Real World Crypto 2026 - Taipei Agenda

完整詳細議程表 (Full Detailed Schedule) | March 9 - 11, 2026

3/9 (Mon) 星期一

08:00 - 09:00

Registration｜報到

09:00 - 09:15

Welcome｜開幕致詞

RWC 2026 General Chair｜大會總主席

09:15 - 10:35

Session: Beyond Secure Messaging
安全通訊的下一篇章

Chair｜主持人：TBD

A Practical Wrapper Protocol for Metadata-Hiding in Messaging
通訊中繼資料隱匿之實用封裝協定
Authors: Lea Thiemt, Paul Rösler, Alexander Bienstock, Rolfe Schmidt, Yevgeniy Dodis
FAU Erlangen-Nürnberg, J.P. Morgan AI Research, Signal Messenger, NYU

Advanced Browsing Protection for Facebook Messenger
Facebook Messenger 之進階瀏覽防護
Authors: Emma Connor, Artem Ignatyev, Kevin Lewi
Meta

Improving the Trustworthiness of JavaScript on the Web
提升網頁 JavaScript 之可信度
Authors: Ezzudin Alkotob, Giulio Berra, Benjamin Beurdouche, Richard Hansen, Daniel Huigens, Dennis Jackson, Cory Francis Myers, Michael Rosenberg
Meta, Freedom of Press Foundation, Mozilla, Proton AG, Cloudflare

Signal Lost (Integrity): The Signal App is More than the Sum of its Protocols
訊號遺失(完整性): Signal App之整體大於協定總和
Authors: Kien Tuong Truong, Noemi Terzo, Peter Schwabe, Kenneth Paterson
ETH Zurich, Max-Planck Institute for Security and Privacy

10:35 - 11:05

Coffee Break｜茶敘

11:05 - 11:35

Levchin Prize

Chair: Dan Boneh

11:35 - 12:05

Invited Talk I｜特邀演講 I

12:05 - 13:35

Lunch｜午餐

3/10 (Tue) 星期二

09:00 - 10:20

Session: Real World Privacy
真實世界中的隱私

Chair: TBD

Deploying Research: On Building and Shipping an Anonymous Whistleblowing System
研究部署：建構並發布匿名揭弊系統
Authors: Daniel Hugenroth, Luke Hoyland, Sam Cutler, Alastair Beresford
University of Cambridge, The Guardian

SecureDrop Next Generation: Lessons from a Decade of Deployment
SecureDrop 次世代：十年部署經驗之回顧與反思
Authors: Giulio Berra, Felix Linker, Luca Maier, Cory Francis Myers, Kenneth G. Paterson, Rowen Shane, Shannon Veitch
Freedom of the Press Foundation, ETH Zurich

Real-World Steganography Against Content-Based Censorship
對抗現代通訊軟體內容審查之實務隱寫術
Authors: Boya Wang, Markus Schiffermüller, Klim Kireev, Carmela Troncoso
MPI-SP, EPFL, TU Graz

At-Compromise Security: The Case for Alert Blindness
帳號遭入侵後的安全性：警報盲點之探討
Authors: Martin R. Albrecht, Simone Colombo, Benjamin Dowling, Rikke Bjerg Jensen
King's College London, Royal Holloway

10:20 - 10:50

Coffee Break｜茶敘

10:50 - 11:20

Invited Talk｜特邀演講

11:20 - 12:00

Session: Login Security
登入安全

Chair: TBD

TBA
Authors: Matilda Backendal, Kenneth Paterson, Matteo Scarlata, Giovanni Torrisi
ETH Zurich

Improving Account Security for Victims of Account Compromise through Client-Side Access Logging
強化帳號受駭者之安全性
Authors: Carolina Ortega Pérez, Paul Gerhart, Alaa Daffalla, Thomas Ristenpart
Cornell University, TU Wien, Cornell Tech

