MEMORANDUM ON RESEARCH AND COLLABORATION

THIS MEMORANDUM is made on 9 November 2008 between:

Katholieke Universiteit Leuven (K.U. LEUVEN), for the purposes of this MEMORANDUM represented by Professor dr. Marc Vervenne, Rector, and its department K.U. LEUVEN RESEARCH & DEVELOPMENT, having its office in 3000 Leuven, Minderbroedersstraat 8A box 5105, Belgium, VAT number BE 419 052173, represented by Professor dr. ir. Koenraad Debackere, Managing Director and Mr. Paul Van Dun, General Manager, acting upon request of Prof.dr.ir. Ingrid Verbauwhede, acting as member of the COSIC (Computer Security and Industrial Cryptography) research lab, hereinafter referred to as "K.U. LEUVEN R&D";

And

SETS (Society for Electronics Transactions and Security), for the purposes of this MEMORANDUM represented by Mr. S. Thiagarajan, Registrar, having its office in 600 034 Chennai, Nungambakkam, Mangadu Swamy Street, no. 21 (old. No. 11), Tamil Nadu, India, hereinafter referred to as "SETS";

which shall hereinafter be referred to individually as a "Party" and collectively as the "Parties".

RECITALS

WHEREAS the Parties wish to collaborate under the terms and conditions as set forth below to jointly develop secure and efficient software and hardware implementations of cryptographic algorithms and protocols (hereafter referred to as the Programme and as further described in Annex 1) and will make their respective Background available to the Programme under the terms and conditions of this agreement to realize the Programme Foreground.

WHEREAS the intention of this MEMORANDUM is to define the general framework under which the Parties shall undertake the Programme in accordance with their respective needs and capabilities.

WHEREAS the Parties, in this respect, wish to express their consent to certain principles laid down in this MEMORANDUM.

WHEREAS the Programme aims at but is not limited to the exchange of researchers, the performance of consulting services, the performance of training and support services, the conduct of joint research, the performance of collaborative Projects, etc.

WHEREAS SETS acknowledges the specific world-leading expertise held by K.U. LEUVEN R&D in the field of Side Channel Analysis (SCA) and is interested in receiving Background from K.U. LEUVEN R&D in the scope of the Programme whereby the conditions of SETS' use of such Background shall be agreed upon between the Parties in the present MEMORANDUM. The latter can be modified, completed or specified on a case-by-case basis by a separate research and collaboration agreement between the Parties.

WHEREAS, SETS' Background shall als be made available as deemed appropriate to K.U. LEUVEN R&D under the terms of this MEMORANDUM.

WHEREAS the Parties will make the Background listed under Annex 2 available to the extent needed for the due performance of the Programme at its own discretion.

WHEREAS in this respect no Party can be forced under the terms of this MEMORANDUM by the other Party to share its Background and no Party shall have to motivate any refusal to share Background.

WHEREAS K.U. LEUVEN R&D and SETS hereby undertake to act in good faith in order to determine the conditions of other future joint research collaboration.

WHEREAS the terms and conditions of this MEMORANDUM shall act as guidelines to the Parties in their negotiations to conclude separate agreements in view of performing specific projects allowing them to realize specific foreground to be agreed upon between the Parties.

THERETO the Parties agree as follows:

ARTICLE 1 - DEFINITIONS

- 1.1. "Codes" shall mean all Hardware and Software Codes, both in object code and in Source Code, enumerated in Annex 2 that are property of K.U. LEUVEN R&D or SETS as the case may be.
- 1.2. "Software" shall mean all Hardware and Software that is the property of K.U. LEUVEN R&D or SETS and that is enumerated in Annex 2.
- 1.3. "Background" is the property of a Party, as the case may be of K.U. LEUVEN R&D or SETS, and shall mean the full range of that Party's intellectual property rights and factual knowledge including but not limited to specifications, methods, practices and procedures in the field of SCA
 - i). existing on the Effective Date of this MEMORANDUM and/or
 - ii). developed by that Party outside of the Project but during the term of this MEMORANDUM and which that Party is free to dispose of.

For the avoidance of doubt Background includes, but is not limited to, all Codes, all Software and all Slides held by that Party on the date of entering into force of this MEMORANDUM.

