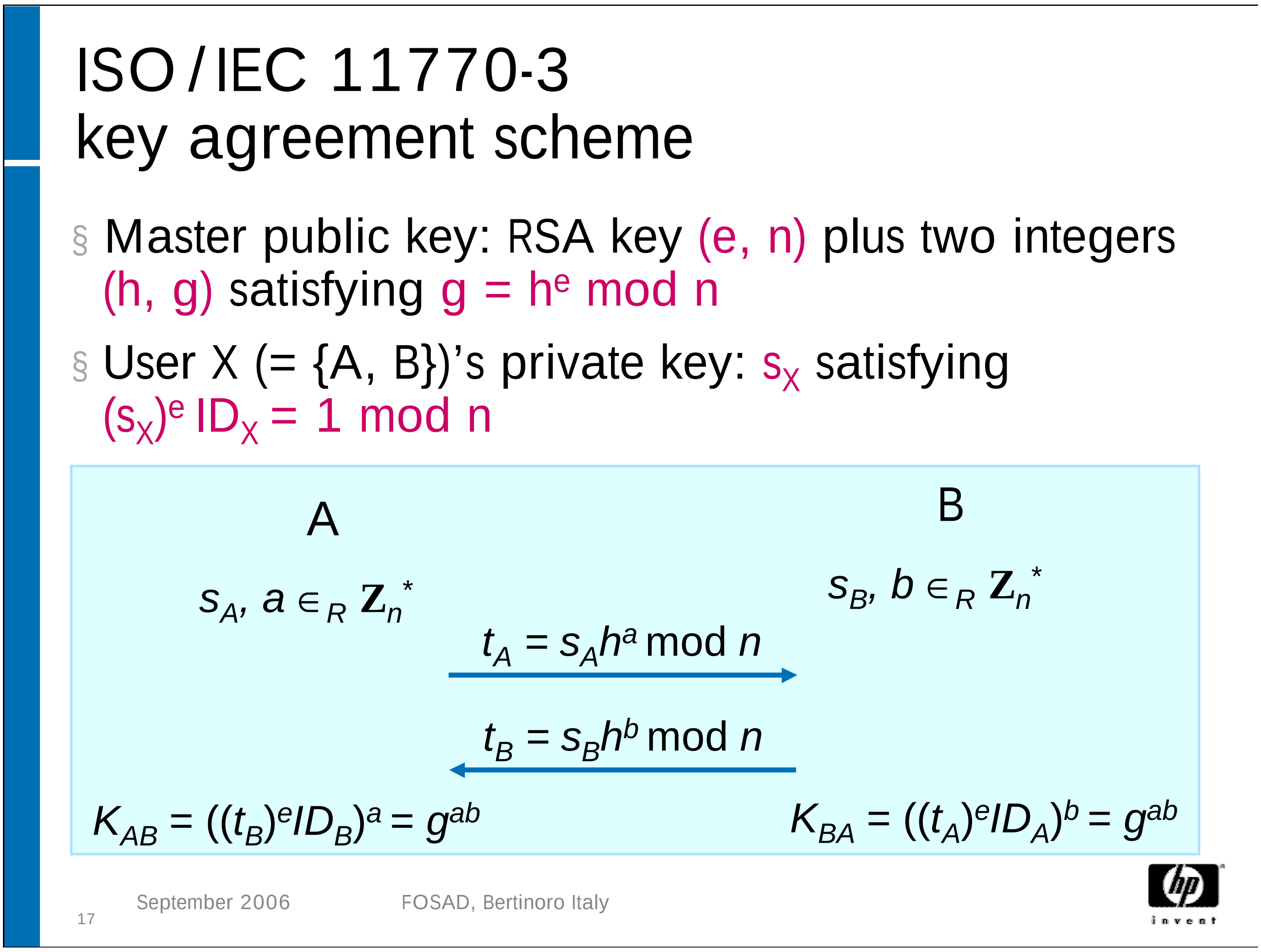


ISO / IEC 14888-2 signature scheme

- An identity-based signature scheme due to Guillou and Quisquater
- A modification of the Shamir scheme

- ISO / IEC 14888-2 Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms
- This standard was published in 1999
- It is now in the revising process

Identity-based key agreement from RSA



ISO / IEC 11770-3 key agreement scheme

- Master public key: RSA key (e, n) plus two integers (h, g) satisfying $g = h^e \bmod n$
- User X (= {A, B})'s private key: s_X satisfying $(s_X)^e ID_X = 1 \bmod n$

A

B

$s_A, a \in_R \mathbf{Z}_n^*$

$s_B, b \in_R \mathbf{Z}_n^*$

$$\xrightarrow{t_A = s_A h^a \bmod n}$$

$$\xleftarrow{t_B = s_B h^b \bmod n}$$

$K_{AB} = ((t_B)^e ID_B)^a = g^{ab}$

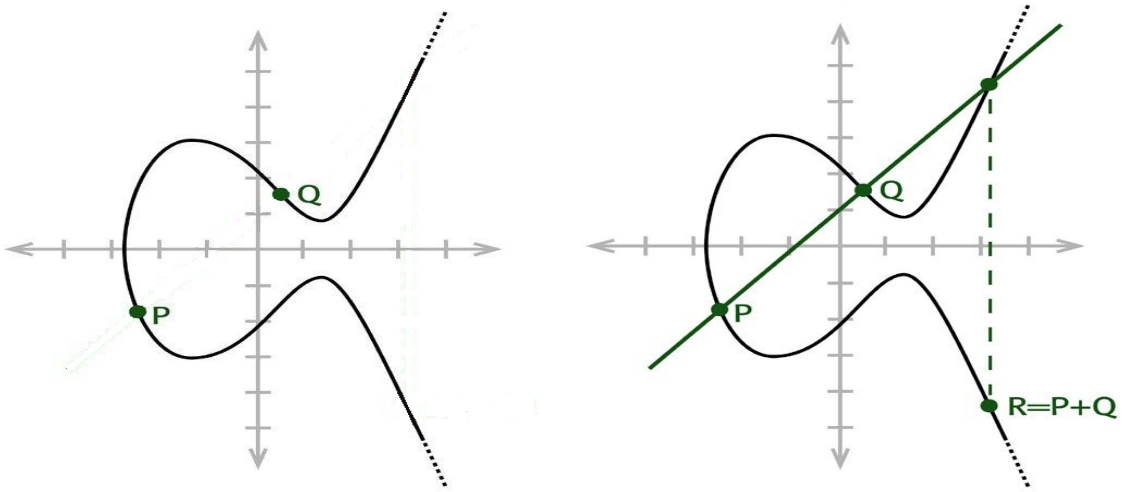
$K_{BA} = ((t_A)^e ID_A)^b = g^{ab}$

- ISO / IEC 11770-3 Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques
- This standard was published in 1999
- It is now in the revising process

- Master public key: RSA modulus n and exponent e, which are the same as in the Shamir key construction, two elements h and g satisfying $g = h^e \bmod n$
- Master private key: RSA private key d, which is the same as in the Shamir key construction as well
- User X (either A or B) has a private key called s_X satisfying $(s_X)^e ID_X = 1 \bmod n$. The value s_X is computed by Trent as $s_X = (1/ID_X)^d \bmod n$, where ID_X is X's identity
- The key agreement protocol works as follows:
  - A chooses the value a at random, computes t_A and sends it to B
  - B chooses the value b at random, computes t_B and sends it to A
  - A and B computes K_{AB} and K_{BA} respectively
  - If both A and B follow the protocol property, and there is no active attacker modifying their communications, $K_{AB} = K_{BA}$ holds
  - A and B then use this value as their shared secret to retrieve a set of shared keys and to run a key confirmation protocol if requested. This part is standard and well-known, and isn't special for identity-based systems.

Pairings

Elliptic curve

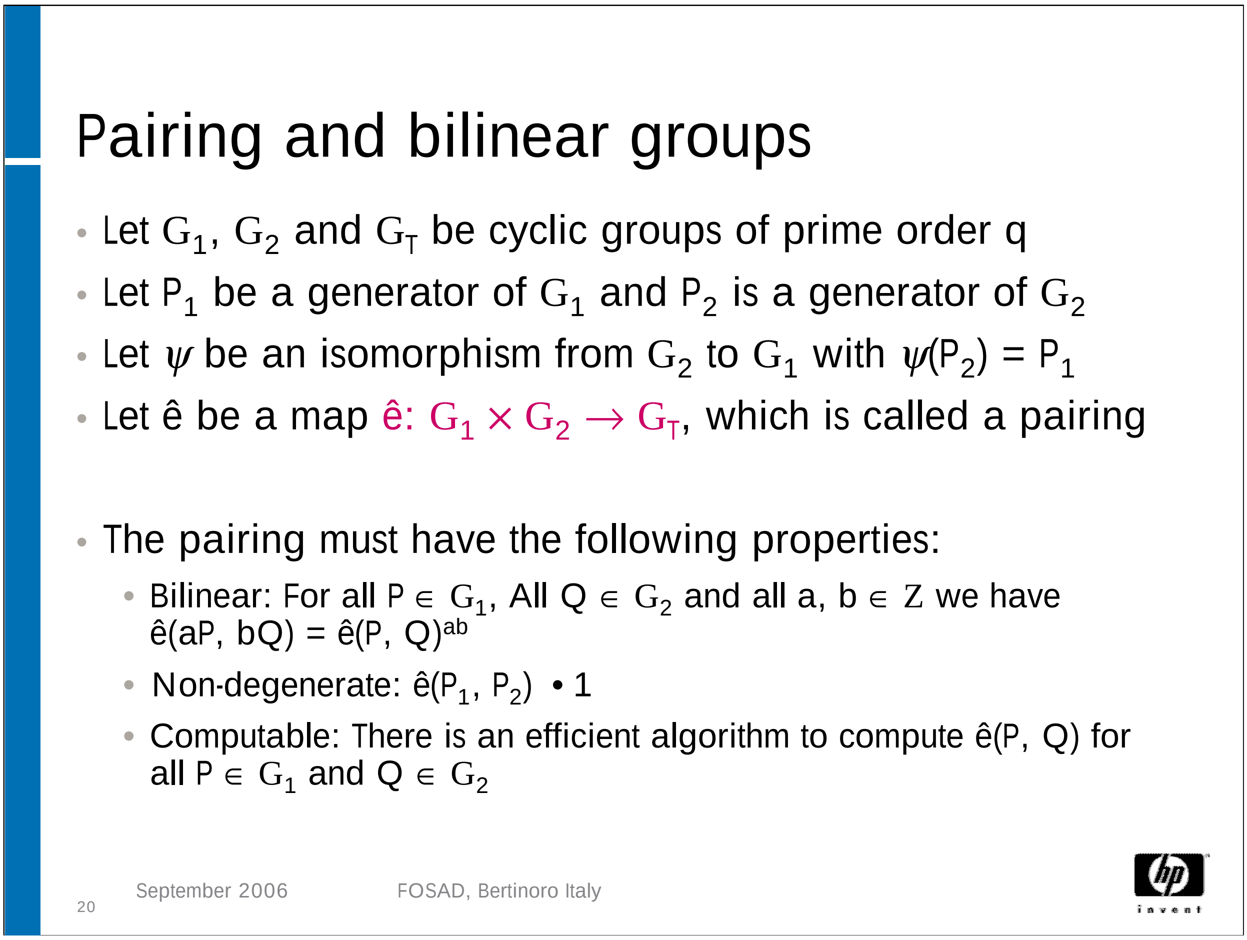


P and Q are points on curve

Let Q = aP denote multiplication operation on the curve, where

Q = P + P + … + P adding a -1 times if a is positive. The operation

satisfies [0]P = 0_E (the point at infinity), and [-a]P = [a](-P).

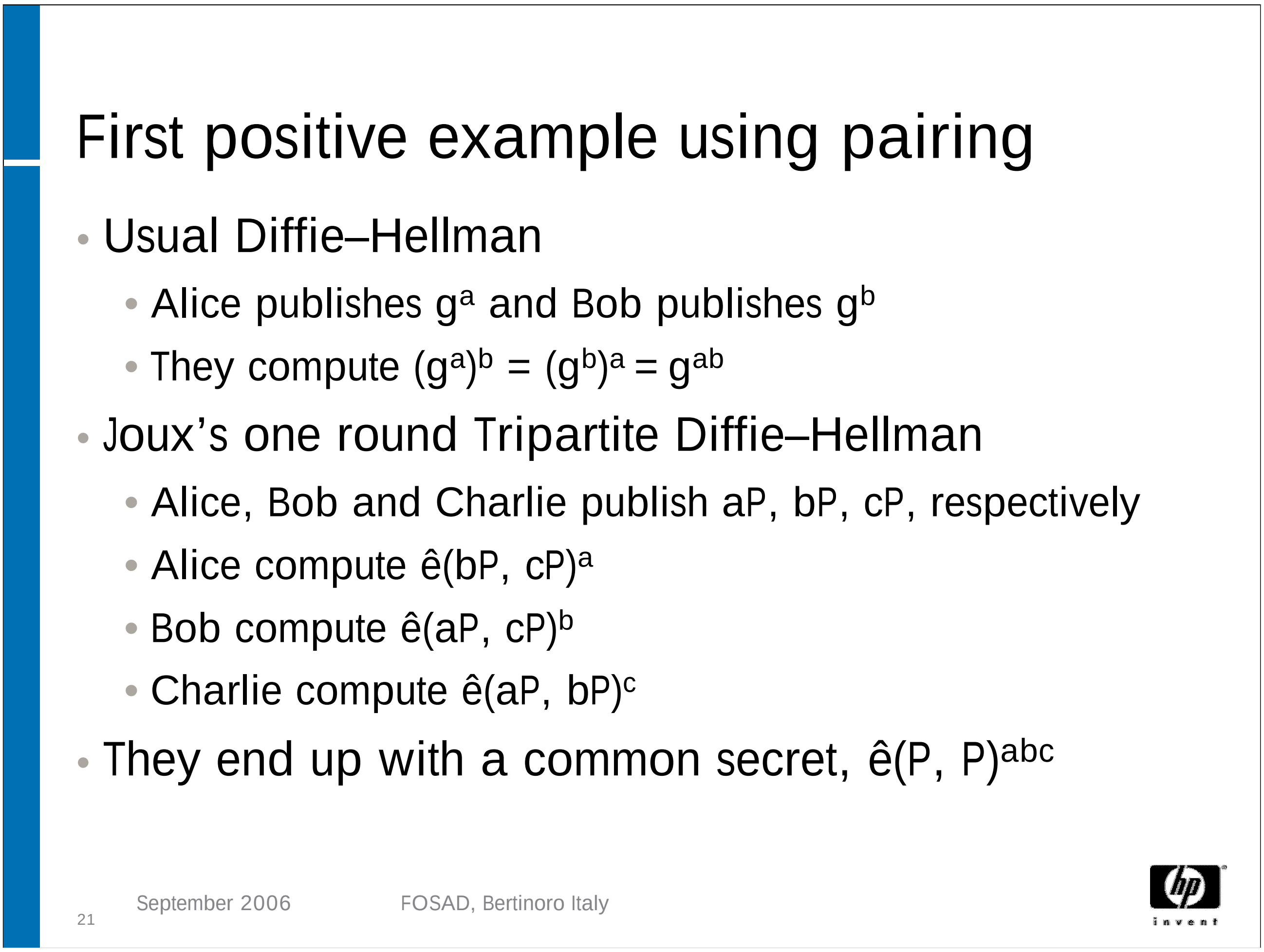


Pairing and bilinear groups

- Let G_1, G_2 and G_T be cyclic groups of prime order q
- Let P_1 be a generator of G_1 and P_2 is a generator of G_2
- Let ψ be an isomorphism from G_2 to G_1 with $\psi(P_2) = P_1$
- Let ê be a map $\hat{e}: G_1 \times G_2 \rightarrow G_T$, which is called a pairing

- The pairing must have the following properties:
  - Bilinear: For all $P \in G_1$, All $Q \in G_2$ and all $a, b \in Z$ we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
  - Non-degenerate: $\hat{e}(P_1, P_2)$ • 1
  - Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P \in G_1$ and $Q \in G_2$

- There are symmetric pairings and asymmetric pairings, dependent on the two input points being in the same group or not. For the purpose of simplicity, we don’t distinguish them in this lecture.
- The most well-known pairings, which have been used in identity-based cryptography, are the Weil pairing and the Tate pairing and their variants.
- The details of these pairings can be found in the following documents:
  - P. Barreto, H. Kim, B. Lynn, and M. Scott, Efficient algorithms for pairing-based cryptosystems, Proceedings of CRYPTO 2002, LNCS 2442, pages 354–369, Springer-Verlag, 2002.
  - D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In Advances in Cryptology - Crypto 2001, Springer-Verlag LNCS 2139, 213-229, 2001.
  - G. Frey, M. Müller, and H. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, IEEE Transactions on Information Theory, 45(5), pp. 1717–1719, 1999.
  - S. Galbraith, Supersingular curves in cryptography, Proceedings of Asiacrypt 2001, LNCS 2248, pp. 495-513, Springer-Verlag, 2001.
  - S. Galbraith, K. Harrison, and D. Soldera, Implementing the Tate-pairing, Proceedings of ANTS-V, LNCS 2369, pp. 324–337, Springer-Verlag, 2002.
  - R. Granger, D. Page and N.P. Smart. High security pairing-based cryptography revisited. To appear ANTS-VII, 2006.
  - F. Hess, N.P. Smart and F. Vercauteren. The Eta pairing revisited. Cryptology ePrint Archive, Report 2006/110.



