第37回

NIAT2011 FDTC2011 CHES2011

NIAT2011：2011年9月25日～27日　FDTC2011：2011年9月28日
CHES2011：2011年9月28日～10月1日
東大寺総合文化センター・エルトピア奈良（奈良県奈良市）

坂根広史 NIST／産業技術総合研究所（NIAT2011）　**伊豆哲也** （株）富士通研究所（FDTC2011）
猪俣敦夫 奈良先端科学技術大学院大学（CHES2011）

暗号にかかわる3つの国際会議

2011年9月25日～10月1日の約1週間，奈良市内で暗号デバイスに関する3つの国際会議NIAT2011，FDTC2011，CHES2011が開催された．それぞれ，非破壊の物理攻撃，フォルト攻撃耐性，暗号ハードウェア全般を主テーマとしたものである．本稿では，会議の概要と現地の様子を運営側の視点から紹介する．


NIAT2011 レセプション風景

NIAT2011

米国標準技術研究所（NIST：National Institute of Standards and Technology）は，米国連邦政府機関が使用する暗号製品のセキュリティ要件を標準規格FIPS 140-2として制定し，それに従って暗号モジュール認証プログラム（CMVP）を運用している．また，米国内にとどまらず，FIPS 140-2をベースに国際規格ISO/IEC 19790も標準化されている．近年，電力や電磁波等を測定・解析して暗号デバイス内部の秘密情報を盗み出すサイドチャネル攻撃など，破壊を伴わない物理的な攻撃（非侵襲攻撃：Non-Invasive Attack）の研究が進み，それらを新たなセキュリティ要件として取り入れる必要性が高まっている．

そこで，NISTと（独）産業技術総合研究所（以下，産総研）は，NIAT2011（Non-Invasive Attack Testing Workshop）を共同で開催し，最新研究成果の集約と学術界とCMVP試験機関の間の情報交換を図った．実行委員長にはNISTのRandall Easter氏，プログラム委員長には産総研の佐藤証氏が就いた．佐藤氏はこの業界における我が国のトップリーダー的研究者であり，この研究分野で標準実験環境として広く活用されているサイドチャネル攻撃評価ボードSASEBO（Side-channel Attack Standard Evaluation BOard）の開発を主導している．本ワークショップはFDTC2011およびCHES2011の協力により併設開催を実現したことで，非侵襲攻撃という特殊テーマ，そして開催告知の遅れにもかかわらず，14カ国から70名を超える参加者を集めることができた．

NIST CMVP Director, Randall Easter 氏


FDTC2011 会場風景

初日（9 月 25 日）夕刻からのレセプションは，100 年以上の歴史を持つ格式の高い奈良ホテルで行われた．CMVP 認証業務で日々忙殺されがちな NIST の関係者はアカデミアとの接点が少ないながらも，和やかな雰囲気のうちに宴は終了した．

翌日からの 2 日間の本セッションは東大寺総合文化センターで行われた．Easter 氏と佐藤氏の開会の辞に続き，Easter 氏による FIPS と CMVP の紹介が行われた．技術論文は，新たな攻撃・防御手法の研究，試験手法や解析ツールなど 12 件が採択され，日本からは東北大学の電力線へノイズを混入するフォルト攻撃の研究と，産総研による SASEBO の最新の実験環境整備の発表が行われた．このほか，フランスの Telecom ParisTech 大学主催の電力解析攻撃の技術を競う DPA Contest，そして試験機関やツールベンダによる試験項目と自動化に関する 2 件のパネルディスカッションも催された．

本ワークショップは，2005 年に NIST が開催した Physical Security Testing Workshop を継承したもので，前述のとおり試験機関側と学術界の間での密な情報交換を 6 年振りに図ったものである．学術界は，自分たちの研究が試験・認証の現場でどう活かされ，また現場で何が要求されているかを知る，一方，試験機関側は攻撃や対策の最前線の研究に触れるよい機会となった．参加者の注目は各技術セッションのなかでも特に試験手法に集まり，試験の再現性確保やコスト低減の重要性が試験機関側から指摘され，統計的検定の導入を具体的に検討したいという声が聞かれた．

ワークショップは，「暗号モジュールの非侵襲攻撃に対する再現性のある試験手法・評価基準の策定，試験ツールの開発，および認証手順などについて，本ワークショップのような場で多くのアイディアを持ち寄って取り組んでいくことが重要である」と Easter 氏が結んで閉幕した．

