Warum wir uns in der Kryptographie nicht auf die Komplexität physikalischer Angriffe verlassen sollten[1]

Juliane Krämer[2]

Abstract: Kryptographische Algorithmen müssen nicht nur mathematisch sicher, sondern auch resistent gegenüber physikalischen Angriffen sein, da physikalische Angriffe die Sicherheit von kryptographischen Algorithmen auch dann bedrohen, wenn die ihnen zugrunde liegende Mathematik eine hohe Sicherheit verspricht. Daher wird bei der Implementierung und Nutzung der Algorithmen sichergestellt, dass Gegenmaßnahmen gegen physikalische Angriffe berücksichtigt werden. Angriffe, die nur theoretisch bekannt sind, aber noch nicht praktisch realisiert wurden, werden dabei häufig außer Acht gelassen, wenn ihre praktische Durchführung als zu komplex eingeschätzt wird. Anhand der erstmaligen praktischen Durchführung zweier als zu komplex eingeschätzter physikalischer Angriffe (photonische Seitenkanal-Analyse sowie ein Instruction-Skip-Fehlerangriff gegen kryptographische Paarungen) zeigt diese Arbeit, dass die Einschätzung der physikalischen Angriffskomplexität fehlerhaft sein kann. Damit macht sie deutlich, dass auch solche Angriffe, die nur theoretisch bekannt sind, bei der Entwicklung von Schutzmechanismen berücksicht werden müssen, da sonst ein zu großes Risiko in Kauf genommen wird.

1 Physikalische Angriffe

Kryptologie ist die Kunst und die Wissenschaft der Geheimhaltung. Sie teilt sich auf in die Kryptographie und die Kryptoanalyse: In der Kryptographie werden Algorithmen entwickelt, die für Geheimhaltung sorgen sollen. Die Kryptoanalyse hingegen hat als Ziel, diese Algorithmen zu brechen und geheime Informationen aus kryptographischen Systemen zu ermitteln. Da kryptographische Algorithmen auf komplexen mathematischen Funktionen basieren, bestand das Ziel von Kryptoanalytikern über Jahrhunderte hinweg darin, mathematische Schwachstellen in solchen Algorithmen zu finden und auszunutzen. Mitte der neunziger Jahre des zwanzigsten Jahrhunderts änderte sich diese Situation grundlegend, als die ersten *physikalischen Angriffe* (oder *Implementierungsangriffe*) auf kryptographische Technologien vorgestellt wurden [Ko96, BDL97]. Diese Angriffe nutzen keine mathematischen Schwachstellen aus; im Gegenteil können sie einen Algorithmus sogar unabhängig von dessen mathematischer Stärke bedrohen. Es werden zwei unterschiedliche Arten der Implementierungsangriffe unterschieden: *Seitenkanalangriffe* (oder *passive* Implementierungsangriffe) messen während der Berechnung einer kryptographischen Operation physikalische Informationen, wie zum Beispiel den Stromverbrauch des Geräts, das die Operation berechnet. Aus der (statistischen) Analyse dieser Informationen kann ein Angreifer Rückschlüsse auf sicherheitsrelevante Daten, wie zum Beispiel den verwendeten geheimen Schlüssel, ziehen. *Fehlerangriffe* (oder *aktive* Implementierungsangriffe) hingegen greifen aktiv in die kryptographische Berechnung ein, indem zum Beispiel durch

[1] Englischer Titel der Dissertation: “Why Cryptography Should Not Rely on Physical Attack Complexity”

[2] Technische Universität Berlin/ Security in Telecommunications, juliane@sec.t-labs.tu-berlin.de

die kurzzeitige Veränderung der Spannung eines Mikrocontrollers ein Zwischenwert der Berechnung zufällig verändert wird. Ein Angreifer kann aus dem fehlerhaften Ergebnis wiederum Rückschlüsse auf geheime Informationen ziehen.

