25th Crypto-Day

SAP

September 22 and 23, 2016

Walldorf, Germany

Thursday, 22. 09.		
13:00	13:05	Welcome
13:05	14:05	***Keynote Talk***
14:05	14:30	*Angela Jäschke:* "Accelerating Homomorphic Computations on Rational Numbers"
14:30	14:55	*Spyros Boukoros:* "A lightweight protocol for privacy preserving floating-point division from homomorphically encrypted data"
14:55	15:15	**Coffee Break**
15:15	15:40	*Zoya Dyka:* "Revisiting random permutation of calculation steps of a field multiplication as a DPA countermeasure"
15:40	16:05	*Ievgen Kabin:* "Influence of multiplier on the security of elliptic curve cryptography design"
16:05	16:30	*Bernhard Esslinger:* "CrypTool - ein E-Learning-Projekt für Kryptographie und Kryptoanalyse"
16:30	16:50	**Coffee Break**
16:50	17:15	*Florian Hahn:* "Poly-Logarithmic Range Queries on Encrypted Data with Small Leakage"
17:15	17:40	*Christian Müller:* Your Smart Home Knows What You Are Doing
17:40	18:05	*Kai Mindermann:* "Zwischenbericht zur Dissertation: Verbesserung der Benutzbarkeit von Krypto-APIs"
18:30		**Bus Drive to Heidelberg**

Friday, 23. 09.		
9:00	10:00	**Visit of Pavillion**
10:20	10:45	*Anselme Tueno:* "Oblivious Order-Preserving Encryption"
10:45	11:10	*Zhi Guan:* "Accelerating Cryptographic Primitives with SIMD"
11:10	11:35	*Christian Wittke:* "Sophisticated placement of flip-flops to protect cryptographic ASICs against Laser FI and localized EMA"
11:35	11:55	**Coffee Break**
11:55	12:20	*Dan Kreiser:* "Generation of cryptographic keys using parameters of a wireless communication channel in an industrial environment"
12:20	12:45	*Robin Fay:* "Secure Sensor Data through Compressed Sensing Encryption Modes"
12:45	13:10	*Nabil Alkeilani Alkadri:* "Post-Quantum Commitment Schemes"
13:10		**End of the Event**

Accelerating Homomorphic Computations on Rational Numbers

Angela Jäschke and Frederik Armknecht

University of Mannheim
Mannheim
Germany

Fully Homomorphic Encryption (FHE) schemes are encryption schemes which allow arbitrary computations on encrypted data, such that the result decrypts to the correct outcome of the computation. Discovered in 2009 [Gen09], these schemes are conceptually very powerful tools for outsourcing computations on confidential data. However, experience shows that FHE-based solutions are not sufficiently efficient for practical applications yet [LNV11]. Hence, there is a huge interest in improving the performance of applying FHE to concrete use cases. What has been mainly overlooked so far is that not only the FHE schemes themselves contribute to the slowdown, but also the choice of data encoding. While FHE schemes usually allow for homomorphic executions of algebraic operations over finite fields (often $\mathbb{Z}_2$), many applications call for different algebraic structures like signed rational numbers. Thus, before an FHE scheme can be used at all, the data needs to be mapped into the structure supported by the FHE scheme.

We show that the choice of the encoding can already incur a significant slowdown of the overall process, which is independent of the efficiency of the employed FHE scheme. We compare different methods for representing signed rational numbers and investigate their impact on the effort needed for processing encrypted values. In addition to forming a new encoding technique which is superior under some circumstances, we also present further techniques to speed up computations on encrypted data under certain conditions, each of independent interest. We confirm our results by experiments.

Literatur

[Gen09] Craig Gentry. A fully homomorphic encryption scheme Dissertation at Stanford University, 2009

[LNV11] Kristin Lauter, Michael Naehrig and Vinod Vaikuntanathan. Can Homomorphic Encryption Be Practical? CCSW, 2011

A lightweight protocol for privacy preserving floating-point division from homomorphically encrypted data

Spyros Boukoros, Nikolaos P. Karvelas and Stefan Katzenbeisser

Security Engineering Group
Technical University of Darmstadt

The increasingly high demand of computational power and storage, has lead corporations to outsource part of their infrastructure to server farms and clouds, owned by third-party providers. Although this has many advantages, one cannot neglect the fact that the privacy of the data is put in danger. Industrial espionage aims (among others) in damaging the financial horizons of a company, while collaterally leaking individuals' private records which in addition, completely destroys the client-corporation trust. To mitigate such problems, two powerful cryptographic primitives, Homomorphic encryption and Secure Two Party Computation (STC) have become well established means of performing various operations on encrypted data such as, computing statistics, data mining etc., and succeed in preserving the privacy of the data. In many of these applications however, the need arises, to perform division over integers and yield a floating point result. In the case of homomorphic encryption schemes, performing such an operation in the encryption domain is cumbersome and in some cases even impossible, while in the case of STC, the protocols suffer from high communication costs. Thus, a great need arises, that demands allowing the performance of fast and privacy preserving divisions.

