

1. Record Nr.	UNISA996464420203316
Titolo	Applied cryptography in computer and communications : first EAI International Conference, AC3 2021, virtual event, May 15-16, 2021, proceedings / / Bo Chen, Xinyi Huang (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-80851-3
Descrizione fisica	1 online resource (216 pages)
Collana	Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering ; ; v.386
Disciplina	005.82
Soggetti	Data encryption (Computer science) Telecommunication systems - Security measures Internet of things - Security measures Huang, Xinyi
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Blockchain -- Anchor: An NDN-Based Blockchain Network -- 1 Introduction -- 2 Our Design -- 2.1 Random Anchor Selection -- 2.2 Two-Layer Cascaded NDN Design -- 2.3 Elimination of Duplicated Transmissions from Multiple Anchors -- 3 Performance Evaluation -- 4 Conclusion -- References -- An Identity-Based Blind Signature and Its Application for Privacy Preservation in Bitcoin -- 1 Introduction -- 2 Preliminaries -- 2.1 Tate Bilinear Pairings -- 2.2 Computational Diffie-Hellman Assumption -- 2.3 System Model -- 3 Review of Sarde et al.' Blind Signature Scheme -- 4 Attack on Sarde et al.' Blind Signature Scheme -- 5 Unlinkable ID-Based Blind Signature Scheme -- 6 Unlinkable ID-Based Proxy Blind Signature Scheme -- 7 Security Analysis -- 7.1 Analysis of Blind Signature -- 7.2 Analysis of Proxy Blind Signature -- 8 Performance Analysis and Comparison -- 9 Application for Privacy Preservation in Bitcoin -- References -- Blockchain-Based Sealed-Bid Domain Name Auction Protocol -- 1 Introduction -- 2 Models and Design Goals -- 2.1 System Model -- 2.2 Security Model -- 2.3 Design Goal -- 3 Preliminaries -- 3.1 Account-Based Consortium Blockchain -- 3.2

Auction Types -- 3.3 Pedersen Commitment -- 3.4 Zero-Knowledge Proof -- 4 Our Proposal -- 4.1 Create the Auction -- 4.2 Commit the Bid -- 4.3 Reveal the Bid -- 4.4 Close the Auction -- 5 Analysis of Our Proposal -- 5.1 Security Analysis -- 5.2 Performance Evaluation -- 6 Related Work -- 6.1 Blockchain-Based DNS -- 6.2 Blockchain-Based Auction -- 7 Conclusion -- References -- Authentication -- A Security Enhanced Key Management Service for ARM Pointer Authentication -- 1 Introduction -- 2 Background -- 2.1 Privilege and Exception Levels -- 2.2 Pointer Authentication -- 3 Threat Model -- 3.1 Attacks -- 3.2 Assumptions -- 4 Design -- 4.1 Architecture. 4.2 Algorithm -- 5 Implementation -- 5.1 EL3 Runtime Service -- 5.2 EL1 Kernel Module -- 5.3 EL0 Calling Convention -- 6 Evaluation -- 6.1 Security Analysis -- 6.2 Performance Analysis -- 7 Related Works -- 8 Conclusion -- References -- Privacy-Preserving ECC-Based Three-Factor Authentication Protocol for Smart Remote Vehicle Control System -- 1 Introduction -- 1.1 Threat Model -- 1.2 Related Works -- 1.3 Motivation and Contribution -- 1.4 Notations -- 1.5 Paper Organization -- 2 Review of Chatterjee et al.'s Scheme -- 2.1 System Initialization and Registration Phase -- 2.2 Authentication and Key Agreement Phase -- 3 Cryptanalysis of Chatterjee et al.'s Scheme -- 4 The Proposed