RUB

RUHR-UNIVERSITÄT BOCHUM

(Hierarchical) Identity-Based Encryption from Affine Message Authentication

Crypto 2014,

Olivier Blazy Eike Kiltz Jiaxin Pan
Horst Görtz Institute for IT Security
Ruhr-University Bochum

hgi
Horst Görtz Institut
für IT-Sicherheit

Outline

Identity-Based Encryption

Alice

$\xrightarrow{\mathsf{C} = \mathsf{Encrypt}(\text{'Bob'}, M)}$

Bob

M

$M = \mathsf{Decrypt}(\mathsf{usk}_{\mathsf{Bob}}, C)$

History of IBE

- Shamir 84

History of IBE

- Shamir 84
- Boneh-Franklin, Cocks

History of IBE

- Shamir 84
- Boneh-Franklin, Cocks
- Boneh-Boyen, Waters 05

History of IBE

- Shamir 84
- Boneh-Franklin, Cocks
- Boneh-Boyen, Waters 05
- Waters 09, Chen-Wee

History of IBE

- Shamir 84
- Boneh-Franklin, Cocks
- Boneh-Boyen, Waters 05
- Waters 09, Chen-Wee
- ...

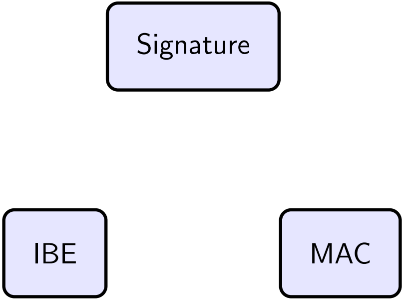
History of IBE

- Shamir 84
- Boneh-Franklin, Cocks
- Boneh-Boyen, Waters 05
- Waters 09, Chen-Wee
- ...