A Party's Background shall comprehensively mean the range of factual knowledge, both existing and those that would be acquired by that Party outside the scope of this Memorandum, including specification methods, practices and proceedings in the field of SCA. It does not include any third party material of productivity and confidential in nature.

1.4 "Programme" means the collaboration the Parties shall set up in accordance with the provisions of this MEMORANDUM and in furtherance of the methods of collaboration set out under Annex 1 using the Codes and Software shared between the Parties enumerated in Annex 2.

ARTICLE 2 - RESEARCH AND COMPENSATION

- 2.1. The Parties shall perform collaborative research as described and agreed in Annex 1. All Parties shall use reasonable efforts to achieve the results of the Programme and provide the other Party with all data, materials and know-how in its possession that are necessary for the other Party to carry out their work under the Programme.
- 2.2. On a timely basis, the Parties shall agree upon a due compensation for each Party's contribution to the Programme and, when appropriate, shall conclude separate agreements specifying the financial aspects of the collaboration.

ARTICLE 3 - PUBLICATIONS

- 3.1. Parties agree that the results obtained through joint research and collaboration, shall be published upon appropriate co-authorship in accordance with academic customs.
- 3.2. Parties recognize that under their respective policies, the results obtained under this MEMORANDUM, in which SETS uses K.U. LEUVEN R&D Software and vice versa, the following shall be applicable. Each Party agrees that the other Parties' researchers shall be permitted to present and to publish the methods and results of each specific Project arising out of this Programme at symposia and professional meetings, in journals, theses or dissertations, or otherwise of their own choosing, subject to the provisions of this Article. With respect to said publications, Parties shall agree upon appropriate co-authorship in accordance with academic customs.
- 3.3. Each Party shall submit to the other Party, who shall accept in confidence, all intentions to publish or to otherwise disclose the methods and results of the Project in which K.U. LEUVEN R&D Software/SETS Software if any is used. The receiving Party shall report in writing within thirty (30) days if such Party is of the opinion that its IP-protection is likely to be prejudiced by the aforementioned publication or disclosure. In case of this prejudice, each Party may request to delay the publication or disclosure and may request to omit Confidential Information of such Party and/or to delay the publication or disclosure. Such delay shall sufficiently be motivated in writing and shall not exceed thirty (30) days, except if otherwise agreed between the Parties.
- 3.4. If appropriate, the Parties can agree otherwise on publication issues by concluding separate agreements.

ARTICLE 4 - CONFIDENTIALITY

- 4.1. For the purposes of this MEMORANDUM, the term "Confidential Information" means all proprietary information and materials (whether or not patentable) communicated to, learned of, developed or otherwise acquired by either Party in furtherance of this MEMORANDUM and further separate agreements, unless otherwise agreed, including the Software that is enumerated in Annex 2 and that is the property of the respective Parties.
- 4.2. The receiving Party shall maintain the Confidential Information in confidence, and shall not, without written permission from the disclosing Party, disclose, divulge or otherwise communicate such Confidential Information to others, except to employees, consultants and/or contractors who are bound by like terms of confidentiality.
- 4.3. The provisions of section 4.2 shall not apply to any Confidential Information of which the receiving Party can prove that:
- at the time a Party discloses it to a third party, it is generally known to the public through no fault of such Party; or
- at the time a Party discloses it to a third party, it has been made available to such Party by a third
 party having the lawful rights to do so without breaching any such obligation of non-use or
 confidentiality to any party to this MEMORANDUM; or
- it has been independently developed by the receiving Party; or
- the receiving Party is required to disclose it pursuant to an order of a judicial or administrative authority, provided the receiving Party promptly notifies the disclosing Party of such order to provide the disclosing Party sufficient time to contest such order.

