Marco Grimm

Konzept zum durchgängigen Schutz von Daten in der verteilten additiven Fertigung

SHAKER VERLAG

Konzept zum durchgängigen Schutz von Daten in der verteilten additiven Fertigung

Vom Fachbereich Maschinenbau
an der Technischen Universität Darmstadt
zur
Erlangung des Grades eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

DISSERTATION

vorgelegt von

Marco Grimm, M.Sc.

aus Frankfurt am Main

Berichterstatter:	Prof. Dr.-Ing. Reiner Anderl
Mitberichterstatter:	Prof. Dr.-Ing. Matthias Weigold
Tag der Einreichung:	21. Mai 2019
Tag der mündlichen Prüfung:	17. Juli 2019

Darmstadt 2019

D17

Forschungsberichte aus dem Fachgebiet
Datenverarbeitung in der Konstruktion

Band 67

Marco Grimm

Konzept zum durchgängigen Schutz von Daten in der verteilten additiven Fertigung

D 17 (Diss. TU Darmstadt)

Shaker Verlag
Düren 2020

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Darmstadt, Techn. Univ., Diss., 2019

ISBN 978-3-8440-7409-3
ISSN 1435-1129

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Telefon: 02421 / 99 0 11 - 0 • Telefax: 02421 / 99 0 11 - 9
Internet: www.shaker.de • E-Mail: info@shaker.de

Vorwort des Herausgebers

Die moderne Informations- und Kommunikationstechnologie (IKT) bietet vielfältige Innovations- und Leistungspotentiale, die im Entstehungsprozess neuer Produkte auszuschöpfen sind. Dies setzt jedoch voraus, dass die wissenschaftlichen Grundlagen zum Einsatz der modernen IKT in der Produktentstehung vorliegen und neue Methoden wissenschaftlich abgesichert sind. Darüber hinaus stellen die wissenschaftliche Durchdringung und die Bereitstellung wissenschaftlicher Forschungsergebnisse eine abgestimmte Kooperation zwischen Forschung und Industrie dar.

Vor diesem Hintergrund informiert diese Schriftenreihe über aktuelle Forschungsergebnisse des Fachgebiets Datenverarbeitung in der Konstruktion (DiK) des Fachbereichs Maschinenbau an der Technischen Universität Darmstadt.

Ziel der Forschungsarbeiten ist die wissenschaftliche Durchdringung innovativer, interdisziplinärer und integrierter Produktentstehungsprozesse und darauf aufbauend die Konzeption neuer Methoden für die Entwicklung, Konstruktion, Arbeitsvorbereitung und Herstellung neuer Produkte.

Die vorliegende Dissertation befasst sich mit der digitalen Prozesskette zur verteilten additiven Fertigung. Diese ist gekennzeichnet durch einen globalen Austausch von Bauteil- und Fertigungsdaten. Im Rahmen dieses unternehmensübergreifenden Datenaustauschs werden von verschiedenen Prozessakteuren Bauteile für die additive Fertigung optimiert, zu Aufträgen zusammengefasst und schließlich am Bestimmungsort gefertigt. Die moderne Informations- und Kommunikationstechnologie bietet hierzu mit ihrer Flexibilität und Schnelligkeit wichtige Wertschöpfungsfaktoren. Andererseits entstehen durch den digitalen Datenaustausch auch Risiken bezüglich Datenverlust und Manipulation. Diese Missbrauchsrisiken werden von den industriell etablierten Prozessketten zur additiven Fertigung nicht gelöst. Es sind heute noch keine geeigneten Mechanismen für eine effektive Nutzungskontrolle in der additiven Fertigung verfügbar, die nicht zu wesentlichen Einschränkungen bezüglich der Flexibilität führen. Die Folge ist, dass Bauteildaten heute in der Industrie weitgehend ungeschützt und unkontrolliert verarbeitet werden.

Herr Grimm nimmt sich dieser Problematik an und entwickelt in seiner Dissertation neue Ansätze für einen durchgängigen kryptografischen Schutz von Bauteil- und Fertigungsdaten in der additiven Fertigung. Er erweitert dazu die Prozesskette zur additiven Fertigung um neue Datensegmentierungs-, Pseudonymisierungs- und Verschlüsselungsschritte. Darauf aufbauend führt er eine auf Fertigungsattributen basierte Autorisierung von Anwendern und Systemen ein. Die Basis hierfür sind Prozessparameter und Einstellungen, welche relevant für die Arbeitsvorbereitung und Fertigung sind. Mit den aus Fertigungsattributen gebildeten Berechtigungen

erhalten Anwender und Fertigungssysteme ausschließlichen Zugriff auf die jeweils benötigten und für sie vorgesehenen Daten. Somit ist es möglich, das zugrunde liegende Bauteil- und Fertigungswissen ortsunabhängig und über die gesamte Prozesskette wirksam vor unberechtigten Zugriffen zu schützen, ohne die Flexibilität der Fertigung einzuschränken.

