T-79.5502 Advanced Course in Cryptology

March 28th, 2006

ID-based authentication frameworks and primitives

Mikko Kiviharju
Helsinki University of Technology
mkivihar@cc.hut.fi

Overview

- Motivation
- History and introduction of IB schemes
- Mathematical basis
- Boneh-Franklin IB cryptosystem
- IB-PKI vs. conventional PKI
- Conclusion

Agenda

- Motivation
- History and introduction of IB schemes
- Mathematical basis
- Boneh-Franklin IB cryptosystem
- IB-PKI vs. conventional PKI
- Conclusion

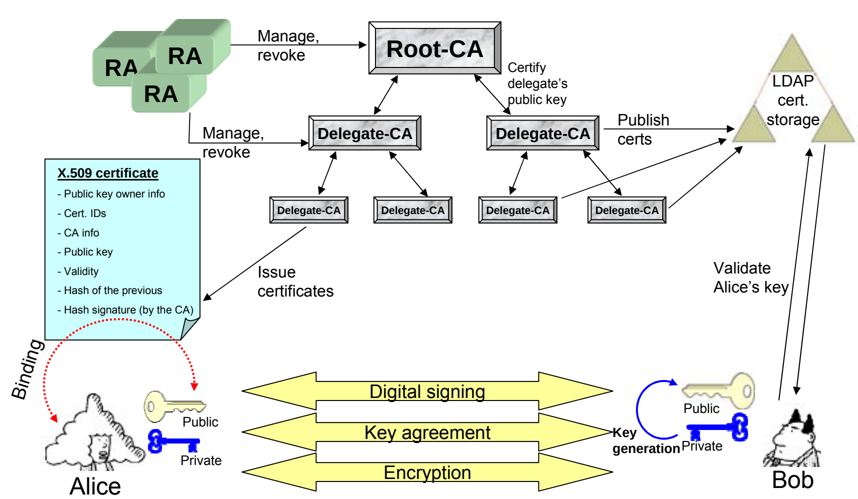
PK authentication infrastructures

- Main functions:
  - signature schemes
  - key agreement
- Functions usually constructed with asymmetric encryption primitives
  - Not a requirement, though
- Main goal: minimize the need for and exchange of secret information

Directory-based PKI

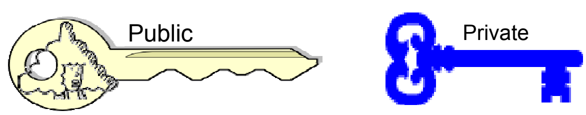
- public_key = **F**(*private_key*)
- Problems: binding the public information to actual identity (due to restrictions in forming the asymmetric key pairs)
- Current PKI solution: certificates and CAs → heavy infrastructure and administration costs

Current PKI (e.g. X.509 & LDAP)

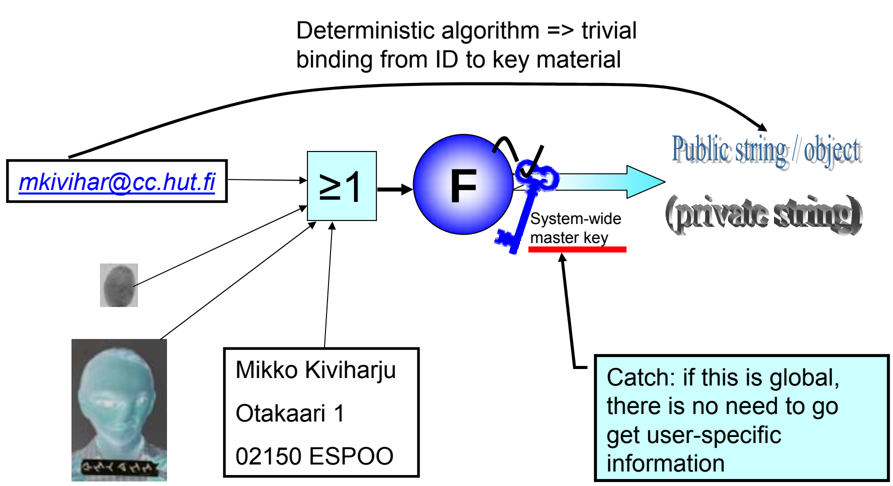


Informative public keys?

