Security Protocols to Prevent Malpractices of Summative E-examinations

Kissan G. Gauns Dessai
Goa University

Prof. V. V. Kamat
Research Guide,
Goa University.

Outline

- ❖ Summative Examination
- ❖ Threats & Security Requirements
- ❖ Research Problem
- ❖ Anonymity & enforced confidentiality in Summative E-Examination
- ❖ References

Summative Examination: Players and Organization

Summative examination form an integral part of any educational system.

Student

Examination Authority

Examiner

Three Roles:

Three Phases:

1. Pre-Conduct

2. Conduct

3. Post-Conduct

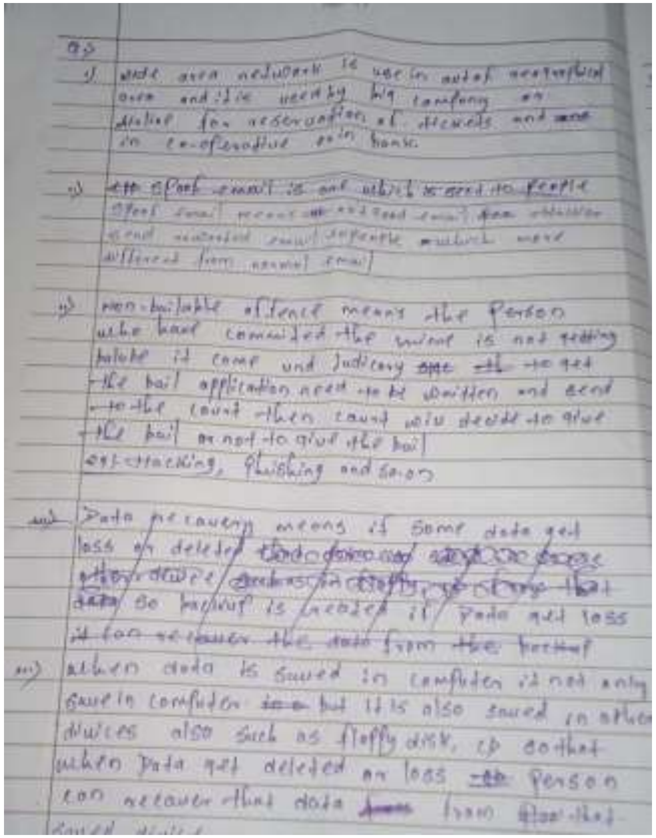
Summative Examination: Crucial Assets

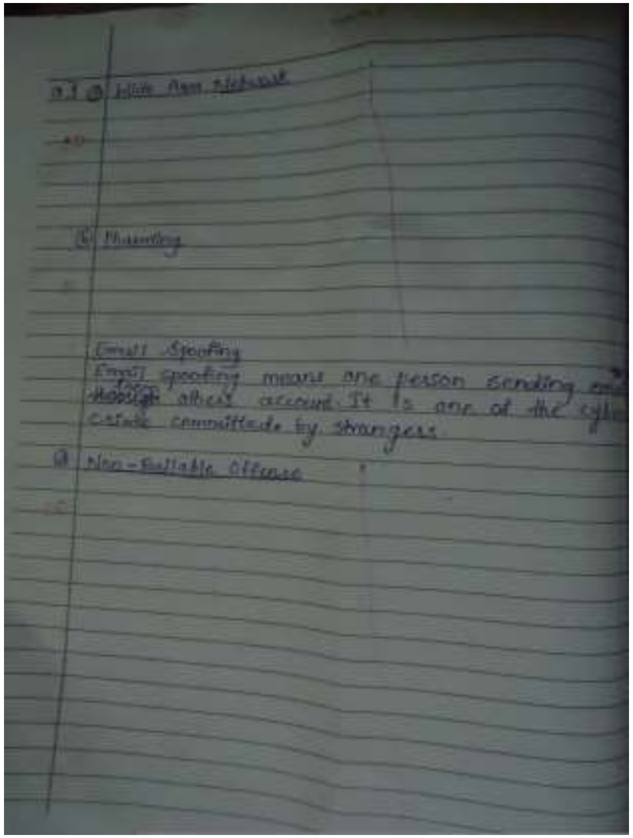
- Question Paper
- Answers-scripts

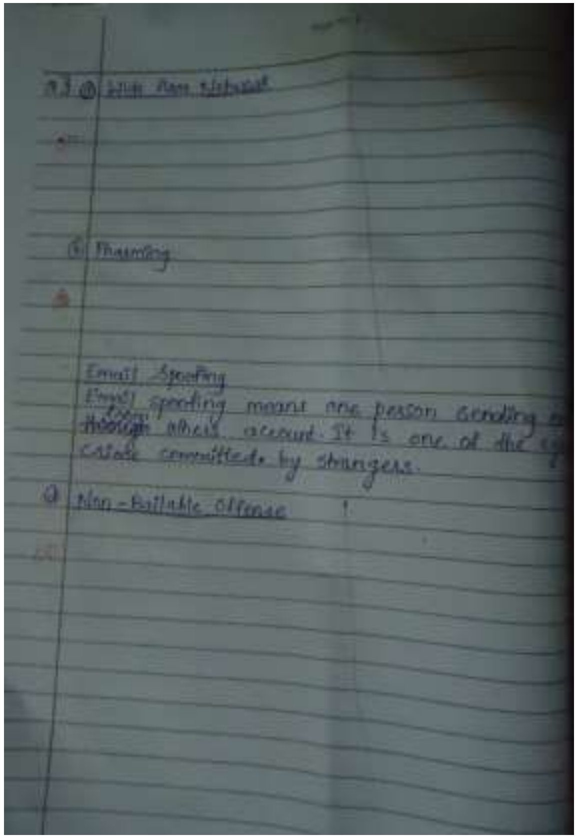
Threats. . .

- Question paper leakage
- Candidate cheating
- Bribed, corrupted or unfair examiners
- Dishonest/untrusted examination authority
- Outside attackers
- …

