A Schnorr-like Lightweight Identity-Based Signature Scheme

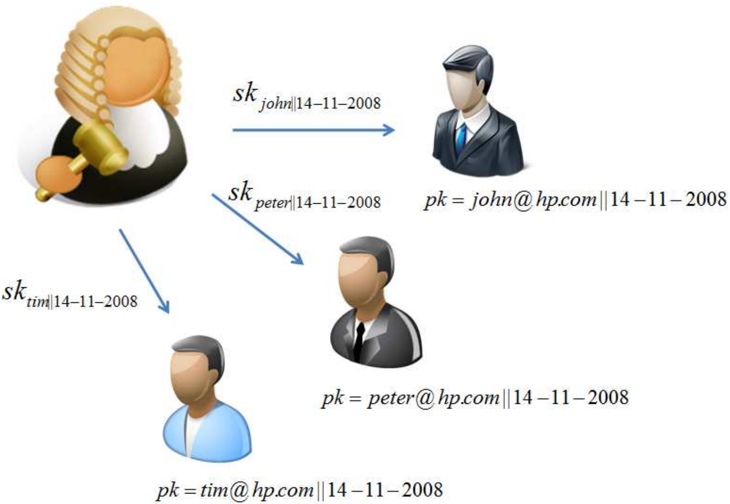
Flavio D. Garcia

Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands.

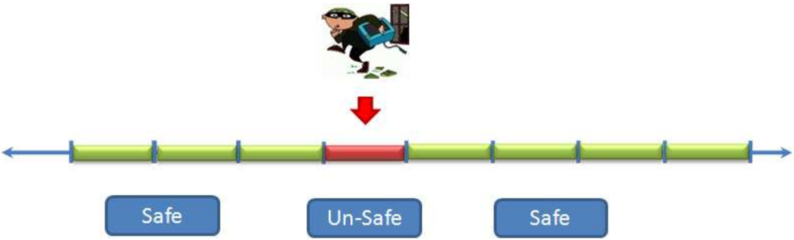
Joint work with: David Galindo

Outline

Identity Based Cryptography



Forward and Backwards Security



Identity Based Cryptography

Pros

- You can remember the public key
- Identities are smaller than PKI certificates
- Forward (and Backwards) security 'for free'
- no need of PKI certificates

Cons

- Key escrowed (horrible)
- Traditionally very expensive computation due to pairings

Identity Based Signatures

Identity Based Signatures

$$\longrightarrow \quad ({\color{red}\mathsf{mpk}}, \mathsf{msk}) \leftarrow \mathcal{G}(1^\eta)$$

$\uparrow$

public

Identity Based Signatures

$$\longrightarrow \quad (\textcolor{red}{\mathsf{mpk}}, \mathsf{msk}) \leftarrow \mathcal{G}(1^\eta)$$

$\uparrow$

public

$$\mathsf{sk}_{\mathsf{id}} \leftarrow \mathcal{E}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$$

$\mathsf{sk}_{\mathsf{id}} \downarrow$

Identity Based Signatures

$$\longrightarrow \quad ({\color{red}\mathsf{mpk}}, \mathsf{msk}) \leftarrow \mathcal{G}(1^\eta)$$

$\uparrow$

public

$$\mathsf{sk}_{\mathsf{id}} \leftarrow \mathcal{E}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$$

$\mathsf{sk}_{\mathsf{id}} \downarrow$

$$\sigma \leftarrow \mathcal{S}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, m)$$

Identity Based Signatures

$\longrightarrow$ $(\textcolor{red}{\mathsf{mpk}}, \mathsf{msk}) \leftarrow \mathcal{G}(1^\eta)$

$\uparrow$

public

$\mathsf{sk}_{\mathsf{id}} \leftarrow \mathcal{E}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$

$\mathsf{sk}_{\mathsf{id}} \downarrow$

$\xrightarrow{\sigma}$

$\sigma \leftarrow \mathcal{S}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{id}}, m)$

$\{0,1\} \leftarrow \mathcal{V}(\mathsf{mpk}, \sigma, m, \mathsf{id})$

Identity Based Signatures

Definition (EUF-IBS-CMA Security)