- What if the key generation is reversed?
- *private_key* = **F**(public_key)
- No secrecy here…
- *private_key* = **F**(*master_key*, public_key)
- Public key has freedom of choice
- Public key ?= user's identity



Identity as the public key



Agenda

- Motivation
- History and introduction of IB schemes
- Mathematical basis
- Boneh-Franklin IB cryptosystem
- IB-PKI vs. conventional PKI
- Conclusion

History

- Shamir introduced the concept in 1984
  - An RSA-based signature scheme
  - No key agreement, nor encryption
- Girault's scheme in 1991
  - RSA-based PKI functionality without actual encryption
  - Not exactly ID-based (public key depends on the secret key as well)
- Mathematical basis
  - Special elliptic curve classes for ECDLP in 1983 by Menezes, Okamoto and Vanstone
- ID-based cryptosystems based on elliptic curves
  - Key agreement schemes by Sakai, Ohgishi & Kasahara (SOK) and Joux in 2000
  - First fully fledged IB-PKI by Boneh and Franklin 2001

Properties of IB-PK-AFs (*)

(*) Identity-Based Public Key Authentication Framework

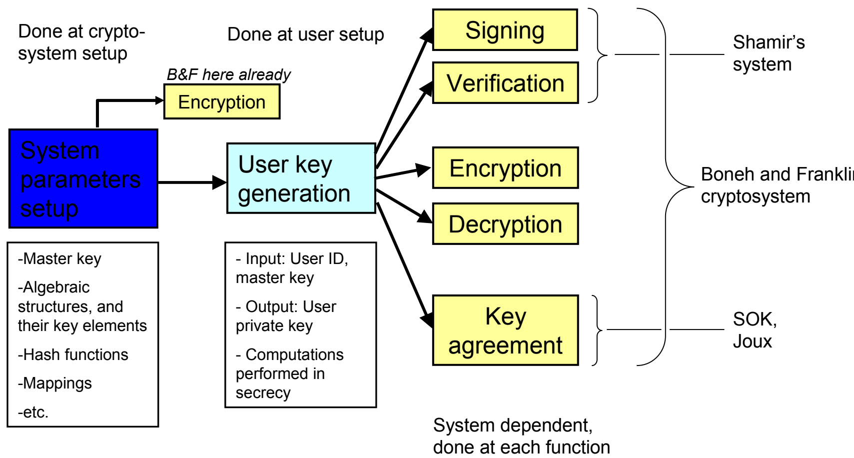
- Trusted Authority (TA) handles key generation for everyone
  - Highly centralized trust element (TA can decrypt everything)
  - Keygen essentially an authentication service (similar to certificate applying in PKI)
- No key channel needed
- Binding of identity and public-key based on trust in
  - The generation function
  - Uncompromised TA master key
  - Sound TA authentication service
- Non-interactivity

Non-interactivity in IB-PK-AFs

- No need to contact directories
  - Verification of a signature
  - Key agreement
- No need to establish key channels
  - Authenticated key establishment
  - (Key) data origin authentication
- … assuming TA is honest, of course

Functions in IB-PK-AFs (*)

(*) Identity-Based Public Key Authentication Framework



Agenda

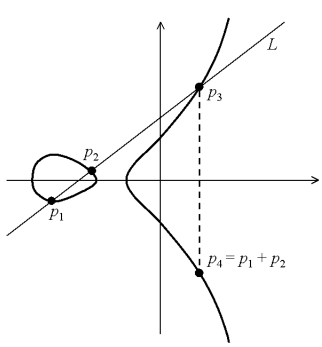
- Motivation
- History and introduction of IB schemes
- Mathematical basis
- Boneh-Franklin IB cryptosystem
- IB-PKI vs. conventional PKI
- Conclusion

Elliptic curves (1/4)

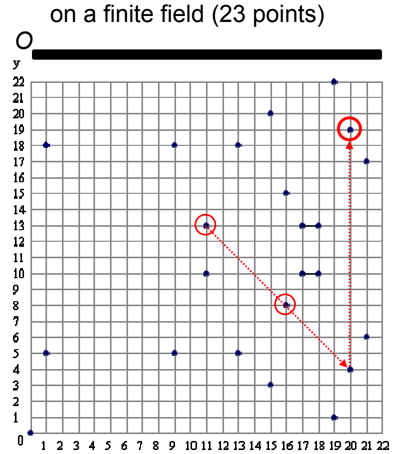
- Sets of pairs of field elements (points) satisfying a third degree polynomial $y^2 \left[+xy\right] = x^3 + ax + b$
- Any field is ok, in EC cryptography finite fields of prime a power of a small prime order are used
- An additive operation is defined on the points of a certain EC => a group is formed.
- Repeated additions of a fixed point equal exponentiation
  - Normal finite field methods for extracting a discrete logarithm do not work due to lack of ”multiplication” operation between group elements