12:00 - 13:30

Lunch｜午餐

3/11 (Wed) 星期三

09:00 - 10:20

Session: Privacy-Enhancing Technologies
隱私強化技術

Chair: TBD

Counter Galois Onion (CGO): Fast Non-Malleable Onion Encryption for Tor
CGO：Tor 之高速不可延展洋蔥加密
Authors: Jean Paul Degabriele, Alessandro Melloni, Jean-Pierre Münch, Martijn Stam
Technology Innovation Institute, Simula UiB, TU Darmstadt

Let's Aggregate? Towards making private telemetry as ubiquitous as TLS
Let's Aggregate？讓隱私遙測如 TLS 般普及
Authors: Ryan Lehmkuhl, Henry Corrigan-Gibbs, Emma Dauterman, David J. Wu
MIT, Stanford, UT Austin

How Private Can Private Advertising Really Be?
「隱私廣告」究竟能有多隱私？
Authors: Kyle Hogan, Alishah Chator, Gabriel Kaptchuk, Mayank Varia, Srinivas Devadas
MIT, Baruch College, UMD, Boston University

Sprinkle Differential Privacy on a Bit of Everything
將差分隱私融入多元應用
Authors: Daniel Pöllmann, Tianxin Tang
ETH Zurich, Eindhoven University of Technology

10:20 - 10:50

Coffee Break｜茶敘

10:50 - 11:30

Session: Bluetooth-based Protocols
藍牙協定安全

Chair: TBD

Security of Bluetooth: A Cryptographic View on Analyzing a Leviathan
藍牙安全性：以密碼學視角剖析龐然巨獸
Authors: Marc Fischlin, Olga Sanina
Technische Universität Darmstadt

The Landscape of Offline Finding Protocols: Privacy, Safety, Problems
離線尋找協定之全景：隱私、安全與挑戰
Authors: Akshaya Kumar, Carolina Ortega Perez, Anna Raymaker, Joseph Jaeger, Michael Specter, Thomas Ristenpart
Georgia Institute of Technology, Cornell University, Cornell Tech

11:30 - 12:00

Lightning Talks｜閃電秀

Chair: Nigel Smart

12:00 - 13:20

Lunch｜午餐

13:20 - 13:50

Invited Talk｜特邀演講

14:00 - 15:10

Session: Verification and Testing
驗證與測試

Chair: TBD

Finding Bugs and Features Using Cryptographically-Informed Functional Testing
運用具密碼學資訊之功能性測試尋找漏洞與特徵

Authors: Giacomo Fenzi, Jan Gilcher, Fernando Virdia

EPFL, ETH Zurich, University of Surrey

Formosa Crypto: End-to-End Formally Verified Crypto Software
Formosa Crypto：端對端形式化驗證之密碼軟體

Authors: José Bacelar Almeida, Gustavo Xavier, Delerue Marinho Alves, Santiago Arranz-Olmos, Manuel Barbosa, Francisca Barros, Gilles Barthe, Lionel Blatter, Chitchanok Chuengsatiansup, Ignacio Cuevas, François Dupressoir, Luís Esquível, Andreas Hülsing, Benjamin Grégoire, Ruben Gonzalez, Jan Jancar, Vincent Hwang, Vincent Laporte, Jean-Christophe Léchenet, Ting-han Lim, Cameron Low, Tiago Oliveira, Hugo Pacheco, Swarn Priya, Miguel Quaresma, Rolfe Schmidt, Peter Schwabe, Antoine Séré, Basavesh Ammanaghatta Shivakumar, Pierre-Yves Strub, Lucas Tabary-Maujean, Yuval Yarom, Zhiyuan Zhang, Jieyu Zheng

Universidade do Minho, PQShield, MPI-SP, INESC TEC, IMDEA, Signal, Neodyme AG, et al.

mlkem-native: a Unified, Fast and Verified ML-KEM Library
mlkem-native：整合式、高效能且可驗證之 ML-KEM 函式庫

Authors: Hanno Becker, Matthias J. Kannwischer, Dusan Kostic, John Harrison, Rod Chapman

Amazon Web Services, Chelpis

Formally Verifying Circuits for Zero Knowledge Proofs
零知識證明電路之形式化驗證

Authors: Alex Ozdemir, Shankara Pailoor

MPI-SP / Georgia Tech, Veridise

Compositional Formal Verification of SNARKs with ArkLib
基於 ArkLib 之 SNARKs 組合式形式化驗證