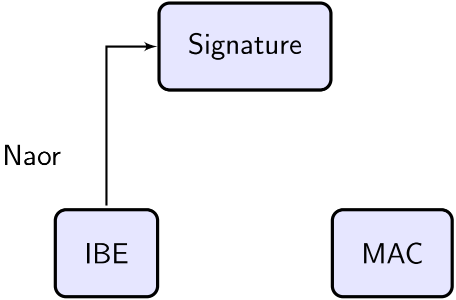
Open Problem

$$\text{????} \xrightarrow{\text{Generic}} \text{IBE}$$

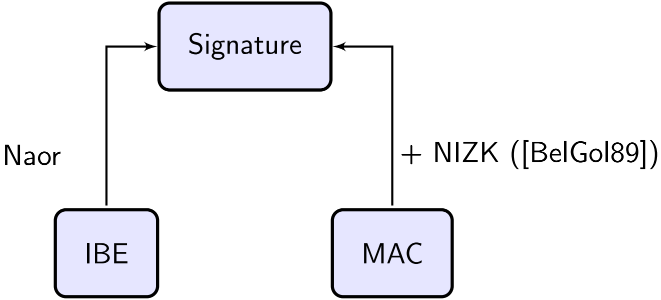
More about History



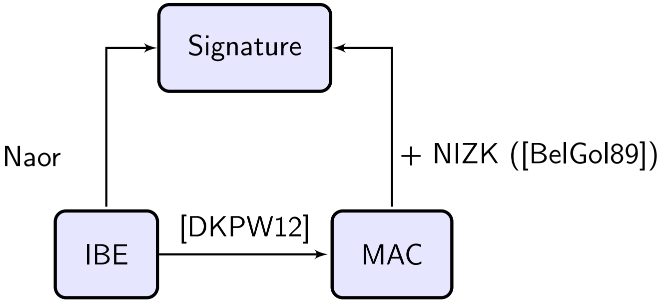
More about History



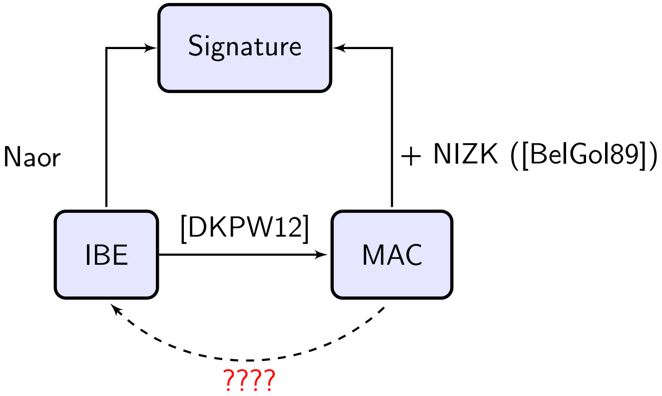
More about History



More about History



More about History



MAC + NIZK → Signature

Signature

- $\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, y)$; $\mathsf{pk} := \mathsf{Commit}(\mathsf{sk}_{\mathsf{MAC}}; y)$
- $\mathsf{Sig}(\mathsf{sk}, \mathsf{m})$:

$$\tau \stackrel{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}), \pi \stackrel{\$}{\leftarrow} \mathsf{Prove}(\text{'}\tau \text{ is valid'})$$

- $\mathsf{Ver} := \mathsf{Ver}_{\mathsf{NIZK}}$

NIZK Proof

$\mathsf{NIZK} := (\mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}})$ for $\mathcal{L}$:
$\{(\tau, \mathsf{m}, \mathsf{pk}) : \exists \mathsf{sk}, y \text{ s.t. } \mathsf{Ver}(\mathsf{sk}, \tau, \mathsf{m}) = 1 \wedge \mathsf{pk} = \mathsf{Commit}(\mathsf{sk}; y)\}$

MAC + NIZK $\stackrel{?}{\to}$ IBE

IBE

- sk $:=$ (sk$_{\mathsf{MAC}}, y$); pk $:=$ Commit(sk$_{\mathsf{MAC}}; y$)
- Sig(sk, m) :
  $$\tau \stackrel{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}), \pi \stackrel{\$}{\leftarrow} \mathsf{Prove}(\text{'}\tau \text{ is valid'})$$
- Ver $:=$ Ver$_{\mathsf{NIZK}}$

NIZK Proof

NIZK $:=$ (Prove, Ver$_{\mathsf{NIZK}}$) for $\mathcal{L}$:

$\{(\tau, \mathsf{m}, \mathsf{pk}) : \exists \mathsf{sk}, y \text{ s.t. } \mathsf{Ver}(\mathsf{sk}, \tau, \mathsf{m}) = 1 \wedge \mathsf{pk} = \mathsf{Commit}(\mathsf{sk}; y)\}$

MAC + NIZK $\overset{?}{\to}$ IBE

IBE

- $\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, y)$; $\mathsf{pk} := \mathsf{Commit}(\mathsf{sk}_{\mathsf{MAC}}; y)$
- USKGen :

$$\tau \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}), \pi \xleftarrow{\$} \mathsf{Prove}(\text{'}\tau \text{ is valid'})$$

- $\mathsf{Ver} := \mathsf{Ver}_{\mathsf{NIZK}}$

NIZK Proof

$\mathsf{NIZK} := (\mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}})$ for $\mathcal{L}$:
$\{(\tau, \mathsf{m}, \mathsf{pk}) : \exists \mathsf{sk}, y \text{ s.t. } \mathsf{Ver}(\mathsf{sk}, \tau, \mathsf{m}) = 1 \wedge \mathsf{pk} = \mathsf{Commit}(\mathsf{sk}; y)\}$

MAC + NIZK $\overset{?}{\to}$ IBE

IBE

- sk := $(\mathsf{sk}_{\mathsf{MAC}}, y)$; pk := $\mathsf{Commit}(\mathsf{sk}_{\mathsf{MAC}}; y)$
- USKGen :

  $\tau \overset{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}), \pi \overset{\$}{\leftarrow} \mathsf{Prove}(\text{'}\tau \text{ is valid'})$
- Enc := ????
- Dec := ????