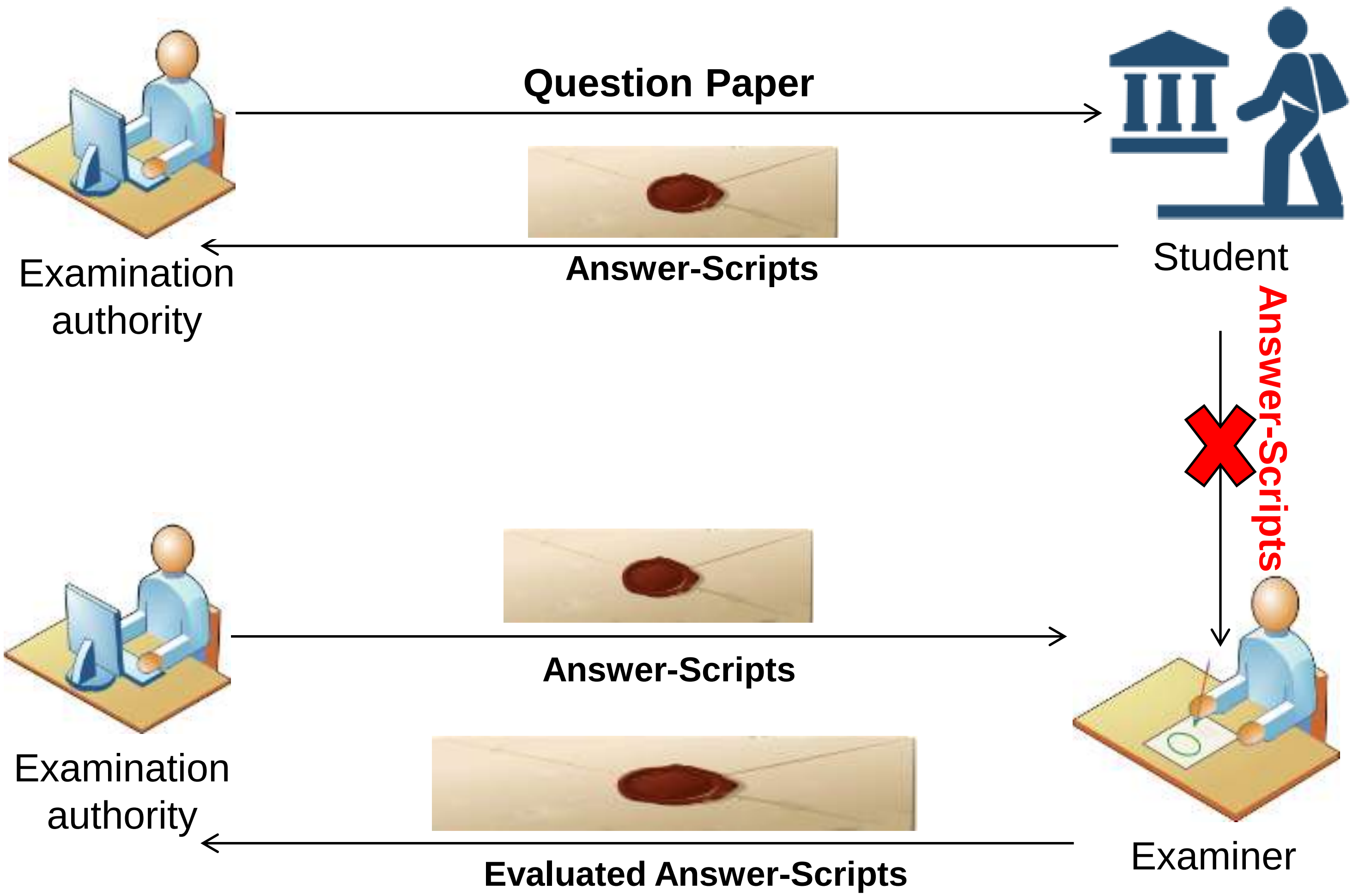
Threats




Q.3 (a) Wide Area Network
(b) Phishing
Email Spoofing
Email spoofing means one person sending
through others account. It is one of the
crime committed by strangers.
(d) Non-Bailable Offense


Q.3 (a) Wide Area Network
(b) Phishing
Email Spoofing
Email spoofing means one person sending
through others account. It is one of the
crime committed by strangers.
(d) Non-Bailable Offense

Typical Answers-scripts Delivery Process



Research Problem

Bind the **unique question paper** provided to the student with the **answer-script** produced by the student unambiguously s.t.

- Non-Repudiable Evidence
- Examiner Anonymity
- Student Anonymity
- Answer-script Secrecy

Security Requirements

Sr. No.	Requirement	Reason
1.	Ensure that at no stage shall the identity of the examiner be available to the student.	To prevent any attempt of the students from approaching examiners with illicit demands or threats.
2.	Ensure that at no stage shall the students identity be available to the examiner.	To prevent any dishonest acts of examiners, such as unfair evaluation, bribe demands etc.
3.	Ensure that at no stage shall the students answers-scripts be available to the examination authority.	Examination authority, do not have any role to play in the answers-script evaluation