Seit ihrem öffentlichen Aufkommen vor 20 Jahren rückt die Bedrohung durch Seitenkanal- und Fehlerangriffe für elektronische Anwendungen wie Chip-Karten, elektronische Pässe oder RFID-Etiketten zunehmend in das Blickfeld der Forschung und der Industrie. Seitdem die ersten Seitenkanal- und Fehlerangriffe auf kryptographische Systeme vorgestellt wurden, werden kontinuierlich neue Möglichkeiten physikalischer Angriffe erforscht. Nach zahlreichen Untersuchungen sind solche Angriffe als ernsthafte Bedrohung für die Sicherheits-Industrie und alltägliche kryptographische Anwendungen wie im Internet of Things oder der Car-to-Car-Kommunikation akzeptiert worden. Der Gefahr, die von diesen Angriffen ausgeht, wird begegnet, indem auf bekannte Angriffe reagiert wird und Gegenmaßnahmen zum Schutz vor ihnen implementiert werden. Diese Gegenmaßnahmen finden sowohl auf Hardware- als auch auf Software-Ebene statt. So werden beispielsweise allgemeine Regeln entwickelt, die bei der Implementierung kryptographischer Algorithmen beachtet werden sollten, um die Verwundbarkeit gegenüber bestimmten Angriffen zu verringern. Bei physikalischen Angriffen, die zwar grundsätzlich bekannt sind, die jedoch noch nicht praktisch umgesetzt wurden, verhält es sich hingegen anders. Erst die praktische Realisierung eines Angriffs führt dazu, dass der Angriff wirklich ernst genommen wird, selbst wenn er in der Theorie schon lange bekannt und sehr mächtig ist. Insbesondere Angriffe, deren Realisierung eine hohe physikalische Komplexität zugeschrieben wird, werden weniger ernst genommen. Das Vertrauen darauf, dass diese Angriffe aufgrund ihrer physikalischen Komplexität tatsächlich nicht möglich sein werden, führt dazu, dass auf keiner Ebene Gegenmaßnahmen für sie entwickelt werden. Dieses Vorgehen ist problematisch, wenn sich im Nachhinein durch die Realisierung solcher Angriffe die Einschätzung der Komplexität als falsch erweist.

1.1 Wissenschaftlicher Beitrag

Die Dissertation *Why Cryptography Should Not Rely on Physical Attack Complexity* [Kr15] präsentiert zwei praktische physikalische Angriffe, deren Theorie bereits seit mehreren Jahren bekannt ist. Da diese Angriffe jedoch zuvor nicht erfolgreich praktisch umgesetzt wurden, wurde in ihnen keine Gefahr gesehen. Die vermeintliche Komplexität ihrer Durchführung wurde als ausreichender Schutz vor ihnen wahrgenommen. Diese Dissertation zeigt jedoch, dass die Komplexität der Durchführung dieser beiden Angriffe überschätzt wurde und Sicherheitssysteme daher nicht frühzeitig gegen sie geschützt wurden. Damit ist sie auch eine Warnung, diesen Fehler bei anderen möglichen Angriffen bzw. technischen Entwicklungen nicht zu wiederholen, um die durch Kryptographie bereitgestellte Sicherheit auch zukünftig zu gewährleisten.

Zunächst wird der *photonische Seitenkanal* vorgestellt, der neben der zeitlichen die größtmögliche räumliche Auflösung bietet, aufgrund der hohen Kosten bei seiner ersten Anwendung jedoch lange nicht ernst genommen wurde. Sowohl einfache als auch differentielle photonische Seitenkanalanalysen werden präsentiert [Sc12, Sc13, Kr13, KKS14].

Anschließend wird ein *Fehlerangriff auf paarungsbasierte Kryptographie* vorgestellt, der aufgrund der Notwendigkeit zweier unabhängiger präziser Fehler in einer einzigen Paarungsberechnung bei der Entwicklung von Gegenmaßnahmen nicht berücksichtigt wurde [Bl14]. Es wird gezeigt, wie Angreifer mit Hilfe dieser physikalischen Angriffe geheimes Schlüsselmaterial symmetrischer und asymmetrischer Algorithmen ermitteln können. Anschließend werden Gegenmaßnahmen auf Software- und Hardware-Ebene beschrieben, mit deren Hilfe diesen neuen Angriffen zukünftig standgehalten werden kann. Nicht wenige dieser Gegenmaßnahmen hätten auch entwickelt und implementiert werden können, ohne die Angriffe praktisch durchzuführen.