NIAT2011 発表論文は下記の URL から入手可能である．

http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/

FDTC2011

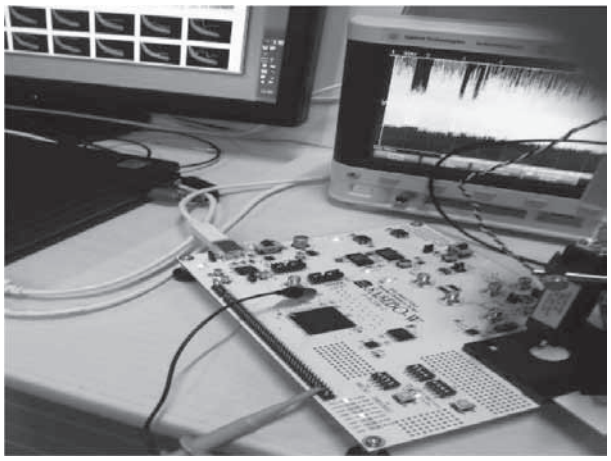
NIAT2011 に引き続き 9 月 28 日に，暗号デバイスへのフォルト攻撃耐性に関する国際会議 FDTC2011（8th International Workshop on Fault Diagnosis and Tolerance in Cryptography）が，エルトピア奈良にて開催された．フォルト攻撃とは，たとえば暗号デバイスの電圧やクロックを急激に変化させて誤動作を誘発し，その振舞いを解析して秘密情報を特定する攻撃である．2004 年より関連が非常に強い CHES と連続して開催されており，本年度は過去最大の 116 人の参加者を集めることができた．

FDTC2011 のプログラム委員長は，Telecom ParisTech 大学の Sylvain Guilley 氏と NTT の高

コラム

“I”見聞録

FDTC2011 会場


サイドチャネル評価ボード SASEBO-W

橋順子氏が，実行委員長はイタリア Politecnico di Milano 大学の Luca Breveglieri 氏と米国 Massachusetts 大学の Israel Koren 氏が就いた．また，現地実行委員は，富士通研究所の酒見由美氏と伊豆哲也氏が担当した．

一般論文 10 件の発表と 2 件の招待講演があった．1 件目の招待講演では，ベルギーの Katholieke Universiteit Leuven の Ingrid Verbauwhede 氏が，楕円曲線暗号を例にフォルト攻撃の攻撃と対策の分類法を紹介した．その中で，対策コストの見極めが設計者にとって重要であると指摘された．2 件目はオランダ Brightsight 社の Rob Bekkers 氏によるもので，フォルト攻撃の実例が紹介され，暗号デバイスにとって現実的な脅威であることが示された．1 日のみの開催ながらも，大変活発な議論が行われたワークショップであった．

FDTC2011 の予稿集は IEEE Computer Society から，また講演資料は下記の URL から入手可能である．
http://conferenze.dei.polimi.it/FDTC11/program.html

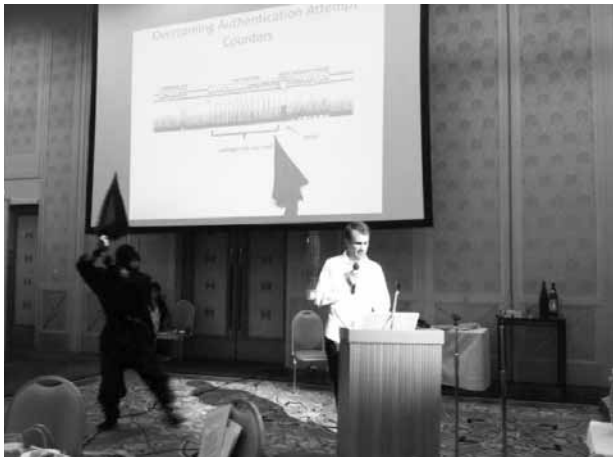
CHES2011

暗号のハードウェアにおけるトップカンファレンスである CHES2011（13th International Workshop on Cryptographic Hardware and Embedded Systems）が，9 月 28 日から 10 月 1 日に東大寺総合文化センターをメイン会場に開催された．CHES は 1999 年に始まり今年で 13 回目，日本での開催は 2006 年の横浜に続き，今回で 2 回目となる．プログラム委員長は，Katholieke Universiteit Leuven の Bart Preneel 氏と九州大学の高木剛氏が，ポスターセッション委員長に産総研の堀洋平氏が，実行委員長は産総研の佐藤証氏がそれぞれ就いた．佐藤氏は CHES の国内誘致に尽力され，暗号ハードウェアに関する著名な学会では佐藤氏らが開発した SASEBO を利用した研究が多数見受けられる．

本年は東京での開催を予定していたが，震災後，急遽，会場を奈良に移したため参加者の減少が危惧されていた．しかし，最終的にはこれまでの 2 番目の記録となる 316 名（国内 101 名）という多数の研究者を迎えることができた．さらに，世界各国からの励ましと暖かい支援を受け，例年の 3 倍を超える 24 の団体・組織からのスポンサー支援をいただいた．論文発表および招待講演のほか，企業展示およびデモ・ポスター発表の会場も用意され，コーヒーブレーク中に Cryptography Research 社および Riscure 社による非侵襲攻撃に関するデモなども行われた．

論文は，26 カ国から 119 件（国内 10 件）の投稿の中から 32 件（国内 2 件）が採択された．最優秀論文賞には，オーストリアの Graz University of Technology の Michael Hutter 氏，Erich Wenger 氏による「Fast Multi-precision Multiplication