Elliptic curves (2/4)

Elliptic curve group defined on real numbers, with addition procedure



Elliptic curve group defined on a finite field (23 points)



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

Elliptic curves (3/4)

- Usage in PKI based on ECDLP
- Encrypting usually done with extracting (hashing) an element from the EC group
- ECC -> ”real” PKI (but still dir-based…)
- Selecting the underlying field order, from:
  - $\left|E\left(\mathrm{F}_q\right)\right| = q+1+t = O(q), -2\sqrt{q} \le t \le 2\sqrt{q}$
  - Best known ECDLP runs in time $O\left(\sqrt{\left|E\left(\mathrm{F}_q\right)\right|}\right) \approx O\left(q^{\frac{1}{2}}\right)$ (cf. DLP of finite fields $e^{c\log^{1/3} q(\log\log q)^{2/3}}$)
  - Key size = 2 * security parameter

Elliptic curves (4/4)

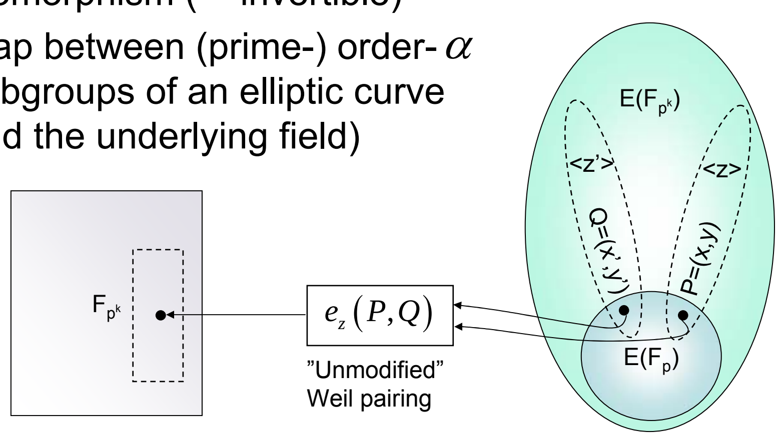
- For a prime power $q=p^m$, the EC group is described by a tuple (q,a,b,G,n,h), where
  - $G \in E\left(F_q\right)$ is the generator of a subgroup of prime order n in the EC group, and $\left|\langle G\rangle\right| = n, n \mid \left|E\left(\mathrm{F}_q\right)\right|$
  - $h = \left|E\left(\mathrm{F}_q\right)\right| / n$ cofactor, preferably small (=1) integer
- MOV-attack resistance requires that n does <u>not</u> divide $q^B - 1$ for all small B (<20, or small enough such that the subexp DL is hard in the underlying field)
- Fortunately, a subset of these weak curves have other applications

Weak elliptic curves

- ECs, for which the underlying field characteristic *p* divides the Frobenius trace *t*, are called supersingular (a subset of the type of elliptic curves susceptible to MOV-attacks)
- Weakness: an efficient mapping from the EC group to the underlying field with a *guaranteed small* extension (which has subexponential solvability for DL)

Weil pairing for ECs (1/2)

- Isomorphism (= invertible)
- Map between (prime-) order-α subgroups of an elliptic curve and the underlying field)



Weil pairing for ECs (2/2)

- Fix an order-α generator $z \in E\left(\mathrm{F}_{p^k}\right)$ such that
  - $P \in \langle z \rangle$ or $Q \in \langle z \rangle$, but not both
- Then the Weil pairing is defined as

$$\left(e_z(P,Q) = \sqrt[\alpha]{1_{\mathrm{F}_{p^k}}}\right) \wedge \left(e_z(P,Q) \neq 1_{\mathrm{F}_{p^k}}\right) \Leftrightarrow$$

$$\left(\mathrm{ord}(P) = \mathrm{ord}(Q) = \alpha\right) \wedge \left(\forall (a,b \in \mathbf{Z}) : P \neq aQ \wedge Q \neq bP\right)$$