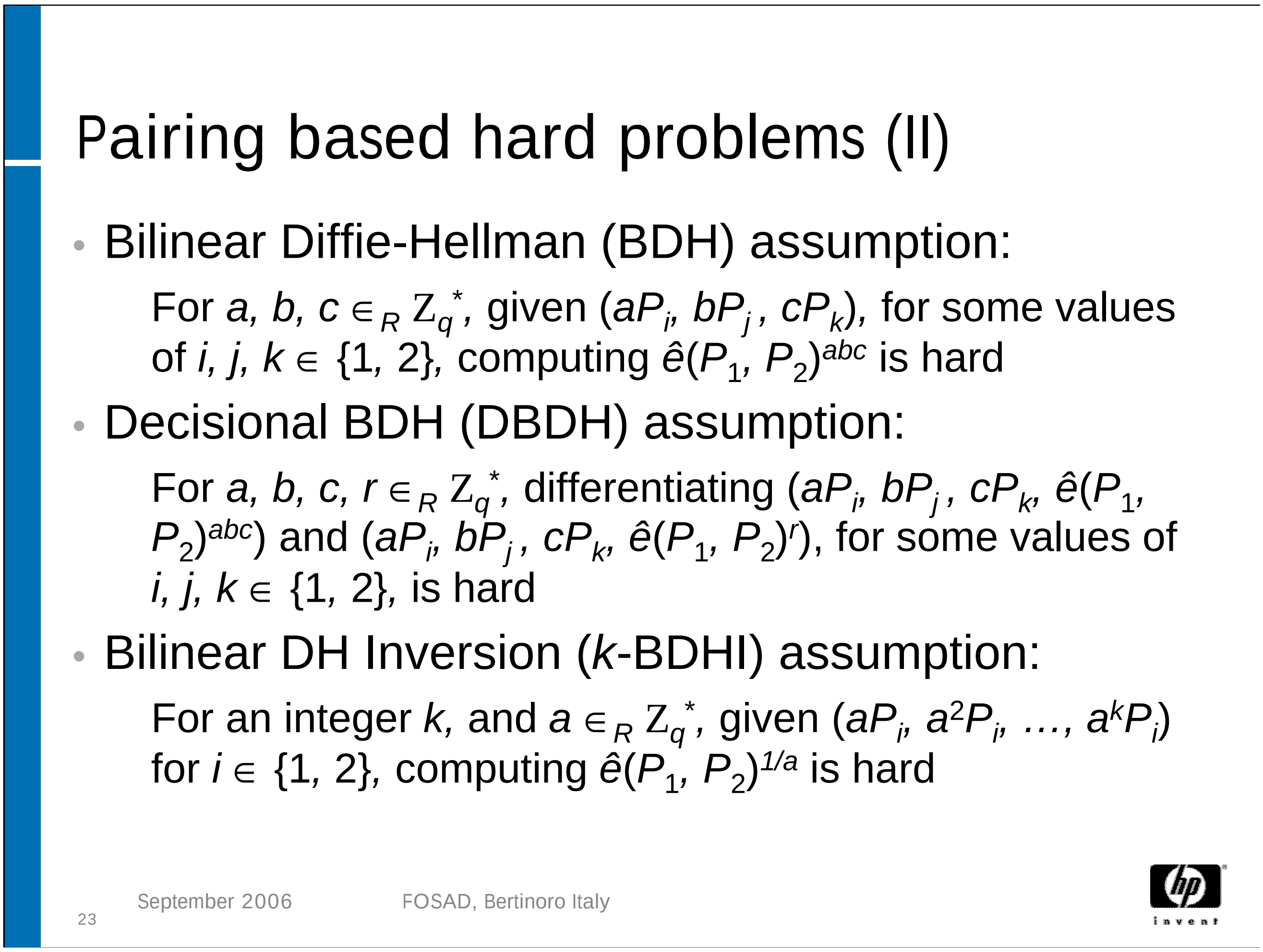
First positive example using pairing

- Usual Diffie–Hellman
  - Alice publishes g^a and Bob publishes g^b
  - They compute $(g^a)^b = (g^b)^a = g^{ab}$
- Joux’s one round Tripartite Diffie–Hellman
  - Alice, Bob and Charlie publish aP, bP, cP, respectively
  - Alice compute $\hat{e}(bP, cP)^a$
  - Bob compute $\hat{e}(aP, cP)^b$
  - Charlie compute $\hat{e}(aP, bP)^c$
- They end up with a common secret, $\hat{e}(P, P)^{abc}$

- A. Joux, A one round protocol for tripartite Diffie-Hellman. In Proceedings of Algorithmic Number Theory Symposium, ANTS-IV, LNCS 1838, pages 385-394, Springer-Verlag, 2000.

Pairing based hard problems (I)

- Usual discrete logarithm assumption
  - given $y = g^x$ mod p, finding x is hard
- discrete logarithm assumption in elliptic curve
  - given $Q = xP \in G$ (either G_1 or G_2), finding x is hard
- Usual Diffie-Hellman assumption
  - given g^a and g^b (mod p), finding g^{ab} mod p is hard
- Diffie-Hellman assumption in elliptic curve
  - given aP, bP $\in G$, finding abP is hard
  - given aP, bP, cP $\in G$, finding abcP is hard



Pairing based hard problems (II)

- Bilinear Diffie-Hellman (BDH) assumption:

  For $a, b, c \in_R \mathbb{Z}_q^*$, given (aP_i, bP_j, cP_k), for some values of $i, j, k \in \{1, 2\}$, computing $\hat{e}(P_1, P_2)^{abc}$ is hard

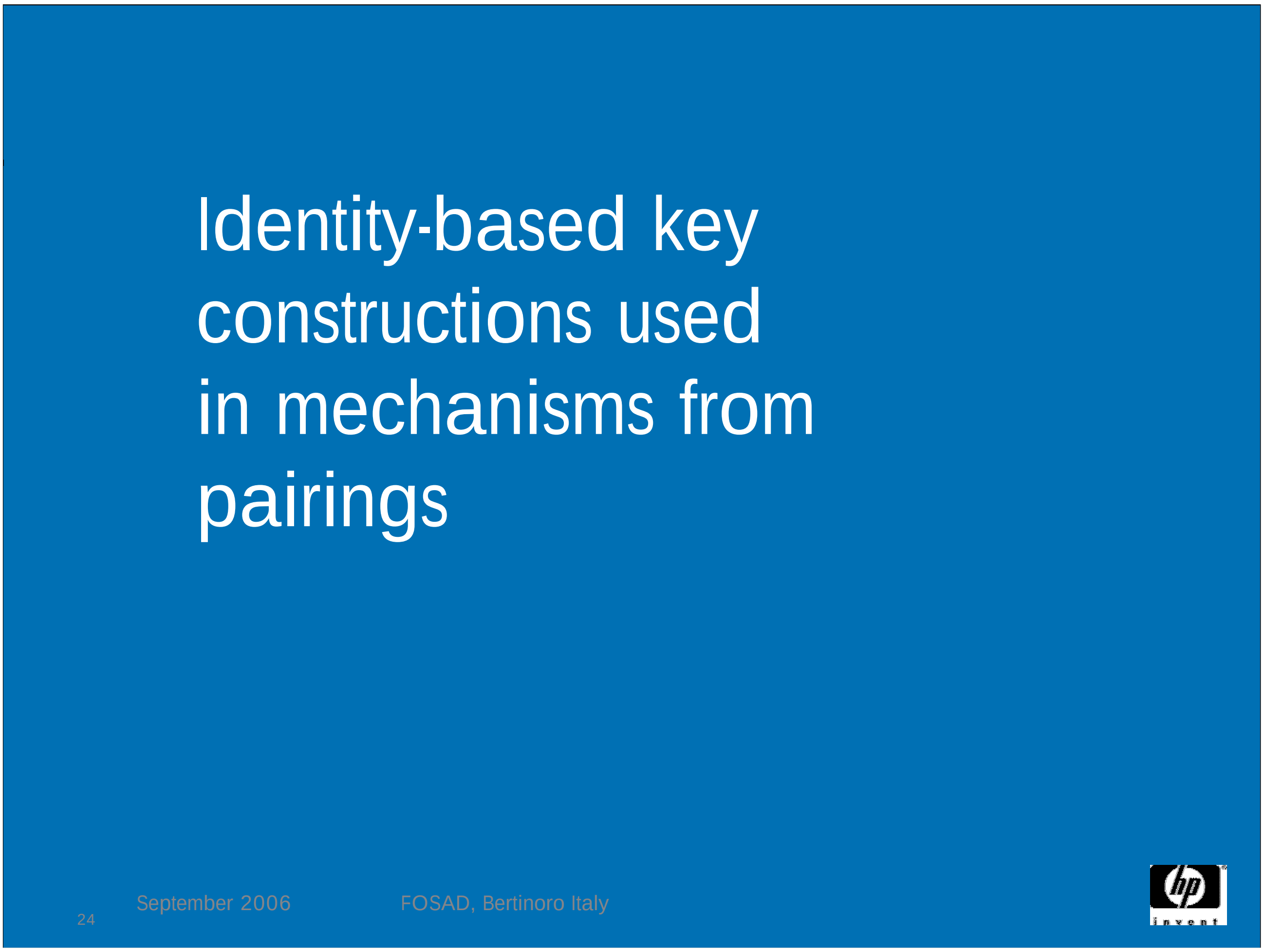
- Decisional BDH (DBDH) assumption:

  For $a, b, c, r \in_R \mathbb{Z}_q^*$, differentiating $(aP_i, bP_j, cP_k, \hat{e}(P_1, P_2)^{abc})$ and $(aP_i, bP_j, cP_k, \hat{e}(P_1, P_2)^r)$, for some values of $i, j, k \in \{1, 2\}$, is hard

- Bilinear DH Inversion (k-BDHI) assumption:

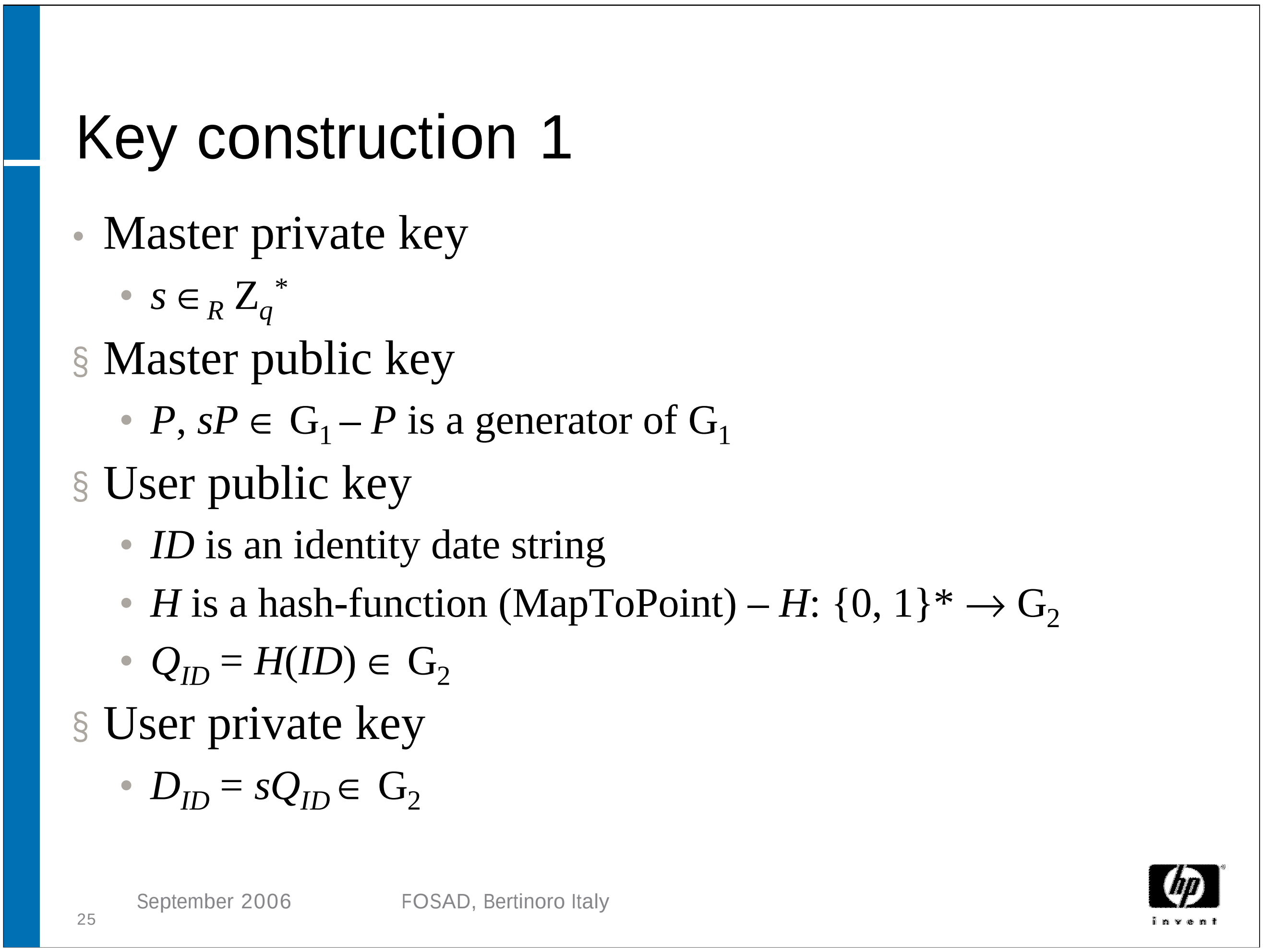
  For an integer k, and $a \in_R \mathbb{Z}_q^*$, given $(aP_i, a^2P_i, \ldots, a^kP_i)$ for $i \in \{1, 2\}$, computing $\hat{e}(P_1, P_2)^{1/a}$ is hard

- The above three are well-known assumptions, which are used to analyse security of pairing based cryptographic mechanisms.
- There are many other assumptions relative to these assumptions.
- A number of variants of these problems and their relationships can be found in the following paper:
  - L. Chen and Z. Cheng. Security proof of Sakai-Kasahar's identity-based encryption scheme. In Proceedings of Cryptography and Coding 2005, volume 3796 of LNCS, pages 442-459. Springer-Verlag, 2005.



Identity-based key constructions used in mechanisms from pairings

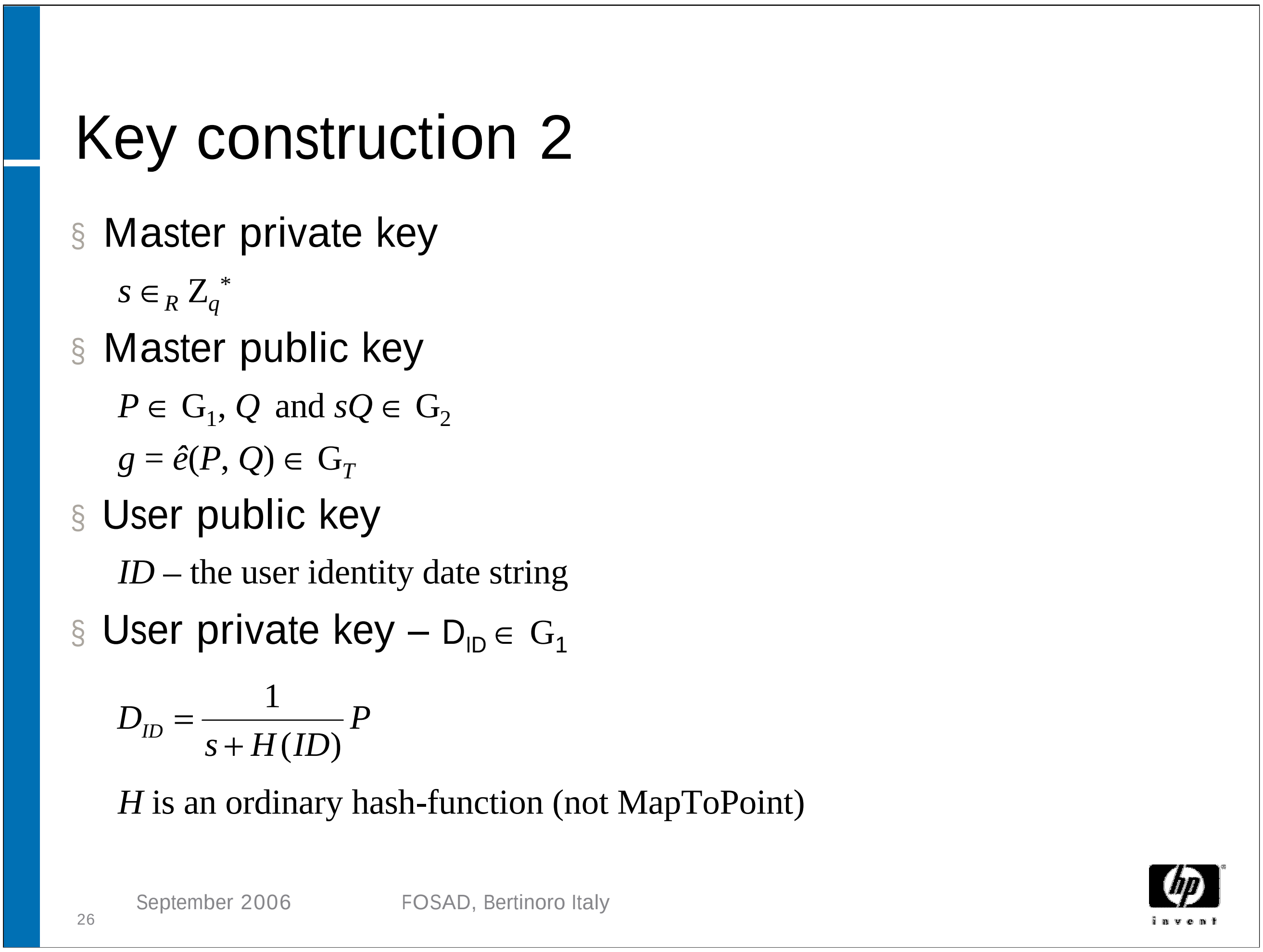
- We only cover two well-known key constructions in this lecture.



