MMU
MULTIMEDIA UNIVERSITY

Faculty of Engineering (FOE)
Cyberjaya, Malaysia

Inquire, Inspire and Innovate

Reset Secure Identity-Based Identification Schemes without Pairing

Ji-Jian Chin, Hiroaki Anada Syh-Yuan Tan

ISIT

A TM University

Direction and Motivations

- Cryptography: the art and science of concealing information (Handbook of Cryptography).
- Goals:

1. Confidentiality
2. Integrity
3. Authentication
4. Non-repudiation

- 2 main settings:

1. Symmetric key: parties need to share a common key
2. Asymmetric key (public key crypto): parties don't have to share a common key

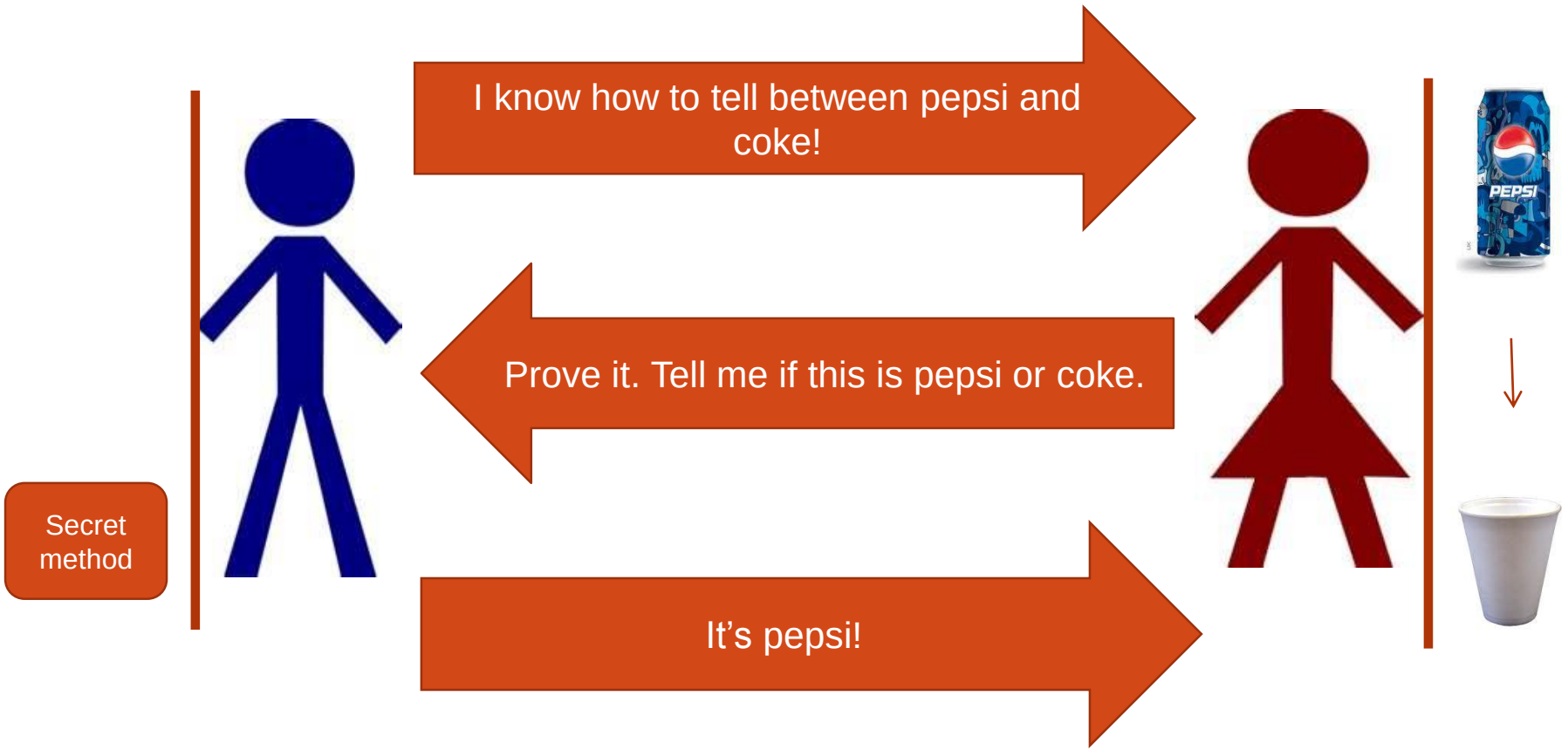
Proving Yourself - Identification Scheme

- **Scenario:** Peggy wants to prove her identity electronically to Victor. If Victor could learn Peggy's identifying information, Victor could impersonate Peggy.