- The supersingular property condition assures that $E(\mathrm{F}_{p^k})$ is non-cyclic, and that there exists a non-empty order-α subgroup for P, the elements of which are not mapped to unity

Weil pairing properties

Notation: $(G_1,+)$, $(G_2,*)$ groups under Weil pairing
(G_1 is the EC subgroup and G_2 the underlying field ext. subgroup)

- Identity: $\forall (P \in G_1) : e_z(P,P) = 1_{G_2}$
- Bilinearity: $\forall (P,Q \in G_1) :, e_z(P+R,Q) = e_z(P,Q)e_z(R,Q)$

$$e_z(P,Q+R) = e_z(P,Q)e_z(P,R)$$

- Non-degeneracy: $\forall (P \in G_1, P \neq O) : e_z(P,z) \neq 1_{G_2} \neq e_z(z,P)$
  - (P and z must be independent according to the mapping definition)
- Efficiency: mapping is practically efficiently computable

Weil pairing: MOV-reduction

- According to Menezes-Okamoto-Vanstone (-83)
- Given $P, nP \in E(\mathrm{F}_p)$
- Apply Weil pairing; according to bilinearity property: $\xi = e_z(P, z)$

$$\eta = e_z(nP, z) = e_z(P, z)^n = \xi^n$$

- … which is a DL problem in a finite field $\mathrm{F}_{p^k}, k \leq 6$
- … with a running time of $O\left(e^{ck \log^{1/3} p (\log(k \log p))^{2/3}}\right)$
- (cf. $O(e^{0,5p})$ for ECDLP)

Modified Weil pairing

- What if P=aQ? (This is the case with e.g. Boneh-Franklin cryptosystem)
  $e_z(P, Q) = e_z(aQ, Q) = e_z(Q, Q)^a = 1_{G_2}^a$
- Apply a distortion function (Verheul, 2001)
- Modified Weil pairing, defined as
  $P, Q \in G_1 : e(P, Q) = e_z(P, \Phi(Q))$ where $\Phi : E(\mathrm{F}_{p^k}) \rightarrow E(\mathrm{F}_{p^k})$ is a ”distortion function” mapping a point to a linearly independent point
- Properties
  - Symmetry
  - Bilinearity

Modified Weil pairing and DDH

- Decisional Diffie-Hellman: given $p, p^a, p^b, p^c \in G$ decide if $ab \equiv c \pmod{|G|}$
- In a general group this seems as hard as DL
- In a supersingular EC group, when given $P, aP, bP, cP \in G_1; a, b, c \in \mathbf{Z}$
- Calculate $\eta = e(P, cP) = e(P, P)^c$ and $\xi = e(aP, bP) = e(P, P)^{ab}$
- Now $ab \equiv c \pmod{|G_1|} \Leftrightarrow \xi = \eta$
- DDH is easy in supersingular EC groups!

Bilinearity "extracts" the discrete logarithm

Agenda

- Motivation
- History and introduction of IB schemes
- Mathematical basis
- Boneh-Franklin IB cryptosystem
- IB-PKI vs. conventional PKI
- Conclusion

Boneh-Franklin IB cryptosystem

- First practical IB cryptosystem (2001)
- Provides actual asymmetric encryption in IB framework
- Provably secure (although not the algorithm 13.2) in IND-CCA2 (indistinguishable adaptive chosen-ciphertext in RO model applied in IB framework – conventional PKI is insecure in CCA already)
- Uses bilinear maps (one instantiation is Weil pairings in supersingular EC groups)
- Relies on the bilinearity property of the Weil pairings (= Bilinear DH problem(*))

$$(*)\langle P, aP, bP, cP\rangle \xrightarrow{compute} e(P,P)^{abc}$$

Boneh-Franklin: `FullIdent`

- Mao's presentation of BF system is not IND-CCA2 – secure (BF's `BasicIdent` is malleable – fails NM-CPA: Malice can modify the ciphertext without knowing the secret r, and NM-CPA is a weaker notion than CCA2-security)
- Extra hash functions and random variables are needed for this purpose
- We present here the IND-CCA2-secure `FullIdent`-scheme

BF: System parameters setup (1/2)

