Encryption Schemes from Bilinear Maps

Eu-Jin Goh

PhD Thesis Defense

30 May 2007

Encryption Schemes

Provide data confidentiality

- building block of crypto protocols
- two main types :

1. Symmetric Key Enc (e.g. DES, AES)
   - Same key used to encrypt and decrypt

2. Public Key Enc (e.g. RSA)
   - Public key used to encrypt
   - Private key to decrypt
   - Much slower than symm key enc
   - Focus of this talk

Encryption Schemes from Bilinear Maps

1. Traditional pub key enc schemes
   - e.g. El Gamal, RSA
   - based on finite groups of prime or composite order

2. Bilinear groups
   - finite groups on certain elliptic curves with special function called bilinear map
   - can build enc schemes on bilinear groups

Thesis

Bilinear groups

allow us to build pub key enc schemes with properties that are difficult to obtain using "traditional" groups

To support thesis, give 2 schemes we built

- Homomorphic enc scheme [BGN05]
- Hierarchical IBE [BBG05]

Part 1 :

Homomorphic Encryption

What is Homomorphic Encryption?

Enc. scheme is homomorphic to function f if

- from E[A], E[B], can compute E[f(A,B)]
  - e.g. f can be +, ×, ⊕, …
  - no secrets needed to compute

e.g. El Gamal (× homomorphic)

$$CT_1 = (g^a, g^{sa} \times M_1) \qquad CT_2 = (g^b, g^{sb} \times M_2)$$

$$CT1 \times CT2 = (g^{a+b}, g^{s(a+b)} \times M_1 M_2)$$

Doubly Homomorphic Encryption

Enc. scheme is homomorphic to function f if

- from E[A], E[B], can compute E[f(A,B)]
  - e.g. f can be $+$, $\times$, $\oplus$, …

Ideally, want f = NAND, or f = $\{+,\times\}$

- Called doubly homomorphic encryption

Can do universal computation on ciphertext!

Why is doubly homomorphic encryption useful?

Efficient solution for many problems:

Most generally

1. 2 party Secure Function Evaluation

Specific problems

- Computing on encrypted databases
- Distributed computing on confidential data

⋮

App: Database Computation

Outsourced server with database containing encrypted data

- User wants to compute function g on encrypted data
  - e.g. data mining, data aggregation

With doubly homomorphic encryption,

- Database encrypted with doubly hom. enc.
- User sends g to server
- Server computes g on encrypted database
- Encrypted result returned to user

These applications are pretty cool,

what does a doubly homomorphic encryption scheme look like?

Sorry, it doesn't exist (yet).

- Open problem from 1978 (Rivest et. al.)
- Existing schemes hom. to 1 function
  - E.g. ElGamal ($\times$), Paillier ($+$), GM ($\oplus$)

But made some progress …

Our Results

Two homomorphic encryption schemes that support one $\times$ and arbitrary +

$\Rightarrow$ Eval multi-var polynomials of total deg 2

1. Subgroup decision scheme
   - Built from finite bilinear groups with composite order
   - Security based on subgroup decision problem
2. Linear scheme
   - Built from finite bilinear groups with prime order
   - Security based on linear problem

For talk, focus on subgroup decision scheme

Related Work

Sander et al. [SYY99]

- Enc. scheme — NC^1 circuit eval. on CTs

  ⇒ Can evaluate 2-DNFs on CTs

But CT len. exponential in circuit depth

- CT size doubles for every + op
  - Poly. len. 2-DNF gives poly. size CT
- Our schemes — constant size CT

  — crucial for apps

Bilinear groups with composite order n

For prime $p = ln - 1$ and $p = 2 \bmod 3$

- G = subgroup of points in F_p on elliptic curve $y^2 = x^3 + 1$ (order n)
- G_1 = subgroup of F_{p^2} (order n)

Weil pairing on curve gives bilinear map $e: G \times G \longrightarrow G_1$ where

1. $e(u^a, v^b) = e(u, v)^{ab}$
2. $e(g, g) \neq 1$ (g = generator of G)

Enc. Scheme

Keygen(τ):

- G: bilinear group order $n = q_1 q_2$ on ell. curve over F_p.
- Pick rand $g, u \in G$. Set $h = u^{q_2}$ ($\Rightarrow$ h order q_1)
- PK = (n, G, G_1, e, g, h) SK = q_1

Encrypt(PK, m): $m \in \{1,\dots,T\}$

- Pick random r from Z_n.
- Output $C = g^m h^r \in G$.