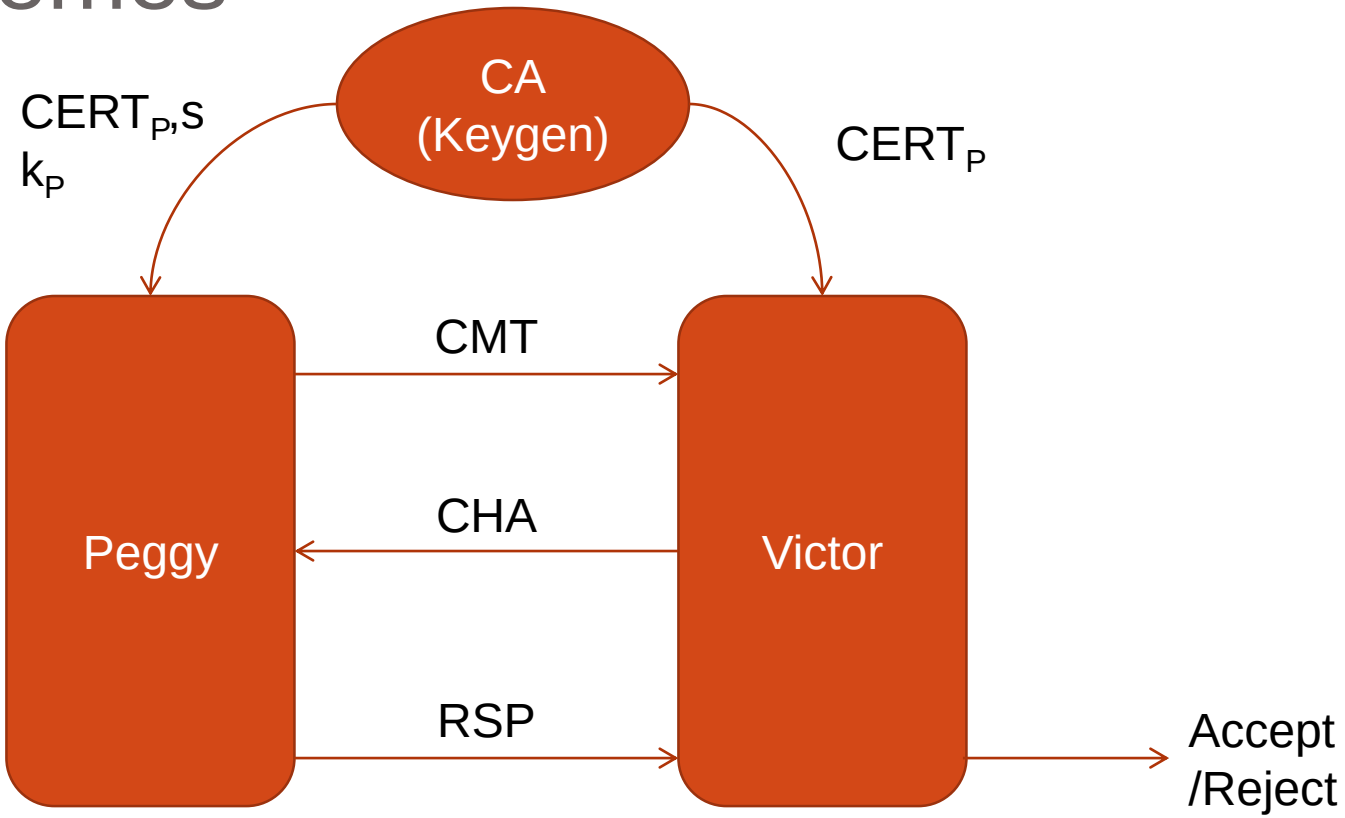
- An identification scheme is a protocol for one to prove her identity electronically without "giving away" her identifying information.
- First developed by Amos Fiat and Adi Shamir in 1986.
- A parallel zero knowledge proof of knowledge.
- Traditional identification schemes use certificates just like encryption and signature schemes to bind entities to their public keys.
- Some examples: FS, FFS, GQ, Schnorr schemes

Example of zero-knowledge

Zero-Knowledge Protocol Example:



Proving Yourself - Identification Schemes



Peggy wants to prove to Victor she is Peggy. They first obtain Peggy's public key through the CA.