Model

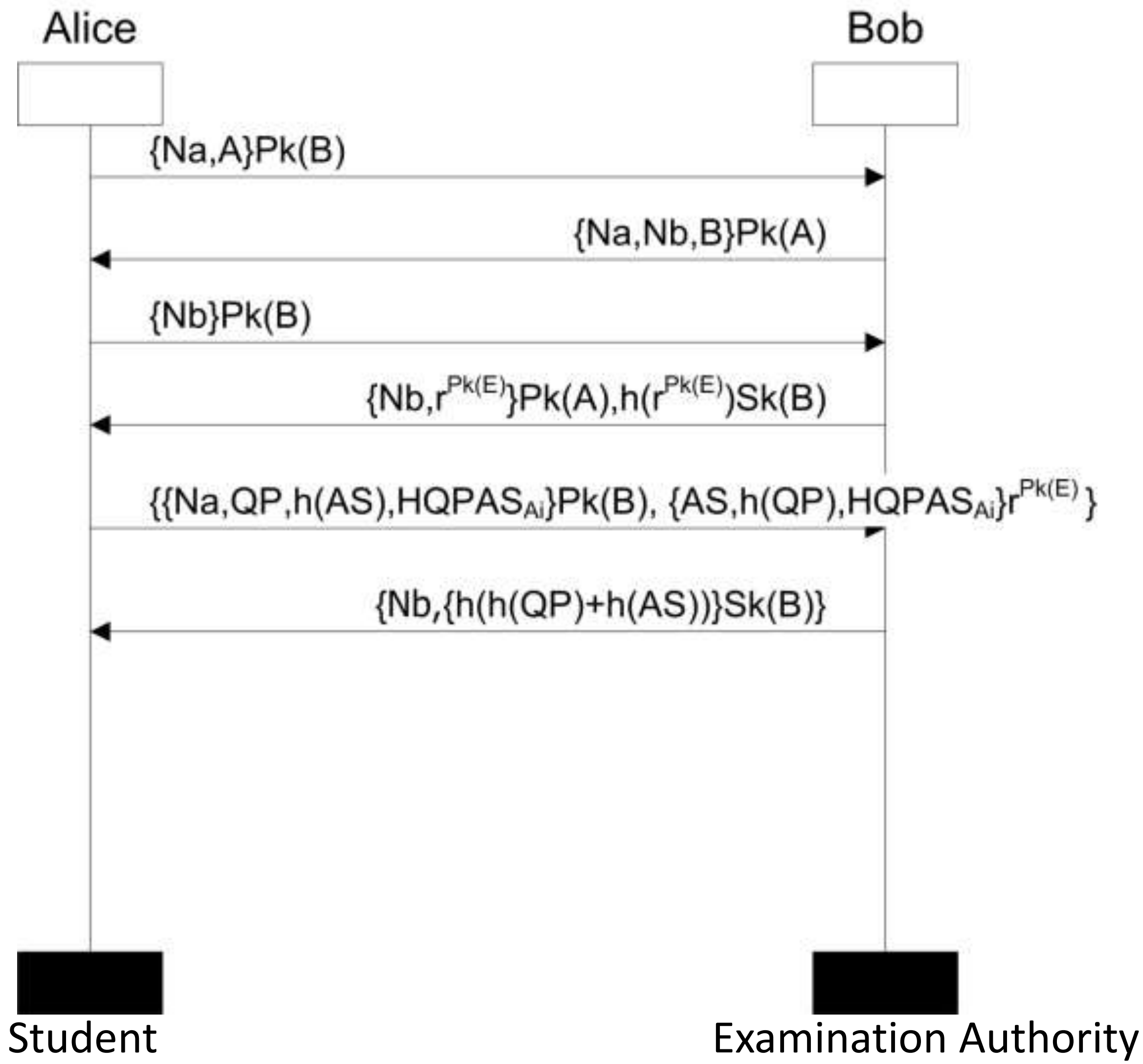
- Processes in the applied π calculus
- Annotated using events
- Privacy properties as **observational equivalence** between instances
- Automatic verification using **ProVerif**

Glossary of Notations

Glossary of notations

Notation	Description
$K_{A_i}, K_{A_i}^{-1}$	Public key and private key of an entity A_i
$K_{A_i}(m)$	Message m is encrypted using public key of entity A_i
$(c)K_{A_i}^{-1}$	Cipher text c is decrypted using private key of entity A_i

Protocol for Answer-scripts Delivery



Protocol for Answer-scripts Delivery using Hybrid Cryptosystem

2: Initially, B disguises the public key of examiner (X) as follows:

- 2.1: First, B select the public key K_X of X and choose a random number (r) to disguise the public key K_X as $(K_X * r)$.
- 2.2: B encrypt the disguised public key $(K_X * r)$ of X using public key K_{A_i} of A_i as $\{(K_X * r)\}K_{A_i}$.
- 2.3: B compute message digest of $(K_X * r)$ and sign it using private key K_B^{-1} of B.
- 2.4: B pairs disguised public key and message digest created in step 2.2 and 2.3 and send it to A_i.

Message 2: $B \rightarrow A_i : \{N_B, (K_X * r)\}K_{A_i}, \{\mathcal{H}(K_X * r)\}K_B^{-1}$

Reason: Sending blind public key of (X) to (A) serves two crucial objectives: It aids in hiding the identity of (X) from students (A) and assists in hiding the student answer-scripts from examination authority (B).