$\Sigma = (\mathcal{G}, \mathcal{E}, \mathcal{S}, \mathcal{V})$ is said to be secure against existential forgery on adaptively chosen message and identity attacks if for all PPTA $\mathcal{A}$, the probability $\mathbb{P}[\textbf{EUF-IBS-CMA}_\Sigma(\mathcal{A}) = 1] < \mathsf{negl}(\eta)$.

$$\boxed{\begin{array}{l} \textbf{EUF-IBS-CMA}_\Sigma(\mathcal{A}): \\ (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathcal{G}(\eta) \\ (\mathsf{id}^\star, m^\star, \sigma^\star) \leftarrow \mathcal{A}^{\mathcal{E}(\cdot), \mathcal{S}(\cdot,\cdot)}(\mathsf{mpk}) \\ \textbf{return } \mathcal{V}(\mathsf{mpk}, \sigma^\star, m^\star, \mathsf{id}^\star) \end{array}}$$

where $\mathsf{id}^\star$ and $(\mathsf{id}^\star, m^\star)$ are not queried to $\mathcal{O}_\mathcal{E}(\cdot)$ and $\mathcal{O}_\mathcal{S}(\cdot,\cdot)$

The Construction

$$\longrightarrow \quad (\text{mpk}, \text{msk}) = ((<\mathcal{G}, g, q>, G, H, g^z), z)$$

H, G are hash functions

$\longrightarrow \quad (\mathsf{mpk}, \mathsf{msk}) = ((<\mathcal{G}, g, q>, G, H, g^z), z)$

$\mathcal{E}(\mathsf{mpk}, z, \mathsf{id})$:
$r \leftarrow \mathbb{Z}_q$;
$c = H(g^r, \mathsf{id})$;
$y = r + z \cdot c \mod q$;
return $\mathsf{sk}_{\mathsf{id}} = (y, g^r)$;

H, G are hash functions

$\mathsf{sk}_{\mathsf{id}} \downarrow$

$$\longrightarrow \quad (\mathrm{mpk}, \mathrm{msk}) = ((<\mathcal{G}, g, q>, G, H, g^z), z)$$

H, G are hash functions

$\mathcal{E}(\mathrm{mpk}, z, \mathrm{id})$:

$r \leftarrow \mathbb{Z}_q$;

$c = H(g^r, \mathrm{id})$;

$y = r + z \cdot c \mod q$;

return $\mathrm{sk}_{\mathrm{id}} = (y, g^r)$;

$\mathrm{sk}_{\mathrm{id}} \downarrow$

$\mathcal{S}(\mathrm{mpk}, (y, g^r), m)$:

$a \leftarrow \mathbb{Z}_q$;

$d = G(\mathrm{id}, g^a, m)$;

$b = a + y \cdot d$;

return $\sigma = (g^a, b, g^r)$

$\longrightarrow \quad (\mathrm{mpk}, \mathrm{msk}) = ((<\mathcal{G}, g, q>, G, H, g^z), z)$

$\mathcal{E}(\mathrm{mpk}, z, \mathrm{id})$:
- $r \leftarrow \mathbb{Z}_q$;
- $c = H(g^r, \mathrm{id})$;
- $y = r + z \cdot c \mod q$;
- **return** $\mathrm{sk}_{\mathrm{id}} = (y, g^r)$;

H, G are hash functions

$\mathrm{sk}_{\mathrm{id}} \downarrow$

$\xrightarrow{\sigma = (g^a, b, g^r)}$

$\mathcal{S}(\mathrm{mpk}, (y, g^r), m)$:
- $a \leftarrow \mathbb{Z}_q$;
- $d = G(\mathrm{id}, g^a, m)$;
- $b = a + y \cdot d$;
- **return** $\sigma = (g^a, b, g^r)$

$\mathcal{V}(\mathrm{mpk}, \sigma, m, \mathrm{id})$:
- $c = H(g^r, \mathrm{id})$;
- $d = G(\mathrm{id}, g^a, m)$;
- **return** $g^b == g^a(g^r g^{zc})^d$

$$\longrightarrow \quad (\mathsf{mpk}, \mathsf{msk}) = ((<\mathcal{G}, g, q>, G, H, g^z), z)$$