Decrypt(SK, C):

- Let $C^{q_1} = (g^m h^r)^{q_1} = (g^{q_1})^m$; $v = g^{q_1}$
- Output m = Dlog of C^{q_1} base v.

Note: decrypt time is $O(\sqrt{T})$.

Homomorphisms

Given $A = g^a h^r$ and $B = g^b h^s$:

To get encryption of a + b

- pick random $t \in Z_n$
- compute $C = A \cdot B \cdot h^t = g^{a+b} h^{r+s+t} \in G$

To get encryption of a × b

- let $h = g^{\alpha q_2}$, $g_1 = e(g,g)$, $h_1 = e(g,h)$
- pick random $t \in Z_n$
- compute

$$C = e(A,B) \cdot h_1^{t} = g_1^{ab} h_1^{r'} \in G_1$$

Semantic Security

For encryption schemes, standard notion of security is semantic security.

Modeled as game btw adversary and challenger

Challenger		Adversary
Keygen(τ)	PK $\longrightarrow$	Pick 2 msgs
	$\longleftarrow$ M_0 , M_1	M_0, M_1 (same len)
Pick random bit $b \in \{0,1\}$	$E[M_b]$ $\longrightarrow$	Output guess for b

Sem sec $\Rightarrow$ can't guess b with prob different from ½

$\Rightarrow$ can't distinguish btw ciphertexts

Complexity Assumption

Decision subgroup assumption:

For rand. bilinear group G of order $n = q_1 q_2$,
given (n, G, G_1, e, x), the distributions :

- x is uniform in G
- x is uniform in q_1—subgroup of G

are indistinguishable

Thm: system is semantically secure, unless the subgroup assumption is false.

Security of Encryption Scheme

Proof Sketch :

1. Assume enc scheme is broken
   - $\Rightarrow$ exists adversary A that can win semantic security game with prob better than ½
   - use A to break complexity assumption
   - i.e. given (n, G, G_1, e, x), use A to determine if x is in q_1 subgroup of G
2. Create simulator S that interacts with A to distinguish x with prob better than ½

Proof of Semantic Security

Simulator | **Adversary**

Given (n, G, G_1, e, x),

decide if $x \in q_1$ subgroup of G

Pick rand $g \in G$

$PK = (n, G, G_1, e, g, x)$ →

Pick 2 msgs M_0, M_1

← M_0 , M_1

Pick random bit $b \in \{0,1\}$

$E[M_b] = g^{m_b} x^r$ →

Output b'

If $x \in q_1$ subgroup of G, then $E[M_b]$ valid CT

If not, then $E[M_b]$ independent of b

Applications

1. Evaluate multi-variate polynomials of total degree 2 (on ciphertexts)
2. Gadget: “check” if CT contains 1 of 2 values
   - Most voter efficient E-voting scheme
   - Universally verifiable computation
3. SFE for 2-DNF formulas $\vee (b_{i,1} \wedge b_{i,2})$
4. Build first perfect NIZK argument for all NP languages [GOS06]
   - 20 year old problem in NIZK

1) Evaluating Quadratic Poly.

Multi-var polynomials of total deg 2

- $x_1 x_2 + x_3 x_4 + \ldots$

- $+, \times$ hom. allow eval. of such poly. on CT
    - e.g. $e\,(E[x_1]\,,\,E[x_2]) \times e\,(E[x_1]\,,\,E[x_2]) \times \ldots$
- evaluate dot products
- but to decrypt, result must be in known poly. size interval.

