Cliptography: Post-Snowden Cryptography

Qiang Tang
New Jersey Institute of Technology
qiang@njit.edu

Moti Yung
Snap. Inc, & Columbia University
moti@cs.columbia.edu

ABSTRACT

This tutorial covers a systematic overview of *kleptography*: stealing information subliminally from black-box cryptographic implementations; and *cliptography*: defending mechanisms that clip the power of kleptographic attacks via specification re-designs (without altering the underlying algorithms).

Despite the laudatory history of development of modern cryptography, applying cryptographic tools to reliably provide security and privacy in practice is notoriously difficult. One fundamental practical challenge, guaranteeing security and privacy without explicit trust in the algorithms and implementations that underlie basic security infrastructure, remains. While the dangers of entertaining adversarial implementation of cryptographic primitives seem obvious, the ramifications of such attacks are surprisingly dire: it turns out that – in wide generality – adversarial implementations of cryptographic (both deterministic and randomized) algorithms may leak private information while producing output that is statistically indistinguishable from that of a faithful implementation. Such attacks were formally studied in Kleptography.

Snowden revelations has shown us how security and privacy can be lost at a very large scale even when traditional cryptography seems to be used to protect Internet communication, when Kleptography was not taken into consideration.

We first explain how the above-mentioned Kleptographic attacks can be carried out in various settings. We then introduce several simple but rigorous immunizing strategies that were inspired by folklore practical wisdoms to protect different algorithms from implementation subversion. Those strategies can be applied to ensure security of most of the fundamental cryptographic primitives such as PRG, digital signatures, public key encryptions against kleptographic attacks when they are implemented accordingly. Our new design principles may suggest new standardization methods that help reducing the threats of subverted implementation. We also hope our tutorial to stimulate a community-wise efforts to further tackle the fundamental challenge mentioned at the beginning.

CCS CONCEPTS

• **Security and privacy → Cryptography**;

KEYWORDS

Kleptography, Cliptography, Cryptography, Backdoor resistance, Implementation subversion, Steganography

CCS '17, October 30-November 3, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-4946-8/17/10.
https://doi.org/10.1145/3133956.3136065

1 INTRODUCTION

In 1996, Young and Yung introduced the concept of *kleptography*, the study of cryptographic attacks in the setting where the fundamental cryptographic algorithms themselves are subject to adversarial subversion [13, 14]. Recent events have created a renewed urgency around the study of security in the kleptographic setting. In September 2013, the New York Times [10] reported the existence of a secret National Security Agency SIGINT Enabling Project designed to "make [systems] exploitable through SIGINT collection" by inserting vulnerabilities, collecting target network data, and influencing policies, standards and specifications for commercial public-key technologies. Beyond the immediate privacy concerns created by this activity, these efforts raise fears that cryptographic "backdoors" might be exploited by unauthorized parties. Indeed, there exists circumstantial evidence that this may have happened: In December 2015, Juniper Networks published a security advisory announcing that an undocumented NSA-designed random number generator within NetScreen Virtual Private Networking (VPN) devices had been modified by a state-sponsored attacker. This sophisticated modification allowed for passive decryption of all VPN connections terminated by a NetScreen device [3, 15].

The existence of well-funded kleptographic programs harms Internet security by reducing trust in cryptographic systems. However, this concern pales in comparison to the possibility that kleptographic efforts will be widely adopted and re-purposed by other threat actors, potentially rendering much of our infrastructure nonviable. In the context of cryptography, the technical ramifications of algorithm subversion are particularly concerning: this is because—in wide generality—*adversarial implementations of cryptographic algorithms may leak private information while producing output that is statistically and computationally indistinguishable from that of a faithful implementation* [1, 2, 7, 13]. This has implications for both cryptographic security and user privacy in general. Identifying these vulnerabilities and developing techniques to mitigate them has become a priority for the applied cryptographic research community [3–6, 8–12].