(Enc and Dec: $\mathsf{Ver}_{\mathsf{NIZK}}$)

NIZK Proof

NIZK := $(\mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}})$ for $\mathcal{L}$:

$\{(\tau, \mathsf{m}, \mathsf{pk}) : \exists \mathsf{sk}, y \text{ s.t. } \mathsf{Ver}(\mathsf{sk}, \tau, \mathsf{m}) = 1 \wedge \mathsf{pk} = \mathsf{Commit}(\mathsf{sk}; y)\}$

MAC + NIZK $\xrightarrow{?}$ IBE

IBE

- $\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, y)$; $\mathsf{pk} := \mathsf{Commit}(\mathsf{sk}_{\mathsf{MAC}}; y)$
- USKGen :

  $\tau \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}), \pi \xleftarrow{\$} \mathsf{Prove}(\text{'}\tau \text{ is valid'})$
- Enc := ????
- Dec := ????

$\left.\begin{array}{l}\mathsf{Enc} := ????\\ \mathsf{Dec} := ????\end{array}\right\}\ \mathsf{Ver}_{\mathsf{NIZK}}$

Our Work

- Use the verification algorithm to define Enc and Dec

MAC + NIZK $\stackrel{?}{\to}$ IBE

IBE

- sk $:= (\mathsf{sk}_{\mathsf{MAC}}, y)$; pk $:= \mathsf{Commit}(\mathsf{sk}_{\mathsf{MAC}}; y)$
- USKGen :

  $$\tau \stackrel{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}), \pi \stackrel{\$}{\leftarrow} \mathsf{Prove}(\text{'}\tau \text{ is valid'})$$

- Enc $:=$????
- Dec $:=$????

$\left.\right\}$ $\mathsf{Ver}_{\mathsf{NIZK}}$

Our Work

- Use the verification algorithm to define Enc and Dec
- Exploit the underlying structure of the MAC + NIZK

Our Contributions

(H)IBE = Affine MAC + Pairings

- Affine MAC: Affine Equations
- Pairings: Groth-Sahai Proofs, Affine Verification

Our Contributions

(H)IBE = Affine MAC + Pairings

- Affine MAC: Affine Equations
- Pairings: Groth-Sahai Proofs, Affine Verification

The affine properties allow to define Enc and Dec.

RUB

Outline

hgi Horst Görtz Institut für IT-Sicherheit

Matrix Notation

- Considering $(\mathbb{G}, g, q)$ and $\mathbf{A} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ & \ddots & \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in \mathbb{Z}_q^{n \times m}$

Implicit Representation

$$[\mathbf{A}] := \begin{pmatrix} g^{a_{11}} & \dots & g^{a_{1m}} \\ & \ddots & \\ g^{a_{n1}} & \dots & g^{a_{nm}} \end{pmatrix} \in \mathbb{G}^{n \times m}.$$

Affine MAC – Intuition

$\mathsf{MAC} := (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver})$.

$$\mathsf{Tag}(\mathsf{sk}, \mathsf{m}) \rightarrow \left(\begin{bmatrix} \vdots \\ \mathbf{t} \\ \vdots \end{bmatrix}, [u] \right)$$

Affine MAC

- $\mathbf{t}$: Random Part
- u: Message-depending Affine Part

Affine MAC – Formal Definition

- $\mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$:

$$\mathsf{sk} := (\ \mathbf{x}_0\ , \dots, \ \mathbf{x}_\ell\ ,\ x'_0, \dots, x'_{\ell'})$$

- $\mathsf{Tag}(\mathsf{sk}, \mathsf{m}) \xrightarrow{\$} \tau := ([\mathbf{t}], [u])$

$\mathbf{t}$

$$u = \sum f_i(\mathsf{m})\mathbf{x}_i^\top \; \mathbf{t} + \sum f_i'(\mathsf{m})x_i' \in \mathbb{Z}_q \qquad (*)$$

Public functions, $f_i, f_i' : \mathcal{M} \to \mathbb{Z}_q$, define different implementations.