Many works have focused on the problem described above, by using either STC or homomorphic encryption schemes, but they are not widely used due to speed and complexity bottleneck. We highlight this, by pointing out to privacy preserving Genomic Wide Association Studies (GWAS), where the DNA of individuals is collected and stored into databases, and various computations are performed [1, 2]. In such studies, various functions, such as frequencies, statistical tests and other complex formulas, require divisions. Those are performed by allowing the nominators and denominators to be in plaintext or assuming, that some entity provides these data in the required format. This however, leaks sensitive information and is prone to exploitation (for example by performing the same test again and noticing if a newly added client in the database suffers from a specific disease or not), which can result into not only financial but also major psychological damage, since the person under attack can become a victim of discrimination. Hence, preserving the privacy of the clients in the aforementioned field is of grave importance.

Our goal, in this on-going work, is to provide a tool-chain, that allows privacy preserving division over additively homomorphic data. We combine the ideas of homomorphism and proxy re-encryption to allow an individual to acquire the correct result of a plain text division of two integers in floating point format, without being able to guess the original values. We describe our idea, analyze our framework and provide measurements that back up our theoretical findings.

References

[1] Murat Kantarcioglu, Wei Jiang, Ying Liu, and Bradley Malin. A cryptographic approach to securely share and query genomic sequences. *IEEE Transactions on information technology in biomedicine*, 12(5):606–617, 2008.

[2] Miran Kim and Kristin Lauter. Private genome analysis through homomorphic encryption. *BMC medical informatics and decision making*, 15(Suppl 5):S3, 2015.

Revisiting random permutation of calculation steps of a field multiplication as a DPA countermeasure

Zoya Dyka, Estuardo A. Bock, Ievgen Kabin and Peter Langendoerfer

IHP

Frankfurt (Oder), Germany

SCA attacks are significant threats for cryptographic devices if an attacker has physical access to the devices. Against vertical differential power analysis (DPA) and collision-based attacks on elliptic curve (EC) cryptosystem randomization approaches, such as the randomization of the private key, the blinding of an EC point or the randomization of its coordinates, were proposed 1999 [1]. These algorithmic countermeasures are well-known and very efficient against vertical DPA attacks, i.e. against attacks using more than one trace with inputs (the EC point or the key candidate) given by the attacker. Another algorithmic countermeasure the randomization of the sequence of the mathematic operations in the decryption algorithm was proposed 2001 in [2].

2009 in [3] a hardware countermeasure against DPA attacks was proposed. This countermeasure exploits the field multiplier as a means to randomize the energy consumption of cryptographic designs clockwise. The field multiplier is a part of the design that performs the multiplication of an EC point P with a scalar k, i.e. the kP operation. To optimize the area and the energy consumption of such devices, the field multiplication is usually designed as a serial multiplier. Both multiplicands (recently about 200 bit long binary numbers) have to be split into segments. In a single clock cycle the product of two one-segment-long operands, i.e. a partial product, is calculated. The polynomial product is then calculated as a sum of the partial products. The polynomial product is finally reduced to obtain the field product. The number of the partial products depends on the segmentation of the multiplicands and on the applied multiplication formula. In [3] it was proposed to randomize the sequence of the calculation of the partial products for each field multiplication.

The efficiency of this countermeasure was not examined neither against vertical nor against horizontal DPA attacks using power traces of a kP design. In our work we implemented the random permutation of the partial products calculation sequence in our kP design. We examined the efficiency of this method as a countermeasure against horizontal DPA attacks (using difference-of-means test) and against a comparative power analysis (PA) attack that is a kind of vertical attacks. We show that the approach proposed in [3] is efficient against horizontal DPA attacks but not efficient against comparative PA if the field product is calculated using a small number of partial products, i.e. if the multiplier needs only few clock cycles for the product calculation. Due to this fact the random permutation of the calculation steps of partial products is not sufficient as a single means against both kinds of DPA attacks.

References

[1] J. Coron: *Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems.* Proc. of CHES 1999, LNCS Vol. 1717, pp. 292302, Springer Berlin Heidelberg, 1999.

[2] E. Oswald, M. Aigner: *Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks* . Proc. of CHES 2001, LNCS Vol. 2162, pp. 3950, Springer Berlin Heidelberg, 2001.