Key construction 1

- Master private key
  - $s \in_R Z_q^*$
- Master public key
  - P, $sP \in G_1$ – P is a generator of G_1
- User public key
  - ID is an identity date string
  - H is a hash-function (MapToPoint) – H: $\{0, 1\}^* \rightarrow G_2$
  - $Q_{ID} = H(ID) \in G_2$
- User private key
  - $D_{ID} = sQ_{ID} \in G_2$

- This key construction was first appeared at
  - R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000.
  - R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing over elliptic curve (in Japanese). The 2001 Symposium on Cryptography and Information Security, Oiso, Japan, January 2001.
- The hash-function H is called MapToPoint in the Boneh and Franklin paper.
- In the original version of this key construction, $G_1 = G_2$ – using symmetric pairings.



Key construction 2

- Master private key

  $s \in_R \mathrm{Z}_q^*$

- Master public key

  $P \in \mathrm{G}_1, Q$ and $sQ \in \mathrm{G}_2$

  $g = \hat{e}(P, Q) \in \mathrm{G}_T$

- User public key

  ID – the user identity date string

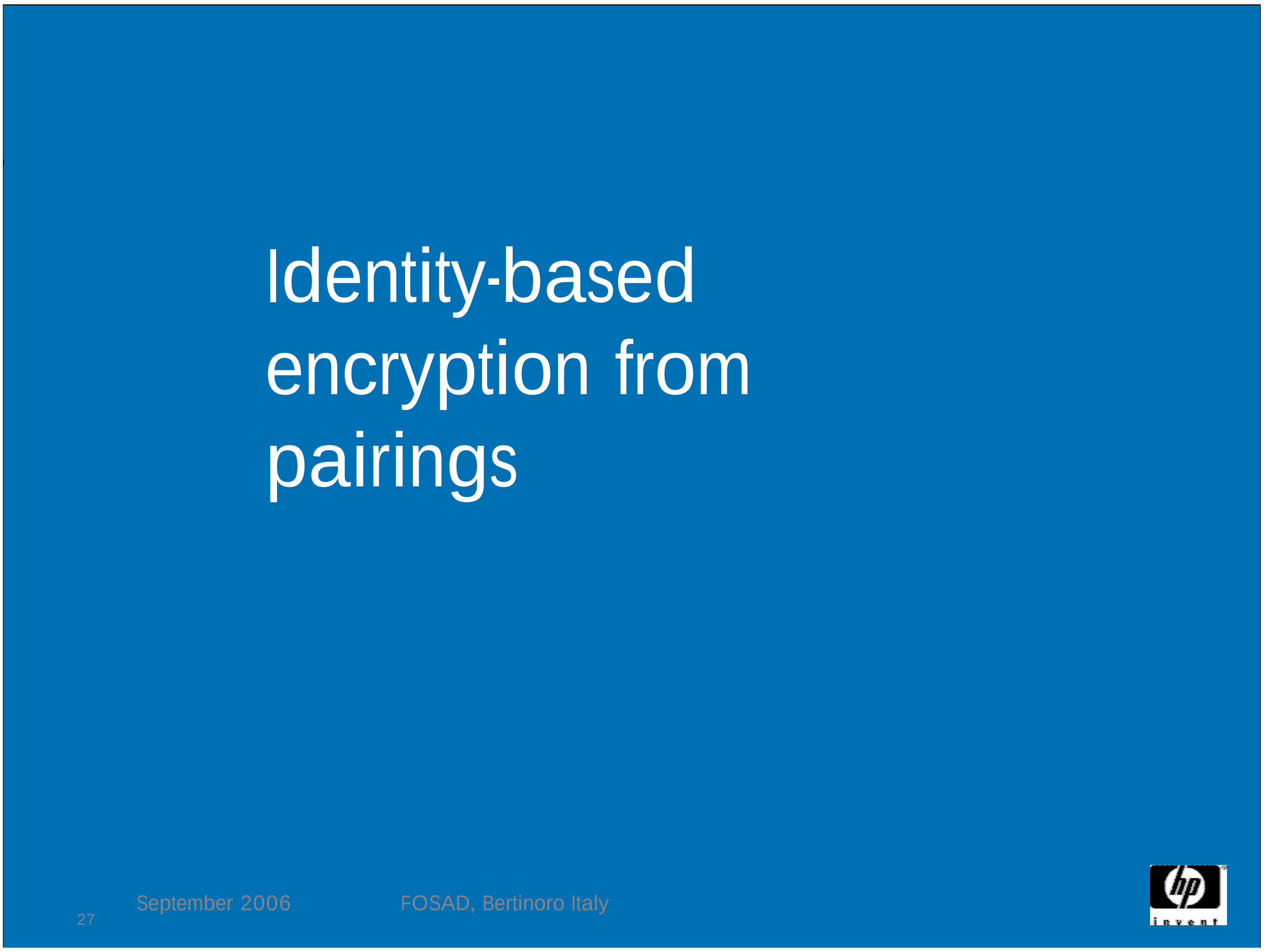
- User private key – $D_{ID} \in \mathrm{G}_1$

  $$D_{ID} = \frac{1}{s + H(ID)} P$$

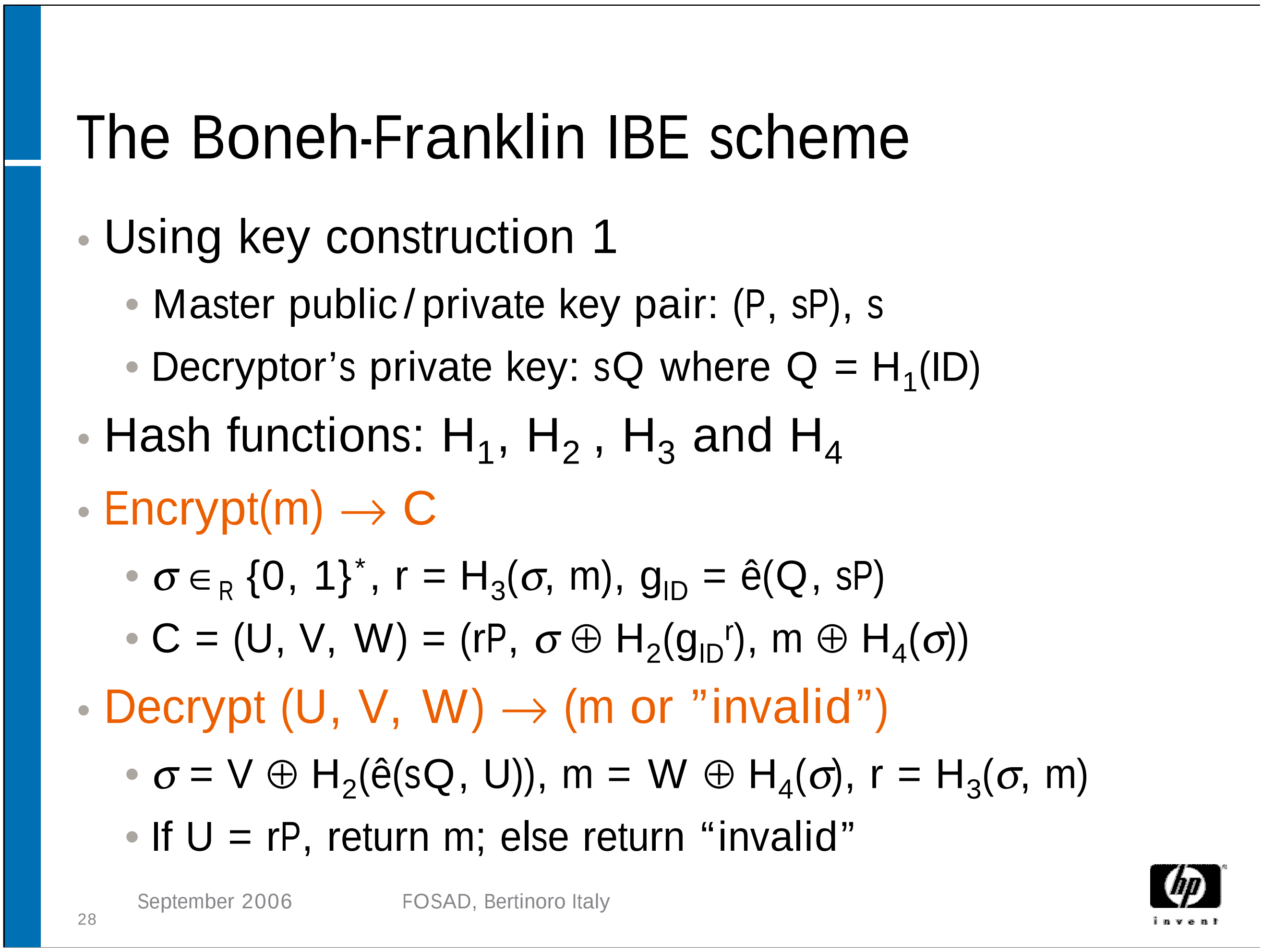
  H is an ordinary hash-function (not MapToPoint)

- This scheme is a simplified version of the scheme in the following paper
  - R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054.
- In the original version of this key construction, $G_1 = G_2$ – again, using symmetric pairings.

- The original one is as follows:
- Master public key
  - $f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$
  - $P, Q \in G_1$, $\hat{e}(P, Q) \in G_T$
  - $a_i Q$ ($i = 0, \dots, d$)
- Master private key
  - a_i ($i = 0, \dots, d$)
- User private key
  - $D_{ID} = (1/f(ID))P$
- In the simplified version, we use $d = 1$.



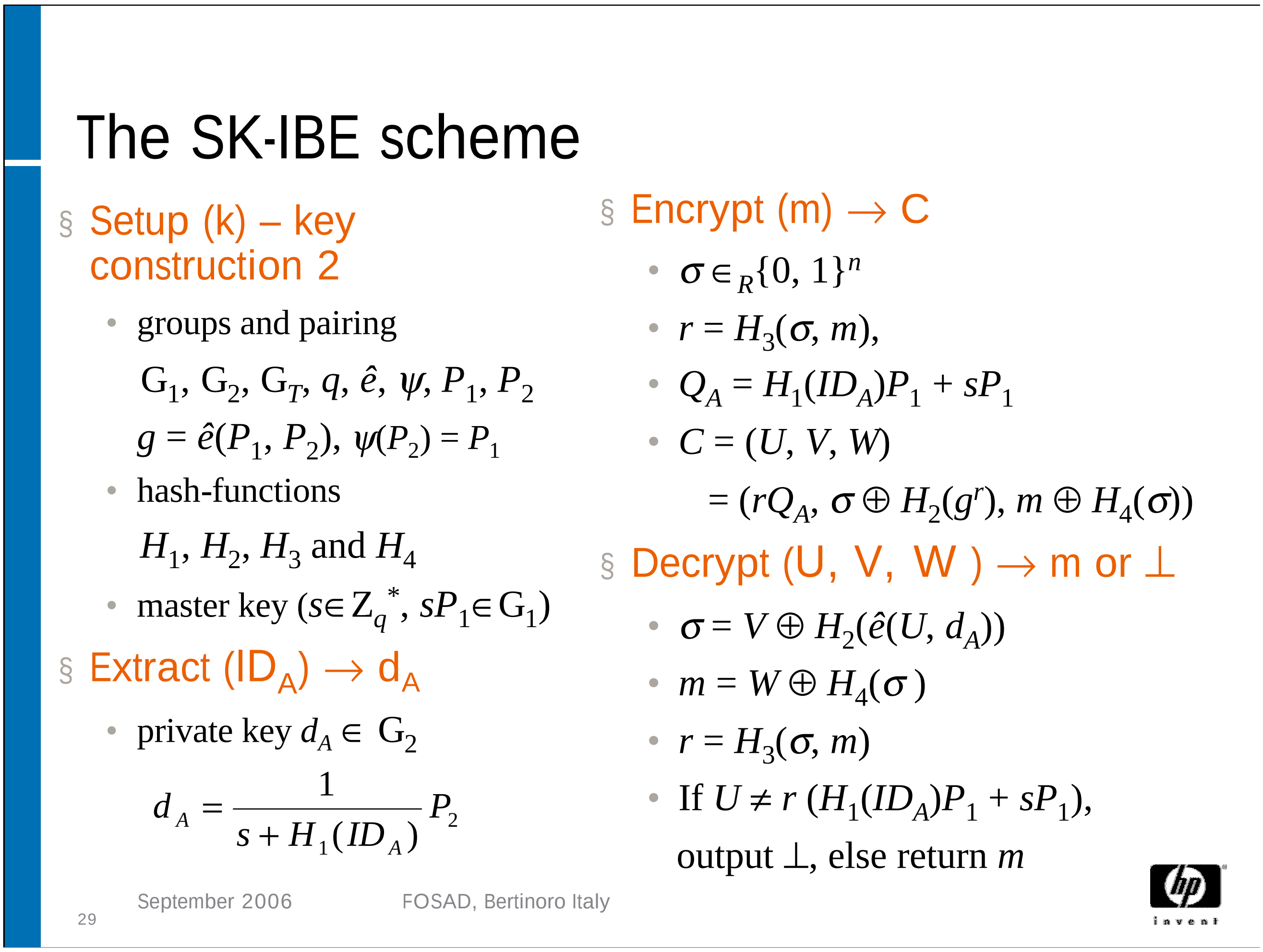
Identity-based encryption from pairings



The Boneh-Franklin IBE scheme

- Using key construction 1
  - Master public/private key pair: (P, sP), s
  - Decryptor's private key: sQ where $Q = H_1(ID)$
- Hash functions: H_1, H_2 , H_3 and H_4
- Encrypt(m) → C
  - $\sigma \in_R \{0, 1\}^*$, $r = H_3(\sigma, m)$, $g_{ID} = \hat{e}(Q, sP)$
  - $C = (U, V, W) = (rP, \sigma \oplus H_2(g_{ID}{}^r), m \oplus H_4(\sigma))$
- Decrypt (U, V, W) → (m or "invalid")
  - $\sigma = V \oplus H_2(\hat{e}(sQ, U))$, $m = W \oplus H_4(\sigma)$, $r = H_3(\sigma, m)$
  - If $U = rP$, return m; else return "invalid"

- D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In Advances in Cryptology - Crypto 2001, Springer-Verlag LNCS 2139, 213-229, 2001.
- In their paper, Boneh and Franklin proposed a formal security model for identity-based encryption, and proved security of their scheme under the BDH assumption in the random oracle model.
- This is the first provable secure identity-based encryption scheme.