- $\mathsf{Ver}(\mathsf{sk}, \mathsf{m}, ([\mathbf{t}], [u])) \to 0/1$:
  Check if $([\mathbf{t}], [u])$ satisfies Eq. $(*)$

PR-CMA Security

PR-CMA

- Decisional Variant of EUF-CMA.

Construction I: Naor-Reingold Approach

Ideas

- Randomized and affine version of Naor-Reingold PRF.
- Security from standard assumption: k-Lin.
- Generalized to any Matrix DH assumption [EHKRV13].

Construction I: Naor-Reingold Approach

Ideas

- Randomized and affine version of Naor-Reingold PRF.
- Security from standard assumption: k-Lin.
- Generalized to any Matrix DH assumption [EHKRV13].

$\mathsf{Tag}(\mathsf{sk}, \mathsf{m}) \xrightarrow{\$} \tau := ([\mathbf{t}], [u])$

$t \xleftarrow{\$} \mathbb{Z}_q^k, u = (\sum_{i=1}^{|\mathsf{m}|} \mathbf{x}_{i,\mathsf{m}_i}^\top)\mathbf{t} + x_0' \in \mathbb{Z}_q$

Construction I: Naor-Reingold Approach

Ideas

- Randomized and affine version of Naor-Reingold PRF.
- Security from standard assumption: k-Lin.
- Generalized to any Matrix DH assumption [EHKRV13].

$$\mathsf{Tag}(\mathsf{sk}, \mathsf{m}) \stackrel{\$}{\to} \tau := ([\mathbf{t}], [u])$$
$$t \stackrel{\$}{\leftarrow} \mathbb{Z}_q^k, u = (\sum_{i=1}^{|\mathsf{m}|} \mathbf{x}_{i,\mathsf{m}_i}^\top)\mathbf{t} + x_0' \in \mathbb{Z}_q$$

- Implicit in Chen-Wee13

✓ Tight Reduction

✗ Linear Size Parameters

Construction II: Hash Proof System Approach

Ideas

- [DKPW12] shows HPS implies EUF-CMA MAC.

Construction II: Hash Proof System Approach

Ideas

- This work shows k-Lin based HPS implies PR-CMA Affine MAC.

Construction II: Hash Proof System Approach

Ideas

- This work shows k-Lin based HPS implies PR-CMA Affine MAC.
- Security from standard assumption: k-Lin.
- Generalized to any Matrix DH assumption.

Construction II: Hash Proof System Approach

Ideas

- This work shows k-Lin based HPS implies PR-CMA Affine MAC.
- Security from standard assumption: k-Lin.
- Generalized to any Matrix DH assumption.

$\mathsf{Tag}(\mathsf{sk}, \mathsf{m}) \xrightarrow{\$} \tau := ([\mathbf{t}], [u])$

$t \overset{\$}{\leftarrow} \mathbb{Z}_q^{k+1}, u = (\mathbf{x}_0^\top + \mathsf{m} \cdot \mathbf{x}_1^\top)\mathbf{t} + x_0' \in \mathbb{Z}_q$

Construction II: Hash Proof System Approach

Ideas

- This work shows k-Lin based HPS implies PR-CMA Affine MAC.
- Security from standard assumption: k-Lin.
- Generalized to any Matrix DH assumption.

$\mathsf{Tag}(\mathsf{sk}, \mathsf{m}) \xrightarrow{\$} \tau := ([\mathbf{t}], [u])$

$t \overset{\$}{\leftarrow} \mathbb{Z}_q^{k+1}, u = (\mathbf{x}_0^\top + \mathsf{m} \cdot \mathbf{x}_1^\top)\mathbf{t} + x_0' \in \mathbb{Z}_q$

✗ Loose Reduction

✓ Constant Parameters.