2 Der photonische Seitenkanal

Die Möglichkeiten des photonischen (oder optischen) Seitenkanals wurden 2008 der interessierten Öffentlichkeit bekannt [FH08]. Mit dem Aufkommen dieses Seitenkanals war ein ganz neuer und sehr gefährlicher Angriffsvektor gefunden worden. Der entscheidende Unterschied der photonischen Analyse gegenüber anderen bis dahin bekannten Seitenkanalangriffen wird deutlich, wenn bedacht wird, dass diese ausschließlich globale physikalische Informationen liefern, deren Veränderung im Zeitverlauf betrachtet wird. Eine Stromverbrauchsanalyse einer Smart Card beispielsweise misst den Stromverbrauch der gesamten Smart Card während einer kryptographischen Operation und analysiert, wie er sich währenddessen verändert. Die Messung photonischer Emissionen hingegen erlaubt nicht nur eine zeitliche, sondern zusätzlich eine räumliche Auflösung. Dadurch wird nicht nur die globale Photonen-Emission des Chips gemessen, sondern die zeitliche Entwicklung der Emission pro räumlichem Messpunkt detektiert. Je nach Qualität der Messinstrumente können die Emissionen für jeden Transistor einzeln gemessen werden. Gerade diese gemeinsame räumliche und zeitliche Auflösung von Seitenkanalinformationen birgt völlig neue Möglichkeiten für Angriffe und damit neue Risiken für die Sicherheits-IC-Industrie. Im extremen Fall kann die lokalisierte Auflösung jegliche Gegenmaßnahmen, die zu den vorher bekannten Strom-, Zeit- und elektromagnetischen Seitenkanal-Angriffen entwickelt worden sind, außer Kraft setzen.

Die Autoren der ersten Veröffentlichung nutzten zwar ein sehr mächtiges, jedoch auch extrem teures Messverfahren, welches auf der sogenannten Picosecond Imaging Circuit Analyse (PICA) basiert. Mit Hilfe eines solchen Instruments konnten die Autoren bereits das grundlegende Prinzip der photonischen Seitenkanalanalysen zeigen, indem Emissionen einzelner Regionen eines Mikrocontroller-Dies separat gemessen wurden. Aufgrund der hohen Kosten für das PICA-Equipment schlossen die Autoren allerdings aus, dass dieser neue Seitenkanal eine realistische Bedrohung darstellt. Ebenso wurde er weder von der Forschung noch von der Industrie als relevant eingestuft.

Diese Dissertation erbringt den endgültigen Beweis, dass photonische Seitenkanal-Angriffe in der Praxis sicherheitsrelevant sind. Die Arbeit zeigt, dass es auch mit wesentlich günstigeren optischen Methoden möglich ist, die Herausforderungen der zeitlich und örtlich hochaufgelösten Photonen-Messung zu bewältigen. Indem mathematisch und kryptographisch anspruchsvolle Analysen entwickelt und implementiert wurden, wird gezeigt, wie

Abb. 1: Optisches Emmissions-Bild der AES-S-Box, gespeichert im SRAM eines ATMega328P-Mikrocontrollers der Firma Atmel. Die 256 Bytes der S-Box sind in 32 Speicherzeilen mit je 8 Bytes gespeichert. Die Emissionen der Zeilentreiber, die links der entsprechenden Speicherzeilen im roten Rechteck zu sehen sind, sind deutlich sichtbar und ermöglichen die sogenannte *Simple Photonic Emission Analysis*.