2) Gadget

Suppose CT: C = E[v].

Given 2 msgs v_0,v_1 and rand r, anyone can compute

$$E\,[\,r \cdot (v - v_0) \cdot (v - v_1)\,]$$

- If $v \neq v_0,v_1$, result is E[random]
- Otherwise, result is E[0]

- Decryptor can verify CT is enc. of either v_0 or v_1
  - but not learn which one

Applications:

1. E-voting: voter ballots need no NIZK proofs
2. Universally Verifiable Computation
   - Anyone can check that public function on private inputs computed correctly without learning anything else

4) Perfect NIZK for all NP lang.

GOS06 built perfect NIZK for circuit sat (CSAT) using our enc scheme

NIZK for CSAT $\Rightarrow$ prove that circuit C is satisfiable without revealing formula that satisfies C

CSAT = NP-complete

4) NIZK for CSAT

Key observations :

- can build NIZK proof that CT contains enc of 0 or 1
- our enc scheme also commitment scheme
  - If A, B, C commitments to bits

$$C = A \text{ NAND } B \quad \text{iff} \quad A + B + 2\,(C - 1) \in \{0,1\}$$

can use homomorphic properties + NIZK proof to verify RHS

If A, B input wires of NAND gate and C output wire

- use NIZK proof to show that A, B, C are enc of bits
- compute RHS and verify result with another NIZK proof

$\Rightarrow$ NAND gate well formed

- Then use this construction in circuit to show satisfaction without revealing formula

Secure Function Evaluation

2 parties : Alice and Bob

- Alice has function f and Bob has input x
- Both want to evaluate f(x) without revealing f to Bob and x to Alice

Two security models :

1. Alice/Bob is semi-honest
   - follow protocol exactly but can learn secret info from interaction (honest but curious)
2. Alice/Bob is malicious
   - can do anything they like but assume that Alice/Bob still interested in learning f(x)
   - can’t prevent aborting, not participating, using input y instead of x, …

4) 2 Party SFE for 2-DNF

Bob

$A = (a_1,\ldots,a_n)$

$\in \{0,1\}^n$

Alice

$\phi(x_1,\ldots,x_n) = \vee^{k}_{i=1}(y_{i,1} \wedge y_{i,2})$ s.t.

$y_{i,*} \in \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$.

Get Arithmetization Φ:

- replace $\vee$ by $+$, $\wedge$ by $\times$, $\neg x_i$ by $(1- x_i)$.
- Φ is poly. with total deg 2!

2-DNF Protocol (Semi-Honest)

Bob	Alice
$A = (a_1,\ldots,a_n)$	$\phi(x_1,\ldots,x_n) = \vee^k_{i=1}(y_{i,1} \wedge y_{i,2})$
	Φ = arith. of ϕ

Invoke Keygen(τ)

Encrypt A

$\xrightarrow{\text{PK, } E[a_1],\ldots,E[a_n]}$

Eval. $E[r \cdot \Phi(A)]$ for random r

$\xleftarrow{E[r \cdot \Phi(A)]}$

If decrypt = 0, emit 0. Else, 1.

Bob's Security: Alice cannot distinguish bet. Bob's possible inputs — from semantic security of E.

Alice's Security: Bob only knows if A satisfies $\phi()$ — by design, Bob output distrib. depends only on this.