- Performed by TA
- Group descriptions $(G_1, +); (G_2, *)$
  - Bilinear map $e : (G_1, +) \times (G_1, +) \rightarrow (G_2, *)$
  - Generator: $P \in G_1$
- Global key material
  - Master key: $s \in_U \mathbf{Z}_p; (p = |G_1| = |G_2|)$
  - Public key: $P_{pub} = sP$

BF: System parameters setup (2/2)

- Hash functions
  - Identity hasher $H_1 : \{0,1\}^* \rightarrow G_1$
  - Public key hasher $H_2 : G_2 \rightarrow \{0,1\}^n$, *n*=log size of message and cipher space
  - Session key / message integrator
    $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbf{Z}_q^*; q = \mathrm{ord}(P)$
  - Session key hasher $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$
- Publish $\mathrm{Desc}\langle G_1, G_2, e, H_1, H_2, H_3, H_4, n, P, P_{pub} \rangle$

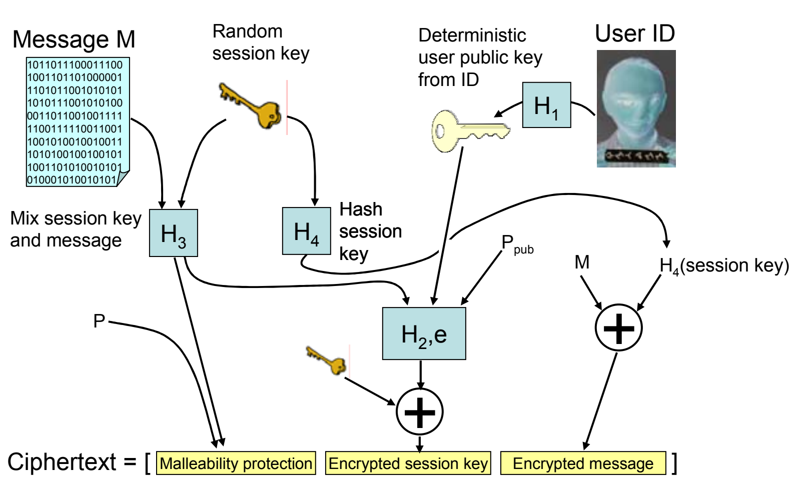
BF: User key generation

- Performed by TA to a user after thorough verification of the user’s identity
- Key material:
  - Public key, deterministically from the ID string:

$$Q_{ID} = H_1(ID) \in G_1$$

  - Private key: $d_{ID} = sQ_{ID}$
- Identity hash need not be straight to G_1, as shown by B&F in their paper: rather a conventional hash followed by an ”admissible encoding function” (simple elliptic curve point calculator)

BF: Encryption, idea



BF: Encryption, operation

- Compute the recipient's $Q_{ID} = H_1(ID) \in G_1$
- Choose a random session key $\sigma \in \{0,1\}^n$
- Set malleability protection $r = H_3(\sigma, M)$
- Calculate ciphertext *C* = <*U,V,W*> =

$$\left\langle rP, \sigma \oplus H_2\left(e\left(Q_{ID}, rP_{pub}\right)\right), M \oplus H_4(\sigma)\right\rangle$$

BF: Decryption, operation

- Compute the session key: $\sigma = V \oplus H_2\left(e\left(d_{ID}, U\right)\right)$
- Decrypt the message: $M = W \oplus H_4(\sigma)$
- Check message integrity: calculate $r = H_3(\sigma, M)$
  - If *U* = *rP*, then message is intact
- Accept message *M*, iff intact

BF: Decryption, correctness

- Message is hidden XORing with an OTP → opened correctly, if session key opened correctly

$$M = W \oplus H_4(\sigma)$$

- For the session key: result of H_2 must equal that of H_2 after encryption

$$H_{2D} = H_2\left(e\left(d_{ID}, U\right)\right) = H_2\left(e\left(sQ_{ID}, rP\right)\right) =$$
$$H_2\left(e\left(Q_{ID}, rP\right)^s\right) = H_2\left(e\left(Q_{ID}, rsP\right)\right) =$$
$$H_2\left(e\left(Q_{ID}, rP_{pub}\right)\right) = H_{2E}$$

BF: Instantiation with ECs (1/2)