Die vorgestellten Methoden werden in einem Assistenzsystem und einem additiven Produktionssystem prototypisch umgesetzt. Abschließend wird der Prototyp anhand des hergeleiteten Anforderungsprofils verifiziert und mit typischen Anwendungsfällen aus der Praxis validiert.

Reiner Anderl

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Symbolverzeichnis

a, b, c	Ganzzahlige Parameter in endlichen Körpern
A, B, H	Koordinatensysteme zur Vektortransformation
α, β	Geheime Schlüsselparameter als Exponenten für MK
AT	Autorisierungsdaten der Autorisierungsinstanz
B	Baum der Berechtigungsrichtlinie
$c_{a,m}$	Schlüsseltext der Segmentzuordnungstabelle
c_i	Segment-Schlüsseltext mit Index i
C_i	Schlüsseltextblöcke mit Index i
C_m	Geschützer Inhaltsschlüssel k_m
C_{Policy}	Über Attribute geschützter Schlüsseltext
ctr_i	Inkrementierbarer Zähler für Blockchiffre
ΔP_{BM}	Relative Differenz (Verlust) der Betriebsmittelproduktivität
D_k	Entschlüsselungsfunktion mit Schlüssel k
E_k	Verschlüsselungsfunktion mit Schlüssel k
$e(g, g)$	Bilineare Paarung der Generatoren g in zwei Gruppen $\mathbb{G}_i$
g, h	Erzeuger (Generatoren) im endlichen Körper $\mathbb{Z}_p$
$\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_2$	Endliche Gruppen der Ornung p
$\mathbb{G}_T$	Endliche Zielgruppe einer bilinearen Paarung
$h_{SHA2}(m)$	Hashwert der Nachricht m mit der Hashfunktion SHA-2
ID	Identifikator
id_i	Segmentidentifikator mit Index i
IV	Initialisierungsvektor für die Blockchiffre
J_i	Teilmenge an Attributen

k	Einbettungsgrad
$k_{cA,i}, k_{cB,i}$	Teilschlüssel A und B
$k_{c,i}$	Inhaltsschlüssel für das Segment i
k_i	Symmetrischer Schlüssel mit Index i
k_m	Symmetrischer Schlüssel der Segmentzuordnungstabelle
m_i	Nachricht mit Index i
MK	Geheimer Generalschlüssel der Zertifizierungsstelle
M_m	Segmentzuordnungstabelle
$\vec{n}$	Normalenvektoren für Flächenfacetten
n_u	Nutzungszähler
p	Primzahl zur Festlegung der Ordnung einer Gruppe
${}^{A}\vec{p}$	Ortsvektor im Bezugssystem A
p_i	Klartext mit Index i
pk	Öffentlicher Schlüssel
ψ, θ, ϕ	Rotationswinkel im Koordinatensystem nach DIN 70000
PK	öffentlicher Schlüssel der attributbasierten Verschlüsselung
P, Q	Punkte auf einer elliptischen Kurve
P_i	Klartextblöcke mit Index i
r, h, q	Ganzzahlige Parameter für die Erzeugung von Paarungen
R	Wurzel des Berechtigungsbaums (Berechtigungsrichtlinie)
${}^{A}\boldsymbol{R}_{B}$	Rotationsmatrix des Bauteils im Bezugssystem A
s	Zufällige Parameter im Berechtigungsbaum
S	Im Schlüssel SK_i zugewiesene Attribute
S_i'	Bei der Zertifizierungsstelle gespeicherte Attribute
sig_m	Digitale Signatur der Nachricht m
sk	Privater geheimer Schlüssel
SK_M	Geheimer Schlüssel einer Maschine M