[3] F. Madlener, M. Stoettinger, S.A. Huss: *Novel hardening techniques against differential power analysis for multiplication in GF(2^n).* Proc. of FPT 2009, Sydney, NSW, December 9-11, 2009, pp. 328 334, IEEE.

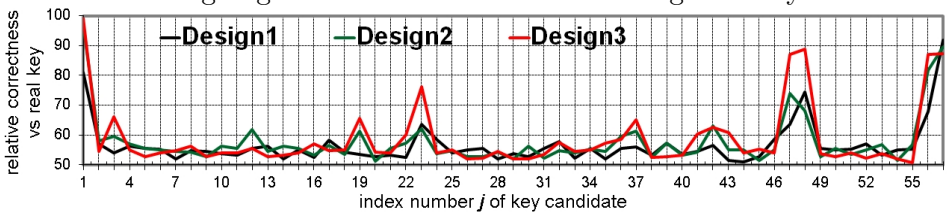
Influence of multiplier on the security of elliptic curve cryptography design

Ievgen Kabin, Zoya Dyka and Peter Langendoerfer

IHP

Frankfurt (Oder), Germany

Elliptic curve (EC) cryptography is a public key encryption technique based on the use of ECs. It can guarantee a high level of security using short key length and can be easily realized in hardware. For attacks on cryptographic hardware the power analysis attack is most frequently used. It is a kind of SCA attack that allows non-invasively extracting the cryptographic key from a hardware device by examining its power consumption during execution of decryption. In this work we will demonstrate how using of different kinds of multipliers of $GF(2^{233})$-elements influence the success of a horizontal DPA attack. The $GF(2^{233})$-multiplier is a part of our design that performs an EC point multiplication with a scalar. This operation, denoted as kP, is the main operation in EC cryptosystems. P is a point of EC and k is a large binary number, i.e. the private key, if the decryption is performed. We implemented three kP designs on the basis of the Montgomery kP algorithm [1] and synthesized them for the IHP 130 nm technology. The only one difference between them was the implementation of the multiplier. Only one block in each design is different - the multiplier for elements of $GF(2^{233})$. The multiplier in the Design1 is implemented using the classic multiplication method (MM). The multiplier in Design2 is a combination of the 4-segment iterative Karatsuba multiplication (IKM) [2] and the classical MM. Design3 contains a multiplier which is a random combination of the classical MM, the 4-segment IKM and the Winograd MM [3]. Multipliers differ in area and therefore in power consumption. We simulated power traces (PTs) for the execution of the same kP operation for all three designs. We performed a horizontal DPA attack using the *difference of means* test for each simulated PT. Design1 is more resistant against the performed attack than other two designs: only one key candidate was extracted with a correctness of 91%. The other two candidates have correctness of 74% and 81% respectively. For the Design2 there is one key candidate extracted with a correctness of 73% and three key candidates were extracted with a correctness between 82% and 96%. For Design3 one key candidate was extracted with a correctness of 76% and next 5 candidates have a correctness between 87% and 99% (see Fig. below). Thus, the correctly selected MM for $GF(2^n)$ elements can increase the resistance of the kP design against horizontal DPA attacks significantly.



References

[1] D. Hankerson, J. Lopez, and A. Menezes, *Software implementation of elliptic curve cryptography over binary fields*, CHES-2000, LNCS Vol. 1965, Springer Berlin Heidelberg, 2000.

[2] Z. Dyka, P. Langendoerfer, *Area efficient hardware implementation of elliptic curve cryptography by iteratively applying Karatsubas method*, Proc. of DATE, 2005, Vol.3, pp: 70-75.

[3] S. Winograd, *Arithmetic Complexity of Computations*, SIAM, 1980, page 35.

CrypTool – ein E-Learning-Projekt für Kryptographie und Kryptoanalyse

Bernhard Esslinger

Universität Siegen, Germany
bernhard.esslinger@uni-siegen.de, esslinger@cryptool.org

Um Kryptologie zu lernen und zu lehren, gibt es unterschiedliche Wege. Da sowohl Lehrende wie Lernende unterschiedlich sind, versuchte das CrypTool-Projekt, die Themen so aufzubereiten, dass sie auch den eher experimentell veranlagten Menschen den Zugang zur Theorie erleichtern.

Gegründet wurde das Open-Source-Projekt CrypTool (CT), um das Wissen und die Awareness über Kryptologie zu fördern und um das Studium von MINT-Fächern zu fördern.

Die verschiedenen CT-Programme enthalten inzwischen über 400 Funktionen und Visualisierungen. Im Lauf der letzten 15 Jahre trugen mehr als 300 Contributers von über 20 Hochschulen und 10 Firmen dazu bei.