- Needed
  - Group descriptions
  - Bilinear map
  - Hash functions
- With a k-bit prime p and another prime q, such that $p \equiv 2 \pmod 3 \wedge p = 6q - 1$
  - G_1 is an EC $y^2 = x^3 + 1$ over F_p
  - G_2 is F_{p^2}
- Use a distortion map $\Phi(x, y) = (\zeta x, y), \zeta \neq 1_{\mathrm{F}_{p^2}}, \zeta^3 - 1 \equiv 0 \pmod p$ and a Weil pairing *e'* defined with the help of divisors of functions over EC groups

BF: Instantiation with ECs (2/2)

- Bilinear map e is now $e(P,Q) = e'\left(P, \Phi(Q)\right)$
- Hash functions (cryptographically strong):
  - $H_2 - H_4$ as described (e.g. Whirlpool, SHA-256)
  - $H_1^* : \{0,1\}^* \to \mathrm{F}_p$ as a ”normal” hash function (above)
- Define function $\texttt{MapToPoint}: \mathrm{F}_p \to G_1$

$$\texttt{MapToPoint}(y_0) = \begin{pmatrix} 6\left(y_0^2 - 1\right)^{(2p-1)/3} \\ 6y_0 \end{pmatrix}$$

- Now the first hash is $H_1(ID) = \texttt{MapToPoint}\left(H_1^*(ID)\right)$

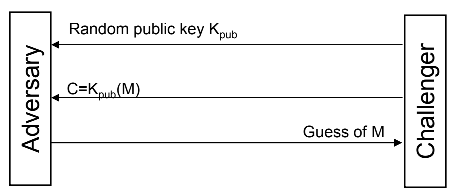
BF: Security parameter

- If r is exposed, adversary can decrypt *M* and *σ* and modify the message at will
- r is protected by the difficulty of extracting discrete logarithm from *rP* (*P* is public)
- … but *rP* belongs to a supersingular EC group, where a DL solver runs in subexponential time
- Extension parameter defines security parameter

BF keylens for 128-bit entropy	
ext.size (l)	*key length*
6	423 bits
5	508 bits
4	635 bits
3	846 bits
2	1269 bits
1	2538 bits (RSA)

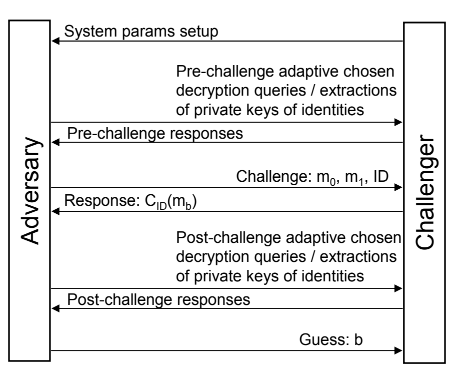
Security notions

- IND-ID-CCA2, adaptive chosen ciphertext attacks for identity-based frameworks
- OWE, One-Way Encryption, defined for standard public-key schemes
- ”all-or-nothing” model: M is either bit-by-bit correctly guessed, or the challenge fails



IND-CCA2 sec. in IB framework (1)

- Challenger-adversary game as in normal IND-CCA2; (called IND-ID-CCA2) decryptions and *private key extractions* are allowed (not for the challenge ID, though)

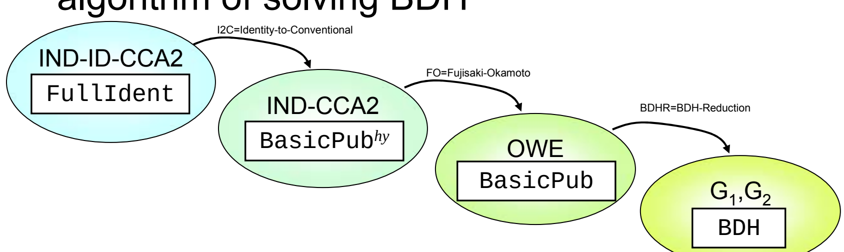


IND-CCA2 sec. in IB framework (2)

- Adversary assumed to be PPT-bounded
- Adversary wins the game, if he guesses, which of the messages was encrypted
- IND-CCA2 notion satisfied, if the adversary cannot gain a non-negligible (inverse polynomial in the size of the security parameter) advantage in guessing correctly
- Semantic security

BF: Security proof (1/5)

- Assumption: Bilinear DH problem (BDH) is hard in the instantiated group (BDH is assumed to be hard (superpolynomial, albeit subexponential) in supersingular EC groups)
- Proof is a reduction through two types of security notions and cryptosystems to an algorithm of solving BDH