ARTICLE 5 - INTELLECTUAL PROPERTY RIGHTS

- 5.1. Each Party shall remain the owner of its own Background and will be responsible for the commercial utilization, exploitation, patent prosecution and management thereof. Except as stated explicitly in this MEMORANDUM, this MEMORANDUM shall not grant or be construed as granting any rights by license or otherwise to the other PARTY.
- 5.2. For the avoidance of doubt, each Party shall remain the sole owner of the Hardware and Software Codes listed as proprietary to that Party in Annex 2. These Hardware and Software Codes shall be subject, when appropriate, to an exploitation agreement, whereby the Parties shall discuss a compensation to be paid by the using Party for such use and exploitation of these Hardware and Software Codes owned by the other Party.
- 5.3. Any improvements or alterations of the Hardware and Software Codes listed as proprietary to one Party in Annex 2 that are a result of the research activities of the other Party shall be jointly owned by the Parties (hereafter referred to as "Jointly Owned Results"). Parties will designate in good faith the Party that shall manage the exploitation in a certain territory and domain of application. Parties shall agree on appropriate ways to protect jointly owned Results by ways of patenting, where appropriate.
- 5.4. The Party that shall manage the exploitation of the Jointly Owned Results. shall collect and distribute any and all revenues accrued from the exploitation of such Jointly Owned Results, which distribution shall equal the ratio of ownership in such Jointly Owned Results.
- 5.5. It is agreed that any license agreement granted by a Party in respect of the Jointly Owned Results shall only be made with a third party in consultation with the other Party. Such a license agreement shall contain, inter alia:
- the terms securing the full indemnification and holding harmless the PARTY, and those employed by them from and against any claim, damage, expense of any kind resulting from any use of the licensee or those authorised by him may make of such invention or other licensed information;
- a disclaimer as to any representations or warranties in respect of such invention, its potential, use, exploitability and/or that it does not infringe third party's rights; specific undertakings of commercialization.

ARTICLE 6 - SOFTWARE LICENSE

- 6.1. In the framework of this MEMORANDUM, each Party hereby grants to the other Party a non-exclusive and non-transferable license, without the right to grant sub-licenses, to use the executable code of the software enumerated in Annex 2 as proprietary to the sharing Party (the "Software"), subject to the terms and conditions of this MEMORANDUM and any other separate agreement and with the sole purpose of the experimental research in the Project. Each Party will deliver to the other Party the executable modules of the Software, which will have to be accepted by the other Party. Each Party will accept the other Party's Software "as is". No support or maintenance services have to be rendered by any Party to the other Party under this MEMORANDUM, unless otherwise agreed upon between the Parties.
- 6.2. Each Party shall utilize the other Party's Software solely in the framework of the Programme or specific project as agreed in this MEMORANDUM or in a separate agreement. No Party shall in any case seek or have any person or corporate body seeking any commercial use of the other Party's Software, unless explicitly agreed upon in this MEMORANDUM or in a separate agreement.

6.3. No Party shall transmit by any means whatsoever all or part of the Software listes as proprietary to the other Party in Annex 2 to any third party without the prior and written consent of said other Party. K.U. LEUVEN R&D and SETS shall confer a fair return for K.U. LEUVEN R&D in due time whenever applicable. This also applies to K.U. LEUVEN if SETS know-how is involved.

ARTICLE 7 - LIABILITY

- 7.1. Each Party agrees to indemnify, defend and hold harmless the other Party and its directors, employees, researchers and students against any and all claims of or liabilities to third parties, including fees, expenses and costs of claims and suits for any such third parties loss, damage, injury, or loss of life, if such claims or liabilities arise directly or indirectly from the omission or performance of the indemnifying Party's rights or obligations arising out of this MEMORANDUM.
 - The indemnifying Party is released from this obligation as far as the aforementioned is caused by gross negligence or malicious intent of the other Party or any of its employees and researchers.
- 7.2. Subject to section 7.1, a Party shall not be liable against the other Party for any damages or loss or loss of profit in connection with this MEMORANDUM unless this is caused by gross negligence or malicious intent of that Party Party, its licensees or any of its directors, employees, researchers or students.
- 7.3. For further specific projects, the Parties can decide to abide by other provisions on liability, which shall in such case be detailed in the separate agreement signed in view of that specific project. In case no other provisions are mentioned in the specific agreement, the provisions of the present MEMORANDUM shall apply.

ARTICLE 8 - VISITING RESEARCHERS

8.1. Each Party shall be able to let their researchers work under the Programme on the premises of the Other Party. The Parties agree that with each visiting researcher under this Programme they will enter into a separate agreement in accordance with Annex 3 ("Visiting Researcher Agreement").

Annex 3 is a Visiting Researcher Agreement for an employee of SETS who is sent to K.U. LEUVEN R&D as a visiting researcher. When an employee of K.U. LEUVEN R&D will be sent to SETS as a visiting researcher the Visiting Researcher Agreement of Annex 3 will hold good in the same way. In such case, the clauses of the Visiting Researcher Agreement shall remain unaltered, unless agreed otherwise.