Der Vortrag erläutert beispielhaft, welche Hochschule was hinzufügte und wie man dieses Lernprogramm zur Verbesserung seiner eigenen Lehre einsetzen kann.

Die folgende Liste vermittelt einen Eindruck von der Spannweite der in den letzten 18 Monaten zu CT2 und JCT hinzugefügten Plugins (siehe www.cryptool.org):

1. Huffman Code (Singidunum University, Serbien)
2. GNFS (TU Eindhoven, Niederlande)
3. Private Programmausführung mit HE (SEAL) und ShapeCPU (Unis Siegen + Hannover)
4. WOTS, (X)MSS-MT (FH Hagenberg, Support von TU Eindhoven)
5. Cramer-Shoup mit EAX-AES (Uni Bochum)
6. Visualisierung von AES und DES (Uni Mannheim)
7. Visualisierung ARC4 / Spritz (FH Hagenberg)
8. Erweiterter Euklid (Schülerfacharbeit Jena)
9. Zertifikats-Validierung nach Ketten- und Schalenmodell (FH Hagenberg)
10. Strip-Cipher M-138: Verschlüsselung + Kryptoanalyse (Uni Kassel)
11. Shanks Babystep-Giantstep (TU Darmstadt)
12. Oblivious Transfer + Yaos Millionärs-Problem (Brno University of Technology)
13. Verteilte Kryptoanalyse per CrypCloud (Uni Kassel).

Aktuell sind folgende größeren Teilprojekte in Arbeit: CT 2.1, eine GUI für BouncyCastle in JCT, neue Webtechnologie für CT-Online und ein neues, Python-basiertes Backbone-System für MysteryTwister C3 (MTC3).

Poly-Logarithmic Range Queries on Encrypted Data with Small Leakage

Florian Hahn and Florian Kerschbaum
SAP
Karlsruhe
Germany

In order to preserve data privacy in data outsourcing scenarios, the outsourced data must be encrypted. In scenarios the user wants to filter the data for user-defined criteria, however, standard encryption prevents the service provider for executing these queries directly. Current solutions leverage property-preserving (*i.e.* deterministic and order-preserving) encryption for providing this functionality on encrypted data. However, these solutions are vulnerable to simple yet effective attacks (*e.g.* ferquency analysis) as presented recently by Naveed *et al.* in [NKW15]. The idea of searchable symmetric encryption as introduced by Song *et al.* in [SWP00] is one way to mitigate these attack vectors. Using searchable symmetric encryption, the data owner can encrypt and outsource his files augmented with additional information (*e.g.* keywords, timestamps). Using the secret key the data owner can create a search token (e.g. for exact pattern matching of a keyword, for a range the timestamp should fall within) and pass it to the cloud service provider. Using this search token the cloud service provider can filter for all ciphertexts that match with the search token.

In this talk we focus on privacy-preserving range queries that allow the encryption o data while still enabling queries on ciphertexts if their corresponding plaintexts fall within a requested range. Based on the work of [SSW09] and [Lu12] we present a novel scheme that achieves small information leakage while supporting amortized poly-logarithmic search time. Our construction is based on the novel idea of enabling the cloud service provider to compare requested range queries. By doing so, the cloud service provider can use the access pattern to speed-up search time for subsequent range queries. On the one hand, values that have fallen within a queried range, are stored in an interactively built index for subsequent requests. On the other hand, values that have not been queried do not leak any information to the cloud service provider and stay perfectly secure.

References

[SWP00] Song, D. X., Wagner, D., and Perrig, A. Practical techniques for searches on encrypted data. In *Proceedings of the 21st IEEE Symposium on Security and Privacy* (2000), S&P.

[NKW15] Naveed, M., Kamara, S., and Wright, C. V. Inference attacks on property-preserving encrypted databases. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security* (2015), CCS.

[SSW09] Shen, E., Shi, E., and Waters, B. Predicate privacy in encryption systems. In *Proceedings of the 6th Theory of Cryptography Conference* (2009), TCC.

[Lu12] Lu, Y. Privacy-preserving logarithmic-time search on encrypted data in cloud. In *Proceedings of the 19th Network and Distributed System Security Symposium* (2012), NDSS.