RUB

Outline

Overview of Transformation to IBE

- $\mathsf{Gen}_{\mathsf{IBE}}(\mathsf{par})$:

$$\begin{aligned} \mathsf{sk}_{\mathsf{MAC}} &= \mathbf{x}_0, \ \ldots \ , \mathbf{x}_\ell, \ x'_0, \ \ldots \ , x'_{\ell'} \\ \mathsf{Rand} &= \mathbf{y}_0, \ \ldots \ , \mathbf{y}_\ell, \ \mathbf{y}'_0, \ \ldots \ , \mathbf{y}'_{\ell'} \end{aligned}$$

Overview of Transformation to IBE

- $\mathsf{Gen}_{\mathsf{IBE}}(\mathsf{par})$:

$$\begin{aligned}\mathsf{sk}_{\mathsf{MAC}} &= \boxed{\mathbf{x}_0}, \ \dots \ ,\mathbf{x}_\ell, \ x'_0, \ \dots \ ,x'_{\ell'} \\ \mathsf{Rand} &= \boxed{\mathbf{y}_0}, \ \dots \ ,\mathbf{y}_\ell, \ \mathbf{y}'_0, \ \dots \ ,\mathbf{y}'_{\ell'}\end{aligned}$$

$$\mathbf{z}_0 = \mathsf{Commit}(\mathbf{x}_0; \mathbf{y}_0)$$

Overview of Transformation to IBE

- $\mathsf{Gen}_{\mathsf{IBE}}(\mathsf{par})$:

$$\begin{array}{r} \mathsf{sk}_{\mathsf{MAC}} = \\ \mathsf{Rand} = \end{array} \begin{bmatrix} \mathbf{x}_0 \\ \mathbf{y}_0 \end{bmatrix}, \cdots, \begin{bmatrix} \mathbf{x}_\ell \\ \mathbf{y}_\ell \end{bmatrix}, \begin{bmatrix} x'_0 \\ \mathbf{y}'_0 \end{bmatrix}, \cdots, \begin{bmatrix} x'_{\ell'} \\ \mathbf{y}'_{\ell'} \end{bmatrix}$$

$$\mathsf{pk} := ([\mathbf{z}_i]_1, [\mathbf{z}'_i]_1)$$

- $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id}) \stackrel{\$}{\to} ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
  - $\mathbf{t}$ // Affine MAC
  - $u = \sum f_i(\mathsf{id})\mathbf{x}_i^\top \mathbf{t} + \sum f_i'(\mathsf{id})x_i'$ // Affine MAC
  - $\mathbf{v} = \sum f_i(\mathsf{id})\mathbf{y}_i \mathbf{t} + \sum f_i'(\mathsf{id})\mathbf{y}_i'$ // 'NIZK' Proof

- $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id}) \xrightarrow{\$} ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
    - $\mathbf{t}$
    - $u = F_{\mathbf{x}}(\mathsf{id}; \mathbf{t}) + F'_{x'}(\mathsf{id}; 1)$
    - $\mathbf{v} = F_{\mathbf{y}}(\mathsf{id}; \mathbf{t}) + F'_{\mathbf{y}'}(\mathsf{id}; 1)$

- USKGen(sk, id) $\xrightarrow{\$}$ $([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
  - $\mathbf{t}$
  - $u = F_{\mathbf{x}}(\mathsf{id}; \mathbf{t}) + F'_{x'}(\mathsf{id}; 1)$
  - $\mathbf{v} = F_{\mathbf{y}}(\mathsf{id}; \mathbf{t}) + F'_{\mathbf{y}'}(\mathsf{id}; 1)$
- Enc(pk, id, $[M]_T$) $\xrightarrow{\$}$ $([\mathsf{C}]_1, [\mathsf{K} \oplus M]_T)$
  - $\mathbf{s} \leftarrow \$$
  - $\mathsf{C} = F_{\mathbf{z}}(\mathsf{id}; \mathbf{s})$, $\mathsf{K} = F'_{\mathbf{z}'}(\mathsf{id}; \mathbf{s})$

