Supervisor(s)	Rishiraj Bhattacharyya
Project title	Security Proofs of Practical Cryptosystems
Funding availability *(select one)*	Directly funded PhD project (UK students only)
Name of funding awarded	PhD studentship

Project description

The security of a modern cryptographic construction is proved via a reduction from the hardness of solving some well-studied mathematical problems. There is, however, a substantial gap between security proved in theory and security achieved in practice.

In general theoretical analysis, the integrity of algorithms and the secrecy of the keys are always assumed to hold. In fact, guarantees of semantic security of many popular and widely deployed cryptosystems may break down if the adversary sees encryptions of the secret key.

In practice, on the other hand, the algorithms may be tampered with to modify a few bits of the keys, commonly known as the *related-key attacks*, or to leak encryptions of (some function of) the secret key, commonly known as the *key-dependent message attacks*. The adversary may even tamper with the algorithms in such a way that a small fraction of outputs is subverted, a generalisation of the *kleptographic attacks*. A line of work has considered the security of cryptosystems in the presence of such key-dependent messages or subverted algorithms. However, practical and deployable cryptographic solutions against such active attacks are still missing for many fundamental problems.

The objective of the project is to analyse the security of deployed cryptosystems along with designing new ones that can withstand key-correlated attacks and general kleptographic attacks. In particular, we wish to address the following.

1. Efficient and secure authentication mechanisms against key-correlated and misuse-resistant attacks. The project will analyse deployed and standardised MAC (message authentication code)

algorithms and authenticated encryptions in the light of simultaneous related-key and key-dependent message attacks.

2. Design principles of key encapsulation mechanisms resisting kleptographic attack. Recent kleptographic attacks against the key encapsulation mechanisms have shown a significant vulnerability of the hybrid encryption protocols. We shall explore whether the widely deployed Fujisaki-Okamoto transformation could be salvaged to achieve security against such kleptographic attacks.

2. Secure modes of operation of hash functions and block ciphers resisting kleptographic attack. Security of modes of operations of hash functions and block ciphers often require the underlying primitive to behave like a random function or a random permutation. We shall analyse the security of these modes when the underlying primitives are modified via a kleptographic attack.

Funding notes

The candidate is expected to have a postgraduate degree or equivalent. Experience in Cryptography is beneficial but not mandatory.

We want our PhD student cohorts to reflect our diverse society. UoB is therefore committed to widening the diversity of our PhD student cohorts. UoB studentships are open to all and we particularly welcome applications from under-represented groups, including, but not limited to BAME, disabled and neuro-diverse candidates. We also welcome applications for part-time study.

The position offered is for three and a half years full-time study. The current (2022-23) value of the award is stipend; £17,668 pa; tuition fee: £4,596 pa. Awards are usually incremented on 1 October each following year.

Eligibility: First or Upper Second Class Honours undergraduate degree and/or postgraduate degree with Distinction (or an international equivalent). We also consider applicants from diverse backgrounds that have provided them with equally rich relevant experience and knowledge. Full-time and part-time study modes are available.

If your first language is not English and you have not studied in an English-speaking country, you will have to provide an English language qualification.

We will consider applications from students wishing to start during the 2022-23 academic year or who wish to begin their studies in autumn 2023.

Contact for enquiries

Name of supervisor	Rishiraj Bhattacharyya
Web page	https://rishirajb.github.io/
Email address	r.bhattacharyya@bham.ac.uk
Phone number	0121 414 2653