SK_N	Geheimer Schlüssel eines Nutzers N
SK_S	Geheimer Schlüssel eines Systems S
S_M	Menge an Attributen einer Maschine
T	Autorisierungstag
${}^{A}\boldsymbol{T}_{B}$	Homogene Transformationsmatrix im Bezugssystem A
t_a	Ablaufzeit
${}^{A}\vec{t}_{B}$	Bauteilverschiebungsvektor im Bezugssystem A
t_{BH}	Hauptzeit des Betriebsmittels
t_{BN}	Nebennutzungszeit des Betriebsmittels
$t_{BN,E}$	Nebennutzungszeitanteil Datenentschlüsselung
$t_{BN,S}$	Nebennutzungszeitanteil Schlüsselabruf
$t_{BN,Z}$	Nebennutzungszeitanteil Entschlüsselung der Segmentzuordnungstabelle
T_o	Eigentümertoken
t_{rv}	Entzugszeitpunkt (Revokation) der Berechtigungen
T_u	Anwendertoken
$t_{u,i}$	Authentisierungstoken mit Index i (z.B. Anwendertoken)
V, Y	Baumknoten V und Blätter Y
$\vec{v_i}$	Ortsvektoren für Eckpunkte
$\mathbb{Z}_p$	Endlicher Körper der Primordnung p

Abkürzungsverzeichnis

2D	zweidimensional
3D	dreidimensional
3MF	3D Manufacturing Format
AABB	Axis Aligned Bounding Box
ABE	Attribute Based Encryption
ADC	Analog-Digital Converter
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AF	Additive Fertigung
AMF	Additive Manufacturing File Format
AM	Additive Manufacturing
API	Application Program Interface
AP	STEP Application Protocol
ARM	Advanced RISC Machines Architektur
ASCII	American Standard Code for Information Interchange
B-Rep	Boundary Representation
BPMN	Business Process Model and Notation
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnik
CAD	Computer Aided Design
CAM	Computer Aided Manufacturing
CAx	Computer Aided X
CA	Certificate Authority
CC	Common Criteria

CDH	Computational Diffie-Hellman Problem
CLI	Common Layer Interface
CNC	Computerized Numerical Control
CPU	Central Processing Unit
DBDH	Decisional Bilinear Diffie-Hellman Problem
DDH	Decisional Diffie-Hellman Problem
DES	Data Encryption Standard
DIN	Deutsche Industrie Norm
DLP	Discrete Logarithm Problem
DRM	Digital Rights Management
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ERM	Enterprise Rights Management
ERP	Enterprise Resource Planning
FDM	Fused Deposition Modeling
FLM	Fused Layer Modeling
GPL	GNU General Public License
GUI	Graphical User Interface
HMI	Human Machine Interface
HTTP	Hypertext Transport Protokoll
IBE	Identity Based Encryption
IC	Integrated Circuit
IDE	Integrated Development Environment
IKT	Informations- und Kommunikationstechnologie
IP	Intellectual Property
ISO	International Organization for Standardization

IT	Informationstechnologie
IV	Initialisierungsvektor
JSON	Javascript Object Notation
LAN	Local Area Network
LLM	Layer Laminated Manufacturing
MAC	Message Authentication Code
MCU	Microcontroller Unit
MPU	Microprocessor Unit
NC	Numerical Control
NDA	Non-Disclosure Aggreement
NIST	National Institute of Standards and Technology
OMAP	Open Multimedia Application Platform
OMG	Object Management Group
OS	Operating System
PDM	Produktdatenmanagement
PEP	Produktentstehungsprozess
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PLM	Product Lifecycle Management
PMI	Product Manufacturing Information
PRU	Programmable Realtime Unit
REFA	Verband für Arbeitsgestaltung, Betriebsorganisation und Unternehmensentwicklung
REST	Representational State Transfer
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RISC	Reduced Instruction Set Computer
RPT	Rapid Prototyping and Tooling
RSA	Rivest Shamir Adleman Cryptosystem

RTOS	Realtime Operating System
SADT	Structured Analysis and Design Technique
SBC	Single Board Computer
SHA	Secure Hash Algorithm
SIAM	Secure Information Exchange for Additive Manufacturing
SIM	Subscriber Identity Module
SLM	Selective Laser Melting
SLS	Selective Laser Sintering
SOA	Service-Oriented Architecture
SQL	Structured Query Language
STEP	Standard for the Exchange of Product Model Data
STL	Surface Triangulation Language
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
UML	Unified Modeling Language
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VDI	Verein Deutscher Ingenieure
VM	Virtuelle Maschine
VPN	Virtual Private Network
XML	Extensible Markup Language
XOR	Exklusiv-Oder-Funktion
XrML	Extensible Rights Markup Language