1. Peggy sends Victor her commitment.
2. Victor challenges her with a random challenge.
3. Peggy sends her response.
4. Victor checks to see if her response is valid, accepts if it is, or rejects if it isn't.

Certificates work fine and are easy to manage when users are few in number, but incurs increasing overhead costs to manage and operate when number of users grow large.

Identity-Based Cryptography

- Introduced by Shamir in 1984.
- Also known as ID-based cryptography.
- First ID-based signature introduced in the 1984 paper.
- First ID-based encryption scheme only done by Boneh and Franklin in 2001.
- Main feature: public key of user is derived from a user's identity.
- First ID-based identification model and schemes introduced and formalized in 2004 independently by:
  - Kurosawa and Heng
  - Bellare, Namprempre and Neven

Pioneers - Transformations to IBI Schemes

Kurosawa and Heng (2004)

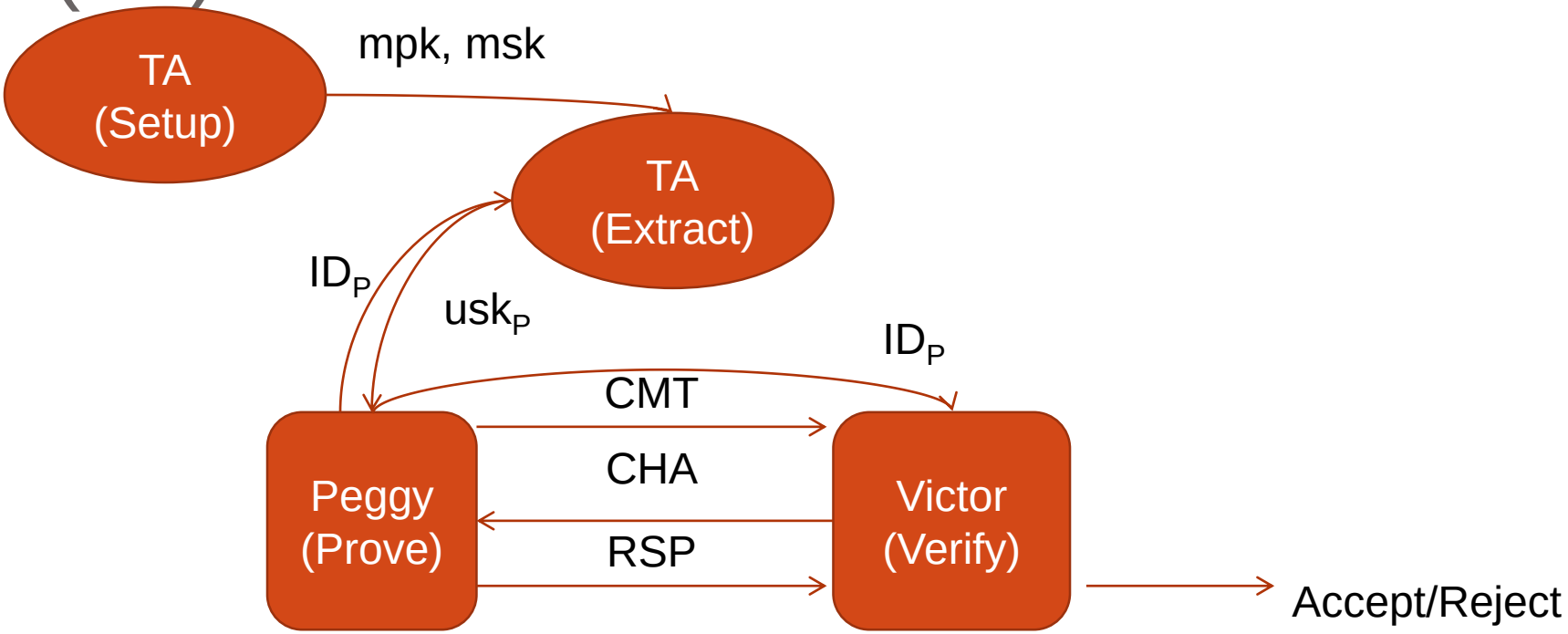
- Transform any digital signature with the following a canonical zero-knowledge interactive proof system on knowledge of signatures which satisfies:

a) Completeness
b) Soundness
c) Zero-knowledge

Bellare, Namprempre and Neven (2004)

- Transform any traditional identification scheme whose key generation process is underlain by a family of trapdoor samplable relations into an identity-based identification scheme.