Authors: Quang Dao, Alexander Hicks, Devon Tuma, Julian Sutherland, Katerina Hristova, Frantisek Silvasi, Ilia Vlasov, Chung Thai Nguyen

CMU, Ethereum Foundation, Nethermind, Imperial College London

15:10 - 15:40

Coffee Break｜茶敘

15:40 - 16:10

TBA (待定)

16:10 - 18:15

Session: Hardware
硬體安全

Chair: TBD

Migrating a Silicon Root of Trust to Post-Quantum Crypto
晶片信任根至後量子密碼之遷移

Authors: Amin Abdulrahman, Andrew 'bunnie' Huang, Evan Apinis, Matthias J. Kannwischer, Ruben Niederhagen, Felix Oberhansl, Hoang Nguyen, Hien Pham, Jade Philipoom, Dominic Rizzo, Robert Schilling, Peter Schwabe, Tobias Stelzer, Augustine Tang, Andreas Zankl

MPI-SP, zeroRISC, Chelpis, Academia Sinica, Fraunhofer AISEC, Rivos Inc.

Chypnosis: Undervolting-based Static Side-channel Attacks
Chypnosis：基於降壓之靜態旁路攻擊

Authors: Kyle Mitard, Saleh Khalaj Monfared, Fatemeh Khojasteh, Dana Robert Dumitru, Yuval Yarom, Shahin Tajik

WPI, Ruhr University Bochum, University of Adelaide

TEE.fail: Breaking Trusted Execution Environments via Memory Bus Interposition
TEE.fail：藉由記憶體匯流排攔截攻破可信執行環境

Authors: Jalen Chuang, Alex Seto, Nicolas Berrios, Stephan van Schaik, Christina Garman, Daniel Genkin

Georgia Tech, Purdue University, van Schaik LLC

Kerckhoff's Principle in Practice: Addressing Security by Obscurity in Secure Hardware
Kerckhoffs 原則之實踐：解決安全硬體中之隱匿式安全

Authors: Vojtech Suchanek, Jan Jancar, Jan Kvapil, Petr Svenda, Łukasz Chmielewski

Masaryk University

Encryption in the Microarchitectural World
微架構層級之加密技術

Authors: Ping-Lun Wang, Fraser Brown, Riccardo Paccagnella, Eyal Ronen, Riad S. Wahby, Yuval Yarom

CMU, Tel Aviv University, Ruhr University Bochum

18:45 - 20:45

Reception｜歡迎晚宴

13:30 - 14:50

Session: Post-Quantum Constructions
後量子建構

Chair: TBD

Keeping up with the KEMbiners
KEM 組合器之最新演進

Authors: Kathrin Hövelmanns, Deirdre Connolly, Andreas Hülsing, Stavros Kousidis, Matthias Meijers

Eindhoven University, Selkie Cryptography, BSI

Efficient Threshold ML-DSA
高效門檻式 ML-DSA

Authors: Guilhem Niot, Thomas Espitau, Thomas Prest, Rafael del Pino, Sofía Celi

PQShield, Univ Rennes, Brave, University of Bristol

XHMQV: Better Efficiency and Stronger Security for Signal's Initial Handshake based on HMQV
XHMQV：提升 Signal 初始握手之效率與安全性

Authors: Rune Fiedler, Felix Günther, Jiaxin Pan, Runzhi Zeng, Rolfe Schmidt

ETH Zurich, IBM Research, University of Kassel, Signal Messenger

A Call to Action: Transitioning Signal's Private Group System to Quantum-Safe
行動呼籲：將 Signal 私密群組系統遷移至量子安全架構

Authors: Graeme Connell, Sebastian Faller, Felix Günther, Julia Hesse, Vadim Lyubashevsky, Rolfe Schmidt