H, G are hash functions

$\mathcal{E}(\mathsf{mpk}, z, \mathsf{id})$:
$r \leftarrow \mathbb{Z}_q$;
$c = H(g^r, \mathsf{id})$;
$y = r + z \cdot c \mod q$;
return $\mathsf{sk}_{\mathsf{id}} = (y, g^r)$;

$\mathsf{sk}_{\mathsf{id}} \downarrow$

$\sigma = (g^a, b, g^r)$
$\longrightarrow$

$\mathcal{S}(\mathsf{mpk}, (y, g^r), m)$:
$a \leftarrow \mathbb{Z}_q$;
$d = G(\mathsf{id}, g^a, m)$;
$b = a + y \cdot d$;
return $\sigma = (g^a, b, g^r)$

$\mathcal{V}(\mathsf{mpk}, \sigma, m, \mathsf{id})$:
$c = H(g^r, \mathsf{id})$; $\quad g^y$
$d = G(\mathsf{id}, g^a, m)$; $\quad ||$
return $g^b == g^a (g^r g^{zc})^d$

$\longrightarrow \quad (\mathrm{mpk}, \mathrm{msk}) = ((< \mathcal{G}, g, q >, G, H, g^z), z)$

H, G are hash functions

$\mathcal{E}(\mathrm{mpk}, z, \mathrm{id})$:
$r \leftarrow \mathbb{Z}_q$;
$c = H(g^r, \mathrm{id})$;
$y = r + z \cdot c \mod q$;
return $\mathrm{sk_{id}} = (y, g^r)$;

$\mathrm{sk_{id}} \downarrow$

$\sigma = (g^a, b, g^r)$
$\longrightarrow$

$\mathcal{S}(\mathrm{mpk}, (y, g^r), m)$:
$a \leftarrow \mathbb{Z}_q$;
$d = G(\mathrm{id}, g^a, m)$;
$b = a + y \cdot d$;
return $\sigma = (g^a, b, g^r)$

$\mathcal{V}(\mathrm{mpk}, \sigma, m, \mathrm{id})$:
$c = H(g^r, \mathrm{id})$;
$d = G(\mathrm{id}, g^a, m)$;
return $g^b == g^a \overset{g^y}{\overset{\parallel}{(g^r g^{zc})}}{}^d = g^a g^{yd}$

Theorem

Our construction is EUF-IBS-CMA secure in the random oracle model, if the group generation function Gen *generates discrete logarithm secure groups.*

Proof strategy.

Use a variant of the Forking lemma [BN06], the Multiple-Forking lemma by [BPW03] . $\square$

Efficiency Comparison by category

Factoring-based

Little chance due to large key lengths.

Efficiency Comparison by category

Factoring-based

Little chance due to large key lengths.

ECDL-based

Our scheme is the most efficient in signature size, signing and verification cost.

Efficiency Comparison by category

Factoring-based

Little chance due to large key lengths.

ECDL-based

Our scheme is the most efficient in signature size, signing and verification cost.

Pairing-based

Most efficient implementations due to Herranz and Barreto et al. (Comparison in the next slide)

Comparison with most efficient Pairing-based Schemes

Scheme	Signature size	Sign	Verify
Schnorr-like	768 b	1 $\exp_{\mathcal{G}_1}$	1.5 $\exp_{\mathcal{G}_1}$
Barreto et al.	512 b	1 $\exp_{\mathcal{G}_2}$ + 1 $\exp_{\mathcal{G}_T}$	$\geq$ 23 $\exp_{\mathcal{G}_1}$
Herranz	512 b	$>$ 1 $\exp_{\mathcal{G}_1}$	31 $\exp_{\mathcal{G}_1}$

Conclusions

- Our scheme has the smallest computational complexity
- Slightly larger signatures (256 bits larger (maybe 128))
- Secure in the random oracle model
- Standard Computational Diffie-Hellman assumption
- Our construction avoids the heavy code machinery needed for pairing-based schemes
- Suitable for resource constrained devices

References

[1] David Galindo and Flavio D. Garcia. A Schnorr-like lightweight identity-based signature scheme. In Bart Preneel, editor, *Progress in Cryptology (AFRICACRYPT 2009)*, volume 5580 of *Lecture Notes in Computer Science*, pages 135–148. Springer Verlag, 2009.