Identity-Based Identification Scheme (IBI)



IBI=(Setup,Extract,Prove,Verify)
4 probabilistic, polynomial-time algorithms

The trusted authority generates the system parameters and master secret key in Setup. Using this master secret key, he then generates the user secret key for Peggy, which will be used in the identification protocol Prove and Verify when proving herself to Victor.

Reset Attacks

- Bellare et al. (2000) posturized the reset attack, where attacker can capture a user's smart card and change it to any state it is in.
- 3-move Σ-protocols are naturally insecure against reset-attacks due to the soundness property.
- Using the same commitment, an reset attacker can reset the prover (smart card) to a
- Practically it can be defended against during implementation. However we are still interested in securing the protocol with provable security.

Example: Schnorr Identification

Keygen
$g \leftarrow G, x \leftarrow Z_q, X = g^x$
$pk: (G, q, g, X), sk = x$

Prover	Channel	Verifier
$y \leftarrow Z_q, Y = g^y$	$\xrightarrow{Y}$	
	$\xleftarrow{c}$	$c \leftarrow Z_q$
$z = y + cx$	$\xrightarrow{z}$	Accept if $g^z = YX^c$

Reset Attack

Prover	Channel	Verifier
$y \leftarrow Z_q, Y = g^y$	$\xrightarrow{Y}$	
	$\xleftarrow{c_1}$	$c_1 \leftarrow Z_q$
$z_1 = y + c_1 x$	$\xrightarrow{z_1}$	Reset to Σ_2
	$\xleftarrow{c_2}$	$c_2 \leftarrow Z_q$
$z_2 = y + c_2 x$	$\xrightarrow{z_2}$	$x = (z_1 - z_2)/(c_1 - c_2)$

Previous Work

- The only reset-secure scheme in literature is by Thorncharoensri et al. 2009.
- Scheme proposed using q-SDHP for CR1 attackers and 2-SDHP for CR2 attackers.
- However, some issues with correctness of the scheme, which affects the way the challenger in the proof is designed.
- Also, the scheme uses many components for usk (up to 6 for PA security and 8 for CR security) and uses bilinear pairings.

Motivations

We seek:

- Faster, more efficient reset secure scheme alternatives.
- A method that can be applied generally to other 3-move IBI schemes in literature.
- Tighter proof of security rather than combining security advantages of 2 adversaries

Contributions

- Combination of PRF/Hash and trapdoor commitment scheme technique ala Bellare et al. 2000.
- 2 pairing-free schemes with security/efficiency tradeoff

a) RS-Schnorr-IBI: Less operations and parameters, but OMDL assumption

b) Twin-RS-Schnorr-IBI: slightly more operations and parameters, but DL assumption

- For PRF/Hash for prover coins, analysis done in 3 flavors – depending on necessity, i.e. via random oracle, PRF or regular hash function
- More concrete bounds for security: analysis taking into account advantage of TDC and PRF/Hash adversaries within impersonation game.

Trapdoor Commitment Scheme

- Cryptographic primitive which allows one to commit to a message and reveal it at a later date.
- 2 security properties:

1) Binding: the sender cannot change the message by altering the commitment
2) Hiding: other observers will not be able to observe the message from the commitment

- Additional trapdoor property for trapdoor commitment scheme: the sender can alter the message in the commitment only with the posession of the trapdoor.

Pedersen's Commitment Scheme

- We use Pedersen's commitment since it's DLOG:

Keygen
- Either receiver or PKG generates pk and sk.
$g \leftarrow G, a \leftarrow Z_q, h = g^a$
$pk: (G, q, g, h), sk = a$

Commit:
Sender commits to a message m. r is a generated nonce.
Commitment is calculated as $c = g^m h^r$

Reveal:
Sender reveals m, r.
Receiver accepts iff $c = g^m h^r$

Trapdoor:
With posession of a, the message can be altered from m to m' by calculating $r' = r + (m - m')a^{-1}$.

Pseudorandom/Hash Function

- A PRF is an efficiently computable function that maps a domain to a range, but is indistinguishable from a truly random function.
- We make use of a PRF to generate the prover's nonce based on the commitment from the TDC.
- For a less-secure but more efficient version, utilize a collision resistant hash function for the same purpose. Otherwise, model the hash function as a random oracle.