The SK-IBE scheme

Setup (k) – key construction 2

- groups and pairing

  $\mathrm{G}_1, \mathrm{G}_2, \mathrm{G}_T, q, \hat{e}, \psi, P_1, P_2$

  $g = \hat{e}(P_1, P_2), \psi(P_2) = P_1$

- hash-functions

  H_1, H_2, H_3 and H_4

- master key ($s \in \mathrm{Z}_q^{\,*}$, $sP_1 \in \mathrm{G}_1$)

Extract (ID_A) → d_A

- private key $d_A \in \mathrm{G}_2$

$$d_A = \frac{1}{s + H_1(ID_A)} P_2$$

Encrypt (m) → C

- $\sigma \in_R \{0, 1\}^n$
- $r = H_3(\sigma, m)$,
- $Q_A = H_1(ID_A)P_1 + sP_1$
- $C = (U, V, W)$

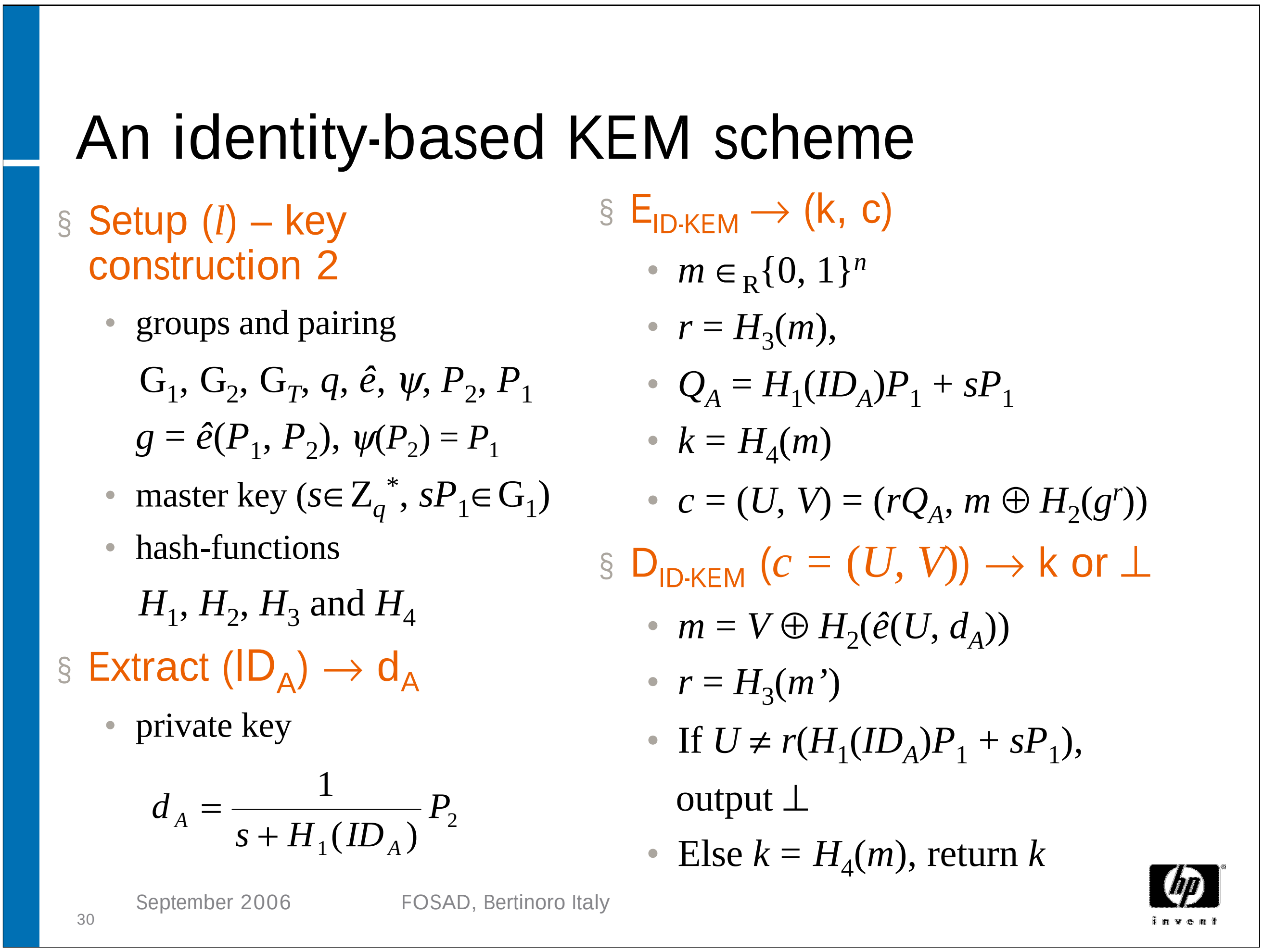
  $= (rQ_A, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma))$

Decrypt (U, V, W) → m or ⊥

- $\sigma = V \oplus H_2(\hat{e}(U, d_A))$
- $m = W \oplus H_4(\sigma\,)$
- $r = H_3(\sigma, m)$
- If $U \neq r\,(H_1(ID_A)P_1 + sP_1)$,

  output ⊥, else return m

- The original scheme was in
  - R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054.
- This is a modified version, and security of this version is proved by Chen and Cheng in
  - L. Chen and Z. Cheng. Security proof of Sakai-Kasahar's identity-based encryption scheme. In Proceedings of Cryptography and Coding 2005, volume 3796 of LNCS, pages 442-459. Springer-Verlag, 2005.
- The security of this scheme relies on the hardness of the k-BDHI problem in the random oracle model.



An identity-based KEM scheme

- Setup (l) – key construction 2
  - groups and pairing

    $G_1, G_2, G_T, q, \hat{e}, \psi, P_2, P_1$

    $g = \hat{e}(P_1, P_2), \psi(P_2) = P_1$
  - master key ($s \in Z_q^*$, $sP_1 \in G_1$)
  - hash-functions

    H_1, H_2, H_3 and H_4
- Extract (ID_A) → d_A
  - private key

$$d_A = \frac{1}{s + H_1(ID_A)} P_2$$

- $E_{ID\text{-}KEM} \rightarrow (k, c)$
  - $m \in_R \{0, 1\}^n$
  - $r = H_3(m)$,
  - $Q_A = H_1(ID_A)P_1 + sP_1$
  - $k = H_4(m)$
  - $c = (U, V) = (rQ_A, m \oplus H_2(g^r))$
- $D_{ID\text{-}KEM}$ ($c = (U, V)$) → k or ⊥
  - $m = V \oplus H_2(\hat{e}(U, d_A))$
  - $r = H_3(m')$
  - If $U \neq r(H_1(ID_A)P_1 + sP_1)$, output ⊥
  - Else $k = H_4(m)$, return k

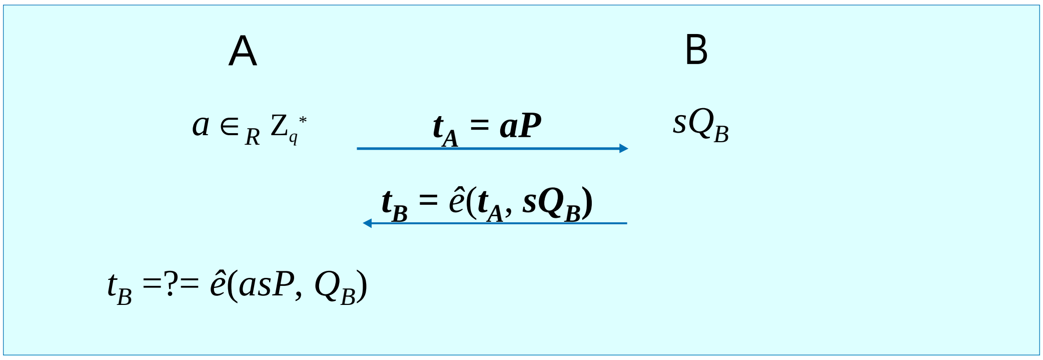
- L. Chen, Z. Cheng, J. Malone-Lee and N. Smart. An efficient ID-KEM based on the Sakai-Kasahara key construction. IEE Proceedings Information Security, Vol. 153, No. 1 (March 2006) 19-26. See also: Cryptology ePrint Archive, Report 2005/224, 2005.
- An extended work, titled "SK-KEM: An Identity-Based KEM", has been submitted to IEEE P1363.3 by M. Barbosa, L. Chen, Z. Cheng, M. Chimley, A. Dent, P. Farshim, K. Harrison, J. Malone-Lee, N. P. Smart, F Vercauteren, which is available at http://grouper.ieee.org/groups/1363/IBC/submissions/index.html.
- The security of this scheme is proved under the k-BDHI assumption in the random oracle model.
- KEM – Key Encapsulation Mechanism.
- DEM – Data Encapsulation Mechanism.
- The best reference for the KEM-DEM technology is
  - V. Shoup. A proposal for an ISO standard for public key encryption (version 2.1), ISO/IEC JTC1/SC27, N2563, http://www.shoup.net/papers/iso-2_1.pdf, Dec. 2001.

Identity-based authentication from pairings

An identity-based entity authentication scheme

Using key construction 1

- Master public/private key pair: (P, sP), s
- Hash-function H: {0, 1}* → G_2
- User B's private key: sQ_B where $Q_B = H(ID_B)$



A

B

$a \in_R Z_q^*$

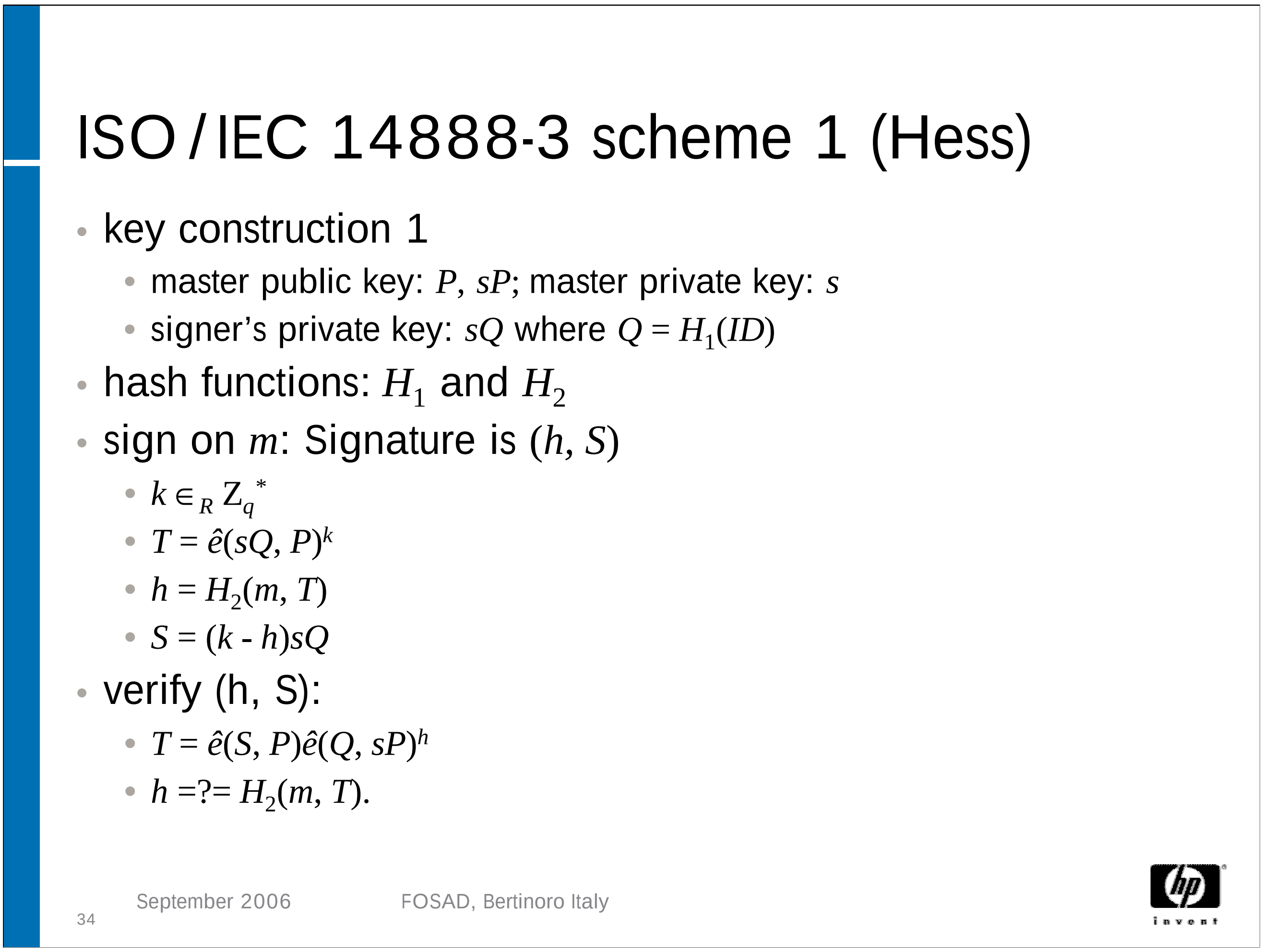
$\boldsymbol{t_A = aP}$ $\xrightarrow{\hphantom{xxxxxx}}$

sQ_B

$\boldsymbol{t_B = \hat{e}(t_A, sQ_B)}$ $\xleftarrow{\hphantom{xxxxxx}}$

$t_B =?= \hat{e}(asP, Q_B)$

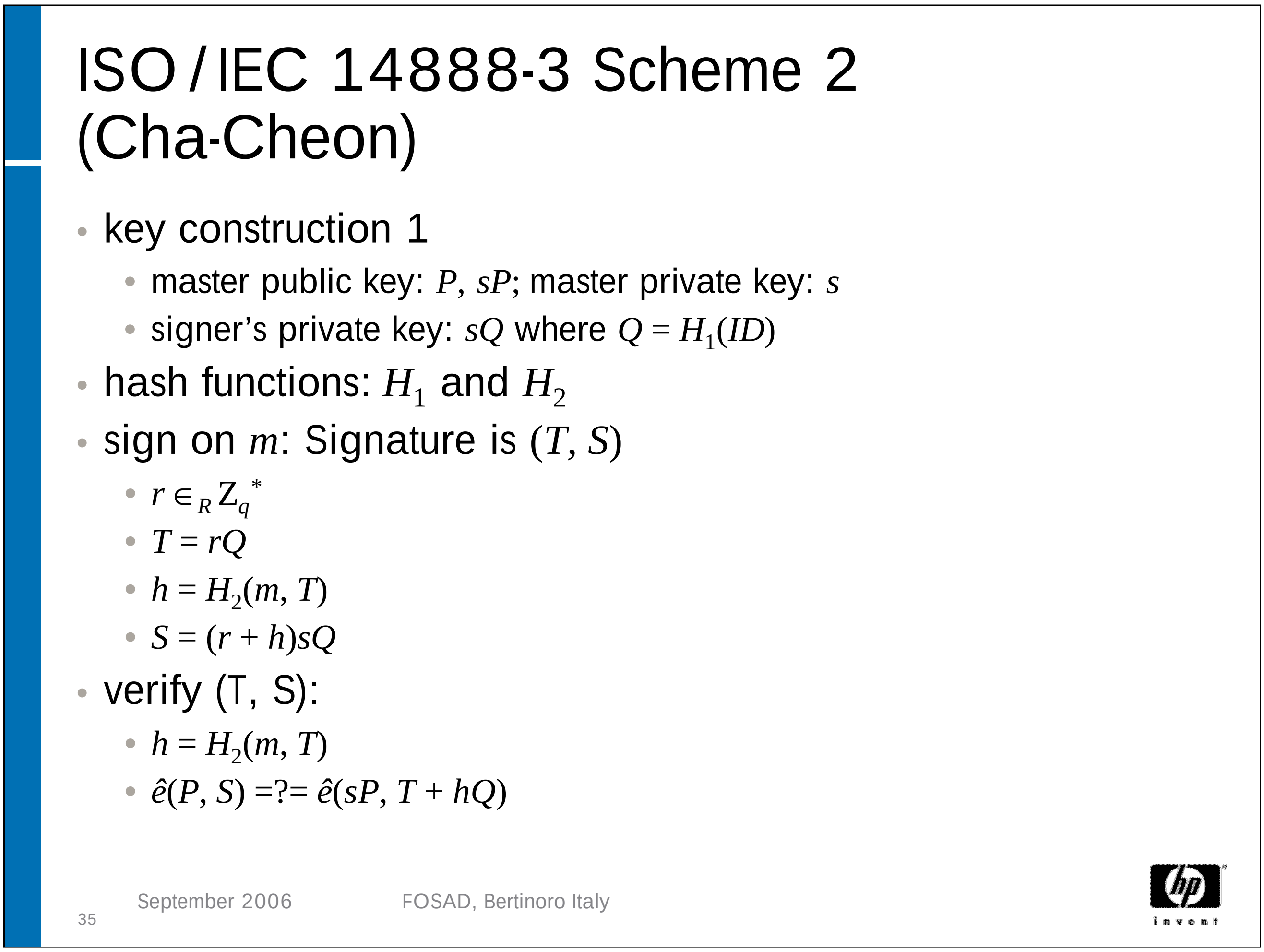
Identity-based signatures from pairings



ISO / IEC 14888-3 scheme 1 (Hess)

- key construction 1
  - master public key: P, sP; master private key: s
  - signer's private key: sQ where $Q = H_1(ID)$
- hash functions: H_1 and H_2
- sign on m: Signature is (h, S)
  - $k \in_R Z_q^*$
  - $T = \hat{e}(sQ, P)^k$
  - $h = H_2(m, T)$
  - $S = (k - h)sQ$
- verify (h, S):
  - $T = \hat{e}(S, P)\hat{e}(Q, sP)^h$
  - $h =?= H_2(m, T)$.