Scheme -- 4.1 Pre-deployment Phase -- 4.2 User Registration Phase -- 4.3 Login and Authentication Phase -- 5 Security Analysis -- 5.1 BAN-Logic Based Proof of Authentication -- 5.2 Further Security Analysis -- 6 Performance Evaluation -- 6.1 Security Features -- 6.2 Computational Overhead -- 7 Conclusion and Future Work -- References -- Secure Computation -- Efficient and Private Divisible Double Auction in Trusted Execution Environment -- 1 Introduction -- 2 Divisible Double Auction -- 2.1 Models -- 2.2 Auction Properties -- 3 Mechanism Design -- 4 ETA System Design -- 4.1 SGX Formalization -- 4.2 ETA System -- 4.3 ETA Execution Program -- 4.4 Threat Model -- 4.5 Security Analysis -- 5 Experiments -- 5.1 ETA Performance Evaluation -- 5.2 Case Study -- 6 Related Work -- 7 Conclusion -- References -- Parallel Implementation and Optimization of SM4 Based on CUDA -- 1 Introduction -- 2 Preliminaries -- 2.1 CUDA -- 2.2 A Brief Description of SM4 -- 3 Parallel Design of SM4 -- 4 Experiment and Discussion -- 4.1 Basic Experiment -- 4.2 Performance Optimization -- 4.3 Analysis of Results -- 5 Conclusion -- References -- Another Algebraic Decomposition Method for Masked Implementation. 1 Introduction -- 2 Preliminaries -- 2.1 Functions over Finite Fields -- 3 Algebraic Decomposition -- 3.1 Algebraic Decomposition Using GM Polynomials -- 3.2 Experimental Result -- 4 Application to Masking -- 5 Conclusion -- A Masking for Quadratic Polynomial -- References -- Practical Crypto Application -- Concealed Communication in Online Social Networks -- 1 Introduction -- 2 Related Work -- 2.1 Privacy Analysis in Online Social Networks -- 2.2 Privacy Leakages -- 2.3 Privacy-Preserving Online Social Networks -- 2.4 Mix Networks -- 3 Proposed Protocols -- 3.1 A Concealed Secure Channel -- 3.2 User Information and Postings -- 3.3 Personal Messages and Group Messages -- 3.4 Groups -- 3.5 Finding and Verifying Participants, Exchanging Keys -- 3.6 Key Revocation -- 3.7 User Registration -- 4 Privacy Analysis -- 4.1 Attacker Model -- 4.2 Structure of Network (NS) -- 4.3 Structure of Data (DS) -- 4.4 Timing (T) -- 4.5 Control Information (CI) -- 5 Performance Analysis -- 6 Conclusions -- References -- MobiWear: A Plausibly Deniable Encryption System for Wearable Mobile Devices -- 1 Introduction -- 2 Background -- 2.1 Wearable Mobile Devices -- 2.2 Plausibly Deniable Encryption -- 2.3 Image Steganography -- 2.4 Digital Watermarking -- 2.5 Peak Signal-

to-Noise Ratio (PSNR) -- 3 Model and Assumptions -- 3.1 System Model -- 3.2 Adversarial Model -- 4 Design -- 4.1 Design Rationale -- 4.2 Design Details -- 5 Implementation and Evaluation -- 5.1 Implementation -- 5.2 Evaluation -- 6 Security Analysis and Discussion -- 6.1 Security Analysis -- 6.2 Discussion -- 7 Related Work -- 7.1 Plausibly Deniable Encryption Systems -- 7.2 Image Steganography -- 8 Conclusion -- References -- Recent Advances in the Web PKI and the Technical Challenges in SCMS -- 1 Introduction -- 2 Recent Advances in the Web PKI -- 2.1 Certificate Transparency. 