SFE for 2-DNF

1. Communication Complexity = $O(n \cdot \tau)$
   - garbled circuit comm. comp. = $\Theta(n^2)$
2. Secure against unbounded Bob
3. Also have protocol secure against malicious Bob (in paper)

Concrete application for 2-DNF

Improve basic step in Kushilevitz-Ostrovsky PIR protocol from $\sqrt{n}$ to $\sqrt[3]{n}$

- PIR = Private Information Retrieval
  - Bob wants entry j in database
  - but does not want database or any eavesdropper to know j
- Trivial solution : send whole db
  - want more communication efficient sol
  - optimize for comm., not computation

PIR/SPIR

Bob: wants D(R,S)

Set assignment A:

$x_R = y_S = 1,$

$x_i = x_j = 0$

for $i \neq R$, $j \neq S$

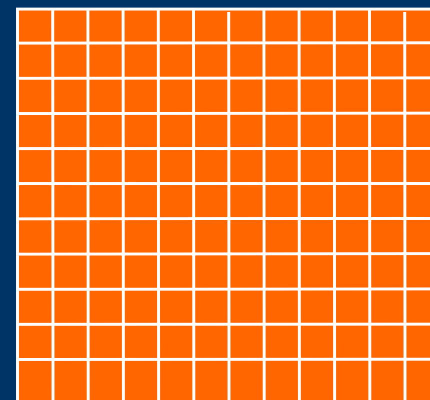
Do 2-DNF SFE

with A and ϕ

Get $\phi(A) = D(R,S)$

Database D

$\sqrt{n}$ $|D| = n$



$\sqrt{n}$

D uses 2-DNF

$\phi(x_1,\ldots,x_{\sqrt{n}}, y_1,\ldots,y_{\sqrt{n}})$

$= \vee_{D(i,j)=1} (x_i \wedge y_j)$

If $D(R,S) = 0 \Rightarrow (x_R \wedge y_S) \notin \phi$. Then $\phi(A) = 0$ if $x_R = y_S = 1$ in A.

If $D(R,S) = 1 \Rightarrow (x_R \wedge y_S) \in \phi$. Then $\phi(A) = 1$ if $x_R = y_S = 1$ in A.

Comm. Complexity $= O(\tau \cdot \sqrt{n})$ [$O(\tau^{0.i3}\sqrt{n})$ balanced]

Alternative scheme — each db entry O(log n) bits

End of Part 1 : Homomorphic Enc

Two homomorphic enc schemes that support one $\times$ and arbitrary +

- based on subgroup decision and linear problems

Despite only one additional mult, still many useful applications :

1. Dot products, quadratic poly
2. 2-DNF, PIR
3. Voting, verifying computation
4. Perfect NIZK for NP

⋮

Questions?

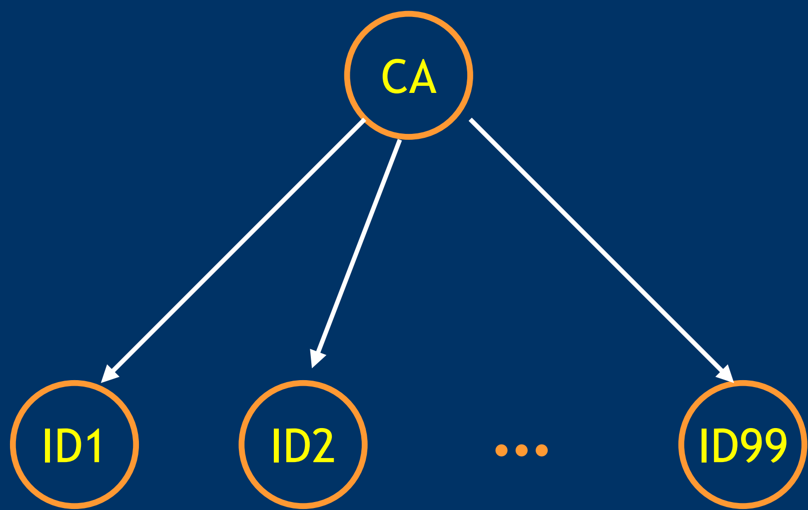
Part 2 :

Identity Based Encryption

Identity Based Encryption (IBE)

IBE — Pub key enc system [S84,BF01,C01]