Your Smart Home Knows What You Are Doing

Philipp Morgner*, Christian Müller†, Matthias Ring*, Frederik Armknecht†, Zinaida Benenson*, and Björn Eskofier*

* University of Erlangen-Nuremburg, Germany † University of Mannheim, Germany

Smart heating systems promise to increase energy efficiency and comfort by collecting and processing room climate data. While it has been suspected that the sensed data may leak crucial personal information about the occupants, this belief has not been supported by evidence so far. In this talk, we shed some light on privacy risks in smart heating scenarios assuming that an attacker has access to the most basic measurements only: temperature and relative humidity. We conducted a series of experiments at two different locations and evaluated the results using various machine learning techniques. We show that knowing a sequence of temperature and relative humidity measurements for a time interval of 2–6 minutes allows to detect occupancy with an accuracy of up to 96%. Moreover, we demonstrate that one can distinguish between reading, working on a PC, standing, and walking, with an accuracy of up to 62% (as compared to the chance of 25% for guessing these four activities), while distinguishing between standing and walking is possible with an accuracy of up to 96.7%. Our results provide evidence that even the leakage of such 'inconspicuous' data like temperature and relative humidity can seriously violate privacy in smart buildings.

Zwischenbericht zur Dissertation: Verbesserung der Benutzbarkeit von Krypto-APIs

Kai Mindermann M.Sc.
Universität Stuttgart, Institut für Softwaretechnologie
kai.mindermann@informatik.uni-stuttgart.de
2016-09-12

I. Einführung

Spätestens seit den bewusstmachenden Veröffentlichungen von Edward Snowden stieg die Nachfrage nach wirksamen Schutz vor Überwachung stark an. Dafür gibt es zahlreiche geeignete und nach aktuellem Stand sichere kryptographische Verfahren die über Application Programmable Interfaces (APIs) den Entwicklern zur Verfügung stehen. Den Verfahren haftet häufig jedoch eine nicht zu unterschätzende Komplexität an, welche ihre Anwendung erschwert. Kryptographen oder Security-Experten haben die nötige Erfahrung damit umzugehen, Softwareentwickler jedoch seltener. Hinzukommt die schlechte Benutzbarkeit der APIs. Dies wird auch in der Literatur zum Beispiel von Georgiev et al. bestätigt. Sie haben schlecht entworfene APIs als Ursache für mögliche Man-in-the-middle-Angriffe auf Transport Layer Security (TLS) identifiziert[1]. Nadi et al. haben verschiedene Studien durchgeführt, bei denen für die javax.crypto-API auch fehlende Benutzbarkeit bemängelt wird[2].

II. Bisherige Arbeit

Neben der Literaturrecherche habe ich bereits ein Positionspapier veröffentlicht [3] in dem ich zum Beispiel auf einen für kryptographische Bibliotheken besonders langen *Reife-Prozess* verweise und das verschiedene Experten besser zusammenarbeiten müssen. Weiterhin habe ich ein kontrolliertes Experiment mit Studenten durchgeführt. Im Experiment habe ich untersucht, wie Anfänger (Softwaretechnik-Studenten im 2. Semester) Vorgehen, wenn Sie kryptographische Verfahren (hier symmetrische Verschlüsselung) in ein bestehendes Programm integrieren müssen. Dabei ist aufgefallen, dass viele Anleitungen im Web gesucht haben, was auch ein Indiz dafür ist, dass die API selbst nicht gut genug dokumentiert und erlernbar ist.

III. Verbesserung der Krypto-APIs

Das Ziel meiner Dissertation ist die **Bereitstellung von praxistauglichen Richtlinien für die Erstellung von benutzbaren und sichereren kryptographischen APIs** bzw. Programmbibliotheken. Dabei sollen diese möglichst unabhängig von der Programmiersprache sein. Dies ist aber vermutlich nicht immer möglich, da Programmiersprachen unterschiedliche Strukturen und Programmierparadigmen unterstützen. Des Weiteren hängt es nicht nur von der Programmiersprache ab, sondern auch welche Erwartung und Erfahrung Entwickler an bzw. mit APIs haben.

Ich gehe davon aus, dass sich die Richtlinien mindestens auf folgende Bereiche beziehen: Benennung von Klassen und Methoden, Struktur und Entwurfsmuster, High-Level bis Low-Level Zugriff/Methoden, Dokumentation (Beispiele) und Fehlermeldungen.

Die Richtlinien müssen sich dabei an den sechs Qualitätsattributen für APIs nach Myers et al. messen lassen: Erlernbarkeit, Produktivität, Fehlervermeidung, Einfachheit, Konsistenz und Übereinstimmung mit dem mentalen Modell des Entwicklers [4].