photonische Seitenkanalinformationen kryptographische Geheimnisse preisgeben können. Es wird gezeigt, dass bisherige Gegenmaßnahmen gegen Seitenkanalangriffe bei weitem nicht ausreichen, um Sicherheitssysteme in Bezug auf den photonischen Seitenkanal zu schützen. Um die praktische Durchführbarkeit unter Beweis zu stellen, wurde eine Implementierung des symmetrischen Standards AES auf verschiedenen Mikrocontrollern der Firma Atmel angegriffen. Insbesondere die SubBytes-Operation wurde auf verschiedene Arten zum Ziel der Analyse. In allen Fällen konnte der geheime Schlüssel fehlerfrei extrahiert werden, unabhängig davon, ob AES-128, AES-192 oder AES-256 angegriffen wurde. In der *Simple Photonic Emission Analysis*, siehe Abbildung 1, wurden Zugriffe auf die in SRAM gespeicherte S-Box direkt beobachtet. Dadurch konnte, mit Wissen über den verwendeten Klartext der Verschlüsselung, der mögliche Schlüsselraum deutlich eingegrenzt und in vielen Fällen, abhängig von der konkreten Speicherung der S-Box, auf einen einzigen möglichen Kandidaten beschränkt werden. In verschiedenen differentiellen Analysen (*Differential Photonic Emission Analysis*) wurde der geheime Schlüssel ebenfalls eindeutig extrahiert. Hierfür wurden erneut Zugriffe auf die S-Box beobachtet, jedoch durch Messung der Emissionen eines Adress-Busses während des Ladens der entsprechenden Speicher-Adresse. Mit Hilfe verschiedener statistischer Methoden, zum Beispiel Difference of Means, Pearson-Korrelation und dem stochastischen Ansatz, konnte der geheime Schlüssel bestimmt werden.

Aufbauend auf den erfolgreichen praktischen photonischen Seitenkanal-Angriffen gegen AES wurde beschrieben, wie auch andere kryptographische Algorithmen mit der pho-

tonischen Analyse angegriffen werden können. Um zu zeigen, wie diese Seitenkanal-Angriffe verhindert oder zumindest deutlich erschwert werden können, wurden anschließend Gegenmaßnahmen zur Abwendung dieser Angriffe entwickelt. Die Software-Gegenmaßnahmen bestehen einerseits aus allgemeinen Implementierungsempfehlungen (z.B. Randomisierung), zum anderen aus AES- und Blockchiffre-spezifischen Ansätzen (zum Beispiel die erzwungene Nutzung einer S-Box, die am Anfang einer SRAM-Zeile ausgerichtet ist). Weiterhin werden Gegenmaßnahmen auf Hardware-Ebene beschrieben, wie zum Beispiel solche, die das Öffnen eines ICs von der Rückseite, wie es für die Durchführung photonischer Seitenkanalangriffe nötig ist, detektieren.

Der photonische Seitenkanal wird mittlerweile auch vom Bundesnachrichtendienst ernstgenommen [Z14] und hat in weiteren sicherheitskritischen Forschungsergebnissen, wie zum Beispiel in der Analyse von Timing-PUFs (PUF = Physical Unclonable Function), Anwendung gefunden [Ga15].

3 Fehlerangriffe auf paarungsbasierte Kryptographie

Paarungsbasierte Kryptographie ist in den letzten Jahren für die Kryptographie interessant geworden, da sie unter anderem verspricht, identitätsbasierte Kryptographie realisieren zu können [BF01]. Identitätsbasierte Kryptographie ist eine Form der Public-Key-Kryptographie, bei der der öffentliche Schlüssel jedes Teilnehmers direkt mit dessen Identität zusammenhängt (beispielsweise könnte die Email-Adresse eines Teilnehmers sein öffentlicher Schlüssel sein). Identitätsbasierte Kryptographie bietet für viele Anwendungen, zum Beispiel Sensornetze, die in der Industrie 4.0 große Bedeutung haben, entscheidende Vorteile. Diese betreffen vor allem die vereinfachte Schlüsselverwaltung. Seit ihrer ersten Beschreibung Mitte der achtziger Jahre konnten sie aufgrund fehlender mathematischer Methoden nicht praktisch realisiert werden. Paarungen jedoch versprechen, identitätsbasierte Kryptographie sicher und effizient umsetzen zu können.