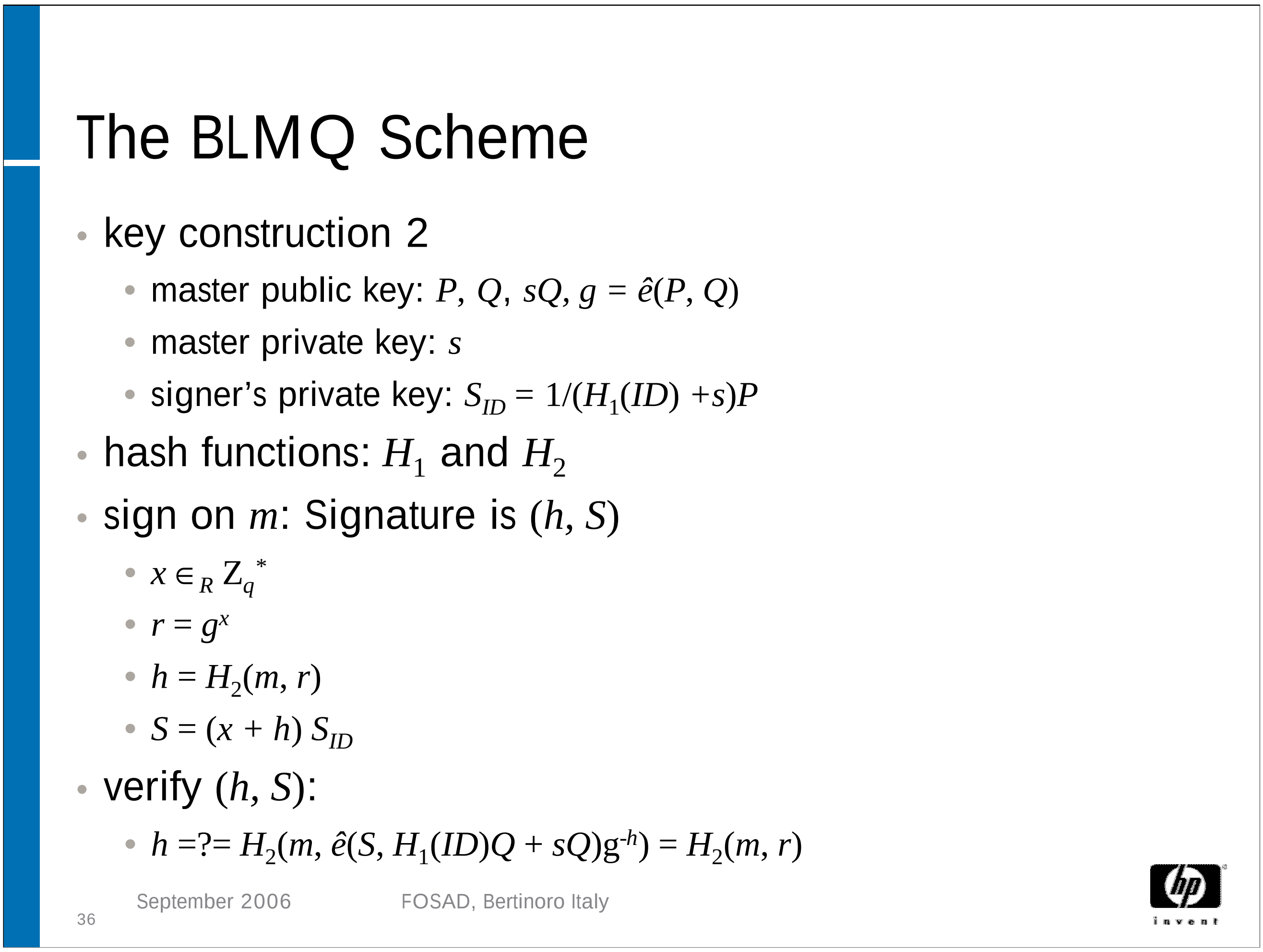
- ISO / IEC 14888-3 Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms
- This standard was published in 1998
- It is in the revising process
- This scheme is in the revised version
- The original scheme was published at
  - F. Hess. Efficient identity based signature schemes based on pairings. In Proceedings of Selected Areas in Cryptography – SAC 2002, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.
- The security of this scheme relies on the hardness of the Diffie-Hellman problem in the random oracle model.



ISO / IEC 14888-3 Scheme 2 (Cha-Cheon)

- key construction 1
  - master public key: P, sP; master private key: s
  - signer’s private key: sQ where $Q = H_1(ID)$
- hash functions: H_1 and H_2
- sign on m: Signature is (T, S)
  - $r \in_R \mathrm{Z}_q^*$
  - $T = rQ$
  - $h = H_2(m, T)$
  - $S = (r + h)sQ$
- verify (T, S):
  - $h = H_2(m, T)$
  - $\hat{e}(P, S) =?= \hat{e}(sP, T + hQ)$

- Again. this scheme is in the revised version
- The original scheme was published at
  - – J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups. In Proceedings of Practice and Theory in Public Key Cryptography – PKC 2003, LNCS 2567, pp. 18-30, Springer-Verlag, 2003. See also Cryptology ePrint Archive, Report 2002/018.
- The security of this scheme relies on the hardness of the Diffie-Hellman problem in the random oracle model.

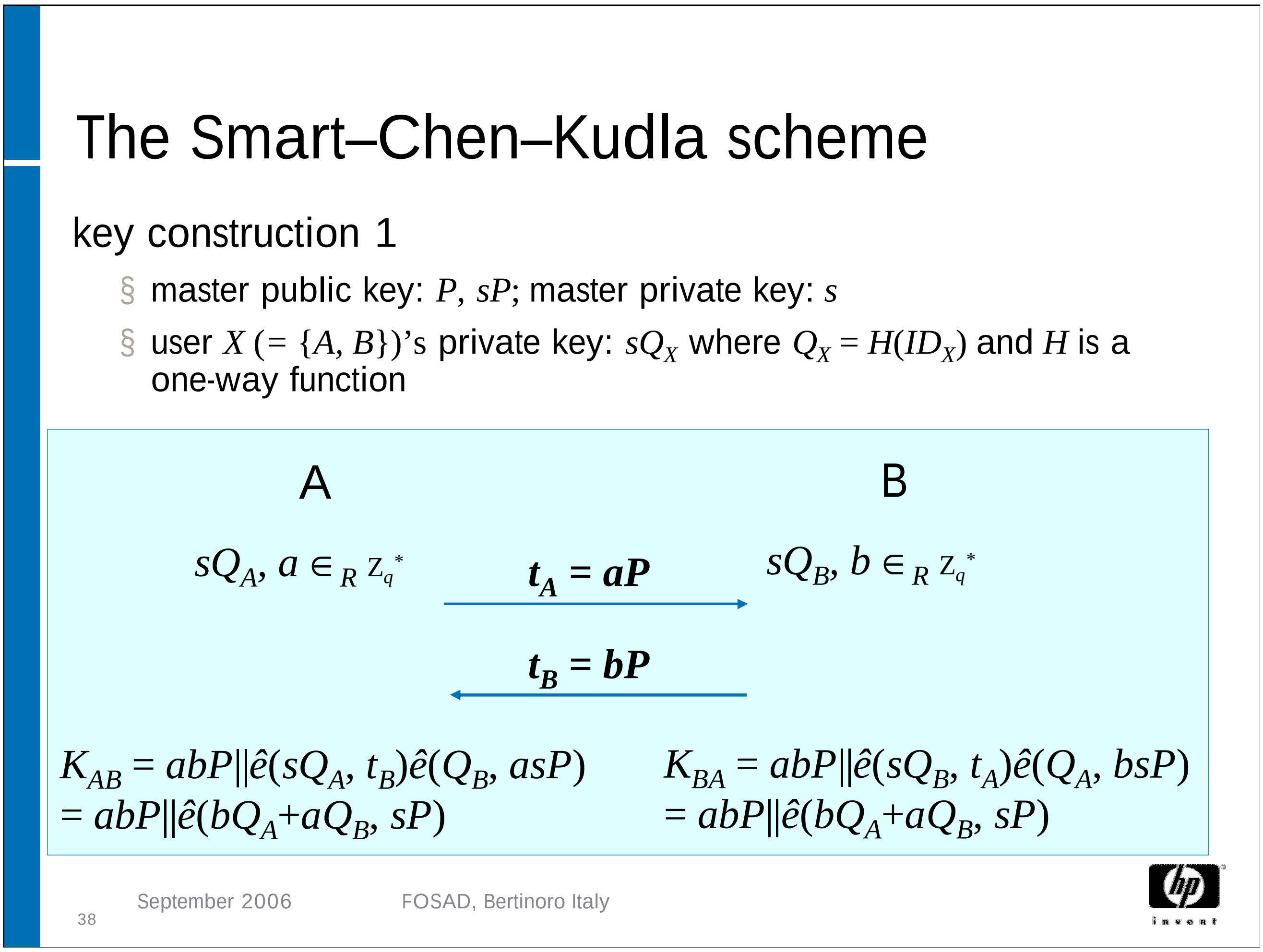


The BLMQ Scheme

- key construction 2
  - master public key: $P, Q, sQ, g = \hat{e}(P, Q)$
  - master private key: s
  - signer's private key: $S_{ID} = 1/(H_1(ID) + s)P$
- hash functions: H_1 and H_2
- sign on m: Signature is (h, S)
  - $x \in_R Z_q^*$
  - $r = g^x$
  - $h = H_2(m, r)$
  - $S = (x + h)\, S_{ID}$
- verify (h, S):
  - $h =?= H_2(m, \hat{e}(S, H_1(ID)Q + sQ)g^{-h}) = H_2(m, r)$

- This scheme has been submitted to IEEE P1363.3 as
  - P. Barreto, B. Libert, N. McCullagh, J-J. Quisquater. Efficient and secure identity-based signatures and signcryption from bilinear maps, which is available at http://grouper.ieee.org/groups/1363/IBC/submissions/index.html.
- The original scheme was published as
  - P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In Asiacrypt'05, volume 3788 of LNCS, pages 515-532. Springer, 2005.
- The security of this scheme relies on the hardness of the k-DHI problem, which is defined as follows:
  - The k-Diffie-Hellman Inversion problem (k-DHI) in (G_1, G_2) consists in, given a $(k + 2)$-tuple $(P, Q, aQ, a^2Q, \ldots, a^kQ)$, finding $(1/a)P$, where $P \in G_1$, $Q \in G_2$ and $a \in_R Z_q^*$, and q is the order of these two groups.

Identity-based key agreement from pairings



The Smart–Chen–Kudla scheme

key construction 1

- master public key: P, sP; master private key: s
- user X (= $\{A, B\}$)'s private key: sQ_X where $Q_X = H(ID_X)$ and H is a one-way function

A

B

sQ_A, $a \in_R Z_q^*$

$\xrightarrow{\boldsymbol{t_A = aP}}$

sQ_B, $b \in_R Z_q^*$

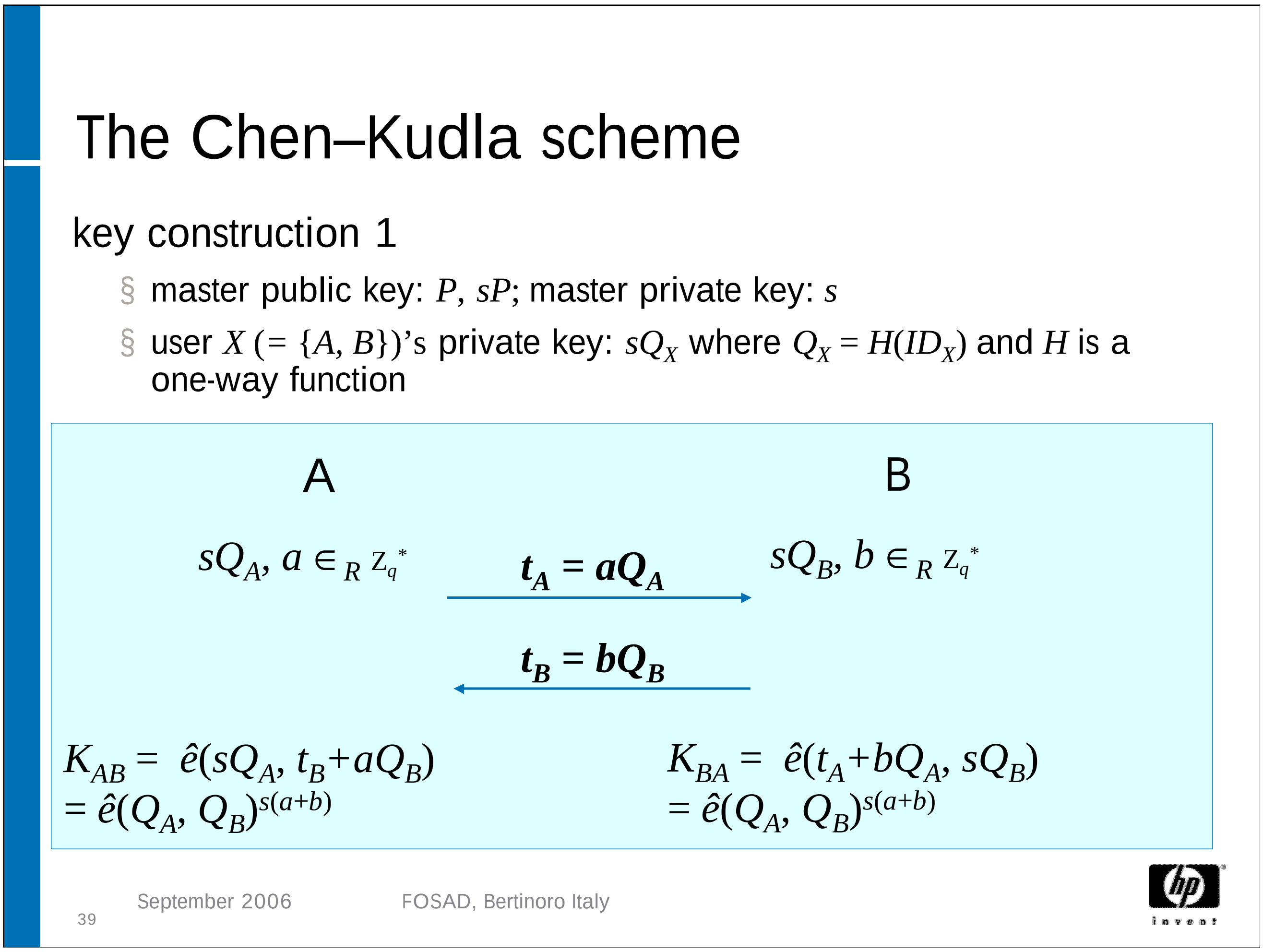
$\xleftarrow{\boldsymbol{t_B = bP}}$

$K_{AB} = abP||\hat{e}(sQ_A, t_B)\hat{e}(Q_B, asP)$
$= abP||\hat{e}(bQ_A+aQ_B, sP)$

$K_{BA} = abP||\hat{e}(sQ_B, t_A)\hat{e}(Q_A, bsP)$
$= abP||\hat{e}(bQ_A+aQ_B, sP)$

The following references are relative to this scheme:

- N.P. Smart. An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 38, 630-632, 2002.
- L. Chen and C. Kudla. Identity based authenticated key agreement from pairings. In IEEE Computer Security Foundations Workshop, 219-233, 2003. A modified version of this paper is available at Cryptology ePrint Archive, Report 2002/184.
- L. Chen, Z. Cheng and N. Smart. Identity-based key agreement protocols from pairings. Cryptology ePrint Archive, Report 2006/199, 2006. This paper lists a list of the existing identity-based key agreement schemes from pairings.
- This scheme has been submitted to IEEE P1363.3 by Chen, Cheng and Smart. It is available at http://grouper.ieee.org/groups/1363/IBC/submissions/index.html.
- The security of this scheme has been proved by Chen, Cheng and Smart under the BDH assumption in the random oracle model.



The Chen–Kudla scheme

key construction 1

- master public key: P, sP; master private key: s
- user X (= $\{A, B\}$)’s private key: sQ_X where $Q_X = H(ID_X)$ and H is a one-way function

A

B

$sQ_A,\ a \in_R Z_q^*$

$\boldsymbol{t_A = aQ_A}$ $\longrightarrow$

$sQ_B,\ b \in_R Z_q^*$

$\longleftarrow$ $\boldsymbol{t_B = bQ_B}$

$K_{AB} = \hat{e}(sQ_A, t_B + aQ_B)$
$= \hat{e}(Q_A, Q_B)^{s(a+b)}$

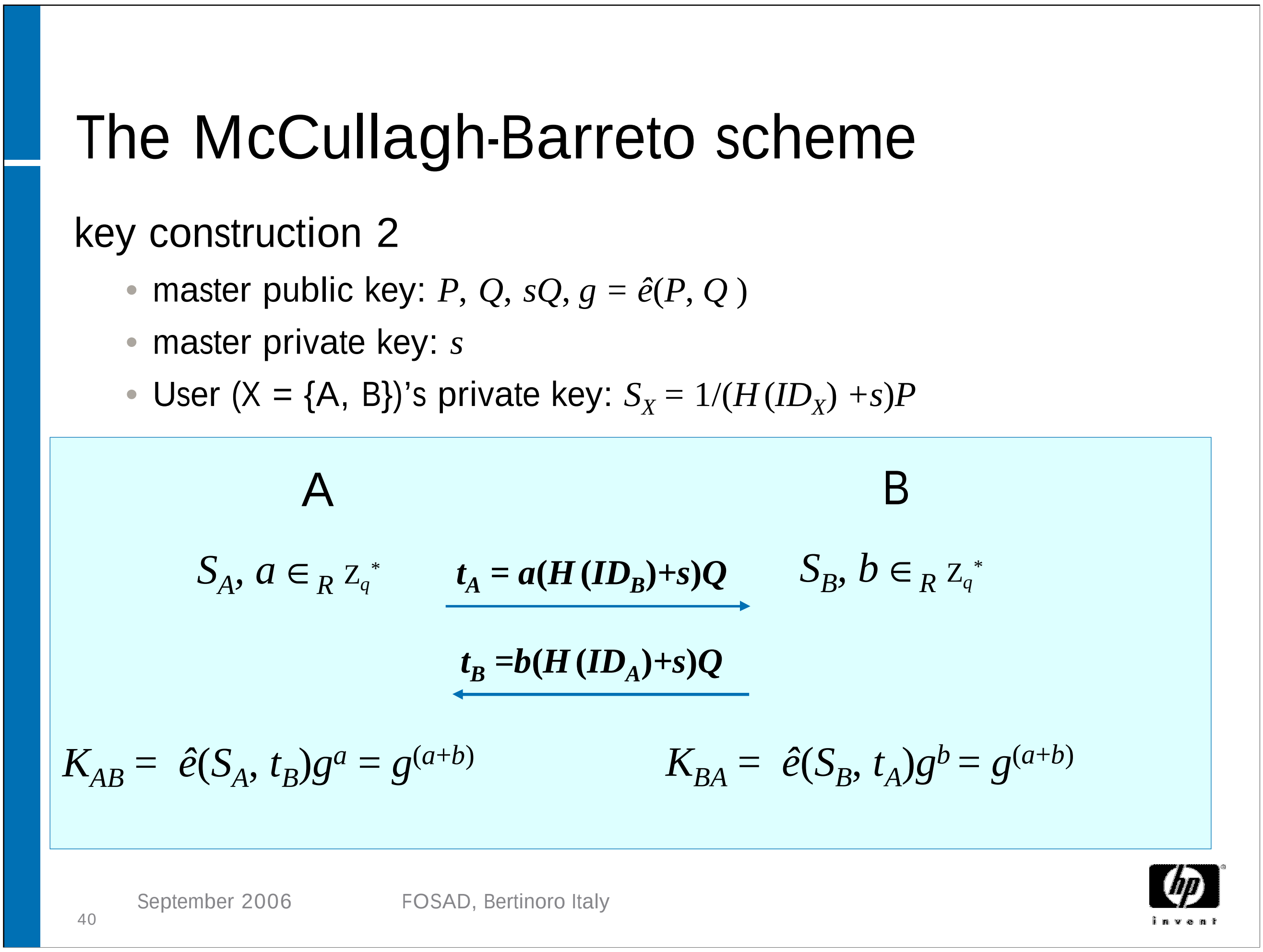
$K_{BA} = \hat{e}(t_A + bQ_A, sQ_B)$
$= \hat{e}(Q_A, Q_B)^{s(a+b)}$

The scheme was proposed in the following paper, where security of this scheme was proved in a weak version of the BR model.