企業ブースおよびデモ展示会場


CHES2011 ランプセッション

for Public-Key Cryptography on Embedded Microprocessors」が選ばれた．RSA 暗号や楕円曲線暗号等の公開鍵暗号の実装のコアとなる多倍長乗算に対して，優れたオペランドのキャッシング手法を提案し，高い性能向上を実現したものである．

その他の発表について以下に簡単にまとめる．

- FPGA ☆1 実装
  FPGA に特化した高速かつ効率的な実装等．
- AES ☆2
  より高速な AES のハードウェア実装等．
- 楕円曲線暗号
  より高速かつ安全な楕円曲線上の演算器等．
- Lattices
  計算負荷の指標として注目されているクラウドや GPGPU ☆3 を用いた計算手法等．
- サイドチャネル攻撃
  研究から実用化に向けた評価環境・手法等．
- Fault Attack
  計算誤りを利用した解析攻撃等．
- Lightweight symmetric algorithm
  超軽量なブロック暗号やハッシュ関数等．
- PUF（Physical Unclonable Function）
  偽造防止技術として注目される，デバイスの物理特性のばらつきを利用した個体識別法等．
- 公開鍵暗号系
  比較的計算負荷が高いとされる Pairing 暗号の高速ハードウェア実装等．
- ハッシュ関数
  FPGA 上に実装したハッシュ関数の性能評価等．

招待講演は，インテル社の Ernie Brickell 氏による「Technologies to Improve Platform Security」，NTT の富永哲欣氏による「Standardization Works for Security regarding the Electromagnetic Environment」であった．毎年，CHES では暗号デバイスの小型・省電力化・高速化，安全性評価などの研究が多いが，暗号実装だけでなく，PUF などの複製困難な物理特性や，ハードウェアウィルスと言える Hardware Trojan の研究が活発化すると見られている．

3 日目の夜は恒例のランプセッションがホテル日航奈良でのバンケットの中で開かれ，数々のユニークな発表が行われた．また，持ち時間をオーバーした発表者に忍者が襲いかかるといった演出もあり，非常に賑やかなセッションとなった．

CHES2011 のレギュラーセッションとランプセッションのスライドは，それぞれ下記の URL から入手可能である．

☆1 FPGA とは，Field Programmable Gate Array の略で，書き換え可能な半導体デバイスである．
☆2 AES とは，Advanced Encryption Standard の略で，現在最も多く使われている共通鍵暗号の 1 つである．
☆3 GPGPU とは，General Purpose computing on Graphics Processing Unit の略で，高い演算能力を持つ演算装置である．

東大寺総合文化センター金鐘ホール


参加者同士の交流の一場面

http://www.iacr.org/workshops/ches/ches2011/program.html
http://www.iacr.org/workshops/ches/ches2011/rump.html

奈良での開催にあたり

国際会議では，本セッションの運営に加え，開催地の魅力をアピールすることも重要で，今回は奈良ならではのイベントを多数盛り込んだ．NIAT2011とCHES2011の会場の東大寺総合文化センターは，国宝を多数展示した博物館のグランドオープンを間近に控え，追い込みの工事が行われる中で特別に利用させていただいた．センターは南大門に隣接する旧東大寺学園の跡地の歴史的にも価値のある場所に建てられ，最新の映像・音響設備を有した美しい木目を基調とする金鐘ホールは，参加者に高く評価された．

CHES2011のレセプションは，奈良国立博物館の中のレストランを利用し，昼食は東大寺門前の「夢風ひろば」を貸し切り，飲食店ごとに工夫を凝らした奈良の食材をふんだんに盛り込んだ和食を参加者が自由に選べるようにした．コーヒーブレークは奈良ホテルや地元のパティスリーに協力いただき，豪華なデザートや季節の果実などが提供された．また，ボランティアガイドによるウォーキングツアーや平城京跡訪問，早朝の鹿寄せなど，多数のイベントも参加者の満足度を大きく向上させた．今回の成功により，これまで欧米が中心であったCHESは，アジアを含めた3地域で順次開催される運びとなった．

奈良公園周辺の複数の施設を中心に奈良の特色を存分に盛り込んだ国際会議は，海外の参加者だけでなく，ご協力いただいた地元の方々にも大変喜んで迎えられた．奈良市では毎年，多くの国際会議が開かれているが，今回のように3つの専門的な国際会議が1週間という長期にわたって開催される大きなイベントは初の試みであり，地元新聞でも今後の大型国際会議誘致のモデルケースとしてアピールしていくべきと高く評価された．

（2011年11月2日受付）

坂根広史（正会員）｜hsakane@nist.gov, hsakane@ni.aist.go.jp
米国標準技術研究所 客員研究員．（独）産業技術総合研究所情報セキュリティ研究センター主任研究員，博士（工学）．

伊豆哲也（正会員）｜izu@labs.fujitsu.com
（株）富士通研究所ソフトウェアシステム研究所セキュアコンピューティング研究部主任研究員，博士（工学）．

猪俣敦夫（正会員）｜atsuo@is.aist-nara.ac.jp
奈良先端科学技術大学院大学総合情報基盤センター（情報科学研究科兼務）准教授，博士（情報科学）．