2.2 Push-Based Certificate Revocation -- 3 The Technical Challenges in SCMS -- 3.1 The Expected Properties of V2V PKI Systems -- 3.2 SCMS -- 3.3 Technical Challenge #1: Certificate Transparency vs. Pseudonym Certificate -- 3.4 Technical Challenge #2: Push-Based Certificate Revocation vs. the Great Volume of Pseudonym Certificates -- 4 Conclusions -- References -- The First International Workshop on Security for Internet of Things (IOTS 2021) -- A Novel Approach for Code Smells Detection Based on Deep Learning -- 1 Introduction -- 2 Code Smells Detection Based on Convolutional Networks -- 3 High Level Design -- 3.1 Experiments Results -- 4 Conclusion -- References -- A Thieves Identification Scheme for Prepaid Systems in Smart Grids -- 1 Introduction -- 2 Related Work -- 3 The Framework -- 3.1 Network Model -- 3.2 Security Requirements -- 4 Our Proposed Approach -- 4.1 Setup -- 4.2 Joining -- 4.3 Power Purchasing -- 4.4 Power Requesting -- 4.5 Identification -- 5 Conclusion -- References -- Using Smart Contracts to Improve Searchable Symmetric Encryption -- 1 Introduction -- 2 Notations -- 3 Preliminaries -- 3.1 Scheme of Searchable Symmetric Encryption -- 3.2 Smart Contract -- 4 Scheme of the Integrity Verification of Search Results -- 4.1 Merkle Tree -- 4.2 Proof of Integrity Verification of Search Results -- 5 Smart Contract Based Searchable Symmetric Encryption -- 5.1 Scheme of Smart Contract Based SSE -- 5.2 Details of Smart Contract Based SSE Scheme -- 6 Security and Performance Analyses -- 6.1 Security Analysis -- 6.2 Performance Analysis -- 6.3 Experimental Analysis -- 7 Conclusion -- References -- Towards the Adaptability of Traffic-Based IoT Security Management Systems to the Device Behavior Evolutions -- 1 Introduction -- 2 IoT Security Management Systems -- 3 IoT Device Behavior Evolutions -- 4 Possible Solutions -- 5 Conclusion. References -- Author Index.

2. Record Nr.	UNINA9910794746003321
Titolo	AGB-Recht : Kommentar zu den [Paragrafen] 305-310 BGB und zum UKlaG // bearbeitet von Dr. Marcus Bieder, Universitätsprofessor in Osnabruck [and seven others]
Pubbl/distr/stampa	Koln : , : Otto Schmidt, , 2016
ISBN	3-504-38427-1
Edizione	[12. neu bearbeitete Auflage.]
Descrizione fisica	1 online resource (2,326 pages)
Classificazione	PD 3525
Soggetti	Standardized terms of contract - Germany Consumer protection - Law and legislation - Germany Actions and defenses - Germany
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	At head of title: Ulmer, Brandner, Hensen.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	AGB-Recht -- Frontmatter -- Vorwort zur zwölften Auflage -- Inhaltsverzeichnis -- Abkürzungs- und Literaturverzeichnis -- Bürgerliches Gesetzbuch (BGB) -- Gesetz über Unterlassungsklagen bei Verbraucherrechtsund anderen Verstößen (Unterlassungsklagengesetz -- UKlaG) -- Richtlinie 93/13/EWG des Rates vom 5.4.1993 über missbräuchliche Klauseln in Verbraucherverträgen -- Teil 1. Kommentierung der §§ 305–310 BGB -- Einleitung -- Buch 2. Recht der Schuldverhältnisse -- Abschnitt 2 Gestaltung rechtsgeschäftlicher Schuldverhältnisse durch Allgemeine Geschäftsbedingungen -- § 305 Einbeziehung Allgemeiner