Università degli Studi di Salerno

.DIEM

**Dipartimento di Ingegneria dell'Informazione
ed Elettrica e Matematica Applicata**

Dottorato di Ricerca in Ingegneria dell'Informazione
Ciclo 35

TESI DI DOTTORATO / PH.D. THESIS

Provable Security: the Good, the Bad, and the Ugly

GENNARO AVITABILE

SUPERVISOR: **PROF. IVAN VISCONTI**

PHD PROGRAM DIRECTOR: **PROF. PASQUALE CHIACCHIO**

Anno 2023

Abstract Inglese

Since modern cryptography was born around the late 1970s, a myriad of cryptographic constructions and protocols have been proposed. The field quickly developed into a science whose results have had great impact on people's lives. Some examples are secure communication over the internet, distributed digital currencies, electronic elections, and more. Such a progress was boosted by the diffusion of a methodology called the *provable security* paradigm. It provides a precise framework to formalize and prove the security of a cryptographic construction. Provable security is based on three pillars: (i) definitions, (ii) assumptions, and (iii) proofs. The definition states when the system can be considered secure and what are the capabilities of an adversary attacking the construction. The proof demonstrates that the construction satisfies the definition, assuming that all the assumptions hold. Provable security provides objective ways to compare different constructions, as well as more reassurances on their security. However, it is not devoid of pitfalls. For example, a definition might not model the real world correctly, and thus any proof that a construction satisfies such definition would be worthless in practice. Furthermore, it might happen that security proofs containing errors will not get detected because of the complexity (or oversimplification) of the proof itself.

This thesis explores such multifaceted nature of provable security through two parts. In the first part, we focus on the recent development of automatic contact tracing systems (ACTs). When the COVID-19 pandemic hit, automatic contact tracing was proposed as an effective way to slow the spread of the virus down by detecting likely infected people earlier with the help of technology. Citizens would use a smartphone app, and users at risk of being infected - as

they were in proximity of an infected individual - would be notified by the smartphone. Due to the widespread adoption that was expected for ACTs, privacy and integrity were both key concerns.

The DP3T team proposed an ACT [3] which was shortly after implemented and deployed over smartphones by Apple and Google with the name of GAEN. Informal security assessments were performed by the DP3T team, including wrong or misleading claims about the privacy and integrity guarantees that ACTs could provide. Several attacks to DP3T pointed out by other researchers were deemed as inherent by analyses that considered very powerful adversaries. However, the concrete attacks could have been carried out by much weaker adversaries to which other ACTs could have possibly resisted. We model these and novel integrity and privacy attacks with a focus on mass surveillance and analyze the security of DP3T w.r.t. them. We propose two new ACTs named Pronto-C2 and Pronto-B2, which encompass DP3T/GAEN both in terms of privacy and integrity guarantees. Our ACTs also demonstrate that such attacks are not inherent. Finally, we consider the terrorist attack conjectured by Vaudenay [4]. It involves a malicious party (i.e., the terrorist) bribing infected users to inject false alerts in the ACT. We show how to concretely implement automated terrorist attacks to jeopardize the integrity of GAEN.

In the second part of this thesis, we provide novel contributions in the area of threshold cryptography. In particular, we focus on proofs over threshold relations, threshold ring signatures, and extendable threshold ring signatures. We point out several fallacies in the usage of the provable security paradigm in prior works published at major cryptography conferences [1,2]. Such issues include errors in the security proofs as well as inadequate definitions where the real-world system's requirements and adversary's capabilities are not matched by the definition. We overcome such issues proposing stronger definitions, new constructions, and revisited security proofs. Additionally, our new constructions improve the previous ones in terms of efficiency, security, and/or features.

Abstract Italiano

Da quando la crittografia moderna è nata intorno alla fine degli anni '70, sono state proposte una miriade di costruzioni e protocolli crittografici. Il campo si è rapidamente sviluppato in una scienza i cui risultati hanno avuto un grande impatto sulla vita delle persone. Alcuni esempi sono la comunicazione sicura su Internet, le valute digitali distribuite, le elezioni elettroniche e altro ancora. Tale progresso è stato favorito dalla diffusione di una metodologia chiamata paradigma della *provable security* (sicurezza dimostrabile). Esso fornisce un quadro preciso per formalizzare e dimostrare la sicurezza di una costruzione crittografica. La sicurezza dimostrabile si basa su tre pilastri: (i) definizioni, (ii) assunzioni e (iii) prove. La definizione indica quando il sistema può essere considerato sicuro e quali sono le capacità di un avversario che attacca la costruzione. La dimostrazione dimostra che la costruzione soddisfa la definizione, assumendo che tutte le assunzioni valgano. La sicurezza dimostrabile fornisce modi oggettivi per confrontare diverse costruzioni, nonché maggiori rassicurazioni sulla loro sicurezza. Tuttavia, non è priva di insidie. Ad esempio, una definizione potrebbe non modellare correttamente il mondo reale, e quindi qualsiasi prova che una costruzione soddisfi tale definizione sarebbe in pratica priva di valore. Inoltre, potrebbe accadere che prove di sicurezza contenenti errori non vengano rilevate a causa della complessità (o dell'eccessiva semplificazione) della prova stessa.