ARTICLE 9 - TERM AND TERMINATION

- 9.1. This MEMORANDUM will become effective upon signature of this MEMORANDUM on 9 November 2008 ("Effective Date").
- 9.2. If either Party fails to observe and perform any promise herein contained, and, where such failure is remediable, fails to remedy the non-observance or non-performance within 30 days of a written notice from the aggrieved Party to do so, then the aggrieved Party may forthwith (or where the aggrieved Party has given a notice as aforesaid, on expiry thereof un remedied) give a written notice that the other Party's rights under this MEMORANDUM are at an end and that the MEMORANDUM itself shall be considered as duly terminated.



9.3. Unless otherwise terminated by operation of law or by acts of the Parties in accordance with the terms of section 9.2 of this MEMORANDUM, it shall be in full force from the Effective Date and shall remain in force for an initial period of five (5) years. Termination or cancellation of this MEMORANDUM shall not affect the rights and obligations of the Parties accrued prior to termination

ARTICLE 10 - FORCE MAJEURE

Neither Party shall be liable for any unforeseeable event beyond its reasonable control not caused by the fault or negligence of such Party, which causes such Party to be unable to perform its obligations under this MEMORANDUM, and which it has been unable to overcome, by the exercise of due diligence. In the event of the occurrence of such force majeure event, the Party unable to perform shall promptly notify the other Party. It shall further use its best efforts to resume performance as quickly as possible and shall suspend performance only for such period of time as is necessary as a result of the force majeure event.

ARTICLE 11 - MISCELLANEOUS

- 11.1. No License. All Parties remain the owner of their respective background information. This MEMORANDUM does not confer by implication, or otherwise any license or other rights under any patents, patent applications, trade secrets or other proprietary rights of either party.
- 11.2. Survivability. Upon termination of this MEMORANDUM, the following articles shall remain in full force and effect: 3, 4, 5, 7 and 11.
- 11.3. Severability. If any provision of this MEMORANDUM shall be held invalid, illegal, or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired thereby, provided that the intent of the Parties in entering into the MEMORANDUM is not materially affected thereto.
- 11.4. Notices. Any notice with legal or administrative character required or permitted to be given to the Parties hereto is properly given if delivered, in writing, in person, sent by first-class certified mail, or by overnight carrier to the following addresses, or to such other addresses as may be designated in writing by the Parties from time to time during the term of this MEMORANDUM:

K.U. LEUVEN R&D:	Paul Van Dun
	General Manager K.U. LEUVEN R&D
	Minderbroedersstraat 8A
	3000 LEUVEN
	BELGIUM
	Tel.: + 32 16 32 65 00
	Fax: + 32 16 32 65 15
SETS	Dr. M.S. Vijayaraghavan,
	Executive Director,
	Society for Electronic Transactions and
	Security (SETS),
	No.21 (Old No.11), Mangadu Swamy Street,
	Nungambakkam, Chennai - 600 034



11.5. Disputes. Parties shall use reasonable endeavours to solve any dispute that will arise in connection to this MEMORANDUM by mutual arrangement. If Parties, for any reason whatsoever, do not come to any solution, any subsisting dispute shall be resolved through arbitration. The Parties shall in such case mutually agree upon and appoint one single arbitrator. The place of arbitration shall be Luxembourg, Grand Duchy of Luxemburg, and proceedings shall be conducted in English in accordance with the arbitration rules of the International Chamber of Commerce (ICC).

IN WITNESS WHEREOF, the PARTIES have caused this MEMORANDUM to be executed by their duly authorized representatives.

Made in two originals on 9 November 2008,

For K.U. LEUVEN R&D:

For SETS:

Prof.dr. Marc Vervenne Rector K.U. LEUVEN Mr. S. Thiagarajan

Registrar

Prof.dr.ir. Koen rand Debackere Managing Director

Paul Van Dun General Manager

ANNEX 1

The Programme

Activities:

General

- 1. Visits of the researchers and students of the parties to each other
- 2. Sharing the materials developed by the researchers and students of two parties
- 3. Joint publication of research papers.