Protocol for Answer-scripts Delivery using Hybrid Cryptosystem

3: When A_i receives message 2 from B:

3.1: A_i decrypts message 2 to read $(K_X * r)$ and $\{\mathcal{H}(K_X * r)\}$.

3.2: A_i computes hash of $(K_X * r)$ and compares it with the message digest $\{\mathcal{H}(K_X * r)\}$ received from B.

3.3: If both hash values match protocol proceeds further.

3.4: Subsequently, A_i produce answer-script AS_{A_i} and compute the message digest $\mathcal{H}(AS_{A_i})$ of AS_{A_i}.

3.5: A_i generates a secret key S_{A_i} .

3.6: A_i encrypts AS_{A_i} using its secret key S_{A_i} and pairs the secret key S_{A_i} and $\mathcal{H}(S_{A_i})$ using disguised public key of examiner (X) send it to B.

Message 3: $A_i \rightarrow B : \{\{N_{A_i}, QP_{A_i}, \mathcal{H}(AS_{A_i}), \{HQPAS_{A_i}\}K_{A_i}^{-1}\}K_B, \{AS_{A_i}\}S_{A_i}, \{S_{A_i}, \mathcal{H}(S_{A_i})\}(K_X * r)\}$

Reason: By using the disguised public key the examination authority(B) is unaware of the answer-script AS_{A_i} of the student A_i(Examination authority only knows $H(AS_i)$.

Privacy Properties

- **Question Indistinguishability**: No premature information about the questions is leaked.
- **Answer-script Secrecy** – Answer-scripts are released only to the examiner for evaluation
- **Anonymous Marking:** An examiner cannot link an answer to a candidate.
- **Anonymous Examiner:** A candidate cannot know which examiner graded his copy.

Equational Theory

Equational Theory($\approx$)

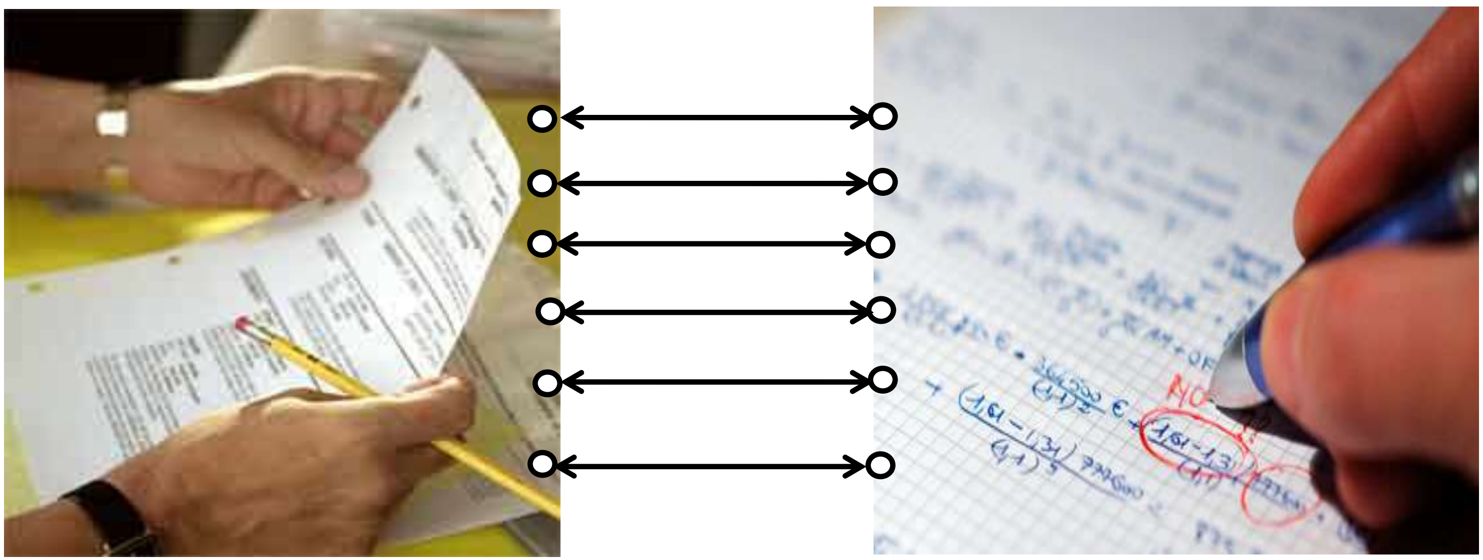
$fst(pair(x, y)) = x$ $\quad$ $snd(pair(x, y)) = y$