- L. Chen and C. Kudla. Identity based authenticated key agreement from pairings. In IEEE Computer Security Foundations Workshop, 219-233, 2003. A modified version of this paper is available at Cryptology ePrint Archive, Report 2002/184.

A modified version of this scheme is given in the following paper, where security of this scheme is proved in the BR model.

- L. Chen, Z. Cheng and N. Smart. Identity-based key agreement protocols from pairings. Cryptology ePrint Archive, Report 2006/199, 2006.



The McCullagh-Barreto scheme

key construction 2

- master public key: $P, Q, sQ, g = \hat{e}(P, Q)$
- master private key: s
- User (X = {A, B})'s private key: $S_X = 1/(H(ID_X) + s)P$

A | B

$S_A, a \in_R Z_q^*$ $\xrightarrow{\mathbf{t_A = a(H(ID_B)+s)Q}}$ $S_B, b \in_R Z_q^*$

$\xleftarrow{\mathbf{t_B = b(H(ID_A)+s)Q}}$

$K_{AB} = \hat{e}(S_A, t_B)g^a = g^{(a+b)}$ $K_{BA} = \hat{e}(S_B, t_A)g^b = g^{(a+b)}$

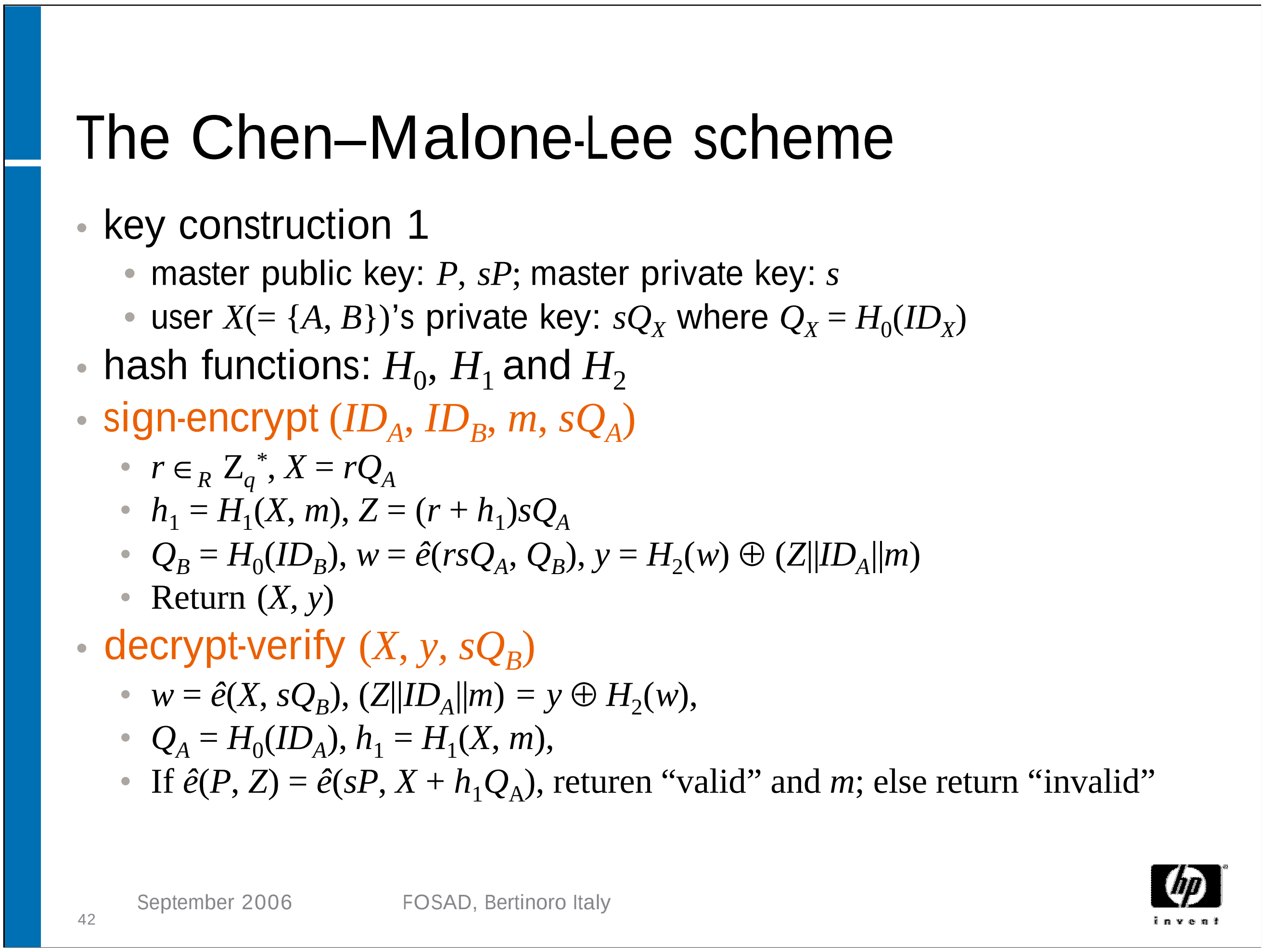
The scheme was proposed in the following papers, where security of this scheme was proved in a weak version of the BR model.

- N. McCullagh and P.S.L.M. Barreto. A new two-party identity-based authenticated key agreement. In Proceedings of CT-RSA 2005, LNCS 3376, pp. 262-274, 2005.
- N. McCullagh and P. S. L. M. Barreto. A new two-party identity-based authenticated key agreement. Cryptology ePrint Archive, Report 2004/122.

A modified version of this scheme is given in the following paper, where security of this scheme is proved in the BR model.

- L. Chen, Z. Cheng and N. Smart. Identity-based key agreement protocols from pairings. Cryptology ePrint Archive, Report 2006/199, 2006.

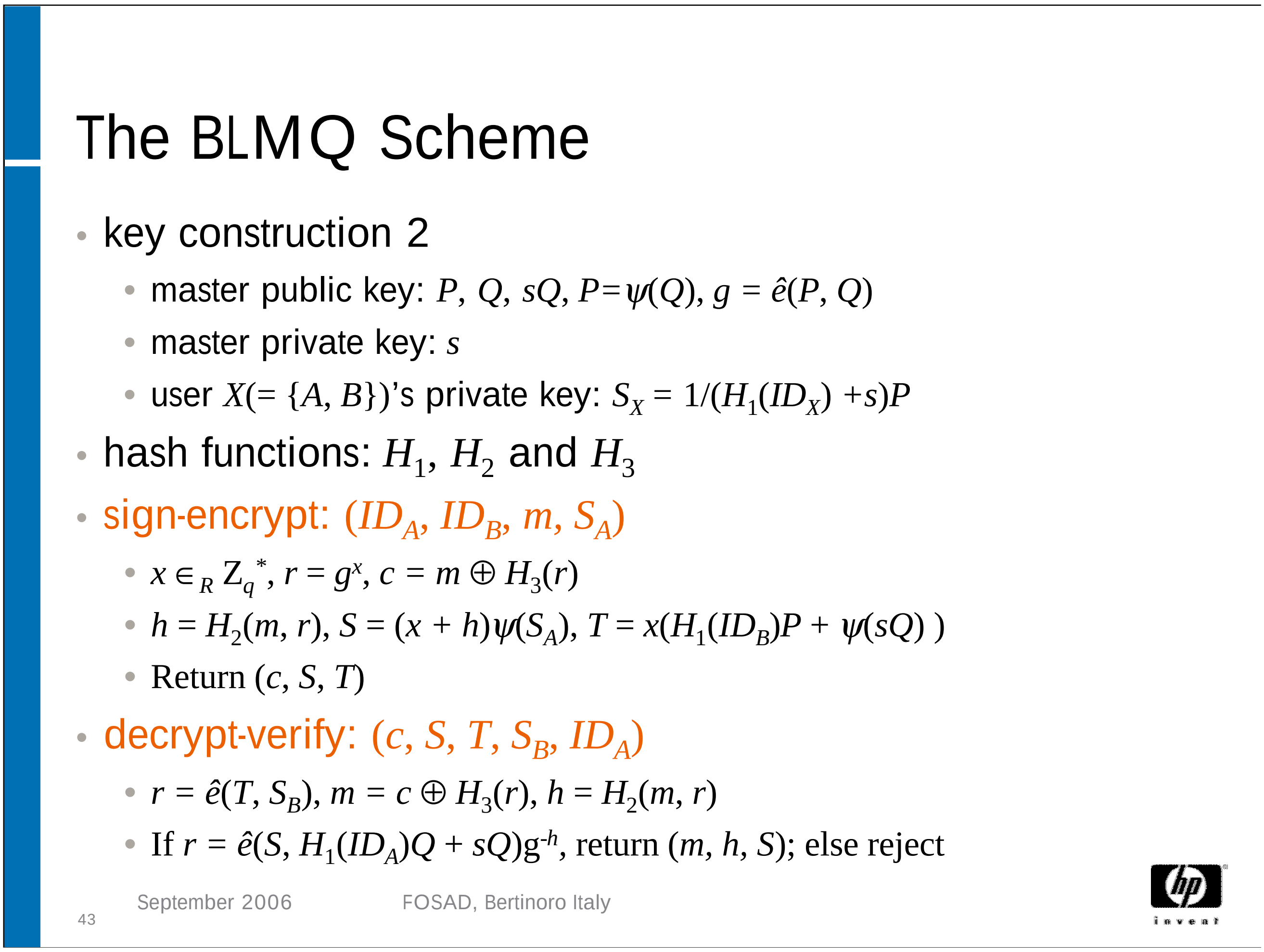
Identity-based signcryption from pairings



The Chen–Malone-Lee scheme

- key construction 1
  - master public key: P, sP; master private key: s
  - user $X(= \{A, B\})$'s private key: sQ_X where $Q_X = H_0(ID_X)$
- hash functions: H_0, H_1 and H_2
- sign-encrypt (ID_A, ID_B, m, sQ_A)
  - $r \in_R \mathbb{Z}_q^*$, $X = rQ_A$
  - $h_1 = H_1(X, m)$, $Z = (r + h_1)sQ_A$
  - $Q_B = H_0(ID_B)$, $w = \hat{e}(rsQ_A, Q_B)$, $y = H_2(w) \oplus (Z \| ID_A \| m)$
  - Return (X, y)
- decrypt-verify (X, y, sQ_B)
  - $w = \hat{e}(X, sQ_B)$, $(Z \| ID_A \| m) = y \oplus H_2(w)$,
  - $Q_A = H_0(ID_A)$, $h_1 = H_1(X, m)$,
  - If $\hat{e}(P, Z) = \hat{e}(sP, X + h_1 Q_A)$, returen "valid" and m; else return "invalid"

- L. Chen and J. Malone-Lee. Improved identity-based signcryption. In V. Serge (Ed.), Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC 2005), LNCS 3386, pp. 362-379, Springer-Verlag, 2005. See also: Cryptology ePrint Archive, Report 2004/114, 2004.
- The security of this scheme relies on the hardness of the BDH problem.



The BLMQ Scheme

- key construction 2
  - master public key: $P, Q, sQ, P{=}\psi(Q), g = \hat{e}(P, Q)$
  - master private key: s
  - user X(= $\{A, B\}$)'s private key: $S_X = 1/(H_1(ID_X) + s)P$
- hash functions: H_1, H_2 and H_3
- sign-encrypt: (ID_A, ID_B, m, S_A)
  - $x \in_R \mathrm{Z}_q^*$, $r = g^x$, $c = m \oplus H_3(r)$
  - $h = H_2(m, r)$, $S = (x + h)\psi(S_A)$, $T = x(H_1(ID_B)P + \psi(sQ))$
  - Return (c, S, T)
- decrypt-verify: (c, S, T, S_B, ID_A)
  - $r = \hat{e}(T, S_B)$, $m = c \oplus H_3(r)$, $h = H_2(m, r)$
  - If $r = \hat{e}(S, H_1(ID_A)Q + sQ)\mathrm{g}^{-h}$, return (m, h, S); else reject

- This scheme has been submitted to IEEE P1363.3 as
  - P. Barreto, B. Libert, N. McCullagh, J-J. Quisquater. Efficient and secure identity-based signatures and signcryption from bilinear maps, which is available at http://grouper.ieee.org/groups/1363/IBC/submissions/index.html.
- The original scheme was published as
  - P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In Asiacrypt'05, volume 3788 of LNCS, pages 515-532. Springer, 2005.
- The security of this scheme relies on the hardness of the k-BDHI problem.

Identity-based cryptography without key escrow

Three types of solutions

- Multiple key generation authorities
- Certificate-based encryption
- Certificateless encryption

Multiple trusted authorities – the CHSS scheme

$ID_{virtual} = f(ID_1, ID_2, \ldots, ID_m)$

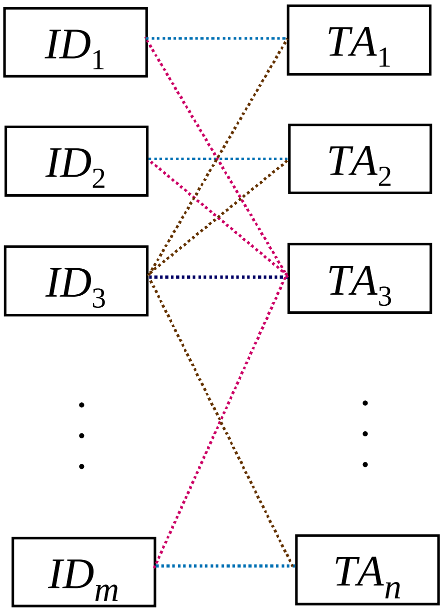
$TA_{virtual} = h(TA_1, TA_2, \ldots, TA_n)$

Example: multiple TAs (TA_i has s_iP) and a single identity (ID_3) using key construction 1