Research

- 1. Research on secure and efficient hardware implementations of cryptographic algorithms and protocols
- 2. Research on software tools for cryptographic hardware development
- 3. Research on software and hardware tools for side channel attacks and countermeasures on cryptographic hardware
- 4. Research on Software Tools to simulate and analyse Side Channel Attacks.

Education

Training, courses, summer courses, conferences

For approval:	
8 Vusamiles_	
ir.	5 higgin
Prof. dr. Ingrid Verbauwhede	Mr. S. Thiagarajan
Supervisor	Registrar, SETS

ANNEX 2

Shared Codes

The list below is not limited to the following. It can be extended or shortened in accordance with the respective needs of the Parties, but only by written separate agreement between K.U. LEUVEN R&D and SETS.

Shared Codes:

Any code developed by K.U. LEUVEN on its own within the field of Side Channel Analysis;

Any code developed by SETS on its own;

unless specified otherwise in separate agreements.



ANNEX 3

VISITING RESEARCHER AGREEMENT

This AGREEMENT, effective on DATE is

Between Society for Electronic Transactions and Security (SETS) a non profit organization duly registered and existing as a Society under Society Registration Act 1860 having its Registered Office at Electronics Corporation of India Ltd., North Zone, B-7, LSC, 'A' Block, Naraina Ring Road, New Delhi and Operational Headquarters Office at No.21 (Old No.11), Mangadu Swamy Street, Nungambakkam, Chennai – 600 034 (hereinafter referred to as 'SETS')

And

the Katholieke Universiteit Leuven (the "University"), for the purposes of this AGREEMENT represented by its department K.U. LEUVEN RESEARCH & DEVELOPMENT, having its office in 3000 Leuven, Minderbroedersstraat 8A, Belgium, VAT number BE 419.052.173, represented by Professor dr. ir. Koenraad Debackere, Managing Director, and Mr. Paul Van Dun, General Manager (hereinafter referred to as "K.U. LEUVEN R&D")

Hereinafter collectively referred to as "the Parties" or individually referred to as "a Party",

WHEREAS SETS has a desire to support and participate in the development of fundamental research in fields having an impact relevant to SETS' interests, and whereas K.U. LEUVEN R&D has an ongoing fundamental research program in those fields at the COSIC (Computer Security and Industrial Cryptography) research lab, (hereinafter referred to as "Unit"), which is consistent with the research interests of the SETS;

WHEREAS SETS has a desire to send an employee to K.U. LEUVEN R&D as a visiting researcher to further his/her experience in the field and whereas K.U. LEUVEN R&D is willing to accept the visiting researcher;

NOW, THEREFORE, in consideration of the premises and mutual covenants herein contained, the parties hereto agree to the following:

ARTICLE 1 - OBJECTIVES OF RESEARCH

Description of the Research and its objectives are identified in Exhibit I, which is attached hereto and incorporated herein.

ARTICLE 2 - PROGRAM ADMINISTRATION AND PERIOD

- 2.1. This program shall be administered by Prof. Ingrid Verbauwhede (Principal Investigator) of the Unit in accordance with the policies and procedures of the University.
- 2.2. It shall commence upon START DATE and terminate on END DATE. It may be renewed for additional periods upon the mutual consent of the parties.

ARTICLE 3 - VISITING RESEARCHER REQUIREMENTS

The visiting researcher will be identified by SETS and arrangements for his arrival at K.U. LEUVEN R&D shall be coordinated between SETS and Principal Investigator. SETS agrees that visiting researcher shall be appointed to an appropriate position and will comply with all K.U. LEUVEN R&D requirements associated with the position as described in the K.U. LEUVEN R&D's policies and procedures.



ARTICLE 4 - PUBLICATIONS AND PUBLICITY

- 4.1. K.U. LEUVEN R&D retains title in and the exclusive right to publish the results of any research conducted by the visiting researcher. Preprints of technical papers intended for publication shall be available to SETS upon request. Periodic reports on progress in research may be produced from time to time, and these reports will be available to SETS upon request. SETS' support will be acknowledged in publications, unless SETS desires otherwise and so advises K.U. LEUVEN R&D in writing.
- 4.2. No advertising or publicity matter having or containing any reference to K.U. LEUVEN R&D or in which the name of the K.U. LEUVEN R&D is mentioned shall be made use of by SETS until written approval has been obtained from the K.U. LEUVEN R&D.