Hierzu sollen zunächst ausgewählte kryptographische Bibliotheken auf ihre bisherige Benutzbarkeit analysiert werden. Danach soll überprüft werden, welche und wie Verbesserungen aus der API-Usability-Forschung angewendet werden können ohne die Sicherheitseigenschaften zu verschlechtern. Diese Untersuchungen sollen durch kontrollierte Experimente mit Softwareentwicklern, die wenig Erfahrung mit kryptographischen Methoden haben, evaluiert werden. Dieses Vorgehen führt dann nach und nach zu den oben genannten Richtlinien. Die Richtlinien müssen am besten bereits während der Erstellung mit den Entwicklern der kryptographischen Programmbibliotheken geteilt werden, um eine frühe Integration und Verbesserung der Benutzbarkeit zu ermöglichen sowie Feedback von diesen Entwicklern zu erhalten.

References

[1] Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov. 2012. *The most dangerous code in the world: validating SSL certificates in non-browser software*. Proc. 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, NY, USA, 38-49. DOI: http://dx.doi.org/10.1145/2382196.2382204

[2] Sarah Nadi, Stefan Krüger, Mira Mezini, and Eric Bodden. 2016. *Jumping through hoops: why do Java developers struggle with cryptography APIs?*. Proc. 38th International Conference on Software Engineering (ICSE '16). ACM, New York, NY, USA, 935-946. DOI=http://dx.doi.org/10.1145/2884781.2884790

[3] Kai Mindermann. 2016. *Are easily usable security libraries possible and how should experts work together to create them?*. Proc. 9th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE '16). ACM, New York, NY, USA, 62-63. DOI: http://dx.doi.org/10.1145/2897586.2897610

[4] Brad A. Myers and Jeffrey Stylos. 2016. *Improving API usability*. Commun. ACM 59, 6 (May 2016), 62-69. DOI: http://dx.doi.org/10.1145/2896587

Accelerating Cryptographic Primitives with SIMD

Zhi Guan
Mannheim University
Germany

Recent year cryptographic primitives are widely and heavily used in application scenarios such as cloud computing. The computation of cryptographic primitives is highly time consuming and brings performance pressure to application environment. SIMD is a classic computation mode that performs the same operation over multiple data simultaneously. SIMD processing has become an indispensable feature of most commercial processors including desktop processors, mobile processors, graphical processors and supercomputers. Accelerating cryptographic primitives through SIMD processing has become an effective and economic solution on commercial hardware. In this talk we will introduce some modern SIMD instruction sets (AVX2/KNC-NI/NEON) and our efforts on optimizing different cryptographic primitives including symmetric encryption, RSA, elliptic curve cryptography, pairing, etc.

Zhi Guan is an associate professor in Peking University, Beijing, China. He is a visiting researcher at Mannheim Univeristy, Germany, since Jan. 2016. His research interests involve applied cryptography and IT Security.

Sophisticated placement of flip-flops to protect cryptographic ASICs against Laser FI and localized EMA

Christian Wittke, Zoya Dyka and Peter Langendoerfer

IHP
Im Technologiepark 25
Frankfurt (Oder), Germany

Cryptographic algorithms implemented in hardware can be attacked in different ways. Semi-invasive attacks such as fault injection (FI) using a laser or localized electromagnetic analysis (EMA) can be performed to reveal the cryptographic key. These attacks require the cryptographic device to be decapsulated and it is important that the IC is still fully functional.

Laser fault injection attacks exploit the sensitiveness of CMOS gates to light. It is possible to manipulate the value of a certain register using a high precisely focused laser beam. This can cause faults in outputs of the attacked cryptographic design. These outputs can be analyzed with the goal to extract the secret key. There are countermeasures against fault injection attacks, e.g. shielding. Another kind of countermeasure is to place all registers of a design near to each other, since it is easier to manipulate precisely a single placed flip-flop of a register than a flip-flop in a group.

In case of localized EMA attacks the attacker observes the activity of registers. Measurements are performed using high resolution EM probes. A certain small area of the IC, e.g. a certain register can be observed. The information about the activity of registers over time during a decryption can be used to extract the key. However there are countermeasures to prevent such local attacks by shielding of the IC or a randomized distribution of storage registers [1]. Thereby the activity of single flip-flops will be covered by surrounding logic gates and can no longer be observed easily.

The approaches to protect cryptographic ICs against laser FI and against localized EMA using an intelligent placement of registers in a layout contradict each other. On the one hand the countermeasure with random spread registers can decrease the success of localized EMA but could increase the vulnerability against fault injection attacks. On the other hand the placement of flip-flops in groups makes the precise FI more complicated but the activity of a group of flip-flops is better observable using high resolution EM probes.

In this work we want to investigate the conditions for an intelligent clustering of flip-flops in an IC with the goal to find an algorithm that resolves the above mentioned contradiction. This algorithm shall then be integrated and used in the design flow of an IC.