Geschäftsbedingungen in den Vertrag -- Anhang zu § 305 -- § 305a Einbeziehung in besonderen Fällen -- § 305b Vorrang der Individualabrede -- § 305c Überraschende und mehrdeutige Klauseln -- § 306 Rechtsfolgen bei Nichteinbeziehung und Unwirksamkeit -- § 306a Umgehungsverbot -- Vorbemerkungen zur Inhaltskontrolle -- § 307 Inhaltskontrolle -- § 308 Klauselverbote mit Wertungsmöglichkeit Nr. 1 -- § 309 Klauselverbote ohne Wertungsmöglichkeit Nr. 1 -- § 310 Anwendungsbereich -- Anhang zu § 310 AGB-Kontrolle im Arbeitsrecht -- Teil 2 Besondere Klauseln, Vertragstypen und AGB-Werke -- (1) Abtretungsausschluss -- (2) Anstellungsverträge für AG-Vorstandsmitglieder und GmbH-Geschäftsführer -- (3) Arbeitskampfklauseln, Streikklauseln -- (4)

Architekten- und Ingenieurverträge -- (5) Arztverträge -- (6)
 Automatenaufstellverträge -- (7) Autowaschanlagenverträge -- (8)
 Banken (Kreditinstitute) -- (9) Baubetreuungsverträge -- (10)
 Bausparbedingungen -- (11) Bauträgerverträge -- (12) Bauverträge --
 (13) Bierlieferungsverträge -- (14) Bildnisverwertungsklauseln -- (15)
 Bürgschaftsverträge -- (16) Darlehensverträge -- (17)
 Einkaufsbedingungen -- (18) Factoringverträge -- (19)
 Franchiseverträge -- (20) Garantieklauseln, Garantieverträge -- (21)
 Gerichtsstandsklauseln -- (22) Girocard-Sonderbedingungen -- (23)
 Gütertransportverträge -- (24) Handelsvertreterverträge -- (25)
 Heimverträge/Wohn- und Betreuungsverträge -- (26) Kaufverträge --
 (27) Kostenvoranschläge -- (28) Krankenhausverträge -- (29)
 Kreditkarten-AGB -- (30) Leasingverträge -- (31) Maklerverträge --
 (32) Mietverträge -- (33) Partnerschaftsvermittlungsverträge -- (34)
 Personenbeförderungsverträge -- (35)
 Qualitätssicherungsvereinbarungen -- (36) Rechtswahlklauseln -- (37)
 Reiseverträge -- (38) Reparaturverträge -- (39) Scheckbedingungen --
 (40) Schiedsgutachtenklauseln, Schieds-, Schlichtungs- und
 Mediationsklauseln -- (41) Schriftformklauseln -- (42)
 Schweigepflichtentbindungsklauseln im Gesundheitswesen -- (43)
 Sicherungsklauseln -- (44) Softwareverträge -- (45)
 Sportstudioverträge -- (46) Telekommunikationsverträge -- (47)
 Textilreinigungsverträge -- (48) Tilgungsbestimmungen (§§ 366, 367
 BGB) -- (49) Treuhandverträge -- (50) Unterrichtsverträge -- (51)
 Urheberrechtsverträge, Verlagsverträge -- (52) Verjährungsklauseln --
 (53) Versandhandelsverträge -- (54) Versicherungsbedingungen -- (55)
 Versorgungsbedingungen in Verträgen mit Sonderabnehmern -- (56)
 Versteigerungsbedingungen -- (57) Vertragshändlerverträge -- (58)
 VOB/B – Vergabe- und Vertragsordnung für Bauleistungen -- (59) VOL
 – Vergabe- und Vertragsordnung für Leistungen (ausgenommen
 Bauleistungen -- (60) Vollmachtsklauseln -- (61) Wartungsverträge --
 (62) Wertpapierbedingungen -- (63)
 Wohnungseigentum/Verwalterverträge -- (64) Zeitschriften- und
 Zeitungsabonnementsverträge -- (65) Zinsanpassungsklauseln -- Teil
 3 Kommentierung der AGB-rechtlichen Vorschriften des
 Unterlassungsklagengesetzes (UKlaG) -- Vorbemerkungen -- Abschnitt
 1. Ansprüche bei Verbraucherrechts- und anderen Verstößen --
 Abschnitt 2 Verfahrensvorschriften -- Abschnitt 3 Auskunft zur