- $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id}) \xrightarrow{\$} ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
  - $\mathbf{t}$
  - $u = F_{\mathbf{x}}(\mathsf{id}; \mathbf{t}) + F'_{x'}(\mathsf{id}; 1)$
  - $\mathbf{v} = F_{\mathbf{y}}(\mathsf{id}; \mathbf{t}) + F'_{\mathbf{y}'}(\mathsf{id}; 1)$
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{id}, [M]_T) \xrightarrow{\$} ([\mathsf{C}]_1, [\mathsf{K} \oplus M]_T)$
  - $\mathbf{s} \leftarrow \$$
  - $\mathsf{C} = F_{\mathbf{z}}(\mathsf{id}; \mathbf{s})$, $\mathsf{K} = F'_{\mathbf{z}'}(\mathsf{id}; \mathbf{s})$
- $\mathsf{Dec}(\mathsf{usk}[\mathsf{id}_1], \mathsf{C}[\mathsf{id}_2]) \rightarrow [M]_T$

If $\mathsf{id}_1 = \mathsf{id}_2$, the $F_*(\mathsf{id})$ will cancel out and leave $\mathsf{K} = F'_{\mathbf{z}'}(\mathsf{id}; \mathbf{s})$

RUB

Outline

Summary

IBE = Affine MAC + Pairings

Summary

IBE = Affine MAC + Pairings

✓ Proven under k-MDDH (e.g. k-Lin)

Summary

$$\text{IBE} = \text{Affine MAC} + \text{Pairings}$$

- ✓ Proven under k-MDDH (e.g. k-Lin)
- ✓ Tight Reduction:

$$\boxed{\text{MAC}_{\text{NR}}} + \text{'Pairings'}$$

- ✓ Compact Construction:

$$\boxed{\text{MAC}_{\text{HPS}}} + \text{'Pairings'}$$

Efficiency Comparison

Tight Schemes

SXDH	$\lvert pk \rvert$	$\lvert usk \rvert$	$\lvert C \rvert$	Loss
CW13	$4\lambda + 3$	4	4	$O(\lambda)$
$\mathsf{IBE}_{\mathsf{NR}}$	$2\lambda + 2$	3	3	$O(\lambda)$

Efficiency Comparison

Tight Schemes

SXDH	|pk|	|usk|	|C|	Loss
CW13	$4\lambda + 3$	4	4	$O(\lambda)$
$\mathsf{IBE}_{\mathsf{NR}}$	$\lambda + 3$	3	3	$O(\lambda)$

Efficiency Comparison

Tight Schemes

SXDH	|pk|	|usk|	|C|	Loss
CW13	$4\lambda + 3$	4	4	$O(\lambda)$
$\mathsf{IBE}_{\mathsf{NR}}$	$\lambda + 3$	3	3	$O(\lambda)$

Compact Schemes

SXDH	|pk|	|usk|	|C|	Loss
CLL[+]12	9	4	4	$O(Q)$
JR13	7	5	4	$O(Q)$
$\mathsf{IBE}_{\mathsf{HPS}}$	7	4	4	$O(Q)$

Extension and Open Problem

Extension

- Tight Signatures,

Extension and Open Problem

Extension

- Tight Signatures,
- Anonymity,

Extension and Open Problem

Extension

- Tight Signatures,
- Anonymity,
- HIBE,

Extension and Open Problem

Extension

- Tight Signatures,
- Anonymity,
- HIBE,
- ID-HPS.

Extension and Open Problem

Extension

- Tight Signatures,
- Anonymity,
- HIBE,
- ID-HPS.

Open Problem

Affine MAC with Tight Security and constant-size sk

Thank you!

- Full version: eprint 2014/581