Signal Messenger, IBM Research, ETH Zurich

14:55 - 15:35

Session: Cloud Encryption
雲端加密

End-to-End Encrypted Collaborative Documents
端對端加密之協作文件

Authors: Christian Knabenhans, Zayd Maradni, Carmela Troncoso

EPFL, MPI-SWS, MPI-SP

Random-Access AEAD for Fast Lightweight Online Encryption
用於快速輕量級線上加密之隨機存取 AEAD

Authors: Andres Fabrega, Greg Rubin, Julia Len, Thomas Ristenpart

Cornell University, Snowflake, UNC Chapel Hill, Cornell Tech

15:35 - 16:05

Coffee Break｜茶敘

16:05 - 17:35

Session: Cryptography and Society
密碼學與社會

Chair: TBD

What is cryptography hiding from itself?
密碼學對自身隱瞞了什麼？

Authors: Diego F. Aranha, Nikolas Melissaris

Aarhus University, IRIF

"Security vs. Interoperability": Real Tension or False Dichotomy?
「安全性與互通性」：真實張力或錯誤二分法？

Authors: Daji Landis, Sunoo Park, Elettra Bietti

NYU, Northeastern University

CRA and Cryptography: The Story Thus Far
歐盟網路韌性法案 (CRA) 與密碼學：目前為止的故事

Authors: Markku-Juhani Saarinen

Tampere University

When Proofs Aren't Enough: Putting Cryptosystems in Context
當證明不足時：將密碼系統置於脈絡中檢視

Authors: Gabriel Kaptchuk, Ran Canetti, Julie Ha

UMD, Boston University

Building Cryptographic Intellectual Infrastructure Where It Means Most...
在最需要之處建立密碼學知識基礎設施：黎巴嫩危機後之應用密碼學教學經驗

Authors: Nadim Kobeissi

American University of Beirut

17:45 - 19:45

Light Food and Beer｜輕食與啤酒之夜

13:50 - 14:45

Session: PKI｜公鑰基礎設施

Chair: TBD

(Dis)patches from the Web PKI: Fina, Static CT, MTC, and PLANTS
Web PKI 之修補與訊息：Fina、靜態 CT、MTC 與 PLANTS

Authors: Luke Valenta, David Benjamin, Matthew McPherrin, Filippo Valsorda

Cloudflare, Inc., Google, Let's Encrypt

Private Key Leaks in the Wild: Insights from Certificate Transparency
野外私鑰外洩：來自憑證透明性之洞見

Authors: Guillaume VALADON, Gaëtan FERRY, David TAO, Philippe BONEFF

GitGuardian, Google

Self-Auditable Key Transparency at Scale
大規模可自我稽核之金鑰透明性

Authors: Hossein Hafezi, Alireza Shirzad, Benedikt Bunz, Joseph Bonneu

New York University, University of Pennsylvania

14:45 - 15:15

Coffee Break｜茶敘

15:15 - 16:10

Session: Secure Channels in Practice
實務安全通道

Chair: TBD

DTLS-SRTP: The Protocol Everyone is Using But Nobody is Checking
DTLS-SRTP：廣泛應用卻乏人檢視之協定

Authors: Martin Bach, Jean Paul Degabriele, Vukašin Karadžić, Lukas Knittel, Robert Merget

TU Darmstadt, Technology Innovation Institute, Ruhr-University Bochum

The widespread popularity of insecure proprietary network encryption in the Android ecosystem
Android 生態系中不安全私有網路加密之泛濫

Authors: Mona Wang, Jeffrey Knockel, Zoë Reichert, Prateek Mittal, Jonathan Mayer

UC Berkeley, The Citizen Lab, Princeton University

Lessons Learned from Cryptography Shortcuts on the Example of TLS Session Tickets
TLS Session Tickets 密碼學實作捷徑之教訓

Authors: Sven Hebrok, Tim Leonhard Storm, Felix Matthias Cramer, Maximilian Radoy, Simon Nachtigall, Marcel Maehren, Nurullah Erinola, Juraj Somorovsky, Robert Merget, Jörg Schwenk

Paderborn University, achelos GmbH, Ruhr University Bochum, Technology Innovation Institute

16:10 - 16:30

Closing Remarks｜閉幕致詞

RWC 2026 General Chair