ARTICLE 5 - CONFIDENTIALITY

- 5.1. If either Party to this AGREEMENT discloses its Confidential Information, the other Party shall maintain such information confidential for five (5) years from the date of disclosure or one (1) year from the termination of this AGREEMENT or any extension thereof, whichever time period is longer.
- 5.2. Information provided by one of the Parties to the other shall be deemed confidential if it is marked confidential or stated in writing to be confidential.
- 5 3. The above obligations of confidentiality, with regard to both K.U. LEUVEN R&D and SETS, shall not apply to information which:
 - was in the possession of the recipient prior to initial receipt hereunder;
 - is now or later becomes generally available to the public without breach of this AGREEMENT;
 - is received without restrictions on its use or secrecy from a third party having the right to
 - disclose such information; or
 - the disclosing Party gives the other Party written permission to publish or use; or
 - the receiving Party develops independently of any disclosure hereunder.

ARTICLE 6 - INVENTIONS AND PATENTS

The provisions of Article 5 ("Intellectual Property Rights") contained in the MEMORANDUM ON RESEARCH AND COLLABORATION executed between K.U. LEUVEN R&D and SETS shall apply, unless agreed otherwise in this AGREEMENT.

ARTICLE 7 - TERMINATION

- 7.1. SETS or K.U. LEUVEN R&D shall have the right, with a thirty (30) days prior written notice, to terminate this AGREEMENT if the Supervisor is unable to continue to comply with the obligations resting upon him/her under this AGREEMENT and if a replacement agreeable to SETS and K.U. LEUVEN R&D is not found within the notice period.
- 7.2. In the event that either Party shall be in default of its material obligations under this AGREEMENT and shall fail to remedy such default within sixty (60) days after receipt of written notice thereof, this AGREEMENT may be terminated upon written notice at the option of the Party not in default upon expiration of the sixty (60) day period.
- 7.3. Any provisions of this AGREEMENT which by their nature extend beyond termination shall survive such termination.

ARTICLE 8 - GENERAL

- 8.1. For the purposes of this AGREEMENT, K.U. LEUVEN R&D shall be deemed to be an independent contractor and not SETS' agent or employee and the same holds good for SETS which should not be taken as K.U. LEUVEN R&D's agent. Neither Party shall have any authority to make any statements, representations or commitments of any kind, or to take any action which shall be binding on the other Party except as provided for herein or authorized in writing by that other Party.
- 8.2. All written communications, including any notice or report, required or permitted under this AGREEMENT shall be deemed to have been sufficiently given for all purposes if mailed by first class mail to the following addresses of either party:

If to K.U. LEUVEN R&D: If to SETS: Paul Van Dun, General Manager Dr. M.S. Vijayaraghavan, Minderbroedersstraat 8A Executive Director, 3000 - LEUVEN Society for Electronic Transactions and Security (SETS) No.21 (Old No.11), Mangadu Swamy Street, tel .: +32 16 32 65 08 Nungambakkam, Chennai - 600 034 fax: +32 16 32 65 15 e-mail: ed@setsindia.net Tel: 044 - 28205655 Miet.Lenaers@lrd.kuleuven.be Fax: 044 - 42132705

- 8.3. This AGREEMENT is personal in its character and cannot be assigned, sold, transferred or encumbered in any manner by any Party hereto without the express written consent of the other Party, any attempt to do so being void.
- 8.4. This AGREEMENT can only be changed by a written document signed by all Parties.
- 8.5. Arbitration: The Parties shall use reasonable endeavours to solve any dispute that will arise in connection to this AGREEMENT by mutual arrangement. If Parties, for any reason whatsoever, do not come to any solution, any subsisting dispute shall be resolved through arbitration. The Parties shall in such case mutually agree upon and appoint one single arbitrator. The place of arbitration shall be Leuven, Belgium, and proceedings shall be conducted in English.

IN WITNESS WHEREOF, the Parties have hereunto set their hands.

FOR K.U. LEUVEN R&D:	FOR SETS
Prof. dr.ir. Koenraad Debackere Managing Director	Mr. S. Thiagarajan Registrar, SETS
Paul Van Dun General Manager	
For approval : Prof.dr. Ingrid Verbauwhede	