$adec(aenc(m, K_A), K_A^{-1}) = m$ $\quad$ $checksign(sign(m, K_A^{-1}), K_A) = m$

$unblind(blind(m, rbf), rbf) = m$ $\quad$ $unblind(sign(blind(m, rbf), K_A^{-1}), rbf) = sign(m, K_A^{-1})$

$$unblind(aenc(m, blind(K_E, rbf)), rbf) = aenc(m, K_E)$$

Associativity & Anonymity(1/5)



Inseparable bonding between Question Paper and Answer-Script

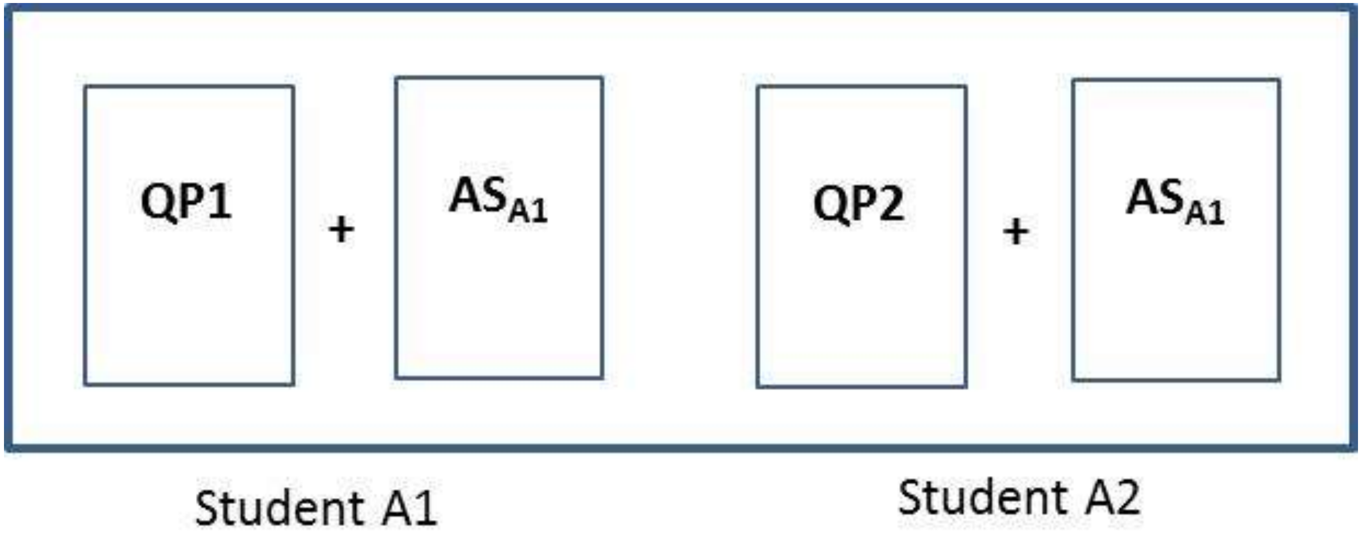
Associativity & Anonymity(2/5)

Question paper & Answer-script Associativity

An examination system with student process A (QP, AS, id) and examination authority process B offers question paper & answer-script associativity, if it is possible to unambiguously distinguish when a student A_1 produce answer-script AS_{A_2} corresponding to the received question paper QP_{A_1} from the case where examination authority/student claim of producing AS_{A_2} corresponding to altogether different question paper QP_{A_2}.

$$v\tilde{n}.(A\{QP_{A_1}/x, AS_{A_2}/y, A_1/z\}|B) \not\approx_l v\tilde{n}.(A\{QP_{A_2}/x, AS_{A_2}/y, A_1/z\}|B) \quad (1)$$

QP and AS Associativity



QP and AS Associativity

$\varphi_0 = \{pk(B)/v1\}|\{pk(A_i)/v2\}|\{pk(E_i)/v3\}|$
$\{hexKey = hide(pk(E_i), rf)\}|\{enc(QP_{Ai}, A_i)$
$|i = 1..n\},$

Initial knowledge of the communicating entities.