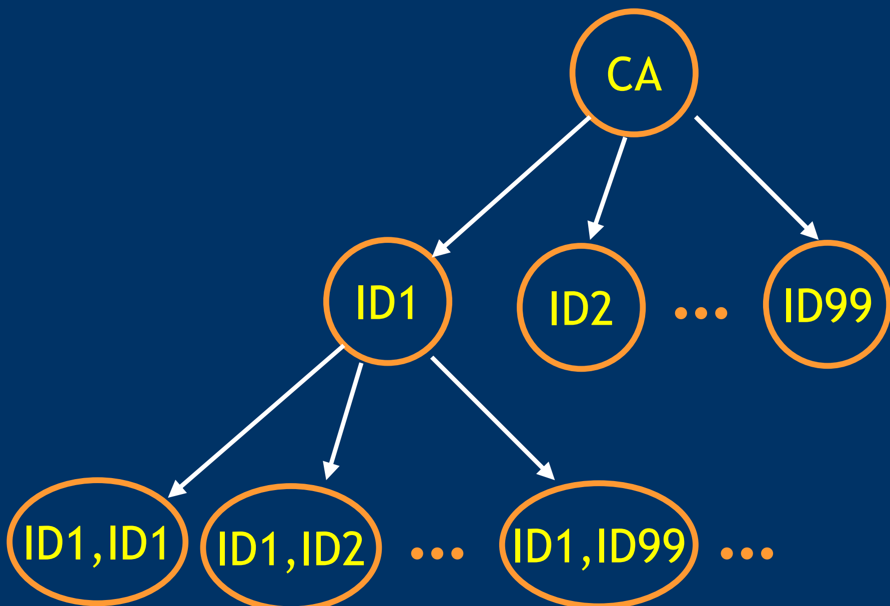
- In IBE, pub keys can be arbitrary strings (ID)
- Traditional Pub Key Enc :
  - need user to have pub/priv key pair before can enc msgs to user
- IBE : since pub key can be arbitrary string
  - can encrypt to user using public id (e.g. email addr)
  - Central auth (CA) issues priv key to user for public id



Hierarchical IBE (HIBE)

HIBE — IBE generalization [HL02,GS02,BB04]

- ID with priv keys can issue priv keys to descendent IDs
  - e.g. with priv key for ID = (A_1,A_2),
    can create priv key for ID = $(A_1,A_2, * , \ldots)$



Applications

ID hierarchy can mirror organization hier.

- Delegate key generation to subordinates

HIBE is a building block for:

- Forward Secure Enc
  - Private key evolves over time s.t.

    CT enc with key at time n cannot be dec with priv key from time > n
- Public Key Broadcast Enc
  - Broadcast enc = enc msg to large user base with ability to revoke users
  - E.g. DVD enc scheme - AACS

Main Result

Existing HIBEs — HL02, GS02, BB04

CT size and dec cost *linear* with hierarchy depth

Our HIBE —

1. CT size and dec cost *constant* with hier depth
   - CT Size = 3 group elmts , Dec Cost = 1 pairing
2. Priv key size shrinks as go down ID hierarchy
3. Selective ID Security in Standard Model
   - Bilinear DH Inversion Problem (BDHI) [BB04]

Using our HIBE in Applications

Existing HIBEs — GS02, BB04

CT size, dec cost *linear* with hierarchy depth.

Forward Secure Enc

- GS,BB — CT size, Dec cost = O(log(time))
- Ours — CT size, Dec cost = O(1)

Broadcast Enc — N = # users, r = # revoked users

- GS,BB — CT size = O(r log N)
- Ours — CT size = O(r)

HIBE Scheme

Setup(l):

- G: bilinear group order p. HIBE max depth = l.
- Pick rand $g, g_2, g_3, h_1, \ldots, h_l \in G$, $\alpha \in Z_p$. Set $g_1 = g^\alpha$.
- Params = $(g, g_1, g_2, g_3, h_1, \ldots, h_l)$ Master Key = g_2^α

KeyGen(d_{ID^*}, ID):