BF: Security proof (2/5)

- Basic theorem:
  - Assume $H_1 \ldots H_4$ are random oracles
  - $\mathcal{A}$ is a t-time, ε-advantage IND-ID-CCA2-adversary on `FullIdent`, n is the blocksize of encryption
  - $\mathcal{A}$ has q_E extraction, q_D decryption and q_{Hi} hash queries (hash queries for oracle H_i)
- There is an algorithm $\mathcal{B}$ for solving BDH in the instantiation groups, such that

$$\mathrm{time}(\mathcal{B}) \le \mathrm{FO}_{time}\left(t, q_{H_4}, q_{H_3}\right)$$

$$\mathrm{Adv}(\mathcal{B}) \ge \frac{\mathrm{FO}_{adv}\left(\frac{\varepsilon}{e(1+q_E+q_D)}, q_{H_4}, q_{H_3}, q_D\right) - 2^{-n}}{q_{H_2}}$$

BF: Security proof (3/5)

- The Fujisaki-Okamoto functions FO are defined as:

$$\mathrm{FO}_{time}\left(t, q_{H_4}, q_{H_3}\right) = t + O\left(n\left(q_{H_4} + q_{H_3}\right)\right)$$

$$\mathrm{FO}_{adv}\left(\varepsilon, q_{H_4}, q_{H_3}, q_D\right) = \frac{1}{2\left(q_{H_4} + q_{H_3}\right)}\left[(\varepsilon+1)\left(1-\frac{2}{q}\right)^{q_D} - 1\right]$$

- I2C reduction states that the adversary in IND-ID-CCA2-setting with its time- and advantage parameters has a time-parameter of the same order, and advantage $\frac{\varepsilon}{e(1+q_E+q_D)}$ against `BasicPub`^{hy} in IND-CCA2-setting

BF: Security proof (4/5)

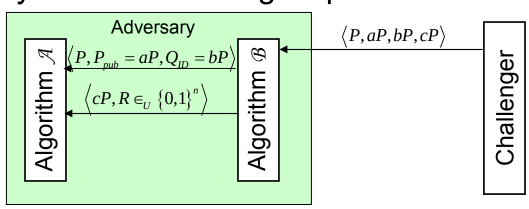
- Scheme `BasicPub`: same as `BasicIdent` (Mao's version of BF-IBE), but public key is random, not generated from any ID
- Scheme `BasicPub`^{hy}: same as `FullIdent`, but public key is random
- Sketch of proof of I2C
  - $\mathcal{B}$ against `BasicPub`^{hy} will use $\mathcal{A}$ against `FullIdent` by
    - Simulating the challenger as a random oracle for $\mathcal{A}$ for extraction queries (there are no identities in `BasicPub`^{hy})
    - Relaying and translating decryption queries to `BasicPub`^{hy} challenger
    - Relaying and translating (probabilistically) challenges and responses between $\mathcal{A}$ and `BasicPub`^{hy} challenger

BF: Security proof (5/5)

- Fujisaki-Okamoto proof omitted
- BDH-reduction premise is that the adversary in OWE-setting with its time- and advantage parameters has a time-parameter of the same order, and advantage $\left(\varepsilon - 2^{-n}\right)/q_{H_2}$ against BDH in the instantiated groups
- Proof of the BDH-reduction follows the same format as the I2C-reduction:
  - $\mathcal{B}$ simulates (as a random oracle) H_2 to $\mathcal{A}$ making sure to respond consistently to queries
  - The input extractable group elements to $\mathcal{B}$ will be translated as system parameters to $\mathcal{A}$: $aP=P_{pub}$, $bP=Q_{ID}$, cP=first part of the ciphertext C = <cP,R>

BF Security proof: BDH (1/6)

- Challenge phase
  - Group descriptions and Weil pairing description are passed as is
  - $\mathcal{B}$ creates an oracle access to H_2 ("keystream generator")
  - BDH instances are translated to parts of the public key and the challenge ciphertext

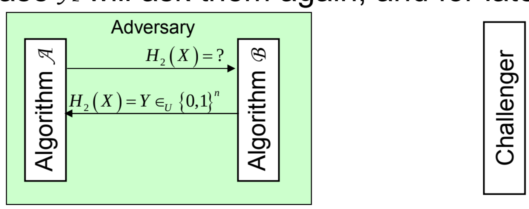


BF Security proof: BDH (2/6)