References

[1] Heyszl, J.: Impact of Localized Electromagnetic Field Measurements on Implementations of Asymmetric Cryptography, Phd Thesis TU Munich, 2013

Generation of cryptographic keys using parameters of a wireless communication channel in an industrial environment

Dan Kreiser[1], Zoya Dyka[1], Peter Langendoerfer[1] and Oliver Stecklina[2]

[1] IHP
Frankfurt (Oder), Germany

[2] BTU Cottbus-Senftenberg
LS Automatisierungstechnik
Cottbus, Germany

The demand of replacing wired automation systems by wireless systems is increasing steadily. The flexibility of such wireless systems is a big advantage for the industry. In order to be able to use such systems, it is crucial to ensure a reliable and secure communication. Cryptographic approaches can be used to guarantee the secure communication of nodes. The generation and agreement of cryptographic keys between nodes is a one of important tasks. At the same time it is necessary to achieve low latency and real-time capabilities.

Based on the reciprocity theorem parameters of a wireless communication channel can be used as the common source of randomness for the sender and the receiver. In an ideal case the sender and receiver Alice and Bob are identical devices and can send each other an identical probe-signal. Alice and Bob receive the probe signal that is distorted because of multiple reflection and diffraction of the signal, caused by the environment. Important is that both communication partners receive the identically distorted probe-signal. Alice and Bob can use a quantization algorithm for the generation of a shared secret key using the received signals. Any device close by (even an identical one) receives the probe-signal with other distortion and obtains another key even the same quantization algorithm was used. This fact makes the generation of the cryptographic keys using channel parameters attractive.

In reality the generation of keys using channel parameters is difficult due to the facts that the communication partners are not identical devices and that the influence of the environment can be not the same over the communication time. This causes differences in generated keys, i.e. Alice and Bob obtain similar but not the same key. Furthermore the entropy of the key can be insufficient, especially in a stationary environment. Thus, the key can be predicted or manipulated.

To evaluate the applicability of the generation of the cryptographic keys using channel parameters for nodes of a wireless automation system we performed measurements of channel parameters in a real industrial environment, which is the model factory of the Innovation Centre Modern Industry Brandenburg, Chair of Automation Technology BTU Cottbus-Senftenberg [1]. This model factory is well suited to make realistic measurements in a controllable environment. We used IHP Feuer-Where sensor nodes [2] for collection of RSSI values. We generated keys using different quantization algorithms and verified the quality of the keys.

References

[1] Model Factory of the Innovation Centre Modern Industry Brandenburg, Chair of Automation Technology BTU Cottbus-Senftenberg ,Oliver Stecklina, `http://www.imi4bb.de/TransferI4/#transf-i4-functional.area`

[2] Krzysztof Piotrowski, Anna Sojka-Piotrowska, IHPNode the experimental platform for wireless sensor networks and Internet of Things, In Proc: XI Scientific Conference on Measurement Systems in Research and in Industry (SP 2016). Poland, 2016, Oficyna Wydaw. Uniwersytetu Zielonogrskiego, Zielona Gra, 2016, pp. 121124, ISBN: 9788378422440.

Secure Sensor Data through Compressed Sensing Encryption Modes

Robin Fay*

*University of Siegen
Hölderlinstr. 3, 57076 Siegen
Germany

Today, a huge amount of sensible sensor data and measurements are obtained in industrial applications. In order to process and store this data, it is compressed directly after sampling. The compression reduces the amount of data to the important information. However, it would be more efficient to sample only the important parts of the data. This pretty intuitive approach is applied in Compressed Sensing. A lot of interesting sensor systems were developed in the past years based on the mathematical theories of Candès, Tao and Donoho [1, 2].
The sampling process is randomized and can be modeled as a multiplication of a signal $\vec{x} \in \mathbb{R}^N$ with a random matrix $A \in \mathbb{R}^{m \times N}$ ($m \ll N$). For example, the entries of A might be drawn uniformly at random from $\{-1, +1\}$. Confidentiality is achieved by treating the sampling matrix as a shared secret between the communicating parties, since A is needed for signal recovery. Compressed sensing based encryption offers a decent level of confidentiality that arises from the large number of sampling matrices and the complexity of the signal recovery. However, if more than one signal is encrypted under the same matrix the encryption scheme becomes deterministic, like ECB mode, and same plaintext will always produce the same ciphertext. To overcome this problem, we have introduced modes of operations to Compressed Sensing based encryption in [3].

This paper presents our recent research results on Compressed Sensing encryption modes and it discusses designs with different properties like parallelizability and self-synchronization. The security of the proposed modes can be reduced to the security of known and trusted primitives or constructions. Bounds on the security of the proposed schemes and requirements on the parameters are derived from this analysis. Compressed Sensing encryption modes are suitable for a wide range of applications and they offer End-to-End confidentiality that starts at the sensor level.