The goal of this tutorial is to give the audience a systematic overview of the kleptographic attacks, and more importantly, how recent progress of cliptography may provide robust security of cryptographic tools in the post-Snowden era. As the inventor of kleptography, Dr. Yung presents the evolution of kleptography from both theoretica perspectives and real-world attack examples. As the main contributor of cliptography, Dr. Tang explains how to leverage conventional security wisdom, such as nothing-up-my-sleeve numbers, and modular design principle, to re-consider the specification design of cryptographic tools to provide rigorous protection against kleptographic attacks. As a new direction, the tutorial covers both theoretical and practical open problems in the field, and also introduce some other security problems that are

motivated by the new methodologies we have developed along the way. The outline of the tutorial is as follows:

- Introduction to Kleptography, including subliminal channel attacks in subverted algorithms, with real-world examples.
- Formal definitional framework of Cliptography.
- Mitigating the damage of subliminal channel attacks, using PRG as an example; defending mechanism that destroys the subliminal channel in subverted randomized algorithm, using encryption as an example; and self-correcting random oracles (hash functions) and its application to subversion-resistant digital signatures.
- Major remaining obstacles, important future directions in the field, and open problems motivated by our framework in related areas.

2 INTENDED AUDIENCES

All security researchers from academia, standardization organization and industry are welcome. We aim to provide (1.) introduction of Kleptography and Cliptography as a scientific subjects to academic researchers and discussion of important theoretical and practical questions; (2.) suggestions of specification design to standardization agencies that may alleviate subversion threats and such kind of undetectable attacks in deployed cryptographic tools; (3.) ideas for industry researchers, whose companies export or sell devices that may not be trusted, to re-consider the architecture of their device to convince the customers that their products can be used as faithfully implemented.

3 PREREQUISITE KNOWLEDGE

Basic knowledge about security notions of the standard cryptographic tools are helpful. Advanced knowledge of steganography, randomness extractor or self-correcting programs are not required, they will be explained in an intuitive level and the tutorial is mostly self-contained.

4 SPEAKER BIOGRAPHY

Qiang Tang is an assistant professor at the Department of Computer Science at New Jersey Institute of Technology (NJIT). Before joining NJIT, he was a postdoctoral associate at Cornell University and was also affiliated with the Initiative of CryptoCurrency and Contracts (IC3). He obtained his Ph.D from the University of Connecticut with a Taylor Booth Scholarship. He also held visiting researcher positions at various institutes including the University of Wisconsin, Madison, NTT Research, Tokyo and the University of Athens, Greece. His research interests are applied and theoretical cryptography, privacy and computer security. In particular, in accountability, post-Snowden cryptography, and blockchain technology. He has made contributions on using cryptocurrency to deter copyright infringement and to enforce key management policy, re-designing cryptographic specifications to defend against implementation subversion, as well as information theoretical security.

Moti Yung is a computer scientist whose main interests are in cryptography, security, and privacy. He is currently with Snap. Inc, and has been holding adjunct professor appointments at Columbia University where he has co-advised several Ph.D. students. He was with IBM, CertCo, RSA Lab, and Google. Dr. Yung made extensive contributions on the foundation of modern cryptography as well as innovative secure industrial technology within actual large scale systems, including the Greek National Lottery system, the security and privacy aspects of Google's global systems such as the Ad Exchange (ADX) and the ephemeral ID efforts for Google's BLE beacons, and Snap's "my eyes only memories" cloud security. Also, his invention of Cryptovirology (including Kleptography) envisioned the explosion of ransomware, and algorithm subversion on crypto systems and standards such as the Dual_EC DRNG subversion. Dr. Yung has been giving distinguished and keynote speeches at numerous top-tier crypto/security/distributed computing conferences. He is a Fellow of ACM, IEEE, IACR, and EATCS.

REFERENCES

[1] Mihir Bellare, Joseph Jaeger, and Daniel Kane. 2015. Mass-surveillance without the State: Strongly Undetectable Algorithm-Substitution Attacks. In *ACM CCS 15*, Indrajit Ray, Ninghui Li, and Christopher Kruegel: (Eds.). ACM Press, 1431–1440.