$ID^* = (I_1, \ldots, I_k)$ $ID = (I_1, \ldots, I_{k+1})$

- $d_{ID^*} = (g_2^\alpha \cdot (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^r , g^r , h_{k+1}^r , \ldots , h_l^r)$ rand $r,t \in Z_p$
  $= (a_0, a_1 , b_{k+1} , \ldots , b_l)$
- $d_{ID} = (a_0 \cdot b_{k+1}^{I_k} \cdot (h_1^{I_1} \cdots h_{k+1}^{I_k} \cdot g_3)^t , a_1 \cdot g^t , b_{k+2}h_{k+2}^t , \ldots, b_l h_l^t)$

Encrypt(Params, ID, m):

$ID = (I_1, \ldots, I_k)$

- Pick rand $s \in Z_p$.
- Output $C = (e(g_1,g_2)^s \cdot M , g^s , (h_1^{I_1} \cdots h_k^{I_k})^s)$.

Decrypt(d_{ID}, CT):

$CT = (A,B,C)$ $d_{ID} = (a_0, a_1 , b_{k+1} \ldots , b_l)$

- Output $A \cdot e(a_1,C) / e(a_0 ,B)$

IND-sID-CCA Security [BF01]

Challenger | ID* | Adversary

Setup Alg | Pub params |

| Either ID or $E_{ID}[M]$ | Priv key and Decrypt Queries

| Priv key for ID or M |

| M_0, M_1 |

Pick rand bit b | $E_{ID^*}[M_b]$ | Challenge

| | More Queries except challenge

Output guess b'. Win if b' = b.

Security Theorem

l^{th} Bilinear DH Inversion assumption [BB04]:

G = Bilinear group of prime order p

e : $G \times G \to G_1$

For rand generators $g, h \in G$, and rand $\alpha \in Z_p^*$
then following two distributions indistinguishable:

- $(g , h , g^{(\alpha)} , g^{(\alpha^2)} , \ldots , g^{(\alpha^l)} , e(g,h)^{1/\alpha})$
- $(g , h , g^{(\alpha)} , g^{(\alpha^2)} , \ldots , g^{(\alpha^l)} , T)$ for rand $T \in G_1$

Thm: HIBE system is IND-sID-CCA, unless l-wBDHI assumption is false.

End of Part 2 : HIBE

HIBE with constant size CT and dec cost

- Secure in Standard Model
- Weak Bilinear DH Inversion Assump.

Open Problem:

- Fully Secure HIBE with tight reduction

Conclusions

Bilinear groups

allow us to build pub key enc schemes with properties that are difficult to obtain using "traditional" groups

Gave 2 examples :

- Subgroup Decision homomorphic enc scheme
- Hierarchical IBE

My Publications

1. Securing Remote Untrusted Storage
   - NDSS 2003
2. Key Recovery in TLS
   - ISC 2003
3. Signature scheme with tight security
   - Eurocrypt 2003
4. Effectiveness of Address Space Randomization
   - ACM CCS 2004
5. Event driven private counters
   - FC 2005
6. Evaluating 2-DNF formulas on Ciphertext
   - Theory of Cryptography 2005
7. Hierarchical IBE with constant size Ciphertext
   - Eurocrypt 2005
8. SFE using Ordered Binary Decision Diagrams
   - ACM CCS 2006
9. Privacy in RFID
   - Currently in submission
10. Secure Indexes
    - Technical Report

Acknowledgements

1. my advisor : Dan Boneh
2. thesis committee members
   - John Mitchell, Rajeev Motwani, Dawson Engler, Nancy Zhang
3. my coauthors
   - Hovav Shacham, Stanislaw Jarecki, Xavier Boyen, Kobbi Nissim, Philippe Golle, Aviv Nisgav, Louis Kruger, Somesh Jha, Matthew Page, Ben Pfaff, Nagendra Modadugu, Benny Pinkas, Ari Juels, Dan Bailey, Brent Waters
4. the Stanford Crypto and Security Group
5. the support of my wife, family, and friends

Questions?