$\varphi_1 = \varphi_0|\{QP_{A1}/x, AS_{A2}/y\},$

Question paper answer-script pair submitted by the dishonest student.

$\varphi_2 = \{QP_{A2}/x, AS_{A2}/y\},$

Claim of the dishonest student after the completion of the examination

$\varphi_k = \{\varphi_{k-1}\}|\{sign(hash(hQP_{A1}hAS_{A2}), ssecST)\}|$
$\{hash(AS_{A2})|hash(hQP_{A1}hAS_{A2})|$
$\{enc((AS_{A2}, hash(QP_{A1})), hexKey)\}$
$\{enc((AS_{A2}, hash(QP_{A1})), pk(E_i)\},$

Knowledge of the examination authority/examiners

$\varphi_\delta = \varphi_n|\{dec(QP_{A1}, B)|\{dec(AS_{A2}, E_i))\}$

Final decryption of the received data.

QP and AS Associativity

- Dual signature ds = hash(hQPA1 hASA2) is signed by the student entity
- New claim of student is ds’ = hash(hQPA2 hASA2)
- It is unlikely that the two distinct question papers map to the same hash value

$\exists\, QP_{A_2}$ s.t. $\mathcal{H}(QP_{A_1}) = \mathcal{H}(QP_{A_2})$ and $\exists\, ds = ds'$

It is unlikely that the two distinct question papers map to the same hash value since

$QP_{A_1} \cap QP_{A_2} \neq \emptyset$

.

Since $(ds = cds)\phi$ and $(ds' \neq cds)\phi 1$, $\phi \not\approx_s \varphi 1$.

i.e., two frames ϕ and $\phi 1$ are statically not equivalent. This means that ϕ and $\phi 1$ are distinguishable to the dispute handling authority.

This holds true for any frame ϕ_i for $i > 0$.

Since, dispute handling authority is successful in distinguishing between original pair and altered pair, i.e, $P[QP_{A_1}/q1, ASA_2/a1] \not\approx P[QPA_2/q1, ASA_2/a1]$, we can conclude that ADAA protocol ensures Unambiguous Associativity between given QP and AS pair.

Associativity & Anonymity(3/5)

Answer-script Secrecy

An examination system with student process A (QP, AS, id) and examination authority process B offers an answer-script secrecy, if it is not possible for the examination authority to distinguish the answer-scripts received.

$$\nu\tilde{n}.(A\{AS_{A_1}/x, AS_{A_2}/y\}|B) \approx_l \nu\tilde{n}.(A\{AS_{A_2}/x, AS_{A_1}/y\}|B) \qquad (2)$$

Associativity & Anonymity(4/5)

Answer-script Anonymity

An examination system with examination authority process B (QP, AS, pseudo_id) and examiner process X, ensures answer-script anonymity, if it is not possible for the examiners to find the author of the answer-scripts from the received answer-scripts, i.e., student A_1 producing an answer-script AS_{A_1} is indistinguishable from student A_2 producing an answer-script AS_{A_2} .

$$v\tilde{n}.(B\{\{AS_{A_1}, pid_{A_1}\}, \{AS_{A_2}, pid_{A_2}\}\}|X) \approx_l v\tilde{n}.(B\{\{AS_{A_2}, pid_{A_1}\}, \{AS_{A_1}, pid_{A_2}\}\}|X) \quad (3)$$