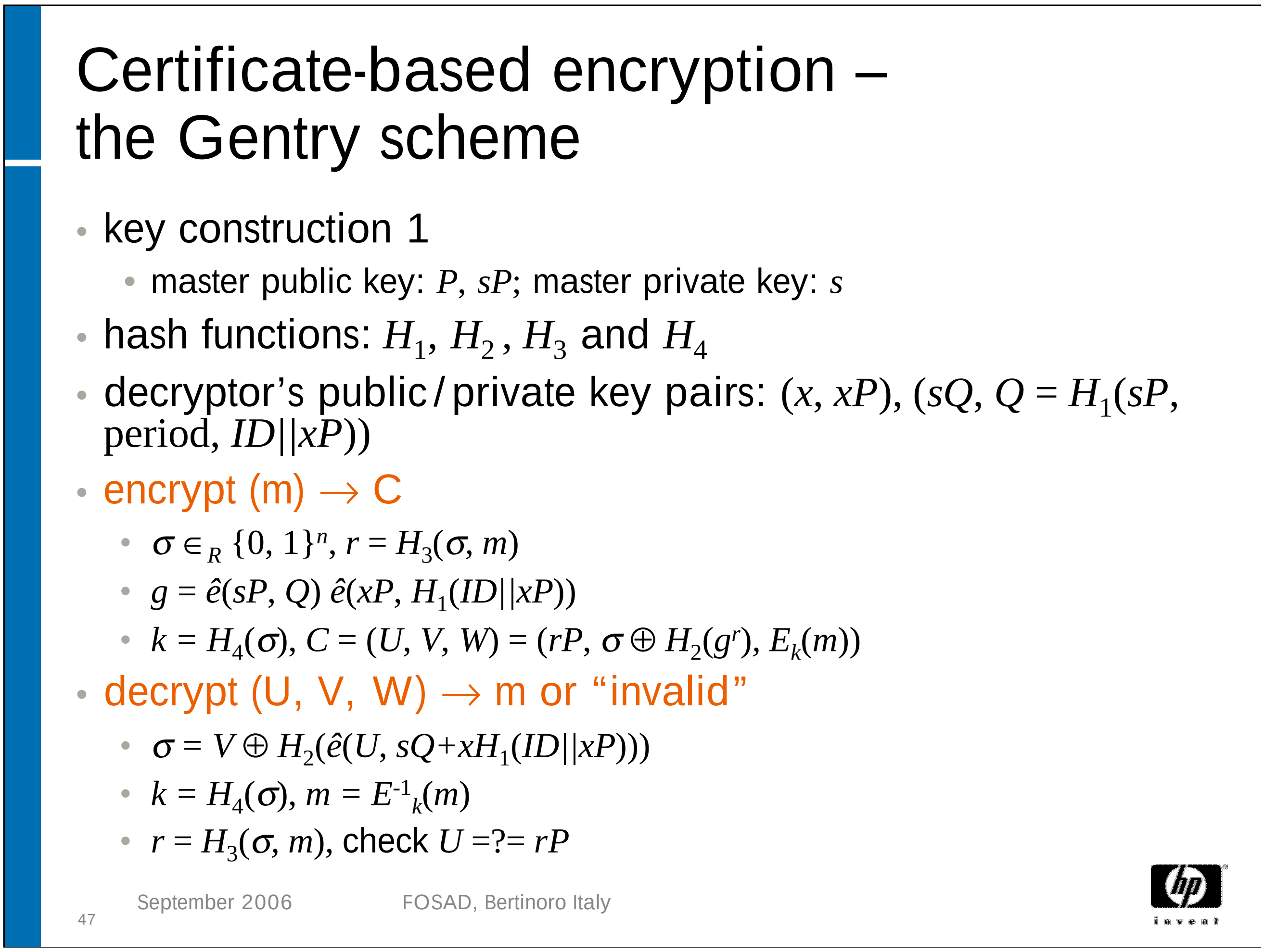
a virtual IB key for ID_3 is

$sQ = \Sigma_{\{i = 1, \ldots, n\}} b_i s_i H(ID_3)$

Where $b_i \in \{0, 1\}$, and H is a secure hash-function



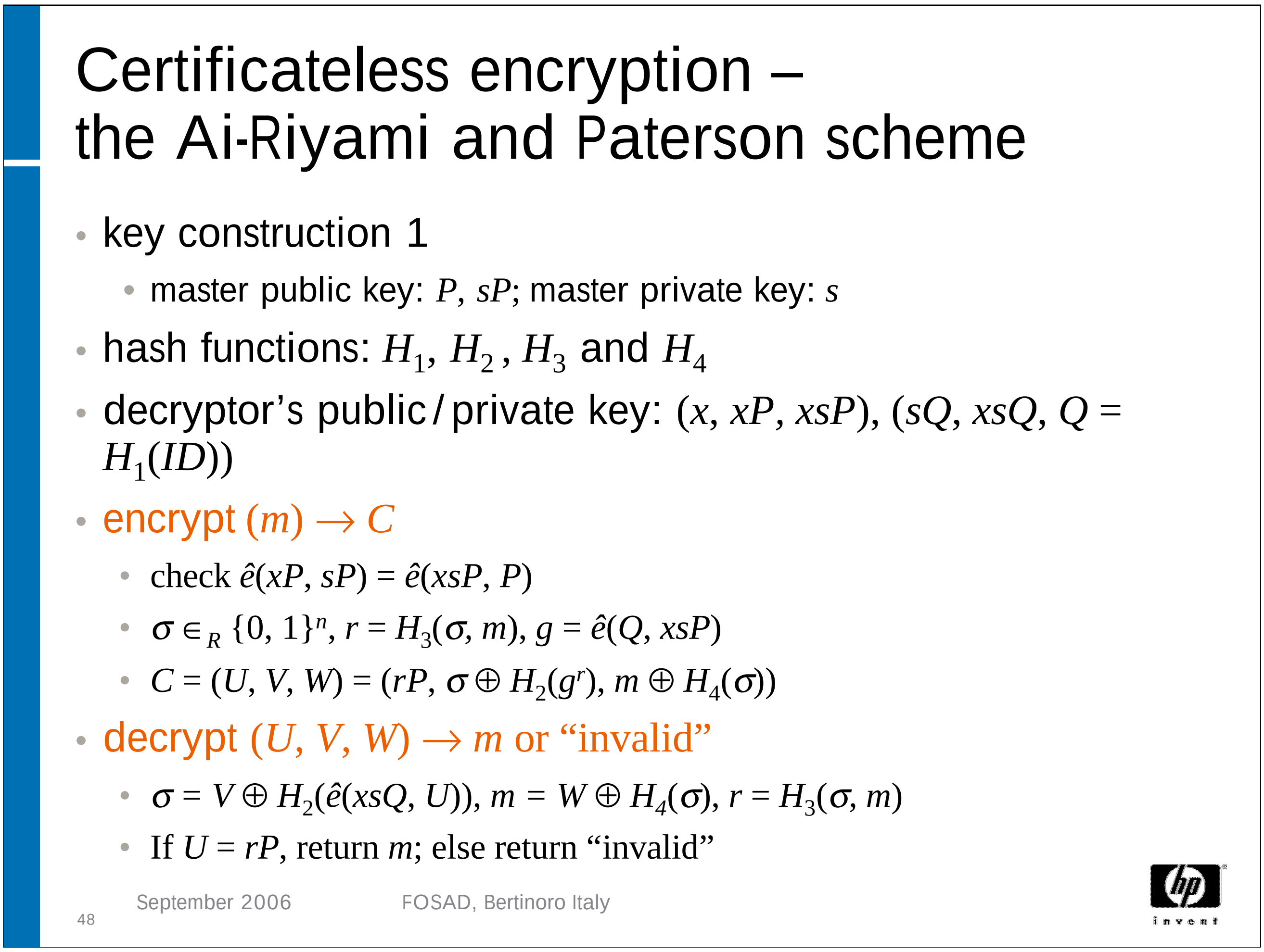
- L. Chen, K. Harrison, D. Soldera, and N.P. Smart. Applications of multiple trust authorities in pairing based cryptosystems. In G. Davida, Y. Frankel, O. Rees (Eds.), Proceedings of the International Conference on Infrastructure Security (InfraSec 2002), LNCS 2437, pp. 260-275, Springer-Verlag, 2002.



Certificate-based encryption – the Gentry scheme

- key construction 1
  - master public key: P, sP; master private key: s
- hash functions: H_1, H_2, H_3 and H_4
- decryptor's public/private key pairs: (x, xP), $(sQ, Q = H_1(sP, \text{period}, ID||xP))$
- encrypt (m) → C
  - $\sigma \in_R \{0, 1\}^n$, $r = H_3(\sigma, m)$
  - $g = \hat{e}(sP, Q)\, \hat{e}(xP, H_1(ID||xP))$
  - $k = H_4(\sigma)$, $C = (U, V, W) = (rP, \sigma \oplus H_2(g^r), E_k(m))$
- decrypt (U, V, W) → m or “invalid”
  - $\sigma = V \oplus H_2(\hat{e}(U, sQ+xH_1(ID||xP)))$
  - $k = H_4(\sigma)$, $m = E^{-1}{}_k(m)$
  - $r = H_3(\sigma, m)$, check U =?= rP

- C. Gentry. Certificate-Based Encryption and the Certificate Revocation Problem. In Advances in Cryptology - EUROCRYPT 2003, volume 2656 of LNCS, pages 272-293. Springer-Verlag, 2003. See also Cryptology ePrint Archive, 2003/183.

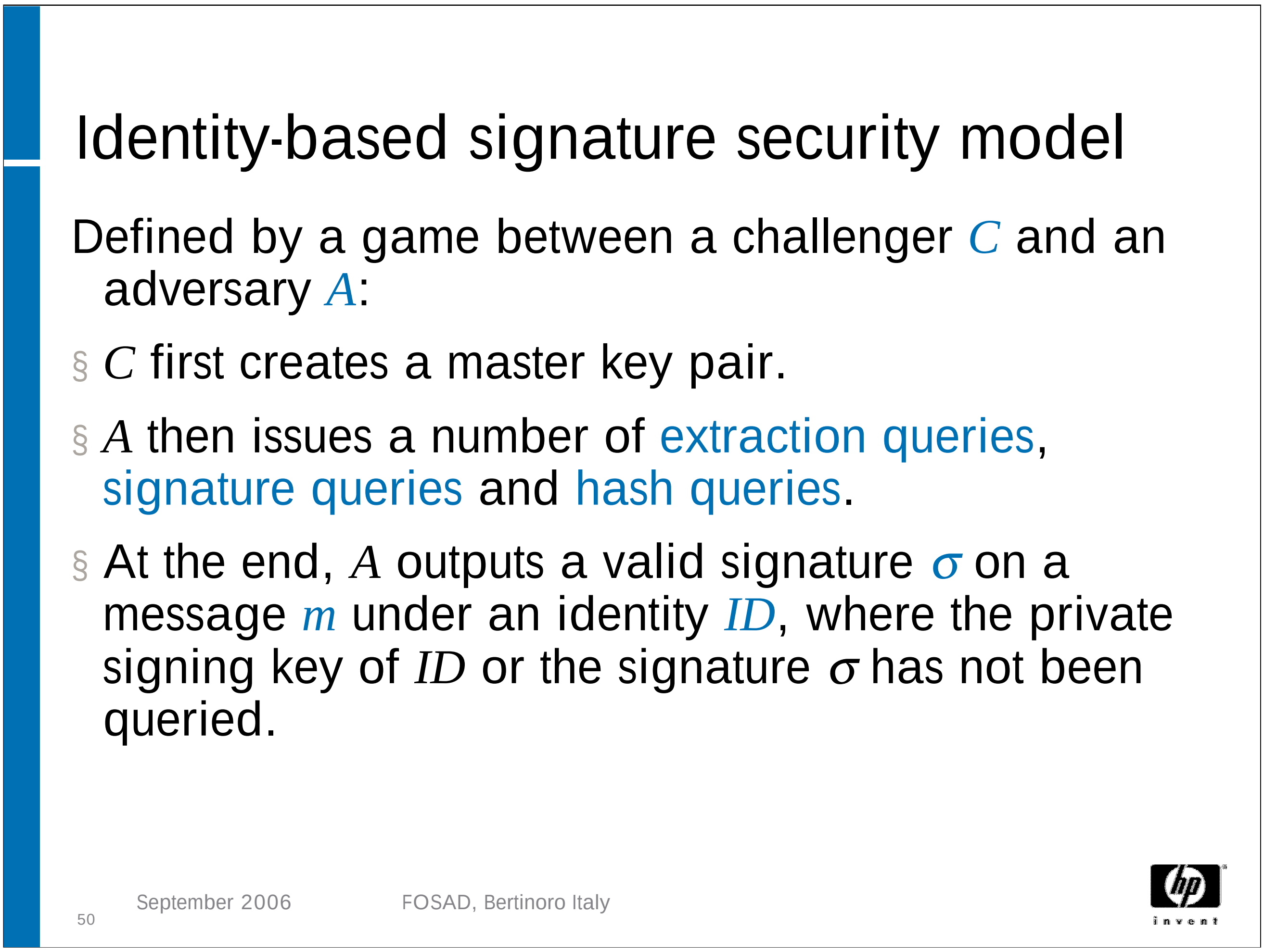


Certificateless encryption – the Ai-Riyami and Paterson scheme

- key construction 1
  - master public key: P, sP; master private key: s
- hash functions: H_1, H_2, H_3 and H_4
- decryptor's public/private key: (x, xP, xsP), $(sQ, xsQ, Q = H_1(ID))$
- encrypt $(m) \rightarrow C$
  - check $\hat{e}(xP, sP) = \hat{e}(xsP, P)$
  - $\sigma \in_R \{0, 1\}^n$, $r = H_3(\sigma, m)$, $g = \hat{e}(Q, xsP)$
  - $C = (U, V, W) = (rP, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma))$
- decrypt $(U, V, W) \rightarrow m$ or "invalid"
  - $\sigma = V \oplus H_2(\hat{e}(xsQ, U))$, $m = W \oplus H_4(\sigma)$, $r = H_3(\sigma, m)$
  - If $U = rP$, return m; else return "invalid"

- Al-Riyami, S.S. and Paterson, K.G., Certifficateless Public Key Cryptography. In Advances in Cryptology - ASIACRYPT 2003, LNCS vol. 2894 pp. 452-C473, Springer-verlag, 2003. See also Cryptology ePrint Archive, Report 2003/126.
- Al-Riyami, S.S. and Paterson, K.G.,CBE from CL-PKE: A Generic Construction and Efficient Schemes. PKC 2005, LNCS 3386 (2005) 398-415.

Security models and formal proof

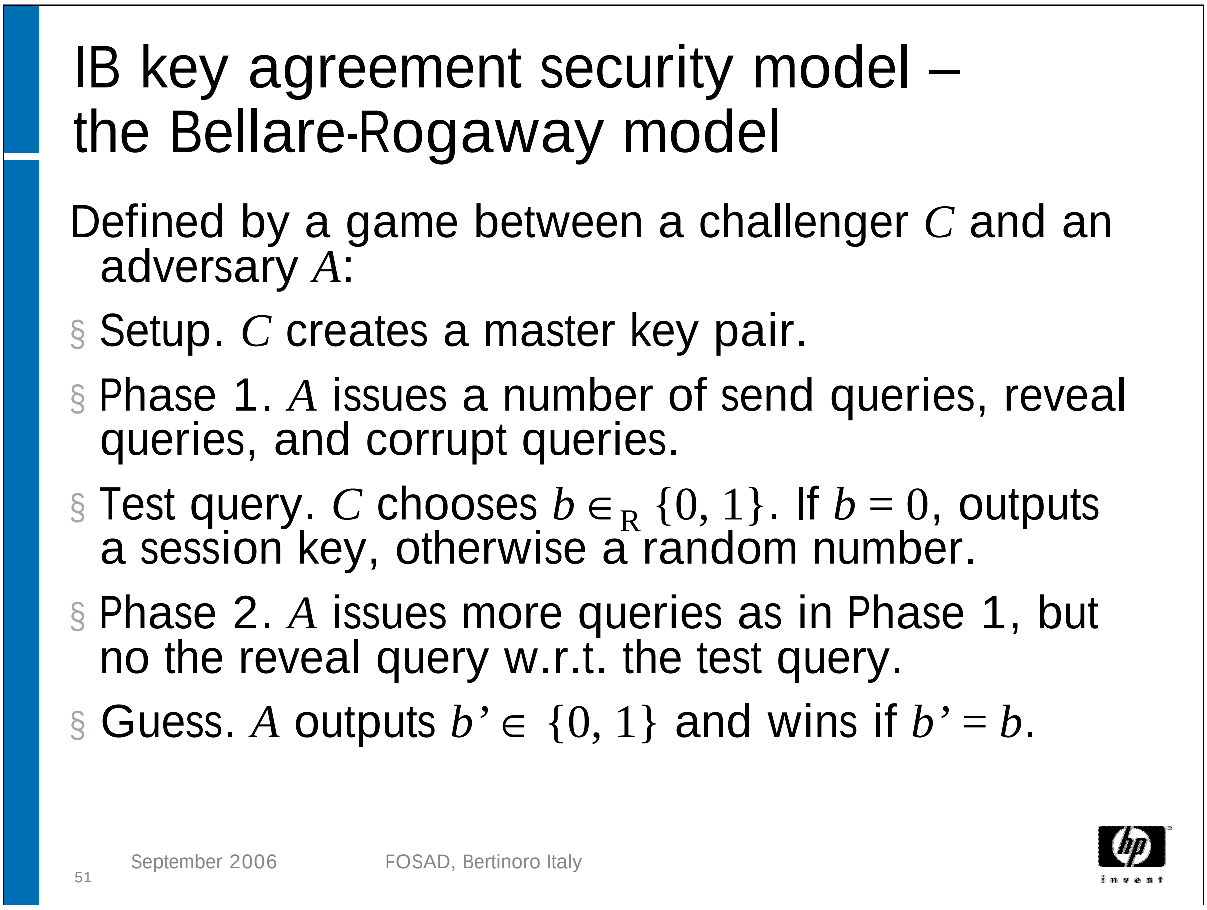


Identity-based signature security model

Defined by a game between a challenger C and an adversary A:

- C first creates a master key pair.
- A then issues a number of extraction queries, signature queries and hash queries.
- At the end, A outputs a valid signature σ on a message m under an identity ID, where the private signing key of ID or the signature σ has not been queried.

- The adversary A is assumed to be a (polynomial time) probabilistic Turing machine.
- The adversary's goal is to produce an existential forgery of a signature by a signer ID of its choice.
- To aid the adversary we allow it to make three types of queries:
- Hash query: for any given input, the challenger C will produce the corresponding hash value.
- Extraction query: for any given identity ID, the challenger C will produce the corresponding private signing key.
- Signature query: for any given message m and identity ID, the challenger C will produce a signature from the user with identity ID on the message m.
- the output of the adversary A should not be a signature such that the secret key of the corresponding identity or the signature itself have been queried.
- If the adversary can output a signature without the extraction query to the signing key and the signature query to the signed message, he wins the game.
- The challenger's goal is to solve a hard problem, for example the BDH problem.
- The basic idea of security proofs is to show if the adversary can break a signature scheme by forging a signature, then the challenger can make use of the adversary to solve the specified hard problem.