Da die paarungsbasierte Kryptographie durch dieses Versprechen in den Fokus der kryptographischen Forschung kam, begannen viele Forscher, auch Fehlerangriffe auf sie zu entwickeln, siehe zum Beispiel [PV04, PV, El09]. Die Berechnung von Paarungen hat jedoch eine entscheidende Eigenschaft, die dazu führte, dass sie lange als resistent gegenüber Fehlerangriffen eingeschätzt wurden und die Fehlerangriffe nur theoretisch beschrieben werden konnten: Eine mathematische Paarung bekommt zwei Eingaben und besteht aus der Berechnung zweier aufeinanderfolgender Funktionen (Miller-Funktion und finale Exponentiation), die beide jeweils für sich schwierig zu invertieren sind. Ein Angreifer müsste aber die gesamte Paarung, also beide Unterfunktionen, invertieren, um geheime Informationen zu erhalten, da diese ein Teil der Eingabe der Paarung sind. Ein entsprechender Fehlerangriff, der die mathematischen Invertierungen umgehen oder deutlich erleichtern könnte, müsste laut aktuellem Wissen daher aus mehreren Fehlern bestehen, da ein einzelner Fehler im Allgemeinen nur eine einzelne Funktion betrifft, so dass die Nicht-Invertierbarkeit der anderen Funktion als Schutz bestehen bliebe. Folglich müsste ein erfolgreicher praktischer Fehlerangriff auf eine Paarungsberechnung mindestens aus zwei unabhängigen Fehlern bestehen. Dies jedoch erschien viele Jahre unrealistisch, wie

verschiedene Zitate aus englischsprachigen Publikationen zeigen: *If the adversary can inject multiple faults [...], then an attack could be launched. This however, is an unrealistic attack scenario* [WS07] und *[...] how to properly override the Final Exponentiation in conjunction with a fault attack on the Miller Algorithm remains an open problem [...]* [La14].

Diese Dissertation zeigt, dass Fehlerangriffe auf paarungsbasierte Kryptographie durchaus realistisch sind und eine reale Gefahr darstellen - trotz der Notwendigkeit zweier unabhängiger Fehler. Der Fehlerangriff wurde physikalisch durch sogenanntes Clock-Glitching realisiert. Hierbei wird das Abarbeiten der Befehle im Mikrocontroller gestört, indem kurzzeitig eine falsche Taktfrequenz eingebracht wird. Dies führt zum Überspringen, das heißt Nicht-Ausführen, einzelner Operationen. Das entwickelte Angriffs-Setup erlaubt nicht nur das Überspringen von zwei Operationen, sondern ermöglicht es theoretisch sogar, bis zu 256 unabhängige Einzel-Operationen zielgerichtet zu überspringen. Nach der erfolgreichen Einbringung beider Fehler kann das fehlerhafte Ergebnis der Paarungsberechnung analysiert werden, so dass die geheime Eingabe der Paarung ermittelt werden kann. Für diese mathematische Analyse wurden unter anderem Gröbner-Basis-Techniken genutzt. Um die praktische Relevanz dieses Angriffs zu erhöhen, wurden nur solche Geräte und Zubehör zu seiner Durchführung genutzt, die im Gebiet der Fehlerangriffe als günstig gelten.

Um die Gefahr, die von Fehlerangriffen auch auf paarungsbasierte Kryptographie ausgeht, abzuschwächen, werden in dieser Arbeit verschiedene Gegenmaßnahmen vorgestellt. Hierbei wird die Eigenschaft der durchgeführten Fehler berücksichtigt: Bestimmte Überprüfungen, die zur Detektion von Fehlerangriffen häufig in Algorithmen eingebaut werden, erweisen sich als unwirksam, wenn berücksichtigt wird, dass auch eine solche Überprüfung mit einem weiteren Fehler leicht übersprungen werden kann. Jedoch gibt es auch hier mit Hilfe von Randomisierung die Möglichkeit, Implementierungen zu stärken. Dies ist in diesem Fall möglich, da der exakte Zeitpunkt der Ziel-Operation bekannt sein muss, um einen efolgreichen Fehler einzubringen. Wird der Algorithmus zeitlich randomisiert berechnet, wird dies erschwert. Weitere Gegenmaßnahmen betreffen konkret die Paarungen. Beispielsweise ist es sehr effektiv, das Ergebnis einer Paarungsberechnung zu hashen, bevor es veröffentlicht (und damit auch dem Angreifer zugänglich gemacht) wird.