Augmentation of Σ –IBI with TDC

Prover	Channel	Verifier
	$\overset{c}{\leftarrow}$	$CHA = IBI_{\Sigma_2}, r \leftarrow \Delta,$ $c = TDC(r, CHA)$
$CMT = IBI_{\Sigma_1}(mpk, ID, H_2/PRF)$, where prover coins are determined via PRF on c.	$\overset{CMT}{\longrightarrow}$	
	$\overset{r,CHA}{\longleftarrow}$	Reveal r, CHA
Proceed with $RSP = IBI_{\Sigma_3}(usk, ID)$ iff $c = TDC(r, m)$	$\overset{RSP}{\longrightarrow}$	Accept iff $IBI_{\Sigma_{vrf}}(mpk, ID, CMT, CHA, RSP) = 1$

Security Model for RS-IBI

- A more powerful version of the imp-aa/ca attacker.
- Security model described as the following game between challenger C and impersonator I.

1) Setup phase : C generates system parameters and passes it to I. It keeps the master secret key to itself.
2) Learning phase: I issues oracle queries that C needs to answer: Extract queries, Identification queries, reset queries.
3) Impersonation phase: I outputs the challenge ID it wishes to impersonate and wins if it convinces C with non-negligible probability. For CR1, not more oracle queries. For CR2, I can still issue more queries.

Chronological Developments of Schnorr-IBI

- Schnorr-IBI proposed by Heng (2004) in Design and Analysis of Some Cryptographic Primitives (Thesis). Results were not published.
- Original Schnorr-IBI is passive secure, but active/concurrent security analysis relied on running protocol $\log_2 q$-times.
- Tan et al. (2009) modified Schnorr-IBI and tightened its security. Active/concurrent achieved using decisional Diffie-Hellman problem.
- Chin et al. (2014) applied a two-key technique previously used on Okamoto-IBI (Bellare et al. 2004) and k-resilient IBI (Chin et al. 2012) to Schnorr-IBI. Achieve active/concurrent security using only DLP with slight increase in operational cost compared to Tan et al.'s solution.

Schnorr-RS-IBI

- First scheme. Applies Pedersen commitment to Heng's 2004 scheme.
- Implicitly shows that Heng's 2004 scheme achieves imp-aa/ca using OMDL – a better security analysis.
- Scheme is secure against reset attacks if Pedersen's commitment is binding/hiding-secure and Heng's IBI scheme is imp-aa/ca secure.
- Main analysis in paper using random oracles.

Schnorr-RS-IBI Construction

Setup(1^k):		**Extract(ID)**
$g \leftarrow G, a \leftarrow Z_q, \boldsymbol{h = g^a}, x \overset{\$}{\leftarrow} \boldsymbol{Z_q}, \boldsymbol{X = g^{-x}}$ $\boldsymbol{H_1}: \{0,1\}^* \times \boldsymbol{G} \times \boldsymbol{G} \rightarrow \boldsymbol{Z_q}$ $\boldsymbol{H_2/PRF}: \{0,1\}^{pcl} \times \boldsymbol{G} \rightarrow \boldsymbol{Z_q}$ ***params:*** $(\boldsymbol{G, q, g, h, X, H_1, H_2/PRF})$ ***msk:*** $(\boldsymbol{x, a})$		$\tau \overset{\$}{\leftarrow} \boldsymbol{Z_q}, \boldsymbol{R = g^\tau}$ $\boldsymbol{\alpha = H(ID, R, X)}$ $\boldsymbol{s = \tau + x\alpha}$ ***usk:*** $(\boldsymbol{s, \alpha})$
Prove$(ID, params, usk)$		Verifier$(ID, params)$
	$\overset{c}{\leftarrow}$	$m, r \leftarrow Z_q, c = g^m h^r$
$y = H_2(\rho, c) \mid PRF(\rho, c)$ $Y = g^y, V = g^s X^\alpha$	$\overset{Y,V}{\rightarrow}$	
	$\overset{m,r}{\leftarrow}$	
$Proceed\ iff\ c = g^m h^r$ $z = y + cs$	$\overset{z}{\rightarrow}$	If $g^z = Y\left(\frac{V}{X^\alpha}\right)^c$ where $\alpha = H(ID, R, X)$output accept else reject.