References – E-Examination Security

1.	A. Huszti, A. Petho, **“A secure electronic exam system”**, Publicationes Mathematicae Debrecen 77 (3-4) (2010) 299-312.
2.	A. Shafarenko, D. Barsky, **“A secure examination system with multi-mode input on the world-wide web”:**, IEEE, 2000.
3.	E. R. Weippl, **“Security in e-learning”,** Vol. 16, Springer Science & Business Media, 2005.
4.	J. Castella-Roca, J. Herrera-Joancomarti, A. Dorca-Josa, **“A secure e-exam management system”**, in: The First International Conference on Availability, Reliability and Security, 2006. ARES 2006., IEEE, 2006.
5.	J. Dreier, R. Giustolisi, A. Kassem, P. Lafourcade, G. Lenzini, **“A framework for analyzing veriability in traditional and electronic exams”**, in: Information Security Practice and Experience, Springer, 2015, pp.514-529.
6.	K. M. Apampa, G. Wills, D. Argles, **“An approach to presence verification in summative e-assessment security”,** in: Information Society (i-Society), 2010 International Conference on, IEEE, 2010, pp. 647-651.

References – Formal Model

1.	Armando, Alessandro, Roberto Carbone, and Luca Compagna. **"LTL model checking for security protocols."** *Journal of Applied Non-Classical Logics* 19.4 (2009): 403-429.
2.	Basin, David, Cas Cremers, and Catherine Meadows. **"Model checking security protocols."** *Handbook of Model Checking* (2011).
3.	Basin, David, and Cas Cremers. **"Modeling and analyzing security in the presence of compromising adversaries."** *Computer Security–ESORICS 2010*. Springer Berlin Heidelberg, 2010. 340-356.
4.	Benerecetti, Massimo, and Fausto Giunchiglia. **"Model checking security protocols using a logic of belief."** *Tools and Algorithms for the Construction and Analysis of Systems*. Springer Berlin Heidelberg, 2000. 519-534.
5.	Kremer, Steve, and Mark Ryan**. "Analysis of an electronic voting protocol in the applied pi calculus."** *Programming Languages and Systems*. Springer Berlin Heidelberg, 2005. 186-200.
6.	T. Chothia. **“Modelling and Analysis of Security Protocols**”, Lecture Notes, **School of Computer Science**,University of Birmigham, available at:

References – Applied Pi Calculus (Applications)

1.	Backes, Michael, Catalin Hritcu, and Matteo Maffei. "**Automated verification of remote electronic voting protocols in the applied pi-calculus**." *Computer Security Foundations Symposium, 2008. CSF'08. IEEE 21st*. IEEE.
2	Dong, Naipeng, Hugo Jonker, and Jun Pang. "**Analysis of a receipt-free auction protocol in the applied pi calculus**." *Formal Aspects of Security and Trust*. Springer Berlin Heidelberg, 2011. 223-238
3.	Kremer, Steve, and Mark Ryan. **"Analysis of an electronic voting protocol in the applied pi calculus."** Programming Languages and Systems. Springer Berlin Heidelberg, 2005. 186-200.
4.	Luo, Zhengqin, et al. "**Analyzing an electronic cash protocol using applied pi calculus**." *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, 2007.
5.	Meng, Bo. **"Formal analysis of key properties in the internet voting protocol using applied pi calculus**." Information Technology Journal 7.8 (2008): 1130-1140.

References – Reachability and Indistinguishability

1.	Abadi, Martín, and Véronique Cortier. **"Deciding knowledge in security protocols under equational theories."** *Theoretical Computer Science* 367. (2006): 2-32.
2.	Abadi, Martin. **"Secrecy by typing in security protocols."** *Theoretical Aspects of Computer Software*. Springer Berlin Heidelberg, 1997.
3.	Amadio, Roberto M., and Denis Lugiez. **"On the reachability problem in cryptographic protocols."** *CONCUR 2000—Concurrency Theory*. Springer Berlin Heidelberg, 2000 . 380-394.
4.	Basin, David, Sebastian Mödersheim, and L. Vigano. **“An on-the-fly model-checker for security protocol analysis.”** Springer, Berlin Heidelberg, 2003.
5.	Baudet, Mathieu. **"Deciding security of protocols against off-line guessing attacks."** *Proceedings of the 12th ACM conference on Computer and communications security*. ACM, 2005.
6.	Blanchet, Bruno. **"Automatic proof of strong secrecy for security protocols."** ***Security and Privacy, 2004.*** *Proceedings. 2004 IEEE Symposium on*. IEEE, 2004.