4 Fazit

Beide Angriffe, die in dieser Dissertation praktisch realisiert werden, waren bereits vorher in der Theorie bekannt. Jedoch wurden sie nicht als Bedrohung für Sicherheits-Systeme wahrgenommen, da ihre praktische Durchführung für zu komplex gehalten wurden. Fahrlässig wurden also Sicherheitslücken in Sicherheits-Systemen in Kauf genommen.

Anhand der beiden vorgestellten Angriffe zeigt diese Arbeit, dass die Einschätzung physikalischer Angriffskomplexität fehlerhaft sein kann. Es ist daher falsch, auf sie zu vertrauen. Die Entwicklung von Gegenmaßnahmen erfordert häufig nicht die erfolgreiche Durchführung praktischer Angriffe, sondern kann bereits erfolgen, sobald das Prinzip eines Seitenkanals oder eines Fehlerangriffs verstanden ist. Kryptographische Technologien

sollten daher gegenüber sämtlichen physikalischen Angriffen geschützt werden, seien diese bereits praktisch umgesetzt oder nur theoretisch bekannt.

Dass die Gefahr zukünftiger technischer Entwicklungen in anderen Bereichen der Kryptographie bereits antizipiert wird, zeigt sich teilweise in aktueller Forschung an zukünftigen Public-Key-Algorithmen: Da alle heute genutzten Algorithmen für Public-Key-Kryptographie von Quantencomputern, die nach Aussage von Experten in einigen Jahren Realität werden könnten (die Europäische Union rechnet damit, dass im Jahr 2035 ausreichend große universelle Quantencomputer existieren [Z16]), gebrochen werden können, wird bereits heute an Alternativen, sogenannter Post-Quantum-Kryptographie, geforscht.

Literaturverzeichnis

[BDL97] Boneh, Dan; DeMillo, Richard A.; Lipton, Richard J.: On the Importance of Checking Cryptographic Protocols for Faults. In (Fumy, Walter, Hrsg.): Advances in Cryptology - EUROCRYPT '97. Jgg. 1233 in Lecture Notes in Computer Science. Springer Berlin Heidelberg, S. 37–51, 1997.

[BF01] Boneh, Dan; Franklin, Matthew K.: Identity-Based Encryption from the Weil Pairing. In (Kilian, Joe, Hrsg.): Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference. Jgg. 2139 in Lecture Notes in Computer Science. Springer-Verlag, S. 213–229, 2001.

[Bl14] Blömer, Johannes; Gomes da Silva, Ricardo; Günther, Peter; Krämer, Juliane; Seifert, Jean-Pierre: A Practical Second-Order Fault Attack against a Real-World Pairing Implementation. In: 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). 2014. To appear. Updated version at https://eprint.iacr.org/2014/543.

[El09] El Mrabet, Nadia: What about Vulnerability to a Fault Attack of the Miller's Algorithm During an Identity Based Protocol? In: Proceedings of the 3rd International Conference and Workshops on Advances in Information Security and Assurance. ISA '09. Springer Berlin Heidelberg, S. 122–134, 2009.

[FH08] Ferrigno, J.; Hlaváč, M.: When AES blinks: introducing optical side channel. Information Security, IET, 2(3):94 –98, 2008.

[Ga15] Ganji, Fatemeh; Krämer, Juliane; Seifert, Jean-Pierre; Tajik, Shahin: Lattice Basis Reduction Attack against Physically Unclonable Functions. In (Ray, Indrajit; Li, Ninghui; Kruegel, Christopher, Hrsg.): Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015. ACM, S. 1070–1080, 2015.