 Durchsetzung von Ansprüchen -- Abschnitt 4 Außergerichtliche
 Schlichtung -- Abschnitt 5 Anwendungsbereich -- Abschnitt 6
 Überleitungsvorschriften -- Sachverzeichnis

Sommario/riassunto

Das Standardwerk zum AGB-Recht wurde erneut rundum auf aktuellen Stand gebracht. Die überaus umfangreiche Rechtsprechung der letzten Jahre war ebenso auszuwerten und einzuarbeiten wie die zwischenzeitlich erfolgten Gesetzesänderungen, etwa durch das Gesetz zur Umsetzung der Verbraucherrechte-Richtlinie und das Gesetz zur Bekämpfung von Zahlungsverzug im Geschäftsverkehr und zur Änderung des Erneuerbare-Energien-Gesetzes, das die neuen Klauselverbote in § 308 Nr. 1a und 1b BGB sowie die neue Vorschrift des § 1a UKlaG mit sich brachte, das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von Verbraucherschützenden Vorschriften des Datenschutzrechts mit dem neuen § 2b UKlaG und Änderungen im UKlaG und bei § 309 Nr. 13 BGB und das Gesetz zur Umsetzung der ADR-Richtlinie, das mit der Kommentierung des neuen § 309 Nr. 14 BGB bereits berücksichtigt werden konnte. Das bietet Ihnen der „Ulmer/Brandner/Hensen“: Kommentierung der §§ 305 – 310 BGB und der AGB-rechtlichen Vorschriften des UKlaG Detaillierte Erläuterung von 65 besonderen Klauseln, Vertragstypen und AGB-

Werken Auswertung und Systematisierung der umfangreichen Kasuistik
Praxisnahe Lösungsvorschläge Richtungweisende, meinungsbildende
Kommentierungen Wissenschaftlich fundierte, gut lesbare Darstellung
Berücksichtigung der Interessen von AGB-Verwendern und
Verbrauchern Aus dem Inhalt: §§ 305 – 310 BGB Besondere Klauseln
und Vertragstypen 1 Abtretungsausschluss 2 AG-
Vorstand/GmbHGeschäftsführer 3 Arbeitskampfklauseln 4
Architektenverträge 5 Arztverträge 6 Automatenaufstellverträge 7
Autowaschanlagen 8 Banken (Kreditinstitute) 9 Baubetreuungsverträge
10 Bausparbedingungen 11 Bauträgerverträge 12 Bauverträge 13
Bierlieferungsverträge 14 Bildnisverwertungsklauseln 15
Bürgschaftsverträge 16 Darlehensverträge 17 Einkaufsbedingungen 18
Factoringverträge 19 Franchiseverträge 20 Garantie 21
Gerichtsstandsklauseln 22 Girocard-Bedingungen 23
Gütertransportverträge 24 Handelsvertreterverträge 25 Heimverträge
26 Kaufverträge 27 Kostenvoranschläge 28 Krankenhausverträge 29
Kreditkarten-AGB 30 Leasingverträge 31 Maklerverträge 32
Mietverträge 33 Partnerschaftsvermittlung 34 Personenbeförderung 35
Qualitätssicherung 36 Rechtswahlklauseln 37 Reiseverträge 38
Reparaturverträge 39 Scheckbedingungen 40 Schieds- und
Schlichtungsklauseln 41 Schriftformklauseln 42
Schweigepflichtentbindung 43 Sicherungsklauseln 44 Softwareverträge
45 Sportstudioverträge 46 Telekommunikationsverträge 47
Textilreinigungsverträge 48 Tilgungsbestimmungen 49
Treuhandverträge 50 Unterrichtsverträge 51 Urheber- und
Verlagsverträge 52 Verjährungsklauseln 53 Versandhandelsverträge 54
Versicherungsbedingungen 55 Versorgungsbedingungen 56
Versteigerungsbedingungen 57 Vertragshändlerverträge 58 VOB/B 59
VOL 60 Vollmachtsklauseln 61 Wartungsverträge 62
Wertpapierbedingungen 63 Wohnungseigentum 64
Zeitung abonements 65 Zinsanpassungsklauseln UKlaG
