1.	Record Nr.	UNINA9910484766303321
	Titolo	Advances in Cryptology – EUROCRYPT 2006 : 25th International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings / / edited by Serge Vaudenay
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
	ISBN	3-540-34547-7
	Edizione	[1st ed. 2006.]
	Descrizione fisica	1 online resource (XIV, 622 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 4004
	Altri autori (Persone)	VaudenaySerge
	Disciplina	005.82
	Soggetti	Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Computer science - Mathematics Discrete mathematics Electronic data processing - Management Cryptology Computer Communication Networks Operating Systems Discrete Mathematics in Computer Science IT Operations
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Cryptanalysis -- Security Analysis of the Strong Diffie-Hellman Problem -- Cryptography in Theory and Practice: The Case of Encryption in IPsec -- Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects -- Invited Talk I -- Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry’s Crypt -- Cryptography Meets Humans -- Hiding Secret Points Amidst Chaff -- Parallel and Concurrent Security of the HB and HB?+? Protocols -- Polling with Physical

Sommario/riassunto

The 2006 edition of the Eurocrypt conference was held in St. Petersburg,Russia from May 28 to June 1, 2006. It was the 25th Eurocrypt conference. Eurocrypt is sponsored by the International Association for Cryptologic Research (IACR). Eurocrypt2006waschairedbyAnatolyLebedev,andIhadtheprivilegetochair the Program Committee. Eurocrypt collected 198 submissions on November 21, 2005. The Program Committee carried out a thorough review process. In total, 863 review reports were written by renowned experts, Program Committee members as well as external referees. Online discussions led to 1,114 additional discussion messages and about 1,000 emails. The review process was run using e-mail and the iChair software by Thomas Baign` eres and Matthieu Finiasz. Every submitted paper received at least three review reports. The Program Committee had a meeting in Lausanne on February 4, 2006. We selected 33 papers, noti?ed acceptance or rejection to the authors, and had a cheese fondue. Authors were then invited to revise their submission. The present proceedings include all the revised papers. Due to time constraints the revised versions could not be reviewed again. We delivered a “Eurocrypt Best Paper Award.” The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize - cellence in the cryptographic research ?elds. Committee members were invited to nominate papers for this award. A poll then yielded a clear majority. This year, we were pleased to deliver the Eurocrypt Best Paper Award to Phong Q.