様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２０　日現在

機関番号：　８２６２６
研究種目：　若手研究(B)
研究期間：　2015～2017
課題番号：　１５Ｋ１６００６

研究課題名（和文）Development of Practical and Error-Resilient Encryption and Authentication Mechanisms for Cloud-based Security Systems

研究課題名（英文）Development of Practical and Error-Resilient Encryption and Authentication Mechanisms for Cloud-based Security Systems

研究代表者

Ｓｃｈｕｌｄｔ　Ｊａｃｏｂ（SCHULDT, Jacob）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：８０７５０８９３

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：クラウドコンピューティングの有用性は急速に高まるとともに、クラウドに基づく極めて多数の情報サービスの実利用がなされている。しかしながら、近年の研究成果に見られるように、これらのシステムを安全に機能させるためには、従来手法の利用では不十分であり、実際に実システムに対する具体的な攻撃手法が示されている。本研究では、クラウド上でも安全に機能する暗号および認証技術の開発を行う。特に、故意または事故により乱数生成部に問題が生じている場合や情報が部分的に漏えいしている場合の安全性に注目し、そのような状況においても安全な方式の設計を行う。

研究成果の概要（英文）：The advantages provided by the cloud computing paradigm have led to a rapid adaptation, and a large number of cloud-based systems and services are in use today. However, recent results illustrate that the standard approach to securing these systems is insufficient due to the unique properties of a cloud-based environment, and attacks on real-world implementations have been demonstrated. This research develops encryption and authentication mechanisms, which are central to the construction of practical security systems, that address security concerns in a cloud-based system. Specifically, the focus is on security using weak or maliciously manipulated randomness and security against leakage and tampering attacks, which are relevant for both virtual machines providing a cloud service and the devices accessing this service.

研究分野：　Information Security

キーワード：　public key encryption　signatures　related randomness　related key attacks

１．研究開始当初の背景

Cloud computing is becoming an increasingly popular paradigm and forms the basis of many deployed systems in use today. This is evidenced by the rise of cloud computing platforms such as Amazon Elastic Compute Cloud and Microsoft Azure. While the use of cloud platforms brings significant advantages, they also give rise to new security challenges which is not yet fully understood. In particular, virtualized environments have properties that are not taken into account in the traditional design and analysis of the cryptographic tools. Hence, security systems, which are believed to be secure in a conventional setting, might become insecure when used in a cloud-based setting. This is illustrated by a recent line of research which explores leakage of information, including private key material, from virtual machines running on commercial cloud platforms.

２．研究の目的

The focus of this research is on the development of cryptographic tools that can securely be deployed in a cloud-based environment. More specifically, the focus is on encryption for preserving confidentiality of both transmitted and stored data, as well as authentication of users and data. Both of these cryptographic techniques are essential building blocks in the vast majority of security systems in use today.

The research is mainly centered around two aspects of cloud-based systems which have been shown to be critical for security: firstly, the use of potentially weak or manipulated randomness, and secondly, leakage of ephemeral or secret values e.g. via tampering. These aspects are not taken into account in the standard approach to the design and analysis of encryption and authentication.

３．研究の方法

The research employs a formal approach to the analysis and design of the desired encryption and authentication mechanisms. Specifically, this includes the development of formal security models capturing the properties of a cloud-based environment as well as security proofs for candidate constructions of encryption and authentication schemes. This development has been done via a combination of experiments, insights and experience from previous research projects involving cloud computing, as well as collaboration with external and internal partners with expertise in analysis of real-world cryptographic protocols and implementations

４．研究成果

A number of results have been obtained throughout the duration of the project. In the following, these are separated into two groups: results regarding weak or manipulated randomness and results regarding tampering attacks.

Results related to weak randomness

(1) *Development of a generic transformation for hardening public key encryption schemes to be secure against certain types of related randomness attacks*. This result demonstrates how any public key encryption scheme can be converted into a scheme secure against related randomness attacks for hard-to-invert relations, thereby providing a general technique for achieving basic security properties desirable in a cloud-based environment. This result was published in the proceedings of IMA Cryptography and Coding 2015, and was furthermore awarded the best paper award.

(2) *Analysis of the security of the standardized RSA-OAEP encryption scheme and RSA-PSS signature scheme when used with weak or maliciously manipulated randomness, which can occur in cloud-based environments based on virtualization*. This result builds upon the result from (1), and shows that as long as encryption is not done for malicious parties, the widely used RSA-OAEP encryption scheme remains secure, even when used with weak or maliciously manipulated randomness. Furthermore, it is shown that a number of other standardized encryption schemes, including RSA-KEM (part of ISO 18033-2) and DHIES (part of IEEE P1363a) cannot provide similar security guarantees. Finally, it is shown that the RSA-PSS is secure against any type of randomness manipulation. This provide guidelines as to what standardized scheme to use in a cloud-based setting in which weak or maliciously manipulated randomness is a concern. These results were published in the proceedings of ACM Asia CCS, 2017.