Questa tesi esplora la natura multiforme della sicurezza dimostrabile in due parti. Nella prima parte, ci concentriamo sul recente sviluppo dei sistemi automatici di tracciamento dei contatti (ACT). Quando la pandemia di COVID-19 ha colpito, il tracciamento automatico dei contatti è stato proposto come un modo efficace per ral-

lentare la diffusione del virus rilevando tempestivamente le persone probabilmente infette con l'aiuto della tecnologia. I cittadini utilizzano un'app per smartphone e gli utenti a rischio di essere infettati - in quanto si trovavano in prossimità di un individuo infetto - vengono avvisati dallo smartphone. Data la gran diffusione prevista per gli ACT, la privacy e l'integrità sono preoccupazioni cruciali.

Il team DP3T ha proposto un ACT [3] che poco dopo è stato implementato e distribuito su smartphone da Apple e Google con il nome di GAEN. Il team DP3T ha eseguito valutazioni informali della sicurezza, comprese affermazioni errate o fuorvianti sulle garanzie di privacy e integrità che gli ACT possono fornire. Diversi attacchi a DP3T segnalati da altri ricercatori sono stati ritenuti intrinseci da analisi che consideravano avversari molto potenti. Tuttavia, gli attacchi concreti avrebbero potuto essere effettuati da avversari molto più deboli a cui altri ACT avrebbero potuto opporre resistenza. In questa tesi, modelliamo questi e nuovi attacchi all'integrità e alla privacy con particolare attenzione alla sorveglianza di massa e analizziamo la sicurezza di DP3T rispetto essi. Proponiamo due nuovi ACT denominati Pronto-C2 e Pronto-B2, che superano DP3T/GAEN sia in termini di garanzie privacy che di integrità. I nostri ACT dimostrano anche che tali attacchi non sono inerenti. Consideriamo infine il *terrorist attack* ipotizzato da Vaudenay [4]. Esso coinvolge una parte malintenzionata (ovvero il terrorista) che corrompe gli utenti infetti per generare falsi allarmi nell'ACT. Mostriamo come implementare concretamente versioni automatizzate di tale attacco per mettere a repentaglio l'integrità di GAEN.

Nella seconda parte di questa tesi, forniamo nuovi contributi nell'area della *threshold cryptography* (crittografia a soglia). In particolare, ci concentriamo sulle proofs over threshold relations (prove su relazioni a soglia), sulle threshold ring signatures (firme ad anello con soglia) e sulle extendable threshold ring signatures (firme ad con soglia estendibili). Segnaliamo diversi errori nell'uso del paradigma di sicurezza dimostrabile in lavori precedenti pubblicati alle principali conferenze di crittografia [1, 2]. Tali problemi includono errori nelle prove di sicurezza e definizioni inadeguate in cui i requisiti del sistema del mondo reale e le capacità dell'avversario non rispecchiano la definizione. Superiamo tali problemi proponendo definizioni più forti, nuove costruzioni

e prove di sicurezza riviste. Inoltre, le nostre nuove costruzioni migliorano le precedenti in termini di efficienza, sicurezza e/o funzionalità.

Bibliography

[1] Diego F. Aranha, Mathias Hall-Andersen, Anca Nitulescu, Elena Pagnin, and Sophia Yakoubov. Count Me In! Extendability for Threshold Ring Signatures. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022: 25th International Conference on Theory and Practice of Public Key Cryptography, Part II*, volume 13178 of *Lecture Notes in Computer Science*, pages 379–406. Springer, Heidelberg, Germany, 2022.

[2] Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and Gabriel Kaptchuk. Stacking sigmas: A framework to compose Σ-protocols for disjunctions. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022, Part II*, volume 13276 of *Lecture Notes in Computer Science*, pages 458–487, Trondheim, Norway, May 30 – June 3, 2022. Springer, Heidelberg, Germany.

[3] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James R. Larus, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth G. Paterson, Srdjan Capkun, David A. Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel P. Smart, Aysajan Abidin, Seda Gurses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, and José Pereira. Decentralized privacy-preserving proximity tracing. 2020. https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

[4] Serge Vaudenay. Centralized or decentralized? the contact tracing dilemma. Cryptology ePrint Archive, Paper 2020/531, 2020. https://eprint.iacr.org/2020/531.