[KKS14] Krämer, Juliane; Kasper, Michael; Seifert, Jean-Pierre: The Role of Photons in Cryptanalysis. In: 19th Asia and South Pacific Design Automation Conference, ASP-DAC 2014. IEEE, S. 780–787, 2014.

[Ko96] Kocher, Paul C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In (Koblitz, Neal, Hrsg.): Advances in Cryptology - CRYPTO 1996, 16th Annual International Cryptology Conference. Jgg. 1109 in Lecture Notes in Computer Science. Springer, S. 104–113, 1996.

[Kr13] Krämer, Juliane; Nedospasov, Dmitry; Schlösser, Alexander; Seifert, Jean-Pierre: Differential Photonic Emission Analysis. In (Prouff, Emmanuel, Hrsg.): Constructive Side-Channel Analysis and Secure Design - 4th International Workshop, COSADE 2013. Jgg. 7864 in Lecture Notes in Computer Science. Springer Berlin Heidelberg, S. 1–16, 2013.

[Kr15] Krämer, Juliane: , Why cryptography should not rely on physical attack complexity. http://dx.doi.org/10.14279/depositonce-4523, 2015. Dissertation, Technische Universität Berlin.

[La14] Lashermes, Ronan; Paindavoine, Marie; El Mrabet, Nadia; Fournier, Jacques; Goubin, Louis: Practical Validation of Several Fault Attacks against the Miller Algorithm. In: 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). 2014.

[PV] Page, Daniel; Vercauteren, Frederik: A Fault Attack on Pairing-Based Cryptography. IEEE Transactions on Computers, 55(9):1075–1080.

[PV04] Page, Daniel; Vercauteren, Frederik: Fault and Side-Channel Attacks on Pairing Based Cryptography. IACR Cryptology ePrint Archive, Report 2004/283, 2004.

[Sc12] Schlösser, Alexander; Nedospasov, Dmitry; Krämer, Juliane; Orlic, Susanna; Seifert, Jean-Pierre: Simple Photonic Emission Analysis of AES - Photonic side channel analysis for the rest of us. In: Cryptographic Hardware and Embedded Systems - CHES 2012. Lecture Notes in Computer Science, 2012.

[Sc13] Schlösser, Alexander; Nedospasov, Dmitry; Krämer, Juliane; Orlic, Susanna; Seifert, Jean-Pierre: Simple photonic emission analysis of AES. J. Cryptographic Engineering, 3(1):3–15, 2013.

[WS07] Whelan, Claire; Scott, Michael: The Importance of the Final Exponentiation in Pairings When Considering Fault Attacks. In: Pairing. Jgg. 4575 in Lecture Notes in Computer Science. Springer Berlin Heidelberg, S. 225–246, 2007.

[Z14] Wie der BND Verschlüsselung knacken will. http://www.zeit.de/digital/datenschutz/2014-11/bnd-chipanalyse-triphemos-verschluesselung-knacken/komplettansicht, 2014. abgerufen am 31. Januar 2016.

[Z16] Eine Milliarde Euro als Quantenbeschleuniger. http://www.faz.net/aktuell/wissen/physik-mehr/eu-will-entwicklung-der-quantentechnologie-foerdern-14236502.html, 2016. abgerufen am 10. Juni 2016.

Juliane Krämer studierte Wirtschaftsmathematik an der Technischen Universität (TU) Berlin und promovierte anschließend ebenda am Lehrstuhl Security in Telecommunications bei Prof. Dr. Jean-Pierre Seifert. In ihrer Promotion beschäftigte sie sich mit Seitenkanal- und Fehlerangriffen und zeigte, dass kryptographische Implementierungen bereits gegen solche Angriffe geschützt werden müssen, bevor sie zum ersten Mal praktisch durchgeführt werden. Seit 2015 ist sie Postdoktorandin an der TU Darmstadt am Lehrstuhl CDC von Prof. Dr. Johannes Buchmann. Dort forscht sie primär an Gitter-Kryptographie, um eine Alternative für Public-Key-Algorithmen bereitzustellen, die resistent gegenüber Quantencomputern ist.