Correctness:

$$Y\left(\frac{V}{X^\alpha}\right)^c = (g^y)\left(\frac{g^s X^\alpha}{X^\alpha}\right)^c = (g^y)(g^s)^c = g^{y+cs} = g^z$$

Twin-Schnorr-RS-IBI Scheme

- Twin-Schnorr-IBI was an effort to improve on original Schnorr-IBI security using Okamoto-IBI proof technique.
- Achieve active/concurrent security using only DLP with slight increase in operational cost compared to Tan et al.’s 2009 solution.

Twin-Schnorr IBI Construction

Setup(1^k):
$g_1, g_2 \leftarrow G, a \leftarrow Z_q, h = g^a$
$x_1, x_2, \overset{\$}{\leftarrow} Z_q, X = g_1^{-x_1} g_2^{-x_2}$
$H: \{0,1\}^* \times G \times G \rightarrow Z_q$, $H_2: \{0,1\}^{pcl} \times G \rightarrow Z_q$
params: $(G, q, g_1, g_2, X, h, H_1, H_2 | PRF_1, H_3 | PRF_2)$
msk: (x_1, x_2)

Extract(ID)
$r_1, r_2, \overset{\$}{\leftarrow} Z_q, R = g_1^{r_1} g_2^{r_2}$
$\alpha = H(ID, R, X)$
$s_1 = r_1 + x_1 \alpha$
$s_2 = r_2 + x_2 \alpha$
usk: (s_1, s_2, α)

Prove($ID, params, usk$)		Verifier($ID, params$)
	$\overset{c}{\leftarrow}$	$m, r \leftarrow Z_q, c = g^m h^r$
$y_1 = H_2(\rho, c) \| PRF_1 \rho, (c), y_2 = H_3(\rho, c) \| PRF\_2(\rho, c)$ $Y = g_1^{y_1} g_2^{y_2}, V = g_1^{s_1} g_2^{s_2} X^{\alpha}$	$\overset{Y,V}{\rightarrow}$	
	$\overset{m,r}{\leftarrow}$	$c \leftarrow Z_q$
Proceed iff $c = g^m h^r$ $z_1 = y_1 + cs_1, z_2 = y_2 + cs_2$	$\overset{z_1,z_2}{\rightarrow}$	If $g_1^{z_1} g_2^{z_2} = Y \left(\frac{V}{X^{\alpha}}\right)^c$ where $\alpha = H(ID, R, X)$output accept else reject.

Correctness:

$$Y \left(\frac{V}{X^{\alpha}}\right)^c = (g_1^{y_1} g_2^{y_2}) \left(\frac{g_1^{s_1} g_2^{s_2} X^{\alpha}}{X^{\alpha}}\right)^c = (g_1^{y_1} g_2^{y_2})(g_1^{s_1} g_2^{s_2})^c = g_1^{y_1 + cs_1} g_2^{y_2 + cs_2} = g_1^{z_1} g_2^{z_2}$$

Security Analysis for Schnorr-RS-IBI

Schnorr-RS-IBI is $Adv^{CR1}_{Schnorr-RS-IBI}$ – secure against impersonation under reset attacks if the OMDL problem is $Adv^{OMDL}_{M,G,q,DL}$ –hard where the Pedersen commitment scheme is $Adv^{Pedersen}_{I,q_I}$-secure, H_1 is modelled as a random oracle and the following settings are applied:

Setting	Advantage of Impersonator
Using Random Oracle for H_2	$Adv^{CR1}_{Schnorr-RS-IBI} \leq \sqrt{\frac{Adv^{OMDL}_{M,G,q,DL}(k)e(q_e+1)}{1-Adv^{Pedersen}_{I,q_I}(k)}}$
Using PRF	$Adv^{CR1}_{Schnorr-RS-IBI} \leq \sqrt{\frac{Adv^{OMDL}_{M,G,q,DL}(k)e(q_e+1)}{(1-Adv^{Pedersen}_{I,q_I}(k))(1-2^{\frac{k}{2}})}}$
Using Collision-Resistant Hash Function for H_2	$Adv^{CR1}_{Schnorr-RS-IBI} \leq \sqrt{\frac{Adv^{OMDL}_{M,G,q,DL}(k)e(q_e+1)}{(1-Adv^{Pedersen}_{I,q_I}(k))(1-2^{k})}}$

Security Analysis for Twin-Schnorr-RS-IBI

Twin-Schnorr-RS-IBI is $Adv^{CR1}_{Twin-Schnorr-RS-IBI}$ – secure against impersonation under reset attacks if the DL problem is $Adv^{DL}_{M,G,q,DL}$ –hard where the Pedersen commitment scheme is $Adv^{Pedersen}_{I,q_I}$-secure, H_1 is modelled as a random oracle and the following settings are applied:

Setting	Advantage of Impersonator
Using Random Oracle for H_2, H_3	$Adv^{CR1}_{Twin-Schnorr-RS-IBI} \leq \sqrt{\frac{Adv^{DL}_{M,G,q}(k)}{1 - Adv^{Pedersen}_{I,q_I}(k)}} + \frac{1}{q}$
Using PRF_1, PRF_2	$Adv^{CR1}_{Twin-Schnorr-RS-IBI} \leq \sqrt{\frac{Adv^{DL}_{M,G,q}(k)}{\left(1 - Adv^{Pedersen}_{I,q_I}(k)\right)(1-2^k)^2}} + \frac{1}{q}$
Using Collision-Resistant Hash Function for H_2, H_3	$Adv^{CR1}_{Twin-Schnorr-RS-IBI} \leq \sqrt{\frac{Adv^{DL}_{M,G,q}(k)}{\left(1 - Adv^{Pedersen}_{I,q_I}(k)\right)(1-2^k)^2}} + \frac{1}{q}$

Comparison with Other DL-RO IBI schemes' protocol

Scheme	Usk Components	Exponentiation	Multiplication in G	Multiplication in Z_q	IMP-AA/CA Security	IMP-CR1 Security
OKDL-IBI	3	8	5	2	DLP	Insecure
BNN-IBI	2	5	2	1	OMDLP	Insecure
Beth-IBI	2	4	2	3	Unknown	Insecure
Tight-Schnorr-IBI	2	6	3	1	DDHP	Insecure
Schnorr-IBI	2	6k	3k	k	DLP	Insecure
Twin-Schnorr-IBI	3	9	6	2	DLP	Insecure
Schnorr-RS-IBI	**3**	**8**	**5**	**1**	**OMDLP**	**OMDLP**
Twin-Schnorr-RS-IBI	**4**	**11**	**7**	**2**	**DLP**	**DLP**

Simulation

- Simulator constructed in Java, using java.security and java.math.BigInteger libraries.
- p=3072, q=256, using DSA FIPS 186-4 NIST standards.
- Simulation using hash SHA-256. Still looking for an efficient PRF instantiation.
- Run 100 iterations per algorithm on two separate machines. Time measured in milliseconds.

a) Machine 1 runs on Windows 7 64-bit with an Intel i5-4440 CPU at 3.10Ghz and 12GB RAM

b) Machine 2 is a Windows 7 32-bit machine running on an Intel i5 M450 CPU at 2.40Ghz and 2GB RAM.

Simulation Results

	Machine 1			Machine 2		
	Setup	Extract	Identification	Setup	Extract	Identification
Schnorr-IBI	15.138	0.450	0.893	68.225	0.786	3.594
Tight-Schnorr-IBI	23.784	0.407	0.899	130.637	1.328	4.586
Twin-Schnorr-IBI	24.175	0.591	1.030	139.483	3.535	5.044
RS-Schnorr-IBI	25.144	0.153	1.076	136.209	0.730	6.631
RS-Twin-Schnorr-IBI	26.937	0.819	1.754	149.343	3.962	7.729

Extension to CR2 Security

- CR2 adversaries can still make oracle queries in impersonation phase.
- To secure against CR2, use session IDs.
- Generate session IDs using Identity-based Pedersen Commitment.
- ID-based Pedersen: 3 generators - $g_1, g_2, g_3 \leftarrow G$. Given a message m, randomness r and session ID SID, commitment calculated as

$$c = \left(g_1^{SID} g_2\right)^m g_3^r$$

Conclusion

- Proposed 2 pairing-free IBI schemes secure against reset attacks in CR1 setting.
- Technique using Pedersen commitment scheme and PRF/Hash functions.
- For each scheme, 3 analysis depending on level of security required.
- Schemes are efficient since no pairings involved.
- For CR2 security, use ID-based Pedersen commitment instead.
- For future work, currently looking at extending simulator to work with mobile phone authenticators.

Thank you

Questions?

The authors thank the Ministry of Education, Malaysia for financial aid for this grant under the Fundamental Research Grant Scheme.
The first and third authors also thank Prof. Kouichi Sakurai for hosting their visits in 2014-2015 under the MMU-ISIT MoU.