- Challenge phase
  - Since $P_{pub}=aP$, a is the secret master key
  - Thus $d_{ID}=aQ_{ID}=abP$
  - $\mathcal{A}$ is assumed to return the "correct" plaintext, so we mark $M = R \oplus H_2(e(cP, d_{ID})) = R \oplus H_2(D)$
  - Also, D is the solution to the BDH problem, since
$$e(cP, d_{ID}) = e(cP, aQ_{ID}) = e(cP, aQ_{ID}) =$$
$$e(cP, aQ_{ID}) = e(cP, abP) = e(P, abcP) =$$
$$e(P, P)^{abc}$$

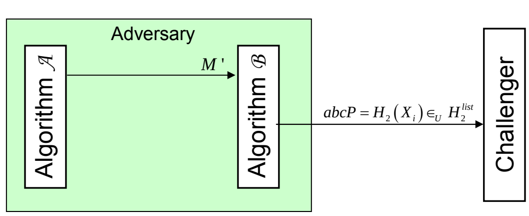
BF Security proof: BDH (3/6)

- Oracle queries ($\mathcal{A}$ will want to map the G_2-group element to a bitstring – which is supposed to happen with the private (unknown) key):
  - The ”hash” H_2 is simulated by randomly producing an n-bit value
  - The already given hashes are memorized in a list in case $\mathcal{A}$ will ask them again, and for later guesses



BF Security proof: BDH (4/6)

- Guess
  - $\mathcal{A}$'s guess is as such, meaningless, since we do not know the hash pre-image (which would correspond to the abcP – or the solution of the BDH-problem)
  - However, in order for $\mathcal{A}$ to have computed the message from interactions with the challenger, the pre-image must be within the memorized list of hashes
  - $\mathcal{B}$ just randomly outputs one of these pre-images



BF Security proof: BDH (5/6)

- Time constraints:
  - $\mathcal{B}$'s work is all about using $\mathcal{A}$, translating instances (O(1) work) and maintaining the oracle query list ($O(q_D)$ work)
  - $\mathcal{B}$'s work is the of same order as $\mathcal{A}$'s => PPT-bounded
- Advantage:
  - Selection of the public key and cipher text depends on the original challenger; $\mathcal{B}$ outputs the "ciphertext" and oracle responses uniformly random
  - If $\mathcal{A}$ has advantage ε, then $P[M'=M] \geq \varepsilon$

BF Security proof: BDH (6/6)

- Advantage:
  - Let T be the event that D appears in the memorized list, and $\delta = P[T]$
  - If $\mathcal{A}$ outputs a correct answer and the D is not found in the list, then $\mathcal{A}$ has acted independently of the hashes. In this case the guess is random: $P[M=M' \mid \neg T] \leq 2^{-n}$
  - From these:

$$\varepsilon \leq P[M=M'] = P[M=M' \mid T]P[T] + P[M=M' \mid \neg T]P[\neg T]$$
$$\leq P[T] + P[M=M' \mid \neg T]P[\neg T] \leq \delta + 2^{-n}(1-\delta)$$

  - Solving for $\delta : \delta > \delta(1-2^{-n}) > \varepsilon - 2^{-n}$
  - The advantage follows by dividing by the number of oracle queries

IB and dir PKI

	Directory	Identity-based (Weil pairing)
TTPs	RA, CA, LDAP-rep.	PKG/TA
Operations needing interaction	System setup, fetching public key, fetching revoc.lists, …	System setup
Key gen.	User	PKG/TA
Key length (128 bit entropy)	2540 bits (RSA) 256 bits (ECC)	420 – 1270 bits (l=6..2)
Revocation	Timed, or lists	Timed

Open problems

- Non-interactive key (/identity) revocation
- Random elements inclusion in the key generation
- Lessening the dependency on a single TA
  (some solutions, not completely satisfactory, exist, e.g. B&F, Mao)
- Multi-party IB-PKI
- Ad hoc – IB-PKI

Conclusion

- Instantiable IB-PKI a new area:
  - More efficient than conventional PKI
  - Important open problems
- Elliptic-curve algebra ”involved”
  - Backed by long history of mathematical research
  - New applications bound to emerge
- Promising applications in ad hoc peering networks