(3) *Research into a new type of attack in which the considered system makes use of a maliciously designed pseudorandom generator*. It is shown that backdoors can be placed into the design of the type of pseudorandom generators typically employed in operating systems, which are undetectable while still allowing an adversary to completely break security. The recent

controversy regarding the standardized Dual EC-DRBG pseudorandom generator highlights the relevance of this type of attack. This research has led to results published in the proceedings of CRYPTO'16, the highest ranking conference on cryptography according to Google Scholar.

(4) *Analysis of the related randomness security model for encryption and a new general conversion technique for achieving security for any maliciously chosen randomness relation.* This research shows that security for arbitrarily complex randomness relations cannot be achieved in the standard related randomness security model used to analyze weak or maliciously chosen randomness. However, a general transformation is shown that achieves security for arbitrary relations in a setting in which the attacker has limited time to attack the system before new entropy is added to the system. This reflects observations made for reset attacks on virtual machines. These results led to a publication in the proceedings of PKC'18.

Results related to tampering attacks

(1) *Investigation and enhancements of the security against related key attacks of commonly used signature schemes*. Security against related key attacks should be considered for devices that might be captured and tampered with by an adversary, and are hence relevant for cloud-based systems in which IoT or mobile user devices interact with a cloud-based service. In this research, enhancements to commonly used signature schemes that strengthen the security against related key attacks are proposed. Such schemes might be used to authenticate data from a device or the device itself. The initial results were published in the proceedings of Information Security and Cryptology 2015, while an extended set of results were published in the IEICE Transactions, 2017.

(2) *Related key attacks for non-interactive key-exchange (NIKE) schemes*. A NIKE scheme is closely related to encryption, but instead of encrypting data, a NIKE scheme allows a common session key to be derived in a non-interactive manner. This research extends related key attack security to NIKE schemes. Specifically, four different models capturing different aspects of security against related key attack for NIKE schemes are proposed, and relations among these are shown. Finally, a previously proposed NIKE scheme is shown secure in the strongest security model, based on standard assumptions. These results were published in IEICE Transactions, 2017.

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　　2 件）

(1) Hiraku Morita, Jacob C. N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, Tetsu Iwata: *On the Security of Schnorr Signatures, DSA, and ElGamal Signatures against Related-Key Attacks*. IEICE Transactions 100-A(1): 73-90 (2017).

(2) Hiraku Morita, Jacob C. N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, Tetsu Iwata: *On the Security of Non-Interactive Key Exchange against Related-Key Attacks*. IEICE Transactions 100-A(9): 1910-1923 (2017)

〔学会発表〕（計　　5 件）

(1) Takahiro Matsuda, Jacob C. N. Schuldt: *Related Randomness Security for Public Key Encryption, Revisited*. 21st IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'18), Proceedings, Part I, Lecture Notes in Computer Science 10769, pp. 280-311, Springer 2018.

(2) Jacob C. N. Schuldt, Kazumasa Shinagawa: *On the Robustness of RSA-OAEP Encryption and RSA-PSS Signatures Against (Malicious) Randomness Failures*. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (AsiaCCS 2017), pp. 241-252, ACM 2017.

(3) Jean Paul Degabriele, Kenneth G. Paterson, Jacob C. N. Schuldt, Joanne Woodage: *Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results*. 36th Annual International Cryptology Conference (CRYPTO'16), Proceedings, Part I, Lecture Notes in Computer Science 9814, pp. 403-432, Springer 2016.

(4) Hiraku Morita, Jacob C. N. Schuldt, Takahiro Matsuda, Goichiro Hanaoka, Tetsu Iwata: *On the Security of the Schnorr Signature Scheme and DSA Against Related-Key Attacks*. Information Security and Cryptology 2015, Lecture Notes in Computer Science 9558, pp. 20-35, Springer, 2015.

(5) Kenneth G. Paterson, Jacob C. N. Schuldt, Dale L. Sibborn, Hoeteck Wee: *Security Against Related Randomness Attacks via Reconstructive Extractors*. IMA International Conference on

Cryptography and Coding 2015, Proceedings, Lecture Notes in Computer Science 9496 pp. 23-40, Springer 2015.

〔図書〕（計　　0 件）

〔産業財産権〕

○出願状況（計　　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
https://www.itri.aist.go.jp/crypto/researcher/jacob.html

６．研究組織

(1)研究代表者
SCHULDT Jacob
国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：*80750893*

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：

(4)研究協力者

PATERSON Kenneth
Royal Holloway, University of London, UK

DEGABRIELE Jean Paul
Royal Holloway, University of London, UK

WOODAGE Joanne
Royal Holloway, University of London, UK

WEE Hoeteck
Ecole Normale Superieure, Paris, France

MATSUDA Takahiro
Advanced Cryptosystems Research Group, National Institute of Industrial Science and Technology (AIST)

HANAOKA Goichiro
Advanced Cryptosystems Research Group, National Institute of Industrial Science and Technology (AIST)

MORITA Hiraku
Advanced Cryptosystems Research Group, National Institute of Industrial Science and Technology (AIST)

IWATA Tetsu
Department of Computational Science and Engineering, Nagoya University