Acknowledgments

This research was funded by the German Research Foundation (DFG) under project number RU 600-11/1.

References

[1] E. J. Candès and T. Tao, "Decoding by Linear Programming," *Information Theory, IEEE Transactions on*, vol. 51, no. 12, pp. 4203–4215, 2005.

[2] D. Donoho, "Compressed Sensing," *Information Theory, IEEE Transactions on*, vol. 52, no. 4, pp. 1289–1306, 2006.

[3] R. Fay, "Introducing the counter mode of operation to Compressed Sensing based encryption," *Information Processing Letters*, vol. 116, no. 4, pp. 279 – 283, 2016. [Online]. Available: `http://www.sciencedirect.com/science/article/pii/S0020019015001945`

Post-Quantum Commitment Schemes

Nabil Alkeilani Alkadri
Department of Computer Science, Cryptography and Computeralgebra
Technische Universität Darmstadt
Germany

Commitment schemes (CSs) are fundamental building blocks in constructions of many cryptographic protocols. Commitments hold two fundamental properties called hiding and binding. However, they can further provide more properties such as universal composability, non-malleability, or trapdoor property.

Commitments were introduced by Blum [Blu82], who implicitly used them in order to flip a coin by telephone. Nowadays, CSs have many applications and are used in various cryptographic protocols.

Since their introduction, many CSs were suggested based on number theoretic problems such as factoring large integers and extracting discrete logarithms. CSs were also suggested using generic complexity assumptions such as any family of collision resistant hash functions. Furthermore, there are CSs based on lattice problems and on decoding random linear codes.

However, cryptographic schemes based on number theoretic problems will become insecure as soon as large enough quantum computers are built. This is due to Shor's algorithm [Sho97]. Despite this fact, important classes of cryptography such as code-based and lattice-based cryptography are believed to remain secure even under quantum attacks.

We provide a systematic and unified description of post-quantum CSs, i.e., CSs that run on conventional computers, and whose security is believed to hold up against quantum computers. Here not only concrete solutions, but also generic approaches are considered. In this work, we concentrate only on the two fundamental properties, i.e., hiding and binding, since they are sufficient for many applications. Based on this unified description we compare different approaches with respect to efficiency and identify the currently most practical and efficient CSs. Finally, we also show how these solutions can be further improved.

References

[Blu82] Manuel Blum. Coin flipping by telephone: A protocol for solving impossible problems. *Advances in Cryptology-A Report on CRYPTO'81*, 1982.

[Sho97] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, 26(5):1484–1509, 1997.

26th Crypto-Day

SAP

June 01 and 02, 2017

Nuremberg, Germany

On June 01 and 02, 2017, the interest group "Angewandte Kryptographie" of Gesellschaft für Informatik e. V. will host the twenty-sixth *Crypto-Day*.

Ambition and Program: The Crypto-Day aims at providing an opportunity for early-stage researchers in the field of cryptography and IT-security to exchange knowledge and establish networks to universities as well as to industry (e.g. for collaboration across Germany, or to find out about research internships and post-doc positions). Therefore, we invite students, doctoral candidates, and experienced researchers to present their research results or research ideas in the form of 20 minute presentations on this upcoming Crypto-Day.

Host: SUSE will host the event and provide insights into the security challenges of developing and maintaining software solutions used by other companies worldwide to run mission critical deployments. For that the SUSE security team stays on top of current security threats and provides our customers with security updates even for very old code.
OpenSSL is a critical piece of software that SUSE maintains for its customers. As part of the Crypto-Day we will explain the challenges of maintaining such a crucial software component for a long time (up to 13 years).

Topics: The presented talks shall cover a broad spectrum from the field of cryptography or IT-security. We invite presentations of work-in-progress, contributions, which may be submitted to a conference, or summarize findings from a thesis or dissertation.
Submitted articles corresponding to the presentations will be arranged in a technical report. Therefore, submissions will be quotable publications and will be published on the web page. Observe that this does not forbid the publication of the result at other conferences or journals.

Attendance: There are **no participation fees**.

Submission: Please submit an abstract of your talk (**one DIN A4 page**). To simplify generation of the technical report, we request you to only use the LaTeX template of the cryptography group and to provide the PDF file additionally to the LaTeX sources.

Further Information (Program, Venue, LaTeX-template): http://www.kryptotag.de

Submission/Registration: Until **May 22, 2017** per email: kryptotag@lists.bit.uni-bonn.de

Organisation: Johannes Segitz, SUSE
Michael Nüsken, Universität Bonn
Frederik Armknecht, Universität Mannheim