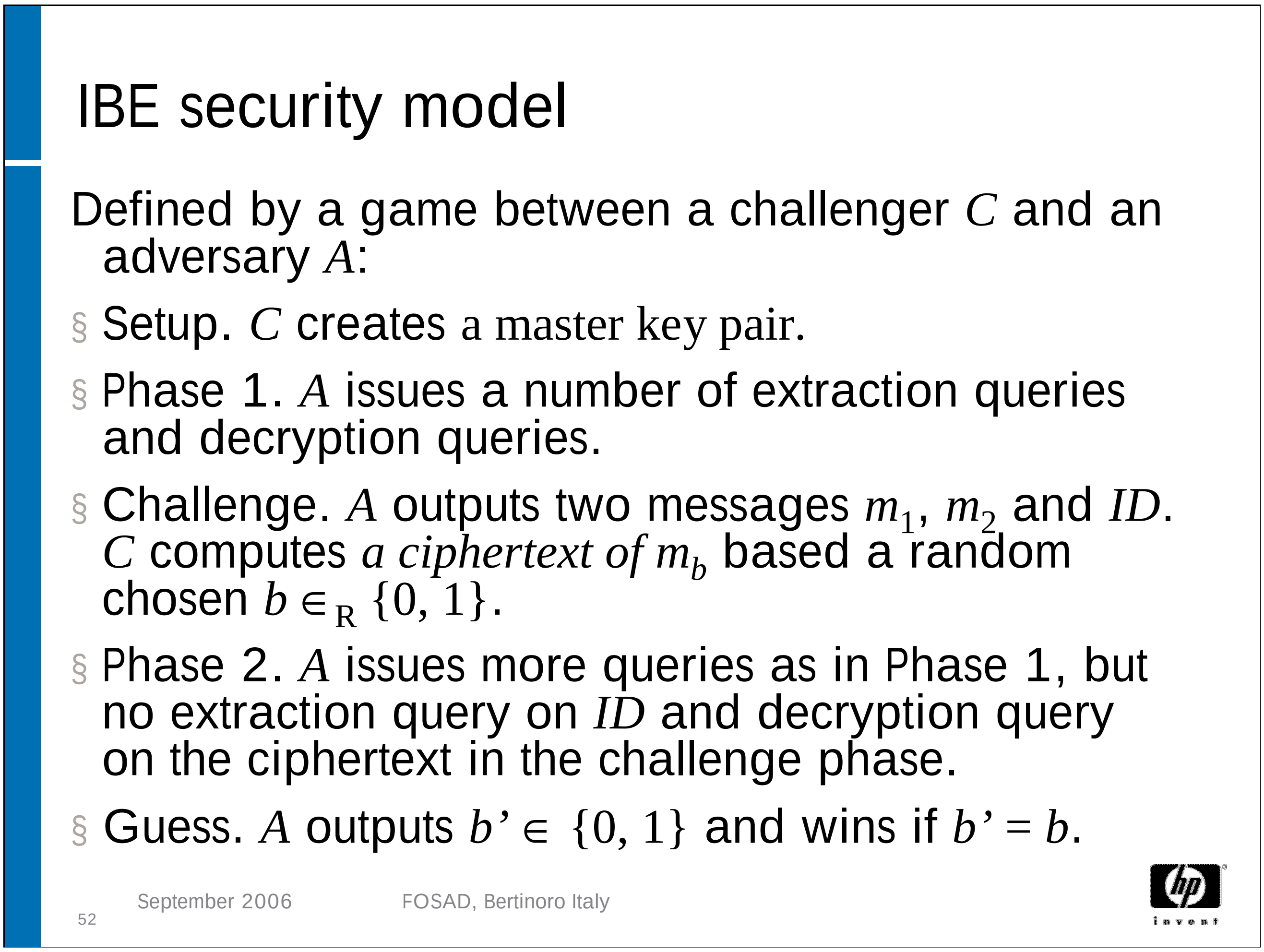


IB key agreement security model – the Bellare-Rogaway model

Defined by a game between a challenger C and an adversary A:

- Setup. C creates a master key pair.
- Phase 1. A issues a number of send queries, reveal queries, and corrupt queries.
- Test query. C chooses $b \in_R \{0, 1\}$. If $b = 0$, outputs a session key, otherwise a random number.
- Phase 2. A issues more queries as in Phase 1, but no the reveal query w.r.t. the test query.
- Guess. A outputs $b' \in \{0, 1\}$ and wins if $b' = b$.

- Send query. Upon receiving a send query with a message x, an oracle executes the protocol and responds with an outgoing message m or a decision to indicate accepting or rejecting the session. If the oracle does not exist, it will be created.
- Reveal query. Upon receiving a reveal query to an oracle, if the oracle has not accepted, it returns “not accepted”; otherwise, it reveals the session key.
- Corrupt query. Upon receiving a corrupt query to a party, the party responds with its private key.
- Test query. The adversary can only choose a fresh oracle to make the test query. The definition of a fresh oracle is various, dependent on what security property one wants to proof.
- The general concept and technology of this model can be found at
  - M. Bellare, D. Pointcheval and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Advances in Cryptology – Eurocrypt 2000, Springer-Verlag LNCS 1807, 139-155, 2000.
  - M. Bellare and P. Rogaway. Entity authentication and key distribution. In Advances in Cryptology – Crypto '93, Springer-Verlag LNCS 773, 232-249, 1993.
  - S. Blake-Wilson, D. Johnson and A. Menezes. Key agreement protocols and their security analysis. In Cryptography and Coding, Springer-Verlag LNCS 1355, 30-45, 1997.
- The details of the security analysis of identity-based key agreement protocols can be found in
  - C. Kudla and K. Paterson. Modular security proofs for key agreement protocols. In Advances in Cryptology – Asiacrypt 2005, Springer-Verlag LNCS 3788, 549-565, 2005.
  - L. Chen, Z. Cheng and N. Smart. Identity-based key agreement protocols from pairings. Cryptology ePrint Archive, Report 2006/199, 2006.



IBE security model

Defined by a game between a challenger *C* and an adversary *A*:

- Setup. *C* creates a master key pair.
- Phase 1. *A* issues a number of extraction queries and decryption queries.
- Challenge. *A* outputs two messages m_1, m_2 and *ID*. *C* computes *a ciphertext of* m_b based a random chosen $b \in_R \{0, 1\}$.
- Phase 2. *A* issues more queries as in Phase 1, but no extraction query on *ID* and decryption query on the ciphertext in the challenge phase.
- Guess. *A* outputs $b' \in \{0, 1\}$ and wins if $b' = b$.

This security model was proposed at

- D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In Proceedings of Advances in Cryptology - Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

- Extraction query: Upon receiving an extraction query with an identity ID, the challenger responds with a private key corresponding to the public key ID.
- Decryption query: Upon receiving a decryption query with an identity and a ciphertext, the challenger extracts the private key corresponding to the identity, decrypts the ciphertext, and then returns the resulting plaintext.
- The constraint in the challenge phase is that the identity did not appear in any private key extraction query in Phase 1.
- The constraint in Phase 2 is that the adversary cannot ask any private key extraction query to the challenger ID and any decryption query to the ciphertext, which was given in the challenge phase.

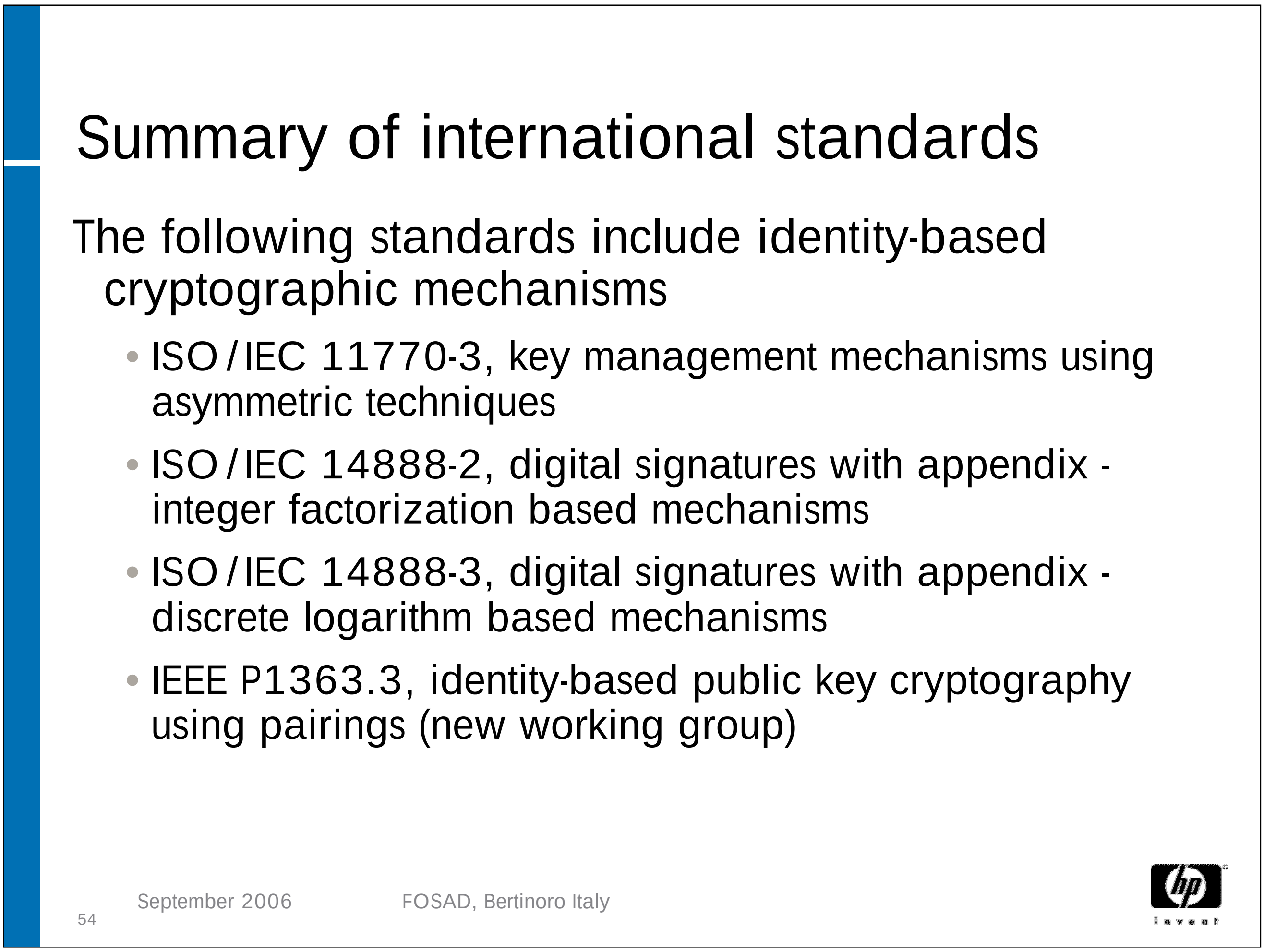
Identity-based Signcryption security notions

- Ciphertext authentication
- Message confidentiality
- Signature non-repudiation
- Ciphertext anonymity

The detailed definition of these security notions can be found at

- L. Chen and J. Malone-Lee. Improved identity-based signcryption. In V. Serge (Ed.), Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC 2005), LNCS 3386, pp. 362-379, Springer-Verlag, 2005. See also: Cryptology ePrint Archive, Report 2004/114, 2004.

- Ciphertext authentication: guarantee to the recipient of a signed and encrypted message that the message was encrypted by the same person who signed it.
- Message confidentiality: guarantee that only the selected recipient is able to decrypt the message.
- Signature non-repudiation: prevent the sender of a signcrypted message from disavowing its signature.
- Ciphertext anonymity: ciphertexts contain no third-party extractable information that helps to identify the sender of the ciphertext or the intended recipient.

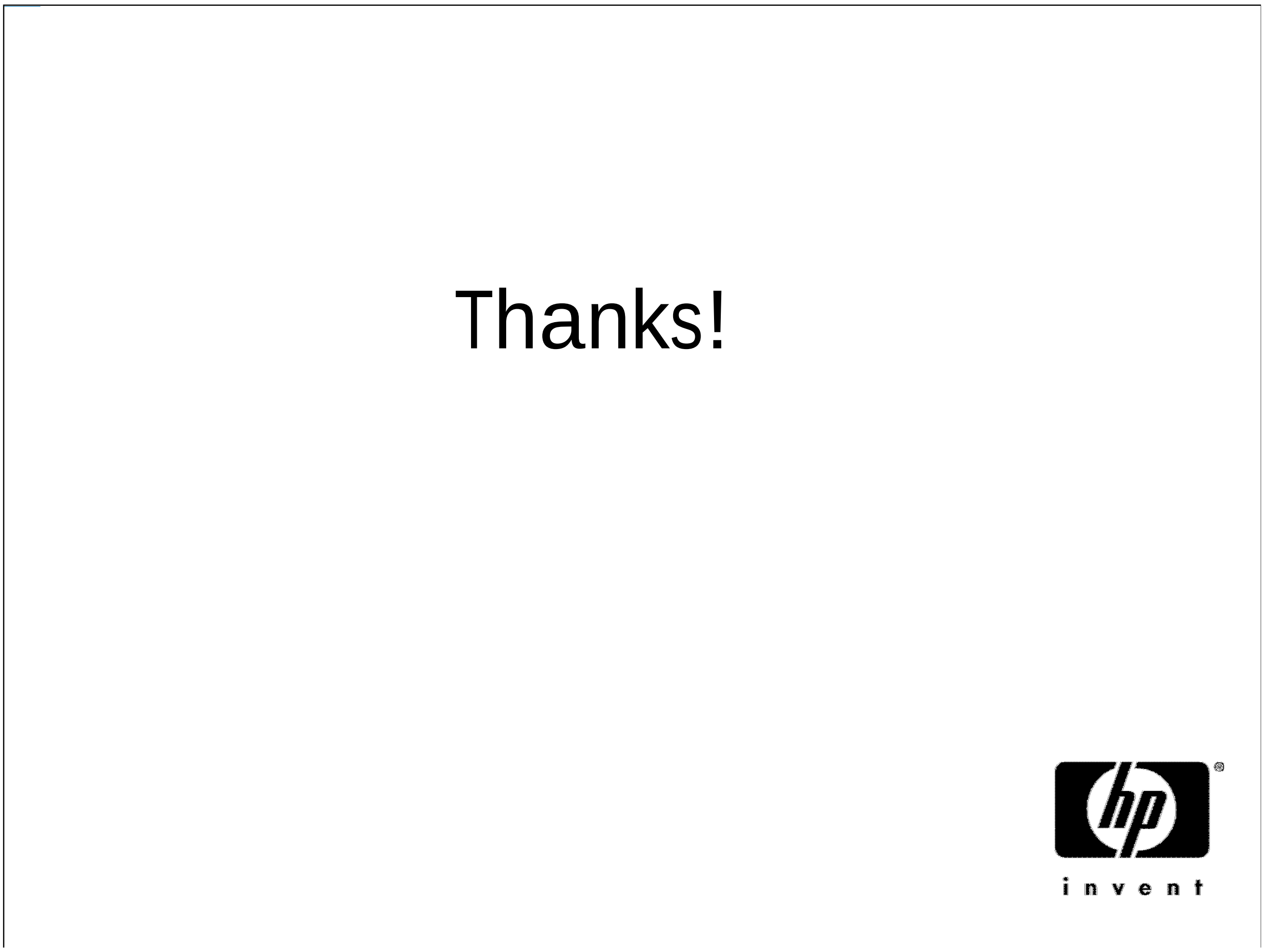


Summary of international standards

The following standards include identity-based cryptographic mechanisms

- ISO/IEC 11770-3, key management mechanisms using asymmetric techniques
- ISO/IEC 14888-2, digital signatures with appendix - integer factorization based mechanisms
- ISO/IEC 14888-3, digital signatures with appendix - discrete logarithm based mechanisms
- IEEE P1363.3, identity-based public key cryptography using pairings (new working group)

- The following IEEE P1363.3 submissions are available at http://grouper.ieee.org/groups/1363/IBC/submissions/index.html.
  - The BF Identity-based encryption system (.pdf), X. Boyen. Submitted 2006-08-14.
  - The BB1 Identity-based cryptosystem: A standard for Encryption and Key Encapsulation (.pdf), X. Boyen. Submitted 2006-08-14.
  - IEEE P1363.3 submission: Pairing-Friendly Elliptic Curves of Prime Order with Embedding Degree 12 (.pdf), P. Barreto, M. Naehrig. Submitted 2006-08-14.
  - Efficient and secure identity-based signatures and signcryption from bilinear maps (.pdf), P. Barreto, B. Libert, N. McCullagh, J-J. Quisquater. Submitted 2006-08-14.
  - Proposal for P1363.3: HIBE, HIBS, IBKIE, NTT DoCoMo. presentation (.pdf). Submitted 2006-08-14.
  - Proposal for P1363.3: Proxy Re-encryption, NTT Data. presentation (.pdf). Submitted 2006-08-14.
  - Identity-based Key Agreement Protocols from Pairings (.pdf), L. Chen, Z. Cheng, N. P. Smart. Submitted 2006-07-03.
  - SK-KEM: An Identity-Based KEM (.pdf), M. Barbosa, L. Chen, Z. Cheng, M. Chimley, A. Dent, P. Farshim, K. Harrison, J. Malone-Lee, N. P. Smart, F Vercauteren. Submitted 2006-06-07.
  - Implicitly Authenticated ID-Based Key Agreement Protocol (.pdf), Yongge Wang. submitted 2006-03-22.



Thanks!

- This lecture is attempted to introduce the basic concept and technology of identity-based cryptography.
- Because of the time limitation, it is impossible to cover every detail and every interesting identity-based cryptographic mechanism.
- If you are really interested in pairing based cryptography, please find a very good collection at Barreto's pairing-based crypto lounge: http://paginas.terra.com.br/informatica/paulobarreto/pblounge.html.