# 米山　一樹（Kazuki Yoneyama）

所属（Domain）　情報科学領域（Domain of Computer and Information Sciences）
・博士後期課程社会インフラシステム科学専攻（Major in Society's Infrastructure Systems Science）

●研究テーマ（Research theme）

①形式手法を用いた安全性自動検証の研究
（Automated security verification based on formal methods）

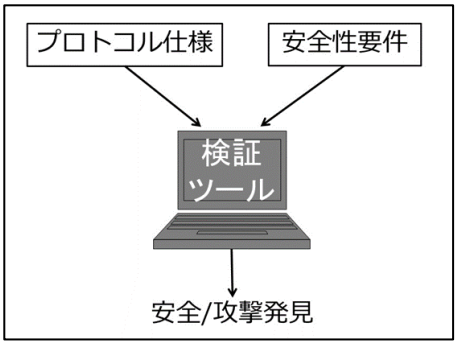
②暗号プロトコルの設計、安全性評価、実装
（Design, security evaluation, and implementation of cryptographic protocols）

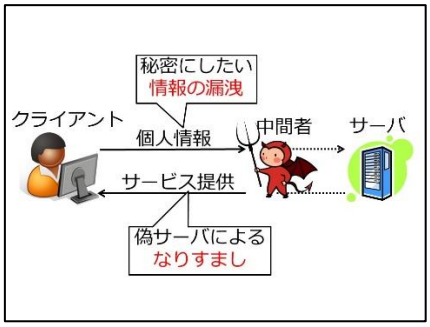
③次世代暗号に資する基礎技術の追求
（Fundamental primitives for next-generation cryptography）

---

①クラウドや電子商取引などの便利なサービスを安心して利用するためには安全性がきちんと保証されている必要があります。しかし、安全性の検証は非専門家には困難です。システム仕様と検証したい安全性を数理的に記述することで、誰でも計算機を用いて安全性を自動検証することができるツールを研究しています。

In order to use useful web-services like the cloud computing and the e-commerce, it is necessary to guarantee security. However, the verification of security of such systems is difficult for non-specialist. In our laboratory, we study automated security verification tools on computers by describing the system specification and the security requirement mathematically.



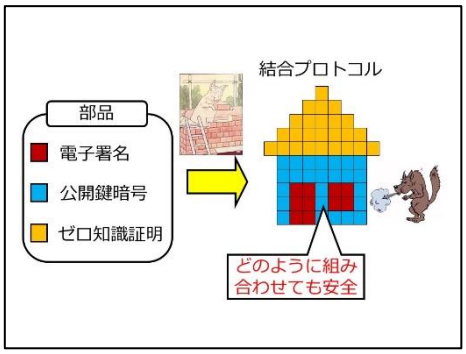




②認証鍵交換（SSL/TLSなど）、電子投票、暗号通貨（Bitcoin）など、暗号技術を応用して様々な機能を安全に実現する暗号プロトコルに関する研究を進めています。新しいプロトコルの設計や実装実験、既存方式への攻撃（安全性評価）などに取り組んでいます。

By using cryptographic primitives, we study cryptographic protocols which securely achieve various functions like authenticated key exchange (e.g., SSL/TLS), e-voting, and cryptocurrencies. Our project includes designs of new cryptographic protocols, implementation experiments, and security evaluation of known protocols.

③次世代の暗号技術に求められる要件を見出し、それを実現するための新しい基礎技術や概念の提案を行っています。例えば、IoTなど新たな環境に適した暗号技術、想定外の状況（ヒューマンエラーや誤った運用）が起こっても最低限の安全性を保持、いかなる外部プロトコルと組み合わせても安全、などの特徴を持った暗号技術が挙げられます。

We study requirements for next-generation cryptography, and propose new primitive and notion to achieve such requirements. Our project includes cryptography for IoT environments, fail-safe cryptography (e.g., human-error, and improper use), and security-preserving composable protocols.




---

| | |
|---|---|
| キーワード（Keyword） | 形式手法（Formal methods）安全性検証（Security verification）<br>暗号理論（Cryptography） |
| 専門分野（Specialized Field） | 情報セキュリティ（Information security） |
| 共同研究可能技術（Possible Technology of Cooperative research） | 情報セキュリティ基盤技術<br>（Foundation of information security） |
| 関連論文・特許情報 website<br>（Related articles･patent information） | https://info.ibaraki.ac.jp/Profiles/28/0002747/profile.html |
| 研究室URL（Lab. URL） | http://www.yoneyama-lab.jp/ |
| E-mail | kazuki.yoneyama.sec@vc.ibaraki.ac.jp |