[2] Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. 2014. Security of Symmetric Encryption against Mass Surveillance. In *CRYPTO 2014, Part I (LNCS)*, Juan A. Garay and Rosario Gennaro (Eds.), Vol. 8616. Springer, Heidelberg, 1–19. https://doi.org/10.1007/978-3-662-44371-2_1

[3] Stephen Checkoway, Shaanan Cohney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Maskiewicz, Eric Rescorla, Hovav Shacham, and Ralf-Philipp Weinmann. 2016. A Systematic Analysis of the Juniper Dual EC Incident. In *Proceedings of ACM CCS 2016*. Full version available at http://eprint.iacr.org/2016/376.

[4] Stephen Checkoway, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, Hovav Shacham, and Matthew Fredrikson. 2014. On the Practical Exploitability of Dual EC in TLS Implementations. In *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014*. 319–335.

[5] Jean Paul Degabriele, Kenneth G. Paterson, Jacob C. N. Schuldt, and Joanne Woodage. 2016. Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results. In *CRYPTO 2016, Part I (LNCS)*, Matthew Robshaw and Jonathan Katz (Eds.), Vol. 9814. Springer, Heidelberg, 403–432. https://doi.org/10.1007/978-3-662-53018-4_15

[6] Yevgeniy Dodis, Ilya Mironov, and Noah Stephens-Davidowitz. 2016. Message Transmission with Reverse Firewalls—Secure Communication on Corrupted Machines. In *CRYPTO 2016, Part I (LNCS)*, Matthew Robshaw and Jonathan Katz (Eds.), Vol. 9814. Springer, Heidelberg, 341–372. https://doi.org/10.1007/978-3-662-53018-4_13

[7] Nicholas J. Hopper, John Langford, and Luis von Ahn. 2002. Provably Secure Steganography. In *CRYPTO 2002 (LNCS)*, Moti Yung (Ed.), Vol. 2442. Springer, Heidelberg, 77–92.

[8] Jeff Larson, Nicole Perlroth, and Scott Shane. 2013. Revealed: The NSA's secret campaign to crack, undermine internet security. Pro-Publica. (2013). http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[9] Ilya Mironov and Noah Stephens-Davidowitz. 2015. Cryptographic Reverse Firewalls. In *EUROCRYPT 2015, Part II (LNCS)*, Elisabeth Oswald and Marc Fischlin (Eds.), Vol. 9057. Springer, Heidelberg, 657–686. https://doi.org/10.1007/978-3-662-46803-6_22

[10] Nicole Perlroth, Jeff Larson, and Scott Shane. 2013. N.S.A. able to foil basic safeguards of privacy on web. The New York Times. (2013). http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.

[11] Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. 2016. Cliptography: Clipping the Power of Kleptographic Attacks. In *ASIACRYPT 2016, Part II (LNCS)*, Jung Hee Cheon and Tsuyoshi Takagi (Eds.), Vol. 10032. Springer, Heidelberg, 34–64. https://doi.org/10.1007/978-3-662-53890-6_2

[12] Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. 2017. Generic Semantic Security against a Kleptographic Adversary. In *Proceedings of the 24nd ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, October 30-November 4, 2017*.

[13] Adam Young and Moti Yung. 1996. The Dark Side of "Black-Box" Cryptography, or: Should We Trust Capstone?. In *CRYPTO'96 (LNCS)*, Neal Koblitz (Ed.), Vol. 1109. Springer, Heidelberg, 89–103.

[14] Adam Young and Moti Yung. 1997. Kleptography: Using Cryptography Against Cryptography. In *EUROCRYPT'97 (LNCS)*, Walter Fumy (Ed.), Vol. 1233. Springer, Heidelberg, 62–74.

[15] Kim Zetter. 2015. Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors. (December 2015).